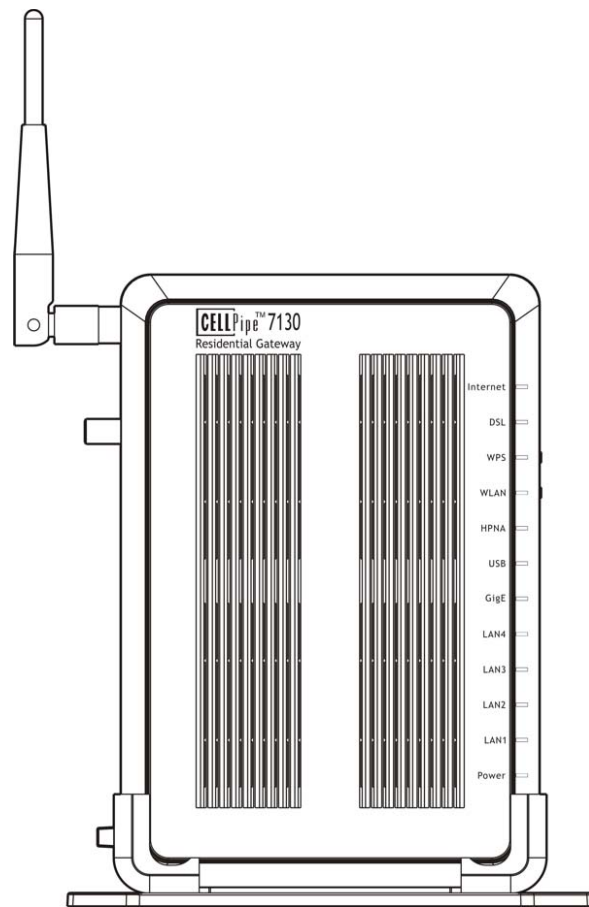


CellPipe 7130 RG

Wireless router with VDSL2/ADSL broadband access

User's Guide



Default Login Details

IP Address	http://192.168.1.1
User Name	admin root tech
Password	telus

Firmware Version 0.0.02.GEN

About This User's Guide

Intended Audience

This manual is intended for people who want to configure the CellPipe 7130 RG using the web configurator.

Related Documentation

Quick Start Guide

The Quick Start Guide is designed to help you get up and running right away. It contains information on setting up your network and configuring for Internet access.

Document Conventions

Warnings and Notes

These are how warnings and notes are shown in this User's Guide.

Warnings tell you about things that could harm you or your device.




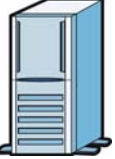
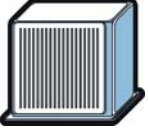




Note: Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

Syntax Conventions

- The CellPipe 7130 RG may be referred to as the "CellPipe 7130 RG", the "device", the "system" or the "product" in this User's Guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the "enter" or "return" key on your keyboard.
- "Enter" means for you to type one or more characters and then press the [ENTER] key. "Select" or "choose" means for you to use one of the predefined choices.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Maintenance > Log > Log Setting** means you first click **Maintenance** in the navigation panel, then the **Log** sub menu and finally the **Log Setting** tab to get to that screen.
- Units of measurement may denote the "metric" value or the "scientific" value. For example, "k" for kilo may denote "1000" or "1024", "M" for mega may denote "1000000" or "1048576" and so on.
- "e.g.," is a shorthand for "for instance", and "i.e.," means "that is" or "in other words".

Icons Used in Figures

Figures in this User's Guide may use the following generic icons. The CellPipe 7130 RG icon is not an exact representation of your device.

CellPipe 7130 RG 	Computer 	Notebook computer 
Server 	DSLAM 	Firewall 
Telephone 	Switch 	Router 

Safety Warnings

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device.
- Connect the power adaptor or cord to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the device and the power source.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Use only No. 26 AWG (American Wire Gauge) or larger telecommunication line cord.
- Antenna Warning! This device meets ETSI and FCC certification requirements when using the included antenna(s). Only use the included antenna(s).
- If you wall mount your device, make sure that no electrical lines, gas or water pipes will be damaged.

Your product is marked with this symbol, which is known as the WEEE mark. WEEE stands for Waste Electronics and Electrical Equipment. It means that used electrical and electronic products should not be mixed with general waste. Used electrical and electronic equipment should be treated separately.



Contents Overview

User's Guide	17
Introducing the CellPipe 7130 RG	19
Tutorials	29
Introducing the Web Configurator	83
Technical Reference	89
Status Screens	91
WAN Setup	101
LAN Setup	131
Wireless LAN	139
Network Address Translation (NAT)	171
File Sharing	181
Media Server	187
Firewall	191
Certificate	197
Static Route	209
Policy Forwarding	213
RIP	217
Quality of Service (QoS)	219
Dynamic DNS Setup	237
Remote Management	239
Universal Plug-and-Play (UPnP)	245
Parental Control	257
IGMP	261
System Settings	267
Logs	271
Tools	275
Diagnostic	283
Troubleshooting	289
Product Specifications	297

Table of Contents

About This User's Guide	3
Document Conventions.....	4
Safety Warnings.....	6
Contents Overview	7
Table of Contents.....	9
Part I: User's Guide.....	17
Chapter 1	
Introducing the CellPipe 7130 RG	19
1.1 Overview	19
1.2 Ways to Manage the CellPipe 7130 RG	19
1.3 Good Habits for Managing the CellPipe 7130 RG	20
1.4 Applications for the CellPipe 7130 RG	20
1.4.1 Internet Access	20
1.4.2 HomePNA	22
1.4.3 CellPipe 7130 RG's USB Support	22
1.5 Hardware Connections	24
1.6 LEDs (Lights)	26
1.7 The RESET Button	28
1.8 The WLAN Button	28
1.9 The WPS Button	28
Chapter 2	
Tutorials	29
2.1 Overview	29
2.2 How to Set up a Wireless Network	29
2.2.1 Example Parameters	30
2.2.2 Configuring the AP	30
2.2.3 Configuring the Wireless Client	32
2.3 HomePNA Example Setup	39
2.4 How to Use ATM QoS with Multiple PVCs	40
2.4.1 Configuring PVCs	41
2.4.2 Setting Policy Forwarding	51

2.5 How to Allow Out-of-band Remote Management from the WAN	53
2.5.1 Configuring Multiple WAN Connections	54
2.5.2 Configuring Remote Management	64
2.5.3 Testing the Connection	65
2.6 Using the Media Server Feature	65
2.6.1 Configuring the CellPipe 7130 RG	65
2.6.2 Using Windows Media Player	66
2.6.3 Using a Digital Media Adapter	69
2.7 Using the File Sharing Feature	71
2.7.1 Set Up File Sharing	71
2.7.2 Access Your Shared Files From a Computer	71
2.8 Setting Up NAT Port Forwarding	72
2.9 Configuring Static Route for Routing to Another Network	74
2.10 Configuring QoS Queue and Class Setup	77
2.11 Access the CellPipe 7130 RG Using DDNS	80
2.11.1 Registering a DDNS Account on www.dyndns.org	81
2.11.2 Configuring DDNS on Your CellPipe 7130 RG	81
2.11.3 Testing the DDNS Setting	82
Chapter 3	
Introducing the Web Configurator	83
3.1 Overview	83
3.2 User Levels	83
3.2.1 Accessing the Web Configurator	84
3.3 Web Configurator Main Screen	85
3.3.1 Navigation Panel	86
3.3.2 Main Window	88
3.3.3 Status Bar	88
Part II: Technical Reference	89
Chapter 4	
Status Screens	91
4.1 Overview	91
4.2 Status Screen	91
4.2.1 WAN Service Statistics	94
4.2.2 Route Info	96
4.2.3 WLAN Station List	97
4.2.4 LAN Statistics	98
4.2.5 Client List	99

Chapter 5	
WAN Setup.....	101
5.1 Overview	101
5.1.1 What You Can Do in this Chapter	102
5.2 What You Need to Know	103
5.3 Before You Begin	104
5.4 The Mode Screen	104
5.5 The Connect Screen	105
5.5.1 Connect Configuration	107
5.6 The Services Screen	110
5.6.1 WAN Connection Configuration	112
5.7 Technical Reference	123
Chapter 6	
LAN Setup.....	131
6.1 Overview	131
6.1.1 What You Can Do in this Chapter	131
6.2 What You Need To Know	132
6.3 The LAN IP Screen	133
6.4 Technical Reference	134
Chapter 7	
Wireless LAN.....	139
7.1 Overview	139
7.1.1 What You Can Do in this Chapter	139
7.2 What You Need to Know	140
7.3 Before You Begin	142
7.4 The General Screen	143
7.4.1 No Security	145
7.4.2 WEP Encryption	146
7.4.3 WPA(2)-PSK	147
7.4.4 WPA(2) Authentication	148
7.4.5 MAC Filter	150
7.4.6 Adding a New MAC Filtering Rule	151
7.5 The More AP Screen	152
7.5.1 More AP Edit	153
7.6 The WPS Screen	153
7.7 The WPS Station Screen	155
7.8 The WDS Screen	156
7.9 The Advanced Setup Screen	158
7.10 Technical Reference	159
7.10.1 Wireless Network Overview	160
7.10.2 Additional Wireless Terms	161

7.10.3 Wireless Security Overview	161
7.10.4 WiFi Protected Setup	163
Chapter 8	
Network Address Translation (NAT).....	171
8.1 Overview	171
8.1.1 What You Can Do in this Chapter	171
8.2 What You Need to Know	171
8.3 The Port Forwarding Screen	172
8.3.1 The Port Forwarding Edit Screen	175
8.4 The DMZ Host Screen	176
8.5 The ALG Screen	177
8.6 Technical Reference	178
Chapter 9	
File Sharing	181
9.1 Overview	181
9.1.1 What You Can Do in this chapter	181
9.1.2 What You Need to Know About File-Sharing	182
9.1.3 Before You Begin	183
9.2 The Server Settings Screen	183
9.2.1 Example of Accessing Your Shared Files From a Computer	184
Chapter 10	
Media Server.....	187
10.1 Overview	187
10.1.1 What You Can Do in this chapter	188
10.1.2 Before You Begin	188
10.2 The Media Server Configuration Screen	188
10.3 The Remove Disk Safely Screen	189
Chapter 11	
Firewall.....	191
11.1 Overview	191
11.1.1 What You Can Do in this Chapter	191
11.2 What You Need to Know	191
11.3 The Firewall Screen	193
11.3.1 Creating Incoming Firewall Rules	194
11.4 The DoS Screen	195
Chapter 12	
Certificate	197
12.1 Overview	197

12.1.1 What You Can Do in this Chapter	197
12.2 What You Need to Know	197
12.3 The Local Certificates Screen	198
12.3.1 Create Certificate Request	199
12.3.2 Import Certificate	200
12.3.3 Certificate Details	202
12.3.4 Load Signed Certificate	203
12.4 The Trusted CA Screen	204
12.4.1 View Trusted CA Certificate	206
12.4.2 Import Trusted CA Certificate	207
Chapter 13	
Static Route	209
13.1 Overview	209
13.1.1 What You Can Do in this Chapter	209
13.2 The Static Route Screen	210
13.2.1 Static Route Edit	211
Chapter 14	
Policy Forwarding	213
14.1 Overview	213
14.1.1 What You Can Do in this Chapter	213
14.2 The Static Route Screen	213
14.2.1 Policy Forwarding Setup	214
Chapter 15	
RIP	217
15.1 Overview	217
15.1.1 What You Can Do in this Chapter	217
15.2 The RIP Screen	217
Chapter 16	
Quality of Service (QoS)	219
16.1 Overview	219
16.1.1 QoS Overview	220
16.1.2 What You Can Do in this Chapter	220
16.2 What You Need to Know	220
16.3 The Quality of Service General Screen	221
16.4 The Queue Setup Screen	222
16.4.1 Adding a QoS Queue	224
16.5 The Class Setup Screen	225
16.5.1 QoS Class Edit	227
16.6 The Policer Setup Screen	231

16.6.1 Policer Setup Edit	232
16.7 The QoS Monitor Screen	233
16.8 Technical Reference	233
Chapter 17	
Dynamic DNS Setup	237
17.1 Overview	237
17.1.1 What You Can Do in this Chapter	237
17.2 What You Need To Know	237
17.3 The Dynamic DNS Screen	238
Chapter 18	
Remote Management.....	239
18.1 Overview	239
18.1.1 What You Can Do in this Chapter	239
18.2 The TR-069 Screen	239
18.3 The TR-064 Screen	241
18.4 The Service Control Screen	242
18.5 The IP Address Screen	243
18.5.1 Adding an IP Address	244
Chapter 19	
Universal Plug-and-Play (UPnP).....	245
19.1 Overview	245
19.1.1 What You Can Do in this Chapter	245
19.2 What You Need to Know	245
19.3 The UPnP Screen	246
19.4 Installing UPnP in Windows Example	247
19.5 Using UPnP in Windows XP Example	250
Chapter 20	
Parental Control	257
20.1 Overview	257
20.1.1 What You Can Do in this Chapter	257
20.2 The Time Restriction Screen	257
20.2.1 Adding a Schedule	258
20.3 The Content Filter Screen	259
20.3.1 Adding Filter Rule	260
Chapter 21	
IGMP.....	261
21.1 Overview	261
21.1.1 What You Can Do in this Chapter	261

21.1.2 What You Need to Know	261
21.2 The IGMP Screen	263
21.3 Interface Source Configuration	265
21.3.1 Add/Edit IGMP Source	266
Chapter 22	
System Settings.....	267
22.1 Overview	267
22.1.1 What You Can Do in this Chapter	267
22.2 The General Screen	267
22.3 The Time Setting Screen	269
Chapter 23	
Logs	271
23.1 Overview	271
23.1.1 What You Can Do in this Chapter	271
23.2 The View Log Screen	271
23.3 The Log Settings Screen	272
Chapter 24	
Tools.....	275
24.1 Overview	275
24.1.1 What You Can Do in this Chapter	275
24.2 The Firmware Screen	276
24.3 The Configuration Screen	278
24.4 The Restart Screen	280
Chapter 25	
Diagnostic.....	283
25.1 Overview	283
25.1.1 What You Can Do in this Chapter	283
25.2 What You Need to Know	283
25.3 The General Diagnostic Screen	284
25.4 The 802.1ag Screen	285
25.5 The OAM Ping Test Screen	287
Chapter 26	
Troubleshooting.....	289
26.1 Power, Hardware Connections, and LEDs	289
26.2 CellPipe 7130 RG Access and Login	290
26.3 Internet Access	292
26.4 USB Device Connection	295
26.5 Wireless LAN Troubleshooting	295

Chapter 27
Product Specifications 297

 27.1 Hardware Specifications 297

 27.2 Firmware Specifications 298

Appendix A Network Troubleshooting 305

Appendix B Setting Up Your Computer's IP Address 321

Appendix C Pop-up Windows, JavaScripts and Java Permissions 351

Appendix D IP Addresses and Subnetting 361

Appendix E Wireless LANs 373

Appendix F Common Services 389

Appendix G Legal Information 393

Index 397

PART I

User's Guide

Introducing the CellPipe 7130 RG

1.1 Overview

The CellPipe 7130 RG is a wireless VDSL2+ router and Gigabit Ethernet gateway with Home Phoneline Networking Alliance (HPNA) capability. It has a DSL port for super-fast Internet access over analog (POTS) telephone lines and a Giga Ethernet port high-speed Internet access through cable. The CellPipe 7130 RG supports both Packet Transfer Mode (PTM) and Asynchronous Transfer Mode (ATM). It is backward compatible with ADSL, ADSL2 and ADSL2+ in case VDSL is not available.

**Only use firmware for your CellPipe 7130 RG's specific model.
Refer to the label on the bottom of your CellPipe 7130 RG.**

The CellPipe 7130 RG has a a USB port used to share files via a USB memory stick or a USB hard drive. The CellPipe 7130 RG can also function as a media server to let other users in the network open media files stored in the USB device.

See [Chapter 27 on page 297](#) for a full list of features.

1.2 Ways to Manage the CellPipe 7130 RG

Use any of the following methods to manage the CellPipe 7130 RG.

- Web Configurator. This is recommended for everyday management of the CellPipe 7130 RG using a (supported) web browser.
- TR-069. This is an auto-configuration server used to remotely configure your device.

1.3 Good Habits for Managing the CellPipe 7130 RG

Do the following things regularly to make the CellPipe 7130 RG more secure and to manage the CellPipe 7130 RG more effectively.

- Change the password. Use a password that's not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the password and put it in a safe place.
- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the device becomes unstable or even crashes. If you forget your password, you will have to reset the CellPipe 7130 RG to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the CellPipe 7130 RG. You could simply restore your last configuration.

1.4 Applications for the CellPipe 7130 RG

Here are some example uses for which the CellPipe 7130 RG is well suited.

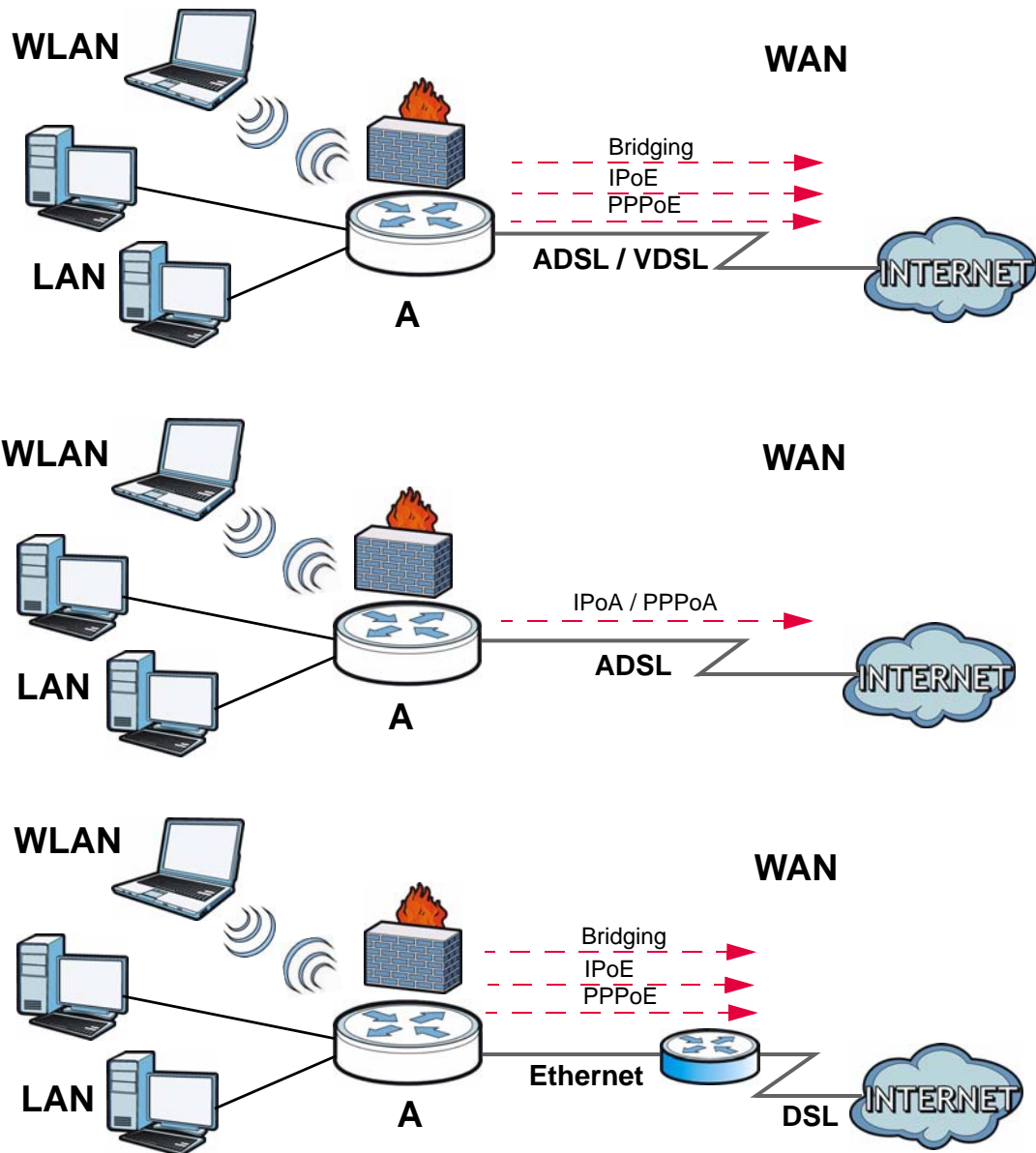
1.4.1 Internet Access

Your CellPipe 7130 RG provides shared Internet access by connecting the DSL port to the **DSL** or **MODEM** jack on a splitter or your telephone jack. You can have up to eight WAN services over one ADSL, VDSL or Ethernet WAN line. The CellPipe 7130 RG cannot work in ADSL, VDSL and Ethernet WAN mode at the same time.

Note: The ADSL, VDSL and Ethernet WAN lines share the same eight WAN **Connect** (or layer-2) interfaces that you configure in the CellPipe 7130 RG. Refer to [Section 5.5 on page 105](#) for the **WAN > Connect** screen.

Computers can connect to the CellPipe 7130 RG's LAN ports (or wirelessly).

Figure 1 CellPipe 7130 RG's Internet Access Application



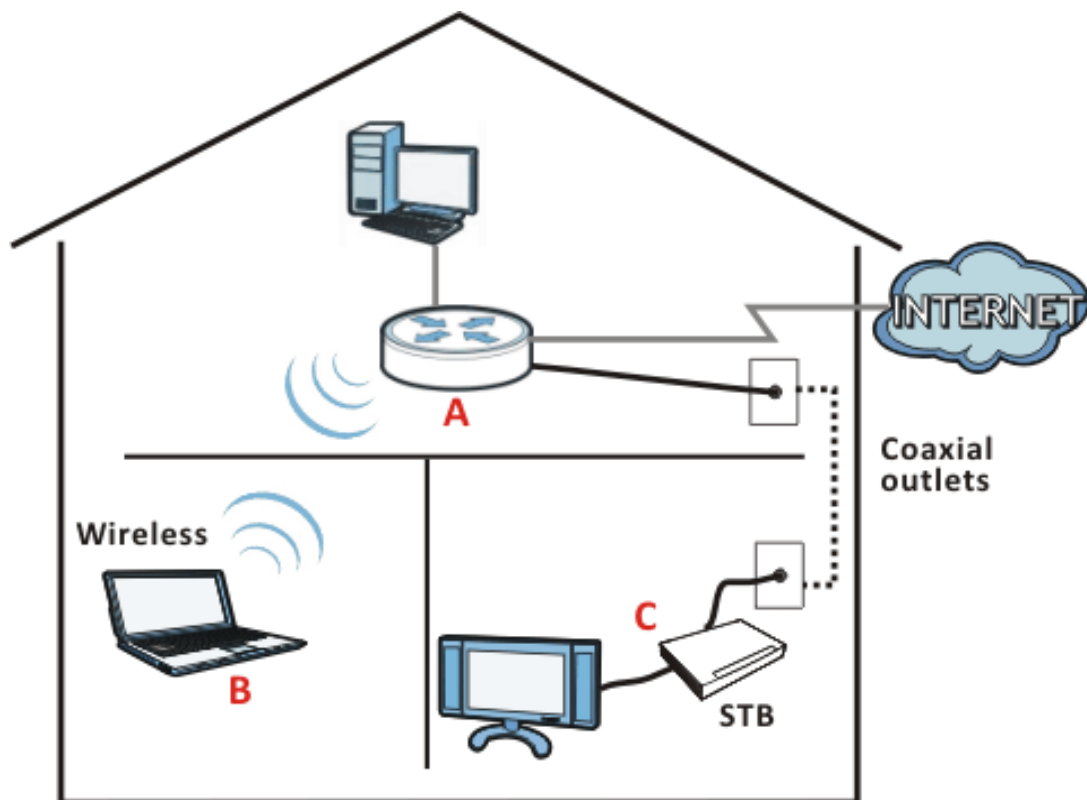
You can also configure IP filtering on the CellPipe 7130 RG for secure Internet access. When the IP filter is on, all incoming traffic from the Internet to your network is blocked by default unless it is initiated from your network. This means that probes from the outside to your network are not allowed, but you can safely browse the Internet and download files.

1.4.2 HomePNA

The CellPipe 7130 RG complies with HomePNA (Home Phoneline Networking Alliance, also known as HPNA) 3.1, a home networking technology for carrying data over existing coaxial cables and telephone wiring.

The figure below shows your CellPipe 7130 RG (**A**) connecting to a phone line outlet for DSL Internet access and a coaxial outlet to relay Internet connectivity to other coaxial outlets in the building. The laptop (**B**) connects wirelessly to the CellPipe 7130 RG. The set-up box (**C**) connects into a coaxial outlet in another part of the house for access to online videos.

Figure 2 HomePNA Application



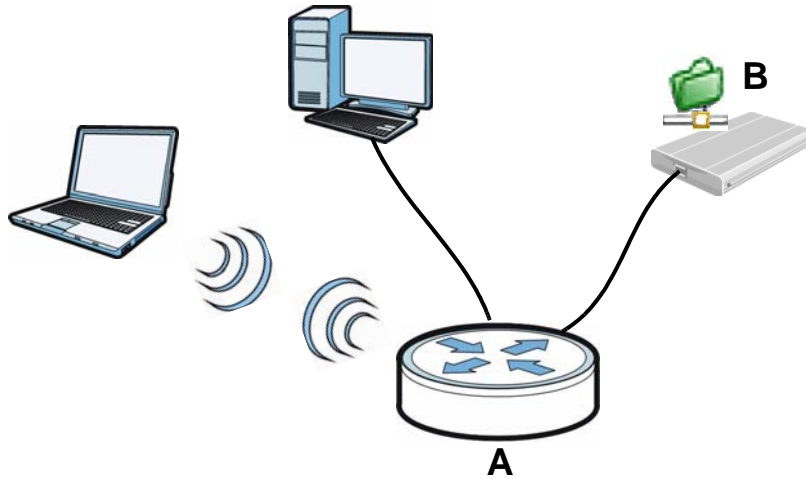
1.4.3 CellPipe 7130 RG's USB Support

The USB port of the CellPipe 7130 RG is used for file-sharing and media server features.

File Sharing

Use the built-in USB 2.0 port to share files via a USB memory stick or a USB hard drive (**B**). You can connect one USB hard drive to the CellPipe 7130 RG at a time.

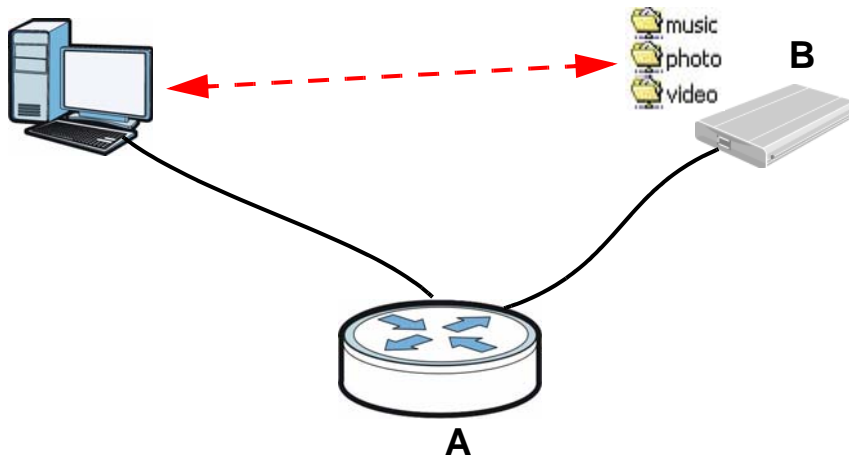
Figure 3 USB File Sharing Application



Media Server

You can also use the CellPipe 7130 RG as a media server. This lets anyone on your network play video, music, and photos from a USB device (**B**) connected to the CellPipe 7130 RG's USB port (without having to copy them to another computer).

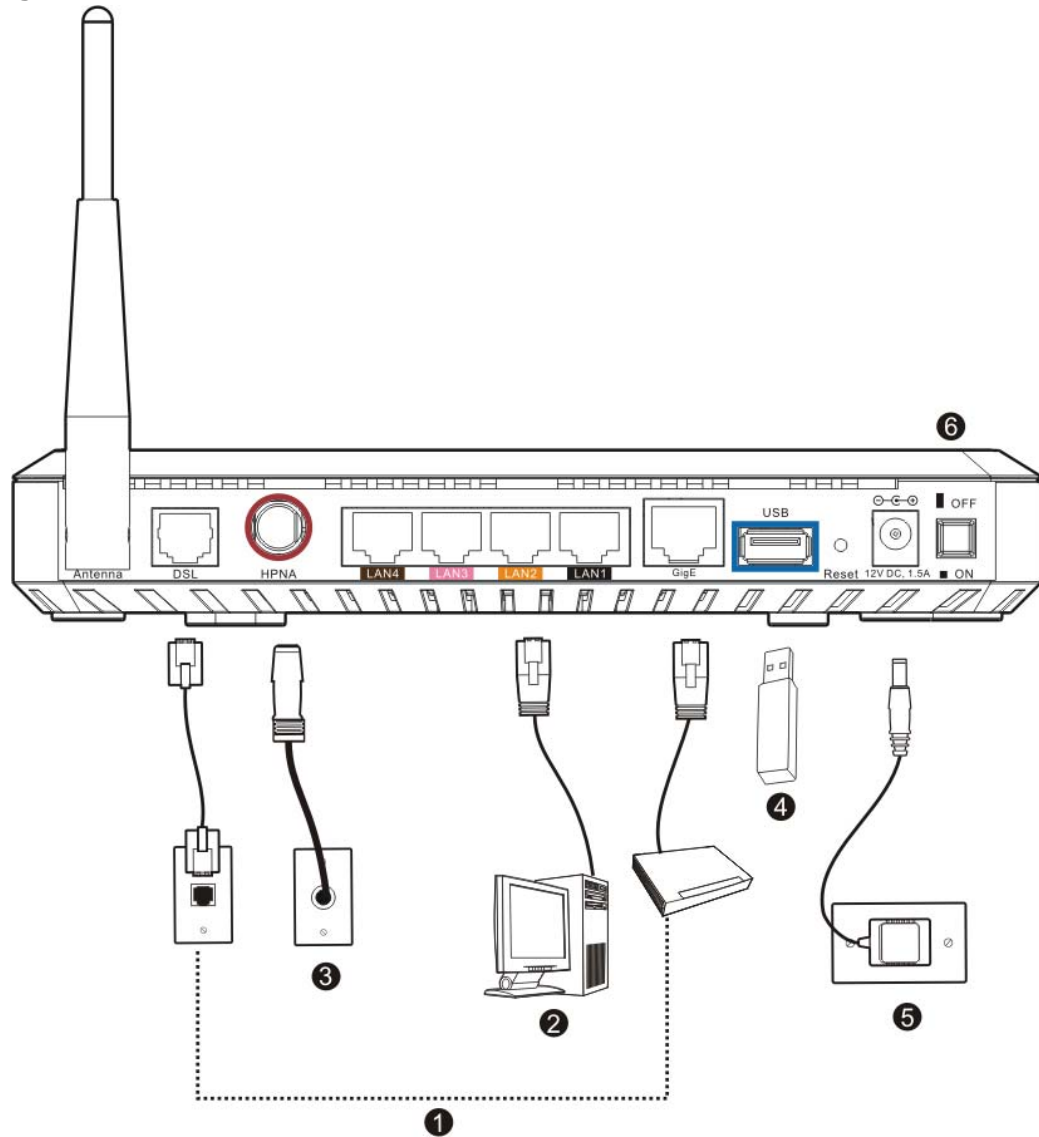
Figure 4 USB Media Server Application



1.5 Hardware Connections

Remove the CellPipe 7130 RG's plastic cover before using it.

Figure 5 Hardware Connections



- 1 Do one of the following for your Internet connection:
 - 1a **DSL:** Use a telephone wire to connect this port to a telephone jack (or the **DSL** or **MODEM** jack on a splitter, if you have one).
 - 1b **GigE:** If you have a broadband router or modem already in your network, use an Ethernet cable to connect this port to an Ethernet jack with Internet access.
- 2 **ETHERNET:** Use an Ethernet cable to connect a computer to one of these ports for initial configuration and/or Internet access.

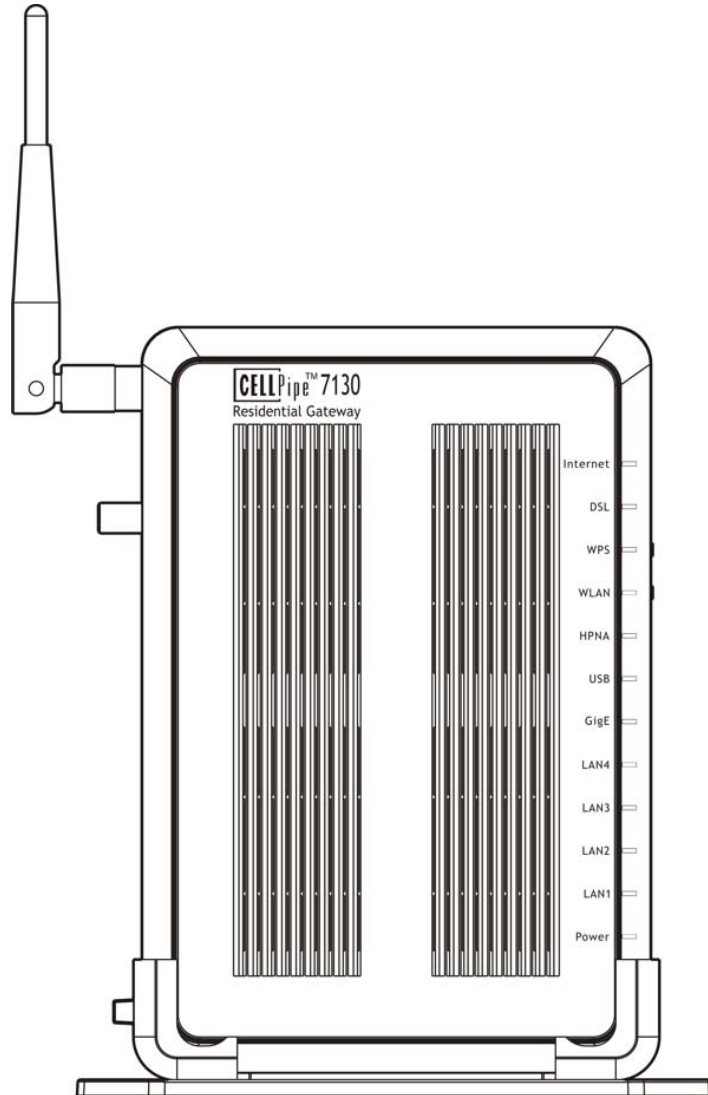
Note: Use an 8-wire Ethernet cable for Gigabit connections. Using a 4-wire Ethernet cable limits your connection to 100 Mbps. Note that the connection speed also depends on what the Ethernet device at the other end can support.

- 3 HPNA:** Use a coaxial cable to connect to a coaxial outlet and relay Internet traffic throughout your house through coaxial cabling.
- 4 USB 2.0:** Connect a USB (version 2.0 or lower) memory stick or a USB hard drive for file sharing. The CellPipe 7130 RG automatically detects the USB device. Use a USB extension cable if the stick is too big to fit.
- 5** Use the power adaptor provided with your CellPipe 7130 RG to connect an appropriate power source to this socket.
- 6** Push the power button to the on position.

1.6 LEDs (Lights)

The following graphic displays the labels of the LEDs.

Figure 6 LEDs on the Device



None of the LEDs are on if the CellPipe 7130 RG is not receiving power.

Table 1 LED Descriptions

LED	COLOR	STATUS	DESCRIPTION
INTERNET	Green	On	The CellPipe 7130 RG has an IP connection but no traffic. Your device has a WAN IP address (either static or assigned by a DHCP server), PPP negotiation was successfully completed (if used) and the DSL connection is up.
		Blinking	The CellPipe 7130 RG is sending or receiving IP traffic.

Table 1 LED Descriptions

LED	COLO R	STATUS	DESCRIPTION
		Off	There is no Internet connection or the gateway is in bridged mode.
DSL	Green	On	The DSL line is up.
		Blinking	The CellPipe 7130 RG is initializing the DSL line.
		Off	The DSL line is down.
WPS	Green	On	The wireless connection is successful. The light turns on for about 3 seconds before turning off.
		Blinking	The CellPipe 7130 RG is connecting with other wireless clients using WPS.
		Off	The WPS feature is not activated or has an error.
WLAN	Green	On	The wireless network is activated and is operating in IEEE 802.11b/g mode.
		Blinking	The CellPipe 7130 RG is communicating with other wireless clients.
		Off	The wireless network is not activated.
HPNA	Green	On	The CellPipe 7130 RG is connected to an HPNA-equipped device through the coaxial cable.
		Blinking	Data is transmitting over the HPNA cable.
		Off	No HPNA device is connected.
USB	Green	On	The CellPipe 7130 RG recognizes a USB connection.
		Blinking	The CellPipe 7130 RG is sending/receiving data to /from the USB device connected to it.
		Off	The CellPipe 7130 RG does not detect a USB connection.
GigE	Green	On	The Giga Ethernet connection is working.
		Blinking	The CellPipe 7130 RG is sending or receiving data to/ from the Giga Ethernet link.
		Off	There is no Giga Ethernet link.
ETHERNET 1-4	Green	On	The CellPipe 7130 RG has a successful 100 Mbps Ethernet connection with a device on the Local Area Network (LAN).
		Blinking	The CellPipe 7130 RG is sending or receiving data to/ from the LAN at 100 Mbps.
		Off	The CellPipe 7130 RG does not have an Ethernet connection with the LAN.
Power	Green	On	The CellPipe 7130 RG is receiving power and ready for use.
		Blinking	The CellPipe 7130 RG is self-testing.
	Red	On	The CellPipe 7130 RG detected an error while self-testing, or there is a device malfunction.
		Off	The CellPipe 7130 RG is not receiving power.
		Blinking	Firmware upgrade is in progress.

Refer to the Quick Start Guide for information on hardware connections.

1.7 The RESET Button

If you forget your password or cannot access the web configurator, you will need to use the **RESET** button at the back of the device to reload the factory-default configuration file. This means that you will lose all configurations that you had previously and the password will be reset to “telus”.

- 1 Make sure the **POWER** LED is on (not blinking).
- 2 To set the device back to the factory default settings, press the **RESET** button for ten seconds or until the **POWER** LED begins to blink and then release it. When the **POWER** LED begins to blink, the defaults have been restored and the device restarts.

1.8 The WLAN Button

You can use the **WLAN** button of the device to turn the wireless LAN off or on.

- 1 Make sure the **POWER** LED is on (not blinking).
- 2 Press the **WLAN** button for one second and release it. The **WLAN** LED should change from on to off or vice versa. Refer to [Section 7.4 on page 143](#) for more information.

1.9 The WPS Button

You can use the WPS button to activate WPS in order to quickly set up a wireless network with strong security.

- 1 Make sure the **POWER** LED is on (not blinking).
- 2 Make sure the wireless LAN is turned on. Refer to [Section 1.8 on page 28](#) and [Section 7.4 on page 143](#) for information or check that the WLAN LED is on.
- 3 Press the **WPS** button for more than one second and release it. Press the WPS button on another WPS -enabled device within range of the CellPipe 7130 RG. The **WPS** LED should flash while the CellPipe 7130 RG sets up a WPS connection with the wireless device. Refer to [Section 7.6 on page 153](#) for more information.

You must activate WPS in the CellPipe 7130 RG and in another wireless device within two minutes of each other. See [Section 7.10.4 on page 163](#) for more information.

Tutorials

2.1 Overview

This chapter describes:

- [How to Set up a Wireless Network on page 29.](#)
- [HomePNA Example Setup on page 39](#)
- [How to Use ATM QoS with Multiple PVCs on page 40.](#)
- [How to Allow Out-of-band Remote Management from the WAN on page 53.](#)
- [Using the Media Server Feature on page 65](#)
- [Using the File Sharing Feature on page 71.](#)
- [Setting Up NAT Port Forwarding on page 72..](#)
- [Configuring Static Route for Routing to Another Network on page 74](#)
- [Configuring QoS Queue and Class Setup on page 77](#)
- [Access the CellPipe 7130 RG Using DDNS on page 80](#)

Note: The tutorials featured in this chapter require a basic understanding of connecting to and using the Web Configurator on your CellPipe 7130 RG. For details, see the included Quick Start Guide. For field descriptions of individual screens, see the related technical reference in this User's Guide.

2.2 How to Set up a Wireless Network

This tutorial gives you examples of how to set up an access point (AP) and wireless client for wireless communication using the following parameters. The wireless clients can access the Internet through an AP wirelessly.

The CellPipe 7130 RG's AP function is enabled by default. The wireless settings, such as the SSID and pre-shared key, are already configured in the CellPipe 7130 RG. Use this tutorial if you want to use wireless settings other than the default values.

2.2.1 Example Parameters

SSID	SSID_Example3
Security	WPA-PSK (Pre-Shared Key: ThisismyWPA-PSKpre-sharedkey)
802.11 mode	IEEE 802.11b/g/n Mixed

An access point or wireless router is referred to as “AP” and a computer with a wireless network card or USB/PCI adapter is referred to as “wireless client” here.

We use the CellPipe 7130 RG web screens and M-302 utility screens as an example. The screens may vary slightly for different models.

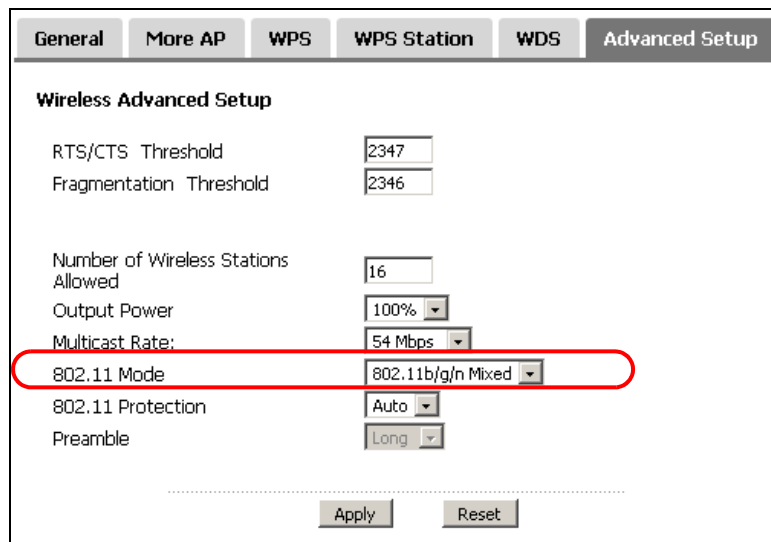
2.2.2 Configuring the AP

Follow the steps below to configure the wireless settings on your AP.

- 1 Open the **Network > Wireless LAN** screen in the AP's web configurator.

The screenshot shows the web configurator interface for the AP's wireless settings. The 'General' tab is selected, and the 'Wireless Setup' section is active. The 'Active Wireless LAN' checkbox is checked. The 'Network Name (SSID)' field contains 'SSID_Example3'. The 'Security Mode' is set to 'WPA-PSK', 'Encryption' is 'TKIP', and the 'Pre-Shared Key' is 'ThisismyWPA-PSKpre-sharedkey'. The 'BSSID' is '40:4A:03:AD:70:48'. The 'Group Key Update Timer' is set to '0' seconds. The 'MAC Filter' section has an 'Edit' button. The 'Apply' and 'Reset' buttons are at the bottom.

- 2 Make sure the **Active Wireless LAN** check box is selected.
- 3 Uncheck **Auto Generate Key**. This lets you enter an SSID and pre-shared key.
- 4 Enter "SSID_Example3" as the SSID and select **Auto** to have the CellPipe 7130 RG automatically determine a channel which is not used by another AP.
- 5 Set security mode to **WPA-PSK** and enter "ThisismyWPA-PSKpre-sharedkey" in the **Pre-Shared Key** field. Click **Apply**.
- 6 Click the **Advanced Setup** tab and make sure **802.11b/g/n Mixed** is selected in the **802.11 Mode** field. Click **Apply**.



The screenshot shows the 'Advanced Setup' tab of a wireless configuration interface. The 'Wireless Advanced Setup' section contains the following fields and values:

Field	Value
RTS/CTS Threshold	2347
Fragmentation Threshold	2346
Number of Wireless Stations Allowed	16
Output Power	100%
Multicast Rate:	54 Mbps
802.11 Mode	802.11b/g/n Mixed
802.11 Protection	Auto
Preamble	Long

At the bottom of the configuration area, there are two buttons: 'Apply' and 'Reset'.

- Open the **Status** screen. Verify your wireless and wireless security settings under **Device Information** and check if the WLAN connection is up under **Interface Status**.

The screenshot shows the TELUS Status page. On the left is a navigation menu with options like Network, WAN, LAN, Wireless LAN, NAT, USB Services, Security, Advanced, and Maintenance. The main content area is titled 'Status' and includes several sections:

- Device Information:** User Name: admin, Model Number: 5Vz.A2011, MAC Address: 40:4a:03:ad:70:47, Firmware Version: 0.0.02.GEN, DSL Firmware Version: A2pv6C030g.d22k.
- WAN 1 Information:** Mode: ETH/IPoW, IP Address: 172.23.26.30, IP Subnet Mask: 255.255.255.0.
- LAN Information:** IP Address: 192.168.1.1, IP Subnet Mask: 255.255.255.0, DHCP: Server.
- WLAN Information:** Channel: 6 (auto), WPS Status: Unconfigured, WDS Status: AP + Bridge.
- AP 1 Information (circled in red):** ESSID: SSID_Example3, Status: Active, Security: WPA-PSK.
- System Status:** System Uptime: 0 days: 0 hours: 1 minutes, Current Date/Time: 01 Jan 2000 00:01:14, System Mode: Routing / Bridging, CPU Usage: 14.00%, Memory Usage: 55%.
- Interface Status Table:**

Interface	Status	Rate
DSL	Link Down	kbps / kbps
ETH WAN	Up	100M / Full
LAN1	NoLink	N/A
LAN2	NoLink	N/A
LAN3	NoLink	N/A
LAN4	Up	100M / Full
HPNA	NoLink	N/A
WLAN	Up	54M

At the bottom, there are links for 'More Status', 'WAN Service Statistics', 'LAN Statistics', 'Route Info', 'Client List', and 'WLAN Station List' (circled in red). A message bar at the bottom left shows 'Message: Ready'.

- Click the **WLAN Station List** hyperlink in the AP's **Status** screen. You can see if any wireless client has connected to the AP.

Figure 7 Status: WLAN Station List

The screenshot shows the 'WLAN Station List' dialog box. It contains a table with the following data:

MAC	SSID	Interface
00:19:CB:41:78:10	SSID_Example3	wl0

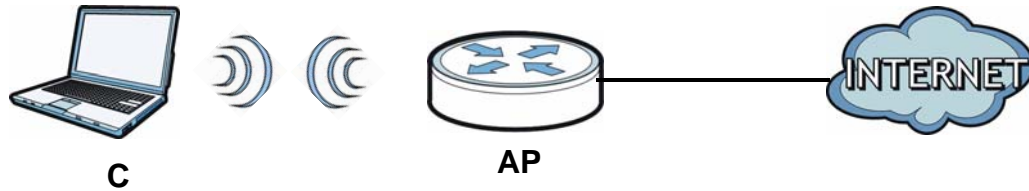
Below the table are a 'Close' button, a 'Refresh Interval : 5 seconds' field, and 'Set Interval' and 'Stop' buttons.

2.2.3 Configuring the Wireless Client

This section describes how to connect the wireless client to a network.

2.2.3.1 Connecting to a Wireless LAN

The following sections show you how to join a wireless network using a wireless utility, as in the following diagram. The wireless client is labeled **C** and the access point is labeled **AP**.



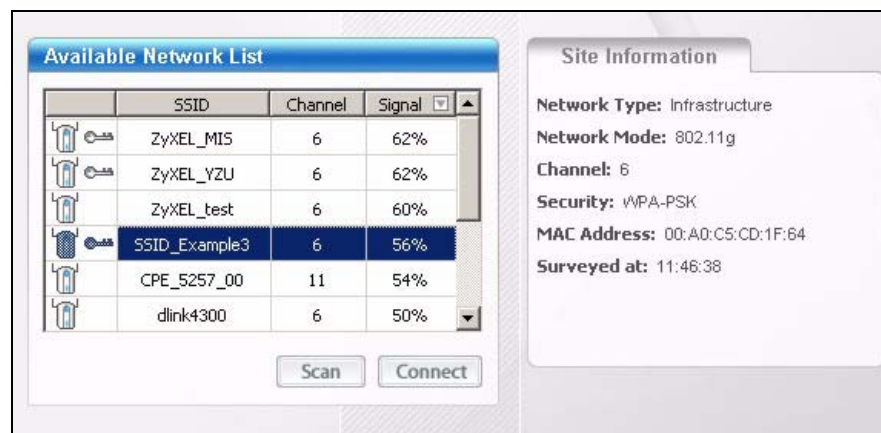
There are three ways to connect the client to an access point.

- Configure nothing and leave the wireless client to automatically scan for and connect to any available network that has no wireless security configured.
- Manually connect to a network.
- Configure a profile to have the wireless client automatically connect to a specific network or peer computer.

This example illustrates how to manually connect your wireless client to an access point (AP) which is configured for WPA-PSK security and connected to the Internet. Before you connect to the access point, you must know its Service Set IDentity (SSID) and WPA-PSK pre-shared key. In this example, the SSID is "SSID_Example3" and the pre-shared key is "ThisismyWPA-PSKpre-sharedkey".

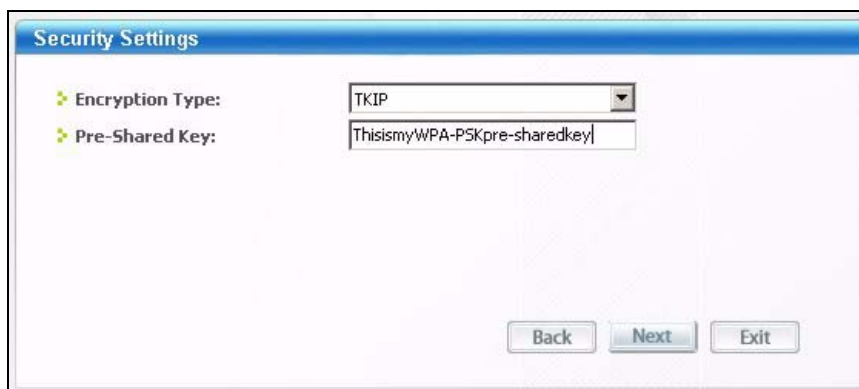
After you install the wireless utility and then insert the wireless client, follow the steps below to connect to a network using the **Site Survey** screen.

- 1 Open the wireless utility and click the **Site Survey** tab to open the screen shown next.



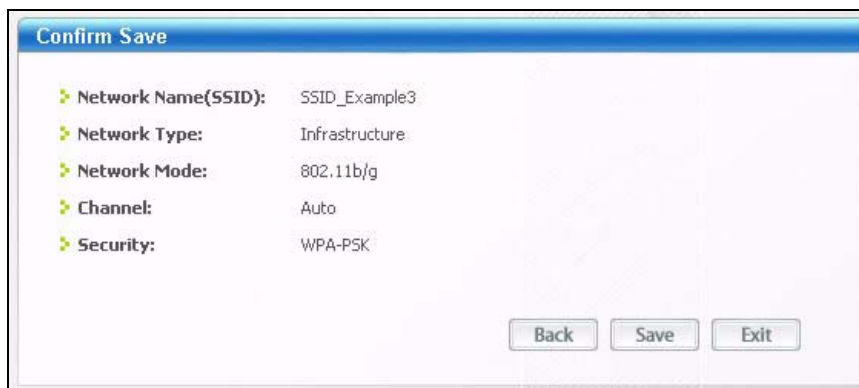
- 2 The wireless client automatically searches for available wireless networks. Click **Scan** if you want to search again. If no entry displays in the **Available Network List**, that means there is no wireless network available within range. Make sure the AP or peer computer is turned on or move the wireless client closer to the AP or peer computer.
- 3 When you try to connect to an AP with security configured, a window will pop up prompting you to specify the security settings. Enter the pre-shared key and leave the encryption type at the default setting.

Use the **Next** button to move on to the next screen. You can use the **Back** button at any time to return to the previous screen, or the **Exit** button to return to the **Site Survey** screen.



The screenshot shows a dialog box titled "Security Settings". It contains two fields: "Encryption Type" with a dropdown menu set to "TKIP", and "Pre-Shared Key" with a text input field containing "ThisismyWPA-PSKpre-sharedkey". At the bottom, there are three buttons: "Back", "Next", and "Exit".

- 4 The **Confirm Save** window appears. Check your settings and click **Save** to continue.



The screenshot shows a dialog box titled "Confirm Save". It displays a summary of the network settings: "Network Name(SSID): SSID_Example3", "Network Type: Infrastructure", "Network Mode: 802.11b/g", "Channel: Auto", and "Security: WPA-PSK". At the bottom, there are three buttons: "Back", "Save", and "Exit".

- 5 The wireless utility returns to the **Link Info** screen while it connects to the wireless network using your settings. When the wireless link is established, the wireless utility icon in the system tray turns green and the **Link Info** screen displays details of the active connection. Check the network information in the **Link Info** screen to verify that you have successfully connected to the selected network. If the wireless client is not connected to a network, the fields in this screen remain blank.



- 6 Open your Internet browser and enter the URL of any other web site in the address bar. If you are able to access the web site, your wireless connection is successfully configured.

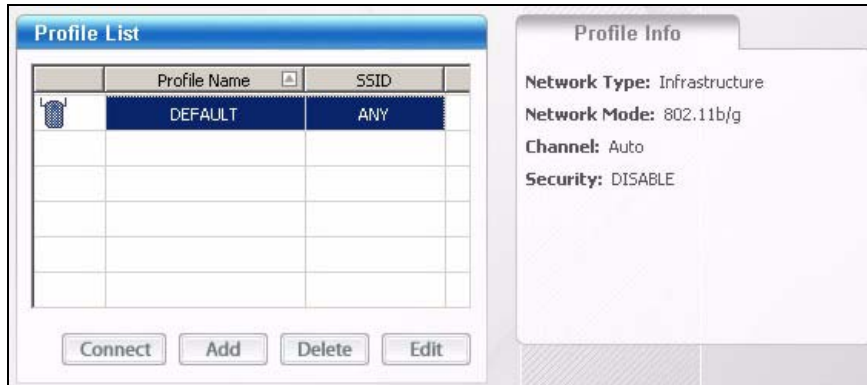
If you cannot access the web site, try changing the encryption type in the **Security Settings** screen, check the Troubleshooting section of this User's Guide or contact your network administrator.

2.2.3.2 Creating and Using a Profile

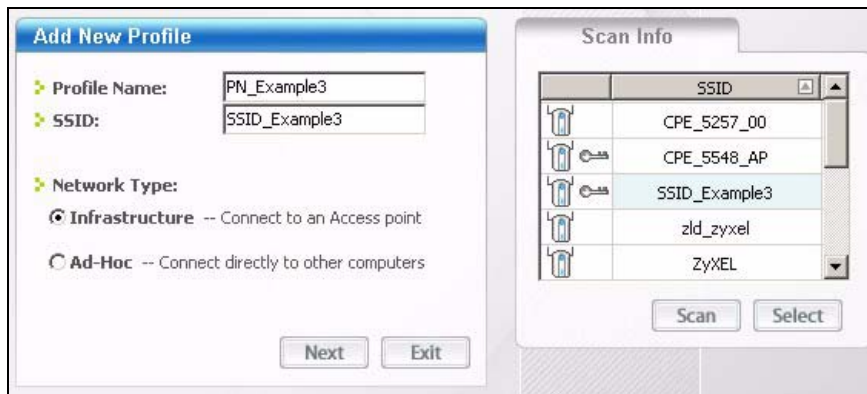
A profile lets you automatically connect to the same wireless network every time you use the wireless client. You can also configure different profiles for different networks, for example if you connect a notebook computer to wireless networks at home and at work.

This example illustrates how to set up a profile and connect the wireless client to an access point configured for WPA-PSK security. In this example, the SSID is "SSID_Example3", the profile name is "PN_Example3" and the pre-shared key is "ThisismyWPA-PSKpre-sharedkey". You have chosen the profile name "PN_Example3".

- 1 Open the wireless utility and click the **Profile** tab to open the screen shown next. Click **Add** to configure a new profile.

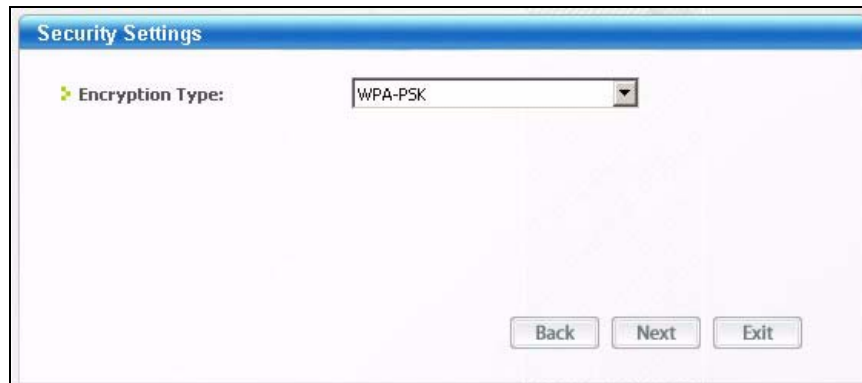


- 2 The **Add New Profile** screen appears. The wireless client automatically searches for available wireless networks, which are displayed in the **Scan Info** box. Click on **Scan** if you want to search again. You can also configure your profile for a wireless network that is not in the list.

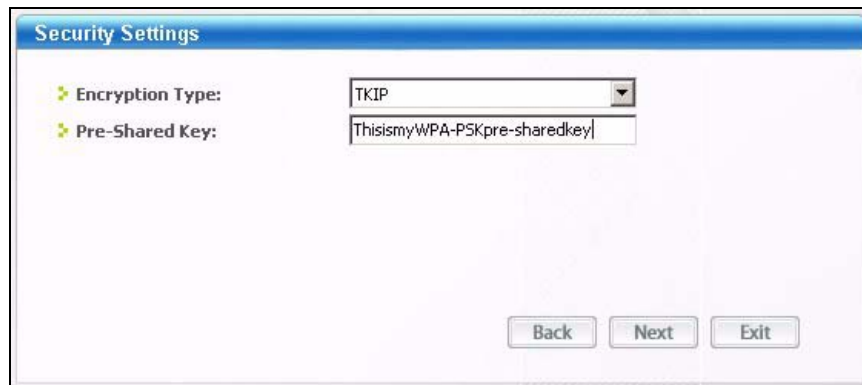


- 3 Give the profile a descriptive name (of up to 32 printable ASCII characters). Select **Infrastructure** and either manually enter or select the AP's SSID in the **Scan Info** table and click **Select**.

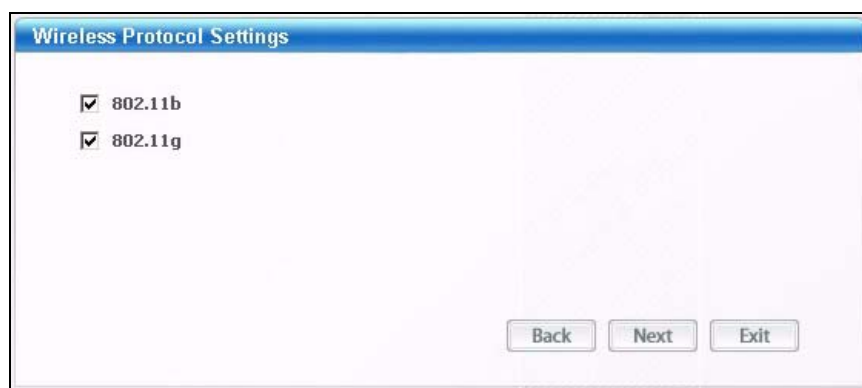
- 4 Choose the same encryption method as the AP to which you want to connect (In this example, WPA-PSK).



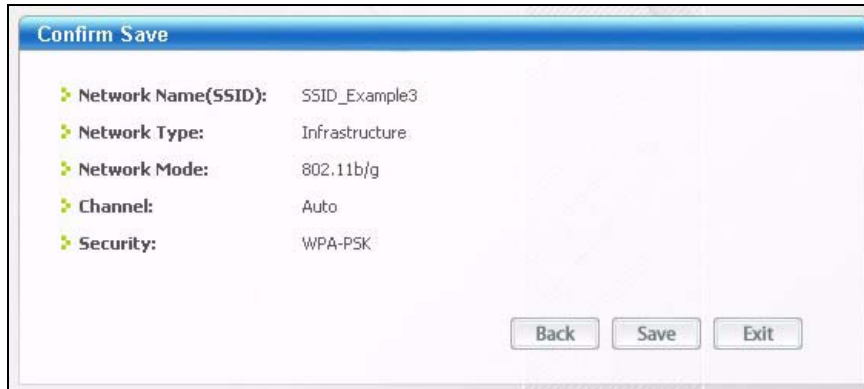
- 5 This screen varies depending on the encryption method you selected in the previous screen. Enter the pre-shared key and leave the encryption type at the default setting.



- 6 In the next screen, leave both boxes checked.



- 7 Verify the profile settings in the read-only screen. Click **Save** to save and go to the next screen.



- 8 Click **Activate Now** to use the new profile immediately. Otherwise, click the **Activate Later** button.

If you clicked **Activate Later**, you can select the profile from the list in the **Profile** screen and click **Connect** to activate it.

Note: Only one profile can be activated and used at any given time.



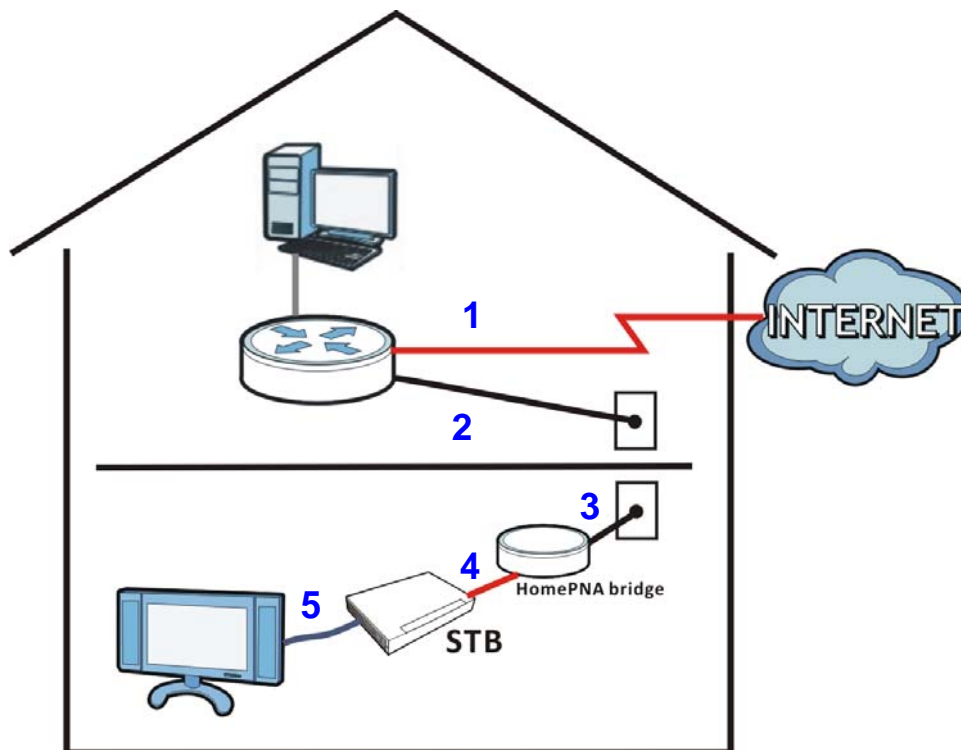
- 9 When you activate the new profile, the wireless utility returns to the **Link Info** screen while it connects to the AP using your settings. When the wireless link is established, the wireless utility icon in the system tray turns green and the **Link Info** screen displays details of the active connection.
- 10 Open your Internet browser, enter the URL of any other web site in the address bar and press ENTER. If you are able to access the web site, your new profile is successfully configured.
- 11 If you cannot access the Internet go back to the **Profile** screen, select the profile you are using and click **Edit**. Check the details you entered previously. Also, refer to the Troubleshooting section of this User's Guide or contact your network administrator if necessary.

2.3 HomePNA Example Setup

This tutorial shows you how you can use the CellPipe 7130 RG's HomePNA feature to connect a television in another part of the house to the Internet through the coaxial port. You will need:

- a Set-Top Box (STB)
- HomePNA Ethernet Bridge
- a television; and
- an active Video On Demand (VOD)/Internet Protocol Television (IPTV) subscription

The figure below shows the hardware setup for this tutorial:



- 1 Connect your CellPipe 7130 RG to the Internet source. This could be either DSL or Ethernet.
- 2 Connect the CellPipe 7130 RG's coaxial port a coaxial outlet in your house. This relays Internet connectivity to other coaxial outlets in other parts of the house.
- 3 In the room where your television is located, connect the HomePNA bridge to a coaxial outlet.

- 4 Using an Ethernet cable, connect the HomePNA bridge device to the STB. This grants Internet access to the STB.
- 5 Refer to the user's guide of your STB for information on how to connect it to your television, as well as configure your account settings on it.

You should now be able to watch online videos in your television using your VOD or IPTV subscription.

2.4 How to Use ATM QoS with Multiple PVCs

The CellPipe 7130 RG allows you to have more than one PVC using the ATM layer-2 interface. You can apply different ATM QoS settings to traffic through different PVCs. In this example, real-time or video service, such as using a webcam to send photos or uploading media content to share videos and images on a blog, comes from IP address 192.168.1.33 and is forwarded out through PVC 1 (0/33). Non-time sensitive data transfers, such as e-mail or FTP, come from IP address 192.168.1.34 and are forwarded out through PVC 2 (0/34). The maximum upstream transmission speed of your ADSL port is 1 Mbps. You want to give the real-time traffic fixed bandwidth 400 Kbps and higher priority over the general data transmission which shares the bandwidth 600 Kbps. You allot more bandwidth to data transmission since there are more volume of this traffic than real-time traffic.

Table 2 ATM QoS and Group Settings

TRAFFIC TYPE	LAN	PVC	ATM QOS	BANDWIDTH	GROUP
Real-time or video service	192.168.1.33	atm0 (0/33)	CBR	400 Kbps	GR1/PVC1
Non-time sensitive data	192.168.1.34	atm1 (0/34)	Non Realtime VBR	600 Kbps	GR2/PVC2

Note: To apply different QoS priorities to different applications over a PVC, use the **Advanced > QoS** screens. The packet-level QoS feature is not applicable to a PVC with CBR or Realtime VBR enabled.

Overview of what you have to do

- 1 Create PVCs using the **Network > WAN** screens. See [Figure 2.4.1 on page 41](#).
- 2 Create policy forwarding rules in the **Advanced > Policy Forwarding** screen to map specific IP addresses to the PVCs you created. See [Figure 2.4.2 on page 51](#).

2.4.1 Configuring PVCs

Follows the steps below to set up two PVCs on the CellPipe 7130 RG.

Table 3 Multiple PVC Settings

PVC	INTERFACE NAME	WAN SERVICE
0/33	ppp0	PPPoE (pppoe_0_0_33)
0/34	atm1	IPoE (ipoe_0_0_34)

- 1 Click **Network > WAN > Connect**.
- 2 Select **ATM** from the **Interface** drop-down list and click **Add**.

Mode **Connect** Services

Interface: ATM

DSL ATM Interface Configuration

Choose Add, or Remove to configure DSL ATM interfaces.

Active	Interface	Vpi	Vci	Category	Link Type	Connection Mode	QoS	Remove
<input type="checkbox"/>	atm0	0	33	UBR	EoA	DefaultMode	Enabled	

Add Apply

- Enter the VPI and VCI values (**0** and **33** in this example) for PVC 1. Select **CBR** in the **Service Category** field and set the **Peak Cell Rate** as **943** (divide the bandwidth 400000 bps by 424). Click **Apply** to save the changes and go back to the **Connect** screen.

DSL ATM Interface Configuration

ATM PVC Configuration
This screen allows you to configure an ATM PVC identifier (VPI and VCI), select DSL latency, select a service category. Otherwise choose an existing interface by selecting the checkbox to enable it.

VPI: [0-255]
VCI: [32-65535]

Select DSL Link Type (EoA is for PPPoE, IPoE, and Bridge.)

EoA
 PPPoA
 IPoA

Encapsulation Mode:
Service Category:

Select Connection Mode

Default Mode - Single service over one connection
 VLAN MUX Mode - Multiple Vlan service over one connection

Enable Quality Of Service

Enabling packet level QoS for a PVC improves performance for selected classes of applications. QoS cannot be set for CBR and Realtime VBR. QoS consumes system resources; therefore the number of PVCs will be reduced. Use **Advanced Setup/Quality of Service** to assign priorities for the applications.

Enable Quality Of Service.

Back

- Click **Add** to configure another PVC.
- Enter the VPI and VCI values (**0** and **34** in this example) for PVC 2. Select **Non Realtime VBR** in the **Service Category** field. Set the **Peak Cell Rate** as **1415** (divide the bandwidth 600000 bps by 424) and set both the **Sustainable Cell Rate** and **Maximum Burst Size** as **1414** (which is less than the peak cell rate).

- Click **Apply** to save the changes and go back to the **Connect** screen.

DSL ATM Interface Configuration

ATM PVC Configuration
This screen allows you to configure an ATM PVC identifier (VPI and VCI), select DSL latency, select a service category. Otherwise choose an existing interface by selecting the checkbox to enable it.

VPI: [0-255]
VCI: [32-65535]

Select DSL Link Type (EoA is for PPPoE, IPoE, and Bridge.)

EoA
 PPPoA
 IPoA

Encapsulation Mode:

Service Category:

Peak Cell Rate: [cells/s]
Sustainable Cell Rate: [cells/s]
Maximum Burst Size: [cells]

Select Connection Mode

Default Mode - Single service over one connection
 VLAN MUX Mode - Multiple Vlan service over one connection

Enable Quality Of Service

Enabling packet level QoS for a PVC improves performance for selected classes of applications. QoS cannot be set for CBR and Realtime VBR. QoS consumes system resources; therefore the number of PVCs will be reduced. Use **Advanced Setup/Quality of Service** to assign priorities for the applications.

Enable Quality Of Service.

2.4.1.1 Internet Connection Settings for PVC 1

- Click **Network > WAN > Services** to configure WAN connection settings for PVC 1. Click **Add**.

Mode

Wide Area Network (WAN) Service Setup

Choose Add, or Remove to configure a WAN service over a selected interface.

Interface	Description	Type	Rate	Vlan8021p	VlanMuxId	ConnId	IGMP	NAT	Firewall	Modify

- 2 Select PVC 1 (**atm0/0_0_33**) as the layer-2 interface. Click **Next**.

WAN Service Interface Configuration

Select a layer 2 interface for this service

atm0/(0_0_33) ▾

.....

Back Next

- 3 Select **PPP over Ethernet** and click **Next**.

WAN Service Configuration

Select WAN service type:

- PPP over Ethernet (PPPoE)
- IP over Ethernet
- Bridging

Enter Service Description:

.....

Back Next

- 4 Enter the user name (**user@isp.net** for example), password (**qwerty12345** for example) and service name (**isp.net** for example) for the PPP connection. Click **Next**.

PPP Username and Password

PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.

PPP Username:

PPP Password:

PPPoE Service Name:

Authentication Method:

Enable Fullcone NAT

Dial on demand (with idle timeout timer)

Use Static IPv4 Address

Enable PPP Debug Mode

Bridge PPPoE Frames Between WAN and Local Ports

Multicast Proxy

Enable IGMP Multicast Proxy

Back Next

- 5 Remove the existing interfaces in the **Selected Default Gateway Interfaces** list. Select and move a WAN interface (**ppp0** in this example) to the **Selected Default Gateway Interfaces** list to use that interface as the default gateway. Click **Next**.

Routing -- Default Gateway

Default gateway interface list can have multiple WAN interfaces served as system default gateways 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 WAN interface is connected(No Backup WAN function support). Priority order can be changed by removing all and adding them back in again.

Selected Default Gateway Interfaces

Available Routed WAN Interfaces

ppp0

Back Next

- 6 Select the first option. Remove the existing interfaces in the **Selected DNS Server Interfaces** list. Select and move a WAN interface (**ppp0** in this example) to the **Selected DNS Server Interfaces** list to use that interface as the system DNS server. Click **Next**.

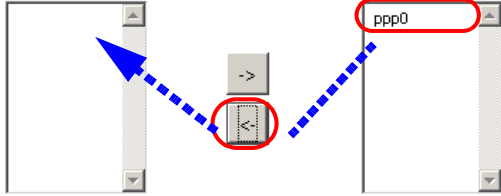
Default DNS Server Configuration

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.

DNS Server Interfaces can have multiple WAN interfaces served as system dns servers 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 WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

Select DNS Server Interface from available WAN interfaces:

Selected DNS Server Interfaces Available WAN Interfaces



Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

.....

Back **Next**

- The summary screen displays. Click **Apply/Save** to save your changes and go back to the **Services** screen.

WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

PORT / VPI / VCI:	0 / 0 / 33
Connection Type:	PPPoE
Service Name:	pppoe_0_0_33
Service Category:	UBR
IP Address:	Automatically Assigned
Service State:	Enabled
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Enabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

.....

Mode **Connect** **Services**

Wide Area Network (WAN) Service Setup

Choose Add, or Remove to configure a WAN service over a selected interface.

Interface	Description	Type	Rate	Vlan8021p	VlanMuxId	ConnId	IGMP	NAT	Firewall	Modify
ppp0	pppoe_0_0_33	ATM/PPPoE	N/A	N/A	N/A	N/A	Disabled	Enabled	Enabled	

.....

2.4.1.2 Internet Connection Settings for PVC 2

- Click **Add** in the **WAN > Services** screen to configure WAN connection settings for PVC 2.
- Select PVC 2 (**atm2/0_0_34**) as the layer-2 interface. Click **Next**.

WAN Service Interface Configuration

Select a layer 2 interface for this service

.....

3 Select IP over Ethernet and click Next.

WAN Service Configuration

Select WAN service type:
 PPP over Ethernet (PPPoE)
 IP over Ethernet
 Bridging

Enter Service Description:

.....

4 Select Obtain an IP address automatically and click Next.

WAN IP Settings

Enter information provided to you by your ISP to configure the WAN IP settings.
Notice: If "Obtain an IP address automatically" is chosen, DHCP client will be enabled
If "Use the following Static IP address" is chosen, enter the WAN IP address, subnet
mask and interface gateway.

 Obtain an IP address automatically
 Enable DHCP Option 60
Vendor class Identifier:
 Enable DHCP Option 61
IAID:
DUID type:
Identifier:
 Enable DHCP Option 125
Manufacturer OUI:
Product class:
Model name:
Serial number:
 Use the following Static IP address:
WAN IP Address:
WAN Subnet Mask:
WAN gateway IP Address:

.....

- 5 Select **Enable NAT** and click **Next**.

Network Address Translation Settings

Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN).

Enable NAT

Enable Fullcone NAT

Enable Firewall

IGMP Multicast

Enable IGMP Multicast Proxy

Back Next

- 6 Remove the existing interfaces in the **Selected Default Gateway Interfaces** list. Select and move a WAN interface (**atm1** in this example) to the **Selected Default Gateway Interfaces** list to use that interface as the default gateway. Click **Next**.

Routing -- Default Gateway

Default gateway interface list can have multiple WAN interfaces served as system default gateways 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 WAN interface is connected (No Backup WAN function support). Priority order can be changed by removing all and adding them back in again.

Selected Default Gateway Interfaces

ppp0

Available Routed WAN Interfaces

atm1

Back Next

- 7 Select the first option. Remove the existing interfaces in the **Selected DNS Server Interfaces** list. Select and move a WAN interface (**atm1** in this example) to the **Selected DNS Server Interfaces** list to use that interface as the system DNS server. Click **Next**.

Default DNS Server Configuration

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.
DNS Server Interfaces can have multiple WAN interfaces served as system dns servers 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 WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

Select DNS Server Interface from available WAN interfaces:

Selected DNS Server Interfaces Available WAN Interfaces

Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

.....

Back Next

- 8 The summary screen displays. Click **Apply/Save** to save your changes and go back to the **Services** screen.

WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.







PORT / VPI / VCI:	0 / 0 / 34
Connection Type:	IPoE
Service Name:	ipoe_0_0_34
Service Category:	VBR-nrt
IP Address:	Automatically Assigned
Service State:	Enabled
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Disabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

.....

Back Apply/Save

- 9 The **Services** screen should look like the following.

Mode	Connect	Services								
Wide Area Network (WAN) Service Setup										
Choose Add, or Remove to configure a WAN service over a selected interface.										
Interface	Description	Type	Rate	Vlan8021p	VlanMuxId	ConnId	IGMP	NAT	Firewall	Modify
ppp0	pppoe_0_0_33	ATM/PPPoE	N/A	N/A	N/A	N/A	Disabled	Enabled	Enabled	 
atm1	ipoe_0_0_34	ATM/IPoE	N/A	N/A	N/A	N/A	Disabled	Enabled	Disabled	 
eth4_1	ipoe_eth4_1	ETH/IPoW	N/A	N/A	N/A	1	Disabled	Enabled	Enabled	 
<input type="button" value="Add"/>										

2.4.2 Setting Policy Forwarding

You can use policy forwarding to map traffic to a specific PVC, but you need to enter the source IP address, port number and/or MAC address of each packet that passes through the PVC. See [Chapter 14 on page 213](#) for more information.

Follow the steps below to map traffic from IP address 192.168.1.33 to PVC 1 and traffic from IP address 192.168.1.34 to PVC 2.

Table 4 DSL Connection Groups

GROUP	LAN IP ADDRESS	PORT	MAC ADDRESS	WAN INTERFACE
GR1	192.168.1.33	80 (HTTP)	AA:BB:AA:BB:AA:BB	ppp0 (0/33)
GR2	192.168.1.34	21 (FTP) 25 (E-mail)	FF:CC:FF:CC:FF:CC	atm2 (0/34)

- 1 Click **Advanced > Policy Forwarding** to open the following screen. Click **Add** to create a new policy forwarding group **GR1**.

Policy Forwarding						
Policy Forwarding						
A maximum 8 entries can be configured.						
Policy Name	SourceIP	Protocol	SourcePort	SourceMac	WAN	Remove
<input type="button" value="Add"/>						

- 2 Enter **GR1** as the **Policy Name**. In this group, we will associate **ppp0** (PVC 1) as the WAN interface with 192.168.1.33 as the IP address. Select **pppoe_0_0_33/ppp0** from the **WAN Interface** list. Enter 192.168.1.33 as the **Source IP Address**. Select the protocol and enter the source port, as well as the source MAC address. Click **Apply** to finish the settings and go back to the **Policy Forwarding** screen.

Policy Route Setup

Policy Name	<input type="text" value="GR1"/>
Source IP Address	<input type="text" value="192.168.1.33"/>
Protocol	<input type="text" value="TCP"/>
Source Port	<input type="text" value="80"/>
Source Mac Address	<input type="text" value="AA:BB:AA:BB:AA:BB"/>
Use Interface	<input type="text" value="pppoe_0_0_33/ppp0"/>

.....

- 3 **GR1** has been added successfully to the interface group list. Click **Add** to create another interface group: **GR2**.
- 4 Enter **GR2** as the **Policy Name**. In this group, we will associate **atm1** (PVC 2) as the WAN interface with 192.168.1.34 as the IP address. Select **ipoe_0_0_34/atm1** from the **WAN Interface** list. Enter 192.168.1.34 as the **Source IP Address**. Again, select the protocol and enter the source port, as well as the source MAC address. Click **Apply** to finish the settings and go back to the **Policy Forwarding** screen.

Policy Route Setup

Policy Name	<input type="text" value="GR2"/>
Source IP Address	<input type="text" value="192.168.1.34"/>
Protocol	<input type="text" value="UDP"/>
Source Port	<input type="text" value="21"/>
Source Mac Address	<input type="text" value="FF:CC:FF:CC:FF:CC"/>
Use Interface	<input type="text" value="ipoe_0_0_34/atm1"/>




.....

- 5 **GR2** has been added successfully to the interface group list. Continue to add groups to associate other services with PVCs. The screen should look like the following.

Policy Forwarding

Policy Forwarding

A maximum 8 entries can be configured.

Policy Name	SourceIP	Protocol	SourcePort	SourceMac	WAN	Remove
GR1	192.168.1.33	TCP	80	AA:BB:AA:BB:AA:BB	ppp0	
GR2	192.168.1.34	UDP	21	FF:CC:FF:CC:FF:CC	atm1	
GR3	192.168.1.34	TCP	25	FF:CC:FF:CC:FF:CC	atm1	

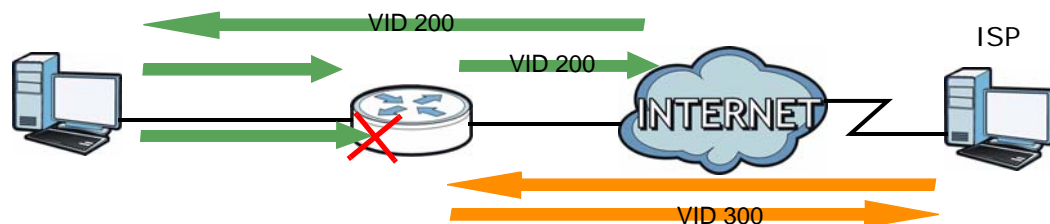
.....

2.5 How to Allow Out-of-band Remote Management from the WAN

This tutorial shows you how to set up a dedicated WAN connection for ISP management of the CellPipe 7130 RG and prevent the clients on the LAN from configuring the CellPipe 7130 RG. You set up two DSL connections with different VLAN IDs and priorities to separate clients traffic from management traffic. The DSL connection for remote management has the highest priority.

Table 5 Multiple VDSL Connection Settings

WAN INTERFACE	DESCRIPTION	CONNECTION METHOD	VLAN ID	PRIORITY
ppp0.200	Internet	PPPoE	200	2
ptm0.300	RemoteMgmt	IPoE	300	7



2.5.1 Configuring Multiple WAN Connections

Follow the steps below to configure two VDSL connections.

- 1 Make sure you set the **WAN Link Mode** to **DSL** in the **Network > WAN > Mode** screen.
- 2 By default, there is a PTM layer-2 interface in VLAN MUX mode configured already on the CellPipe 7130 RG.

Mode Connect Services

Interface:
PTM

DSL PTM Interface Configuration

Choose Add, or Remove to configure DSL PTM interfaces.

Active	Interface	Connection Mode	QoS	Remove
<input type="checkbox"/>	ptm0	VlanMuxMode	Enabled	

.....

Add Apply

DSL Connection for Internet Access

- 1 Go to the **WAN > Services** screen. Click **Add**.

Mode Connect Services

Wide Area Network (WAN) Service Setup

Choose Add, or Remove to configure a WAN service over a selected interface.

Interface	Description	Type	Rate	Vlan8021p	VlanMuxId	ConnId	IGMP	NAT	Firewall	Modify
-----------	-------------	------	------	-----------	-----------	--------	------	-----	----------	--------

.....

Add

- 2 Select **ptm0/(0_0_1)** as the layer-2 interface. Click **Next**.

WAN Service Interface Configuration

Select a layer 2 interface for this service

- 3 Select **PPP over Ethernet**, enter a descriptive service name (**Internet** in this example), and set the priority level to **2** and VLAN ID to **200**. Click **Next**.

WAN Service Configuration

Select WAN service type:

- PPP over Ethernet (PPPoE)
- IP over Ethernet
- Bridging

Enter Service Description:

Rate limit: kbps

Tag VLAN ID for egress packets

Enter 802.1P Priority [0-7]:

Enter 802.1Q VLAN ID [0-4094]:

- 4 Enter the user name (**user@isp.net** for example), password (**qwerty12345** for example) and service name (**isp.net** for example) for the PPP connection. Click **Next**.

PPP Username and Password

PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.

PPP Username:

PPP Password:

PPPoE Service Name:

Authentication Method:

Enable Fullcone NAT

Dial on demand (with idle timeout timer)

Use Static IPv4 Address

Enable PPP Debug Mode

Bridge PPPoE Frames Between WAN and Local Ports

Multicast Proxy

Enable IGMP Multicast Proxy

.....

- 5 Remove the existing interfaces in the **Selected Default Gateway Interfaces** list. Select and move a WAN interface (**ppp1.200** in this example) to the **Selected Default Gateway Interfaces** list to use that interface as the default gateway. Click **Next**.

Routing -- Default Gateway

Default gateway interface list can have multiple WAN interfaces served as system default gateways 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 WAN interface is connected(No Backup WAN function support). Priority order can be changed by removing all and adding them back in again.

Selected Default Gateway Interfaces	Available Routed WAN Interfaces
ppp1.200	atm1 eth4_1 ppp0

Back Next

- 6 Select the first option. Remove the existing interfaces in the **Selected DNS Server Interfaces** list. Select and move a WAN interface (**ppp1.200** in this example) to the **Selected DNS Server Interfaces** list to use that interface as the system DNS server. Click **Next**.

Default DNS Server Configuration

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.

DNS Server Interfaces can have multiple WAN interfaces served as system dns servers 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 WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

Select DNS Server Interface from available WAN interfaces:

Selected DNS Server Interfaces	Available WAN Interfaces
ppp1.200	atm1 eth4_1 ppp0

Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

Back Next

- The summary screen displays. The VLAN ID is appended to the service name you specified automatically. Click **Apply/Save** to save your changes and go back to the **Internet Connection** screen.

WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

PORT / VPI / VCI:	0 / 0 / 1
Connection Type:	PPPoE
Service Name:	pppoe_0_0_1.200
Service Category:	
IP Address:	Automatically Assigned
Service State:	Enabled
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Enabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

DSL Connection for Remote Management

- Go to the **WAN > Services** screen. Click **Add**.

Mode **Connect** **Services**

Wide Area Network (WAN) Service Setup

Choose Add, or Remove to configure a WAN service over a selected interface.

Interface	Description	Type	Rate	Vlan8021p	VlanMuxId	ConnId	IGMP	NAT	Firewall	Modify
ppp0	pppoe_0_0_33	ATM/PPPoE	N/A	N/A	N/A	N/A	Disabled	Enabled	Enabled	
atm1	ipoe_0_0_34	ATM/IPoE	N/A	N/A	N/A	N/A	Disabled	Enabled	Disabled	
ppp1.200	pppoe_0_0_1.200	PTM/PPPoE	N/A	2	200	1	Disabled	Enabled	Enabled	
eth4_1	ipoe_eth4_1	ETH/IPoW	N/A	N/A	N/A	1	Disabled	Enabled	Enabled	

- 2 Select **ptm0/(0_0_1)** as the layer-2 interface. Click **Next**.

WAN Service Interface Configuration

Select a layer 2 interface for this service

ptm0/(0_0_1) ▾

Back Next

- 3 Select **IP over Ethernet**, enter a descriptive service name (**RemoteMgmt** in this example), and set the priority level to **7** and VLAN ID to **300**. Click **Next**.

WAN Service Configuration

Select WAN service type:

PPP over Ethernet (PPPoE)

IP over Ethernet

Bridging

Enter Service Description: RemoteMgmt

Rate limit: _____ kbps

Tag VLAN ID for egress packets

Enter 802.1P Priority [0-7]: 7

Enter 802.1Q VLAN ID [0-4094]: 300

Back Next

4 Select **Obtain an IP address automatically** and click **Next**.

WAN IP Settings

Enter information provided to you by your ISP to configure the WAN IP settings.
Notice: If "Obtain an IP address automatically" is chosen, DHCP client will be enabled
If "Use the following Static IP address" is chosen, enter the WAN IP address, subnet mask and interface gateway.

Obtain an IP address automatically

Enable DHCP Option 60
Vendor class Identifier:

Enable DHCP Option 61
IAID:
DUID type:
Identifier:

Enable DHCP Option 125
Manufacturer OUI:
Product class:
Model name:
Serial number:

Use the following Static IP address:
WAN IP Address:
WAN Subnet Mask:
WAN gateway IP Address:

.....

5 Make sure **Enable NAT** is not selected and click **Next**.

Network Address Translation Settings

Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN).

Enable NAT

Enable Fullcone NAT

Enable Firewall

IGMP Multicast

Enable IGMP Multicast Proxy

.....

- 6 Keep the WAN interface (**ptm0.300** in this example) in the **Available Routed WAN Interfaces** list to not have the clients use this interface as the default gateway. Click **Next**.

Routing -- Default Gateway

Default gateway interface list can have multiple WAN interfaces served as system default gateways 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 WAN interface is connected (No Backup WAN function support). Priority order can be changed by removing all and adding them back in again.

Selected Default Gateway Interfaces

ppp0
atm1
eth4_1
ppp1.200

->
<-

Available Routed WAN Interfaces

ptm0.300

Back Next

- 7 Select the first option. Keep the WAN interface (**ptm0.300** in this example) in the **Available WAN Interfaces** list to not have the clients use this interface as the system DNS server. Click **Next**.

Default DNS Server Configuration

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.

DNS Server Interfaces can have multiple WAN interfaces served as system dns servers 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 WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

Select DNS Server Interface from available WAN interfaces:

Selected DNS Server Interfaces

ppp1.200
ppp0
atm1
eth4_1

->
<-

Available WAN Interfaces

ptm0.300

Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

Back Next

- The summary screen displays. Click **Apply/Save** to save your changes and go back to the **Services** screen. The VLAN ID is appended to the service name you specified automatically.

WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

PORT / VPI / VCI:	0 / 0 / 1
Connection Type:	IPoE
Service Name:	RemoteMgmt.300
Service Category:	
IP Address:	Automatically Assigned
Service State:	Enabled
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Disabled
IGMP Multicast:	Disabled
Quality Of Service:	Enabled











Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

- The **Internet Connection** screen should look like the following.

Mode **Connect** **Services**

Wide Area Network (WAN) Service Setup

Choose Add, or Remove to configure a WAN service over a selected interface.

Interface	Description	Type	Rate	Vlan8021p	VlanMuxId	ConnId	IGMP	NAT	Firewall	Modify
ppp0	pppoe_0_0_33	ATM/PPPoE	N/A	N/A	N/A	N/A	Disabled	Enabled	Enabled	 
atm1	ipoe_0_0_34	ATM/IPoE	N/A	N/A	N/A	N/A	Disabled	Enabled	Disabled	 
ptm0.300	RemoteMgmt.300	PTM/IPoE	N/A	7	300	2	Disabled	Enabled	Disabled	 
ppp1.200	Internet	PTM/PPPoE	N/A	2	200	1	Disabled	Enabled	Enabled	 
eth4_1	ipoe_eth4_1	ETH/IPoW	N/A	N/A	N/A	1	Disabled	Enabled	Enabled	 

.....
Add

- 3 The **WAN Service Statistics** screen displays. Check if any packets are transmitted or received through the two WAN connections you just configured.

WAN Services Statistics

Interface	Description	Received				Transmitted			
		Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
atm1	ipoe_0_0_34	0	0	0	0	0	0	0	2727
ppp0	pppoe_0_0_33	0	0	0	0	0	0	0	2727
ptm0.300	RemoteMgmt.300	12229	5122	0	0	36952	124	0	0
ppp1.200	Internet	25122	6617	0	0	36952	124	0	0
eth4_1	ipoe_eth4_1	0	0	0	0	279402	3253	0	0

Close

Refresh Interval : 5 seconds Set Interval Stop

2.5.2 Configuring Remote Management

Follow the steps below to not allow access to the CellPipe 7130 RG from the LAN.

- 1 Click **Advanced > Remote MGNT > Service Control**.
- 2 Select the **Enable** option, and deselect all service options in the **LAN** column. Click **Apply**.

Service Control: Disable Enable

#	Services	LAN	WAN
1	FTP	<input type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable
2	HTTP	<input type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable
3	SSH	<input type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable
4	TELNET	<input type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable
5	TFTP	<input type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable

Apply

2.5.3 Testing the Connection

After you finish all the settings in this tutorial, you would not be able to access the web configurator from the LAN anymore. Check if you can use the WAN IP address for the **RemoteMgmt** WAN connection to access the CellPipe 7130 RG. You should also be able to access the Internet using the computer which is connected to the CellPipe 7130 RG's LAN port.

2.6 Using the Media Server Feature

Use the media server feature to play files on a computer or on your television using a Digital Media Adapter (DMA).

This section shows you how the media server feature works using the following media clients:

- Microsoft (MS) Windows Media Player

Media Server works with Windows Vista and Windows 7. Make sure your computer is able to play media files (music, videos and pictures).

- A DMA

You need to set up the DMA to work with your television (TV). Refer to your DMA's Quick Start Guide for the correct hardware connections.

Before you begin, connect the USB storage device containing the media files you want to play to the USB port of your CellPipe 7130 RG.

2.6.1 Configuring the CellPipe 7130 RG

Note: The Media Server feature is enabled by default.

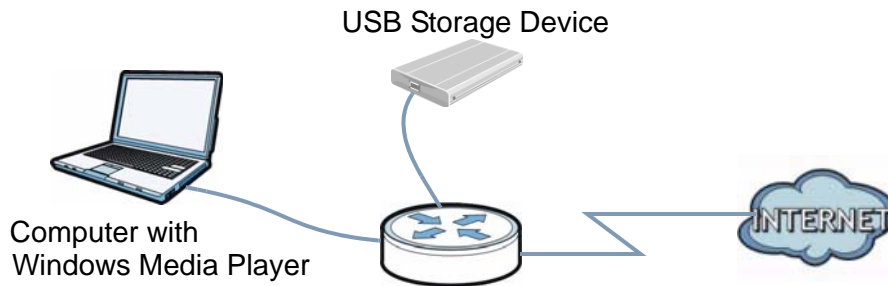
To use your CellPipe 7130 RG as a media server, click **USB Services > Media Server**.



Check **Enable Media Server** and click **Apply**. This enables DLNA-compliant media clients to play the video, music and image files in your USB storage device.

2.6.2 Using Windows Media Player

This section shows you how to play the media files on the USB storage device connected to your CellPipe 7130 RG using Windows Media Player.

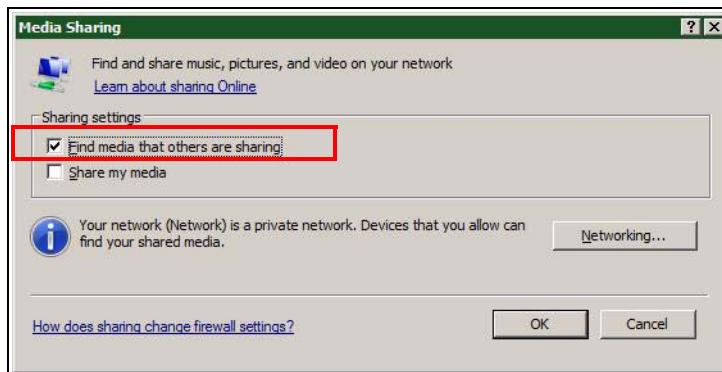


Windows Vista

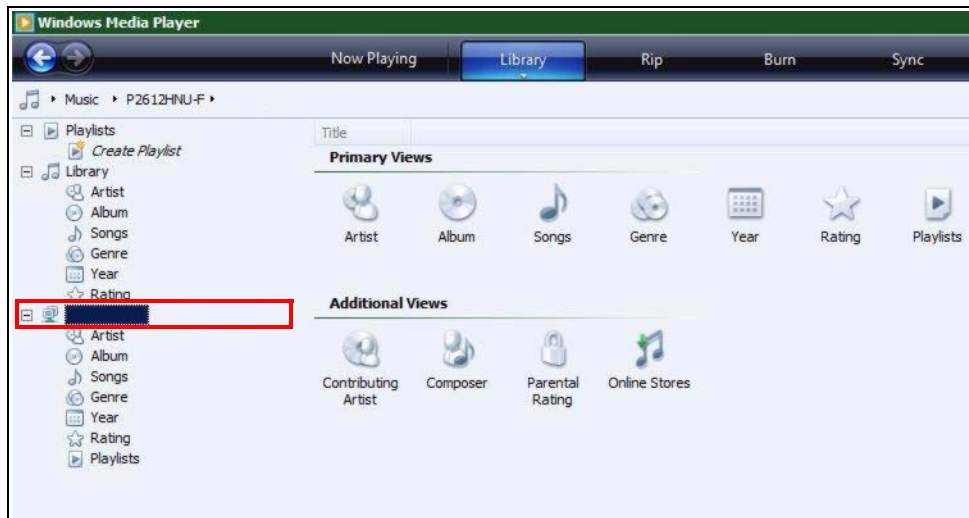
- 1 Open Windows Media Player and click **Library > Media Sharing** as follows.



- 2 Check **Find media that others are sharing** in the following screen and click **OK**.



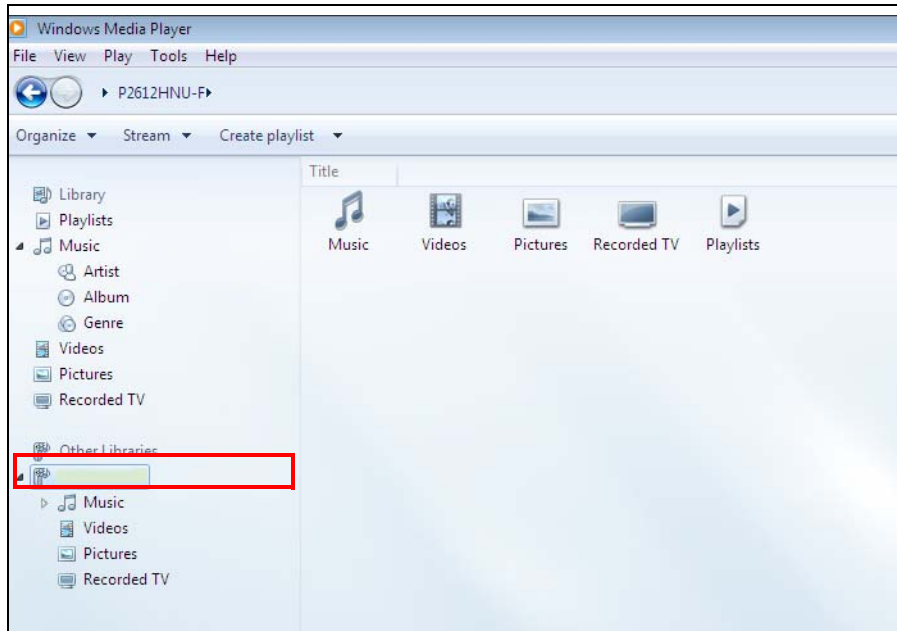
- 3 In the **Library** screen, check the left panel. The Windows Media Player should detect the CellPipe 7130 RG.



The CellPipe 7130 RG displays as a playlist. Clicking on the category icons in the right panel shows you the media files in the USB storage device attached to your CellPipe 7130 RG.

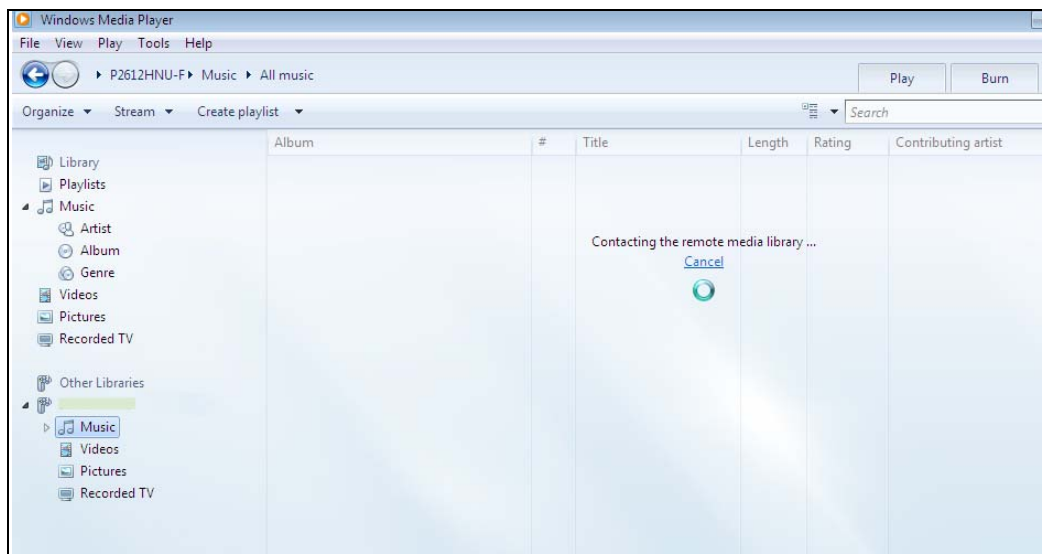
Windows 7

- 1 Open Windows Media Player. It should automatically detect the CellPipe 7130 RG.

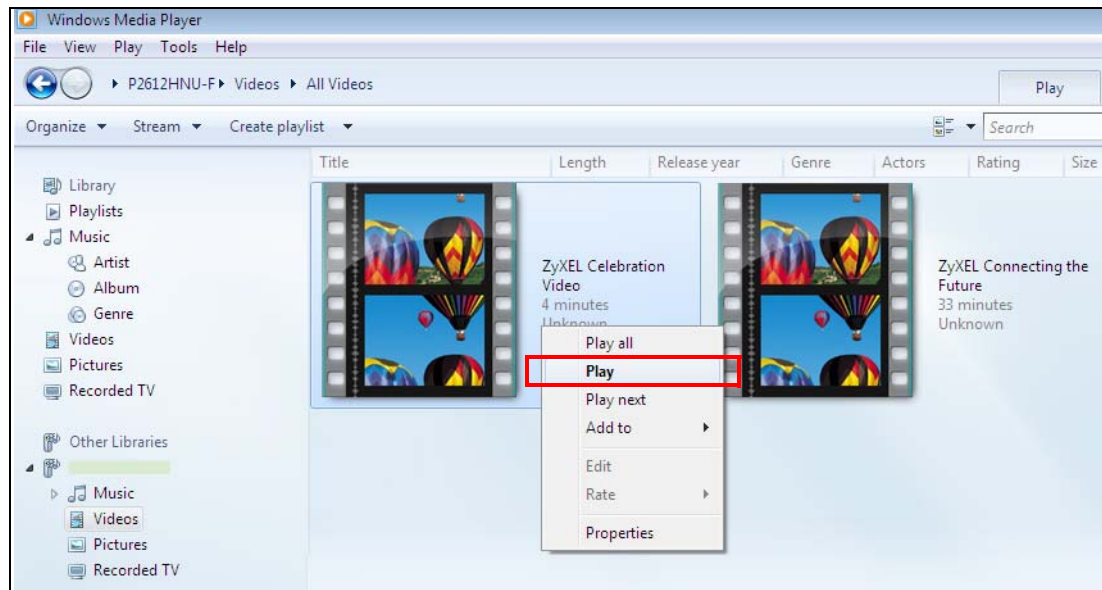


If you cannot see the CellPipe 7130 RG in the left panel as shown above, right-click **Other Libraries > Refresh Other Libraries**.

- 2 Select a category in the left panel and wait for Windows Media Player to connect to the CellPipe 7130 RG.



- 3 In the right panel, you should see a list of files available in the USB storage device.

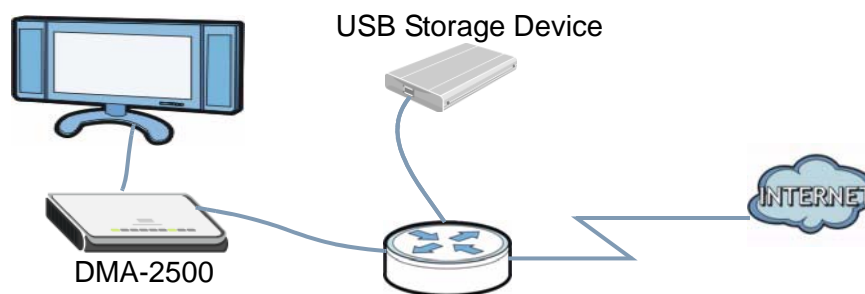


2.6.3 Using a Digital Media Adapter

This section shows you how you can use the CellPipe 7130 RG with a DMA to play media files stored in the USB storage device in your TV screen.

Note: For this tutorial, your DMA should already be set up with the TV according to the instructions in the DMA's Quick Start Guide.

- 1 Connect the DMA to an available LAN port in your CellPipe 7130 RG.



- 2 Turn on the TV and wait for the DMA's **Home** (or similar) screen to appear. Using the remote control, go to **MyMedia** (or similar) to open the following screen. Select the CellPipe 7130 RG as your media server.



- 3 The screen shows you the list of available media files in the USB storage device. Select the file you want to open and push the **Play** button in the remote control.



2.7 Using the File Sharing Feature

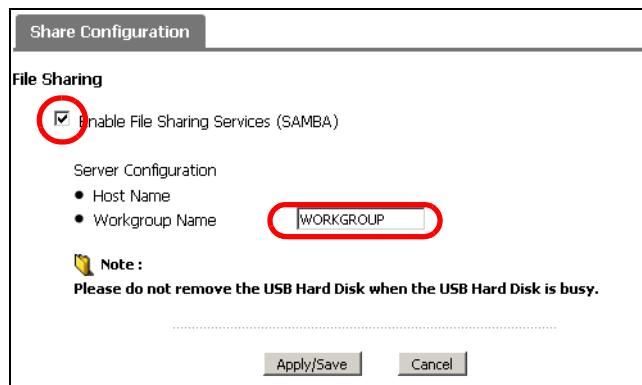
In this section you can:

- Set up file sharing
- Access the shared files from a computer

2.7.1 Set Up File Sharing

To set up file sharing, you need to enable file sharing on your CellPipe 7130 RG. This shares the files in your USB device to other users in the local network.

Go to **USB Services > File Sharing > Share Configuration** to enable file sharing and enter a workgroup name. Click **Apply** to save your settings.



This sets up the file sharing server.

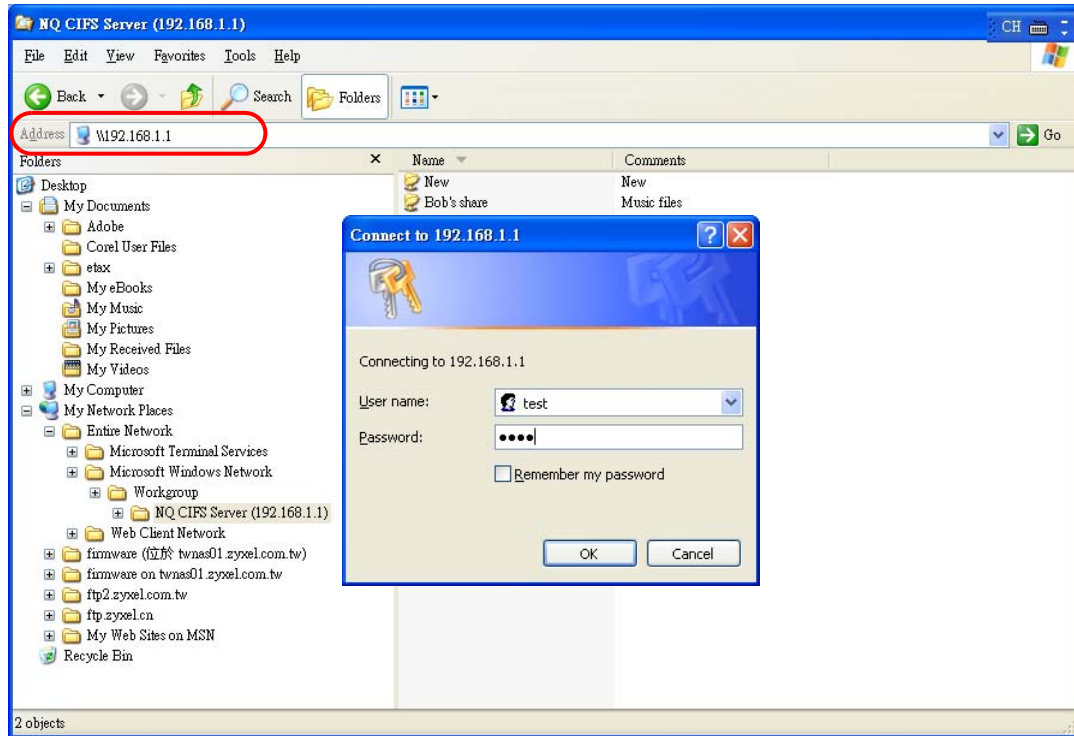
2.7.2 Access Your Shared Files From a Computer

You can use Windows Explorer to access the file storage devices connected to the CellPipe 7130 RG.

Note: The examples in this User's Guide show you how to use Microsoft's Windows XP to browse your shared files. Refer to your operating system's documentation for how to browse your file structure.

Open Windows Explorer to access Bob's Share using Windows Explorer browser.

- 1 In Windows Explorer's Address bar type a double backslash “\\” followed by the IP address of the CellPipe 7130 RG (the default IP address of the CellPipe 7130 RG is 192.168.1.1) and press [ENTER]. A screen asking for password authentication appears. Type the user name and password and click **OK**.

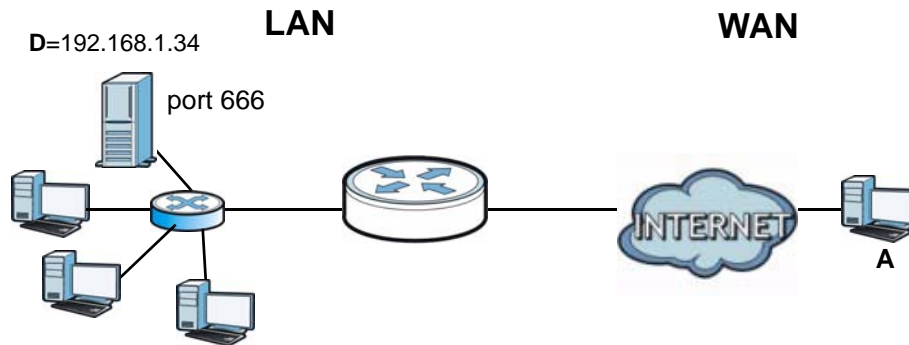


Once you log in to the shared folder via your CellPipe 7130 RG, you do not have to re-log in unless you restart your computer.

2.8 Setting Up NAT Port Forwarding

Thomas manages the Doom server on a computer behind the CellPipe 7130 RG. In order for players on the Internet (like **A** in the figure below) to communicate with the Doom server, Thomas needs to configure the port settings and IP address on the CellPipe 7130 RG. Traffic should be forwarded to the port 666 of the Doom server computer which has an IP address of 192.168.1.34. Additionally, players

are only allowed to access the Doom server on Friday to Saturday, from 1PM to 8PM.



Thomas may set up the port settings by configuring the port settings for the Doom server computer (see [Section 8.3 on page 172](#) for more information).

- 1 Click **Network** > **NAT** to open the **Port Forwarding** screen. Enter the following values:

Service Name	Select User Defined . In the screen that opens, enter Doom_Server as the Service Name .
WAN Interface	Select the WAN interface through which the Doom service is forwarded. This is the default interface for this example, which is ipoe_eth4_1 .
Server IP Address	Enter the IP address of the Doom server. This is 192.168.1.34 for this example.
External Port/s	Enter 666 as the Start and End port.
Protocol	Select TCP/UDP . This should be the protocol supported by the Doom server.
Start/Stop Time Select Days	Enter 13:00 ~ 20:00 in the time fields and select Friday ~ Saturday in the day field.

- 2 The screen should display as follows. Click **Add**.

Rule Setup

Active

Service Name:

WAN Interface:

External Start Port:

External End Port:

Internal Start Port:

Internal End Port:

Server IP Address:

Protocol:

Start Time:

Stop Time:

Select Days: SUN MON TUE WED THU FRI SAT

- 3 The port forwarding settings you configured should appear in the table. Click **Apply** to have the CellPipe 7130 RG start forwarding port 666 traffic to the computer with IP address 192.168.1.34.

Port Forwarding												
Port Forwarding												
Service Name	WAN Interface	Server IP Address	External port		Internal port		Protocol	Time(24H)		Time(24H)		
WWW	ipoe_0_33/atm0	192.168.1.	Start:80	End:80	Start:80	End:80	TCP	Start:00:00	Stop:23:59		Add	
Select Days: <input type="checkbox"/> SUN <input type="checkbox"/> MON <input type="checkbox"/> TUE <input type="checkbox"/> WED <input type="checkbox"/> THU <input type="checkbox"/> FRI <input type="checkbox"/> SAT												
No.	Active	Service Name	WAN Interface	External Start Port	External End Port	Internal Start Port	Internal End Port	Server IP Address	Start Time	Stop Time	Days	Modif.
1	<input checked="" type="checkbox"/>	Doom_Server	eth4_1	666	666	666	666	192.168.1.34	13:00	20:00	Fri,Sat	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

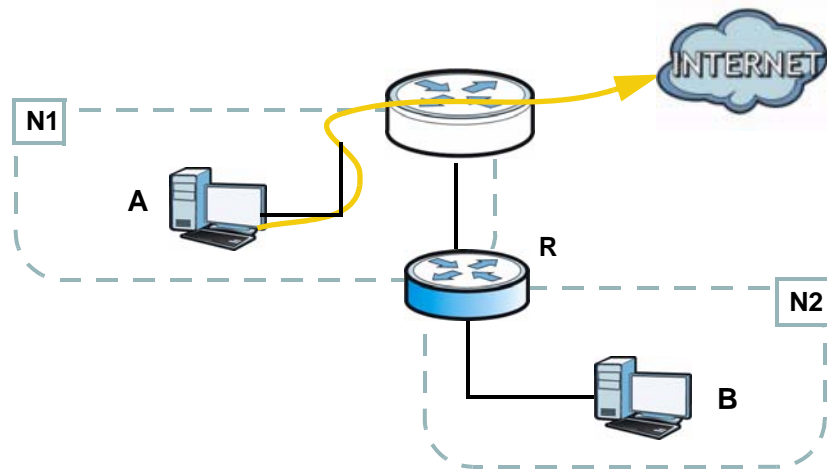
Players on the Internet then can have access to Thomas' Doom server.

2.9 Configuring Static Route for Routing to Another Network

In order to extend your Intranet and control traffic flowing directions, you may connect a router to the CellPipe 7130 RG's LAN. The router may be used to separate two department networks. This tutorial shows how to configure a static routing rule for two network routings.

In the following figure, router **R** is connected to the CellPipe 7130 RG's LAN. **R** connects to two networks, **N1** (192.168.1.x/24) and **N2** (192.168.10.x/24). If you want to send traffic from computer **A** (in **N1** network) to computer **B** (in **N2**

network), the traffic is sent to the CellPipe 7130 RG's WAN default gateway by default. In this case, **B** will never receive the traffic.



You need to specify a static routing rule on the CellPipe 7130 RG to specify **R** as the router in charge of forwarding traffic to **N2**. In this case, the CellPipe 7130 RG routes traffic from **A** to **R** and then **R** routes the traffic to **B**. This tutorial uses the following example IP settings:

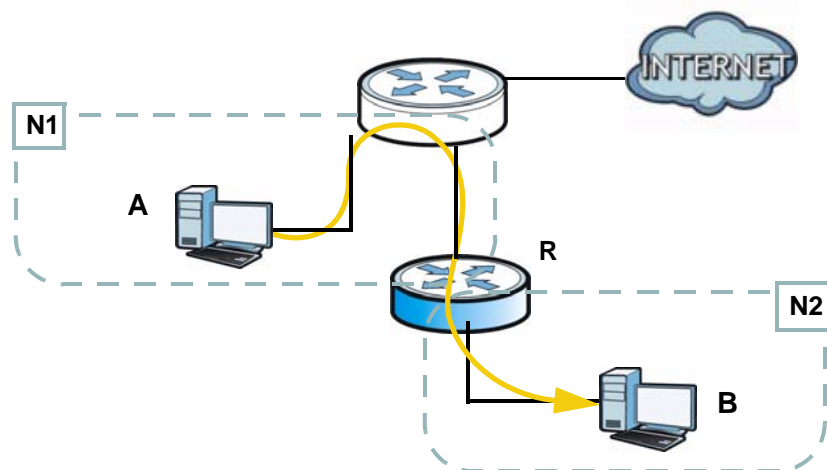


Table 6 IP Settings in this Tutorial

DEVICE / COMPUTER	IP ADDRESS
The CellPipe 7130 RG's WAN	172.16.1.1
The CellPipe 7130 RG's LAN	192.168.1.1
A	192.168.1.34
R's N1	192.168.1.253

Table 6 IP Settings in this Tutorial

DEVICE / COMPUTER	IP ADDRESS
R's N2	192.168.10.2
B	192.168.10.33

To configure a static route to route traffic from **N1** to **N2**:

- 1 Click **Advanced** > **Static Route**. Click **Add**.

The screenshot shows the 'IP Static Route' configuration window. At the top, there is a tab labeled 'IP Static Route'. Below it, the section 'Static Route Rules' contains a table with columns: #, Active, Destination, Netmask, Gateway, Interface, and Modify. Below the table, there are two buttons: 'Add' and 'Apply'. The 'Add' button is circled in red.

- 2 Configure the **Static Route Setup** screen using the following settings:

- Select **Active**.
- Type **192.168.10.0** and subnet mask **255.255.255.0** for the destination, **N2**.
- Select the Internet connection interface for this route, **ipoe_0_0_33/atm0** in this example.
- Type **192.168.1.253** (**R's N1** address) in the **Gateway IP Address** field.

The screenshot shows the 'Static Route Setup' configuration window. It has several fields:

- Active
- Destination IP Address: 192.168.10.0
- IP Subnet Mask: 255.255.255.0
- Use Interface: ipoe_0_0_33/atm0 (selected from a dropdown)
- Use Gateway IP Address: 192.168.1.253

 At the bottom, there are three buttons: 'Back', 'Apply', and 'Cancel'.

Click **Apply**. The **Advanced** > **Static Route** screen should display the route you just added.

The screenshot shows the 'IP Static Route' configuration window after applying the settings. The 'Static Route Rules' table now contains one entry:

#	Active	Destination	Netmask	Gateway	Interface	Modify
1	<input checked="" type="checkbox"/>	192.168.10.0	255.255.255.0	192.168.1.253	atm0	

 The first row of the table is circled in red. Below the table are 'Add' and 'Apply' buttons.

Now **B** should be able to receive traffic from **A**. You may need to additionally configure **B's** firewall settings to allow specific traffic to pass through.

2.10 Configuring QoS Queue and Class Setup

This section contains tutorials on how you can configure the QoS screen.

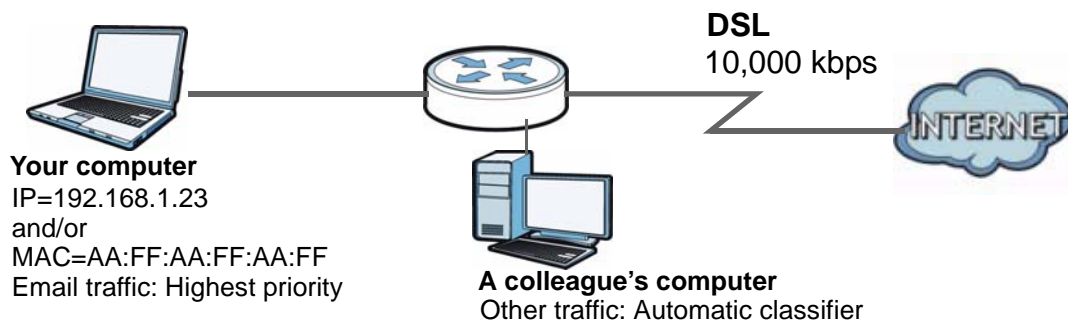
Let's say you are a team leader of a small sales branch office. You want to prioritize e-mail traffic because your task includes sending urgent updates to clients at least twice every hour. You also upload data files (such as logs and e-mail archives) to the FTP server throughout the day. Your colleagues use the Internet for research, as well as chat applications for communicating with other branch offices.

In the following figure, your Internet connection has an upstream transmission bandwidth of 10,000 kbps. For this example, you want to configure QoS so that e-mail traffic gets the highest priority with at least 5,000 kbps. You can do the following:

- Configure a queue to assign the highest priority queue (7) to e-mail traffic from the LAN interface, so that e-mail traffic would not get delayed when there is network congestion.
- Note the IP address (192.168.1.23 for example) and/or MAC address (AA:FF:AA:FF:AA:FF for example) of your computer and map it to queue 7.

Note: QoS is applied to traffic flowing out of the CellPipe 7130 RG.

Traffic that does not match this class is assigned a priority queue based on the internal QoS mapping table on the CellPipe 7130 RG.



- 1 Click **Advanced > QoS > General** and check **Active**. Set your **WAN Managed Upstream Bandwidth** to 10,000 kbps (or leave this blank to have the CellPipe 7130 RG automatically determine this figure).

General Queue Setup Class Setup Policer Setup Monitor

General

Active QoS

WAN Managed Upstream Bandwidth 10000 (kbps)

(You can assign the upstream bandwidth manually. If the field is empty, the CPE set the value automatically.)

Apply Cancel

- 2 Go to **Advanced > QoS > Queue Setup**. Click **Add** to create a new queue. In the screen that opens, check **Active** and enter or select the following values:
 - **Name:** E-mail
 - **Priority:** 4 (High)
 - **Weight:** 8
 - **Rate Limit:** 5,000 (kbps)

Queue Configuration

Active

Name: E-Mail

Interface: LAN1

Priority: 4

Weight: 8

Buffer Management: Drop Tail (DT)

Scheduler Algorithm: PQWFQ

Rate Limit: 5000 (kbps)

Back Apply Cancel

- 3 Go to **Advanced > QoS > Class Setup**. Click **Add** to create a new class. Check **Active** and follow the settings as shown in the screen below.

Class Configuration

Active

Class Name

Classification Order

Forward To Interface

DSCP Mark (0~63)

802.1P Mark

VLAN ID Tag (0~4094)

To Queue

Criteria Configuration

Basic

From Interface

Ether Type

Source

MAC Address MAC Mask Exclude

IP Address IP Subnet Mask Exclude

TCP/UDP Port Range ~ Exclude

Destination

MAC Address MAC Mask Exclude

IP Address IP Subnet Mask Exclude

TCP/UDP Port Range ~ Exclude

Others

802.1P Exclude

VLAN ID (0~4094) Exclude

IP Protocol Exclude

IP Packet Length ~ Exclude

DSCP (0~63) Exclude

TCP ACK Exclude

DHCP Exclude

Note :
Support DHCP options only when routing mode.

Class Name	Give a class name to this traffic, such as E-mail in this example.
To Queue	Link this to an item in the Advanced > QoS > Queue Setup screen, which is the E-mail queue created in this example.
From Interface	This is the interface from which the traffic will be coming from. Select LAN1 .

Ether Type	Select IP to identify the traffic source by its IP address or MAC address.
MAC Address	Type the MAC address of your computer - AA:FF:AA:FF:AA:FF . Type the MAC Mask if you know it.
IP Address	Type the IP address of your computer - 192.168.1.23 . Type the IP Subnet Mask if you know it.

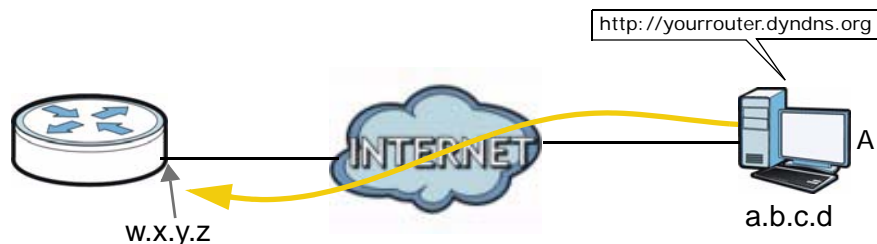
This maps e-mail traffic coming from port 25 to the highest priority, which you have created in the previous screen (see the **IP Protocol** field). This also maps your computer's IP address and MAC address to the **E-mail** queue (see the **Source** fields).

- 4 Verify that the queue setup works by checking **Advanced > QoS > Monitor**. This shows the bandwidth allotted to e-mail traffic compared to other network traffic.

General Queue Setup Class Setup Policer Setup Monitor				
Monitor				
Refresh Interval <input type="text" value="No Refresh"/>				
Queue Monitor				
No.	Name	Pass Rate (bps)	Drop Rate (bps)	
1	E-mail	802	94	

2.11 Access the CellPipe 7130 RG Using DDNS

If you connect your CellPipe 7130 RG to the Internet and it uses a dynamic WAN IP address, it is inconvenient for you to manage the device from the Internet. The CellPipe 7130 RG's WAN IP address changes dynamically. Dynamic DNS (DDNS) allows you to access the CellPipe 7130 RG using a domain name.



To use this feature, you have to apply for DDNS service at www.dyndns.org.

This tutorial shows you how to:

- [Registering a DDNS Account on \[www.dyndns.org\]\(http://www.dyndns.org\)](#)
- [Configuring DDNS on Your CellPipe 7130 RG](#)
- [Testing the DDNS Setting](#)

Note: If you have a private WAN IP address, then you cannot use DDNS.

2.11.1 Registering a DDNS Account on www.dyndns.org

- 1 Open a browser and type **<http://www.dyndns.org>**.
- 2 Apply for a user account. This tutorial uses **UserName1** and **12345** as the username and password.
- 3 Log into www.dyndns.org using your account.
- 4 Add a new DDNS host name. This tutorial uses the following settings as an example.
 - Hostname: **yourrouter.dyndns.org**
 - Service Type: **Host with IP address**
 - IP Address: Enter the WAN IP address that your CellPipe 7130 RG is currently using. You can find the IP address on the CellPipe 7130 RG's Web Configurator **Home** page.

Then you will need to configure the same account and host name on the CellPipe 7130 RG later.

2.11.2 Configuring DDNS on Your CellPipe 7130 RG

Configure the following settings in the **Advanced > Dynamic DNS** screen.

- Select **Active Dynamic DNS**.
- Select **Dynamic DNS** for the DDNS type.
- Type **yourrouter.dyndns.org** in the **Host Name** field.

- Enter the user name (**UserName1**) and password (**12345**).

Dynamic DNS Setup

Service Provider	WWW.DynDNS.ORG
Host Name	yourrouter.dyndns.org
Interface	ipoe_eth4_1/eth4_1
User Name	UserName1
Password
Email	
Key	

Apply Cancel

Click **Apply**.

2.11.3 Testing the DDNS Setting

Now you should be able to access the CellPipe 7130 RG from the Internet. To test this:

- 1 Open a web browser on the computer (using the IP address **a.b.c.d**) that is connected to the Internet.
- 2 Type **http://yourrouter.dyndns.org** and press [Enter].
- 3 The CellPipe 7130 RG's login page should appear. You can then log into the CellPipe 7130 RG and manage it.

Introducing the Web Configurator

3.1 Overview

The web configurator is an HTML-based management interface that allows easy device setup and management via Internet browser. Use Internet Explorer 6.0 and later versions. The recommended screen resolution is 1024 by 768 pixels.

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

See [Appendix C on page 351](#) if you need to make sure these functions are allowed in Internet Explorer.

3.2 User Levels

There are three (3) user levels for logging into the CellPipe 7130 RG. The accounts have different access rights as follows :

- **Subscriber** - the default user name is **admin** and the password is **telus**. You can change the user name and password for this account. You can also change all the Web Configurator screens using this account.
- **Privileged** - the default user name is **root** and the password is **telus**. You can change the user name and password for this account. You cannot access the **Advanced > Remote MGMT > Service Control** screen but you can still use the SSH service. You can also modify the rest of the Web Configurator screens.
- **Installer** - the default user name is **tech** and the password is **telus**. You cannot change the user name or password for this account. The Web Configurator is read-only so you also cannot modify any of the screens using this account. In addition, this account cannot view the following screens:

Advanced > Remote MGNT > Service Control
Network > WLAN > WPS Station
Maintenance > Tools > Firmware
Maintenance > Tools > Configuration
Maintenance > Tools > Restart

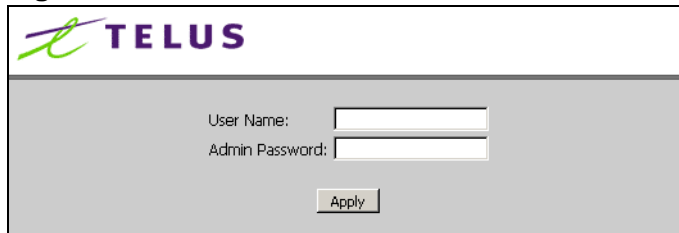
This account has no access to files shared through the **USB Services** screens.

Note: The CellPipe 7130 RG supports multiple remote management sessions running at one time.

3.2.1 Accessing the Web Configurator

- 1 Make sure your CellPipe 7130 RG hardware is properly connected (refer to the Quick Start Guide).
- 2 Launch your web browser.
- 3 Type "http://192.168.1.1" as the URL.
- 4 A password screen displays. Enter the default administrator user name **admin** and default administrator password **telus**. The password displays in non-readable characters. If you have changed the password, enter your password and click **OK**. Click **Cancel** to revert to the default password in the password field.

Figure 8 Password Screen



The screenshot shows a web browser window with the TELUS logo at the top left. Below the logo, there are two input fields: "User Name:" and "Admin Password:". The "Admin Password:" field is masked with asterisks. Below the input fields is an "Apply" button.

Note: Refer to [Section 3.2 on page 83](#) for user level information. Each user level has its own account information for logging into the CellPipe 7130 RG.

3.3 Web Configurator Main Screen

Figure 9 Home

The screenshot shows the TELUS Web Configurator Home screen. The interface is divided into four main sections:

- A**: Title bar containing the TELUS logo and 'Home' and 'Logout' buttons.
- B**: Navigation panel on the left with a tree view: Network (WAN, LAN, Wireless LAN, NAT, USB Services), Security, Advanced, and Maintenance.
- C**: Main window displaying system status information:
 - Device Information**: User Name: admin, Model Number: 5Vz.A2011, MAC Address: 40:4a:03:ad:70:47, Firmware Version: 0.0.01.GEN, DSL Firmware Version: A2pv6C016.d22f.
 - System Status**: System Uptime: 0 days: 6 hours:24 minutes, Current Date/Time: 01 Jan 2000 06:24:30, System Mode: Routing / Bridging, CPU Usage: 4.00%, Memory Usage: 55%.
 - WAN 0 Information**: Mode: ATM/IPoE, IP Address: 0.0.0.0, IP Subnet Mask: 0.0.0.0.
 - WAN 1 Information**: Mode: PTM/IPoE, IP Address: 0.0.0.0, IP Subnet Mask: 0.0.0.0.
 - LAN Information**: IP Address: 172.23.26.249, IP Subnet Mask: 255.255.255.0, DHCP: Server.
 - WLAN Information**: Channel: 6 (auto), WPS Status: Configured, WDS Status: AP.
 - AP 1 Information**: ESSID: CellPipe_5Vz.A2011_AD7048, Status: Active, Security: Mixed WPA2-PSK/WPA-PSK.
 - Interface Status** table:

Interface	Status	Rate
DSL	Link Down	kbps / kbps
ETH WAN	NoLink	N/A
LAN1	NoLink	N/A
LAN2	NoLink	N/A
LAN3	NoLink	N/A
LAN4	Up	100M / Full
HPNA	NoLink	N/A
WLAN	Up	150M
 - More Status**: Links for WAN Service Statistics, LAN Statistics, Route Info, Client List, and WLAN Station List.
- D**: Status bar at the bottom showing a message 'Ready'.

As illustrated above, the main screen is divided into these parts:

- **A** - title bar
- **B** - navigation panel
- **C** - main window
- **D** - status bar

3.3.1 Navigation Panel

Use the menu items on the navigation panel to open screens to configure CellPipe 7130 RG features. The following tables describe each menu item.

Table 7 Navigation Panel Summary

LINK	TAB	FUNCTION
Home		This screen shows the CellPipe 7130 RG's general device and network status information. Use this screen to access the statistics and client list.
Network		
WAN	Mode	Use this screen to choose between DSL and Ethernet for your Internet connection.
	Connect	Use this screen to add or remove a DSL PTM (Packet Transfer Mode) interface.
	Services	Use this screen to configure ISP parameters, WAN IP address assignment, and other advanced properties.
LAN	IP	Use this screen to configure LAN TCP/IP, DHCP and IP alias settings.
Wireless LAN	General	Use this screen to configure the wireless LAN settings, WLAN authentication/security settings and MAC filtering rules.
	More AP	Use this screen to configure multiple BSSs on the CellPipe 7130 RG.
	WPS	Use this screen to enable WPS (Wi-Fi Protected Setup) and view the WPS status.
	WPS Station	Use this screen to use WPS to set up your wireless network.
	WDS	Use this screen to set up Wireless Distribution System links to other access points.
	Advanced Setup	Use this screen to configure the advanced wireless LAN settings.
NAT	Port Forwarding	The NAT screens are available only when you enable NAT in a WAN connection. Use this screen to make your local servers visible to the outside world.
	DMZ Host	Use this screen to configure a default server which receives packets from ports that are not specified in the Port Forwarding screen.
	ALG	Use this screen to allow SIP sessions to pass through the CellPipe 7130 RG.
USB Services		
File Sharing	Share Configuration	Use this screen to enable file sharing via the CellPipe 7130 RG.
Media Server	Media Server Configuration	Use this screen to enable the media server on the CellPipe 7130 RG.
	Remove Disk Safely	Use this screen to safely disconnect the USB device from the CellPipe 7130 RG

Table 7 Navigation Panel Summary

LINK	TAB	FUNCTION
Security		
Firewall	Incoming	This screen shows a summary of the IP filtering rules, and allows you to add or remove an incoming IP filtering rule that allows incoming traffic from the WAN.
	DoS	Use this screen to activate protection against Denial of Service (DoS) attacks.
Certificate	Local Certificates	Use this screen to view a summary list of certificates and manage certificates and certification requests.
	Trusted CA	Use this screen to view and manage the list of the trusted CAs.
Advanced		
Static Route	IP Static Route	Use this screen to configure IP static routes to tell your device about networks beyond the directly connected remote nodes.
Policy Forwarding		Use this screen to configure policy routing on the CellPipe 7130 RG.
RIP		Use this screen to configure RIP (Routing Information Protocol) settings.
QoS	General	Use this screen to enable QoS.
	Queue Setup	Use this screen to configure QoS queues.
	Class Setup	Use this screen to define a classifier.
	Policer Setup	Use this screen to specify the committed rate and committed burst size for incoming packets.
	Monitor	Use this screen to view QoS packets statistics.
Dynamic DNS		This screen allows you to use a static hostname alias for a dynamic IP address.
Remote MGMT	TR069	Use this screen to configure the CellPipe 7130 RG to be managed by an ACS (Auto Configuration Server).
	TR064	Use this screen to enable management via TR-064 on the LAN.
	ServiceControl	Use this screen to configure which services/protocols can access which CellPipe 7130 RG interface.
	IPAddress	Use this screen to configure from which IP address(es) users can manage the CellPipe 7130 RG.
UPnP	General	Use this screen to turn UPnP on or off.
Parental Control	Time Restriction	Use this screen to configure the days and times when the restrictions are enforced.
	Content Filter	Use this screen to prevent users of your network from viewing inappropriate web content.
IGMP	IGMP	Use this screen to select the IGMP version to use as well as configure the settings for IGMP.
	IGMP Source Configuration	Use this screen to set the server where the CellPipe 7130 RG gets the multicast group information
Maintenance		

Table 7 Navigation Panel Summary

LINK	TAB	FUNCTION
System	General	Use this screen to configure your device's name, domain name, management inactivity timeout and password.
	Time Setting	Use this screen to change your CellPipe 7130 RG's time and date.
Logs	View Log	Use this screen to view the logs for the level that you selected.
	Log Settings	Use this screen to change your CellPipe 7130 RG's log settings.
Tools	Firmware	Use this screen to upload firmware to your device.
	Configuration	Use this screen to backup and restore your device's configuration (settings) or reset the factory default settings.
	Restart	This screen allows you to reboot the CellPipe 7130 RG without turning the power off.
Diagnostic	General	Use this screen to test the connections to other devices.
	802.1ag	Use this screen to configure CFM (Connectivity Fault Management) MD (maintenance domain) and MA (maintenance association), perform connectivity tests and view test reports.
	OAM Ping Test	These screen displays information to help you identify problems with the DSL connection.

3.3.2 Main Window

The main window displays information and configuration fields. It is discussed in the rest of this document.

Right after you log in, the **Status** screen is displayed. See [Chapter 4 on page 91](#) for more information about the **Status** screen.

3.3.3 Status Bar

Check the status bar when you click **Apply** or **OK** to verify that the configuration has been updated.

PART II

Technical Reference

Status Screens

4.1 Overview

Use the **Status** screens to look at the current status of the device, system resources and interfaces (LAN, WAN and WLAN). The **Status** screen also provides detailed information from DHCP and statistics from traffic.


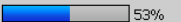
4.2 Status Screen

Click **Home** to open this screen.

Figure 10 Status Screen

Refresh Interval :

Device Information		
User Name:	admin	
Model Number:	5Vz.A2011	
MAC Address:	40:4a:03:ad:70:47	
Firmware Version:	0.0.01.GEN	
DSL Firmware Version:	A2pv6C016.d22f	
WAN 0 Information		
- Mode:	ATM/IPoE	
- IP Address:	0.0.0.0	
- IP Subnet Mask:	0.0.0.0	
WAN 1 Information		
- Mode:	PTM/IPoE	
- IP Address:	0.0.0.0	
- IP Subnet Mask:	0.0.0.0	
LAN Information		
- IP Address:	172.23.26.249	
- IP Subnet Mask:	255.255.255.0	
- DHCP:	Server	
WLAN Information		
- Channel:	11 (auto)	
- WPS Status:	Configured	
- WDS Status:	AP	
AP 1 Information		
- ESSID:	CellPipe_5Vz.A2011_AD7048	
- Status:	Active	
- Security:	Mixed WPA2-PSK/WPA-PSK	

System Status		
System Uptime:	0 days: 0 hours:27 minutes	
Current Date/Time:	01 Jan 2000 00:27:31	
System Mode:	Routing / Bridging	
CPU Usage:	 3.00%	
Memory Usage:	 53%	

Interface Status		
Interface	Status	Rate
DSL	Link Down	kbps / kbps
ETH WAN	NoLink	N/A
LAN1	NoLink	N/A
LAN2	NoLink	N/A
LAN3	NoLink	N/A
LAN4	Up	100M / Full
HPNA	NoLink	N/A
WLAN	Up	150M

More Status

[WAN Service Statistics](#) [LAN Statistics](#)

[Route Info](#) [Client List](#)

[WLAN Station List](#)

Each field is described in the following table.

Table 8 Status Screen

LABEL	DESCRIPTION
Refresh Interval	Enter how often you want the CellPipe 7130 RG to update this screen.
Apply	Click this to update this screen immediately.
Device Information	
User Name	This field displays the CellPipe 7130 RG system name. It is used for identification. Click this to go to the screen where you can change it.
Model Number	This is the model name of your device.
MAC Address	This is the MAC (Media Access Control) or Ethernet address unique to your CellPipe 7130 RG.
Firmware Version	This field displays the current version of the firmware inside the device. It also shows the date the firmware version was created. Click this to go to the screen where you can change it.
DSL Firmware Version	This field displays the current version of the device's DSL modem code.
WAN Information	Information displays for each WAN interface you add to the CellPipe 7130 RG.
Mode	This is the method of encapsulation used by your ISP.
IP Address	This field displays the current IP address of the CellPipe 7130 RG in the WAN.
IP Subnet Mask	This field displays the current subnet mask in the WAN.
LAN Information	
IP Address	This field displays the current IP address of the CellPipe 7130 RG in the LAN. Click this to go to the screen where you can change it.
IP Subnet Mask	This field displays the current subnet mask in the LAN.
DHCP	<p>This field displays what DHCP services the CellPipe 7130 RG is providing to the LAN. Choices are:</p> <p>Server - The CellPipe 7130 RG is a DHCP server in the LAN. It assigns IP addresses to other computers in the LAN.</p> <p>Relay - The CellPipe 7130 RG acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients.</p> <p>None - The CellPipe 7130 RG is not providing any DHCP services to the LAN.</p> <p>Click this to go to the screen where you can change it.</p>
WLAN Information	
Channel	This is the channel number used by the CellPipe 7130 RG now.

Table 8 Status Screen

LABEL	DESCRIPTION
WPS Status	This field displays the status of WPS (Wi-Fi Protected Setup). Click this to go to the screen where you can change it.
WDS Status	This field displays <ul style="list-style-type: none"> • AP when WDS is disabled. • Bridge when the CellPipe 7130 RG functions as a wireless network bridge only to use WDS (Wireless Distribution System) to establish wireless links with other APs. • AP+Bridge when WDS is enabled and the CellPipe 7130 RG acts as a bridge and access point simultaneously. Click this to go to the screen where you can change it
AP Information	Information displays for each AP profile you activate on the CellPipe 7130 RG.
ESSID	This is the descriptive name used to identify the CellPipe 7130 RG in this wireless network. Click this to go to the screen where you can change it.
Status	This shows the current status of the wireless network.
Security	This shows the level of wireless security the CellPipe 7130 RG is using in this wireless network.
System Status	
System Uptime	This field displays how long the CellPipe 7130 RG has been running since it last started up. The CellPipe 7130 RG starts up when you plug it in, when you restart it (Maintenance > Tools > Restart), or when you reset it (see Section 1.7 on page 28).
Current Date/Time	This field displays the current date and time in the CellPipe 7130 RG. You can change this in Maintenance > System > Time Setting .
System Mode	This displays whether the CellPipe 7130 RG is functioning as a router or a bridge.
CPU Usage	This field displays what percentage of the CellPipe 7130 RG's processing ability is currently used. When this percentage is close to 100%, the CellPipe 7130 RG is running at full load, and the throughput is not going to improve anymore. If you want some applications to have more throughput, you should turn off other applications (for example, using QoS; see Chapter 16 on page 219).
Memory Usage	This field displays what percentage of the CellPipe 7130 RG's memory is currently used. Usually, this percentage should not increase much. If memory usage does get close to 100%, the CellPipe 7130 RG is probably becoming unstable, and you should restart the device. See Section 24.4 on page 280 , or turn off the device (unplug the power) for a few seconds.
Interface Status	
Interface	This column displays each interface the CellPipe 7130 RG has.

Table 8 Status Screen

LABEL	DESCRIPTION
Status	<p>This field indicates whether or not the CellPipe 7130 RG is using the interface.</p> <p>For the DSL interface, this field displays LinkDown (line is down) or Up (line is up or connected).</p> <p>For the LAN or Ethernet WAN interface, this field displays Up when the CellPipe 7130 RG is using the interface and NoLink when the line is disconnected.</p> <p>For the WLAN interface, it displays Up when WLAN is enabled or Disabled when WLAN is not active.</p>
Rate	<p>For the DSL interface, it displays the downstream and upstream transmission rate.</p> <p>For the LAN or Ethernet WAN interface, this displays the port speed and duplex setting.</p> <p>For the WLAN interface, it displays the maximum transmission rate.</p>
More Status	
WAN Service Statistics	Click this link to view packet specific statistics of the WAN connection(s). See Section 4.2.1 on page 94 .
Route Info	Click this link to view the internal routing table on the CellPipe 7130 RG. See Section 4.2.2 on page 96 .
WLAN Station List	Click this link to display the MAC address(es) of the wireless stations that are currently associating with the CellPipe 7130 RG. See Section 4.2.3 on page 97 .
LAN Statistics	Click this link to view packet specific statistics on the LAN and WLAN interfaces. See Section 4.2.4 on page 98 .
Client List	Click this link to view current DHCP client information. See Section 4.2.5 on page 99 .

4.2.1 WAN Service Statistics

Click **Status > WAN Service Statistics** to access this screen. Use this screen to view the WAN statistics.

Figure 11 Status > WAN Service Statistics

WAN Services Statistics									
Interface	Description	Received				Transmitted			
		Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
atm0	ipoe_0_0_33	0	0	0	0	0	0	0	915
ptm0_1	ipoe_0_0_1_1	0	0	0	0	269010	915	0	0
eth4_1	ipoe_eth4_1	0	0	0	0	269010	915	0	0

Close

Refresh Interval : sec

The following table describes the labels in this screen.

Table 9 Status > WAN Service Statistics

LABEL	DESCRIPTION
Interface	<p>This shows the name of the WAN interface used by this connection.</p> <p>A default name ipoa0, pppoa1, atmx (where x starts from 0 and is the index number of ATM layer-2 interfaces using different VPI and/or VCI values) or ptm0 indicates the DSL port. The pppx name (where x starts from 0 and is the index number of PPP connection on the CellPipe 7130 RG) indicates a PPP connection via any one of the WAN interface. eth4 indicates the Ethernet WAN interface (the physical Ethernet WAN port).</p> <p>The number after the dot (.) represents the VLAN ID number assigned to traffic sent through this connection. The number after the underscore (_) represents the index number of connections through the same interface.</p> <p>(null) means the entry is not valid.</p>
Description	<p>This shows the descriptive name of this connection.</p> <p>0 and 35 or 0 and 1 are the default VPI and VCI numbers. The last number represents the index number of connections over the same PVC or the VLAN ID number assigned to traffic sent through this connection.</p> <p>(null) means the entry is not valid.</p>
Received	
Bytes	This indicates the number of bytes received on this interface.
Pkts	This indicates the number of transmitted packets on this interface.
Errs	This indicates the number of frames with errors received on this interface.
Drops	This indicates the number of received packets dropped on this interface.
Transmitted	
Bytes	This indicates the number of bytes transmitted on this interface.
Pkts	This indicates the number of transmitted packets on this interface.
Errs	This indicates the number of frames with errors transmitted on this interface.
Drops	This indicates the number of outgoing packets dropped on this interface.
Close	Click this to close the window.
Refresh Interval	Enter the time interval for refreshing statistics in this field.
Set Interval	Click this button to apply the new poll interval you entered in the Refresh Interval field.
Stop	Click Stop to stop refreshing statistics.

4.2.2 Route Info

Routing is based on the destination address only and the CellPipe 7130 RG takes the shortest path to forward a packet. Click **Status > Route Info** to access this screen. Use this screen to view the internal routing table on the CellPipe 7130 RG.

Figure 12 Status > Route Info

Route Info						
Flags: U - up, ! - reject, G - gateway, H - host, R - reinstate, D - dynamic (redirect), M - modified (redirect).						
Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
172.23.26.0	0.0.0.0	255.255.255.0	U	0		br0
<input type="button" value="Close"/>						

The following table describes the labels in this screen.

Table 10 Status > Route Info

LABEL	DESCRIPTION
Destination	This indicates the destination IP address of this route.
Gateway	This indicates the IP address of the gateway that helps forward this route's traffic.
Subnet Mask	This indicates the destination subnet mask of this route.
Flag	<p>This indicates the route status.</p> <p>Up: The route is up.</p> <p>!(Reject): The route is blocked and will force a route lookup to fail.</p> <p>Gateway: The route uses a gateway to forward traffic.</p> <p>Host: The target of the route is a host.</p> <p>Reinstate: The route is reinstated for dynamic routing.</p> <p>Dynamic (redirect): The route is dynamically installed by a routing daemon or redirect</p> <p>Modified (redirect): The route is modified from a routing daemon or redirect.</p>
Metric	The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". The smaller the number, the lower the "cost".
Service	This indicates the name of the service used to forward the route.

Table 10 Status > Route Info (continued)

LABEL	DESCRIPTION
Interface	<p>This indicates the name of the interface through which the route is forwarded.</p> <ul style="list-style-type: none"> • br0 indicates the LAN interface. • ptm0 indicates the VDSL WAN interface using IPoE or in bridge mode. • atmx (where x starts from 0 and is the index number of ATM layer-2 interfaces using different VPI and/or VCI values) indicates the ADSL WAN interface using IPoE or in bridge mode. • pppoa1 indicates the ADSL WAN interface using PPPoA. • ipoa0 indicates the ADSL WAN interface using IPoA. • ppp0 indicates the WAN interface using PPPoE. • eth4 indicates the Ethernet WAN interface using IPoE.
Close	Click this to close the window.

4.2.3 WLAN Station List

Click **Status > WLAN Station List** to access this screen. Use this screen to view the wireless stations that are currently associated to the CellPipe 7130 RG.

Figure 13 Status > WLAN Station List

MAC	SSID	Interface
00:19:CB:41:78:10	CellPipe_5Vz.A2011_AD7048	wl0

Close

Refresh Interval : 5 sec Set Interval Stop

The following table describes the labels in this screen.

Table 11 Status > WLAN Station List

LABEL	DESCRIPTION
MAC	This field shows the MAC (Media Access Control) address of an associated wireless station.
SSID	This field shows the SSID to which the wireless station is connected.
Interface	This field shows the wireless interface to which the wireless station is connected.
Close	Click this to close the window.
Refresh Interval	Enter the time interval for refreshing statistics in this field.
Set Interval	Click this button to apply the new poll interval you entered in the Refresh Interval field.
Stop	Click Stop to stop refreshing statistics.

4.2.4 LAN Statistics

Click **Status > LAN Statistics** to access this screen. Use this screen to view the LAN statistics.

Figure 14 Status > LAN Statistics

LAN Statistics								
Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
LAN1	0	0	0	0	3320134	30267	0	0
LAN2	0	0	0	0	3320070	30266	0	0
LAN3	0	0	0	0	3320006	30265	0	0
LAN4	18269018	76802	0	0	7229573	9634	0	0
HPNA	18000	255	0	0	3337824	30512	0	0
WLAN	444	5	23	0	76882	657	911	0

Close

Refresh Interval : sec

The following table describes the labels in this screen.

Table 12 Status > LAN Statistics

LABEL	DESCRIPTION
Interface	This shows the LAN or WLAN interface.
Received	
Bytes	This indicates the number of bytes received on this interface.
Pkts	This indicates the number of transmitted packets on this interface.
Errs	This indicates the number of frames with errors received on this interface.
Drops	This indicates the number of received packets dropped on this interface.
Transmitted	
Bytes	This indicates the number of bytes transmitted on this interface.
Pkts	This indicates the number of transmitted packets on this interface.
Errs	This indicates the number of frames with errors transmitted on this interface.
Drops	This indicates the number of outgoing packets dropped on this interface.
Close	Click this to close the window.
Refresh Interval	Enter the time interval for refreshing statistics in this field.
Set Interval	Click this button to apply the new poll interval you entered in the Refresh Interval field.
Stop	Click Stop to stop refreshing statistics.

4.2.5 Client List

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the CellPipe 7130 RG as a DHCP server or disable it. When configured as a server, the CellPipe 7130 RG provides the TCP/IP configuration for the clients. If DHCP service is disabled, you must have another DHCP server on your LAN, or else the computer must be manually configured.

Click **Status > Client List** to open the following screen. The read-only DHCP table shows current DHCP client information (including **IP Address**, **Host Name** and **MAC Address**) of all network clients using the CellPipe 7130 RG's DHCP server.

Figure 15 Status > Client List

Hostname	MAC Address	IP Address
tw13032	00:16:17:cd:eb:a3	172.23.26.250
x200	00:1f:16:2f:90:fe	172.23.26.251
ubuntu-Raymond-NB	00:0c:29:f7:22:b4	172.23.26.250
Joseph-nb	00:1d:72:4a:7b:11	172.23.26.251

Close

The following table describes the labels in this screen.

Table 13 Status > Client List

LABEL	DESCRIPTION
Host Name	This indicates the computer host name.
MAC Address	Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. This indicates the MAC address of the client computer.
IP Address	This indicates the IP address assigned to this client computer.

WAN Setup

5.1 Overview

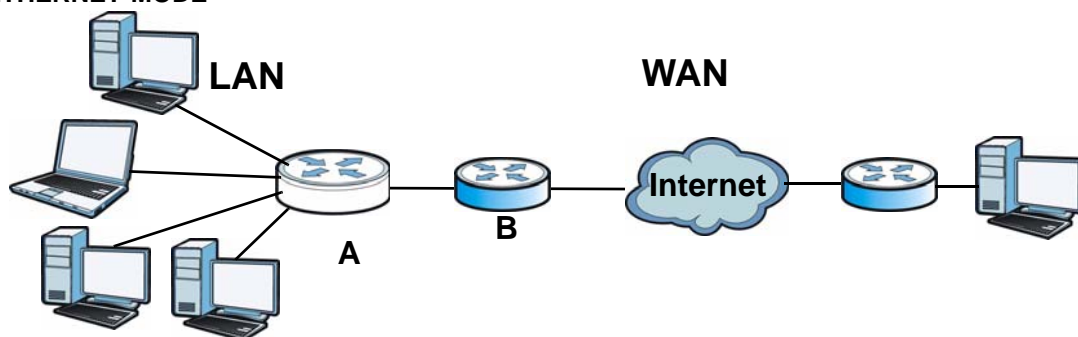
This chapter discusses the CellPipe 7130 RG's **WAN** screens. Use these screens to configure your CellPipe 7130 RG for Internet access.

A WAN (Wide Area Network) connection is an outside connection to another network or the Internet. It connects your private networks, such as a LAN (Local Area Network), and other networks, so that a computer in one location can communicate with computers in other locations.

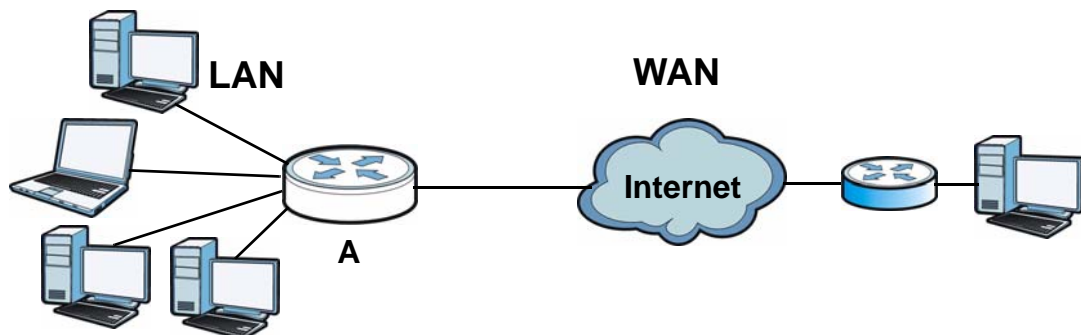
The figure below shows the WAN modes supported by the CellPipe 7130 RG (**A**): Ethernet Mode and DSL mode. Note that in Ethernet mode, **B** is the Internet Access Device (IAD).

Figure 16 LAN and WAN

ETHERNET MODE



DSL MODE



See [Section 5.7 on page 123](#) for advanced technical information on WAN.

5.1.1 What You Can Do in this Chapter

- The **Mode** screen lets you choose between DSL and Ethernet for your Internet connection ([Section 5.4 on page 104](#)).
- The **Connect** screen lets you view, remove or add a layer-2 WAN interface ([Section 5.5 on page 105](#)).
- The **Services** screen lets you view and configure the WAN settings on the CellPipe 7130 RG for Internet access ([Section 5.6 on page 110](#)).

Table 14 WAN Setup Overview

CONNECT			SERVICES	
INTERFACE	DSL LINK TYPE	CONNECTION MODE	WAN SERVICE TYPE	CONNECTION SETTINGS
ATM	EoA	Default Mode VLAN MUX Mode	PPPoE	PPP user name and password, WAN IP address, DNS server and default gateway
			IPoE	WAN IP address, NAT, DNS server and default gateway
			Bridging	N/A
	PPPoA			PPP user name and password, WAN IP address, DNS server and default gateway
	IPoA			WAN IP address, NAT, DNS server and default gateway
PTM		VLAN MUX Mode MSC Mode	PPPoE	PPP user name and password, WAN IP address, DNS server and default gateway
			IPoE	WAN IP address, NAT, DNS server and default gateway
			Bridging	N/A

Table 14 WAN Setup Overview

CONNECT			SERVICES	
INTERFACE	DSL LINK TYPE	CONNECTION MODE	WAN SERVICE TYPE	CONNECTION SETTINGS
Ethernet		Default Mode	PPPoE	PPP user name and password, WAN IP address, DNS server and default gateway
			IPoE	WAN IP address, NAT, DNS server and default gateway
		VLAN MUX Mode	PPPoE	PPP user name and password, WAN IP address, DNS server and default gateway
			IPoE	WAN IP address, NAT, DNS server and default gateway
			Bridging	N/A

5.2 What You Need to Know

Encapsulation Method

Encapsulation is used to include data from an upper layer protocol into a lower layer protocol. To set up a WAN connection to the Internet, you need to use the same encapsulation method used by your ISP (Internet Service Provider). If your ISP offers a dial-up Internet connection using PPPoE (PPP over Ethernet) or PPPoA, they should also provide a username and password (and service name) for user authentication.

WAN IP Address

The WAN IP address is an IP address for the CellPipe 7130 RG, which makes it accessible from an outside network. It is used by the CellPipe 7130 RG to communicate with other devices in other networks. It can be static (fixed) or dynamically assigned by the ISP each time the CellPipe 7130 RG tries to access the Internet.

If your ISP assigns you a static WAN IP address, they should also assign you the subnet mask and DNS server IP address(es) (and a gateway IP address if you use the Ethernet or ENET ENCAP encapsulation method).

ATM

Asynchronous Transfer Mode (ATM) is a LAN and WAN networking technology that provides high-speed data transfer. ATM uses fixed-size packets of information called cells. With ATM, a high QoS (Quality of Service) can be guaranteed. ATM uses a connection-oriented model and establishes a virtual circuit (VC) between two endpoints before the actual data exchange begins.

PTM

Packet Transfer Mode (PTM) is packet-oriented and supported by the VDSL2 standard. In PTM, packets are encapsulated directly in the High-level Data Link Control (HDLC) frames. It is designed to provide a low-overhead, transparent way of transporting packets over DSL links, as an alternative to ATM.

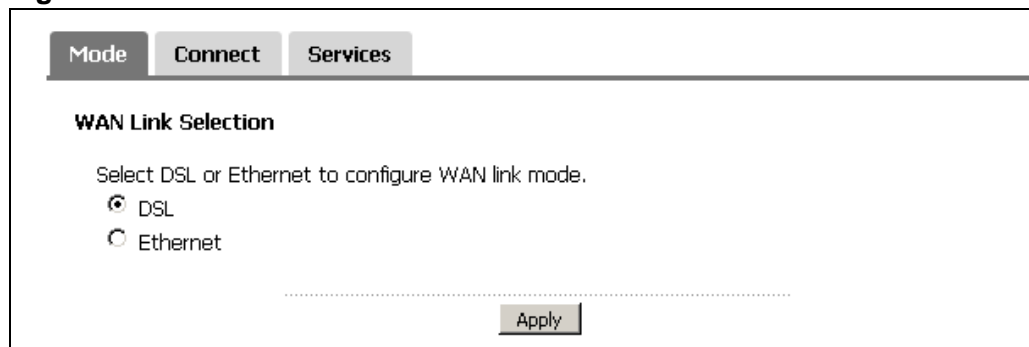
5.3 Before You Begin

You need to know your Internet access settings such as encapsulation and WAN IP address. Get this information from your ISP.

5.4 The Mode Screen

The CellPipe 7130 RG can work in DSL or Ethernet mode depending on your Internet account subscription. Note that you can only enable one mode at a time.

Figure 17 Network > WAN > Mode



Mode Connect Services

WAN Link Selection

Select DSL or Ethernet to configure WAN link mode.

DSL

Ethernet

Apply

The following table describes the fields in this screen.

Table 15 Network > WAN > Mode

LABEL	DESCRIPTION
WAN Link Selection	Select how you want to connect to the Internet: DSL: Select this if you have a DSL account and you want to connect to the Internet using the DSL port. Ethernet: Select this if you have a broadband modem or router to access the Internet. Connect the GigE port to your broadband modem or router.
Apply	Click this button to save your changes.

5.5 The Connect Screen

The CellPipe 7130 RG must have a layer-2 interface to allow users to use the DSL port or Ethernet WAN port to access the Internet. The **Connect** screen lets you choose the layer-2 interface that the CellPipe 7130 RG uses. The layer-2 interface determines how data is transported, whether in frames (Ethernet) or cells (DSL), from the source (such as a computer on your LAN) to the destination. The screen varies depending on the interface type you select.

Note: The ATM, PTM and Ethernet layer-2 interfaces cannot work at the same time.

Figure 18 Network > WAN > Connect: PTM or Ethernet

Mode **Connect** Services

Interface: PTM

DSL PTM Interface Configuration

Choose Add, or Remove to configure DSL PTM interfaces.

Active	Interface	Connection Mode	QoS	Remove
<input checked="" type="checkbox"/>	ptm0	MultipleServiceMode	Enabled	

.....

Add Apply

Figure 19 Network > WAN > Connect: ATM

Mode **Connect** Services

Interface: ATM

DSL ATM Interface Configuration

Choose Add, or Remove to configure DSL ATM interfaces.

Active	Interface	Vpi	Vci	Category	Link Type	Connection Mode	QoS	Remove
<input checked="" type="checkbox"/>	atm0	0	33	UBR	EoA	DefaultMode	Enabled	

.....

Add Apply

The following table describes the fields in this screen.

Table 16 Network > WAN > Connect

LABEL	DESCRIPTION
Active	<p>Check this to enable the current Connect (or layer-2) interface. Note that checking this automatically:</p> <ul style="list-style-type: none"> • Disables the other Connect interfaces • Configures the WAN > Mode screen <p>If you check Active in the WAN > Connect: DSL ATM Interface Configuration screen, the CellPipe 7130 RG uses DSL ATM to connect to the Internet. It also selects DSL in the WAN > Mode screen.</p> <p>If you check Active in the WAN > Connect: ETH WAN Interface Configuration screen. The CellPipe 7130 RG disables the previous DSL ATM connection and starts connecting to the Internet through Ethernet. It also selects Ethernet in the WAN > Mode screen.</p>
Interface	<p>Select an interface for which you want to configure here.</p> <p>PTM: The CellPipe 7130 RG uses the VDSL technology for data transmission over the DSL port.</p> <p>ATM: The CellPipe 7130 RG uses the ADSL technology for data transmission over the DSL port.</p> <p>Ethernet: The CellPipe 7130 RG transmits data over the Ethernet WAN port. Select this if you have a DSL router or modem in your network already.</p>
Interface	This is the name of the interface.
Vpi	This is the Virtual Path Identifier (VPI).
Vci	This is the Virtual Channel Identifier (VCI).
Category	This is the ATM traffic class.
Link Type	This is the DSL link type of the ATM Connect interface.
Connection Mode	This displays the connection mode of the connect interface.
QoS	This displays whether QoS (Quality of Service) is enabled on the CellPipe 7130 RG.
Remove	<p>Click the Remove button to delete this interface from the CellPipe 7130 RG. A window displays asking you to confirm that you want to delete the interface.</p> <p>Note: You cannot remove the Connect interface when a WAN service is associated with it.</p>
Add	Click this button to create a new Connect interface.

5.5.1 Connect Configuration

Click the **Add** button in the **Connect** screen to open the following. Use this screen to create a new Connect (or layer-2) interface. At the time of writing, you can configure only one PTM or Ethernet Connect interface on the CellPipe 7130 RG.

You can configure and use multiple ATM Connect interfaces using different VPI and/or VCI values. The screen varies depending on the interface type you select.

Figure 20 Network > WAN > Connect: Add/Edit DSL ATM

DSL ATM Interface Configuration

ATM PVC Configuration
This screen allows you to configure an ATM PVC identifier (VPI and VCI), select DSL latency, select a service category. Otherwise choose an existing interface by selecting the checkbox to enable it.

VPI: [0-255]

VCI: [32-65535]

Select DSL Link Type (EoA is for PPPoE, IPoE, and Bridge.)

EoA
 PPPoA
 IPoA

Encapsulation Mode:

Service Category:

Peak Cell Rate: [cells/s]

Sustainable Cell Rate: [cells/s]

Maximum Burst Size: [cells]

Select Connection Mode

Default Mode - Single service over one connection
 VLAN MUX Mode - Multiple Vlan service over one connection

Enable Quality Of Service

Enabling packet level QoS for a PVC improves performance for selected classes of applications. QoS cannot be set for CBR and Realtime VBR. QoS consumes system resources; therefore the number of PVCs will be reduced. Use **Advanced Setup/Quality of Service** to assign priorities for the applications.

Enable Quality Of Service.

.....

Figure 21 Network > WAN > Connect: Add/Edit: DSL PTM/Ethernet WAN

DSL PTM Interface Configuration

Select Connection Mode

VLAN MUX Mode - Multiple Vlan service over one connection
 MSC Mode - Multiple Service over one Connection

Enable Quality Of Service

Enabling packet level QoS for this PTM interface. Use **Advanced Setup/Quality of Service** to assign priorities for the applications.

Enable Quality Of Service.

.....

The following table describes the fields in this screen.

Table 17 Network > WAN > Connect: Add/Edit

LABEL	DESCRIPTION
ATM PVC Configuration	VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) define a virtual circuit. This section is available only when you configure an ATM Connect interface.
VPI	The valid range for the VPI is 0 to 255. Enter the VPI assigned to you.

Table 17 Network > WAN > Connect: Add/Edit (continued)

LABEL	DESCRIPTION
VCI	The valid range for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Enter the VCI assigned to you.
Select DSL Link Type	<p>Select EoA (Ethernet over ATM) to have an Ethernet header in the packet, so that you can have multiple services/connections over one PVC. You can set each connection to have its own MAC address or all connections share one MAC address but use different VLAN IDs for different services. EoA supports ENET ENCAP (IPoE), PPPoE and RFC1483/2684 bridging encapsulation methods.</p> <p>Select PPPoA (PPP over ATM) to allow just one PPPoA connection over a PVC.</p> <p>Select IPoA (IP over ATM) to allow just one RFC 1483 routing connection over a PVC.</p>
Encapsulation Mode	<p>Select the method of multiplexing used by your ISP from the drop-down list. Choices are:</p> <ul style="list-style-type: none"> • VC/MUX: In VC multiplexing, each protocol is carried on a single ATM virtual circuit (VC). To transport multiple protocols, the CellPipe 7130 RG needs separate VCs. There is a binding between a VC and the type of the network protocol carried on the VC. This reduces payload overhead since there is no need to carry protocol information in each Protocol Data Unit (PDU) payload. • LLC/ENCAPSULATION: More than one protocol can be carried over the same VC. This is available only when you select PPPoA in the Select DSL Link Type field. • LLC/SNAP-ROUTING: In LCC encapsulation, an IEEE 802.2 Logical Link Control (LLC) header is prefixed to each routed PDU to identify the PDUs. The LLC header can be followed by an IEEE 802.1a SubNetwork Attachment Point (SNAP) header. This is available only when you select IPoA in the Select DSL Link Type field. • LLC/SNAP-BRIDGING: In LCC encapsulation, bridged PDUs are encapsulated by identifying the type of the bridged media in the SNAP header. This is available only when you select EoA in the Select DSL Link Type field.
Service Category	<p>Select UBR Without PCR or UBR With PCR for applications that are non-time sensitive, such as e-mail.</p> <p>Select CBR (Continuous Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic.</p> <p>Select Realtime VBR (real-time Variable Bit Rate) for applications with bursty connections that require closely controlled delay and delay variation.</p> <p>Select Non Realtime VBR (non real-time Variable Bit Rate) for connections that do not require closely controlled delay and delay variation.</p>
Peak Cell Rate	<p>Divide the DSL line rate (bps) by 424 (the size of an ATM cell) to find the Peak Cell Rate (PCR). This is the maximum rate at which the sender can send cells. Type the PCR here.</p> <p>This field is not available when you select UBR Without PCR.</p>

Table 17 Network > WAN > Connect: Add/Edit (continued)

LABEL	DESCRIPTION
Sustainable Cell Rate	<p>The Sustain Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted. Type the SCR, which must be less than the PCR. Note that system default is 0 cells/sec.</p> <p>This field is available only when you select Non Realtime VBR or Realtime VBR.</p>
Maximum Burst Size	<p>Maximum Burst Size (MBS) refers to the maximum number of cells that can be sent at the peak rate. Type the MBS, which is less than 65535.</p> <p>This field is available only when you select Non Realtime VBR or Realtime VBR.</p>
Select Connection Mode	<p>Select Default Mode to allow only one WAN service over a single virtual circuit.</p> <p>Select MSC Mode to allow multiple WAN services over a single virtual circuit. Each WAN connection has its own MAC address.</p> <p>Select VLAN MUX Mode to allow multiplexing of multiple protocols over a single virtual circuit. You need to assign a VLAN ID and priority level to traffic through each WAN connection. All WAN connections share one MAC address.</p> <p>This field is not available if you select PPPoA or IPoA as the DSL link type. The CellPipe 7130 RG uses Default Mode automatically for PPPoA or IPoA.</p>
Enable Quality Of Service	<p>Select this option to activate QoS (Quality of Service) on this interface to group and prioritize traffic. Traffic is grouped according to the VLAN group.</p> <p>The QoS setting applies to all WAN connections over the same PVC.</p> <p>This field is not available when you select CBR or Realtime VBR.</p>
Back	Click this button to return to the previous screen without saving any changes.
Apply/Save	Click this button to save your changes and go back to the previous screen.

5.6 The Services Screen

Use this screen to view and/or create WAN services over a layer-2 interface. Click **Network > WAN > Internet Connection**. The summary table shows you the configured WAN services (connections) on the CellPipe 7130 RG.

To use NAT, firewall or IGMP proxy in the CellPipe 7130 RG, you need to configure a WAN connection with PPPoE or IPoE.

Note: When a **Connect** interface is in **VLAN MUX Mode** or **MSC Mode**, you can configure up to eight WAN services shared by both interfaces.

Figure 22 Network > WAN > Services

Mode	Connect	Services																																												
<p>Wide Area Network (WAN) Service Setup</p> <p>Choose Add, or Remove to configure a WAN service over a selected interface.</p> <table border="1"> <thead> <tr> <th>Interface</th> <th>Description</th> <th>Type</th> <th>Rate</th> <th>Vlan8021p</th> <th>VlanMuxId</th> <th>ConnId</th> <th>IGMP</th> <th>NAT</th> <th>Firewall</th> <th>Modify</th> </tr> </thead> <tbody> <tr> <td>atm0</td> <td>ipoe_0_0_33</td> <td>ATM/IPoE</td> <td>N/A</td> <td>N/A</td> <td>N/A</td> <td>N/A</td> <td>Disabled</td> <td>Enabled</td> <td>Enabled</td> <td> </td> </tr> <tr> <td>ptm0_1</td> <td>ipoe_0_0_1_1</td> <td>PTM/IPoE</td> <td>N/A</td> <td>N/A</td> <td>N/A</td> <td>1</td> <td>Disabled</td> <td>Enabled</td> <td>Enabled</td> <td> </td> </tr> <tr> <td>eth4_1</td> <td>ipoe_eth4_1</td> <td>ETH/IPoW</td> <td>N/A</td> <td>N/A</td> <td>N/A</td> <td>1</td> <td>Disabled</td> <td>Enabled</td> <td>Enabled</td> <td> </td> </tr> </tbody> </table> <p style="text-align: center;">.....</p> <p style="text-align: center;"><input type="button" value="Add"/></p>			Interface	Description	Type	Rate	Vlan8021p	VlanMuxId	ConnId	IGMP	NAT	Firewall	Modify	atm0	ipoe_0_0_33	ATM/IPoE	N/A	N/A	N/A	N/A	Disabled	Enabled	Enabled		ptm0_1	ipoe_0_0_1_1	PTM/IPoE	N/A	N/A	N/A	1	Disabled	Enabled	Enabled		eth4_1	ipoe_eth4_1	ETH/IPoW	N/A	N/A	N/A	1	Disabled	Enabled	Enabled	
Interface	Description	Type	Rate	Vlan8021p	VlanMuxId	ConnId	IGMP	NAT	Firewall	Modify																																				
atm0	ipoe_0_0_33	ATM/IPoE	N/A	N/A	N/A	N/A	Disabled	Enabled	Enabled																																					
ptm0_1	ipoe_0_0_1_1	PTM/IPoE	N/A	N/A	N/A	1	Disabled	Enabled	Enabled																																					
eth4_1	ipoe_eth4_1	ETH/IPoW	N/A	N/A	N/A	1	Disabled	Enabled	Enabled																																					

The following table describes the labels in this screen.

Table 18 Network > WAN > Services

LABEL	DESCRIPTION
Interface	<p>This shows the name of the interface used by this connection.</p> <p>A default name atmx or ptm0_x (where x starts from 0 and is the index number of ATM layer-2 interface) indicates the DSL port.</p> <p>The ppp0_x name (where x starts from 1 and is the index number of PPP connection on the CellPipe 7130 RG) indicates a PPP connection via any one of the WAN interface.</p> <p>The eth4_x (where x starts from 1 and is the index number of ethernet connection on the CellPipe 7130 RG) indicates the Ethernet WAN interface (the physical Ethernet WAN port).</p> <p>The number after the underscore (_) represents either the index number of connections through the same interface or the VPI/VCI values assigned to the ATM layer-2 interface.</p> <p>The number after the dot (.) represents the VLAN ID number assigned to traffic sent through this connection.</p> <p>(null) means the entry is not valid.</p>
Description	<p>This is the service name of this connection.</p> <p>The first number represents the index number of connections over the same PVC or the VLAN ID number assigned to traffic sent through this connection. The next two numbers are the VPI and VCI numbers. 0 and 33 are the default VPI and VCI numbers.</p> <p>(null) means the entry is not valid.</p>
Type	<p>This shows the layer-2 interface type and method of encapsulation used by this connection.</p> <p>IPoW stands for IPoE used in an Ethernet WAN connection.</p>

Table 18 Network > WAN > Services

LABEL	DESCRIPTION
Rate	This shows the maximum data rate (in Kbps) allowed for traffic sent through this connection. This displays N/A when there is no limit on transmission rate.
Vlan8021p	This indicates the 802.1P priority level assigned to traffic sent through this connection. This displays N/A when there is no priority level assigned.
VlanMuxId	This indicates the VLAN ID number assigned to traffic sent through this connection. This displays N/A when there is no VLAN ID number assigned.
ConnId	This shows the index number of each connection. This displays N/A when the interface used by the connection is in Default Mode .
IGMP	This shows whether IGMP (Internet Group Multicast Protocol) is activated or not for this connection. IGMP is not available when the connection uses the bridging service.
NAT	This shows whether NAT is activated or not for this interface. NAT is not available when the connection uses the bridging service.
Firewall	This shows whether the firewall is activated or not for this connection. The firewall is not available when the connection uses the bridging service.
Modify	Click the Edit icon to configure the WAN connection. Click the Remove icon to delete the WAN connection.
Add	Click Add to create a new connection.

5.6.1 WAN Connection Configuration

Click the **Edit** or **Add** button in the **WAN Service** screen to configure a WAN connection.

5.6.1.1 WAN Interface

This screen displays when you add a new WAN connection.

Figure 23 Network > WAN > Services: Add/Edit

WAN Service Interface Configuration

Select a layer 2 interface for this service

ptm0/(0_0_1)

Back Next

The following table describes the labels in this screen.

Table 19 Network > WAN > Services: Add/Edit

LABEL	DESCRIPTION
Select a layer 2 interface for this service	Select ptm0 to use the DSL port as the WAN port and use the VDSL technology for data transmission. Select atmx (where x starts from 0 and is the index number of ATM layer-2 interfaces using different VPI and/or VCI values) to use the DSL port as the WAN port and use the ADSL technology for data transmission. Select eth4 if you want to use the Ethernet WAN port as the WAN port.
Back	Click this button to return to the previous screen.
Next	Click this button to continue.

5.6.1.2 Service Type

If you set the DSL link type to **PPPoA** or **IPoA** for the ATM interface and configure a WAN connection using the ATM interface, you only need to configure the **Enter Service Description** field in this screen.

Figure 24 Network > WAN > Services > Add/Edit: Service Type

WAN Service Configuration

Select WAN service type:

- PPP over Ethernet (PPPoE)
- IP over Ethernet
- Bridging

Enter Service Description:

Tag VLAN ID for egress packets

Enter 802.1P Priority [0-7]:

Enter 802.1Q VLAN ID [1-4094]:

.....

Figure 25 Network > WAN > Services > Add/Edit: Service Type - PPPoA or IPoA

WAN Service Configuration

Enter Service Description:

.....

The following table describes the labels in this screen.

Table 20 Network > WAN > Services > Add/Edit

LABEL	DESCRIPTION
Select WAN service type	Select the method of encapsulation used by your ISP. Choices are PPP over Ethernet (PPPoE) , IP over Ethernet and Bridging .
Enter Service Description	Specify a name for this connection or use the automatically generated one.
Rate Limit	Enter the maximum transmission rate in Kbps for traffic sent through the WAN connection. Otherwise, leave this field blank to disable the rate limit. This field is not available for an ATM connection. For the PTM connection, the Connection Mode in the Connect > Add: PTM screen should be MSC Mode with QoS enabled.
Tag VLAN ID for egress packets	Select this option to add the VLAN tag (specified below) to the outgoing traffic through this connection. This field is available when the Connect interface is in VLAN MUX mode.
Enter 802.1P Priority	IEEE 802.1p defines up to 8 separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service. Type the IEEE 802.1p priority level (from 0 to 7) to add to traffic through this connection. The greater the number, the higher the priority level. This field is available when the Connect interface is in VLAN MUX mode.
Enter 802.1Q VLAN ID	Type the VLAN ID number (from 1 to 4094) for traffic through this connection. This field is available when the PTM interface is in VLAN MUX mode.
Back	Click this button to return to the previous screen.
Next	Click this button to continue.

5.6.1.3 WAN IP Address and DNS Server

The screen differs by the encapsulation you selected in the previous screen. See [Section 5.7 on page 123](#) for more information.

PPPoE or PPPoA

This screen displays when you select **PPP over Ethernet (PPPoE)** in the **WAN Service Configuration** screen or set the DSL link type to **PPPoA** for the ATM interface and configure a WAN connection using the ATM interface.

Figure 26 Network > WAN > Services > Add/Edit Service Type 2: PPPoE or PPPoA

PPP Username and Password

PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.

PPP Username:

PPP Password:

PPPoE Service Name:

Authentication Method:

Enable Fullcone NAT

Dial on demand (with idle timeout timer)

Inactivity Timeout (minutes) [1-4320]:

Use Static IPv4 Address

IPv4 Address:

Enable PPP Debug Mode

Bridge PPPoE Frames Between WAN and Local Ports

Multicast Proxy

Enable IGMP Multicast Proxy

.....

The following table describes the labels in this screen.

Table 21 Network > WAN > Services > Add/Edit Service Type 2: PPPoE or PPPoA

LABEL	DESCRIPTION
PPP User Name	Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
PPP Password	Enter the password associated with the user name above.
PPPoE Service Name	Type the name of your PPPoE service here. This field is not available for a PPPoA connection.

Table 21 Network > WAN > Services > Add/Edit Service Type 2: PPPoE or PPPoA

LABEL	DESCRIPTION
Authentication Method	<p>The CellPipe 7130 RG supports PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol). CHAP is more secure than PAP; however, PAP is readily available on more platforms.</p> <p>Use the drop-down list box to select an authentication protocol for outgoing calls. Options are:</p> <p>AUTO - Your CellPipe 7130 RG accepts either CHAP or PAP when requested by this remote node.</p> <p>CHAP - Your CellPipe 7130 RG accepts CHAP only.</p> <p>PAP - Your CellPipe 7130 RG accepts PAP only.</p> <p>MSCHAP - Your CellPipe 7130 RG accepts MSCHAP only. MS-CHAP is the Microsoft version of the CHAP.</p>
Enable Fullcone NAT	Select this option to enable full cone NAT on the CellPipe 7130 RG.
Dial on Demand	Select this check box when you do not want the connection up all the time and specify an idle time-out in the Inactivity Timeout field.
Inactivity Timeout	Specify an idle time-out when you select Dial on Demand . The default setting is 0, which means the Internet session will not timeout.
Use Static IPv4 Address	A static IPv4 address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. Select this if you do not have a dynamic IP address.
IPv4 Address	Enter the static IP address provided by your ISP.
Enable PPP Debug Mode	Select this option to display PPP debugging messages on the console.
Bridge PPPoE Frames Between WAN and Local Ports	<p>Select this option to forward PPPoE packets from the WAN port to the LAN ports and from the LAN ports to the WAN port.</p> <p>In addition to the CellPipe 7130 RG's built-in PPPoE client, you can select this to allow up to ten hosts on the LAN to use PPPoE client software on their computers to connect to the ISP via the CellPipe 7130 RG. Each host can have a separate account and a public WAN IP address.</p> <p>This is an alternative to NAT for application where NAT is not appropriate.</p> <p>Clear this if you do not need to allow hosts on the LAN to use PPPoE client software on their computers to connect to the ISP.</p> <p>This field is not available for a PPPoA connection.</p>
Enable IGMP Multicast Proxy	Select this check box to have the CellPipe 7130 RG act as an IGMP proxy on this connection. This allows the CellPipe 7130 RG to get subscribing information and maintain a joined member list for each multicast group. It can reduce multicast traffic significantly.
Back	Click this button to return to the previous screen.
Next	Click this button to continue.

IPoE

This screen displays when you select **IP over Ethernet** in the **WAN Service Configuration** screen.

Figure 27 Network > WAN > Services > Add/Edit Service Type 2: IPoE

WAN IP Settings

Enter information provided to you by your ISP to configure the WAN IP settings.
 Notice: If "Obtain an IP address automatically" is chosen, DHCP client will be enabled.
 If "Use the following Static IP address" is chosen, enter the WAN IP address, subnet mask and interface gateway.

Obtain an IP address automatically

Enable DHCP Option 60
 Vendor class Identifier:

Enable DHCP Option 61
 IAID:
 DUID type:
 Identifier:

Enable DHCP Option 125
 Manufacturer OUI:
 Product class:
 Model name:
 Serial number:

Use the following Static IP address:
 WAN IP Address:
 WAN Subnet Mask:
 WAN gateway IP Address:

.....

The following table describes the labels in this screen.

Table 22 Network > WAN > Services > Add/Edit Service Type 2: IPoE

LABEL	DESCRIPTION
Obtain an IP address automatically	A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. Select this if you have a dynamic IP address.
Enable DHCP Option 60	Select this to identify the vendor and functionality of the CellPipe 7130 RG in DHCP requests that the CellPipe 7130 RG sends to a DHCP server when getting a WAN IP address.
Vendor Class Identifier	Enter the Vendor Class Identifier (Option 60), such as the type of the hardware or firmware.
Enable DHCP Option 61	Select this to identify the CellPipe 7130 RG in DHCP requests that the CellPipe 7130 RG sends to a DHCP server when getting a WAN IP address.
IAID	Enter the Identity Association Identifier (IAID) of the CellPipe 7130 RG. For example, the WAN connection index number.

Table 22 Network > WAN > Services > Add/Edit Service Type 2: IPoE

LABEL	DESCRIPTION
DUID Type	Select Other to enter any string that identifies the CellPipe 7130 RG in the DUID field. Select DUID-LL (DUID Based on Link-layer Address) to enter the CellPipe 7130 RG's hardware address, that is the MAC address in the DUID field. Select DUID-EN (DUID Assigned by Vendor Based on Enterprise Number) to enter the vendor's registered private enterprise number.
DUID	Enter the DHCP Unique Identifier (DUID) of the CellPipe 7130 RG.
Identifier	Enter a unique identifier assigned by the vendor. This field is available when you select DUID-EN in the DUID Type field.
Enable DHCP Option 125	Select this to add vendor specific information to DHCP requests that the CellPipe 7130 RG sends to a DHCP server when getting a WAN IP address.
Manufacturer OUI	Specify the vendor's OUI (Organization Unique Identifier). It is usually the first three bytes of the MAC address.
Product Class	Enter the product class of the CellPipe 7130 RG.
Model Name	Enter the model name of the CellPipe 7130 RG.
Serial Number	Enter the serial number of the CellPipe 7130 RG.
Use the following Static IP address	Select this if you have a static IP address.
WAN IP Address	Enter the static IP address provided by your ISP.
WAN Subnet Mask	Enter the subnet mask provided by your ISP.
WAN gateway IP Address	Enter the gateway IP address provided by your ISP.
Back	Click this button to return to the previous screen.
Next	Click this button to continue.

IPoA

This screen displays only when you set the DSL link type to **IPoA** for the ATM interface and configure a WAN connection using the ATM interface.

Figure 28 Network > WAN > Services > Add/Edit Service Type 2: IPoA

DSL PTM Interface Configuration

WAN IP Settings

Enter information provided to you by your ISP to configure the WAN IP settings.

WAN IP Address:

WAN Subnet Mask:

The following table describes the labels in this screen.

Table 23 Network > WAN > Services > Add/Edit Service Type 2: IPoA

LABEL	DESCRIPTION
WAN IP Address	Enter the static IP address provided by your ISP.
WAN Subnet Mask	Enter the subnet mask provided by your ISP.
Back	Click this button to return to the previous screen.
Next	Click this button to continue.

5.6.1.4 NAT, IGMP Multicast and Firewall Activation

The screen is available only when you select **IP over Ethernet** in the **WAN Service Configuration** screen or set the DSL link type to **IPoA** for the ATM interface and configure a WAN connection using the ATM interface.

Figure 29 Network > WAN > Services > Add/Edit - NAT and IGMP: IPoE/IPoA

Network Address Translation Settings

Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN).

Enable NAT

Enable Fullcone NAT

Enable Firewall

IGMP Multicast

Enable IGMP Multicast Proxy

.....

Back Next

The following table describes the labels in this screen.

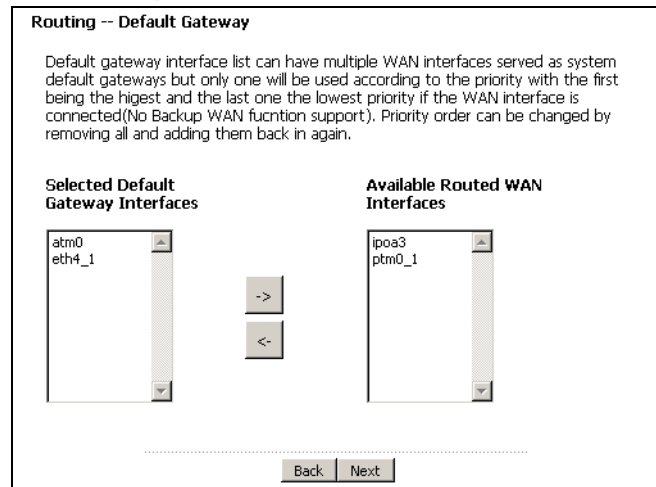
Table 24 Network > WAN > Services > Add/Edit - NAT and IGMP: IPoE/IPoA

LABEL	DESCRIPTION
Enable NAT	Select this check box to activate NAT on this connection.
Enable Fullcone NAT	Select this check box to activate full cone NAT on this connection. This field is available only when you select Enable NAT .
Enable Firewall	Select this check box to activate Firewall on this connection.
Enable IGMP Multicast Proxy	Select this check box to have the CellPipe 7130 RG act as an IGMP proxy on this connection. This allows the CellPipe 7130 RG to get subscribing information and maintain a joined member list for each multicast group. It can reduce multicast traffic significantly.
Back	Click this button to return to the previous screen.
Next	Click this button to continue.

5.6.1.5 Default Gateway

The screen is not available when you select **Bridging** in the **WAN Service Configuration** screen.

Figure 30 Network > WAN > Services > Add/Edit - Default Gateway: PPPoE, PPPoA, IPoE or IPoA



The following table describes the labels in this screen.

Table 25 Network > WAN > Services > Add/Edit - Default Gateway: PPPoE, PPPoA, IPoE or IPoA

LABEL	DESCRIPTION
Selected Default Gateway Interfaces	Select a WAN interface through which you want to forward the traffic.
Available Routed WAN Interfaces	Select a WAN interface in the Available Routed WAN Interfaces and use the left-facing arrow to move it to the Selected Default Gateway Interfaces to use that interface as the default gateway. To remove a WAN interface from the Selected Default Gateway Interfaces , use the right-facing arrow. The interface on the top of the list gets the highest priority.
Back	Click this button to return to the previous screen.
Next	Click this button to continue.

5.6.1.6 DNS Server

The screen is not available when you select **Bridging** in the **WAN Service Configuration** screen.

Note: If you configure only one PVC with IPoA or static IPoE connection using the ATM interface on the CellPipe 7130 RG, you must enter the static DNS server address.

Figure 31 Network > WAN > Services > Add/Edit - DNS Server: PPPoE, PPPoA, IPoE or IPoA

Default DNS Server Configuration

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.

DNS Server Interfaces can have multiple WAN interfaces served as system dns servers 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 WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

Select DNS Server Interface from available WAN interfaces:

Selected DNS Server Interfaces

atm0
eth4_1

->

<-

Available WAN Interfaces

ptm0_1

Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

.....

The following table describes the labels in this screen.

Table 26 Network > WAN > Services > Add/Edit - DNS Server: PPPoE, PPPoA, IPoE or IPoA

LABEL	DESCRIPTION
Select DNS Server Interface from available WAN interfaces	Select this to have the CellPipe 7130 RG get the DNS server addresses from the ISP automatically.
Selected DNS Server Interfaces	Select a WAN interface through which you want to obtain the DNS related information.
Available WAN Interfaces	<p>Select a WAN interface in the Available WAN Interfaces and use the left-facing arrow to move it to the Selected DNS Server Interfaces to use that interface as the DNS server.</p> <p>To remove a WAN interface from the Selected DNS Server Interfaces, use the right-facing arrow.</p> <p>The interface on the top of the list gets the highest priority.</p>
Use the following Static DNS IP address	Select this to have the CellPipe 7130 RG use the DNS server addresses you configure manually.
Primary DNS server	Enter the first DNS server address assigned by the ISP.

Table 26 Network > WAN > Services > Add/Edit - DNS Server: PPPoE, PPPoA, IPoE or IPoA

LABEL	DESCRIPTION
Secondary DNS server	Enter the second DNS server address assigned by the ISP.
Back	Click this button to return to the previous screen.
Next	Click this button to continue.

5.6.1.7 Configuration Summary

This read-only screen shows the current WAN connection settings.

Figure 32 Network > WAN > Services > Add/Edit - Configuration Summary

WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

PORT / VPI / VCI:	0 / 0 / 37
Connection Type:	IPoA
Service Name:	ipoa_0_0_37
Service Category:	UBR
IP Address:	1.2.3.4
Service State:	Enabled
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Disabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

.....

The following table describes the labels in this screen.

Table 27 Network > WAN > Services > Add/Edit - Configuration Summary

LABEL	DESCRIPTION
Port / VPI / VCI	This is the DSL port number, VPI and VCI for an ATM connection. This displays N/A for an Ethernet WAN connection or not available for a PTM connection.
Connection Type	This is the encapsulation method used by this connection.
Service Name	This is the name of the service.
Service Category	This is the ATM traffic class. This field is blank for a PTM or Ethernet WAN connection.
IP Address	This shows whether the WAN IP address is assigned by the ISP, manually configured or not configurable.
Service State	This shows whether this service is active or not.

Table 27 Network > WAN > Services > Add/Edit - Configuration Summary

LABEL	DESCRIPTION
NAT	This shows whether NAT is active or not for this connection.
Full Cone NAT	This shows whether full cone NAT is active or not for this connection.
Firewall	This shows whether Firewall is active or not for this connection.
IGMP Multicast	This shows whether IGMP multicasting is active or not for this connection.
Quality Of Service	This shows whether QoS is active or not for this connection.
Back	Click this button to return to the previous screen.
Apply/Save	Click this button to save your changes.

5.7 Technical Reference

The following section contains additional technical information about the CellPipe 7130 RG features described in this chapter.

Encapsulation

Be sure to use the encapsulation method required by your ISP. The CellPipe 7130 RG can work in bridge mode or routing mode. When the CellPipe 7130 RG is in routing mode, it supports the following methods.

IP over Ethernet

IP over Ethernet (IPoE) is an alternative to PPPoE. IP packets are being delivered across an Ethernet network, without using PPP encapsulation. They are routed between the Ethernet interface and the WAN interface and then formatted so that they can be understood in a bridged environment. For instance, it encapsulates routed Ethernet frames into bridged Ethernet cells.

PPP over Ethernet

Point-to-Point Protocol over Ethernet (PPPoE) provides access control and billing functionality in a manner similar to dial-up services using PPP. PPPoE is an IETF standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (DSL, cable, wireless, etc.) connection.

For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for example RADIUS).

One of the benefits of PPPoE is the ability to let you access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for individuals.

Operationally, PPPoE saves significant effort for both you and the ISP or carrier, as it requires no specific configuration of the broadband modem at the customer site.

By implementing PPPoE directly on the CellPipe 7130 RG (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the CellPipe 7130 RG does that part of the task. Furthermore, with NAT, all of the LANs' computers will have access.

PPPoA

PPPoA stands for Point to Point Protocol over ATM Adaptation Layer 5 (AAL5). A PPPoA connection functions like a dial-up Internet connection. The CellPipe 7130 RG encapsulates the PPP session based on RFC1483 and sends it through an ATM PVC (Permanent Virtual Circuit) to the Internet Service Provider's (ISP) DSLAM (digital access multiplexer). Please refer to RFC 2364 for more information on PPPoA. Refer to RFC 1661 for more information on PPP.

RFC 1483

RFC 1483 describes two methods for Multiprotocol Encapsulation over ATM Adaptation Layer 5 (AAL5). The first method allows multiplexing of multiple protocols over a single ATM virtual circuit (LLC-based multiplexing) and the second method assumes that each protocol is carried over a separate ATM virtual circuit (VC-based multiplexing). Please refer to RFC 1483 for more detailed information.

Multiplexing

There are two conventions to identify what protocols the virtual circuit (VC) is carrying. Be sure to use the multiplexing method required by your ISP.

VC-based Multiplexing

In this case, by prior mutual agreement, each protocol is assigned to a specific virtual circuit; for example, VC1 carries IP, etc. VC-based multiplexing may be dominant in environments where dynamic creation of large numbers of ATM VCs is fast and economical.

LLC-based Multiplexing

In this case one VC carries multiple protocols with protocol identifying information being contained in each packet header. Despite the extra bandwidth and processing overhead, this method may be advantageous if it is not practical to

have a separate VC for each carried protocol, for example, if charging heavily depends on the number of simultaneous VCs.

Traffic Shaping

Traffic Shaping is an agreement between the carrier and the subscriber to regulate the average rate and fluctuations of data transmission over an ATM network. This agreement helps eliminate congestion, which is important for transmission of real time data such as audio and video connections.

Peak Cell Rate (PCR) is the maximum rate at which the sender can send cells. This parameter may be lower (but not higher) than the maximum line speed. 1 ATM cell is 53 bytes (424 bits), so a maximum speed of 832Kbps gives a maximum PCR of 1962 cells/sec. This rate is not guaranteed because it is dependent on the line speed.

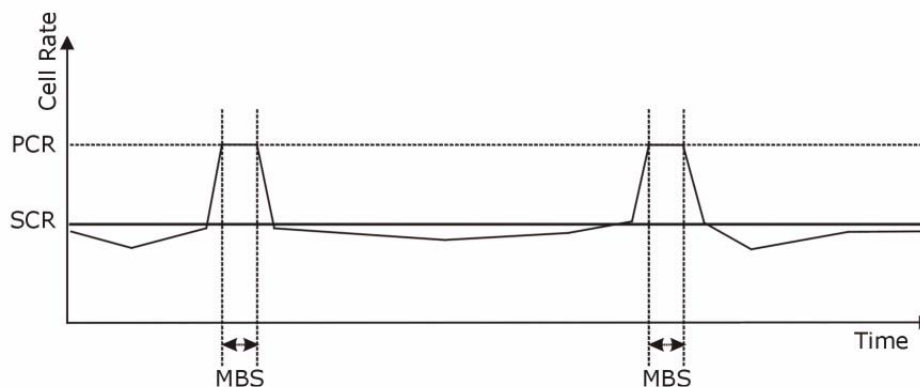
Sustained Cell Rate (SCR) is the mean cell rate of each bursty traffic source. It specifies the maximum average rate at which cells can be sent over the virtual connection. SCR may not be greater than the PCR.

Maximum Burst Size (MBS) is the maximum number of cells that can be sent at the PCR. After MBS is reached, cell rates fall below SCR until cell rate averages to the SCR again. At this time, more cells (up to the MBS) can be sent at the PCR again.

If the PCR, SCR or MBS is set to the default of "0", the system will assign a maximum value that correlates to your upstream line rate.

The following figure illustrates the relationship between PCR, SCR and MBS.

Figure 33 Example of Traffic Shaping



ATM Traffic Classes

These are the basic ATM traffic classes defined by the ATM Forum Traffic Management 4.0 Specification.

Constant Bit Rate (CBR)

Constant Bit Rate (CBR) provides fixed bandwidth that is always available even if no data is being sent. CBR traffic is generally time-sensitive (doesn't tolerate delay). CBR is used for connections that continuously require a specific amount of bandwidth. A PCR is specified and if traffic exceeds this rate, cells may be dropped. Examples of connections that need CBR would be high-resolution video and voice.

Variable Bit Rate (VBR)

The Variable Bit Rate (VBR) ATM traffic class is used with bursty connections. Connections that use the Variable Bit Rate (VBR) traffic class can be grouped into real time (VBR-RT) or non-real time (VBR-nRT) connections.

The VBR-RT (real-time Variable Bit Rate) type is used with bursty connections that require closely controlled delay and delay variation. It also provides a fixed amount of bandwidth (a PCR is specified) but is only available when data is being sent. An example of an VBR-RT connection would be video conferencing. Video conferencing requires real-time data transfers and the bandwidth requirement varies in proportion to the video image's changing dynamics.

The VBR-nRT (non real-time Variable Bit Rate) type is used with bursty connections that do not require closely controlled delay and delay variation. It is commonly used for "bursty" traffic typical on LANs. PCR and MBS define the burst levels, SCR defines the minimum level. An example of an VBR-nRT connection would be non-time sensitive data file transfers.

Unspecified Bit Rate (UBR)

The Unspecified Bit Rate (UBR) ATM traffic class is for bursty data transfers. However, UBR doesn't guarantee any bandwidth and only delivers traffic when the network has spare bandwidth. An example application is background file transfer.

IP Address Assignment

A static IP is a fixed IP that your ISP gives you. A dynamic IP is not fixed; the ISP assigns you a different one each time. The Single User Account feature can be enabled or disabled if you have either a dynamic or static IP. However the encapsulation method assigned influences your choices for IP address and default gateway.

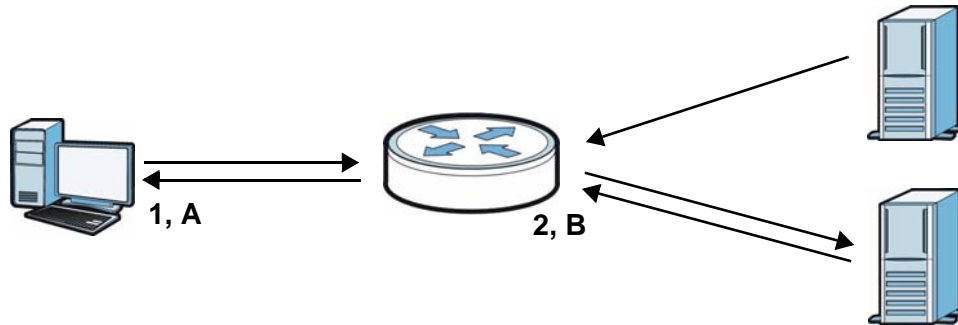
Full Cone NAT

In full cone NAT, the NAT router maps all outgoing packets from an internal IP address and port to a single IP address and port on the external network. The NAT

router also maps packets coming to that external IP address and port to the internal IP address and port.

In the following example, the CellPipe 7130 RG maps the source address of all packets sent from the internal IP address **1** and port **A** to IP address **2** and port **B** on the external network. The CellPipe 7130 RG also performs NAT on all incoming packets sent to IP address **2** and port **B** and forwards them to IP address **1**, port **A**.

Figure 34 Full Cone NAT Example



Symmetric NAT

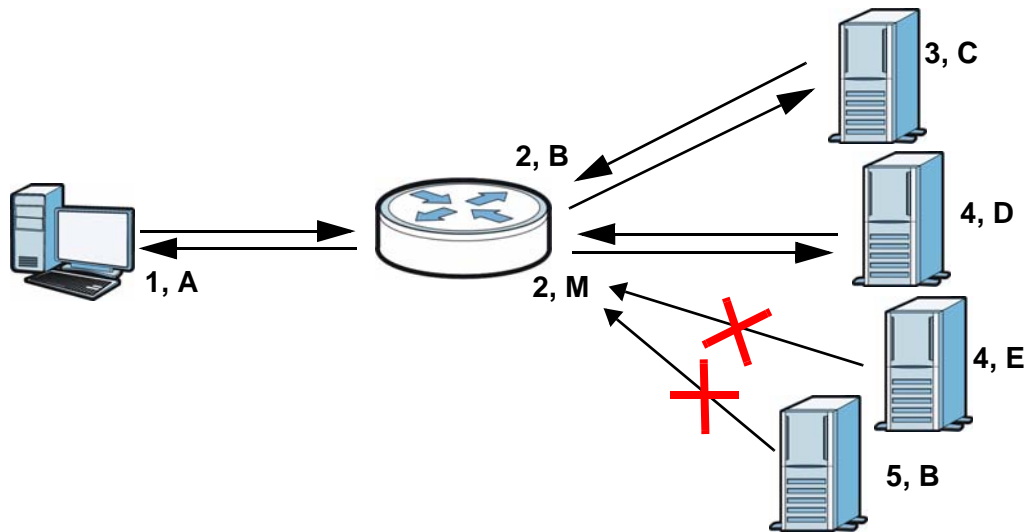
The full, restricted and port restricted cone NAT types use the same mapping for an outgoing packet's source address regardless of the destination IP address and port. In symmetric NAT, the mapping of an outgoing packet's source address to a source address in another network is different for each different destination IP address and port.

In the following example, the CellPipe 7130 RG maps the source address IP address **1** and port **A** to IP address **2** and port **B** on the external network for packets sent to IP address **3** and port **C**. The CellPipe 7130 RG uses a different mapping (IP address **2** and port **M**) for packets sent to IP address **4** and port **D**.

A host on the external network (IP address **3** and port **C** for example) can only send packets to the internal host via the external IP address and port that the NAT router used in sending a packet to the external host's IP address and port. So in

the example, only **3, C** is allowed to send packets to **2, B** and only **4, D** is allowed to send packets to **2, M**.

Figure 35 Symmetric NAT



Introduction to VLANs

A Virtual Local Area Network (VLAN) allows a physical network to be partitioned into multiple logical networks. Devices on a logical network belong to one group. A device can belong to more than one group. With VLAN, a device cannot directly talk to or hear from devices that are not in the same group(s); the traffic must first go through a router.

In Multi-Tenant Unit (MTU) applications, VLAN is vital in providing isolation and security among the subscribers. When properly configured, VLAN prevents one subscriber from accessing the network resources of another on the same LAN, thus a user will not see the printers and hard disks of another user in the same building.

VLAN also increases network performance by limiting broadcasts to a smaller and more manageable logical broadcast domain. In traditional switched environments, all broadcast packets go to each and every individual port. With VLAN, all broadcasts are confined to a specific broadcast domain.

Introduction to IEEE 802.1Q Tagged VLAN

A tagged VLAN uses an explicit tag (VLAN ID) in the MAC header to identify the VLAN membership of a frame across bridges - they are not confined to the switch on which they were created. The VLANs can be created statically by hand or dynamically through GVRP. The VLAN ID associates a frame with a specific VLAN and provides the information that switches need to process the frame across the network. A tagged frame is four bytes longer than an untagged frame and

contains two bytes of TPID (Tag Protocol Identifier), residing within the type/length field of the Ethernet frame) and two bytes of TCI (Tag Control Information), starts after the source address field of the Ethernet frame).

The CFI (Canonical Format Indicator) is a single-bit flag, always set to zero for Ethernet switches. If a frame received at an Ethernet port has a CFI set to 1, then that frame should not be forwarded as it is to an untagged port. The remaining twelve bits define the VLAN ID, giving a possible maximum number of 4,096 VLANs. Note that user priority and VLAN ID are independent of each other. A frame with VID (VLAN Identifier) of null (0) is called a priority frame, meaning that only the priority level is significant and the default VID of the ingress port is given as the VID of the frame. Of the 4096 possible VIDs, a VID of 0 is used to identify priority frames and value 4095 (FFF) is reserved, so the maximum possible VLAN configurations are 4,094.

TPID	User Priority	CFI	VLAN ID
2 Bytes	3 Bits	1 Bit	12 Bits

Multicast

IP packets are transmitted in either one of two ways - Unicast (1 sender - 1 recipient) or Broadcast (1 sender - everybody on the network). Multicast delivers IP packets to a group of hosts on the network - not everybody and not just 1.

Internet Group Multicast Protocol (IGMP) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236. The class D IP address is used to identify host groups and can be in the range 224.0.0.0 to 239.255.255.255. The address 224.0.0.0 is not assigned to any group and is used by IP multicast computers. The address 224.0.0.1 is used for query messages and is assigned to the permanent group of all IP hosts (including gateways). All hosts must join the 224.0.0.1 group in order to participate in IGMP. The address 224.0.0.2 is assigned to the multicast routers group.

At start up, the CellPipe 7130 RG queries all directly connected networks to gather group membership. After that, the CellPipe 7130 RG periodically updates this information.

DNS Server Address Assignment

Use Domain Name System (DNS) to map a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it.

The CellPipe 7130 RG can get the DNS server addresses in the following ways.

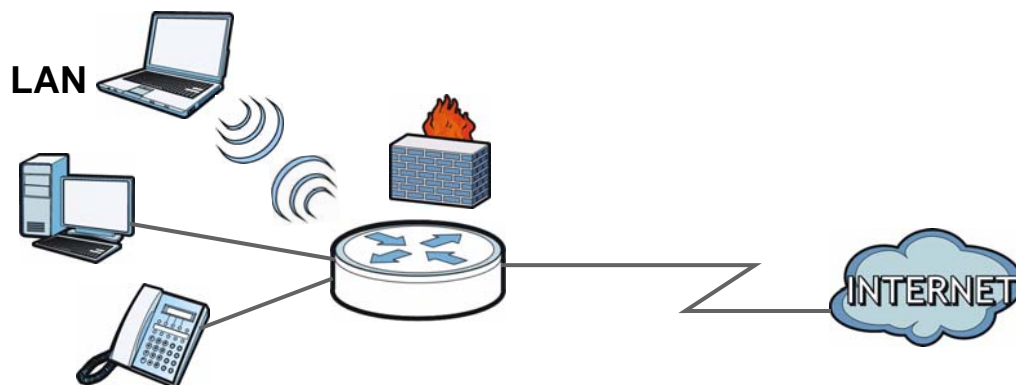
- 1 The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, manually enter them in the DNS server fields.
- 2 If your ISP dynamically assigns the DNS server IP addresses (along with the CellPipe 7130 RG's WAN IP address), set the DNS server fields to get the DNS server address from the ISP.

LAN Setup

6.1 Overview

A Local Area Network (LAN) is a shared communication system to which many computers are attached. A LAN is usually located in one immediate area such as a building or floor of a building.

The LAN screens can help you configure a LAN DHCP server and manage IP addresses.



- See [Section 6.4 on page 134](#) for more information on LANs.
- See [Appendix E on page 373](#) for more information on IP addresses and subnetting.

6.1.1 What You Can Do in this Chapter

The **LAN IP** screen lets you set the LAN IP address and subnet mask of your CellPipe 7130 RG and configure other LAN TCP/IP settings ([Section 6.3 on page 133](#)).

6.2 What You Need To Know

IP Address

Similar to the way houses on a street share a common street name, so too do computers on a LAN share one common network number. This is known as an Internet Protocol address.

Subnet Mask

The subnet mask specifies the network number portion of an IP address. Your CellPipe 7130 RG will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the CellPipe 7130 RG unless you are instructed to do otherwise.

DHCP

DHCP (Dynamic Host Configuration Protocol) allows clients to obtain TCP/IP configuration at start-up from a server. This CellPipe 7130 RG has a built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

RIP

RIP (Routing Information Protocol) allows a router to exchange routing information with other routers.

Multicast and IGMP

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender - 1 recipient) or Broadcast (1 sender - everybody on the network). Multicast delivers IP packets to a group of hosts on the network - not everybody and not just 1.

IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. There are two versions 1 and 2. IGMP version 2 is an improvement over version 1 but IGMP version 1 is still in wide use.

DNS

DNS (Domain Name System) maps a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. The DNS server addresses you enter when you set up DHCP are passed to the client machines along with the assigned IP address and subnet mask.

6.3 The LAN IP Screen

Click **Network > LAN** to open the **IP** screen. See [Section 6.4 on page 134](#) for background information. Use this screen to set the Local Area Network IP address and subnet mask of your CellPipe 7130 RG.

Figure 36 LAN > IP

IP

LAN TCP/IP

IP Address

IP Subnet Mask

DHCP Setup

Active DHCP

IP Pool Starting Address

Pool Size

DNS Server

DNS Servers Assigned by DHCP Server

First DNS Server

Second DNS Server

IGMP Snooping

Active IGMP Snooping

IP Alias

Active IP Alias

IP Address

IP Subnet Mask

.....

The following table describes the fields in this screen.

Table 28 LAN > IP

LABEL	DESCRIPTION
LAN TCP/IP	
IP Address	Enter the LAN IP address you want to assign to your CellPipe 7130 RG in dotted decimal notation, for example, 192.168.1.1 (factory default).
IP Subnet Mask	Type the subnet mask of your network in dotted decimal notation, for example 255.255.255.0 (factory default).
DHCP Setup	

Table 28 LAN > IP

LABEL	DESCRIPTION
Active DHCP	Select this to have the CellPipe 7130 RG act as a DHCP server or DHCP relay agent. Otherwise, deselect this to not have the CellPipe 7130 RG provide any DHCP services. The DHCP server will be disabled.
IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.
Pool Size	This field specifies the size, or count of the IP address pool.
DNS Servers Assigned by DHCP Server If you do not configure DNS servers, the CellPipe 7130 RG uses its LAN IP address and tells the DHCP clients on the LAN that itself is the DNS server. When a LAN client sends a DNS query to the CellPipe 7130 RG, the CellPipe 7130 RG forwards the query to its system DNS server you configured in the WAN screen.	
First DNS Server	Enter the first DNS (Domain Name System) server IP address the CellPipe 7130 RG passes to the DHCP clients.
Second DNS Server	Enter the second DNS (Domain Name System) server IP address the CellPipe 7130 RG passes to the DHCP clients.
IGMP Snooping	
Active IGMP Snooping	Select this option to enable IGMP snooping. This allows the CellPipe 7130 RG to passively learn multicast group.
Active IP Alias	Select the check box to configure another LAN network for the CellPipe 7130 RG.
IP Address	Enter the IP address of your CellPipe 7130 RG in dotted decimal notation.
IP Subnet Mask	Type the subnet mask of your network in dotted decimal notation, for example 255.255.255.0 (factory default).
Apply	Click Apply to save your changes back to the CellPipe 7130 RG.

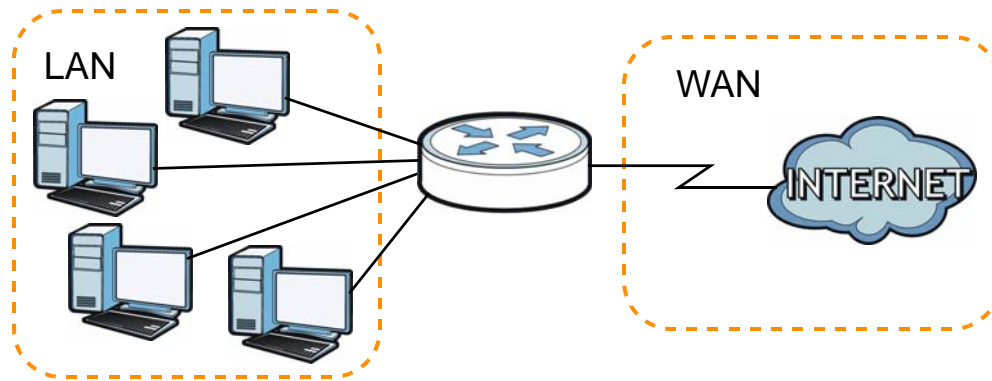
6.4 Technical Reference

The following section contains additional technical information about the CellPipe 7130 RG features described in this chapter.

LANs, WANs and the CellPipe 7130 RG

The actual physical connection determines whether the CellPipe 7130 RG ports are LAN or WAN ports. There are two separate IP networks, one inside the LAN network and the other outside the WAN network as shown next.

Figure 37 LAN and WAN IP Addresses



DHCP Setup

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the CellPipe 7130 RG as a DHCP server or disable it. When configured as a server, the CellPipe 7130 RG provides the TCP/IP configuration for the clients. If you turn DHCP service off, you must have another DHCP server on your LAN, or else the computer must be manually configured.

IP Pool Setup

The CellPipe 7130 RG is pre-configured with a pool of IP addresses for the DHCP clients (DHCP Pool). See the product specifications in the appendices. Do not assign static IP addresses from the DHCP pool to your LAN computers.

LAN TCP/IP

The CellPipe 7130 RG has built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

IP Address and Subnet Mask

Similar to the way houses on a street share a common street name, so too do computers on a LAN share one common network number.

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP

addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0 and you must enable the Network Address Translation (NAT) feature of the CellPipe 7130 RG. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. Let's say you select 192.168.1.0 as the network number; which covers 254 individual addresses, from 192.168.1.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first three numbers specify the network number while the last number identifies an individual computer on that network.

Once you have decided on the network number, pick an IP address that is easy to remember, for instance, 192.168.1.1, for your CellPipe 7130 RG, but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your CellPipe 7130 RG will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the CellPipe 7130 RG unless you are instructed to do otherwise.

Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet, for example, only between your two branch offices, you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Note: Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, "Address Allocation for Private Internets" and RFC 1466, "Guidelines for Management of IP Address Space".

IP Alias

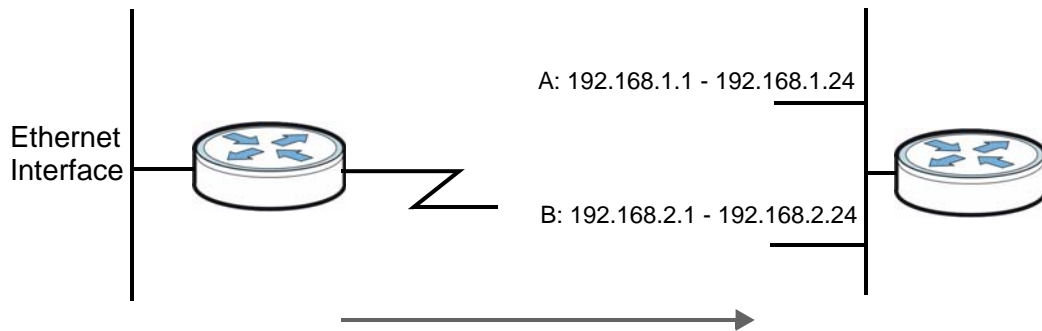
IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The CellPipe 7130 RG supports three logical LAN interfaces via its single physical Ethernet interface with the CellPipe 7130 RG itself as the gateway for each LAN network.

When you use IP alias, you can also configure firewall rules to control access between the LAN's logical networks (subnets).

Note: Make sure that the subnets of the logical networks do not overlap.

The following figure shows a LAN divided into subnets A and B.

Figure 38 Physical Network & Partitioned Logical Networks



Wireless LAN

7.1 Overview

This chapter describes how to perform tasks related to setting up and optimizing your wireless network, including the following.

- Turning the wireless connection on or off.
- Configuring a name, wireless channel and security for the network.
- Using WiFi Protected Setup (WPS) to configure your wireless network.
- Using a MAC (Media Access Control) address filter to restrict access to the wireless network.

See [Chapter 2 on page 29](#) for a tutorial showing how to set up your wireless connection in an example scenario.

See [Section 7.10 on page 159](#) for advanced technical information on wireless networks.

7.1.1 What You Can Do in this Chapter

This chapter describes the CellPipe 7130 RG's **Network > Wireless LAN** screens. Use these screens to set up your CellPipe 7130 RG's wireless connection.

- The **General** screen lets you turn the wireless connection on or off, set up wireless security and make other basic configuration changes ([Section 7.4 on page 143](#)). You can also configure the MAC filter to allow or block access to the CellPipe 7130 RG based on the MAC addresses of the wireless stations.
- The **More AP** screen lets you set up multiple wireless networks on your CellPipe 7130 RG ([Section 7.5 on page 152](#)).
- Use the **WPS** screen and the **WPS Station** screen to use WiFi Protected Setup (WPS). WPS lets you set up a secure network quickly, when connecting to other WPS-enabled devices.

Use the **WPS** screen (see [Section 7.6 on page 153](#)) to enable or disable WPS, generate a security PIN (Personal Identification Number) and see information about the CellPipe 7130 RG's WPS status.

Use the **WPS Station** (see [Section 7.7 on page 155](#)) screen to set up WPS by pressing a button or using a PIN.

- The **WDS** screen lets you set up a Wireless Distribution System, in which the CellPipe 7130 RG acts as a bridge with other access points ([Section 7.8 on page 156](#)).
- The **Advanced Setup** screen lets you change the wireless mode, and make other advanced wireless configuration changes ([Section 7.9 on page 158](#)).

You don't necessarily need to use all these screens to set up your wireless connection. For example, you may just want to set up a network name, a wireless radio channel and some security in the **General** screen.

7.2 What You Need to Know

Wireless Basics

"Wireless" is essentially radio communication. In the same way that walkie-talkie radios send and receive information over the airwaves, wireless networking devices exchange information with one another. A wireless networking device is just like a radio that lets your computer exchange information with radios attached to other computers. Like walkie-talkies, most wireless networking devices operate at radio frequency bands that are open to the public and do not require a license to use. However, wireless networking is different from that of most traditional radio communications in that there a number of wireless networking standards available with different methods of data encryption.

Wireless Network Construction

Wireless networks consist of wireless clients, access points and bridges.

- A wireless client is a radio connected to a user's computer.
- An access point is a radio with a wired connection to a network, which can connect with numerous wireless clients and let them access the network.
- A bridge is a radio that relays communications between access points and wireless clients, extending a network's range.

Traditionally, a wireless network operates in one of two ways.

- An "infrastructure" type of network has one or more access points and one or more wireless clients. The wireless clients connect to the access points.
- An "ad-hoc" type of network is one in which there is no access point. Wireless clients connect to one another in order to exchange information.

Network Names

Each network must have a name, referred to as the SSID - "Service Set Identifier". The "service set" is the network, so the "service set identifier" is the

network's name. This helps you identify your wireless network when wireless networks' coverage areas overlap and you have a variety of networks to choose from.

Radio Channels

In the radio spectrum, there are certain frequency bands allocated for unlicensed, civilian use. For the purposes of wireless networking, these bands are divided into numerous channels. This allows a variety of networks to exist in the same place without interfering with one another. When you create a network, you must select a channel to use.

Since the available unlicensed spectrum varies from one country to another, the number of available channels also varies.

Wireless Security

By their nature, radio communications are simple to intercept. For wireless data networks, this means that anyone within range of a wireless network without security can not only read the data passing over the airwaves, but also join the network. Once an unauthorized person has access to the network she/he can either steal information or introduce malware (malicious software) intended to compromise the network. For these reasons, a variety of security systems have been developed to ensure that only authorized people can use a wireless data network, or understand the data carried on it.

These security standards do two things. First, they authenticate. This means that only people presenting the right credentials (often a username and password, or a "key" phrase) can access the network. Second, they encrypt. This means that the information sent over the air is encoded. Only people with the code key can understand the information, and only people who have been authenticated are given the code key.

These security standards vary in effectiveness. Some can be broken, such as the old Wired Equivalent Protocol (WEP). Using WEP is better than using no security at all, but it will not keep a determined attacker out. Other security standards are secure in themselves but can be broken if a user does not use them properly. For example, the WPA-PSK security standard is perfectly secure if you use a long key which is difficult for an attacker's software to guess - for example, a twenty-letter long string of apparently random numbers and letters - but it is not very secure if you use a short key which is very easy to guess.

Because of the damage that can be done by a malicious attacker, it's not just people who have sensitive information on their network who should use security. Everybody who uses any wireless network should ensure that effective security is in place.

A good way to come up with effective security keys, passwords and so on is to use obscure information that you personally will easily remember, and to enter it in a way that appears random and does not include real words. For example, if your mother owns a 1970 Dodge Challenger and her favorite movie is Vanishing Point (which you know was made in 1971) you could use “70dodchal71vanpoi” as your security key.

Signal Problems

Because wireless networks are radio networks, their signals are subject to limitations of distance, interference and absorption.

Problems with distance occur when the two radios are too far apart. Problems with interference occur when other radio waves interrupt the data signal. Interference may come from other radio transmissions, such as military or air traffic control communications, or from machines that are coincidental emitters such as electric motors or microwaves. Problems with absorption occur when physical objects (such as thick walls) are between the two radios, muffling the signal.

7.3 Before You Begin

Before you start using these screens, ask yourself the following questions. See [Section 7.2 on page 140](#) if some of the terms used here do not make sense to you.

- What wireless standards do the other wireless devices support (IEEE 802.11g, for example)? What is the most appropriate standard to use?
- What security options do the other wireless devices support (WPA-PSK, for example)? What is the best one to use?
- Do the other wireless devices support WPS (Wi-Fi Protected Setup)? If so, you can set up a well-secured network very easily.

Even if some of your devices support WPS and some do not, you can use WPS to set up your network and then add the non-WPS devices manually, although this is somewhat more complicated to do.

- What advanced options do you want to configure, if any? If you want to configure advanced options, ensure that you know precisely what you want to do. If you do not want to configure advanced options, leave them alone.

7.4 The General Screen

Note: If you are configuring the CellPipe 7130 RG from a computer connected to the wireless LAN and you change the CellPipe 7130 RG's SSID or security settings, you will lose your wireless connection when you press **Apply** to confirm. You must then change the wireless settings of your computer to match the CellPipe 7130 RG's new settings.

Click **Network > Wireless LAN** to open the **General** screen.

Figure 39 Network > Wireless LAN > General

The following table describes the labels in this screen.

Table 29 Network > Wireless LAN > General

LABEL	DESCRIPTION
Active Wireless LAN	Click the check box to activate wireless LAN.
Channel Selection	Set the operating frequency/channel depending on your particular region. Select a channel or use Auto to have the CellPipe 7130 RG automatically determine a channel to use. If you are having problems with wireless interference, changing the channel may help. Try to use a channel that is as many channels away from any channels used by neighboring APs as possible. The channel number which the CellPipe 7130 RG is currently using then displays next to this field.

Table 29 Network > Wireless LAN > General

LABEL	DESCRIPTION
Bandwidth	<p>Select whether the CellPipe 7130 RG uses a wireless channel width of 20MHz or 40MHz.</p> <p>A standard 20MHz channel offers transfer speeds of up to 150Mbps whereas a 40MHz channel uses two standard channels and offers speeds of up to 300 Mbps.</p> <p>40MHz (channel bonding or dual channel) bonds two adjacent radio channels to increase throughput. The wireless clients must also support 40 MHz. It is often better to use the 20 MHz setting in a location where the environment hinders the wireless signal.</p> <p>Select 20MHz if you want to lessen radio interference with other wireless devices in your neighborhood or the wireless clients do not support channel bonding.</p> <p>This field is available only when you set the 802.11 Mode to 802.11n Only or 802.11b/g/n Mixed in the Advanced Setup screen.</p>
Control Sideband	<p>This is available for some regions when you select a specific channel and set the Bandwidth field to 40MHz. Set whether the control channel (set in the Channel field) should be in the Lower or Upper range of channel bands.</p> <p>This field is available only when you set the 802.11 Mode to 802.11n Only or 802.11b/g/n Mixed in the Advanced Setup screen.</p>
Network Name (SSID)	<p>The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN.</p> <p>Note: If you are configuring the CellPipe 7130 RG from a computer connected to the wireless LAN and you change the CellPipe 7130 RG's SSID or wireless security settings, you will lose your wireless connection when you press Apply to confirm. You must then change the wireless settings of your computer to match the CellPipe 7130 RG's new settings.</p>
Hide Network Name (SSID)	<p>Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.</p>
Enable Wireless Multicast Forwarding (WMF)	<p>Select this check box to allow the CellPipe 7130 RG to convert wireless multicast traffic into wireless unicast traffic.</p>
BSSID	<p>This shows the MAC address of the wireless interface on the CellPipe 7130 RG when wireless LAN is enabled.</p>
Security Mode	<p>See the following sections for more details about this field.</p>
MAC Filter	<p>Click this button to go to the MAC Filter screen to configure whether the wireless devices with the MAC addresses listed are allowed or denied to access the CellPipe 7130 RG using this SSID.</p>

Table 29 Network > Wireless LAN > General

LABEL	DESCRIPTION
Apply	Click this to save your changes back to the CellPipe 7130 RG.
Reset	Click this to reload the previous configuration for this screen.

7.4.1 No Security

Select **No Security** to allow wireless devices to communicate with the access points without any data encryption or authentication.

Note: If you do not enable any wireless security on your CellPipe 7130 RG, your network is accessible to any wireless networking device that is within range.

Figure 40 Wireless LAN > General: No Security

The screenshot shows the configuration interface for the Wireless LAN > General page. The 'General' tab is selected. Under 'Wireless Setup', 'Active Wireless LAN' is checked. Channel Selection is set to 'Auto' (Current: 6), Bandwidth is '20MHz', and Control Sideband is 'Lower'. Under 'Common Setup', the Network Name (SSID) field is empty, and 'Hide Network Name (SSID)' and 'Enable Wireless Multicast Forwarding (WMF)' are unchecked. A note indicates that only IGMP v2 report messages are supported for wireless multicast forwarding. The BSSID is 40:4A:03:AD:70:48. The Security Mode is set to 'No Security'. There is an 'Edit' button for the MAC Filter. At the bottom, there are 'Apply' and 'Reset' buttons.

The following table describes the labels in this screen.

Table 30 Wireless LAN > General: No Security

LABEL	DESCRIPTION
Security Mode	Choose No Security from the drop-down list box.

7.4.2 WEP Encryption

In order to configure and enable WEP encryption; click **Network > Wireless LAN** to display the **General** screen. Select **WEP** from the **Security Mode** list.

Figure 41 Wireless LAN > General: Static WEP Encryption

The screenshot shows the configuration page for Wireless LAN > General. The 'General' tab is selected. Under 'Wireless Setup', 'Active Wireless LAN' is checked. Channel Selection is set to 'Auto' (Current: 6), Bandwidth is '20MHz', and Control Sideband is 'Lower'. Under 'Common Setup', Network Name (SSID) is empty, and 'Hide Network Name (SSID)' and 'Enable Wireless Multicast Forwarding (WMF)' are unchecked. A note states: 'Only IGMP v2 report message is supported for wireless multicast forwarding function.' BSSID is 40:4A:03:AD:70:48. Security Mode is set to 'WEP' and WEP Encryption is '128-bit'. Another note states: '64-bit WEP: Enter 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F") for each Key (1-4). 128-bit WEP: Enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F") for each Key (1-4). (Select one WEP key as an active key to encrypt wireless data transmission.)' Four keys are listed, all with the value '1234567890123'. Key 1 is selected. A 'MAC Filter' section has an 'Edit' button. At the bottom are 'Apply' and 'Reset' buttons.

The following table describes the wireless LAN security labels in this screen.

Table 31 Network > Wireless LAN > General: Static WEP Encryption

LABEL	DESCRIPTION
Security Mode	Choose WEP from the drop-down list box.

Table 31 Network > Wireless LAN > General: Static WEP Encryption

LABEL	DESCRIPTION
WEP Encryption	WEP (Wired Equivalent Privacy) provides data encryption to prevent unauthorized wireless stations from accessing data transmitted over the wireless network. Select 64-bit or 128-bit to enable data encryption.
Key 1 to Key 4	The WEP key is used to secure your data from eavesdropping by unauthorized wireless users. Both the CellPipe 7130 RG and the wireless stations must use the same WEP key for data transmission. Only one key can be activated at any one time. Select a default key to use for data encryption. If you chose 64-bit in the WEP Encryption field, then enter any 5 characters (ASCII string) or 10 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key. If you chose 128-bit in the WEP Encryption field, then enter 13 characters (ASCII string) or 26 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key.

7.4.3 WPA(2)-PSK

In order to configure and enable WPA(2)-PSK authentication; click **Network > Wireless LAN** to display the **General** screen. Select **WPA-PSK** or **WPA2-PSK** from the **Security Mode** list.

Figure 42 Wireless LAN > General: WPA(2)-PSK

The screenshot displays the configuration interface for WPA(2)-PSK. It features several sections:

- Wireless Setup:** Includes checkboxes for 'Active Wireless LAN', 'Channel Selection' (set to Auto), 'Bandwidth' (set to 20MHz), and 'Control Sideband' (set to Lower).
- Common Setup:** Includes a text field for 'Network Name (SSID)', checkboxes for 'Hide Network Name (SSID)' and 'Enable Wireless Multicast Forwarding (WMF)', and a 'Note' about IGMP v2 support.
- Security Mode:** Includes a dropdown menu set to 'WPA2-PSK', a checkbox for 'Active Compatible', and a dropdown menu set to 'WPA-PSK Compatible'.
- Encryption:** Includes a dropdown menu set to 'AES'.
- Pre-Shared Key:** Includes a text field containing '0409sanrio'.
- Group Key Update Timer:** Includes a text field set to '0' and a unit label 'sec'.
- MAC Filter:** Includes an 'Edit' button.

At the bottom of the page, there are 'Apply' and 'Reset' buttons.

The following table describes the wireless LAN security labels in this screen.

Table 32 Wireless LAN > General: WPA(2)-PSK

LABEL	DESCRIPTION
Auto Generate Key	This field is only available for WPA-PSK. Select this option to have the CellPipe 7130 RG automatically generate an SSID and pre-shared key. The SSID and Pre-Shared Key fields will not be configurable when you select this option.
Security Mode	Choose WPA-PSK or WPA2-PSK from the drop-down list box.
Active Compatible	This field is only available for WPA2-PSK. Select this if you want the CellPipe 7130 RG to support WPA-PSK and WPA2-PSK simultaneously.
Encryption	Select the encryption type (TKIP , AES or TKIP+AES) for data encryption. Select TKIP if your wireless clients can all use TKIP. Select AES if your wireless clients can all use AES. Select TKIP+AES to allow the wireless clients to use either TKIP or AES.
Pre-Shared Key	The encryption mechanisms used for WPA(2) and WPA(2)-PSK are the same. The only difference between the two is that WPA(2)-PSK uses a simple common password, instead of user-specific credentials. Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols).
Group Key Update Timer	The Group Key Update Timer is the rate at which the AP sends a new group key out to all clients.

7.4.4 WPA(2) Authentication

Use this screen to configure and enable WPA or WPA2 authentication; click the **Wireless LAN** link under **Network** to display the **General** screen. Select **WPA** or **WPA2** from the **Security Mode** list.

Note: WPA or WPA2 is not available if you enable WPS before you configure WPA or WPA2 in the **Wireless LAN > General** screen.

Note: If you select **WPA** or **WPA2** in the **Wireless LAN > General** screen, the WDS and WPS features are not available on the CellPipe 7130 RG.

Figure 43 Wireless LAN > General: WPA(2)

The screenshot shows the configuration interface for the wireless LAN. At the top, there are tabs for 'General', 'More AP', 'WPS', 'WPS Station', 'WDS', and 'Advanced Setup'. The 'General' tab is selected. Under 'Wireless Setup', 'Active Wireless LAN' is checked. Channel Selection is set to 'Auto' (Current: 6), Bandwidth is '20MHz', and Control Sideband is 'Lower'. Under 'Common Setup', there is a text field for 'Network Name (SSID)', and checkboxes for 'Hide Network Name (SSID)' and 'Enable Wireless Multicast Forwarding (WMF)'. A note states: 'Only IGMP v2 report message is supported for wireless multicast forwarding function.' Below this, the BSSID is '40:4A:03:AD:70:48'. Security Mode is 'WPA2', with 'Active Compatible' unchecked and 'WPA Compatible' selected. Encryption is 'AES', and WPA2 Preauthentication is 'Disabled'. Network Re-auth Interval is '36000' sec and Group Key Update Timer is '0' sec. Authentication Server settings include IP Address '0.0.0.0', Port Number '1812', and a Shared Secret field. A 'MAC Filter' section has an 'Edit' button. At the bottom, there are 'Apply' and 'Reset' buttons.

The following table describes the wireless LAN security labels in this screen.

Table 33 Wireless LAN > General: WPA(2)

LABEL	DESCRIPTION
Security Mode	Choose WPA or WPA2 from the drop-down list box.
Active Compatible	This field is only available for WPA2. Select this if you want the CellPipe 7130 RG to support WPA and WPA2 simultaneously.
Encryption	Select the encryption type (TKIP , AES or TKIP+AES) for data encryption. Select TKIP if your wireless clients can all use TKIP. Select AES if your wireless clients can all use AES. Select TKIP+AES to allow the wireless clients to use either TKIP or AES.

Table 33 Wireless LAN > General: WPA(2)

LABEL	DESCRIPTION
WPA2 Preauthentication	This field is available only when you select WPA2 . Pre-authentication enables fast roaming by allowing the wireless client (already connecting to an AP) to perform IEEE 802.1x authentication with another AP before connecting to it. Select Enabled to turn on preauthentication in WAP2. Otherwise, select Disabled .
Network Re-auth Interval	This field is available only when you select WPA2 . Specify how often wireless clients have to resend usernames and passwords in order to stay connected. Enter a time interval between 10 and 2147483647 seconds. Note: If wireless client authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Group Key Update Timer	The Group Key Update Timer is the rate at which the RADIUS server sends a new group key out to all clients.
Authentication Server	
IP Address	Enter the IP address of the external authentication server in dotted decimal notation.
Port Number	Enter the port number of the external authentication server. The default port number is 1812 . You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the CellPipe 7130 RG. The key must be the same on the external authentication server and your CellPipe 7130 RG. The key is not sent over the network.

7.4.5 MAC Filter

This screen allows you to configure the CellPipe 7130 RG to give exclusive access to specific devices (**Allow**) or exclude specific devices from accessing the CellPipe 7130 RG (**Deny**). Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC addresses of the devices to configure this screen.

Use this screen to change your CellPipe 7130 RG's MAC filter settings. Click the **Edit** button in the **Wireless LAN > General** screen. The following screen displays.

Figure 44 Wireless LAN > MAC Filter

The following table describes the labels in this screen.

Table 34 Wireless LAN > MAC Filter

LABEL	DESCRIPTION
MAC Restrict Mode	Define the filter action for the list of MAC addresses in the table below. Select Disabled to turn off MAC address filtering. Select Allow to permit access to the CellPipe 7130 RG, MAC addresses not listed will be denied access to the CellPipe 7130 RG. Select Deny to block access to the CellPipe 7130 RG, MAC addresses not listed will be allowed to access the CellPipe 7130 RG
#	This is the index number of the MAC address.
MAC Address	This is the MAC addresses of the wireless devices that are allowed or denied access to the CellPipe 7130 RG.
Modify	Click the Remove icon to delete the entry.
Back	Click this to return to the previous screen without saving changes.
Add	Click this to create a new MAC filtering rule.

7.4.6 Adding a New MAC Filtering Rule

Click the **Add** button in the **MAC Filter** screen. The following screen displays.

Figure 45 Wireless LAN > MAC Filter > Add

The following table describes the labels in this screen.

Table 35 Wireless LAN > MAC Filter > Add

LABEL	DESCRIPTION
MAC Address	Enter the MAC addresses of the wireless devices that are allowed or denied access to the CellPipe 7130 RG in these address fields. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.
Back	Click this to return to the previous screen without saving changes.
Apply	Click this to save your changes and go back to the previous screen.

7.5 The More AP Screen

This screen allows you to enable and configure multiple wireless networks on the CellPipe 7130 RG.

Click **Network > Wireless LAN > More AP**. The following screen displays.

Figure 46 Network > Wireless LAN > More AP

#	Active	SSID	Security	Modify
1	<input type="checkbox"/>	Guest1	No Security	
2	<input type="checkbox"/>	Guest2	No Security	
3	<input type="checkbox"/>	Guest3	No Security	

Apply Reset

The following table describes the labels in this screen.

Table 36 Network > Wireless LAN > More AP

LABEL	DESCRIPTION
#	This is the index number of each SSID profile.
Active	Select the check box to activate an SSID profile.
SSID	An SSID profile is the set of parameters relating to one of the CellPipe 7130 RG's BSSs. The SSID (Service Set Identifier) identifies the Service Set with which a wireless device is associated. This field displays the name of the wireless profile on the network. When a wireless client scans for an AP to associate with, this is the name that is broadcast and seen in the wireless client utility.
Security	This field indicates the security mode of the SSID profile.
Modify	Click the Edit icon to configure the SSID profile.

Table 36 Network > Wireless LAN > More AP

LABEL	DESCRIPTION
Apply	Click Apply to save your changes back to the CellPipe 7130 RG.
Reset	Click Reset to reload the previous configuration for this screen.

7.5.1 More AP Edit

Use this screen to edit an SSID profile. Click the **Edit** icon next to an SSID in the **More AP** screen. The following screen displays.

Figure 47 Network > Wireless LAN > More AP: Edit

Common Setup

Active

Network Name (SSID)

Hide Network Name (SSID)

Enable Wireless Multicast Forwarding (WMF)

Note:
Only IGMP v2 report message is supported for wireless multicast forwarding function.

BSSID

Security Mode

MAC Filter

See [Section 7.4 on page 143](#) for more details about the fields in this screen.

7.6 The WPS Screen

Use this screen to configure WiFi Protected Setup (WPS) on your CellPipe 7130 RG.

WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Set up each WPS connection between two devices. Both devices must support WPS.

Click **Network > Wireless LAN > WPS**. The following screen displays.

Figure 48 Network > Wireless LAN > WPS

The following table describes the labels in this screen.

Table 37 Network > Wireless LAN > WPS

LABEL	DESCRIPTION
WPS Setup	
Enable WPS	Select the check box to activate WPS on the CellPipe 7130 RG.
PIN Number	This shows the PIN (Personal Identification Number) of the CellPipe 7130 RG. Enter this PIN in the configuration utility of the device you want to connect to using WPS. The PIN is not necessary when you use WPS push-button method.
Generate	Click this button to have the CellPipe 7130 RG create a new PIN.
WPS Status	This displays Configured when the CellPipe 7130 RG has connected to a wireless network using WPS or Enable WPS is selected and wireless or wireless security settings have been changed. The current wireless and wireless security settings also appear in the screen. This displays Unconfigured if WPS is disabled and there is no wireless or wireless security changes on the CellPipe 7130 RG or you click Release_Configuration to remove the configured wireless and wireless security settings.
Release_Configuration	This button is available when the WPS status is Configured but not configurable if you disable WPS. Click this button to remove all configured wireless and wireless security settings for WPS connections on the CellPipe 7130 RG.
Apply	Click Apply to save your changes back to the CellPipe 7130 RG.

7.7 The WPS Station Screen

Use this screen to set up a WPS wireless network using either Push Button Configuration (PBC) or PIN Configuration.

Note: If you select **No Security** in the **Wireless LAN > General** screen and click **Push Button** in the **WPS Station** screen, the CellPipe 7130 RG automatically changes to use WPA-PSK/WPA2-PSK mixed mode and generates a pre-shared key.

Click **Network > Wireless LAN > WPS Station**. The following screen displays.

Figure 49 Network > Wireless LAN > WPS Station

The following table describes the labels in this screen.

Table 38 Network > Wireless LAN > WPS Station

LABEL	DESCRIPTION
Push Button	Click this button to add another WPS-enabled wireless device (within wireless range of the CellPipe 7130 RG) to your wireless network. This button may either be a physical button on the outside of device, or a menu button similar to the Push Button on this screen. Note: You must press the other wireless device's WPS button within two minutes of pressing this button.
Or input station's PIN number	Enter the PIN of the device that you are setting up a WPS connection with and click Start to authenticate and add the wireless device to your wireless network. You can find the PIN either on the outside of the device, or by checking the device's settings. Note: You must also activate WPS on that device within two minutes to have it present its PIN to the CellPipe 7130 RG.

7.8 The WDS Screen

A Wireless Distribution System (WDS) is a wireless connection between two or more APs. Use this screen to set up your WDS links between the CellPipe 7130 RGs. You need to know the MAC address of the peer device. Once the security settings of peer sides match one another, the connection between the devices is made.

Note: You cannot use WDS when WPS is enabled or wireless security is set to "WPA" or "WPA2". The wireless security settings apply to both WDS links and the connections between the CellPipe 7130 RG and any wireless clients.

Note: At the time of writing, WDS is only compatible with other CellPipe 7130 RGs of the same model.

Click **Network > Wireless LAN > WDS**. The following screen displays. WDS is turned on and this screen is configurable when the CellPipe 7130 RG's wireless security mode is **No Security, WEP** or **WPA(2)-PSK**.

Figure 50 Network > Wireless LAN > WDS

WDS

Operating Mode:

Bridge Restrict:

Remote Bridges MAC Address:

	SSID	BSSID
<input type="checkbox"/>	ZyXEL_3YEEMN	00:11:22:33:44:54
<input type="checkbox"/>	ZyXEL_MIS	00:23:F8:55:B6:7F
<input type="checkbox"/>	ZyXEL_MIS	00:19:CB:8A:34:D0
<input type="checkbox"/>	Digicel	00:23:F8:23:BD:CF
<input type="checkbox"/>	ZyXEL_4WM444	40:4A:03:F9:DB:04
<input type="checkbox"/>	ZyXEL_MIS_WPA	06:23:F8:55:B6:7F

Note :

1. The WDS function only works on the No Security, WEP, WPA-PSK and WPA2-PSK security mode.
2. The WDS function only works on the basic SSID.
3. The WDS function works when disable WPS.
4. The SSID should be the same when the WDS function works in WPA-PSK or WPA2-PSK security mode.

The following table describes the labels in this screen.

Table 39 Network > Wireless LAN > WDS

LABEL	DESCRIPTION
WDS	
Operating Mode	<p>Select the operating mode for your CellPipe 7130 RG.</p> <ul style="list-style-type: none"> • Access Point + Bridge - The CellPipe 7130 RG functions as a bridge and access point simultaneously. • Wireless Bridge - The CellPipe 7130 RG acts as a wireless network bridge and establishes wireless links with other APs. In this mode, clients cannot connect to the CellPipe 7130 RG wirelessly. <p>You need to know the MAC address of the peer device, which must be of the same model and also WDS-enabled. The CellPipe 7130 RG can establish up to four wireless links with other APs.</p>
Bridge Restrict	<p>This field is available only when you set operating mode to Access Point + Bridge.</p> <p>Select Enabled to turn on WDS and enter the peer device's MAC address manually in the table below.</p> <p>Select Enabled(Scan) to turn on WDS, search and display the available APs within range in the table below.</p>
Remote Bridges MAC Address	<p>Enter the MAC address of the peer device that your CellPipe 7130 RG wants to make a bridge connection with.</p> <p>You can connect to up to 4 peer devices.</p>
	<p>This field is available only when you select Enabled(Scan) in the Bridge Restrict field.</p> <p>Select the check box and click Apply to have the CellPipe 7130 RG establish a wireless link with the selected wireless device.</p>
SSID	<p>This field is available only when you select Enabled(Scan) in the Bridge Restrict field.</p> <p>This shows the SSID of the available wireless device within range.</p>
BSSID	<p>This field is available only when you select Enabled(Scan) in the Bridge Restrict field.</p> <p>This shows the MAC address of the available wireless device within range.</p>
Refresh	<p>Click Refresh to update the Remote Bridges MAC Address table when Bridge Restrict is set to Enabled(Scan).</p>
Apply	<p>Click Apply to save your changes to CellPipe 7130 RG.</p>

7.9 The Advanced Setup Screen

To configure advanced wireless settings, click **Network > Wireless LAN > Advanced Setup**. The screen appears as shown.

Figure 51 Wireless LAN > Advanced Setup

The screenshot shows the 'Advanced Setup' tab selected. The settings are as follows:

- RTS/CTS Threshold: 2347
- Fragmentation Threshold: 2346
- Number of Wireless Stations Allowed: 16
- Output Power: 100%
- Multicast Rate: 54 Mbps
- 802.11 Mode: 802.11b/g/n Mixed
- 802.11 Protection: Auto
- Preamble: Long

Buttons for 'Apply' and 'Reset' are located at the bottom of the configuration area.

The following table describes the labels in this screen.

Table 40 Wireless LAN > Advanced Setup

LABEL	DESCRIPTION
RTS/CTS Threshold	Enter a value between 0 and 2432.
Fragmentation Threshold	This is the maximum data fragment size that can be sent. Enter a value between 256 and 2432.
Number of Wireless Stations Allowed	Specify the maximum number (from 1 to 64) of the wireless stations that may connect to the CellPipe 7130 RG.
Output Power	Set the output power of the CellPipe 7130 RG. If there is a high density of APs in an area, decrease the output power to reduce interference with other APs. Select one of the following 20% , 40% , 60% , 80% or 100% .
Multicast Rate	Select a data rate at which the CellPipe 7130 RG transmits wireless multicast traffic. If you select a high rate, multicast traffic may occupy all the bandwidth and cause network congestion.

Table 40 Wireless LAN > Advanced Setup

LABEL	DESCRIPTION
802.11 Mode	<p>Select 802.11b Only to only allow IEEE 802.11b compliant WLAN devices to associate with the CellPipe 7130 RG.</p> <p>Select 802.11g Only to allow IEEE 802.11g compliant WLAN devices to associate with the CellPipe 7130 RG. IEEE 802.11b compliant WLAN devices can associate with the CellPipe 7130 RG only when they use the short preamble type.</p> <p>Select 802.11n Only to only allow IEEE 802.11n compliant WLAN devices to associate with the CellPipe 7130 RG. This can increase transmission rates, although IEEE 802.11b or IEEE 802.11g clients will not be able to connect to the CellPipe 7130 RG.</p> <p>Select 802.11b/g Mixed to allow either IEEE 802.11b or IEEE 802.11g compliant WLAN devices to associate with the CellPipe 7130 RG. The CellPipe 7130 RG adjusts the transmission rate automatically according to the wireless standard supported by the wireless devices.</p> <p>Select 802.11 b/g/n mixed mode to allow both IEEE802.11b, IEEE802.11g and IEEE802.11n compliant WLAN devices to associate with the CellPipe 7130 RG. The transmission rate of your CellPipe 7130 RG might be reduced.</p>
802.11 Protection	<p>Enabling this feature can help prevent collisions in mixed-mode networks (networks with both IEEE 802.11b and IEEE 802.11g traffic).</p> <p>Select Auto to have the wireless devices transmit data after a RTS/CTS handshake. This helps improve IEEE 802.11g performance.</p> <p>Select Off to disable 802.11 protection. The transmission rate of your CellPipe 7130 RG might be reduced in a mixed-mode network.</p> <p>This field displays Off and is not configurable when you set 802.11 Mode to 802.11b Only.</p>
Preamble	<p>Select a preamble type from the drop-down list menu. Choices are Long or Short. The default setting is Long. See the appendix for more information.</p> <p>This field is not configurable and the CellPipe 7130 RG uses Short when you set 802.11 Mode to 802.11g Only or 802.11n Only.</p>
Apply	Click this to save your changes back to the CellPipe 7130 RG.
Reset	Click this to reload the previous configuration for this screen.

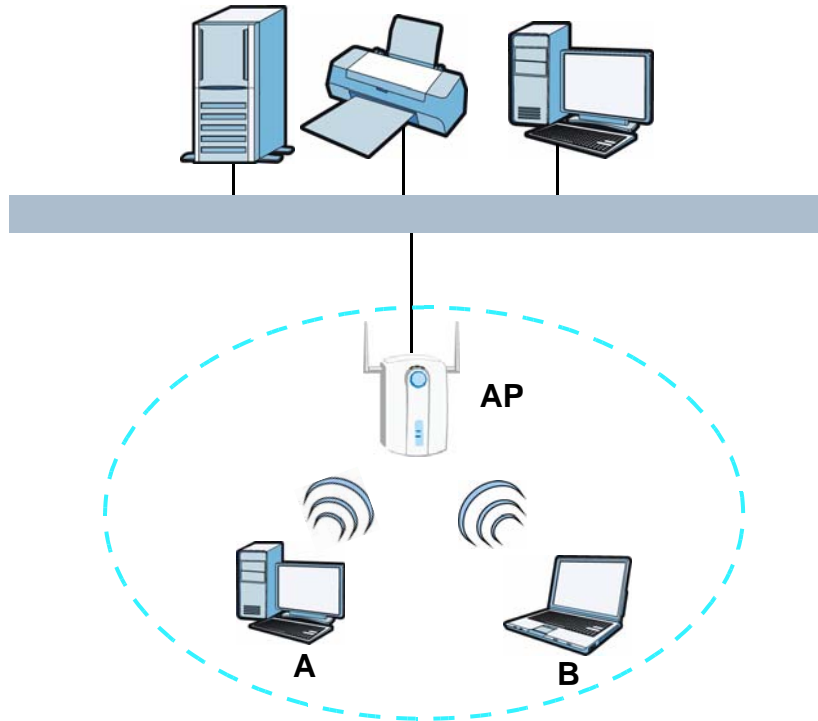
7.10 Technical Reference

This section discusses wireless LANs in depth. For more information, see the appendix.

7.10.1 Wireless Network Overview

The following figure provides an example of a wireless network.

Figure 52 Example of a Wireless Network



The wireless network is the part in the blue circle. In this wireless network, devices **A** and **B** use the access point (**AP**) to interact with the other devices (such as the printer) or with the Internet. Your CellPipe 7130 RG is the AP.

Every wireless network must follow these basic guidelines.

- Every device in the same wireless network must use the same SSID.
The SSID is the name of the wireless network. It stands for Service Set IDentity.
- If two wireless networks overlap, they should use a different channel.
Like radio stations or television channels, each wireless network uses a specific channel, or frequency, to send and receive information.
- Every device in the same wireless network must use security compatible with the AP.
Security stops unauthorized devices from using the wireless network. It can also protect the information that is sent in the wireless network.

7.10.2 Additional Wireless Terms

The following table describes some wireless network terms and acronyms used in the CellPipe 7130 RG's Web Configurator.

Table 41 Additional Wireless Terms

TERM	DESCRIPTION
RTS/CTS Threshold	<p>In a wireless network which covers a large area, wireless devices are sometimes not aware of each other's presence. This may cause them to send information to the AP at the same time and result in information colliding and not getting through.</p> <p>By setting this value lower than the default value, the wireless devices must sometimes get permission to send information to the CellPipe 7130 RG. The lower the value, the more often the devices must get permission.</p> <p>If this value is greater than the fragmentation threshold value (see below), then wireless devices never have to get permission to send information to the CellPipe 7130 RG.</p>
Preamble	A preamble affects the timing in your wireless network. There are two preamble modes: long and short. If a device uses a different preamble mode than the CellPipe 7130 RG does, it cannot communicate with the CellPipe 7130 RG.
Authentication	The process of verifying whether a wireless device is allowed to use the wireless network.
Fragmentation Threshold	A small fragmentation threshold is recommended for busy networks, while a larger threshold provides faster performance if the network is not very busy.

7.10.3 Wireless Security Overview

The following sections introduce different types of wireless security you can set up in the wireless network.

7.10.3.1 SSID

Normally, the CellPipe 7130 RG acts like a beacon and regularly broadcasts the SSID in the area. You can hide the SSID instead, in which case the CellPipe 7130 RG does not broadcast the SSID. In addition, you should change the default SSID to something that is difficult to guess.

This type of security is fairly weak, however, because there are ways for unauthorized wireless devices to get the SSID. In addition, unauthorized wireless devices can still see the information that is sent in the wireless network.

7.10.3.2 MAC Address Filter

Every device that can use a wireless network has a unique identification number, called a MAC address.¹ A MAC address is usually written using twelve hexadecimal

characters²; for example, 00A0C5000002 or 00:A0:C5:00:00:02. To get the MAC address for each device in the wireless network, see the device's User's Guide or other documentation.

You can use the MAC address filter to tell the CellPipe 7130 RG which devices are allowed or not allowed to use the wireless network. If a device is allowed to use the wireless network, it still has to have the correct information (SSID, channel, and security). If a device is not allowed to use the wireless network, it does not matter if it has the correct information.

This type of security does not protect the information that is sent in the wireless network. Furthermore, there are ways for unauthorized wireless devices to get the MAC address of an authorized device. Then, they can use that MAC address to use the wireless network.

7.10.3.3 User Authentication

Authentication is the process of verifying whether a wireless device is allowed to use the wireless network. You can make every user log in to the wireless network before they can use it. However, every device in the wireless network has to support IEEE 802.1x to do this.

For wireless networks, you can store the user names and passwords for each user in a RADIUS server. This is a server used in businesses more than in homes. If you do not have a RADIUS server, you cannot set up user names and passwords for your users.

Unauthorized wireless devices can still see the information that is sent in the wireless network, even if they cannot use the wireless network. Furthermore, there are ways for unauthorized wireless users to get a valid user name and password. Then, they can use that user name and password to use the wireless network.

7.10.3.4 Encryption

Wireless networks can use encryption to protect the information that is sent in the wireless network. Encryption is like a secret code. If you do not know the secret code, you cannot understand the message.

-
1. Some wireless devices, such as scanners, can detect wireless networks but cannot use wireless networks. These kinds of wireless devices might not have MAC addresses.
 2. Hexadecimal characters are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, and F.

The types of encryption you can choose depend on the type of authentication. (See [Section 7.10.3.3 on page 162](#) for information about this.)

Table 42 Types of Encryption for Each Type of Authentication

	NO AUTHENTICATION	RADIUS SERVER
Weakest ↑ ↓	No Security	WPA
	Static WEP	
	WPA-PSK	
Strongest	WPA2-PSK	WPA2

For example, if the wireless network has a RADIUS server, you can choose **WPA** or **WPA2**. If users do not log in to the wireless network, you can choose no encryption, **Static WEP**, **WPA-PSK**, or **WPA2-PSK**.

Usually, you should set up the strongest encryption that every device in the wireless network supports. For example, suppose you have a wireless network with the CellPipe 7130 RG and you do not have a RADIUS server. Therefore, there is no authentication. Suppose the wireless network has two devices. Device A only supports WEP, and device B supports WEP and WPA. Therefore, you should set up **Static WEP** in the wireless network.

Note: It is recommended that wireless networks use **WPA-PSK**, **WPA**, or stronger encryption. The other types of encryption are better than none at all, but it is still possible for unauthorized wireless devices to figure out the original information pretty quickly.

When you select **WPA2** or **WPA2-PSK** in your CellPipe 7130 RG, you can also select an option (**WPA compatible**) to support WPA as well. In this case, if some of the devices support WPA and some support WPA2, you should set up **WPA2-PSK** or **WPA2** (depending on the type of wireless network login) and select the **WPA compatible** option in the CellPipe 7130 RG.

Many types of encryption use a key to protect the information in the wireless network. The longer the key, the stronger the encryption. Every device in the wireless network must have the same key.

7.10.4 WiFi Protected Setup

Your CellPipe 7130 RG supports WiFi Protected Setup (WPS), which is an easy way to set up a secure wireless network. WPS is an industry standard specification, defined by the WiFi Alliance.

WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Each WPS connection works

between two devices. Both devices must support WPS (check each device's documentation to make sure).

Depending on the devices you have, you can either press a button (on the device itself, or in its configuration utility) or enter a PIN (a unique Personal Identification Number that allows one device to authenticate the other) in each of the two devices. When WPS is activated on a device, it has two minutes to find another device that also has WPS activated. Then, the two devices connect and set up a secure network by themselves.

7.10.4.1 Push Button Configuration

WPS Push Button Configuration (PBC) is initiated by pressing a button on each WPS-enabled device, and allowing them to connect automatically. You do not need to enter any information.

Not every WPS-enabled device has a physical WPS button. Some may have a WPS PBC button in their configuration utilities instead of or in addition to the physical button.

Take the following steps to set up WPS using the button.

- 1 Ensure that the two devices you want to set up are within wireless range of one another.
- 2 Look for a WPS button on each device. If the device does not have one, log into its configuration utility and locate the button (see the device's User's Guide for how to do this - for the CellPipe 7130 RG, see [Section 7.7 on page 155](#)).
- 3 Press the button on one of the devices (it doesn't matter which). For the CellPipe 7130 RG you must press the WPS button for more than three seconds.
- 4 Within two minutes, press the button on the other device. The registrar sends the network name (SSID) and security key through an secure connection to the enrollee.

If you need to make sure that WPS worked, check the list of associated wireless clients in the AP's configuration utility. If you see the wireless client in the list, WPS was successful.

7.10.4.2 PIN Configuration

Each WPS-enabled device has its own PIN (Personal Identification Number). This may either be static (it cannot be changed) or dynamic (in some devices you can generate a new PIN by clicking on a button in the configuration interface).

Use the PIN method instead of the push-button configuration (PBC) method if you want to ensure that the connection is established between the devices you specify, not just the first two devices to activate WPS in range of each other. However, you need to log into the configuration interfaces of both devices to use the PIN method.

When you use the PIN method, you must enter the PIN from one device (usually the wireless client) into the second device (usually the Access Point or wireless router). Then, when WPS is activated on the first device, it presents its PIN to the second device. If the PIN matches, one device sends the network and security information to the other, allowing it to join the network.

Take the following steps to set up a WPS connection between an access point or wireless router (referred to here as the AP) and a client device using the PIN method.

- 1 Ensure WPS is enabled on both devices.
- 2 Access the WPS section of the AP's configuration interface. See the device's User's Guide for how to do this.
- 3 Look for the client's WPS PIN; it will be displayed either on the device, or in the WPS section of the client's configuration interface (see the device's User's Guide for how to find the WPS PIN - for the CellPipe 7130 RG, see [Section 7.6 on page 153](#)).
- 4 Enter the client's PIN in the AP's configuration interface.

Note: If the client device's configuration interface has an area for entering another device's PIN, you can either enter the client's PIN in the AP, or enter the AP's PIN in the client - it does not matter which.

- 5 Start WPS on both devices within two minutes.

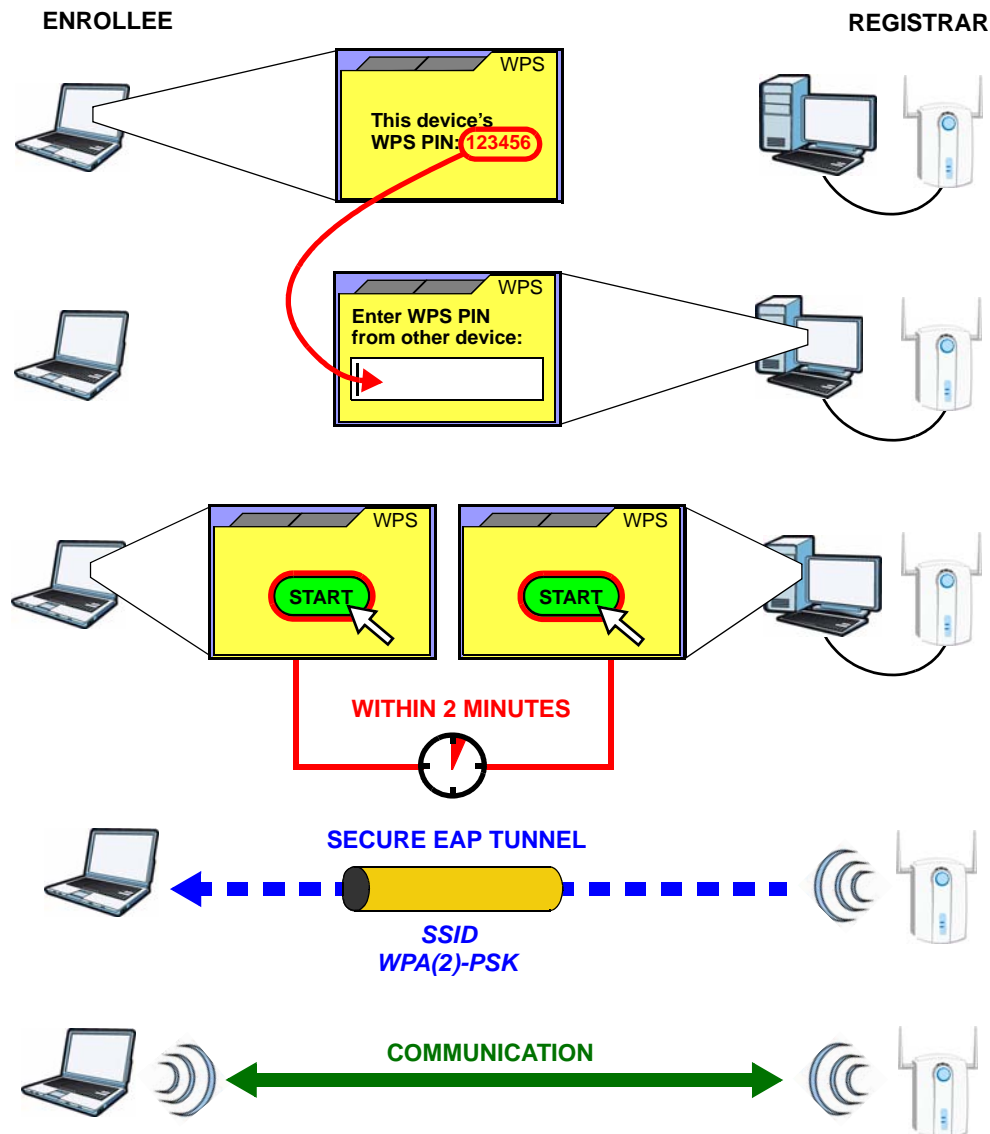
Note: Use the configuration utility to activate WPS, not the push-button on the device itself.

- 6 On a computer connected to the wireless client, try to connect to the Internet. If you can connect, WPS was successful.

If you cannot connect, check the list of associated wireless clients in the AP's configuration utility. If you see the wireless client in the list, WPS was successful.

The following figure shows a WPS-enabled wireless client (installed in a notebook computer) connecting to the WPS-enabled AP via the PIN method.

Figure 53 Example WPS Process: PIN Method

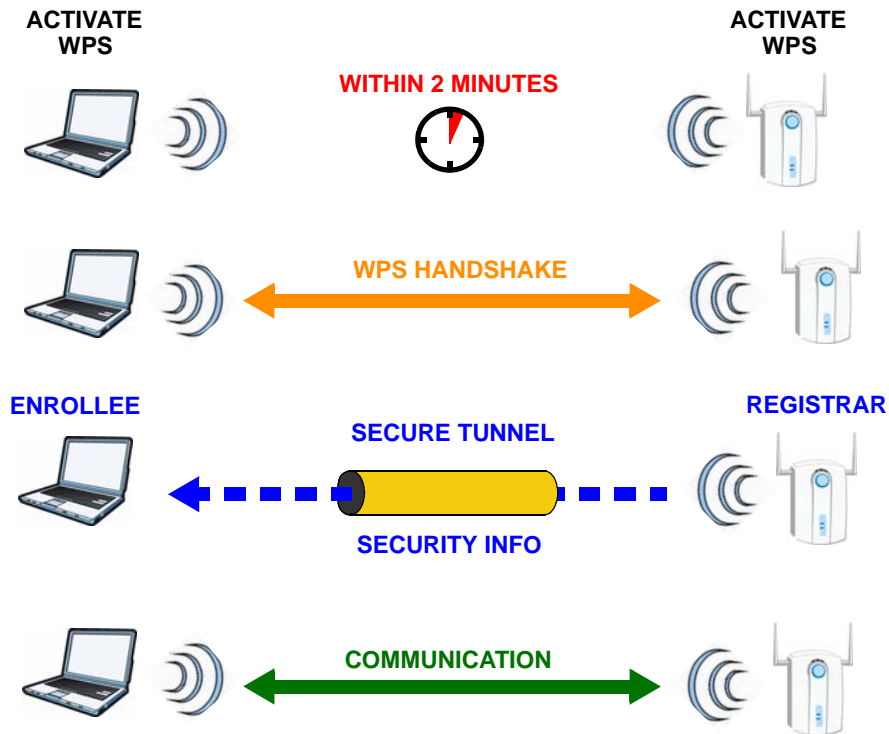


7.10.4.3 How WPS Works

When two WPS-enabled devices connect, each device must assume a specific role. One device acts as the registrar (the device that supplies network and security settings) and the other device acts as the enrollee (the device that receives network and security settings). The registrar creates a secure EAP (Extensible Authentication Protocol) tunnel and sends the network name (SSID) and the WPA-PSK or WPA2-PSK pre-shared key to the enrollee. Whether WPA-PSK or WPA2-PSK is used depends on the standards supported by the devices. If the registrar is already part of a network, it sends the existing information. If not, it generates the SSID and WPA(2)-PSK randomly.

The following figure shows a WPS-enabled client (installed in a notebook computer) connecting to a WPS-enabled access point.

Figure 54 How WPS works



The roles of registrar and enrollee last only as long as the WPS setup process is active (two minutes). The next time you use WPS, a different device can be the registrar if necessary.

The WPS connection process is like a handshake; only two devices participate in each WPS transaction. If you want to add more devices you should repeat the process with one of the existing networked devices and the new device.

Note that the access point (AP) is not always the registrar, and the wireless client is not always the enrollee. All WPS-certified APs can be a registrar, and so can some WPS-enabled wireless clients.

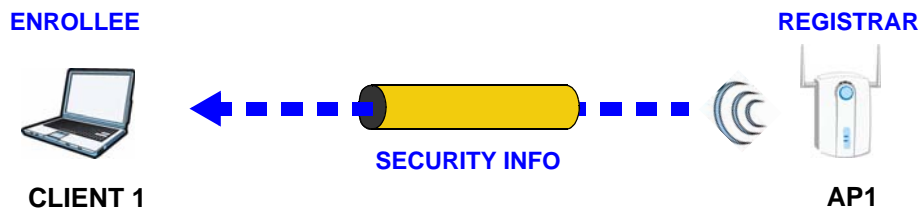
By default, a WPS device is “unconfigured”. This means that it is not part of an existing network and can act as either enrollee or registrar (if it supports both functions). If the registrar is unconfigured, the security settings it transmits to the enrollee are randomly-generated. Once a WPS-enabled device has connected to another device using WPS, it becomes “configured”. A configured wireless client can still act as enrollee or registrar in subsequent WPS connections, but a configured access point can no longer act as enrollee. It will be the registrar in all subsequent WPS connections in which it is involved. If you want a configured AP to act as an enrollee, you must reset it to its factory defaults.

7.10.4.4 Example WPS Network Setup

This section shows how security settings are distributed in an example WPS setup.

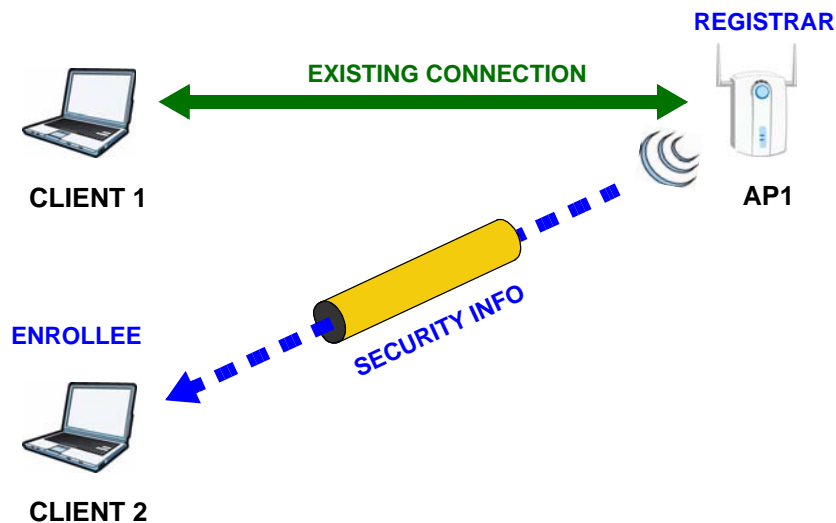
The following figure shows an example network. In step **1**, both **AP1** and **Client 1** are unconfigured. When WPS is activated on both, they perform the handshake. In this example, **AP1** is the registrar, and **Client 1** is the enrollee. The registrar randomly generates the security information to set up the network, since it is unconfigured and has no existing information.

Figure 55 WPS: Example Network Step 1



In step **2**, you add another wireless client to the network. You know that **Client 1** supports registrar mode, but it is better to use **AP1** for the WPS handshake with the new client since you must connect to the access point anyway in order to use the network. In this case, **AP1** must be the registrar, since it is configured (it already has security information for the network). **AP1** supplies the existing security information to **Client 2**.

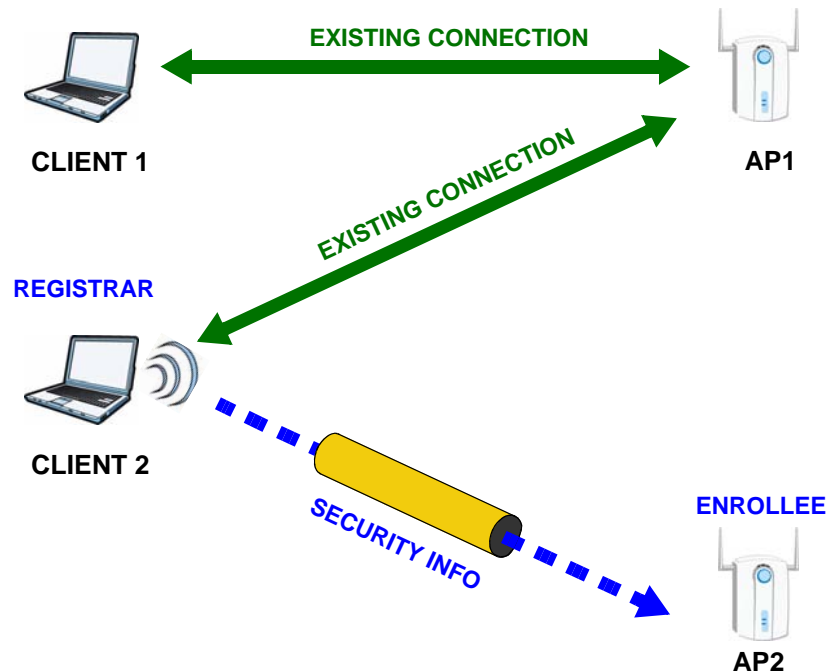
Figure 56 WPS: Example Network Step 2



In step **3**, you add another access point (**AP2**) to your network. **AP2** is out of range of **AP1**, so you cannot use **AP1** for the WPS handshake with the new access

point. However, you know that **Client 2** supports the registrar function, so you use it to perform the WPS handshake instead.

Figure 57 WPS: Example Network Step 3



7.10.4.5 Limitations of WPS

WPS has some limitations of which you should be aware.

- WPS works in Infrastructure networks only (where an AP and a wireless client communicate). It does not work in Ad-Hoc networks (where there is no AP).
- When you use WPS, it works between two devices only. You cannot enroll multiple devices simultaneously, you must enroll one after the other.

For instance, if you have two enrollees and one registrar you must set up the first enrollee (by pressing the WPS button on the registrar and the first enrollee, for example), then check that it successfully enrolled, then set up the second device in the same way.

- WPS works only with other WPS-enabled devices. However, you can still add non-WPS devices to a network you already set up using WPS.

WPS works by automatically issuing a randomly-generated WPA-PSK or WPA2-PSK pre-shared key from the registrar device to the enrollee devices. Whether the network uses WPA-PSK or WPA2-PSK depends on the device. You can check the configuration interface of the registrar device to discover the key the network is using (if the device supports this feature). Then, you can enter the key into the non-WPS device and join the network as normal (the non-WPS device must also support WPA-PSK or WPA2-PSK).

- When you use the PBC method, there is a short period (from the moment you press the button on one device to the moment you press the button on the other device) when any WPS-enabled device could join the network. This is because the registrar has no way of identifying the “correct” enrollee, and cannot differentiate between your enrollee and a rogue device. This is a possible way for a hacker to gain access to a network.

You can easily check to see if this has happened. WPS works between only two devices simultaneously, so if another device has enrolled your device will be unable to enroll, and will not have access to the network. If this happens, open the access point’s configuration interface and look at the list of associated clients (usually displayed by MAC address). It does not matter if the access point is the WPS registrar, the enrollee, or was not involved in the WPS handshake; a rogue device must still associate with the access point to gain access to the network. Check the MAC addresses of your wireless clients (usually printed on a label on the bottom of the device). If there is an unknown MAC address you can remove it or reset the AP.

Network Address Translation (NAT)

8.1 Overview

This chapter discusses how to configure NAT on the CellPipe 7130 RG.

Network Address Translation (NAT, RFC 1631) is the translation of the IP address of a host in a packet, for example, the source address of an outgoing packet, used within one network to a different IP address known within another network.

8.1.1 What You Can Do in this Chapter

- The **Port Forwarding** screen lets you configure forward incoming service requests to the server(s) on your local network ([Section 8.3 on page 172](#)).
- The **DMZ Host** screen lets you configure a default server ([Section 8.4 on page 176](#)).
- The **ALG** screen lets you enable SIP ALG on the CellPipe 7130 RG ([Section 8.5 on page 177](#)).

8.2 What You Need to Know

The following terms and concepts may help as you read through this chapter.

NAT

In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host.

Port Forwarding

A port forwarding set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make visible to the outside world even though NAT makes your whole inside network appear as a single computer to the outside world.

8.3 The Port Forwarding Screen

This summary screen provides a summary of all port forwarding rules and their configuration. In addition, this screen allows you to create new port forwarding rules and delete existing rules.

You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers. You can allocate a server IP address that corresponds to a port or a range of ports.

Note: Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP.

To access this screen, click **Network > NAT**. The following screen appears.

Figure 58 NAT Port Forwarding

Port Forwarding **DMZ Host** **ALG**

Port Forwarding

Service Name	WAN Interface	Server IP Address	External port		Internal port		Protocol	Time(24H)						
www	poe_0_0_33/atm0	192.168.1.	Start: 80	End: 80	Start: 80	End: 80	TCP	Start: 00:00	Stop: 23:59	Add				
Select Days:	<input type="checkbox"/> SUN		<input type="checkbox"/> MON		<input type="checkbox"/> TUE		<input type="checkbox"/> WED		<input type="checkbox"/> THU		<input type="checkbox"/> FRI		<input type="checkbox"/> SAT	

No.	Active	Service Name	WAN Interface	External Start Port	External End Port	Internal Start Port	Internal End Port	Server IP Address	Start Time	Stop Time	Days	Modify
1	<input checked="" type="checkbox"/>	Web(HTTP)	atm0	80	80	80	80	192.168.1.23	0:0	23:59	Tue	

Apply Cancel

The following table describes the labels in this screen.

Table 43 NAT Port Forwarding

LABEL	DESCRIPTION
Service Name	Select a pre-defined service from the drop-down list box. The pre-defined service port number(s) and protocol will display in the External port , Internal port and Protocol fields. Otherwise, select User Define to open the Rule Setup screen where you can manually enter the port number(s) and select the IP protocol.
WAN Interface	Select the WAN interface through which the service is forwarded. You must have already configured a WAN connection with NAT enabled.
Server IP Address	Enter the IP address of the server for the specified service.
External Port Start	Enter the original destination port for the packets. To forward only one port, enter the port number again in the External Port End field. To forward a series of ports, enter the start port number here and the end port number in the External Port End field.
External Port End	Enter the last port of the original destination port range. To forward only one port, enter the port number in the External Port Start field above and then enter it again in this field. To forward a series of ports, enter the last port number in a series that begins with the port number in the External Port Start field above.
Internal Port Start	Enter the port number to which you want the CellPipe 7130 RG to translate the incoming port. To forward only one port, enter the port number again in the Internal Port End field. For a range of ports, enter the first number of the range to which you want the incoming ports translated.
Internal Port End	Enter the last port of the translated port range.
Protocol	This is the transport layer protocol used for the service.
Time Start (24H)	Specify the hour and minute when the port forwarding schedule begins. Hour - 0 - 23 Minute - 0 - 59 The time is in 24-hour format, for example 15:00 is 3:00 PM.
Time Stop (24H)	Specify the hour and minute when the port forwarding schedule stops. Hour - 0 - 23 Minute - 0 - 59 The time is in 24-hour format, for example 15:00 is 3:00 PM.
Select Days	Select each day of the week the recurring schedule is effective.
Add	Click this button to add a rule to the table below.

Table 43 NAT Port Forwarding (continued)

LABEL	DESCRIPTION
No.	This is the rule index number (read-only).
Active	This field indicates whether the rule is active or not. Clear the check box to disable the rule. Select the check box to enable it.
Service Name	This field displays the name of the service used by the packets for this virtual server.
WAN Interface	This field displays the WAN interface through which the service is forwarded.
External Start Port	This is the first external port number that identifies a service.
External End Port	This is the last external port number that identifies a service.
Internal Start Port	This is the first internal port number that identifies a service.
Internal End Port	This is the last internal port number that identifies a service.
Server IP Address	This field displays the inside IP address of the server.
Time Start (24H)	This displays the time at which the port forwarding schedule begins.
Time Stop (24H)	This displays the time at which the port forwarding schedule ends.
Days	This displays the day(s) of the week the recurring schedule is effective.
Modify	Click the Edit icon to go to the screen where you can edit the port forwarding rule. Click the Remove icon to delete an existing port forwarding rule. Note that subsequent rules move up by one when you take this action.
Apply	Click Apply to save your changes back to the CellPipe 7130 RG.
Cancel	Click Cancel to return to the previous configuration.

8.3.1 The Port Forwarding Edit Screen

This screen lets you create or edit a port forwarding rule. Select **User Define** in the **Service Name** field or click the rule's **Edit** icon in the **Port Forwarding** screen to open the following screen.

Figure 59 Port Forwarding Edit

The following table describes the labels in this screen.

Table 44 Port Forwarding Edit

LABEL	DESCRIPTION
Active	Clear the check box to disable the rule. Select the check box to enable it. This field is not editable if you are configuring a User Define rule.
Service Name	Enter a name to identify this rule. This field is read-only if you click the Edit icon in the Port Forwarding screen.
WAN Interface	Select a WAN interface for which you want to configure port forwarding rules.
External Start Port	Enter the original destination port for the packets. To forward only one port, enter the port number again in the External End Port field. To forward a series of ports, enter the start port number here and the end port number in the External End Port field.
External End Port	Enter the last port of the original destination port range. To forward only one port, enter the port number in the External Start Port field above and then enter it again in this field. To forward a series of ports, enter the last port number in a series that begins with the port number in the External Start Port field above.
Internal Start Port	Enter the port number here to which you want the CellPipe 7130 RG to translate the incoming port. For a range of ports, enter the first number of the range to which you want the incoming ports translated.

Table 44 Port Forwarding Edit (continued)

LABEL	DESCRIPTION
Internal End Port	Enter the last port of the translated port range.
Server IP Address	Enter the inside IP address of the virtual server here.
Protocol	Select the transport layer protocol supported by this virtual server. Choices are TCP , UDP , or TCP/UDP .
Time Start (24H)	Specify the hour and minute when the port forwarding schedule begins. Hour - 0 - 23 Minute - 0 - 59 The time is in 24-hour format, for example 15:00 is 3:00 PM.
Time Stop (24H)	Specify the hour and minute when the port forwarding schedule stops. Hour - 0 - 23 Minute - 0 - 59 The time is in 24-hour format, for example 15:00 is 3:00 PM.
Select Days	Select each day of the week the recurring schedule is effective.
Back	Click Back to return to the previous screen.
Apply	Click Apply to save your changes back to the CellPipe 7130 RG.
Cancel	Click Cancel to begin configuring this screen afresh.

8.4 The DMZ Host Screen

In addition to the servers for specified services, NAT supports a default server IP address. A default server receives packets from ports that are not specified in the **NAT Port Forwarding Setup** screen.

Figure 60 NAT > DMZ Host

The screenshot shows the 'DMZ Host' configuration screen. At the top, there are three tabs: 'Port Forwarding', 'DMZ Host', and 'ALG'. The 'DMZ Host' tab is selected. Below the tabs, the text 'DMZ Host' is displayed. Underneath, there is a 'Default Server' label followed by a text input field containing the IP address '192.168.1.'. Below the input field is a yellow note icon followed by the text: 'Note : Enter IP address and click "Apply" to activate the DMZ host. Clear the IP address field and click "Apply" to deactivate the DMZ host.' At the bottom right of the screen, there is a button labeled 'Apply'.

The following table describes the fields in this screen.

Table 45 NAT > DMZ Host

LABEL	DESCRIPTION
Default Server	Enter the IP address of the default server which receives packets from ports that are not specified in the NAT Port Forwarding screen. Note: If you do not assign a Default Server , the CellPipe 7130 RG discards all packets received for ports that are not specified in the NAT Port Forwarding screen.
Apply	Click Apply to save your changes back to the CellPipe 7130 RG.

8.5 The ALG Screen

Some NAT routers may include a SIP Application Layer Gateway (ALG). A SIP ALG allows SIP calls to pass through NAT by examining and translating IP addresses embedded in the data stream. The SIP ALG translates the CellPipe 7130 RG's private IP address inside the SIP data stream to a public IP address. You do not need to use STUN or an outbound proxy if you enable the SIP ALG.

Use this screen to enable or disable the SIP ALG in the CellPipe 7130 RG. To access this screen, click **NAT > ALG**.

Figure 61 NAT > ALG



Each field is described in the following table.

Table 46 NAT > ALG

LABEL	DESCRIPTION
Active SIP ALG	Select this check box to allow SIP sessions to pass through the CellPipe 7130 RG. SIP is a signaling protocol used in sending of voice signals over Internet Protocol.
Apply	Click Apply to save your customized settings.

Wait for the CellPipe 7130 RG to fully reboot before accessing it again.

8.6 Technical Reference

The following section contains additional technical information about the CellPipe 7130 RG features described in this chapter.

Port Forwarding: Services and Port Numbers

The most often used port numbers are shown in the following table. Please refer to RFC 1700 for further information about port numbers. Please also refer to the Supporting CD for more examples and details on port forwarding and NAT.

Table 47 Services and Port Numbers

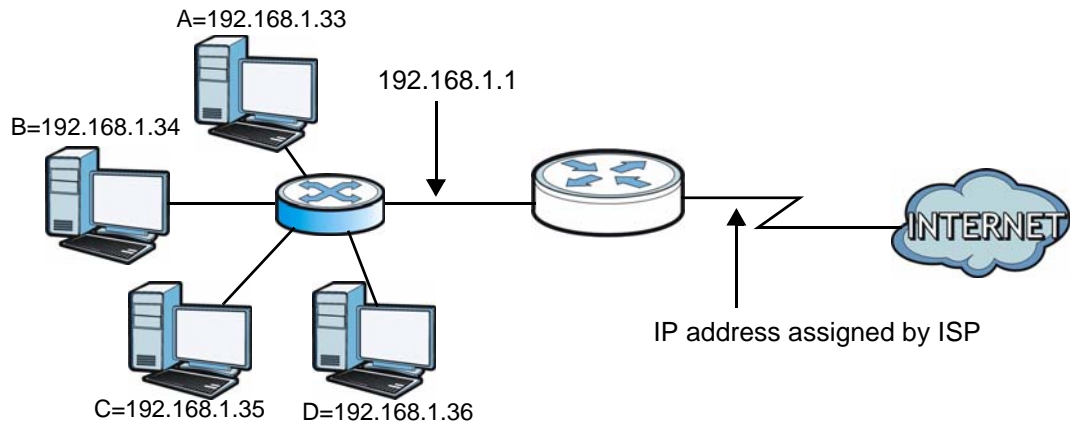
SERVICES	PORT NUMBER
ECHO	7
FTP (File Transfer Protocol)	21
SMTP (Simple Mail Transfer Protocol)	25
DNS (Domain Name System)	53
Finger	79
HTTP (Hyper Text Transfer protocol or WWW, Web)	80
POP3 (Post Office Protocol)	110
NNTP (Network News Transport Protocol)	119
SNMP (Simple Network Management Protocol)	161
SNMP trap	162
PPTP (Point-to-Point Tunneling Protocol)	1723

Port Forwarding Example

Let's say you want to assign ports 21-25 to one FTP, Telnet and SMTP server (**A** in the example), port 80 to another (**B** in the example) and assign a default server IP address of 192.168.1.35 to a third (**C** in the example). You assign the LAN IP

addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

Figure 62 Multiple Servers Behind NAT Example



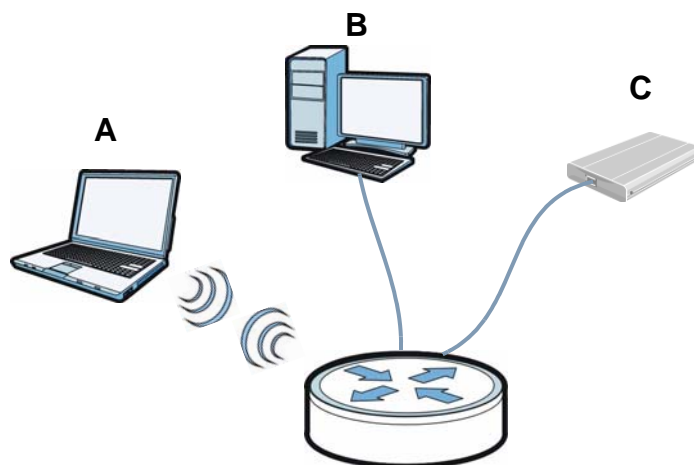
File Sharing

9.1 Overview

Share files on a USB memory stick or hard drive connected to your CellPipe 7130 RG with users on your network.

The following figure is an overview of the CellPipe 7130 RG's file server feature. Computers **A** and **B** can access files on a USB device (**C**) which is connected to the CellPipe 7130 RG.

Figure 63 File Sharing Overview



- See [Section 9.1.2 on page 182](#) for an explanation of file-sharing terms.
- See [Section 9.2.1 on page 184](#) for file-sharing examples.

9.1.1 What You Can Do in this chapter

Use the **File Sharing** screen ([Section 9.2 on page 183](#)) to enable file-sharing server on the CellPipe 7130 RG and configure the workgroup name.

9.1.2 What You Need to Know About File-Sharing

Workgroup name

This is the name given to a set of computers that are connected on a network and share resources such as a printer or files. Windows automatically assigns the workgroup name when you set up a network.

Shares

When settings are set to default, each USB device connected to the CellPipe 7130 RG is given a folder, called a "share". If a USB hard drive connected to the CellPipe 7130 RG has more than one partition, then each partition will be allocated a share. You can also configure a "share" to be a sub-folder or file on the USB device.

File Systems

A file system is a way of storing and organizing files on your hard drive and storage device. Often different operating systems such as Windows or Linux have different file systems. The file-sharing feature on your CellPipe 7130 RG supports File Allocation Table (FAT) and FAT32 file systems.

Windows/CIFS

Common Internet File System (CIFS) is a standard protocol supported by most operating systems in order to share files across the network.

CIFS runs over TCP/IP but uses the SMB (Server Message Block) protocol found in Microsoft Windows for file and printer access; therefore, CIFS will allow all applications, not just Web browsers, to open and share files across the Internet.

The CellPipe 7130 RG uses Common Internet File System (CIFS) protocol for its file sharing functions. CIFS compatible computers can access the USB file storage devices connected to the CellPipe 7130 RG. CIFS protocol is supported on Microsoft Windows, Linux Samba and other operating systems (refer to your systems specifications for CIFS compatibility).

NFS

Network File System (NFS) is a protocol most commonly used on Unix-like systems in order to share files across the network.

Samba

SMB is a client-server protocol used by Microsoft Windows systems for sharing files, printers, and so on.

Samba is a free SMB server that runs on most Unix and Unix-like systems. It provides an implementation of an SMB client and server for use with non-Microsoft operating systems.

File Transfer Protocol

This is a method of transferring data from one computer to another over a network such as the Internet.

9.1.3 Before You Begin

Make sure the CellPipe 7130 RG is connected to your network and turned on.

- 1 Connect the USB device to one of the CellPipe 7130 RG's USB ports. Make sure the CellPipe 7130 RG is connected to your network.
- 2 The CellPipe 7130 RG detects the USB device and makes its contents available for browsing. If you are connecting a USB hard drive that comes with an external power supply, make sure it is connected to an appropriate power source that is on.

Note: If your USB device cannot be detected by CellPipe 7130 RG, see the troubleshooting for suggestions.

9.2 The Server Settings Screen

Use this screen to set up file sharing via the CellPipe 7130 RG. To access this screen, click **USB Services > File Sharing**.

Figure 64 USB Services > File Sharing

The screenshot shows a 'Share Configuration' dialog box. The title bar reads 'Share Configuration'. Below the title bar, the section 'File Sharing' is visible. It contains a checked checkbox labeled 'Enable File Sharing Services (SAMBAs)'. Underneath, the 'Server Configuration' section lists 'Host Name' as '5Vz.A2011' and 'Workgroup Name' as 'WORKGROUP'. A yellow note icon is followed by the text: 'Please do not remove the USB Hard Disk when the USB Hard Disk is busy.' At the bottom of the dialog, there are two buttons: 'Apply/Save' and 'Cancel'.

Each field is described in the following table.

Table 48 USB Services > File Sharing

LABEL	DESCRIPTION
Enable File Sharing Services	Select this to enable file sharing through the CellPipe 7130 RG.
Server Configuration	
Host Name	This displays the CellPipe 7130 RG system name.
Workgroup Name	<p>You can add the CellPipe 7130 RG to an existing or a new workgroup on your network. Enter the name of the workgroup which your CellPipe 7130 RG automatically joins.</p> <p>You can set the CellPipe 7130 RG's workgroup name to be exactly the same as the workgroup name to which your computer belongs to.</p> <p>Note: The CellPipe 7130 RG will not be able to join the workgroup if your local area network has restrictions set up that do not allow devices to join a workgroup. In this case, contact your network administrator.</p>
Apply/Save	Click this to save your changes to the CellPipe 7130 RG.
Reset	Click this to set every field in this screen to its last-saved value.

9.2.1 Example of Accessing Your Shared Files From a Computer

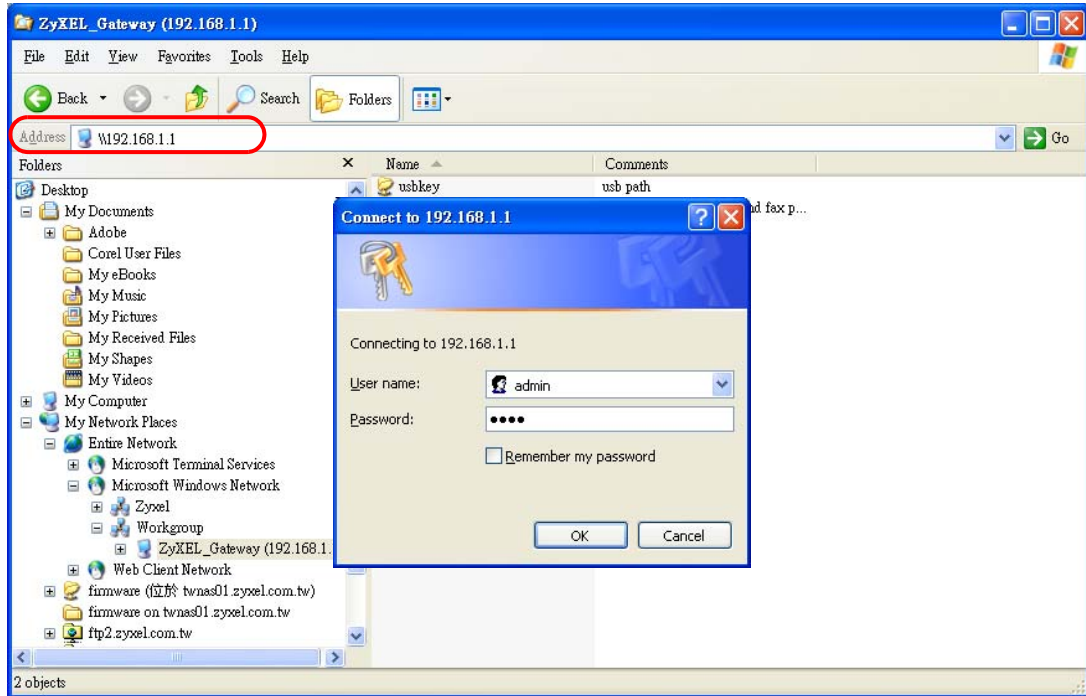
You can use Windows Explorer to access the file storage devices connected to the CellPipe 7130 RG.

Note: The example in this User's Guide shows you how to use Microsoft's Windows XP to browse your shared files. Refer to your operating system's documentation for how to browse your file structure.

- 1 Open Windows Explorer to share files in the attached USB device using Windows Explorer browser.

- 2 In Windows Explorer's Address bar type a double backslash "\\ " followed by the IP address of the CellPipe 7130 RG (the default IP address of the CellPipe 7130 RG is 192.168.1.1) and press [ENTER]. A screen asking for password authentication appears. Type the user name and password you use to access the system and click **OK**. (The default system user name is **admin** and the default system password is **telus**.)

Figure 65 File Sharing via Windows Explorer



Note: Once you log in to the file share via your CellPipe 7130 RG, you do not have to log in again unless you restart your computer.

Note: Refer to [Section 3.2 on page 83](#) for user level information. Each user level has its own account information for logging into the CellPipe 7130 RG.

Media Server

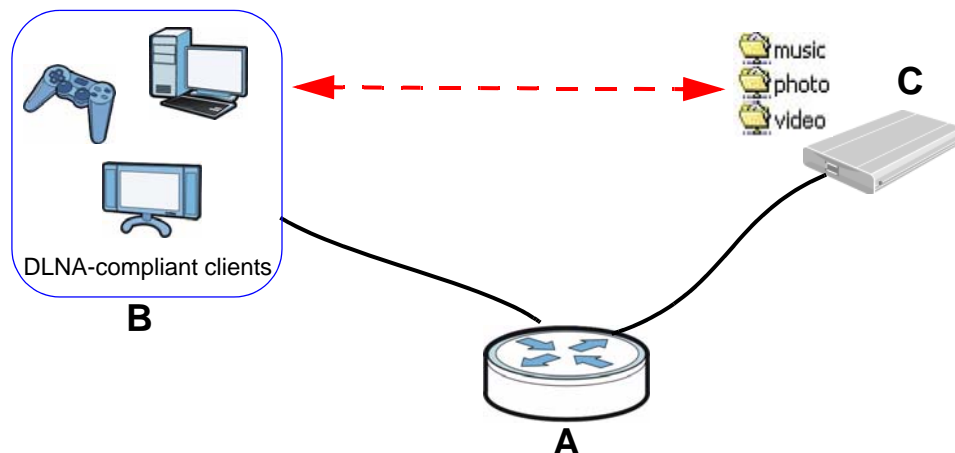
10.1 Overview

The media server feature lets anyone on your network play video, music, and photos from a USB storage device connected to your CellPipe 7130 RG (without having to copy them to another computer). The CellPipe 7130 RG can function as a DLNA-compliant media server. The CellPipe 7130 RG streams files to DLNA-compliant media clients, such as the Xbox 360, Playstation 3 and so on.

The Digital Living Network Alliance (DLNA) is a group of personal computer and electronics companies that works to make products compatible in a home network.

In the following figure, DLNA-compliant devices (**B**) can play music and video files or view images stored on a USB device (**C**) that is connected to the CellPipe 7130 RG (**A**).

Figure 66 File Sharing Overview



Refer to [Section 2.6 on page 65](#) for a tutorial on using this feature on Windows 7 and a Digital Media Adapter.

10.1.1 What You Can Do in this chapter

- Use the **Media Server Configuration** screen (Section 10.3 on page 189) to enable the media server on the CellPipe 7130 RG.
- Use the **Remove Disk Safely** screen (Section 10.3 on page 189) to safely disconnect the USB device from the CellPipe 7130 RG.

10.1.2 Before You Begin

Make sure the CellPipe 7130 RG is connected to your network and turned on.

- 1 Connect the USB device to one of the CellPipe 7130 RG's USB ports. Make sure the CellPipe 7130 RG is connected to your network.
- 2 The CellPipe 7130 RG detects the USB device and makes its contents available for browsing. If you are connecting a USB hard drive that comes with an external power supply, make sure it is connected to an appropriate power source that is on.

Note: If your USB device cannot be detected by CellPipe 7130 RG, see the troubleshooting for suggestions.

10.2 The Media Server Configuration Screen

Use this screen to enable the media server on your CellPipe 7130 RG. To access this screen, click **USB Services > Media Server**.

Figure 67 USB Services > Media Server



Each field is described in the following table.

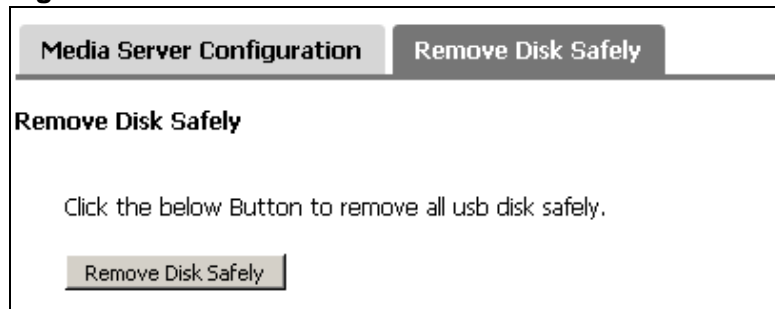
Table 49 USB Services > Media Server

LABEL	DESCRIPTION
Enable Media Server (DLNA)	Select this to turn on the media server and let (DLNA-compliant) media clients on your network play media files located in the published shares.
Apply/Save	Click this to save your changes to the CellPipe 7130 RG.
Cancel	Click this to set every field in this screen to its last-saved value.

10.3 The Remove Disk Safely Screen

Use this screen to safely remove the USB device from the CellPipe 7130 RG. This stops processes to the USB device and prevents your data from being corrupted. To access this screen, click **USB Services > Media Server > Remove Disk Safely**.

Figure 68 USB Services > Media Server > Remove Disk Safely



Each field is described in the following table.

Table 50 USB Services > Media Server > Remove Disk Safely

LABEL	DESCRIPTION
Remove Disk Safely	Click this stop all processes to the USB device. You can then disconnect the USB device safely.

Firewall

11.1 Overview

This chapter shows you how to enable and configure the CellPipe 7130 RG firewall settings.

The CellPipe 7130 RG firewall is a packet filtering firewall and restricts access based on the source/destination computer network address of a packet and the type of application.

11.1.1 What You Can Do in this Chapter

- The **Incoming** screen lets you view and configure incoming IP filtering rules ([Section 11.4 on page 195](#)).
- The **DoS** screen lets you activate protection against Denial of Service (DoS) attacks ([Section 11.4 on page 195](#)).

11.2 What You Need to Know

The following terms and concepts may help as you read through this chapter.

Basics

Computers share information over the Internet using a common language called TCP/IP. TCP/IP, in turn, is a set of application protocols that perform specific functions. An "extension number", called the "TCP port" or "UDP port" identifies these protocols, such as HTTP (Web), FTP (File Transfer Protocol), POP3 (E-mail), etc. For example, Web traffic by default uses TCP port 80.

When computers communicate on the Internet, they are using the client/server model, where the server "listens" on a specific TCP/UDP port for information requests from remote client computers on the network. For example, a Web server typically listens on port 80. Please note that while a computer may be intended for use over a single port, such as Web on port 80, other ports are also

active. If the person configuring or managing the computer is not careful, a hacker could attack it over an unprotected port.

Some of the most common IP ports are:

Table 51 Common IP Ports

21	FTP	53	DNS
23	Telnet	80	HTTP
25	SMTP	110	POP3

Default Filtering Policies

Filtering rules are grouped based on the direction of travel of packets to which they apply.

The default rule for incoming traffic blocks all incoming connections from the WAN to the LAN. If you wish to allow certain WAN users to have access to your LAN, you will need to create custom rules to allow it.

Note: If you configure filtering rules without a good understanding of how they work, you might inadvertently introduce security risks to the firewall and to the protected network. Make sure you test your rules after you configure them.

These custom rules work by comparing the Source IP address, Destination IP address and IP protocol type of network traffic to rules set by the administrator. Your customized rules take precedence and override the CellPipe 7130 RG's default rules.

Denial of Service (DoS)

Denial of Service (DoS) prevents customers, users, clients or other computers from accessing data on a computer. This is usually accomplished by interrupting or overwhelming the computer with bad or excessive information requests.

11.3 The Firewall Screen

Click **Security > Firewall > Incoming** to display the following screen. This screen displays a list of the configured incoming filtering rules.

Figure 69 Firewall > Incoming

The following table describes the labels in this screen.

Table 52 Firewall > Incoming

LABEL	DESCRIPTION
Active Firewall	Select this check box to enable the firewall on the CellPipe 7130 RG. When the firewall is enabled, the CellPipe 7130 RG blocks all incoming traffic from the WAN to the LAN. Create custom rules below to allow certain WAN users to access your LAN or to allow traffic from the WAN to a certain computer on the LAN.
Active	Select this check box to enable the rule.
Filter Name	This displays the name of the rule.
Interfaces	This displays the WAN interface(s) to which this rule is applied.
Protocol	This displays the transport layer protocol that defines the service to which this rule applies.
Source Address / Mask	This displays the source IP addresses and subnet mask to which this rule applies. Please note that a blank source address is equivalent to Any .
Source Port	This is the source port number.
Dest. Address / Mask	This displays the destination IP addresses and subnet mask to which this rule applies. Please note that a blank destination address is equivalent to Any .
Dest. Port	This is the destination port number.
Start. Time	This displays the time at which the firewall schedule begins.
Stop. Time	This displays the time at which the firewall schedule ends.
Week. Days	This displays the day(s) of the week the firewall schedule is effective.
Modify	Click the Edit icon to go to the screen where you can edit the rule. Click the Remove icon to delete an existing rule. Note that subsequent rules move up by one when you take this action.

Table 52 Firewall > Incoming (continued)

LABEL	DESCRIPTION
Add	Click Add to create a new rule.
Apply	Click Apply to save your changes back to the CellPipe 7130 RG.

11.3.1 Creating Incoming Firewall Rules

In the **Incoming** screen, click **Add** to display this screen and refer to the following table for information on the labels.

Figure 70 Firewall > Incoming: Add

Add Firewall ACL rule -- Incoming

The screen allows you to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition below. All of the conditions in this filter rule must be satisfied for the rule to take effect. Click 'Apply/Save' to save and activate the filter.

Active

Filter Name:

Protocol:

Source IP address:

Source Subnet Mask:

Source Port (port or port:port):

Destination IP address:

Destination Subnet Mask:

Destination Port (port or port:port):

Start Time (HH:MM 24H format):

Stop Time (HH:MM 24H format):

Select Days: SUN MON TUE WED THU FRI SAT

Interface: Select All ipoe_0_0_33/atm0 ipoe_0_0_1_1/ptm0_1 ipoe_eth4_1/eth4_1

The following table describes the labels in this screen.

Table 53 Firewall > Incoming: Add

LABEL	DESCRIPTION
Active	Select this check box to enable the rule.
Filter Name	Enter a descriptive name of up to 16 printable English keyboard characters, including spaces. To add a firewall rule, you need to configure at least one of the following fields (except the Interface field).
Protocol	Select the transport layer protocol (TCP/UDP , TCP , UDP or ICMP) and enter the protocol (service type) number in the port field. Select NONE to apply the rule to any protocol.
Source IP Address	Enter the source IP address in dotted decimal notation.
Source Subnet Mask	Enter the source subnet mask.

Table 53 Firewall > Incoming: Add (continued)

LABEL	DESCRIPTION
Source Port	Enter a single port number or the range of port numbers of the source.
Destination IP Address	Enter the destination IP address in dotted decimal notation.
Destination Subnet Mask	Enter the destination subnet mask.
Destination Port	Enter the port number of the destination.
Start Time	Specify the hour and minute when the firewall schedule begins. Hour - 0 - 23 Minute - 0 - 59 The time is in 24-hour format, for example 15:00 is 3:00 PM.
Stop Time	Specify the hour and minute when the firewall schedule stops. Hour - 0 - 23 Minute - 0 - 59 The time is in 24-hour format, for example 15:00 is 3:00 PM.
Select Days	Select each day of the week the firewall schedule is effective.
Interface	Select Select All to apply the rule to all interfaces on the CellPipe 7130 RG or select the specific WAN interface(s) to which this rule applies.
Back	Click Back to return to the previous screen.
Apply	Click Apply to save your customized settings and exit this screen.

11.4 The DoS Screen

Click **Security > Firewall > DoS** to display the following screen. This lets you turn on protection against DoS attacks.

Figure 71 Security > Firewall > DoS

The screenshot shows a web-based configuration interface. At the top, there are two tabs: 'Incoming' and 'DoS'. The 'DoS' tab is active. Below the tabs, the text 'DoS' is displayed. Underneath, there is a checkbox labeled 'Active DoS' which is currently unchecked. At the bottom of the screen, there is an 'Apply' button.

The following table describes the labels in this screen.

Table 54 Security > Firewall > DoS

LABEL	DESCRIPTION
Active DoS	Select this check box to detect and reject old or duplicate packets to protect against Denial-of-Service attacks
Apply	Click Apply to save your changes back to the CellPipe 7130 RG.

Certificate

12.1 Overview

The CellPipe 7130 RG can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. A certificate contains the certificate owner's identity and public key. Certificates provide a way to exchange public keys for use in authentication.

12.1.1 What You Can Do in this Chapter

- The **Local Certificates** screen lets you generate certification requests and import the CellPipe 7130 RG's CA-signed certificates ([Section 12.4 on page 204](#)).
- The **Trusted CA** screen lets you save the certificates of trusted CAs to the CellPipe 7130 RG ([Section 12.4 on page 204](#)).

12.2 What You Need to Know

The following terms and concepts may help as you read through this chapter.

Certification Authority

A Certification Authority (CA) issues certificates and guarantees the identity of each certificate owner. There are commercial certification authorities like CyberTrust or VeriSign and government certification authorities. The certification authority uses its private key to sign certificates. Anyone can then use the certification authority's public key to verify the certificates. You can use the CellPipe 7130 RG to generate certification requests that contain identifying information and public keys and then send the certification requests to a certification authority.

12.3 The Local Certificates Screen

Click **Security > Certificates** to open the **Local Certificates** screen. This is the CellPipe 7130 RG's summary list of certificates and certification requests.

Figure 72 Local Certificates

Name	In Use	Subject	Type	Action
Testthis		CN=Sample1/O=Ex/ST=OK/C=US	request	<input type="button" value="View"/> <input type="button" value="Load Signed"/> <input type="button" value="Remove"/>

The following table describes the labels in this screen.

Table 55 Local Certificates

LABEL	DESCRIPTION
Name	This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name.
In Use	This field displays how many applications use the certificate.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Type	<p>This field displays what kind of certificate this is.</p> <p>request represents a certification request and is not yet a valid certificate. Send a certification request to a certification authority, which then issues a certificate. Use the Load Certificate screen to import the certificate and replace the request.</p> <p>signed represents a certificate issued by a certification authority.</p>
Action	<p>Click the View button to open a screen with an in-depth list of information about the certificate (or certification request).</p> <p>Click the Load Signed button to import a valid certification to replace the request.</p> <p>Click the Remove button to delete the certificate (or certification request). You cannot delete a certificate that one or more features is configured to use.</p>

Table 55 Local Certificates (continued)

LABEL	DESCRIPTION
Create Certificate Request	Click this button to go to the screen where you can have the CellPipe 7130 RG generate a certification request.
Import Certificate	Click this button to open a screen where you can save the certificate that you have enrolled from a certification authority from your computer to the CellPipe 7130 RG.

12.3.1 Create Certificate Request

Click **Security > Certificates > Local Certificates** and then **Create Certificate Request** to open the **My Certificate Create** screen. Use this screen to have the CellPipe 7130 RG generate a certification request.

Figure 73 Create Certificate Request

Create new certificate request

To generate a certificate signing request you need to include Common Name, Organization Name, State/Province Name, and the 2-letter Country Code for the certificate.

Certificate Name:

Common Name:

Organization Name:

State/Province Name:

Country/Region Name:

The following table describes the labels in this screen.

Table 56 Create Certificate Request

LABEL	DESCRIPTION
Certificate Name	Type up to 31 ASCII characters (not including spaces) to identify this certificate.
Common Name	Select a radio button to identify the certificate's owner by IP address, domain name or e-mail address. Type the IP address (in dotted decimal notation), domain name or e-mail address in the field provided. The domain name or e-mail address can be up to 31 ASCII characters. The domain name or e-mail address is for identification purposes only and can be any string.
Organization Name	Type up to 127 characters to identify the company or group to which the certificate owner belongs. You may use any character, including spaces, but the CellPipe 7130 RG drops trailing spaces.
State/Province Name	Type up to 127 characters to identify the state or province where the certificate owner is located. You may use any character, including spaces, but the CellPipe 7130 RG drops trailing spaces.
Country/Region Name	Select a country to identify the nation where the certificate owner is located.

Table 56 Create Certificate Request (continued)

LABEL	DESCRIPTION
Back	Click Back to return to the previous screen.
Apply	Click Apply to begin certificate or certification request generation.

After you click **Apply**, the **Certificate Request Details** screen displays. Click **Load Signed Certificate** to import a certificate signed by the CA to replace the request (see [Section 12.3.4 on page 203](#)). Otherwise, click **Back** to return to the **Local Certificates** screen. See [Section 12.3.3 on page 202](#) for field information.

Figure 74 Certificate Request Details

Certificate Request Details

Certificate signing request successfully created. Note a request is not yet functional - have it signed by a Certificate Authority and load the signed certificate to this device.

Name	Test12
Type	request
Subject	CN=Sample2/O=Sample2/ST=OK/C=US
Signing Request	<pre> -----BEGIN CERTIFICATE REQUEST----- MIIBfTCB5wIBADA+MRAwDgYDVQQDEwdTYW1wbGUyMRAwDgYDVQQKEwdTYW1wbGUy MQswCQYDVQQIEwJPSzELMAkGA1UEBhMCVVMwZ8wDQYJKoZIhvcNAQEBBQADgYOA MIGJAoGBAmeUsSJEZr7ILfc6WQUsn9r9fBZZXxjjfRHSSjL269FNyRbZ1VQWc6PP5 mJTft2+/QoiZlpE6yQOvwG525uUhEm1vn&8TwoyPStESzc4KrdEjkdsKrze5r1R6 wth6zxx7dVm17B08tOE1diMRRPq63ouPSYH3UrWigg6tb6hX1Be+1AgMBAAAG&ADAN Egkqhk1G9w0BAQQFAA0BgQAQa4eMHVubPY5kxXRBSWhPOEcyDeixzs1/xqsgKU1z +jqcrg/aJcNKI8Km0USO4Zj6p&6OUC2UuCB/HXbpDtd9qGIvicM8RxfH9cjwOGJmo NiROB8VTUu+sLMvGFUG/I8LV3m+IeFNK3Ec5YoTkeSrnqiE91kN8XVzS1u8Yn2PGw EQ== -----END CERTIFICATE REQUEST----- </pre>

12.3.2 Import Certificate

Click **Security > Certificates > Local Certificates** and then **Import Certificate** to open the **Import Local Certificate** screen. Follow the instructions in this screen to save an existing certificate to the CellPipe 7130 RG.

Note: You must remove any spaces from the certificate's filename before you can import it.

Figure 75 Import Local Certificate

Import Local Certificate

Enter certificate name, paste certificate content and private key

Certificate Name:

Certificate:

```

-----BEGIN CERTIFICATE-----
<insert certificate here>
-----END CERTIFICATE-----

```

Private Key:

```

-----BEGIN RSA PRIVATE KEY-----
<insert private key here>
-----END RSA PRIVATE KEY-----

```

The following table describes the labels in this screen.

Table 57 Import Local Certificate

LABEL	DESCRIPTION
Certificate Name	Type up to 31 ASCII characters (not including spaces) to identify this certificate.
Certificate	Copy and paste the certificate into the text box to store it on the CellPipe 7130 RG.
Private Key	Copy and paste the private key into the text box to store it on the CellPipe 7130 RG.
Back	Click Back to return to the previous screen.
Apply	Click Apply to save the certificate on the CellPipe 7130 RG.

12.3.3 Certificate Details

Click **Security > Certificates > Local Certificates** to open the **My Certificates** screen (see [Figure 72 on page 198](#)). Click the **View** icon to open the **Certificate Details** screen. Use this screen to view in-depth certificate information and change the certificate's name.

Figure 76 Certificate Details

Certificate Details	
Name	Test12
Type	request
Subject	CN=Sample2/O=Sample2/ST=OK/C=US
Certificate	(null)
Private Key	<pre>-----BEGIN RSA PRIVATE KEY----- MIICXAIIBAAKBgQDH1LEiRGa+yC3301kFLJ/a/XwWV8Y43OR0koy9uvRTckW2dVUF nQJz+ZiU37dvvOKImZaROskDr8Budub1IRJtb5wPE8KMjOrRes3OCq3RI5HbCq83 ua6UesLYes8ce3VZteWtVlThJXYjEUT6ut6Lj+WB91K1ooILW+oV9QXvtQIDAQAB AoGAXFu6/RiaU39fhiFCQNq9vyG+4rgLyXHIAsRh1uV5WfkSuNRTR+nzjf+bVImS 4euoZn5s5xhFHaefbX8ocq/7Tkg45u3Zup2dXCC+bNmK+nVtLR8mdphBA/KGdRCT neSCmhGxZfcX9aZFBDPuHdiVpX+EFg68JOV3S2OadqyJcqEQCQDkNLDYmVrhKRbR PtHnqVv8TsK6epdIUh8qOx2ckD5LxRw7neMEVfbSdTHCAHBP6iSxCuYTq8nFXiTF dg9+77p/AkEA3+N+DI49bXk6x0+HT+iIphVbVRR:Z1SdMT9WpQVfItHEWekaykrUb 5626ED6EA3jGCrvnbf+86v7nPRRANnpzywJAJ6k4qvqAGnrHqmoelQKMKBeQJFS2 Ai2zmOVZSiKPkR+avom8ML63/O+9TBhDbMamzFY2kmi10piAD41rPAZyBQJBALhy yx288Y6HGY2qT2fdwvZREfWDMU5YgD6Lv+xtsWUNn18Ob3++BUdRRMdBQDE8Bqx MeDFL/ZiGk+Pp3XjoxECQHw1qONj3m/YtWjOURL659UKYOHISci8ko7z4z9uwoa 72yX+nHHAdQAay8kJAdXOVf4i71Nc6+/hF1UNAc2eMM= -----END RSA PRIVATE KEY-----</pre>
Signing Request	<pre>-----BEGIN CERTIFICATE REQUEST----- MIIBfTCB5wIBAD4+MRAwDgYDVOQDEwdTYW1wbGUyMRAwDgYDVOQKEwdTYW1wbGUy MQswCQYDVQQIEwJPSzELMAkGA1UEBhMCVWwzZ8wDQYJKoZIhvcNAQEBBQADgYOA MIGIAoGBAMEUsSJEZr7ILfc6WQUsn9r9fBZXxjJfRHSSjL269FNyRbZ1VQWc6PP5 mJTft2+/Qo1Z1pE6yQOvwG525uUhm1vnA8TwoyPStESzc4KrdEjKdsKrz5r1R6 wth6zxx7dVn17B08tOE1diMRRPq63ouP5YH3UrWigg7b6hX1Be+1AgMBAAAGADAN BgkqhkiG9wOBAQQAoOBgQAQa4eMHVubPY5kxXRBSWhPOEcyDeixzs1/xqsgKUIz +icrg/aJcNKI8KmOUSO4Zj6pA6OUC2UuCB/HXbpDtd9qGIVicM8RXfH9cjuOGJmo NiROBSVTUu+sLMvGFUG/I81V3m+IfnK3Ec5YoTkeSrnqiE91kN8XVzS1u8Yn2PGw eQ== -----END CERTIFICATE REQUEST-----</pre>

The following table describes the labels in this screen.

Table 58 Certificate Details

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate. If you want to change the name, type up to 31 characters to identify this certificate. You may use any character (not including spaces).
Type	This field displays general information about the certificate. signed means that a Certification Authority signed the certificate. request means this is a certification request.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organization (O), State (ST) and Country (C).
Certificate	This read-only text box displays the certificate in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form. This displays null in a certification request. You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Private Key	This read-only text box displays the private key in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form. You can copy and paste the private key into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Signing Request	This read-only text box displays the request information in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form. This displays null in a signed certificate.
Back	Click Back to return to the previous screen.
Load Signed Certificate	This button is available only in a certification request details screen Click this to import a certificate signed by the CA to replace the request.

12.3.4 Load Signed Certificate

Click **Security > Certificates > Local Certificates** and then **Load Signed** or the **Load Signed Certificate** button in the **Certificate Details** screen of a

certification request to open the **Load Certificate** screen. Follow the instructions in this screen to save a valid certificate to replace the request.

Figure 77 Load Certificate

The following table describes the labels in this screen.

Table 59 Load Certificate

LABEL	DESCRIPTION
Certificate Name	This field is read-only and displays the identifying name of this certificate.
Certificate	Copy and paste the certificate into the text box to store it on the CellPipe 7130 RG.
Back	Click Back to return to the previous screen.
Apply	Click Apply to save the certificate on the CellPipe 7130 RG.

12.4 The Trusted CA Screen

Click **Advanced Setup > Certificates > Trusted CA** to open the following screen. This screen displays a summary list of certificates of the certification authorities that you have set the CellPipe 7130 RG to accept as trusted. The CellPipe 7130 RG accepts any valid certificate signed by a certification authority on

this list as being trustworthy; thus you do not need to import any certificate that is signed by one of these certification authorities.

Figure 78 Trusted CA



The following table describes the fields in this screen.

Table 60 Trusted CA

LABEL	DESCRIPTION
Name	This field displays the name used to identify this certificate.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), OU (Organizational Unit or department), Organization (O), State (ST) and Country (C). It is recommended that each certificate have unique subject information.
Type	This field displays general information about the certificate. ca means that a Certification Authority signed the certificate.
Action	Click View to open a screen with an in-depth list of information about the certificate. Click Remove to delete the certificate.
Import Certificate	Click this button to open a screen where you can save the certificate of a certification authority that you trust to the CellPipe 7130 RG.

12.4.1 View Trusted CA Certificate

Click the **View** button in the **Trusted CA** screen to open the following screen. Use this screen to view in-depth information about the certification authority's certificate.

Figure 79 Trusted CA: View

Security > Certificate

Certificate Details	
Name	Testthis
Type	request
Subject	CN=Sample1/O=Ex/ST=OK/C=US
Certificate	(null)

Back

The following table describes the fields in this screen.

Table 61 Trusted CA: View

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate.
Type	This field displays general information about the certificate. ca means that a Certification Authority signed the certificate.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).

Table 61 Trusted CA: View (continued)

LABEL	DESCRIPTION
Certificate	This read-only text box displays the certificate in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form. You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Back	Click this button to return to the previous screen.

12.4.2 Import Trusted CA Certificate

Click the **Import Certificate** button in the **Trusted CA** screen to open the following screen. The CellPipe 7130 RG trusts any valid certificate signed by any of the imported trusted CA certificates.

Figure 80 Trusted CA: Import Certificate

The following table describes the fields in this screen.

Table 62 Trusted CA: Import Certificate

LABEL	DESCRIPTION
Certificate Name	Enter the name that identifies this certificate.
Certificate	Copy and paste the certificate into the text box to store it on the CellPipe 7130 RG.
Back	Click this button to return to the previous screen.
Apply	Click this button to save your changes back to the CellPipe 7130 RG.

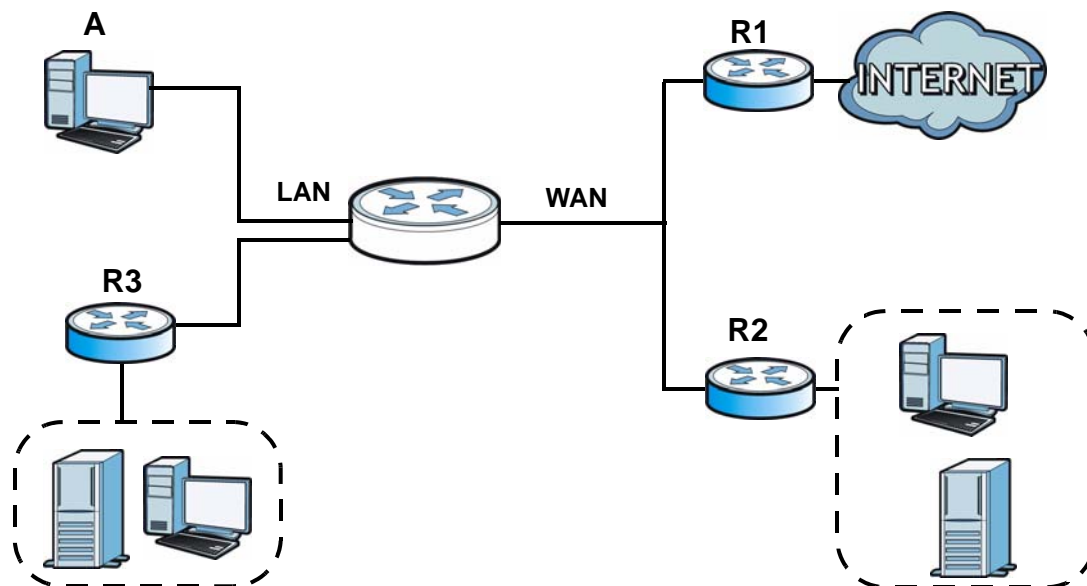
Static Route

13.1 Overview

The CellPipe 7130 RG usually uses the default gateway to route outbound traffic from computers on the LAN to the Internet. To have the CellPipe 7130 RG send data to devices not reachable through the default gateway, use static routes.

For example, the next figure shows a computer (**A**) connected to the CellPipe 7130 RG's LAN interface. The CellPipe 7130 RG routes most traffic from **A** to the Internet through the CellPipe 7130 RG's default gateway (**R1**). You create one static route to connect to services offered by your ISP behind router **R2**. You create another static route to communicate with a separate network behind a router **R3** connected to the LAN.

Figure 81 Example of Static Routing Topology



13.1.1 What You Can Do in this Chapter

The **Static Route** screens let you view and configure IP static routes on the CellPipe 7130 RG ([Section 13.2 on page 210](#)).

13.2 The Static Route Screen

Click **Advanced > Static Route** to open the **Static Route** screen.

Figure 82 Advanced > Static Route

#	Active	Destination	Netmask	Gateway	Interface	Modify
1	<input checked="" type="checkbox"/>	192.168.1.2	255.255.255.255		eth4_1	

The following table describes the labels in this screen.

Table 63 Advanced > Static Route

LABEL	DESCRIPTION
#	This is the number of an individual static route.
Active	This field indicates whether the rule is active or not. Clear the check box to disable the rule. Select the check box to enable it.
Destination	This parameter specifies the IP network address of the final destination. Routing is always based on network number.
Netmask	This parameter specifies the IP network subnet mask of the final destination.
Gateway	This is the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Interface	This is the WAN interface through which the traffic is routed.
Remove	Click the icon to remove a static route from the CellPipe 7130 RG. A window displays asking you to confirm that you want to delete the route.
Add	Click this to create a new rule.
Apply	Click this to apply your changes to the CellPipe 7130 RG.

13.2.1 Static Route Edit

Click the **Add** button in the **Static Route** screen. Use this screen to configure the required information for a static route.

Figure 83 Static Route: Add

The screenshot shows a 'Static Route Setup' window with the following fields and values:

- Destination IP Address: 0.0.0.0
- IP Subnet Mask: 0.0.0.0
- Use Interface: ipoe_0_0_33/atm0 (dropdown menu)
- Use Gateway IP Address: 0.0.0.0

At the bottom of the window are three buttons: Back, Apply, and Cancel.

The following table describes the labels in this screen.

Table 64 Static Route: Add

LABEL	DESCRIPTION
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the IP subnet mask here.
Use Interface	Select a WAN interface through which the traffic is sent. You must have the WAN interface(s) already configured in the WAN screens.
Use Gateway IP Address	Select this option and enter the IP address of the next-hop gateway. The gateway is a router or switch on the same segment as your CellPipe 7130 RG's interface(s). The gateway helps forward packets to their destinations.
Back	Click Back to return to the previous screen without saving.
Apply	Click Apply to save your changes back to the CellPipe 7130 RG.
Cancel	Click Cancel to begin configuring this screen afresh.

Policy Forwarding

14.1 Overview

Traditionally, routing is based on the destination address only and the CellPipe 7130 RG takes the shortest path to forward a packet. Policy forwarding allows the CellPipe 7130 RG to override the default routing behavior and alter the packet forwarding based on the policy defined by the network administrator. Policy-based routing is applied to outgoing packets, prior to the normal routing.

You can use source-based policy forwarding to direct traffic from different users through different connections or distribute traffic among multiple paths for load sharing.

14.1.1 What You Can Do in this Chapter

The **Policy Forwarding** screens let you view and configure routing policies on the CellPipe 7130 RG ([Section 14.2 on page 213](#)).

14.2 The Static Route Screen

Click **Advanced > Policy Forwarding** to open the **Policy Forwarding** screen.

Figure 84 Advanced > Policy Forwarding

Policy Name	SourceIP	Protocol	SourcePort	SourceMac	WAN	Remove
Example	192.168.1.2	TCP	21	aa:ff:11:22:33:bb	atm0	

.....

The following table describes the labels in this screen.

Table 65 Advanced > Policy Forwarding

LABEL	DESCRIPTION
Policy Name	This is the name of the rule.
SourceIP	This is the source IP address.
Protocol	This is the transport layer protocol.
SourcePort	This is the source port number.
SourceMAC	This is the source MAC address.
WAN	This is the WAN interface through which the traffic is routed.
Remove	Click the icon to remove a rule from the CellPipe 7130 RG. A window displays asking you to confirm that you want to delete the rule.
Add	Click this to create a new rule.

14.2.1 Policy Forwarding Setup

Click the **Add** button in the **Policy Forwarding** screen. Use this screen to configure the required information for a policy route.

Figure 85 Policy Forwarding: Add

The following table describes the labels in this screen.

Table 66 Policy Forwarding: Add

LABEL	DESCRIPTION
Policy Name	Enter a descriptive name of up to 16 printable English keyboard characters, including spaces.
Source IP Address	Enter the source IP address.
Protocol	Select the transport layer protocol (TCP or UDP).
Source Port	Enter the source port number.
Source Mac Address	Enter the source MAC address.
Use Interface	Select a WAN interface through which the traffic is sent. You must have the WAN interface(s) already configured in the WAN screens.
Back	Click Back to return to the previous screen without saving.

Table 66 Policy Forwarding: Add

LABEL	DESCRIPTION
Apply	Click Apply to save your changes back to the CellPipe 7130 RG.
Cancel	Click Cancel to begin configuring this screen afresh.

15.1 Overview

Routing Information Protocol (RIP, RFC 1058 and RFC 1389) allows a device to exchange routing information with other routers.

15.1.1 What You Can Do in this Chapter

The **RIP** screen lets you set up RIP settings on the CellPipe 7130 RG ([Section 15.2 on page 217](#)).

15.2 The RIP Screen

Click **Advanced > RIP** to open the **RIP** screen.

Figure 86 Advanced > RIP

RIP

RIP

NOTE: RIP CANNOT BE CONFIGURED on the WAN interface which has NAT enabled (such as PPPoE).

To activate RIP for the WAN Interface, select the desired RIP version and operation and place a check in the 'Enabled' checkbox. To stop RIP on the WAN Interface, uncheck the 'Enabled' checkbox. Click the 'Apply/Save' button to star/stop RIP and save the configuration.

Interface	Version	Operation	Enabled
eth4_1	2 ▾	Passive ▾	<input type="checkbox"/>

.....

The following table describes the labels in this screen.

Table 67 Advanced > RIP

LABEL	DESCRIPTION
Interface	This is the name of the interface in which the RIP setting is used.
Version	The RIP version controls the format and the broadcasting method of the RIP packets that the CellPipe 7130 RG sends (it recognizes both formats when receiving). RIP version 1 is universally supported but RIP version 2 carries more information. RIP version 1 is probably adequate for most networks, unless you have an unusual network topology.
Operation	Select Passive to have the CellPipe 7130 RG update the routing table based on the RIP packets received from neighbors but not advertise its route information to other routers in this interface. Select Active to have the CellPipe 7130 RG advertise its route information and also listen for routing updates from neighboring routers.
Enabled	Select the check box to activate the settings.
Apply/Save	Click Apply/Save to save your changes back to the CellPipe 7130 RG.

Quality of Service (QoS)

16.1 Overview

Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to control the use of bandwidth. Without QoS, all traffic data is equally likely to be dropped when the network is congested. This can cause a reduction in network performance and make the network inadequate for time-critical application such as video-on-demand.

Configure QoS on the CellPipe 7130 RG to group and prioritize application traffic and fine-tune network performance. Setting up QoS involves these steps:

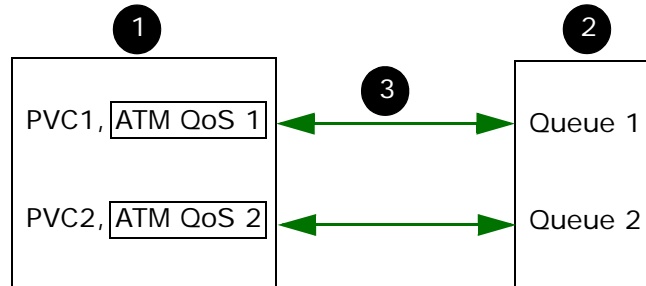
- 1 Configure classifiers to sort traffic into different flows.
- 2 Assign priority and define actions to be performed for a classified traffic flow.

The CellPipe 7130 RG assigns each packet a priority and then queues the packet accordingly. Packets assigned a high priority are processed more quickly than those with low priority if there is congestion, allowing time-sensitive applications to flow more smoothly. Time-sensitive applications include both those that require a low level of latency (delay) and a low level of jitter (variations in delay) such as Internet gaming, and those for which jitter alone is a problem such as Internet radio or streaming video.

This chapter contains information about configuring QoS and editing classifiers.

16.1.1 QoS Overview

The following figure gives an overview of how to configure QoS on this CellPipe 7130 RG:



- 1 First, you have to configure WAN connection(s) in **Network > WAN > Connect**. Refer to [Section 2.4 on page 40](#) for a tutorial on how to prioritize traffic and eliminate congestion over the ATM network (at the ATM layer).
- 2 Configure queue settings in **Advanced > QoS > Queue Setup** according to the priority you want to apply to different types of traffic.

Configure class settings in **Advanced > QoS > Class Setup**. This associates queues with PVCs by mapping the priority of queues to the index number of PVCs.

16.1.2 What You Can Do in this Chapter

- The **General** screen lets you enable or disable QoS and set the upstream bandwidth ([Section 16.3 on page 221](#)).
- The **Queue Setup** screen lets you configure QoS queue assignment ([Section 16.4 on page 222](#)).
- The **Class Setup** screen lets you add, edit or delete QoS classifiers ([Section 16.5 on page 225](#)).
- The **Policer Setup** screen lets you specify the committed rate and committed burst size for incoming packets ([Section 16.5 on page 225](#)).
- The **Monitor** screen lets you view the CellPipe 7130 RG's QoS-related packet statistics ([Section 16.7 on page 233](#)).

16.2 What You Need to Know

The following terms and concepts may help as you read through this chapter.

QoS versus Cos

QoS is used to prioritize source-to-destination traffic flows. All packets in the same flow are given the same priority. CoS (class of service) is a way of managing traffic in a network by grouping similar types of traffic together and treating each type as a class. You can use CoS to give different priorities to different packet types.

CoS technologies include IEEE 802.1p layer 2 tagging and DiffServ (Differentiated Services or DS). IEEE 802.1p tagging makes use of three bits in the packet header, while DiffServ is a new protocol and defines a new DS field, which replaces the eight-bit ToS (Type of Service) field in the IP header.

Tagging and Marking

In a QoS class, you can configure whether to add or change the DSCP (DiffServ Code Point) value, IEEE 802.1p priority level and VLAN ID number in a matched packet. When the packet passes through a compatible network, the networking device, such as a backbone switch, can provide specific treatment or service based on the tag or marker.

16.3 The Quality of Service General Screen

Click **Advanced Setup** > **Quality of Service** to open the screen as shown next.

Use this screen to enable or disable QoS and set the upstream bandwidth. See [Section 16.1 on page 219](#) for more information.

Figure 87 QoS General

The screenshot shows a configuration window for QoS. At the top, there are five tabs: 'General', 'Queue Setup', 'Class Setup', 'Policer Setup', and 'Monitor'. The 'General' tab is active. Below the tabs, the 'General' section contains the following elements:

- A checkbox labeled 'Active QoS' which is currently unchecked.
- A text input field labeled 'WAN Managed Upstream Bandwidth' followed by '(kbps)'. The field is currently empty.
- A note below the input field: '(You can assign the upstream bandwidth manually. If the field is empty, the CPE set the value automatically.)'
- At the bottom of the window, there are two buttons: 'Apply' and 'Cancel'.

The following table describes the labels in this screen.

Table 68 QoS General

LABEL	DESCRIPTION
Active QoS	Select the check box to turn on QoS to improve your network performance.
WAN Managed Upstream Bandwidth	<p>Enter the amount of upstream bandwidth for the WAN interface that you want to allocate using QoS.</p> <p>The recommendation is to set this speed to match the interface's actual transmission speed. For example, set the WAN interface speed to 100000 kbps if your Internet connection has an upstream transmission speed of 100 Mbps.</p> <p>You can set this number higher than the interface's actual transmission speed. The CellPipe 7130 RG uses up to 95% of the DSL port's actual upstream transmission speed even if you set this number higher than the DSL port's actual transmission speed.</p> <p>You can also set this number lower than the interface's actual transmission speed. This will cause the CellPipe 7130 RG to not use some of the interface's available bandwidth.</p> <p>If you leave this field blank, the CellPipe 7130 RG automatically sets this number to be 95% of the DSL port's actual upstream transmission speed.</p>
Apply	Click Apply to save your changes back to the CellPipe 7130 RG.
Cancel	Click Cancel to begin configuring this screen afresh.

16.4 The Queue Setup Screen

Click **QoS > Queue Setup** to open the screen as shown next.

Use this screen to configure QoS queue assignment.

Figure 88 QoS Queue Setup

General Queue Setup Class Setup Policer Setup Monitor

Queue Setup

Create a new Queue : (maximum 7 configurable entries for WAN port, and maximum 3 configurable entries for each LAN port)

The QoS function has been disabled. Queues would not take effects.

No.	Active	Name	Interface	Priority	Weight	Buffer Management	Scheduler Algorithm	Rate Limit	Modify
.....									

The following table describes the labels in this screen.

Table 69 QoS Queue Setup

LABEL	DESCRIPTION
Add	Click this button to create a new entry.
No.	This is the index number of this entry.
Active	Select the check box to enable the queue.
Name	This shows the descriptive name of this queue.
Interface	This shows the name of the CellPipe 7130 RG's interface through which traffic in this queue passes.
Priority	This shows the priority of this queue.
Weight	This shows the weight of this queue.
Buffer Management	This shows the queue management algorithm used for this queue. Queue management algorithms determine how the CellPipe 7130 RG should handle packets when it receives too many (network congestion).
Scheduler Algorithm	This shows the scheduling algorithm that the CellPipe 7130 RG uses. A scheduling algorithm is how the CellPipe 7130 RG selects packets for QoS.
Rate Limit	This shows the maximum transmission rate allowed for traffic on this queue.
Modify	Click the Edit icon to go to the screen where you can edit the queue. Click the Remove icon to delete an existing queue. Note that subsequent rules move up by one when you take this action.
Apply	Click Apply to save your changes back to the CellPipe 7130 RG.

16.4.1 Adding a QoS Queue

Click the **Add** button or the edit icon in the **Queue Setup** screen to configure a queue.

Figure 89 QoS Queue Setup: Add

The screenshot shows the 'Queue Configuration' window. It contains the following elements:

- Active
- Name:
- Interface:
- Priority:
- Weight:
- Buffer Management:
- Scheduler Algorithm:
- Rate Limit: (kbps)
- Buttons: Back, Apply, Cancel

The following table describes the labels in this screen.

Table 70 QoS Queue Setup: Add

LABEL	DESCRIPTION
Active	Select to enable or disable this queue.
Name	Enter a descriptive name of up to 15 printable English keyboard characters, including spaces.
Interface	Select the interface to which this queue is applied.
Priority	Select the priority level (from 1 to 4) of this queue. The smaller the number, the higher the priority level. Traffic assigned to higher priority queues gets through faster while traffic in lower priority queues is dropped if the network is congested.
Weight	Select the weight (from 1 to 8) of this queue. If two queues have the same priority level, the CellPipe 7130 RG divides the bandwidth across the queues according to their weights. Queues with larger weights get more bandwidth than queues with smaller weights.
Buffer Management	This field displays Drop Tail (DT) . Drop Tail (DT) is a simple queue management algorithm that allows the CellPipe 7130 RG buffer to accept as many packets as it can until it is full. Once the buffer is full, new packets that arrive are dropped until there is space in the buffer again (packets are transmitted out of it).
Scheduler Algorithm	As of writing, this is set to PQWFQ by default. This stands for Priority Queue Weighted Fair Queuing, which is a packet-based scheduling algorithm that allocates more bandwidth to critical applications.

Table 70 QoS Queue Setup: Add

LABEL	DESCRIPTION
Rate Limit	Specify the maximum transmission rate (in Kbps) allowed for traffic on this queue.
Back	Click Back to return to the previous screen without saving.
Apply	Click Apply to save your changes back to the CellPipe 7130 RG.
Cancel	Click Cancel to begin configuring this screen afresh.

16.5 The Class Setup Screen

Use this screen to add, edit or delete QoS classifiers. A classifier groups traffic into data flows according to specific criteria such as the source address, destination address, source port number, destination port number or incoming interface. For example, you can configure a classifier to select traffic from the same protocol port (such as Telnet) to form a flow.

You can give different priorities to traffic that the CellPipe 7130 RG forwards out through the WAN interface. Give high priority to voice and video to make them run more smoothly. Similarly, give low priority to many large file downloads so that they do not reduce the quality of other applications.

Click **QoS > Class Setup** to open the following screen.

Figure 90 QoS Class Setup

The following table describes the labels in this screen.

Table 71 QoS Class Setup

LABEL	DESCRIPTION
Add	Click this button to create a new classifier.
Order	This field displays the index number of the classifier.
Active	Select the check box to enable the classifier.
Class Name	This is the name of the classifier.

Table 71 QoS Class Setup (continued)

LABEL	DESCRIPTION
Classification Criteria	This shows criteria specified in this classifier, for example the interface from which traffic of this class should come and the source MAC address of traffic that matches this classifier.
Forward To	This is the interface through which traffic that matches this classifier is forwarded out.
DSCP Mark	This is the DSCP number added to traffic of this classifier.
802.1P Mark	This is the IEEE 802.1p priority level assigned to traffic of this classifier.
VLAN ID Tag	This is the VLAN ID number assigned to traffic of this classifier.
To Queue	This is the name of the queue in which traffic of this classifier is put.
Modify	Click the Edit icon to go to the screen where you can edit the classifier. Click the Remove icon to delete an existing classifier. Note that subsequent rules move up by one when you take this action.
Apply	Click Apply to save your changes back to the CellPipe 7130 RG.

16.5.1 QoS Class Edit

Click the **Add** button or the **Edit** icon in the **Class Setup** screen to configure a classifier.

Figure 91 QoS Class Setup: Add

Class Configuration

Active

Class Name

Classification Order

Forward To Interface

DSCP Mark (0~63)

802.1P Mark

VLAN ID Tag (0~4094)

To Queue

Criteria Configuration

Basic

From Interface

Ether Type

Source

MAC Address MAC Mask Exclude

IP Address IP Subnet Mask Exclude

TCP/UDP Port Range ~ Exclude

Destination

MAC Address MAC Mask Exclude

IP Address IP Subnet Mask Exclude

TCP/UDP Port Range ~ Exclude

Others

802.1P Exclude

VLAN ID (0~4094) Exclude

IP Protocol Exclude

IP Packet Length ~ Exclude

DSCP (0~63) Exclude

TCP ACK Exclude

DHCP Exclude

Note :
Support DHCP options only when routing mode.

The following table describes the labels in this screen.

Table 72 QoS Class Configuration

LABEL	DESCRIPTION
Class Configuration	
Active	Select to enable or disable this classifier.
Class Name	Enter a descriptive name of up to 15 printable English keyboard characters, including spaces.
Classification Order	<p>Select an existing number to set the classifier's order. The order takes effect after clicking Apply and can be viewed in QoS > Class Setup.</p> <p>Select Last to put this rule in the end of the classifier list.</p>
Forward to Interface	Select a WAN interface through which traffic of this class will be forwarded out. If you select Unchange , the CellPipe 7130 RG forward traffic of this class according to the default routing table.
DSCP Mark	<p>This field is available only when you select the Ether Type check box.</p> <p>If you select Mark, enter a DSCP value with which the CellPipe 7130 RG replaces the DSCP field in the packets.</p> <p>If you select Unchange, the CellPipe 7130 RG keep the DSCP field in the packets.</p>
802.1p Mark	<p>Select a priority level with which the CellPipe 7130 RG replaces the IEEE 802.1p priority field in the packets.</p> <p>If you select Unchange, the CellPipe 7130 RG keep the 802.1p priority field in the packets.</p>
VLAN ID Tag	<p>If you select Remark, enter a VLAN ID number (between 1 and 4095) with which the CellPipe 7130 RG replaces the VLAN ID of the frames.</p> <p>If you select Remove, the CellPipe 7130 RG deletes the VLAN ID of the frames before forwarding them out.</p> <p>If you select Add, the CellPipe 7130 RG treat all matched traffic untagged and add a second VLAN ID.</p> <p>If you select Unchange, the CellPipe 7130 RG keep the VLAN ID in the packets.</p>
To Queue	<p>Select a queue that applies to this class.</p> <p>You should have configured a queue in the Queue Setup screen already.</p>
<p>Criteria Configuration</p> <p>Use the following fields to configure the criteria for traffic classification.</p>	
Basic	
From Interface	Select from which Ethernet port or wireless interface traffic of this class should come.

Table 72 QoS Class Configuration (continued)

LABEL	DESCRIPTION
Ether Type	<p>Select a predefined application to configure a class for the matched traffic.</p> <p>If you select IP, you also need to configure source or destination MAC address, IP address, DHCP options, DSCP value or the protocol type.</p> <p>If you select 8021Q, you can configure an 802.1p priority level and VLAN ID in the Others section.</p>
Source	
MAC Address	Select the check box and enter the source MAC address of the packet.
MAC Mask	<p>Type the mask for the specified MAC address to determine which bits a packet's MAC address should match.</p> <p>Enter "f" for each bit of the specified source MAC address that the traffic's MAC address should match. Enter "0" for the bit(s) of the matched traffic's MAC address, which can be of any hexadecimal character(s). For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria.</p>
IP Address	Select the check box and enter the source IP address in dotted decimal notation. A blank source IP address means any source IP address.
IP Subnet Mask	Enter the source subnet mask.
TCP/UDP Port Range	If you select TCP or UDP in the IP Protocol field, select the check box and enter the port number(s) of the source.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Destination	
MAC Address	Select the check box and enter the destination MAC address of the packet.
MAC Mask	<p>Type the mask for the specified MAC address to determine which bits a packet's MAC address should match.</p> <p>Enter "f" for each bit of the specified source MAC address that the traffic's MAC address should match. Enter "0" for the bit(s) of the matched traffic's MAC address, which can be of any hexadecimal character(s). For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria.</p>
IP Address	Select the check box and enter the destination IP address in dotted decimal notation. A blank source IP address means any source IP address.
IP Subnet Mask	Enter the destination subnet mask.
TCP/UDP Port Range	If you select TCP or UDP in the IP Protocol field, select the check box and enter the port number(s) of the source.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Others	

Table 72 QoS Class Configuration (continued)

LABEL	DESCRIPTION
802.1P	<p>This field is available only when you select 802.1Q in the Ether Type field.</p> <p>Select this option and select a priority level (between 0 and 7) from the drop down list box.</p> <p>"0" is the lowest priority level and "7" is the highest.</p>
VLAN ID	<p>This field is available only when you select 802.1Q in the Ether Type field.</p> <p>Select this option and specify a VLAN ID number between 1 and 4095.</p>
IP Protocol	<p>This field is available only when you select IP in the Ether Type field.</p> <p>Select this option and select the protocol (service type) from TCP, UDP, ICMP or IGMP. If you select User defined, enter the protocol (service type) number.</p>
IP Packet Length	<p>This field is available only when you select IP in the Ether Type field.</p> <p>Select this option and enter the minimum and maximum packet length (from 28 to 1500) in the fields provided.</p>
DSCP	<p>This field is available only when you select IP in the Ether Type field.</p> <p>Select this option and specify a DSCP (DiffServ Code Point) number between 0 and 63 in the field provided.</p>
TCP ACK	<p>This field is available only when you select IP in the Ether Type field.</p> <p>If you select this option, the matched TCP packets must contain the ACK (Acknowledge) flag.</p>
DHCP	<p>This field is available only when you select IP in the Ether Type field.</p> <p>Select this option and select a DHCP option.</p> <p>If you select Vendor Class ID (DHCP Option 60), enter the Vendor Class Identifier (Option 60) of the matched traffic, such as the type of the hardware or firmware.</p> <p>If you select User Class ID (DHCP Option 77), enter a string that identifies the user's category or application type in the matched DHCP packets.</p>
Exclude	<p>Select this option to exclude the packets that match the specified criteria from this classifier.</p>
Back	<p>Click Back to return to the previous screen without saving.</p>
Apply	<p>Click Apply to save your changes back to the CellPipe 7130 RG.</p>
Cancel	<p>Click Cancel to begin configuring this screen afresh.</p>

16.6 The Policer Setup Screen

Click **QoS > Policer Setup** to open the following screen. The CellPipe 7130 RG can control ingress (or incoming) traffic by dropping packets that exceed the committed rate and/or committed burst size specified in this screen.

A policer is a QoS policy.

Figure 92 Policer Setup

The following table describes the labels in this screen.

Table 73 Policer Setup

LABEL	DESCRIPTION
Add	Click this button to create a new policy.
No	This field displays the index number of the policy.
Active	Select the check box to enable the policy.
Name	This is the name of the policy.
Regulated Classes	This shows to which classes the policy applies.
Meter Type	This is set to Simple Token Bucket , which is similar to tokens in a bucket to control when traffic can be transmitted. The bucket is a buffer that temporarily stores outgoing packets and transmits them at an average rate.
Committed Rate	This shows the maximum committed rate for the specified class/es.
Committed Burst Size	This shows the maximum committed burst size for the specified class/es.
Modify	Click the Edit icon to go to the screen where you can edit the classifier. Click the Remove icon to delete an existing classifier. Note that subsequent rules move up by one when you take this action.
Apply	Click Apply to save your changes back to the CellPipe 7130 RG.

16.6.1 Policer Setup Edit

Click the **Add** button or the **Edit** icon in the **Policer Setup** screen to configure a classifier.

Figure 93 Add/Edit Policer Setup

The following table describes the labels in this screen.

Table 74 Add/Edit Policer Setup

LABEL	DESCRIPTION
Active	Select the check box to enable the policy.
Name	Enter a descriptive name of up to 15 printable English keyboard characters, including spaces.
Meter Type	This is set to Simple Token Bucket , which uses tokens in a bucket to control when traffic can be transmitted. The bucket is a buffer that temporarily stores outgoing packets and transmits them at an average rate.
Committed Rate	Enter the maximum committed rate for the class/es.
Committed Burst Size	Enter the the maximum committed burst size for the class/es.
Available Class	This shows all the classes created in the CellPipe 7130 RG. Select the class that you want to include in the policy and click Add to move it to selected class.
Selected Class	This shows to which classes the policy applies. Select the class that you want to exclude from the policy and click Remove to move it to the available class.
Add/Remove	Use these buttons to add or remove a class from either Available Class and Selected Class boxes.

Table 74 Add/Edit Policer Setup (continued)

LABEL	DESCRIPTION
Back	Click Back to return to the previous screen without saving.
Apply	Click Apply to save your changes back to the CellPipe 7130 RG.
Cancel	Click Cancel to begin configuring this screen afresh.

16.7 The QoS Monitor Screen

To view the CellPipe 7130 RG's QoS packet statistics, click **Advanced > QoS > Monitor**. The screen appears as shown.

Figure 94 QoS > Monitor

The following table describes the labels in this screen.

Table 75 QoS > Monitor

LABEL	DESCRIPTION
Monitor	
Refresh Interval	Enter how often you want the CellPipe 7130 RG to update this screen. Select No Refresh to stop refreshing statistics.
Queue Monitor	
No.	This is the index number of the entry.
Name	This shows the name of the queue.
Pass Rate	This shows how many packets assigned to this queue are transmitted successfully.
Drop Rate	This shows how many packets assigned to this queue are dropped.

16.8 Technical Reference

The following section contains additional technical information about the CellPipe 7130 RG features described in this chapter.

IEEE 802.1Q Tag

The IEEE 802.1Q standard defines an explicit VLAN tag in the MAC header to identify the VLAN membership of a frame across bridges. A VLAN tag includes the 12-bit VLAN ID and 3-bit user priority. The VLAN ID associates a frame with a specific VLAN and provides the information that devices need to process the frame across the network.

IEEE 802.1p specifies the user priority field and defines up to eight separate traffic types. The following table describes the traffic types defined in the IEEE 802.1d standard (which incorporates the 802.1p).

Table 76 IEEE 802.1p Priority Level and Traffic Type

PRIORITY LEVEL	TRAFFIC TYPE
Level 7	Typically used for network control traffic such as router configuration messages.
Level 6	Typically used for voice traffic that is especially sensitive to jitter (jitter is the variations in delay).
Level 5	Typically used for video that consumes high bandwidth and is sensitive to jitter.
Level 4	Typically used for controlled load, latency-sensitive traffic such as SNA (Systems Network Architecture) transactions.
Level 3	Typically used for "excellent effort" or better than best effort and would include important business traffic that can tolerate some delay.
Level 2	This is for "spare bandwidth".
Level 1	This is typically used for non-critical "background" traffic such as bulk transfers that are allowed but that should not affect other applications and users.
Level 0	Typically used for best-effort traffic.

DiffServ

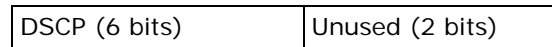
QoS is used to prioritize source-to-destination traffic flows. All packets in the flow are given the same priority. You can use CoS (class of service) to give different priorities to different packet types.

DiffServ (Differentiated Services) is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCPs) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.

DSCP and Per-Hop Behavior

DiffServ defines a new Differentiated Services (DS) field to replace the Type of Service (TOS) field in the IP header. The DS field contains a 2-bit unused field and a 6-bit DSCP field which can define up to 64 service levels. The following figure illustrates the DS field.

DSCP is backward compatible with the three precedence bits in the ToS octet so that non-DiffServ compliant, ToS-enabled network device will not conflict with the DSCP mapping.



The DSCP value determines the forwarding behavior, the PHB (Per-Hop Behavior), that each packet gets across the DiffServ network. Based on the marking rule, different kinds of traffic can be marked for different kinds of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

Dynamic DNS Setup

17.1 Overview

Dynamic DNS allows you to update your current dynamic IP address with one or many dynamic DNS services so that anyone can contact you (in NetMeeting, CU-SeeMe, etc.). You can also access your FTP server or Web site on your own computer using a domain name (for instance myhost.dhs.org, where myhost is a name of your choice) that will never change instead of using an IP address that changes each time you reconnect. Your friends or relatives will always be able to call you even if they don't know your IP address.

First of all, you need to have registered a dynamic DNS account with www.dyndns.org. This is for people with a dynamic IP from their ISP or DHCP server that would still like to have a domain name. The Dynamic DNS service provider will give you a password or key.

17.1.1 What You Can Do in this Chapter

Use the **Dynamic DNS** screen ([Section 17.3 on page 238](#)) to enable DDNS and configure the DDNS settings on the CellPipe 7130 RG.

17.2 What You Need To Know

DYNDNS Wildcard

Enabling the wildcard feature for your host causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.

If you have a private WAN IP address, then you cannot use Dynamic DNS.

17.3 The Dynamic DNS Screen

To change your CellPipe 7130 RG's DDNS, click **Advanced > Dynamic DNS**. The screen appears as shown.

Figure 95 Advanced > Dynamic DNS

The following table describes the fields in this screen.

Table 77 Advanced > Dynamic DNS

LABEL	DESCRIPTION
Service Provider	Select the name of your Dynamic DNS service provider.
Host Name	Type the domain name assigned to your CellPipe 7130 RG by your Dynamic DNS provider. You can specify up to two host names in the field separated by a comma (",").
Interface	Select the WAN interface to use for updating the IP address of the domain name.
User Name	Type your user name.
Password	Type the password assigned to you.
Email	If you select TZO in the Service Provider field, enter the user name you used to register for this service.
Key	If you select TZO in the Service Provider field, enter the password you used to register for this service.
Apply	Click Apply to save your changes back to the CellPipe 7130 RG.
Cancel	Click Cancel to begin configuring this screen afresh.

Remote Management

18.1 Overview

This chapter explains how to configure the remote management and access control settings on the CellPipe 7130 RG.

The CellPipe 7130 RG supports multiple remote management sessions running at one time.

Note: Refer to [Section 3.2 on page 83](#) for user level information. Each user level has its own account information for logging into the CellPipe 7130 RG.

18.1.1 What You Can Do in this Chapter

- The **TR-069** screen lets you configure the CellPipe 7130 RG's TR-069 auto-configuration settings ([Section 18.3 on page 241](#)).
- The **TR-064** screen lets you enable management via TR-064 on the CellPipe 7130 RG ([Section 18.3 on page 241](#)).
- The **Service Control** screens let you configure through which interface(s) users can use which service(s) to manage the CellPipe 7130 RG ([Section 18.4 on page 242](#)).
- The **IP Address** screens let you configure from which IP address(es) users can use a service to manage the CellPipe 7130 RG ([Section 18.5 on page 243](#)).

18.2 The TR-069 Screen

TR-069 defines how Customer Premise Equipment (CPE), for example your CellPipe 7130 RG, can be managed over the WAN by an Auto Configuration Server (ACS). TR-069 is based on sending Remote Procedure Calls (RPCs) between an ACS and a client device. RPCs are sent in Extensible Markup Language (XML) format over HTTP or HTTPS.

An administrator can use an ACS to remotely set up the CellPipe 7130 RG, modify settings, perform firmware upgrades as well as monitor and diagnose the CellPipe

7130 RG. You have to enable the device to be managed by the ACS and specify the ACS IP address or domain name and username and password.

Click **Advanced > Remote MGMT** to open the following screen. Use this screen to configure your CellPipe 7130 RG to be managed by an ACS.

Figure 96 TR-069

The following table describes the fields in this screen.

Table 78 TR-069

LABEL	DESCRIPTION
Inform	Select Enable to activate remote management via TR-069 on the WAN. Otherwise, select Disable .
Inform Interval	Enter the time interval (in seconds) at which the CellPipe 7130 RG sends information to the auto-configuration server.
ACS URL	Enter the URL or IP address of the auto-configuration server.
ACS User Name	Enter the TR-069 user name for authentication with the auto-configuration server.
ACS Password	Enter the TR-069 password for authentication with the auto-configuration server.
WAN Interface used by TR-069 client	Select a WAN interface through which the TR-069 traffic passes. If you select Multi_WAN , you should also select the pre-configured WAN connection(s).
Display SOAP messages on serial console	Select Enable to show the SOAP messages on the console.
Connection Request Authentication	Select this option to enable authentication when there is a connection request from the ACS.

Table 78 TR-069 (continued)

LABEL	DESCRIPTION
Connection Request User Name	Enter the connection request user name. When the ACS makes a connection request to the CellPipe 7130 RG, this user name is used to authenticate the ACS.
Connection Request Password	Enter the connection request password. When the ACS makes a connection request to the CellPipe 7130 RG, this password is used to authenticate the ACS.
Connection Request URL	This shows the connection request URL. The ACS can use this URL to make a connection request to the CellPipe 7130 RG.
Apply	Click this button to save your changes back to the CellPipe 7130 RG.
Cancel	Click Cancel to begin configuring this screen afresh.

18.3 The TR-064 Screen

TR-064 is a LAN-Side DSL CPE Configuration protocol defined by the DSL Forum. TR-064 is built on top of UPnP. It allows the users to use a TR-064 compliant CPE management application on their computers from the LAN to discover the CPE and configure user-specific parameters, such as the username and password.

Click **Advanced** > **Remote MGMT** > **TR064** to open the following screen.

Figure 97 TR-064

The following table describes the fields in this screen.

Table 79 TR-064

LABEL	DESCRIPTION
Enanble TR064	Select the check box to activate management via TR-064 on the LAN.
Apply	Click this button to save your changes back to the CellPipe 7130 RG.

18.4 The Service Control Screen

Click **Advanced > Remote MGMT > Service Control** to open the following screen. Use this screen to decide what services you may use to access which CellPipe 7130 RG interface.

Figure 98 Service Control

#	Services	LAN	WAN
1	FTP	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable
2	HTTP	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable
3	SSH	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable
4	TELNET	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable
5	TFTP	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable

The following table describes the fields in this screen.

Table 80 Access Control: Services

LABEL	DESCRIPTION
Service Control	Select Enable to turn on service control. Otherwise, select Disable .
#	This is the index number of the entry.
Services	This is the service you may use to access the CellPipe 7130 RG.
LAN	Select the Enable check box for the corresponding services that you want to allow access to the CellPipe 7130 RG from the LAN.
WAN	Select the Enable check box for the corresponding services that you want to allow access to the CellPipe 7130 RG from the WAN.
Apply	Click this button to save your changes back to the CellPipe 7130 RG.

18.5 The IP Address Screen

Click **Advanced > Remote MGMT > IP Address** to open the following screen. Use this screen to specify the “trusted” computers from which an administrator may use a service to manage the CellPipe 7130 RG.

Figure 99 IP Address

Access Control -- IP Address

The IP Address Access Control mode, if enabled, permits access to local management services from IP addresses contained in the Access Control List. If the Access Control mode is disabled, the system will not validate IP addresses for incoming packets. The services are the system applications listed in the Service Control List

Access Control Mode: Disable Enable

IP Address	Remove
192.168.1.33	<input type="checkbox"/>

The following table describes the fields in this screen.

Table 81 IP Address

LABEL	DESCRIPTION
Access Control Mode	Select Enable to activate the secured client list. Select Disable to disable the list without deleting it.
IP Address	This is the IP address of the trusted computer from which you can manage the CellPipe 7130 RG.
Remove	Select this check box and click the Remove button to delete this entry from the CellPipe 7130 RG.
Add	Click this button to create a new entry.
Remove	Click this button to delete the selected entry.

18.5.1 Adding an IP Address

Click the **Add** button in the **IP Address** screen to open the following screen.

Figure 100 IP Address: Add

Access Control -- IP Address

Enter the IP address of the management station permitted to access the local management services, and click 'Apply/Save.'

IP Address:

The following table describes the fields in this screen.

Table 82 IP Address: Add

LABEL	DESCRIPTION
IP Address	Enter the IP address of the trusted computer from which you can manage the CellPipe 7130 RG.
Apply/Save	Click this button to save your changes back to the CellPipe 7130 RG.
Back	Click this button to return to the previous screen without saving.

Universal Plug-and-Play (UPnP)

19.1 Overview

Universal Plug and Play (UPnP) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use.

19.1.1 What You Can Do in this Chapter

The **UPnP** screen lets you enable UPnP on the CellPipe 7130 RG ([Section 19.3 on page 246](#)).

19.2 What You Need to Know

How do I know if I'm using UPnP?

UPnP hardware is identified as an icon in the Network Connections folder (Windows XP). Each UPnP compatible device installed on your network will appear as a separate icon. Selecting the icon of a UPnP device will allow you to access the information and properties of that device.

NAT Traversal

UPnP NAT traversal automates the process of allowing an application to operate through NAT. UPnP network devices can automatically configure network addressing, announce their presence in the network to other UPnP devices and enable exchange of simple product and service descriptions. NAT traversal allows the following:

- Dynamic port mapping
- Learning public IP addresses
- Assigning lease times to mappings

Windows Messenger is an example of an application that supports NAT traversal and UPnP.

See the NAT chapter for more information on NAT.

Cautions with UPnP

The automated nature of NAT traversal applications in establishing their own services and opening firewall ports may present network security issues. Network information and configuration may also be obtained and modified by users in some network environments.

When a UPnP device joins a network, it announces its presence with a multicast message. For security reasons, the CellPipe 7130 RG allows multicast messages on the LAN only.

All UPnP-enabled devices may communicate freely with each other without additional configuration. Disable UPnP if this is not your intention.

UPnP and CellPipe 7130 RG

This device has achieved UPnP certification from the Universal Plug and Play Forum UPnP™ Implementers Corp. (UIC). The UPnP implementation supports Internet Gateway Device (IGD) 1.0.

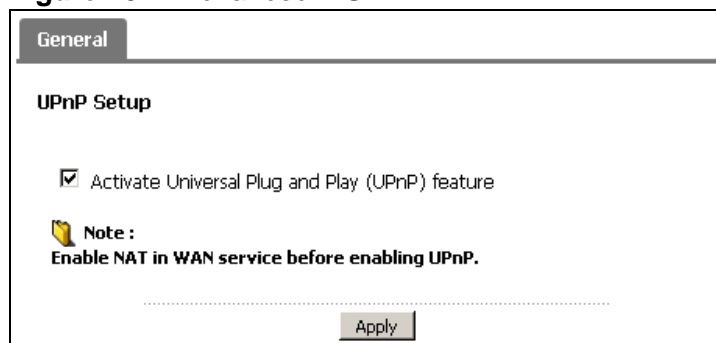
See the following sections for examples of installing and using UPnP.

19.3 The UPnP Screen

Click **Advanced > UPnP** to display the screen shown next.

See [Section 19.1 on page 245](#) for more information.

Figure 101 Advanced > UPnP



The following table describes the fields in this screen.

Table 83 Advanced > UPnP

LABEL	DESCRIPTION
Activate Universal Plug and Play (UPnP) Feature	Select this check box to enable UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the CellPipe 7130 RG's IP address (although you must still enter the password to access the web configurator).
Apply/Save	Click this to save the setting to the CellPipe 7130 RG.

19.4 Installing UPnP in Windows Example

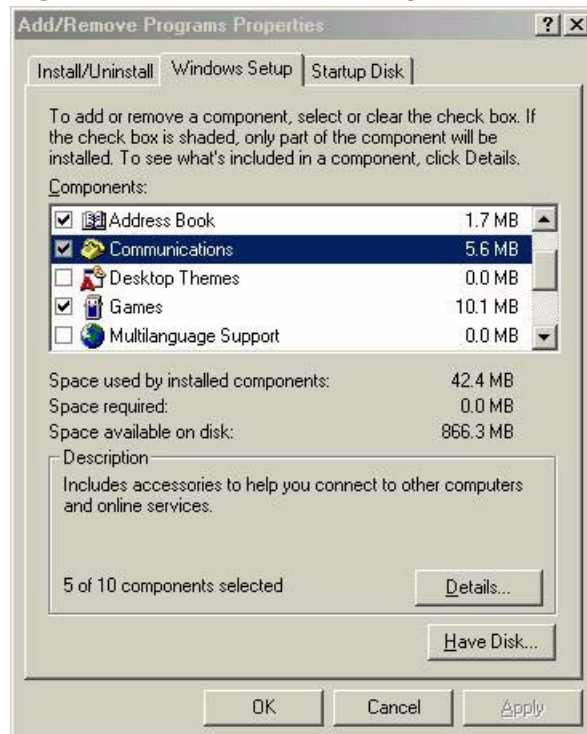
This section shows how to install UPnP in Windows Me and Windows XP.

Installing UPnP in Windows Me

Follow the steps below to install the UPnP in Windows Me.

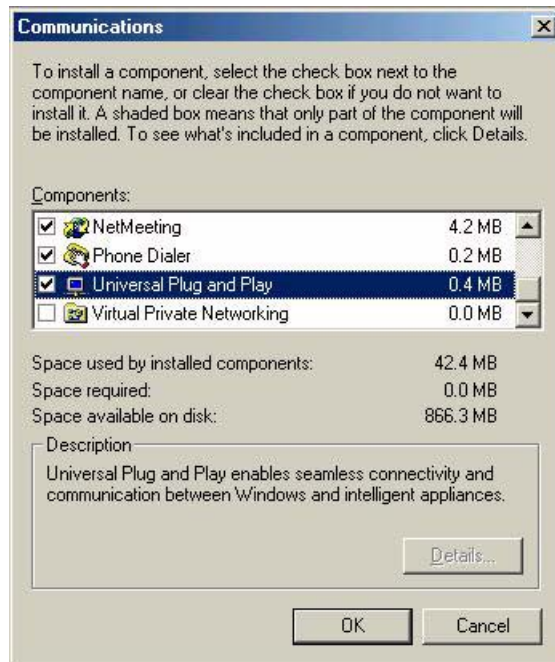
- 1 Click **Start** and **Control Panel**. Double-click **Add/Remove Programs**.
- 2 Click on the **Windows Setup** tab and select **Communication** in the **Components** selection box. Click **Details**.

Figure 102 Add/Remove Programs: Windows Setup: Communication



- 3 In the **Communications** window, select the **Universal Plug and Play** check box in the **Components** selection box.

Figure 103 Add/Remove Programs: Windows Setup: Communication: Components



- 4 Click **OK** to go back to the **Add/Remove Programs Properties** window and click **Next**.
- 5 Restart the computer when prompted.

Installing UPnP in Windows XP

Follow the steps below to install the UPnP in Windows XP.

- 1 Click **Start** and **Control Panel**.
- 2 Double-click **Network Connections**.

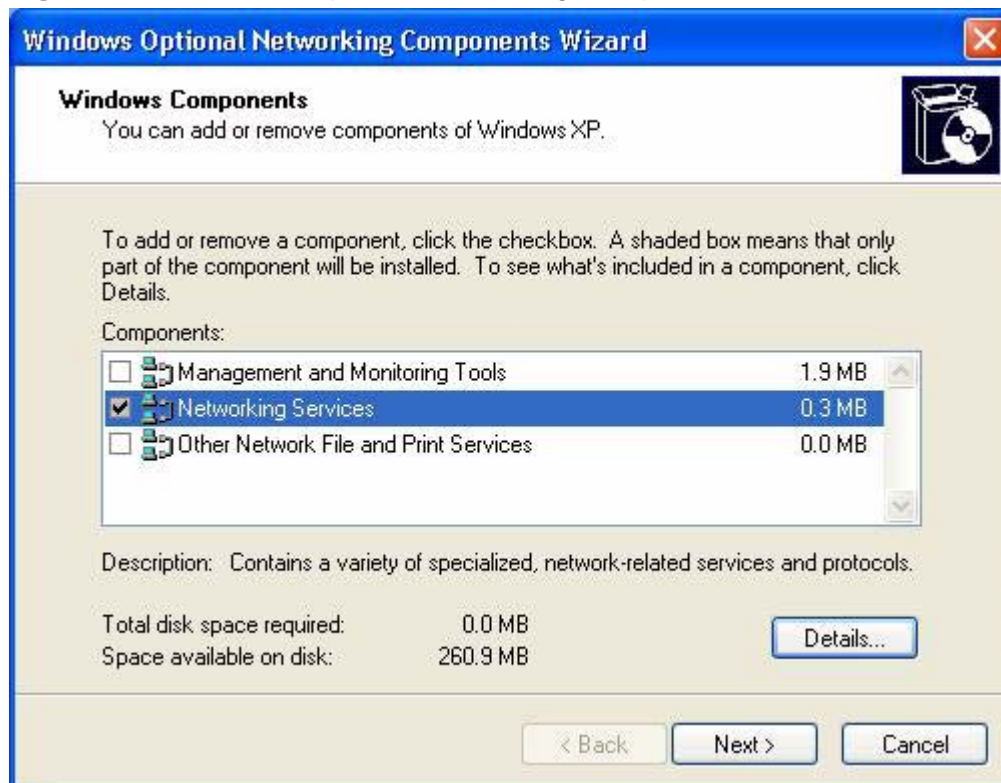
- 3 In the **Network Connections** window, click **Advanced** in the main menu and select **Optional Networking Components**

Figure 104 Network Connections



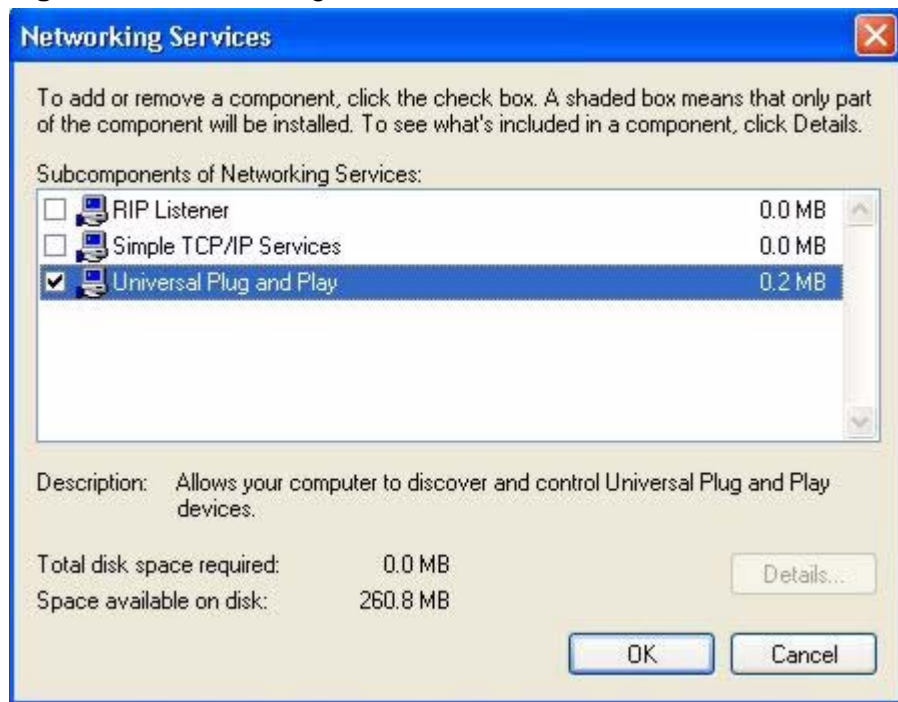
- 4 The **Windows Optional Networking Components Wizard** window displays. Select **Networking Service** in the **Components** selection box and click **Details**.

Figure 105 Windows Optional Networking Components Wizard



- 5 In the **Networking Services** window, select the **Universal Plug and Play** check box.

Figure 106 Networking Services



- 6 Click **OK** to go back to the **Windows Optional Networking Component Wizard** window and click **Next**.

19.5 Using UPnP in Windows XP Example

This section shows you how to use the UPnP feature in Windows XP. You must already have UPnP installed in Windows XP and UPnP activated on the CellPipe 7130 RG.

Make sure the computer is connected to a LAN port of the CellPipe 7130 RG. Turn on your computer and the CellPipe 7130 RG.

Auto-discover Your UPnP-enabled Network Device

- 1 Click **Start** and **Control Panel**. Double-click **Network Connections**. An icon displays under Internet Gateway.

- 2 Right-click the icon and select **Properties**.

Figure 107 Network Connections



- 3 In the **Internet Connection Properties** window, click **Settings** to see the port mappings there were automatically created.

Figure 108 Internet Connection Properties



- 4 You may edit or delete the port mappings or click **Add** to manually add port mappings.

Figure 109 Internet Connection Properties: Advanced Settings

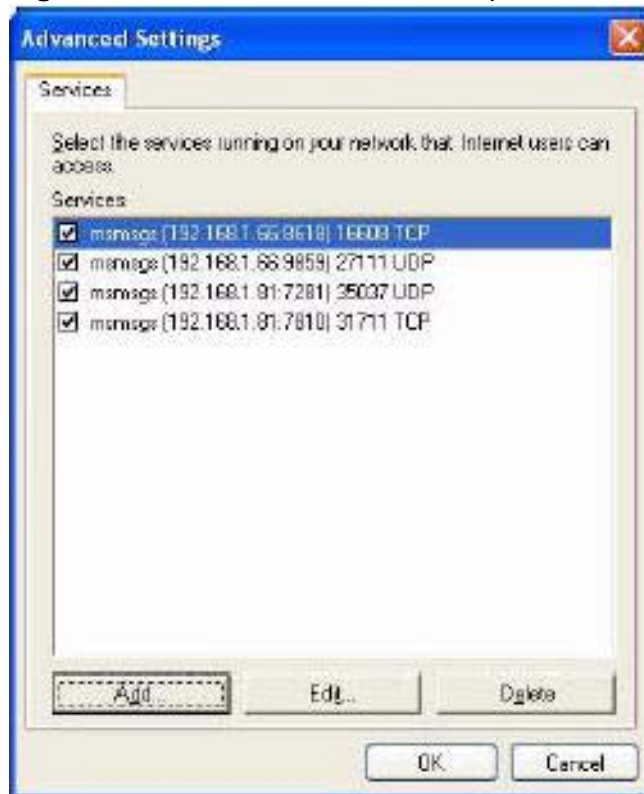
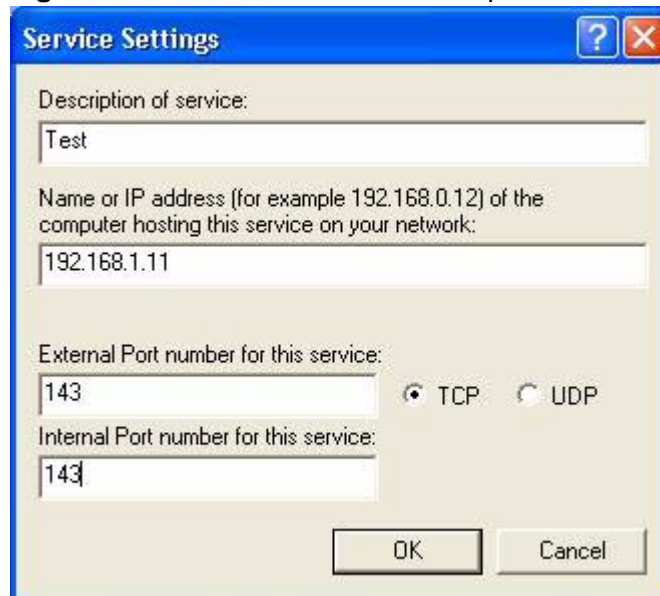


Figure 110 Internet Connection Properties: Advanced Settings: Add



- 5 When the UPnP-enabled device is disconnected from your computer, all port mappings will be deleted automatically.

- 6 Select **Show icon in notification area when connected** option and click **OK**. An icon displays in the system tray.

Figure 111 System Tray Icon



- 7 Double-click on the icon to display your current Internet connection status.

Figure 112 Internet Connection Status



Web Configurator Easy Access

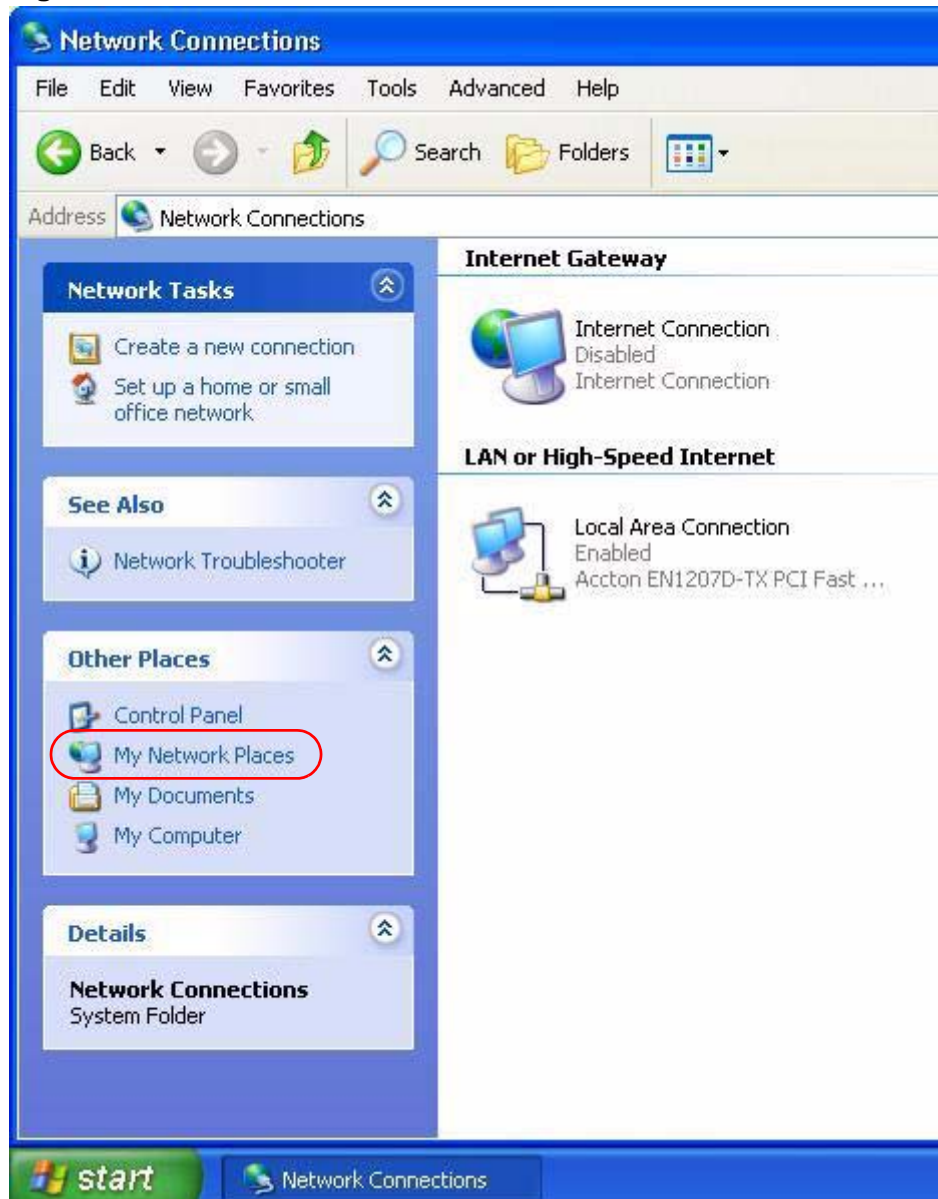
With UPnP, you can access the web-based configurator on the CellPipe 7130 RG without finding out the IP address of the CellPipe 7130 RG first. This comes helpful if you do not know the IP address of the CellPipe 7130 RG.

Follow the steps below to access the web configurator.

- 1 Click **Start** and then **Control Panel**.
- 2 Double-click **Network Connections**.

- 3 Select **My Network Places** under **Other Places**.

Figure 113 Network Connections



- 4 An icon with the description for each UPnP-enabled device displays under **Local Network**.

- 5 Right-click on the icon for your CellPipe 7130 RG and select **Invoke**. The web configurator login screen displays.

Figure 114 Network Connections: My Network Places



- 6 Right-click on the icon for your CellPipe 7130 RG and select **Properties**. A properties window displays with basic information about the CellPipe 7130 RG.

Figure 115 Network Connections: My Network Places: Properties: Example



Parental Control

20.1 Overview

Parental control allows you to block web sites with the specific URL. You can also define time periods and days during which the CellPipe 7130 RG performs parental control on a specific user.

20.1.1 What You Can Do in this Chapter

- The **Time Restriction** screen lets you give different time restrictions to each user of your network ([Section 20.2 on page 257](#)).
- The **Content Filter** screen lets you restrict home network users from viewing inappropriate websites ([Section 20.3 on page 259](#)).

20.2 The Time Restriction Screen

Use this screen to view the schedules and enable parental control on a specific user during certain periods.

Click **Advanced Setup > Parental Control** to open the following screen.

Figure 116 Parental Control > Time restriction

#	Active	username	MAC	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start	Stop	Modify
1	<input checked="" type="checkbox"/>	Child1	aa:bb:ff:ff:bb:11	x	x	x	x			x	20:00	21:00	

The following table describes the fields in this screen.

Table 84 Parental Control > Time Restriction

LABEL	DESCRIPTION
#	This shows the index number of the schedule.
Active	Select the check box to enable the schedule.
username	This shows the name of the user.
MAC	This shows the MAC address of the LAN user's computer to which this schedule applies.
Mon ~ Sun	x indicates the day(s) on which parental control is enabled.
Start	This shows the time when the schedule starts.
Stop	This shows the time when the schedule ends.
Modify	Click the Edit icon to go to the screen where you can edit the schedule. Click the Remove icon to delete an existing schedule.
Add	Click Add to create a new schedule.
Apply	Click Apply to save your changes back to the CellPipe 7130 RG.

20.2.1 Adding a Schedule

Click the **Add** button in the **Time Restriction** screen to open the following screen. Use this screen to configure a restricted access schedule for a specific user on your network.

Figure 117 Time Restriction Configuration

Add Access Time Restriction

This page adds time of day restriction to a special LAN device connected to the Router. To restrict the LAN device, enter the MAC address of the LAN device. To find out the MAC address of a Windows based PC, go to command window and type "ipconfig /all".

User Name

MAC Address

Days of the week	Mon	Tue	Wed	Thu	Fri	Sat	Sun
Click to select	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Start Blocking Time (hh:mm)

End Blocking Time (hh:mm)

.....

The following table describes the fields in this screen.

Table 85 Time Restriction Configuration

LABEL	DESCRIPTION
User Name	Enter the name of the user.
MAC Address	Enter the MAC address of the LAN user's computer to which this schedule applies.
Days of the week	Select check boxes for the days that you want the CellPipe 7130 RG to perform parental control.
Start Blocking Time End Blocking Time	Enter the time period of each day, in 24-hour format, during which parental control will be enforced.
Back	Click this button to return to the previous screen without saving any changes.
Save/Apply	Click this button to save your settings back to the CellPipe 7130 RG.

20.3 The Content Filter Screen

Use this screen to configure filtering settings to block the users on your network from accessing certain web sites.

Click **Advanced Setup > Parental Control > Content Filter** to open the following screen.

Figure 118 Parental Control > Content Filter

Content Filter

A maximum 100 entries can be configured.

Active Filter

Blocking list

#	Active	Keyword	Port	Modify
1	<input checked="" type="checkbox"/>	guns	80	

.....

The following table describes the fields in this screen.

Table 86 Parental Control >Content Filter

LABEL	DESCRIPTION
Active Filter	Select the check box to enable URL filtering on the CellPipe 7130 RG.
Blocking list	The table shows the keywords contained in the URL that the CellPipe 7130 RG prohibits the users from viewing. It also shows through which port the keyword is blocked.
#	This is the index number of the rule.
Active	Select the check box to enable the filtering rule.
Keyword	This is the keyword that is blocked in this rule.
Port	This is the port number the web server uses to forward HTTP traffic.
Modify	Click the Edit icon to go to the screen where you can edit the rule. Click the Remove icon to delete an existing rule.
Add	Click Add to create a new rule.
Apply	Click this button to save your settings back to the CellPipe 7130 RG.

20.3.1 Adding Filter Rule

Click the **Add** button in the **URL Filter** screen to open the following screen.

Figure 119 URL Filter Configuration

Add Filter Rule

Keyword :

Port Number: (Default 80 will be applied if leave blank.)

.....

The following table describes the fields in this screen.

Table 87 URL Filter Configuration

LABEL	DESCRIPTION
Keyword	Enter the keyword that the CellPipe 7130 RG blocks.
Port Number	Specify the port number the web server uses to forward HTTP traffic.
Back	Click this button to return to the previous screen without saving any changes.
Save/Apply	Click this button to save your settings back to the CellPipe 7130 RG.

21.1 Overview

This chapter discusses the IGMP screens.

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender to 1 recipient) or Broadcast (1 sender to everybody on the network). Multicast delivers IP packets to just a group of hosts on the network.

IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a multicast group - it is not used to carry user data. See RFC 1112 and RFC 2236 for information on IGMP versions 1 and 2, respectively.

21.1.1 What You Can Do in this Chapter

- The **IGMP** screen lets you select the IGMP version to use as well as configure the settings for IGMP ([Section 21.2 on page 263](#)).
- The **IGMP Source Configuration** screen lets you set the server where the CellPipe 7130 RG gets the multicast group information ([Section 21.2 on page 263](#)).

21.1.2 What You Need to Know

IP Multicast Addresses

In IPv4, a multicast address allows a device to send packets to a specific group of hosts (multicast group) in a different sub-network. A multicast IP address represents a traffic receiving group, not individual receiving devices. IP addresses in the Class D range (224.0.0.0 to 239.255.255.255) are used for IP multicasting. Certain IP multicast numbers are reserved by IANA for special purposes (see the IANA web site for more information).

IGMP Snooping

A layer-2 switch can passively snoop on IGMP Query, Report and Leave (IGMP version 2) packets transferred between IP multicast routers/switches and IP multicast hosts to learn the IP multicast group membership. It checks IGMP

packets passing through it, picks out the group registration information, and configures multicasting accordingly. IGMP snooping allows the CellPipe 7130 RG to learn multicast groups without you having to manually configure them.

The CellPipe 7130 RG forwards multicast traffic destined for multicast groups (that it has learned from IGMP snooping or that you have manually configured) to ports that are members of that group. The CellPipe 7130 RG discards multicast traffic destined for multicast groups that it does not know. IGMP snooping generates no additional network traffic, allowing you to significantly reduce multicast traffic passing through your device.

IGMP Proxy

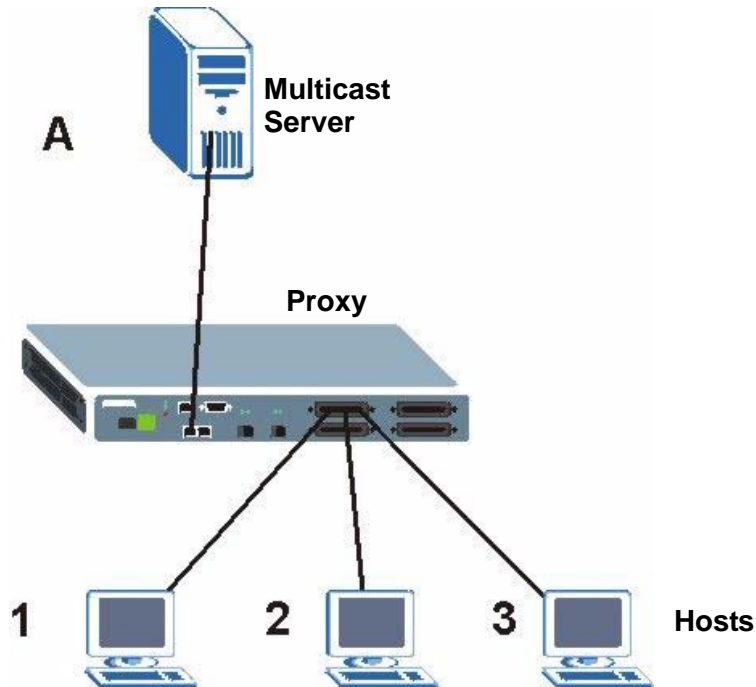
To allow better network performance, you can use IGMP proxy instead of a multicast routing protocol in a simple tree network topology.

Note: Your CellPipe 7130 RG is an IGMP proxy.

In IGMP proxy, an upstream interface is the port that is closer to the source (or the root of the multicast tree) and is able to receive multicast traffic. There should only be one upstream interface (also known as the query port) for one query VLAN on the CellPipe 7130 RG. A downstream interface is a port that connects to a host (such as a computer).

The following figure shows a network example where **A** is the multicast source while computers 1, 2 and 3 are the receivers. In the figure **A** is connected to the upstream interface and 1, 2 and 3 are connected to the downstream interface.

Figure 120 IGMP Proxy Network Example



The CellPipe 7130 RG will not respond to IGMP join and leave messages on the upstream interface. The CellPipe 7130 RG only responds to IGMP query messages on the upstream interface. The CellPipe 7130 RG sends IGMP query messages to the hosts that are members of the query VLAN.

The CellPipe 7130 RG only sends an IGMP leave message via the upstream interface when the last host leaves a multicast group.

21.2 The IGMP Screen

Use this screen to select the IGMP version to use as well as configure the settings for IGMP.

Click **Advanced Setup > IGMP** to open the following screen.

Figure 121 IGMP

The screenshot shows the 'IGMP Source Configuration' screen. It features a title bar with 'IGMP' and 'IGMP Source Configuration' tabs. Below the title bar, the 'IGMP Configuration' section contains the following fields and values:

- Version: IGMP-v3 (dropdown menu)
- Query Interval (seconds): 125
- Query Response Time (0.1 sec): 10
- Last Member Query Response Time (0.1 sec): 10
- Robustness Value: 2
- Maximum Multicast Groups: 10
- Maximum Multicast Data Sources (for IGMPv3): 10
- Maximum Multicast Group Members: 32
- Fast Leave Enable:

An 'Apply' button is located at the bottom right of the configuration area.

The following table describes the fields in this screen.

Table 88 IGMP

LABEL	DESCRIPTION
Version	There are three versions of IGMP. IGMP version 2 and 3 are improvements over version 1, but IGMP version 1 is still in wide use. IGMP version 3 supports source address filtering, reporting or ignoring traffic from specific source address to a particular host on the network. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236. Select the IGMP version that you would like the CellPipe 7130 RG to use.
Query Interval	Specify how many seconds since the last query the CellPipe 7130 RG waits before it queries all directly connected networks to gather multicast group membership.
Query Response Time	Specify how many seconds the host allots for gathering membership information from directly connected networks before it sends a report.
Last Member Query Response Time	Specify how many seconds the host allots for gathering membership information from a specific IP address before it sends a report.
Robustness Value	This is the number of times the host sends a report to the CellPipe 7130 RG when the CellPipe 7130 RG queries for the host's status.
Maximum Multicast Groups	Enter the number of multicast groups that the CellPipe 7130 RG is allowed to join.
Maximum Multicast Data Sources (for IGMPv3)	This is the maximum number of multicast servers that the host can handle.

Table 88 IGMP (continued)

LABEL	DESCRIPTION
Maximum Multicast Group Members	This is the maximum number of members allowed for a multicast group.
Fast Leave Enable	Enable this to have the host stop sending multicast messages to an IP address that has left the multicast group or a multicast group with no members.
Apply	Click this button to save your settings back to the CellPipe 7130 RG.

21.3 Interface Source Configuration

Use this screen to configure the server where the CellPipe 7130 RG gets the multicast group information. Click **Advanced > IGMP Source Configuration** to open the following screen.

Figure 122 IGMP Source Configuration

The screenshot shows the 'IGMP Source Configuration' screen. At the top, there are two tabs: 'IGMP' and 'IGMP Source Configuration'. Below the tabs, the title 'IGMP Source Configuration' is displayed. A checkbox labeled 'Active Source List' is checked. Below this is a table with the following data:

#	Active	Address	Modify
1	<input checked="" type="checkbox"/>	192.168.1.1	

Below the table, there are two buttons: 'Add' and 'Apply'.

The following table describes the fields in this screen.

Table 89 IGMP Source Configuration

LABEL	DESCRIPTION
Active Source List	Check this to stop having the CellPipe 7130 RG act as an IGMP proxy. Deselect this to have the CellPipe 7130 RG act as an IGMP proxy and then create the IP address(es) of the actual IGMP multicast servers.
#	This is the index number of the server.
Active	Enable this to use the server as the IGMP source configuration.
Address	This is the IP address of the server that has the multicast group membership information that the host will use.
Modify	Click the Edit icon to change the entry. Click the Delete icon to delete the entry,

Table 89 IGMP Source Configuration (continued)

LABEL	DESCRIPTION
Add	Click this button to create a new rule.
Apply	Click this button to save your settings back to the CellPipe 7130 RG.

21.3.1 Add/Edit IGMP Source

Click the **Add** button or **Edit** icon in the **IGMP Source Configuration** screen to open the following. Use this screen to add or edit an IGMP source entry.

Figure 123 Interface Grouping Criteria

The screenshot shows a 'Rule Setup' window. At the top left, there is a checked checkbox labeled 'Active'. Below it is the label 'Address' followed by a text input field containing the IP address '0.0.0.0'. A horizontal dotted line separates the input fields from the bottom of the window, which contains two buttons: 'Back' and 'Apply'.

The following table describes the fields in this screen.

Table 90 Interface Grouping Criteria

LABEL	DESCRIPTION
Active	This shows whether the entry is active or not.
Address	Enter the IP address of the server that has the multicast grouping information that the host will use.
Back	Click this button to return to the previous screen without saving any changes.
Apply	Click this button to save your settings back to the CellPipe 7130 RG.

System Settings

22.1 Overview

This chapter shows you how to configure system related settings, such as system time, password, name, the domain name and the inactivity timeout interval.

22.1.1 What You Can Do in this Chapter

- The **General** screen lets you configure system settings ([Section 22.2 on page 267](#)).
- The **Time Setting** screen lets you set the system time ([Section 22.3 on page 269](#)).

22.2 The General Screen

Use the **General** screen to configure system settings such as the system password.

Click **Maintenance > System** to open the **General** screen.

Figure 124 Maintenance > System > General

The screenshot shows a web interface for system settings. At the top, there are two tabs: 'General' and 'Time Setting'. The 'General' tab is active. Below the tabs, there are two main sections. The first section is titled 'UserName/Password' and contains four input fields: 'UserName' (with the value 'admin'), 'Old Password', 'New Password', and 'Retype to Confirm'. Below these fields is a warning icon (a yellow triangle with an exclamation mark) followed by the text: 'Caution: Please record your new password whenever you change it. The system will lock you out if you have forgotten your password.' The second section is titled 'Web Session Timeout' and contains one input field: 'Timeout Value (sec)' with the value '300'. At the bottom of the form are two buttons: 'Apply' and 'Cancel'.

The following table describes the labels in this screen.

Table 91 Maintenance > System > Genera

LABEL	DESCRIPTION
UserName/ Password	
UserName	Type the user name you use to access the system.
Old Password	Type the default password or the existing password you use to access the system in this field.
New Password	Type your new system password (up to 30 characters). Note that as you type a password, the screen displays a (*) for each character you type. After you change the password, use the new password to access the CellPipe 7130 RG.
Retype to Confirm	Type the new password again for confirmation.
Web Session Timeout	
Timeout Value (sec)	Enter how many minutes of inactivity the CellPipe 7130 RG waits before automatically disconnecting a session. You need to enter the username and password again before accessing the Web Configurator.
Apply	Click Apply to save your changes back to the CellPipe 7130 RG.
Cancel	Click Cancel to begin configuring this screen afresh.

22.3 The Time Setting Screen

To change your CellPipe 7130 RG's time and date, click **Maintenance > System > Time Setting**. The screen appears as shown. Use this screen to configure the CellPipe 7130 RG's time based on your local time zone.

Figure 125 Maintenance > System > Time Setting

The following table describes the fields in this screen.

Table 92 Maintenance > System > Time Setting

LABEL	DESCRIPTION
Current Time	
Current Time	This field displays the time of your CellPipe 7130 RG. Each time you reload this page, the CellPipe 7130 RG synchronizes the time with the time server.
Current Date	This field displays the date of your CellPipe 7130 RG. Each time you reload this page, the CellPipe 7130 RG synchronizes the date with the time server.
Time and Date Setup	
Manual	Select this option to enter the time and date manually.
Get from Time Server	Select this option to have the CellPipe 7130 RG get the time and date from the time server you specified below.

Table 92 Maintenance > System > Time Setting (continued)

LABEL	DESCRIPTION
First NTP time server Second NTP time server Third NTP time server Fourth NTP time server Fifth NTP time server	Select an NTP time server from the drop-down list box. Otherwise, select Other and enter the IP address or URL (up to 20 extended ASCII characters in length) of your time server. Select None if you don't want to configure the time server. Check with your ISP/network administrator if you are unsure of this information.
Time zone offset	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Apply	Click Apply to save your changes back to the CellPipe 7130 RG.
Cancel	Click Cancel to begin configuring this screen afresh.

23.1 Overview

This chapter contains information about configuring general log settings and viewing the CellPipe 7130 RG's logs.

The web configurator allows you to choose which categories of events and/or alerts to have the CellPipe 7130 RG log and then display the logs or have the CellPipe 7130 RG send them to a syslog server.

23.1.1 What You Can Do in this Chapter

- The **View Log** screen lets you see the logs for the categories that you selected in the **Log Settings** screen ([Section 23.2 on page 271](#)).
- The **Log Settings** screen lets you configure to where the CellPipe 7130 RG is to send logs and which logs and/or immediate alerts the CellPipe 7130 RG is to record ([Section 23.3 on page 272](#)).

23.2 The View Log Screen

Click **Maintenance > Logs** to open the **View Log** screen. Use the **View Log** screen to see the logs for the categories that you selected in the **Log Settings** screen (see [Section 23.3 on page 272](#)).

The log wraps around and deletes the old entries after it fills.

Figure 126 Maintenance > Logs > View Log

The following table describes the fields in this screen.

Table 93 Maintenance > Logs > View Log

LABEL	DESCRIPTION
Display	Select a severity level of logs to view. The CellPipe 7130 RG displays the logs with the severity level equal to or higher than what you selected.
#	This field is a sequential value and is not associated with a specific entry.
Date/Time	This field displays the time the log was recorded.
Severity	This field displays the severity level of the log.
System	This field displays the system module from which the logs come.
Message	This field states the reason for the log.

23.3 The Log Settings Screen

Use the **Log Settings** screen to configure to where the CellPipe 7130 RG is to send logs and which logs and/or immediate alerts the CellPipe 7130 RG is to record and display.

To change your CellPipe 7130 RG's log settings, click **Maintenance > Logs > Log Settings**. The screen appears as shown.

Figure 127 Maintenance > Logs > Log Settings

The following table describes the fields in this screen.

Table 94 Maintenance > Logs > Log Settings

LABEL	DESCRIPTION
Active	Select to enable or disable system logging.
Log Level	Select the severity level of the logs that you want the CellPipe 7130 RG to display, record and send to the log server. The CellPipe 7130 RG displays and records the logs with the severity level equal to or higher than what you selected.
Mode	Select Local to record the logs and store them in the local memory of the CellPipe 7130 RG only. Select Remote to send logs to the specified log server. Select Both to record the logs and store them in the local memory and also send logs to the log server.
Syslog Server IP Address	Enter the server name or the IP address of the log server.
Syslog Server UDP Port	Enter the UDP port of the log server.
Apply	Click Apply to save your customized settings.

Do not interrupt the file transfer process as this may PERMANENTLY DAMAGE your CellPipe 7130 RG.

24.1 Overview

This chapter explains how to upload new firmware, manage configuration files and restart your CellPipe 7130 RG.

Use the instructions in this chapter to change the device's configuration file or upgrade its firmware. After you configure your device, you can backup the configuration file to a computer. That way if you later misconfigure the device, you can upload the backed up configuration file to return to your previous settings. You can alternately upload the factory default configuration file if you want to return the device to the original default settings. The firmware determines the device's available features and functionality.

Only use firmware for your device's specific model. Refer to the label on the bottom of your CellPipe 7130 RG.

24.1.1 What You Can Do in this Chapter

- The **Firmware** screen lets you upload firmware to your device ([Section 24.2 on page 276](#)).
- The **Configuration** screen lets you backup and restore device configurations ([Section 24.3 on page 278](#)). You can also reset your device settings back to the factory default.
- The **Restart** screen lets you restart your CellPipe 7130 RG ([Section 24.4 on page 280](#)).

24.2 The Firmware Screen

Click **Maintenance > Tools** to open the **Firmware** screen. Follow the instructions in this screen to upload firmware to your CellPipe 7130 RG. The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot.

Do NOT turn off the CellPipe 7130 RG while firmware upload is in progress!

Figure 128 Maintenance > Tools > Firmware

The screenshot shows a web interface with three tabs: **Firmware**, **Configuration**, and **Restart**. The **Firmware** tab is active. Below the tabs, the heading is **Firmware Upgrade**. The main content area contains the following text:

To upgrade the internal router firmware, browse to the location of the binary (.BIN) upgrade file and click **Upload**. Upgrade files can be downloaded from website. If the upgrade file is compressed (.ZIP file), you must first extract the binary (.BIN) file. In some cases, you may need to reconfigure.

NOTE: The update process takes about 2 minutes to complete, and the DSL Router will reboot.

Current Firmware Version: **0.0.01.GEN**

File Path:

.....

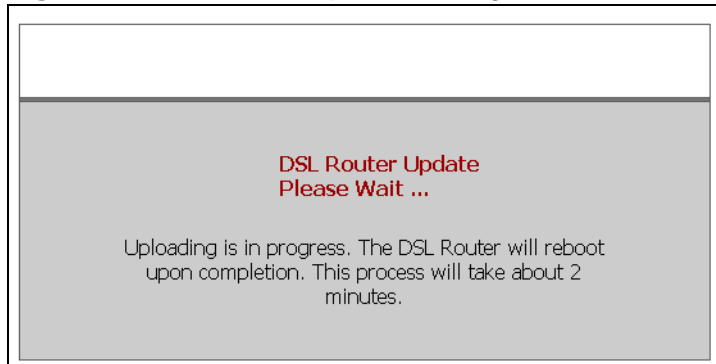
The following table describes the labels in this screen.

Table 95 Maintenance > Tools > Firmware

LABEL	DESCRIPTION
Current Firmware Version	This is the present Firmware version and the date created.
File Path	Type in the location of the file you want to upload in this field or click Browse ... to find it.
Browse...	Click Browse... to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click Upload to begin the upload process. This process may take up to two minutes.

After you see the **Firmware Upload in Progress** screen, wait two minutes before logging into the CellPipe 7130 RG again.

Figure 129 Firmware Upload In Progress



The CellPipe 7130 RG automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

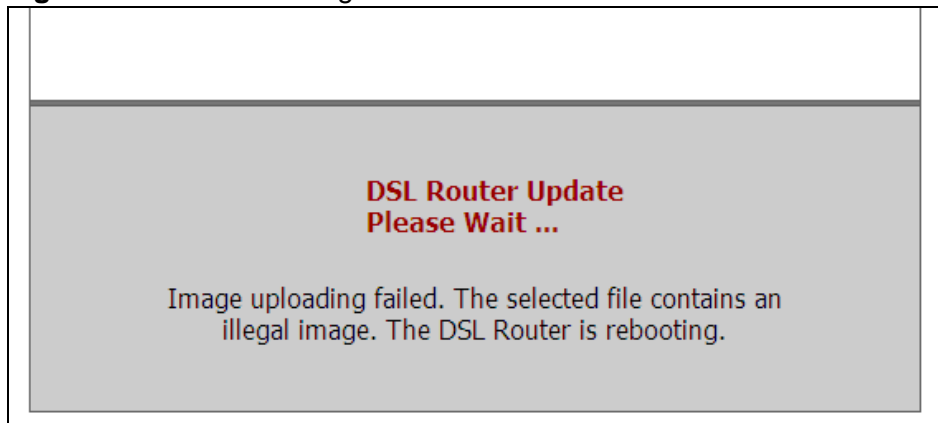
Figure 130 Network Temporarily Disconnected



After two minutes, log in again and check your new firmware version in the **Status** screen.

If the upload was not successful, the following screen will appear. Click **Tools** to go back to the **Firmware** screen.

Figure 131 Error Message



24.3 The Configuration Screen

Click **Maintenance > Tools > Configuration**. Information related to factory defaults, backup configuration, and restoring configuration appears in this screen, as shown next.

Figure 132 Maintenance > Tools > Configuration

The screenshot shows a web interface with three tabs: 'Firmware', 'Configuration' (selected), and 'Restart'. The 'Configuration' section is active and contains three main areas:

- Backup Configuration:** A text instruction 'Click **Backup** to save the current configuration of your system to your computer.' followed by a 'Backup' button.
- Restore Configuration:** A text instruction 'To restore a previously saved configuration file to your system, browse to the location of the configuration file and click **Upload**.' followed by a 'File Path' input field, a 'Browse...' button, and an 'Upload' button.
- Back to Factory Defaults:** A text instruction 'Click **Reset** to clear all user-entered configuration information and return to factory defaults.' followed by a 'Reset' button.

Backup Configuration

Backup Configuration allows you to back up (save) the CellPipe 7130 RG's current configuration to a file on your computer. Once your CellPipe 7130 RG is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Click **Backup** to save the CellPipe 7130 RG's current configuration to your computer.

Restore Configuration

Restore Configuration allows you to upload a new or previously saved configuration file from your computer to your CellPipe 7130 RG.

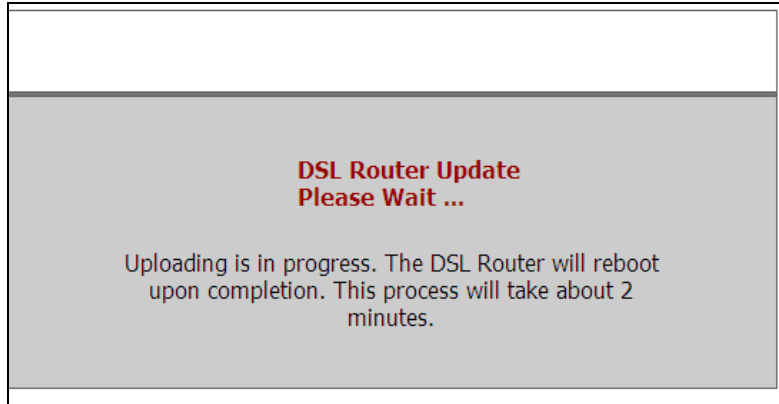
Table 96 Restore Configuration

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click Browse ... to find it.
Browse...	Click Browse... to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload	Click Upload to begin the upload process.

Do not turn off the CellPipe 7130 RG while configuration file upload is in progress.

After you see a “restore configuration successful” screen, you must then wait one minute before logging into the CellPipe 7130 RG again.

Figure 133 Configuration Upload Successful



The CellPipe 7130 RG automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

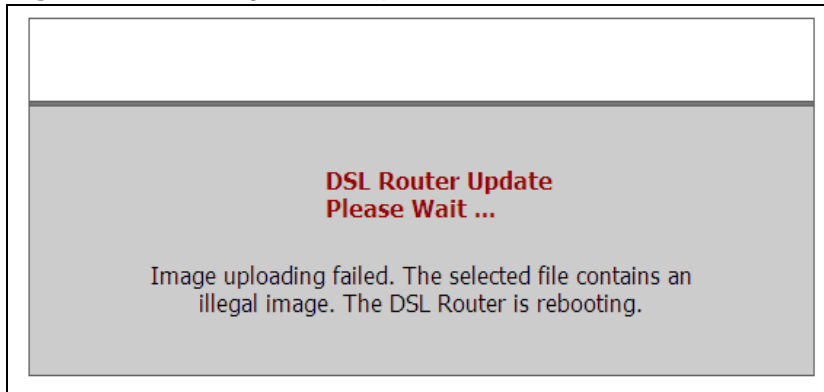
Figure 134 Network Temporarily Disconnected



If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default device IP address (192.168.1.1). See [Appendix B on page 321](#) for details on how to set up your computer's IP address.

If the upload was not successful, the following screen will appear. Click **Tools > Configuration** to go back to the **Configuration** screen.

Figure 135 Configuration Upload Error



Reset to Factory Defaults

Click the **Reset** button to clear all user-entered configuration information and return the CellPipe 7130 RG to its factory defaults. The following warning screen appears.

Figure 136 Reset Warning Message



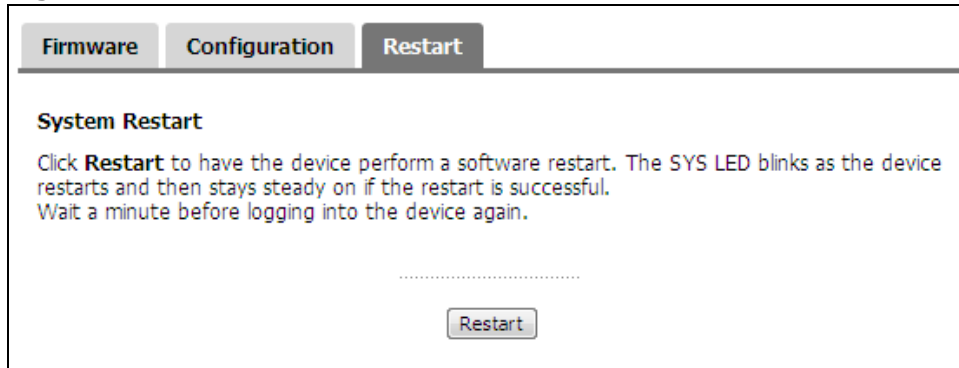
You can also press the **RESET** button on the rear panel to reset the factory defaults of your CellPipe 7130 RG. Refer to [Section 1.7 on page 28](#) for more information on the **RESET** button.

24.4 The Restart Screen

System restart allows you to reboot the CellPipe 7130 RG without turning the power off.

Click **Maintenance > Tools > Restart**. Click **Restart** to have the CellPipe 7130 RG reboot. This does not affect the CellPipe 7130 RG's configuration.

Figure 137 Maintenance > Tools >Restart



Diagnostic

25.1 Overview

The **Diagnostic** screens display information to help you identify problems with the CellPipe 7130 RG.

The route between a CO VDSL switch and one of its CPE may go through switches owned by independent organizations. A connectivity fault point generally takes time to discover and impacts subscriber's network access. In order to eliminate the management and maintenance efforts, IEEE 802.1ag is a Connectivity Fault Management (CFM) specification which allows network administrators to identify and manage connection faults. Through discovery and verification of the path, CFM can detect, analyze and isolate connectivity faults in bridged LANs.

25.1.1 What You Can Do in this Chapter

- The **General** screen lets you ping an IP address or trace the route packets take to a host ([Section 25.3 on page 284](#)).
- The **802.1ag** screen lets you perform CFM actions ([Section 25.4 on page 285](#)).
- The **OAM Ping Test** screen lets you send an ATM OAM (Operation, Administration and Maintenance) packet to verify the connectivity of a specific PVC. ([Section 25.4 on page 285](#))

25.2 What You Need to Know

The following terms and concepts may help as you read through this chapter.

How CFM Works

A Maintenance Association (MA) defines a VLAN and associated Maintenance End Point (MEP) ports on the device under a Maintenance Domain (MD) level. An MEP port has the ability to send Connectivity Check Messages (CCMs) and get other MEP ports information from neighbor devices' CCMs within an MA.

CFM provides two tests to discover connectivity faults.

- Loopback test - checks if the MEP port receives its Loop Back Response (LBR) from its target after it sends the Loop Back Message (LBM). If no response is received, there might be a connectivity fault between them.
- Link trace test - provides additional connectivity fault analysis to get more information on where the fault is. If an MEP port does not respond to the source MEP, this may indicate a fault. Administrators can take further action to check and resume services from the fault according to the line connectivity status report.

25.3 The General Diagnostic Screen

Click **Maintenance > Diagnostic** to open the screen shown next. Ping and traceroute help check availability of remote hosts and also help troubleshoot network or Internet connections.

Figure 138 Maintenance > Diagnostic > General

The following table describes the fields in this screen.

Table 97 Maintenance > Diagnostic > General

LABEL	DESCRIPTION
TCP/IP Address	Type the IP address of a computer that you want to ping in order to test a connection or trace the route packets take to.
Ping	Click this button to ping the IP address that you entered.
Traceoute	Click this button to perform the traceroute function. This determines the path a packet takes to the specified host.

25.4 The 802.1ag Screen

Click **Diagnostic** to open the following screen. Use this screen to perform CFM actions.

Figure 139 802.1ag

The following table describes the fields in this screen.

Table 98 Maintenance > Diagnostic > 802.1ag

LABEL	DESCRIPTION
802.1ag Connectivity Fault Management	
Maintenance Domain (MD) Name	Type a name of up to 39 printable English keyboard characters for this MD. The combined length of the MD Name and MA name must be less or equal to 44bytes.
Maintenance Domain (MD) Level	Select a level (0-7) under which you want to create an MA.

Table 98 Maintenance > Diagnostic > 802.1ag (continued)

LABEL	DESCRIPTION
Maintenance Association (MA) Name	<p>Type a name of up to 39 printable English keyboard characters for this MA.</p> <p>The combined length of the MD Name and MA name must be less or equal to 44bytes.</p>
Maintenance Association (MA) Format	<p>Select the format which the CellPipe 7130 RG uses to send this MA information in the domain (MD). Options are VID, String and Integer.</p> <p>If you select VID or Integer, the CellPipe 7130 RG adds the VLAN ID you specified for an MA in the CCM.</p> <p>If you select String, the CellPipe 7130 RG adds the MA name you specified above in the CCM.</p> <p>Note: The MEPs in the same MA should use the same MA format.</p>
Destination MAC Address	Enter the target device's MAC address to which the CellPipe 7130 RG performs a CFM loopback test.
Count	Set how many times the CellPipe 7130 RG send loopback messages (LBMs).
802.1Q VLAN ID	Type a VLAN ID (0-4095) for this MA.
Maintenance End Point ID	Enter an ID number (1-8191) for this MEP port. Each MEP port needs a unique ID number within an MD. The MEP ID is to identify an MEP port used when you perform a CFM action
Status	
Continuity Check Message (CCM)	This shows how many Connectivity Check Messages (CCMs) are sent and if there is any invalid CCM or cross-connect CCM.
Loopback Message (LBM)	This shows how many Loop Back Messages (LBMs) are sent and if there is any in-order or out-of-order Loop Back Response (LBR) received from a remote MEP.
Linktrace Message (LTM)	This shows the destination MAC address in the Link Trace Response (LTR).
Save	Click this to save your changes back to the CellPipe 7130 RG.
Enable CCM	Click this button to have the selected MEP send Connectivity Check Messages (CCMs) to other MEPs.
Disable CCM	Click this button to disallow the selected MEP to send Connectivity Check Messages (CCMs) to other MEPs.
Update CC status	Click this button to reload the test result.
Send Loopback	Click this button to have the selected MEP send the LBM (Loop Back Message) to a specified remote end point.
Send Linktrace	Click this button to have the selected MEP send the LTMs (Link Trace Messages) to a specified remote end point.

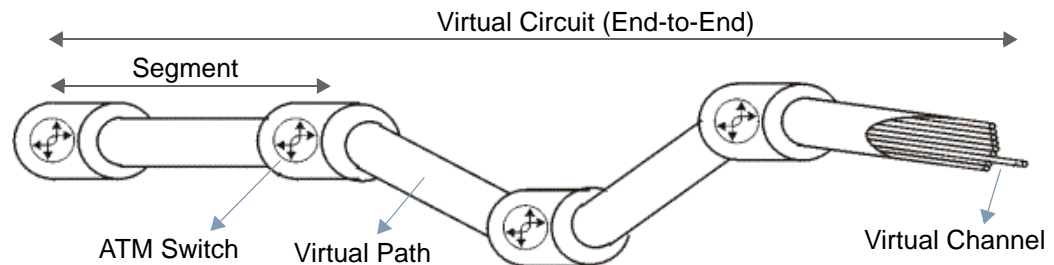
25.5 The OAM Ping Test Screen

Click **Maintenance > Diagnostic > OAM Ping Test** to open the screen shown next. Use this screen to perform an OAM (Operation, Administration and Maintenance) F4 or F5 loopback test on a PVC. The CellPipe 7130 RG sends an OAM F4 or F5 packet to the DSLAM or ATM switch and then returns it to the CellPipe 7130 RG. The test result then displays in the text box.

ATM sets up virtual circuits over which end systems communicate. The terminology for virtual circuits is as follows:

- Virtual Channel (VC) Logical connections between ATM devices
- Virtual Path (VP) A bundle of virtual channels
- Virtual Circuits A series of virtual paths between circuit end points

Figure 140 Virtual Circuit Topology



Think of a virtual path as a cable that contains a bundle of wires. The cable connects two points and wires within the cable provide individual circuits between the two points. In an ATM cell header, a VPI (Virtual Path Identifier) identifies a link formed by a virtual path; a VCI (Virtual Channel Identifier) identifies a channel within a virtual path. A series of virtual paths make up a virtual circuit.

F4 cells operate at the virtual path (VP) level, while F5 cells operate at the virtual channel (VC) level. F4 cells use the same VPI as the user data cells on VP connections, but use different predefined VCI values. F5 cells use the same VPI and VCI as the user data cells on the VC connections, and are distinguished from data cells by a predefined Payload Type Identifier (PTI) in the cell header. Both F4 flows and F5 flows are bidirectional and have two types.

- segment F4 flows (VCI=3)
- end-to-end F4 flows (VCI=4)
- segment F5 flows (PTI=100)
- end-to-end F5 flows (PTI=101)

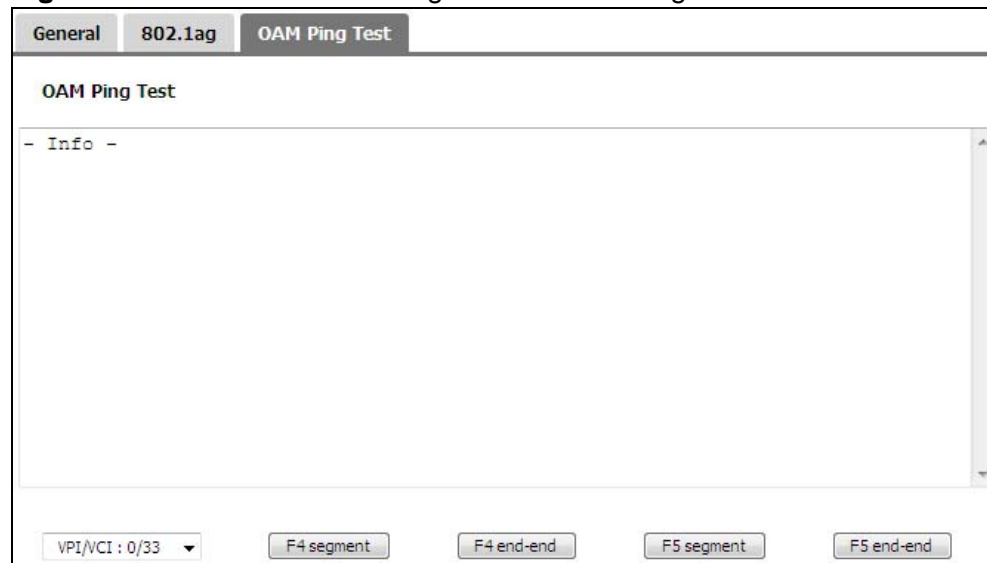
OAM F4 or F5 tests are used to check virtual path or virtual channel availability between two DSL devices. Segment flows are terminated at the connecting point

which terminates a VP or VC segment. End-to-end flows are terminated at the end point of a VP or VC connection, where an ATM link is terminated. Segment loopback tests allow you to verify integrity of a PVC to the nearest neighboring ATM device. End-to-end loopback tests allow you to verify integrity of an end-to-end PVC.

Note: The DSLAM to which the CellPipe 7130 RG is connected must also support ATM F4 and/or F5 to use this test.

Note: This screen is available only when you configure an ATM layer-2 interface.

Figure 141 Maintenance > Diagnostic > OAM Ping Test



The following table describes the fields in this screen.

Table 99 Maintenance > Diagnostic > OAM Ping Test

LABEL	DESCRIPTION
	Select a PVC on which you want to perform the loopback test.
F4 segment	Press this to perform an OAM F4 segment loopback test.
F4 end-end	Press this to perform an OAM F4 end-to-end loopback test.
F5 segment	Press this to perform an OAM F5 segment loopback test.
F5 end-end	Press this to perform an OAM F5 end-to-end loopback test.

Troubleshooting

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- [Power, Hardware Connections, and LEDs](#)
- [CellPipe 7130 RG Access and Login](#)
- [Internet Access](#)
- [USB Device Connection](#)
- [Wireless LAN Troubleshooting](#)

26.1 Power, Hardware Connections, and LEDs

The CellPipe 7130 RG does not turn on. None of the LEDs turn on.

- 1 Make sure the CellPipe 7130 RG is turned on.
- 2 Make sure you are using the power adaptor or cord included with the CellPipe 7130 RG.
- 3 Make sure the power adaptor or cord is connected to the CellPipe 7130 RG and plugged in to an appropriate power source. Make sure the power source is turned on.
- 4 Turn the CellPipe 7130 RG off and on.
- 5 If the problem continues, contact the vendor.

One of the LEDs does not behave as expected.

- 1 Make sure you understand the normal behavior of the LED. See [Section 1.6 on page 26](#).
- 2 Check the hardware connections. See the Quick Start Guide.
- 3 Inspect your cables for damage. Contact the vendor to replace any damaged cables.
- 4 Turn the CellPipe 7130 RG off and on.
- 5 If the problem continues, contact the vendor.

26.2 CellPipe 7130 RG Access and Login

Note: Refer to [Section 3.2 on page 83](#) for user level information. Each user level has its own account information for logging into the CellPipe 7130 RG.

I forgot the IP address for the CellPipe 7130 RG.

- 1 The default IP address is **http://192.168.1.1**.
- 2 If you changed the IP address and have forgotten it, you might get the IP address of the CellPipe 7130 RG by looking up the IP address of the default gateway for your computer. To do this in most Windows computers, click **Start > Run**, enter **cmd**, and then enter **ipconfig**. The IP address of the **Default Gateway** might be the IP address of the CellPipe 7130 RG (it depends on the network), so enter this IP address in your Internet browser.
- 3 If this does not work, you have to reset the device to its factory defaults. See [Section 1.7 on page 28](#).

I forgot the password.

- 1 The default admin password is **telus** and the default user password is **admin**.

Note: Refer to [Section 3.2 on page 83](#) for user level information. Each user level has its own account information for logging into the CellPipe 7130 RG.

- 2 If this does not work, you have to reset the device to its factory defaults. See [Section 1.7 on page 28](#).

I cannot see or access the **Login** screen (or other screens) in the web configurator.

- 1 Make sure you are using the correct IP address.
 - The default IP address is **http://192.168.1.1**.
 - If you changed the IP address ([Section on page 135](#)), use the new IP address.
 - If you changed the IP address and have forgotten it, see the troubleshooting suggestions for [I forgot the IP address for the CellPipe 7130 RG](#).
- 2 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide.
- 3 Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled. See [Appendix C on page 351](#).
- 4 Reset the device to its factory defaults, and try to access the CellPipe 7130 RG with the default IP address. See [Section 1.7 on page 28](#).
- 5 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- If your computer is connected to the WAN port or is connected wirelessly, use a computer that is connected to an **ETHERNET** port.
- Try to access the CellPipe 7130 RG using another service, such as Telnet. If you can access the CellPipe 7130 RG, check the remote management settings and firewall rules to find out why the CellPipe 7130 RG does not respond to HTTPS.

I can see the **Login** screen, but I cannot log in to the CellPipe 7130 RG.

- 1 Make sure you have entered the user name and password correctly. The default admin user name is **admin** and default admin password is **telus**. These fields are case-sensitive, so make sure [Caps Lock] is not on.

Note: Refer to [Section 3.2 on page 83](#) for user level information. Each user level has its own account information for logging into the CellPipe 7130 RG.

- 2 Turn the CellPipe 7130 RG off and on.

- 3 If this does not work, you have to reset the device to its factory defaults. See [Section 26.1 on page 289](#).

I cannot Telnet to the CellPipe 7130 RG.

See the troubleshooting suggestions for [I cannot see or access the Login screen \(or other screens\) in the web configurator](#). Ignore the suggestions about your browser.

I cannot use FTP to upload / download the configuration file. / I cannot use FTP to upload new firmware.

See the troubleshooting suggestions for [I cannot see or access the Login screen \(or other screens\) in the web configurator](#). Ignore the suggestions about your browser.

I cannot access the CellPipe 7130 RG again after configuring a new interface group.

Make sure your computer is connected to a LAN port in the default group. Otherwise, you need to use the CellPipe 7130 RG's LAN IP address for the new group to access the CellPipe 7130 RG again.

26.3 Internet Access

I cannot access the Internet.

- 1 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and [Section 1.6 on page 26](#).
- 2 Make sure you entered your ISP account information correctly in the WAN screens. These fields are case-sensitive, so make sure [Caps Lock] is not on.

- 3 If you are trying to access the Internet wirelessly, make sure the wireless settings in the wireless client are the same as the settings in the AP.
- 4 Disconnect all the cables from your device, and follow the directions in the Quick Start Guide again.
- 5 If the problem continues, contact your ISP.

I cannot access the Internet through a DSL connection.

- 1 Check if you have set the **Network > WAN > Mode** screen to **DSL** to have the CellPipe 7130 RG use the DSL port for Internet access.
- 2 Make sure you configured a proper ATM or PTM layer-2 interface and WAN services with the Internet account information provided by your ISP.
- 3 If you set up a WAN connection using bridging service, make sure you turn off the DHCP feature in the **LAN** screen to have the clients get WAN IP addresses directly from your ISP's DHCP server.

I cannot access the Internet through an Ethernet WAN connection.

- 1 Check if you have set the **Network > WAN > Mode** screen to **WAN** to have the CellPipe 7130 RG use the Ethernet WAN port for Internet access.
- 2 Make sure you connect the Ethernet WAN port to a DSL modem or router in your network.
- 3 Make sure you configured a proper Ethernet layer-2 interface and WAN services with the Internet account information provided by your ISP.
- 4 If you set up a WAN connection using bridging service, make sure you turn off the DHCP feature in the **LAN** screen to have the clients get WAN IP addresses directly from your ISP's DHCP server.

I cannot connect to the Internet using a second DSL connection.

ADSL and VDSL connections cannot work at the same time. You can only use one type of DSL connection, either ADSL or VDSL connection at one time.

I cannot create multiple connections of the same type.

Your layer-2 interface must be in VLAN MUX Mode or MSC mode to create multiple WAN services for each connection.

I cannot access the Internet anymore. I had access to the Internet (with the CellPipe 7130 RG), but my Internet connection is not available anymore.

- 1 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and [Section 1.6 on page 26](#).
- 2 Turn the CellPipe 7130 RG off and on.
- 3 If the problem continues, contact your ISP.

The Internet connection is slow or intermittent.

- 1 There might be a lot of traffic on the network. Look at the LEDs, and check [Section 1.6 on page 26](#). If the CellPipe 7130 RG is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.
- 2 Check the signal strength. If the signal strength is low, try moving your computer closer to the CellPipe 7130 RG if possible, and look around to see if there are any devices that might be interfering with the wireless network (for example, microwaves, other wireless networks, and so on).
- 3 Turn the CellPipe 7130 RG off and on.
- 4 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Check the settings for QoS. If it is disabled, you might consider activating it. If it is enabled, you might consider raising or lowering the priority for some applications.

26.4 USB Device Connection

The CellPipe 7130 RG fails to detect my USB device.

- 1 Disconnect the USB device.
- 2 Reboot the CellPipe 7130 RG.
- 3 If you are connecting a USB hard drive that comes with an external power supply, make sure it is connected to an appropriate power source that is on.
- 4 Re-connect your USB device to the CellPipe 7130 RG.

26.5 Wireless LAN Troubleshooting

I cannot access the CellPipe 7130 RG or ping any computer from the WLAN (wireless AP or router).

- 1 Make sure the wireless LAN is enabled on the CellPipe 7130 RG.
- 2 Make sure the wireless adapter on the wireless station is working properly.
- 3 Make sure the wireless adapter installed on your computer is IEEE 802.11 compatible and supports the same wireless standard as the CellPipe 7130 RG.
- 4 Make sure your computer (with a wireless adapter installed) is within the transmission range of the CellPipe 7130 RG.
- 5 Check that both the CellPipe 7130 RG and your wireless station are using the same wireless and wireless security settings.
- 6 Check if MAC Filter is configured to deny wireless access to certain MAC addresses to the CellPipe 7130 RG. See [Chapter 7 Wireless LAN](#) in the User's Guide for more information.

I cannot use WDS connection.

- 1 You can use WDS only when WPS is disabled or wireless security is set to “No Security”, “WEP”, “WPA-PSK” or “WPA2-PSK”. The wireless security settings apply to both WDS links and the connections between the CellPipe 7130 RG and any wireless clients.
- 2 WDS is only compatible with other devices of the same model.

Product Specifications

The following tables summarize the CellPipe 7130 RG's hardware and firmware features.

27.1 Hardware Specifications

Table 100 Hardware Specifications

Dimensions	208 (W) x 178 (D) x 36 (H) mm
Weight	465 g
Power Specification	12 V 1.5 A
Power Input	100 ~ 240 VAC 50~60HZ
RESET Button	Restores factory defaults
WPS Button	at least 1 second: enable WPS (Wi-Fi Protected Setup)
WLAN Button	at least 1 second: enable wireless LAN
Antennas	One attached external dipole antenna, 2dBi
Built-in Switch	Four auto-negotiating, auto MDI/MDI-X 10/100 Mbps RJ-45 Ethernet ports
DSL Port	One RJ-11 connector over POTS
Giga Ethernet WAN Port	One RJ-45 connector for GBE WAN
HomePNA Coaxial Port	One port for HPNA v3.1 access, coax F type connector
USB Ports	One USB v2.0 port for file sharing
Operation Temperature	0° C ~ 40° C
Storage Temperature	-20° ~ 60° C
Operation Humidity	20% ~ 85% RH (non-condensing)
Storage Humidity	20% ~ 90% RH (non-condensing)

27.2 Firmware Specifications

Table 101 Firmware Specifications

Default IP Address	192.168.1.1
Default Subnet Mask	255.255.255.0 (24 bits)
Default User Name	admin root tech Note: Refer to Section 3.2 on page 83 for user level information. Each user level has its own account information for logging into the CellPipe 7130 RG.
Default Password	telus
DHCP Server IP Pool	192.168.1.33 to 192.168.1.132
Static Routes	16
Device Management	Use the web configurator to easily configure the rich range of features on the CellPipe 7130 RG.
Wireless Functionality (wireless devices only)	Allow the IEEE 802.11b, IEEE 802.11g and/or IEEE 802.11n wireless clients to connect to the CellPipe 7130 RG wirelessly. Enable wireless security (WEP, WPA(2), WPA(2)-PSK) and/or MAC filtering to protect your wireless network.
Firmware Upgrade	Download new firmware (when available) from the web site and use the web configurator to put it on the CellPipe 7130 RG. Note: Only upload firmware for your specific model!
Configuration Backup & Restoration	Make a copy of the CellPipe 7130 RG's configuration. You can put it back on the CellPipe 7130 RG later if you decide to revert back to an earlier configuration.
HomePNA (Home Phoneline Networking Alliance, also known as HPNA) 3.1	Extend your Internet connection to the coaxial outlets in your house. HPNA is a home networking technology for carrying data over existing coaxial cables and telephone wiring.
DLNA Server	The CellPipe 7130 RG is a DLNA-compliant media server that lets DLNA-compliant media clients play video, audio, and photo content files stored on the CellPipe 7130 RG. The DLNA (Digital Living Network Alliance) group of companies works to make products compatible and able to work in a home network in order to make digital living easy and seamless. DLNA clients play files stored on DLNA servers.
Port Forwarding	If you have a server (mail or web server for example) on your network, you can use this feature to let people access it from the Internet.

Table 101 Firmware Specifications (continued)

DHCP (Dynamic Host Configuration Protocol)	Use this feature to have the CellPipe 7130 RG assign IP addresses, an IP default gateway and DNS servers to computers on your network. Your device can also act as a surrogate DHCP server (DHCP Relay) where it relays IP address assignment from the actual real DHCP server to the clients.
Dynamic DNS Support	With Dynamic DNS (Domain Name System) support, you can use a fixed URL with a dynamic IP address. You must register for this service with a Dynamic DNS service provider.
IP Multicast	IP multicast is used to send traffic to a specific group of computers. The CellPipe 7130 RG supports versions 2 and 3 of IGMP (Internet Group Management Protocol) used to join multicast groups (see RFC 2236).
Time and Date	Get the current time and date from an external server when you turn on your CellPipe 7130 RG. You can also set the time manually. These dates and times are then used in logs.
Logs	Use logs for troubleshooting. You can send logs from the CellPipe 7130 RG to an external syslog server.
Universal Plug and Play (UPnP)	A UPnP-enabled device can dynamically join a network, obtain an IP address and convey its capabilities to other devices on the network.
QoS (Quality of Service)	You can efficiently manage traffic on your network by reserving bandwidth and giving priority to certain types of traffic and/or to particular computers.
Remote Management	This allows you to decide whether a service (HTTPS or FTP traffic for example) from a computer on a network (LAN or WAN for example) can access the CellPipe 7130 RG.
PPPoE Support (RFC2516)	PPPoE (Point-to-Point Protocol over Ethernet) emulates a dial-up connection. It allows your ISP to use their existing network configuration with newer broadband technologies such as ADSL. The PPPoE driver on your device is transparent to the computers on the LAN, which see only Ethernet and are not aware of PPPoE thus saving you from having to manage PPPoE clients on individual computers.
Other PPPoE Features	PPPoE idle time out PPPoE dial on demand
Packet Filters	Your device's packet filtering function allows added network security and management.

Table 101 Firmware Specifications (continued)

VDSL Standards	<p>ITU-T G.993.1 VDSL Annex A (North American) Standard</p> <p>ITU G.993.2 (2/06) VDSL2 Annex A (North American) Standard</p> <ul style="list-style-type: none"> • Corrigendum 1 (12/06) + Amendment 1 (4/07) + Amendment 1 Corrigendum 1 (7/07) • Corrigendum 2 (7/07) + Amendment 2 (2/08) + Amendment 4 (1/09) <p>Supported band plans:</p> <ul style="list-style-type: none"> • Plan 997 (symmetrical) • Plan 998 (asymmetrical) <p>Supported profiles: 8a, 8b, 8c, 8d, 12a, 12b, 17a</p> <p>POTS overlay, Supported US0 types: A (normal US0), M (extended US0), - (no US0)</p> <p>ITU G.994.1 (2/07) (G.hs) Handshake</p> <p style="padding-left: 40px;">Amendment 1 (11/07) + Amendment 2 (4/08)</p> <p>Supported Transport Protocol Specific Transmission Convergence (TPS-TC) functions:</p> <p style="padding-left: 40px;">PTM (via 64/65b encapsulation method defined in IEEE 802.3ah-2004)</p> <p>HDLC encapsulation for pre-VDSL2 standard interoperability</p> <p>Impulse Noise Protection (INP) up to 16 symbols</p> <p>SNR target met, delay maximized: The maximum allowable delay will be 16 ms for down and 16ms for up.</p> <p>Support for ITU-T G.INP</p> <p>Dying Gasp support</p> <p>Modulation : Multi-Carrier-Modulation (MCM)</p> <p>Interleaving: General Convolution</p> <p>Support of maximum SNRM configuration (directed by the central office)</p> <p>Seamless Rate Adaptation (SRA) as described in Amendment 1 of G.993.2</p> <p>Tone Spacing: 4.3KHz/8.6KHz</p>
----------------	---

Table 101 Firmware Specifications (continued)

ADSL Standards	<p>ADSL ITU-T G.992.1 (G.dmt), Annex A and ETSI TS 101 388 V1.3.1 (05/2002)</p> <p>1TR112 (U-R2 Deutsche Telekom AG) Version 7.0 including support of Dying Gasp and report of Self-Test-Result (ATU-T Register#3)</p> <p>EOC as specified in ITU-T G.992.1 (G.dmt)</p> <p>Handshake ITU G.994.1 (G.hs)</p> <p>Supported Transport Protocol Specific Transmission Convergence (TPS-TC) functions:</p> <ul style="list-style-type: none"> ATM PTM (via 64/65b encapsulation method defined in IEEE 802.3ah-2004) <p>Support of Vendor ID during Handshake in the Vendor ID information block including vendor specific information as specified in 1TR112 and ITU-T G.994.1 (G.hs)</p> <p>ADSL ITU-T G.992.2 (G.lite)</p> <p>ADSL2 ITU-T G.992.3 (G.dmt.bis), Annex A</p> <p>RE-ADSL2 ITU-T G.992.3 (G.dmt.bis), Annex L</p> <p>ADSL2 ITU-T G.992.4 (G.lite.bis), Annex A</p> <p>ADSL2+ ITU-T G.992.5, Annex A</p> <p>Support Multi-Mode Standard: ANSI T1.413 Issue 2; G.dmt (ITU-T G.992.1), ADSL2 (ITU-T G.992.3), ADSL2+ (ITU-T G.992.5)</p> <p>Dual Latency support</p>
Other Protocol Support	<p>PPP (Point-to-Point Protocol) link layer protocol</p> <p>Transparent bridging for unsupported network layer protocols</p> <p>RIP I/RIP II</p> <p>ICMP</p> <p>ATM QoS</p> <p>IP Multicasting IGMP v2 and v3</p> <p>IGMP Proxy</p>
Management	<p>Embedded Web Configurator</p> <p>Remote Firmware Upgrade</p> <p>Embedded FTP/TFTP Server for firmware upgrade and configuration file backup and restore</p> <p>Syslog</p> <p>TR-069</p> <p>TR-064</p>

The following list, which is not exhaustive, illustrates the standards supported in the CellPipe 7130 RG.

Table 102 Standards Supported

STANDARD	DESCRIPTION
RFC 1058	RIP-1 (Routing Information Protocol)
RFC 1112	IGMP v1
RFC 1157	SNMPv1: Simple Network Management Protocol version 1
RFC 1305	Network Time Protocol (NTP version 3)
RFC 1441	SNMPv2 Simple Network Management Protocol version 2
RFC 1483	Multiprotocol Encapsulation over ATM Adaptation Layer 5
RFC 1631	IP Network Address Translator (NAT)
RFC 1661	The Point-to-Point Protocol (PPP)
RFC 1723	RIP-2 (Routing Information Protocol)
RFC 2236	Internet Group Management Protocol, Version 2.
RFC 2364	PPP over AAL5 (PPP over ATM over ADSL)
RFC 2516	A Method for Transmitting PPP Over Ethernet (PPPoE)
RFC 2684	Multiprotocol Encapsulation over ATM Adaptation Layer 5
RFC 2766	Network Address Translation - Protocol
IEEE 802.11	Also known by the brand Wi-Fi, denotes a set of Wireless LAN/WLAN standards developed by working group 11 of the IEEE LAN/MAN Standards Committee (IEEE 802).
IEEE 802.11b	Uses the 2.4 gigahertz (GHz) band
IEEE 802.11g	Uses the 2.4 gigahertz (GHz) band
IEEE 802.11d	Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges
IEEE 802.11x	Port Based Network Access Control.
IEEE 802.11e QoS	IEEE 802.11 e Wireless LAN for Quality of Service
ANSI T1.413, Issue 2	Asymmetric Digital Subscriber Line (ADSL) standard.
G dmt(G.992.1)	G.992.1 Asymmetrical Digital Subscriber Line (ADSL) Transceivers
ITU G.992.1 (G.DMT)	ITU standard for ADSL using discrete multitone modulation.
ITU G.992.2 (G. Lite)	ITU standard for ADSL using discrete multitone modulation.
ITU G.992.3 (G.dmt.bis)	ITU standard (also referred to as ADSL2) that extends the capability of basic ADSL in data rates.
ITU G.992.4 (G.lite.bis)	ITU standard (also referred to as ADSL2) that extends the capability of basic ADSL in data rates.
ITU G.992.5 (ADSL2+)	ITU standard (also referred to as ADSL2+) that extends the capability of basic ADSL by doubling the number of downstream bits.
ITU-T G.993.2 (VDSL2)	ITU standard that defines VDSL2.
TR-069	DSL Forum Standard for CPE Wan Management.
TR-064	DSL Forum LAN-Side DSL CPE Configuration

Network Troubleshooting

Overview

The three most basic utilities for troubleshooting network connection issues are: `ipconfig`, `ping` and `tracert`. This appendix gives a quick overview of them as well as some common usage examples. Moreover, three slightly more advanced utilities are also discussed: `arp`, `route`, and `netstat`.

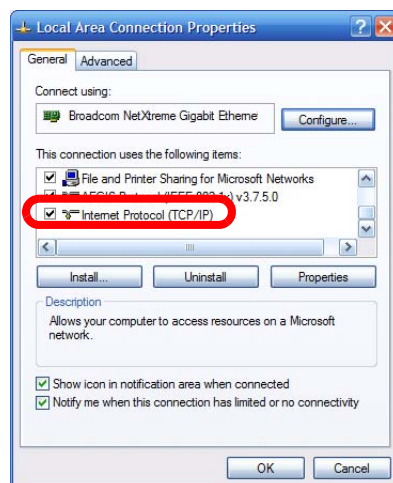
Note: All command examples here use the Microsoft Windows operating system version of the commands.

Before Getting Started

Before using the commands described in this section, ensure that you have the TCP/IP networking component installed and properly configured for your network adapter.

Click **Start > Control Panel > Network Connections** and then open a **Local Area Connection** to display the following screen.

Figure 142 TCP/IP Networking Component

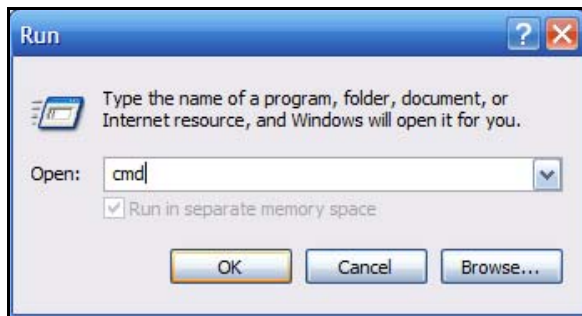


Note: Most operating systems ship with TCP/IP already installed and enabled. See your Windows documentation for details on installing or configuring TCP/IP.

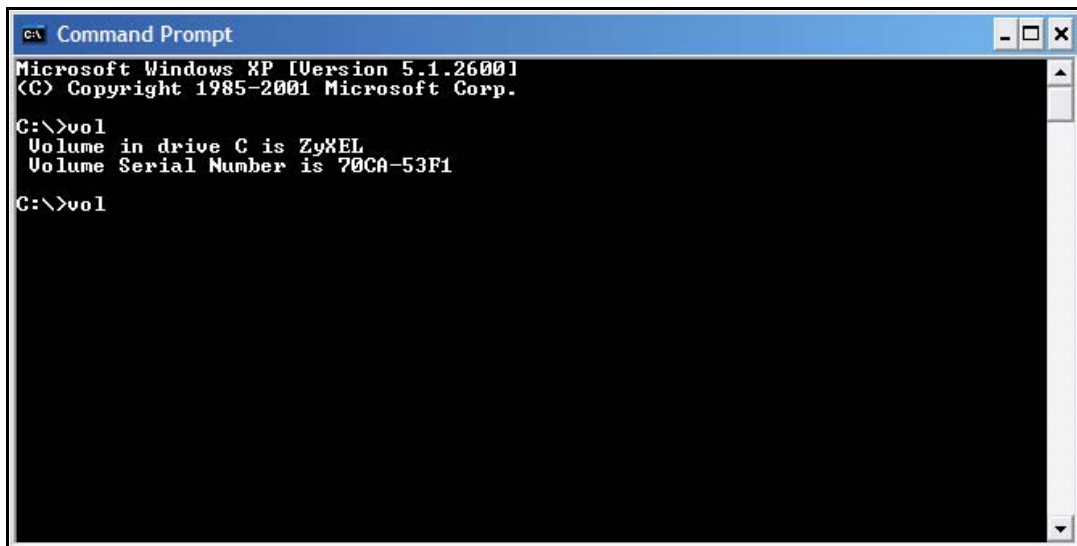
The Command Line Interface

To open the Windows command line interface:

- 1 Click **Start > Run**.
- 2 In the **Run** dialog box, enter **cmd** then click **OK**.



- 3 The **Command Prompt** window opens.



Command Syntax and Parameters

Command descriptions always indicate the default syntax you must use when entering them on the command line. Some commands require additional parameters in order to execute properly. Some may have optional parameters.

Parameters are displayed as follows: `command [parameter]`

For example, the `date` command has the optional `/t` and `date` parameters. If you do not use either of them and enter just `date` by itself, then the system shows you the date it is currently using and then prompts you to change it.

```
C:\>date
The current date is: 2009/10/21
Enter the new date: (mm-dd-yy)
```

However, if you use the `/t` parameter it just displays the date and nothing more.

```
C:\>date /t
2009/10/21

C:\>
```

To view the parameters for any given command, enter `help [command]`.

ipconfig

The `ipconfig` command line utility allows you to display current network (TCP/IP) configuration settings and, in some cases, adjust them. When you have network connectivity problems, the first thing you should do is run this command to ensure that your device or computer does in fact have an IP address as well as display the source of that IP address (such as a default gateway).

Syntax: `ipconfig`

Parameters: `ipconfig [/release] [/renew]`

There are other parameters, but these are the only ones you need to use for now.

The following examples show the typical output of this command:

```
C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : example.com
    IP Address. . . . . : 192.168.1.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 1.1.1.4

C:\>
```

Here you can see that the device has IP address of 1.1.1.1 and example.com is its Domain Name Server (DNS).

If the device is disconnected then you would see the following instead:

```
Ethernet adapter Local Area Connection:

Media State . . . . . : Media disconnected
```

If the device is connected but cannot get an IP address then you would see:

```
Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . :
IP Address. . . . . : 0.0.0.0
Subnet Mask . . . . . : 0.0.0.0
Default Gateway . . . . . :
```

In some cases, your computer may be properly connected to the network or the CellPipe 7130 RG but it is not receiving an IP address for whatever reason. Use the /release parameter followed by /renew:

```
C:\>ipconfig /release

Windows IP Configuration

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . :
IP Address. . . . . : 0.0.0.0
Subnet Mask . . . . . : 0.0.0.0
Default Gateway . . . . . :

C:\>ipconfig /renew

Windows IP Configuration

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . : example.com
IP Address. . . . . : 192.168.1.2
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 2.2.2.4

C:\>
```

ping

The `ping` command line utility allows you to verify the connection and latency between your computer and either the CellPipe 7130 RG or other devices on the network. If you cannot reach a target using this command, then it may indicate possible network trouble.

Syntax: `ping target`

The `target` can be an IP address or a host name.

Parameters: `ping [-w timeout] target`

The `timeout` parameter allows you to input the number of seconds (in milliseconds) that your computer waits for a reply.

The following examples show the typical output of this command:

```
C:\>ping www.example.com

Pinging a1524.g.akamai.net [203.69.113.18] with 32 bytes of data:

Reply from 203.69.113.18: bytes=32 time=6ms TTL=56
Reply from 203.69.113.18: bytes=32 time=6ms TTL=56
Reply from 203.69.113.18: bytes=32 time=6ms TTL=56
Reply from 203.69.113.18: bytes=32 time=7ms TTL=48

Ping statistics for 203.69.113.18:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 6ms, Maximum = 7ms, Average = 6ms

>
```

The number of bytes here indicates packet size. As most data is broken up into smaller packets, this makes the ping test fairly representative of a typical network connection. The default packet size on Windows is 32 bytes.

Time is the number of milliseconds the data requires to make the roundtrip journey from your computer to the destination host and back again. The lower the number, the faster the connection between the two points.

Note: Some hosts are deliberately configured to not respond to ping requests. As such, we suggest pinging two or three hosts when performing your ping test.

If your ping test fails to get a response, then you may see a message like this:

```
C:\>ping www.example.com

Pinging www.example.com [192.0.32.10] with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.0.32.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

When a request times out it may mean:

- your computer is not connected to the network
- your Internet access device is not connected to the network
- or the device which you are pinging is not connected to the network

If you think the destination is active but responding slowly, you can try increasing the ping timeout value from its default of 4 seconds (4000 milliseconds) to something like 8 seconds (or 8000 milliseconds).

```
C:\>ping -w 8000 www.example.com

Pinging www.example.com [192.0.32.10] with 32 bytes of data:

Reply from 192.0.32.10: bytes=32 time=157ms TTL=238
Reply from 192.0.32.10: bytes=32 time=154ms TTL=238
Reply from 192.0.32.10: bytes=32 time=152ms TTL=236
Reply from 192.0.32.10: bytes=32 time=162ms TTL=236

Ping statistics for 192.0.32.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 152ms, Maximum = 162ms, Average = 156ms

C:\>
```

A long ping response could indicate network problems:

- on your side of the connection
- between the start and end points of the connection
- on the receiving end

To determine where the slowdown is, you may need to use traceroute.

tracert

The `tracert` command line utility allows you to determine the network path between your computer and a host you specify. When you communicate with other devices on a network, the data is not often sent directly from point A to point B; rather, it moves through a series of intermediate servers, passed along until eventually the server closest to point B hands it off directly. This command can be useful for helping determine whether your connection issues are happening locally, somewhere in transit, or at the destination end.

- Each step in the chain of connections is called a 'hop'.
- The time it takes for a server at any given hop to pass the data packet is called 'latency' and is measured in milliseconds.

When a `tracert` command is run, it sends out a burst of three data packets per hop. The results table, therefore, always displays three values for latency in addition to the IP address and domain name (where available) of the server on that leg of the journey.

Syntax: `tracert target`

The `target` can be an IP address or a host name.

Parameters: `tracert [-d] [-h maximumhops] target`

There are other parameters but these are the only ones you need to use for now.

The following examples show the typical output of this command:

```
C:\>tracert www.example.com

Tracing route to www.example.com [192.0.32.10]
over a maximum of 30 hops:

  1  <1 ms  <1 ms  <1 ms  172.23.x.x
  2   5 ms   4 ms   5 ms  172.23.x.x
  3   4 ms   4 ms   4 ms  172.23.x.x
  4   5 ms   4 ms   6 ms  219-87-158-97.static.tfn.tw [219.87.158.97]
  5   6 ms   5 ms   4 ms  10.42.232.150
  6   5 ms   4 ms   4 ms  hc-c12r2.router.tw [220.128.7.86]
  7  10 ms   7 ms  10 ms  tp-s2-cl2r12.router.tw [220.128.2.90]
  8   9 ms   7 ms   8 ms  pr03-s2.tp.tw [220.128.4.181]
  9   6 ms   6 ms   9 ms  220-128-3-249.NET-IP.tw [220.128.3.249]
 10 138 ms  137 ms  138 ms  r11-pa.NET-IP.net [211.72.108.129]
 11 138 ms  138 ms  138 ms  po4-0.core01.sjc04.atlas.com [154.54.11.129]
 12 128 ms  139 ms  140 ms  te9-2.mpd01.sjc04.atlas.com [154.54.0.173]
 13 140 ms  139 ms  136 ms  61.58.33.173
 14 154 ms  153 ms  137 ms  xe-0-0-0.r20.gin.ntt.net [129.250.16.161]
 15 154 ms  154 ms  137 ms  as-2.r21.tokyjp01.jp.ntt.net [129.250.4.81]
 16 562 ms  553 ms  553 ms  38.106.6.34
 17 554 ms  554 ms  553 ms  po-2.r00.lsanca19.us.ntt.net [129.250.6.42]
 18 254 ms  254 ms  248 ms  204.1.254.150
 19 154 ms  253 ms  154 ms  192.0.32.10

Trace complete.

C:\>
```

Here, the `tracert` to `www.example.com` took 18 hops to reach its destination. Looking at the latency data, you'll see the first slow down happens at hop 10.

The extremely low latency on the first few hops indicates a network local to the computer where the `tracert` command originated, such as a home or office LAN. The packets then move onto the local WAN (such as your Internet Service Provider's network). Because of the close proximity of those servers to your computer, the latency remains low.

Once the data packets move out of the regional network to the first international server (at hop 10 in this example), the latency increases. This is because of the distance between the regional and international servers - it physically takes longer for the response to get back to your computer.

Finally, on transition hop 15 from the server in Japan to the server in California, another latency spike occurs. If you were having connection problems, this would most likely be the source of it. For whatever reason, the server in Japan has a less than optimal connection with its counterpart in the United States.

In this example, we abridge the `tracert` results table to show only server IP addresses and not domain names by using the `-d` parameter. We also use the `-h` parameter to limit the number of hops to 5 to test local connections only.

```
C:\>tracert -d -h 5 www.example.com

Tracing route to a1524.g.akamai.net [203.69.113.16]
over a maximum of 5 hops:

  1  <1 ms  <1 ms  <1 ms  172.23.31.254
  2   5 ms   4 ms   4 ms   172.23.6.113
  3   5 ms   5 ms   6 ms   172.23.6.253
  4  17 ms  16 ms  14 ms  218.160.188.254
  5  24 ms  25 ms  24 ms  10.42.232.150

Trace complete.

C:\>
```

arp

Local network transmission is based on MAC addresses. Data transmission between two networks is based on IP addresses.

Address Resolution Protocol (ARP) is a protocol that converts IP addresses into MAC addresses. Before a computer transmits data to an IP address on the same network, it will check whether the IP address exists in its ARP table. If it does, the computer then sends the data directly to the mapped MAC address. If it does not, the computer broadcasts an ARP request to the network. The host whose MAC address maps to the IP address responds.

When you use `ping` to check the connection to a computer, no response does not mean the computer is not alive on the network. The destination computer may be configured not to respond to any ping requests. However, you can use the `arp -a` command line utility to check the IP addresses and MAC addresses of your neighboring computers or devices.

Syntax: `arp -a`

Parameters: `arp [-d inet_addr] [-s inet_addr eth_addr]`

The `-d` parameter can be use alone to remove all entries from an arp table or in conjunction with an IP address to remove just that IP address (*inet_addr*). The `-s` parameter allows you to add entries based on IP address (*inet_addr*) and/or MAC address (*eth_addr*).

There are other parameters but these are the only ones you need to use for now.

To check the ARP table on a Windows XP computer:

- 1 Click **Start > Programs > Accessories > Command Prompt**. The **Command Prompt** screen appears.
- 2 Type `arp -a` and press [Enter].

The following examples show the typical output of this command:

```
C:\>arp -a
Interface: 172.16.1.28 on Interface 0x1000003
  Internet Address      Physical Address      Type
172.16.1.5             00-00-aa-19-07-38    dynamic
172.16.1.25           00-18-f3-f0-aa-34    dynamic
172.16.1.44           00-0e-a6-2c-60-10    dynamic
172.16.1.210          00-19-cb-e9-66-33    dynamic
172.16.1.254          00-04-80-4c-a8-05    dynamic
```

In this example, the **Physical Address** indicates the associated MAC address. A **Type** entry with **dynamic** means it was dynamically learned through an ARP response. Use the `arp -s [inet_addr eth_addr]` to manually add an ARP entry if you want your computer to connect to the host with the specified MAC address when you access the specified IP address.

You can additionally check whether the MAC address associated with the IP address that you are looking for is correct. In some circumstances, your ARP table may keep a wrong MAC address until the entry expires. You can then manually update the ARP table.

To update the ARP table:

- 1 Type `arp -d [inet_addr]` or just use `arp -d` to remove all entries in the ARP table. For example, type `arp -d 172.16.1.5`.
- 2 Type `ping 172.16.1.5` and press [Enter].
- 3 Next, use the `arp -a` command again to check whether the MAC address matches what you expected. If it does not, another computer may be using a duplicate IP address on the network. Change the IP address on either computer to an unused one to fix this problem.

route

The `route` command line utility allows you to display or adjust your computer's network table. The routing table on your computer contains the default gateway

and other route information. When your computer wants to access an IP address on another network, it references this table.

Syntax: `route print`

Parameters: For the purposes of this section, the `print` parameter is the most important. If you enter `route` by itself, the command's help page displays.

The following example shows the typical output of this command:

```
C:\>route print
=====
Interface List
0x1 ..... MS TCP Loopback interface
0x1000003 ...00 02 e3 a1 b2 c3 ..... Broadcom NetXtreme Gigabit Ethernet
Driver

=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
          0.0.0.0            0.0.0.0        172.16.1.254     172.16.1.32         1
          127.0.0.0          255.0.0.0           127.0.0.1       127.0.0.1         1
          172.16.1.0        255.255.255.0     172.16.1.32     172.16.1.32         1
          172.16.1.32      255.255.255.255     127.0.0.1       127.0.0.1         1
          172.16.255.255    255.255.255.255   172.16.1.32     172.16.1.32         1
          224.0.0.0           224.0.0.0       172.16.1.32     172.16.1.32         1
          255.255.255.255    255.255.255.255   172.16.1.32     172.16.1.32         1
Default Gateway:          172.16.1.254
=====
Persistent Routes:
None
```

The following table describes labels shown in the command output:

Table 103 route print Command Output

OUTPUT	DESCRIPTION
Active Routes	This section lists all available routes that are automatically learned from the network.
Network Destination	<p>The destination IP address of packets that this route entry is to route. The destination can be an IP address for a network or host, 0.0.0.0 for the default route or 127.0.0.0 for the loopback interface which is used mainly for self-test.</p> <p>The destination 224.0.0.0 is for multicasting packets or reserved for testing. But if you are not using multicast applications, just ignore it.</p> <p>The destination 255.255.255.255 is used to find computers when an IP address is not known. For example, before the DHCP IP address of your computer is determined, your computer sends packets with the destination looking for DHCP servers on the network.</p>

Table 103 route print Command Output

OUTPUT	DESCRIPTION
Netmask	The destination subnet mask of packets that this route entry is to route. The subnet mask can be the appropriate subnet mask for a network, 255.255.255.255 for a host, or 0.0.0.0 for the default route.
Gateway	The IP address of the gateway through which this computer should send the matched packets.
Interface	The IP address of an physical interface on this computer used to send the matched packets for this route entry.
Metric	The metric (hop count) of this route. Normally, the lower the number, the faster to a destination.
Default Gateway	The IP address of the gateway through which this computer sends all the rest packets if this computer cannot find any other matched routes for the packets.
Persistent Routes	This section lists all routes that are manually configured.

In this example, the 172.16.1.0 is the network address. The 172.16.1.32 is the address of the local computer. 172.16.1.255 is the network broadcast address which sends broadcast packets to all computers on the 172.16.1.x network. 172.16.1.254 is the default gateway.

You may have more than one 0.0.0.0 entry if your computer has two or more network cards installed. This may cause packets to be routed somewhere unexpected. Delete all 0.0.0.0 entries except the one that you want to use for the default gateway. In the following example, the computer uses the first 0.0.0.0 entry for the default gateway.

Network	Destination	Netmask	Gateway	Interface	Metric
	0.0.0.0	0.0.0.0	192.168.1.254	192.168.1.33	1
	0.0.0.0	0.0.0.0	172.16.1.254	172.16.1.32	1

- To delete the route to the default route with the gateway of 192.168.1.254, type: `route delete 0.0.0.0 mask 0.0.0.0 192.168.1.254`.
- To add a route to the destination 172.16.2.0 with the subnet mask of 255.255.255.0, the next hop address of 172.16.1.250, and the cost metric of 7, type: `route add 172.16.2.0 mask 255.255.255.0 172.16.1.250 metric 7`.
- To add a persistent route to the destination 172.16.3.0 with the subnet mask of 255.255.255.0 and the next hop address of 172.16.1.252, type: `route -p add 172.16.3.0 mask 255.255.255.0 172.16.1.252`.

Note that the metric will be set to 1 if you do not specify any.

netstat

The `netstat` command line utility is used to show Ethernet statistics and current TCP/IP network connections.

Syntax: `netstat`

With no parameters, this command simply displays only active statistics for ports that are currently in use by one process or another.

Parameter: `netstat [-a] [-e]`

The `-a` parameter displays all available listening ports and connections whether they are active or not, while the `-e` parameter displays Ethernet statistics.

There are other parameters but these are the only ones you need to use for now.

The following examples show the typical output of this command:

```
C:\>netstat

Active Connections

    Proto Local Address           Foreign Address         State
    TCP    COMPUTERA:1056         localhost:5091          ESTABLISHED
    TCP    COMPUTERA:1091         localhost:27015         ESTABLISHED
    TCP    COMPUTERA:1120         localhost:40000         ESTABLISHED
    TCP    COMPUTERA:3243         localhost:3244          ESTABLISHED
    TCP    COMPUTERA:3244         localhost:3243          ESTABLISHED
    TCP    COMPUTERA:3246         localhost:3247          ESTABLISHED
    TCP    COMPUTERA:3247         localhost:3246          ESTABLISHED
    TCP    COMPUTERA:5091         localhost:1056          ESTABLISHED
    TCP    COMPUTERA:5152         localhost:3245          CLOSE_WAIT
    TCP    COMPUTERA:27015        localhost:1091          ESTABLISHED
    TCP    COMPUTERA:40000        localhost:1120          ESTABLISHED
    TCP    COMPUTERA:3229         172.20.0.201:http      CLOSE_WAIT
    TCP    COMPUTERA:3234         172.16.1.29:1155       ESTABLISHED
    TCP    COMPUTERA:3237         172.16.1.29:1155       ESTABLISHED
    TCP    COMPUTERA:3240         172.16.1.29:1155       ESTABLISHED

C:\>
```

Use the -a parameter to display all possible connections to your device, not just the ones that are currently in use:

```
C:\>netstat -a
Active Connections

Proto Local Address           Foreign Address         State
TCP   COMPUTERA:http         COMPUTERA:0            LISTENING
TCP   COMPUTERA:http         172.16.x.x:4036       ESTABLISHED
TCP   COMPUTERA:2744         NAS:microsoft-ds      ESTABLISHED
TCP   COMPUTERA:5152         172.16.x.x.example.com:0 LISTENING
TCP   COMPUTERA:5152         localhost:4067        CLOSE_WAIT
TCP   COMPUTERA:5354         172.16.x.x.example.com:0 LISTENING
TCP   COMPUTERA:27015        172.16.x.x.example.com:0 LISTENING
TCP   COMPUTERA:40000        localhost:0            LISTENING
TCP   COMPUTERA:40000        localhost:1120        ESTABLISHED
TCP   COMPUTERA:netbios-ssn 172.16.x.x.example.com:0 LISTENING
TCP   COMPUTERA:4177         172.16.x.x:1155       ESTABLISHED
TCP   COMPUTERA:4178         172.16.x.x:1155       ESTABLISHED
TCP   COMPUTERA:4180         172.16.x.x:1155       ESTABLISHED
TCP   COMPUTERA:4182         172.16.x.x:1025       ESTABLISHED
TCP   COMPUTERA:4317         NAS:microsoft-ds      ESTABLISHED
TCP   COMPUTERA:4539         NAS:microsoft-ds      TIME_WAIT
TCP   COMPUTERA:netbios-ssn 172.16.x.x:0          LISTENING
TCP   COMPUTERA:netbios-ssn 172.16.x.x:0          LISTENING

C:\>
```

The following table describes the three entries in the output example above:

Table 104 netstat -a Command Output

OUTPUT	DESCRIPTION
TCP COMPUTERA:http COMPUTERA:0 LISTENING	A web server is available on COMPUTERA as an HTTP service is in a LISTENING state.
TCP COMPUTERA:http 172.16.1.29:4036 ESTABLISHED	A computer with an IP address of 172.16.1.29 is accessing the web service on the COMPUTERA .
TCP COMPUTERA:2744 NAS:microsoft-ds ESTABLISHED	COMPUTERA has established a TCP/IP NETBIOS connection (microsoft-ds) with a NAS device.

Additionally, you can use `netstat -e` to display Ethernet statistics as the following example.

```
C:\ >netstat -e
Interface Statistics

                Received                Sent
Bytes           25250033                7060325
Unicast packets    38838                34744
Non-unicast packets 38227                175
Discards          0                    0
Errors            0                    35
Unknown protocols  787
```


Setting Up Your Computer's IP Address

Note: Your specific CellPipe 7130 RG may not support all of the operating systems described in this appendix. See the product specifications for more information about which operating systems are supported.

This appendix shows you how to configure the IP settings on your computer in order for it to be able to communicate with the other devices on your network. Windows Vista/XP/2000, Mac OS 9/OS X, and all versions of UNIX/LINUX include the software components you need to use TCP/IP on your computer.

If you manually assign IP information instead of using a dynamic IP, make sure that your network's computers have IP addresses that place them in the same subnet.

In this appendix, you can set up an IP address for:

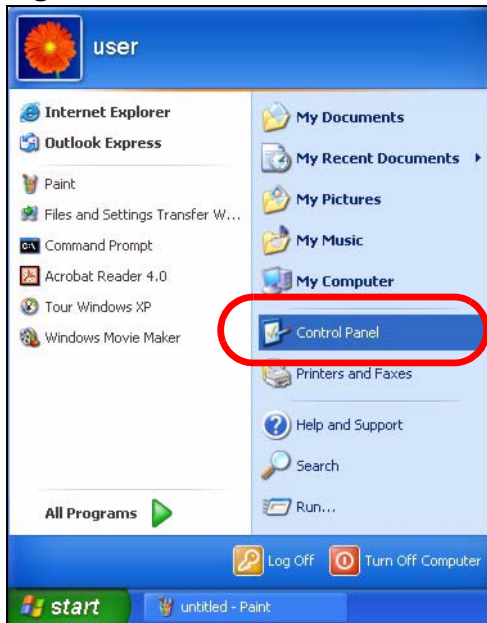
- [Windows XP/NT/2000](#) on [page 321](#)
- [Windows Vista](#) on [page 325](#)
- [Windows 7](#) on [page 329](#)
- [Mac OS X: 10.3 and 10.4](#) on [page 333](#)
- [Mac OS X: 10.5 and 10.6](#) on [page 337](#)
- [Linux: Ubuntu 8 \(GNOME\)](#) on [page 340](#)
- [Linux: openSUSE 10.3 \(KDE\)](#) on [page 345](#)

Windows XP/NT/2000

The following example uses the default Windows XP display theme but can also apply to Windows 2000 and Windows NT.

- 1 Click **Start > Control Panel**.

Figure 143 Windows XP: Start Menu



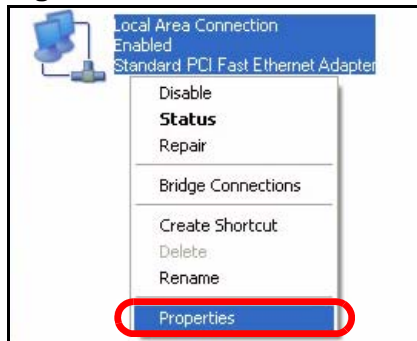
- 2 In the **Control Panel**, click the **Network Connections** icon.

Figure 144 Windows XP: Control Panel



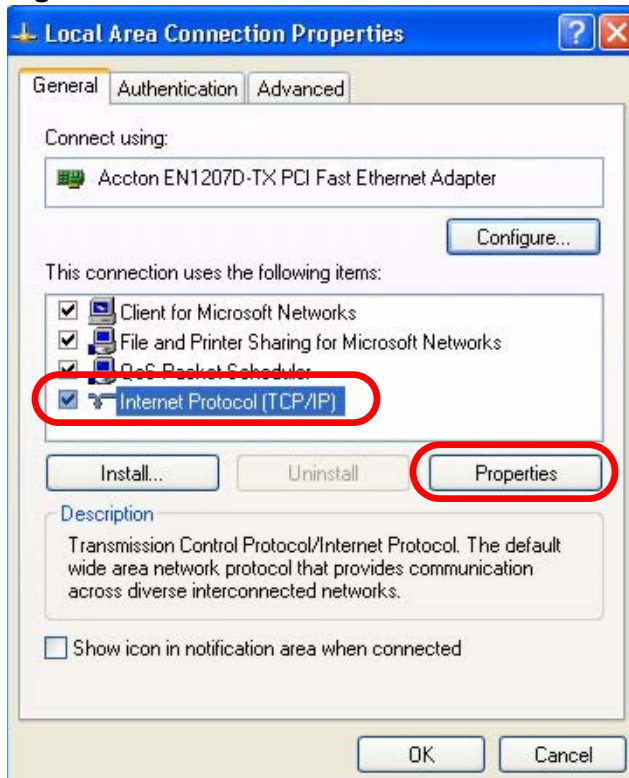
- 3 Right-click **Local Area Connection** and then select **Properties**.

Figure 145 Windows XP: Control Panel > Network Connections > Properties



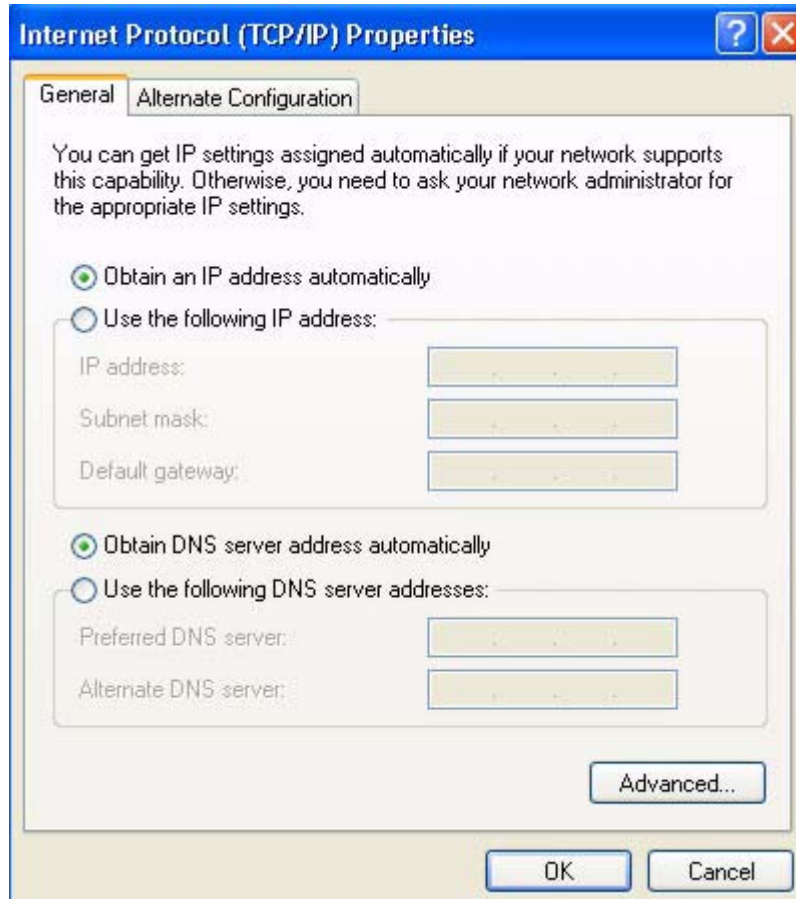
- 4 On the **General** tab, select **Internet Protocol (TCP/IP)** and then click **Properties**.

Figure 146 Windows XP: Local Area Connection Properties



- 5 The **Internet Protocol TCP/IP Properties** window opens.

Figure 147 Windows XP: Internet Protocol (TCP/IP) Properties



- 6 Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.

Select **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields if you have a static IP address that was assigned to you by your network administrator or ISP. You may also have to enter a **Preferred DNS server** and an **Alternate DNS server**, if that information was provided.

- 7 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.
- 8 Click **OK** to close the **Local Area Connection Properties** window.

Verifying Settings

- 1 Click **Start > All Programs > Accessories > Command Prompt**.

- 2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

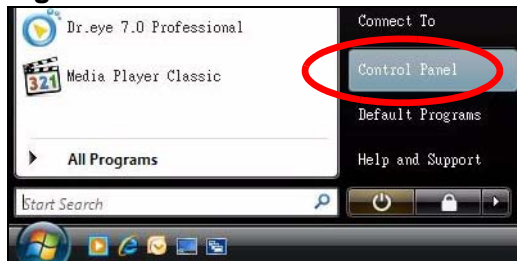
You can also go to **Start > Control Panel > Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab to view your IP address and connection information.

Windows Vista

This section shows screens from Windows Vista Professional.

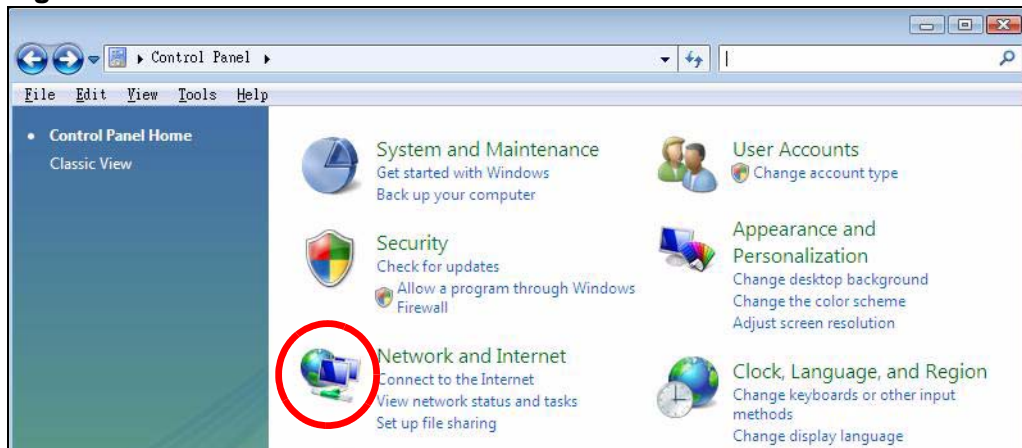
- 1 Click **Start > Control Panel**.

Figure 148 Windows Vista: Start Menu



- 2 In the **Control Panel**, click the **Network and Internet** icon.

Figure 149 Windows Vista: Control Panel



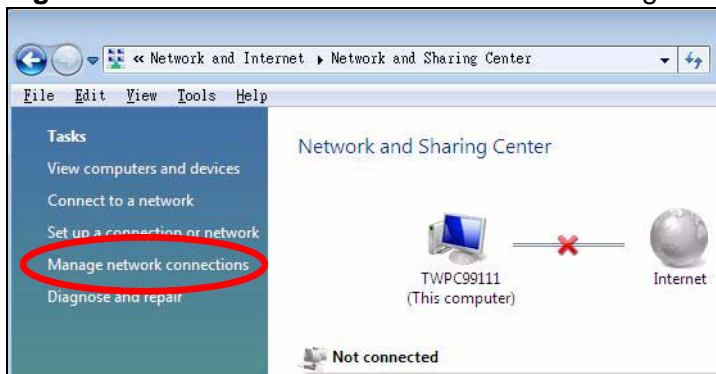
- 3 Click the **Network and Sharing Center** icon.

Figure 150 Windows Vista: Network And Internet



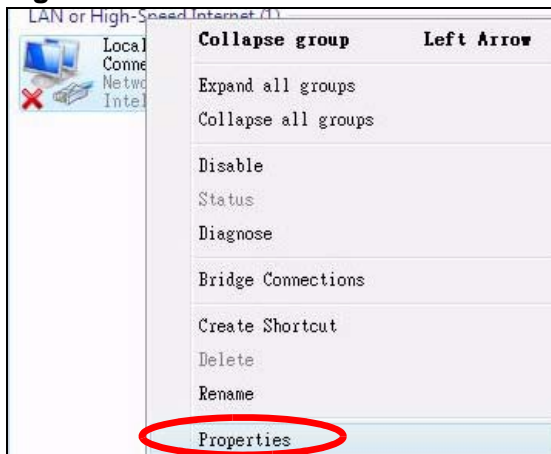
- 4 Click **Manage network connections**.

Figure 151 Windows Vista: Network and Sharing Center



- 5 Right-click **Local Area Connection** and then select **Properties**.

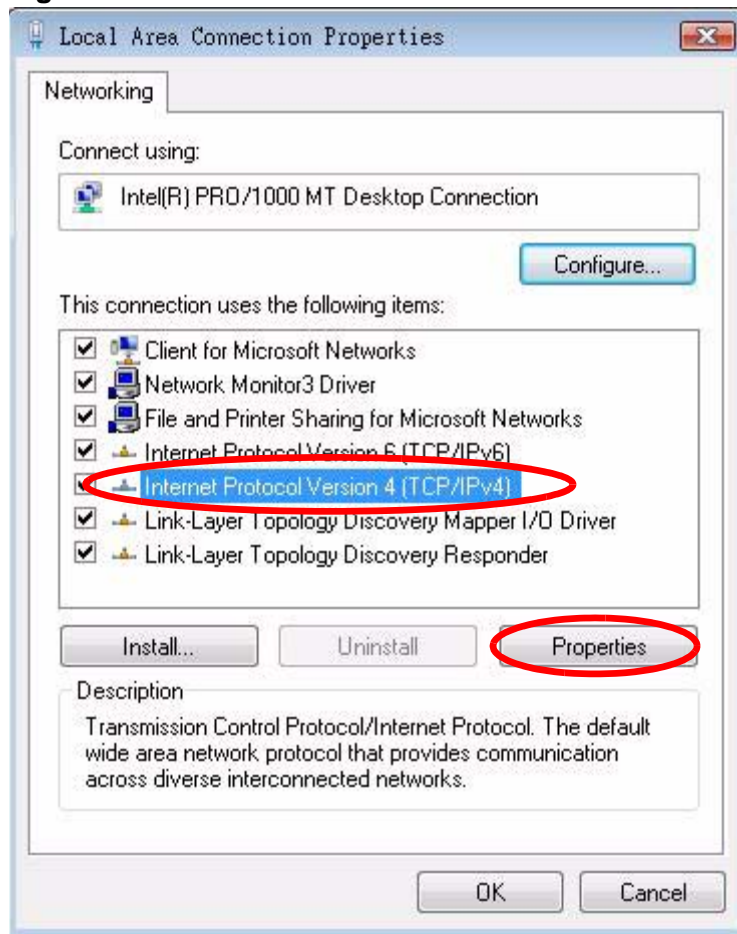
Figure 152 Windows Vista: Network and Sharing Center



Note: During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.

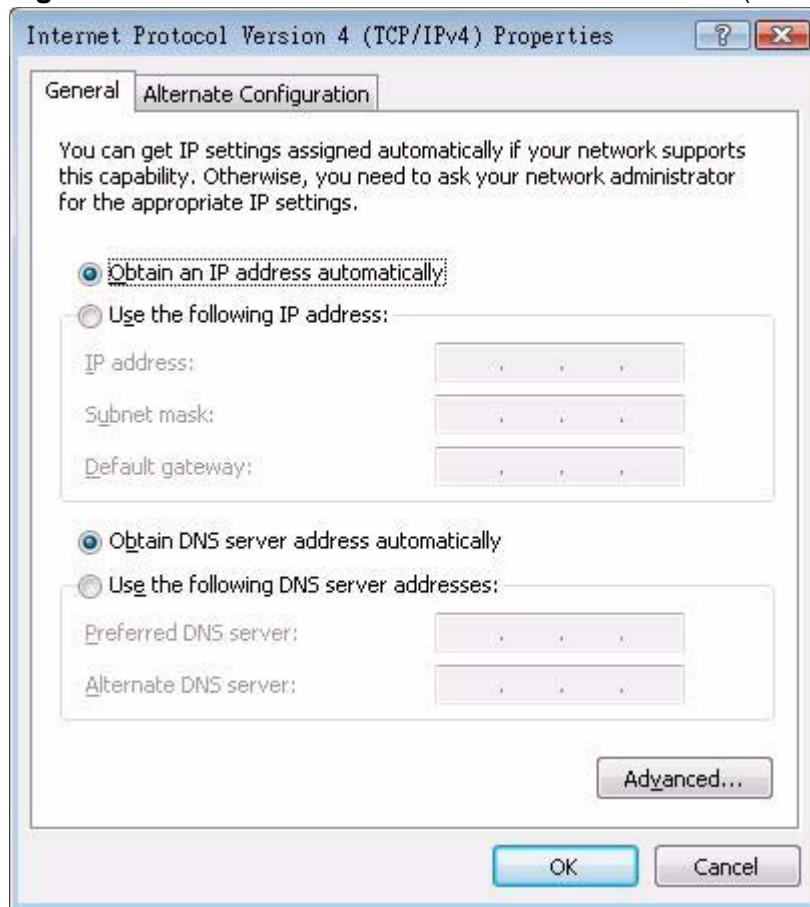
- 6 Select **Internet Protocol Version 4 (TCP/IPv4)** and then select **Properties**.

Figure 153 Windows Vista: Local Area Connection Properties



- 7 The **Internet Protocol Version 4 (TCP/IPv4) Properties** window opens.

Figure 154 Windows Vista: Internet Protocol Version 4 (TCP/IPv4) Properties



- 8 Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.

Select **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields if you have a static IP address that was assigned to you by your network administrator or ISP. You may also have to enter a **Preferred DNS server** and an **Alternate DNS server**, if that information was provided. Click **Advanced**.

- 9 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.
- 10 Click **OK** to close the **Local Area Connection Properties** window.

Verifying Settings

- 1 Click **Start > All Programs > Accessories > Command Prompt**.

- 2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

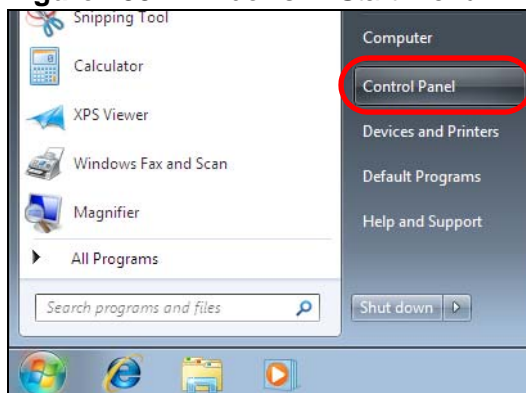
You can also go to **Start > Control Panel > Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab to view your IP address and connection information.

Windows 7

This section shows screens from Windows 7 Enterprise.

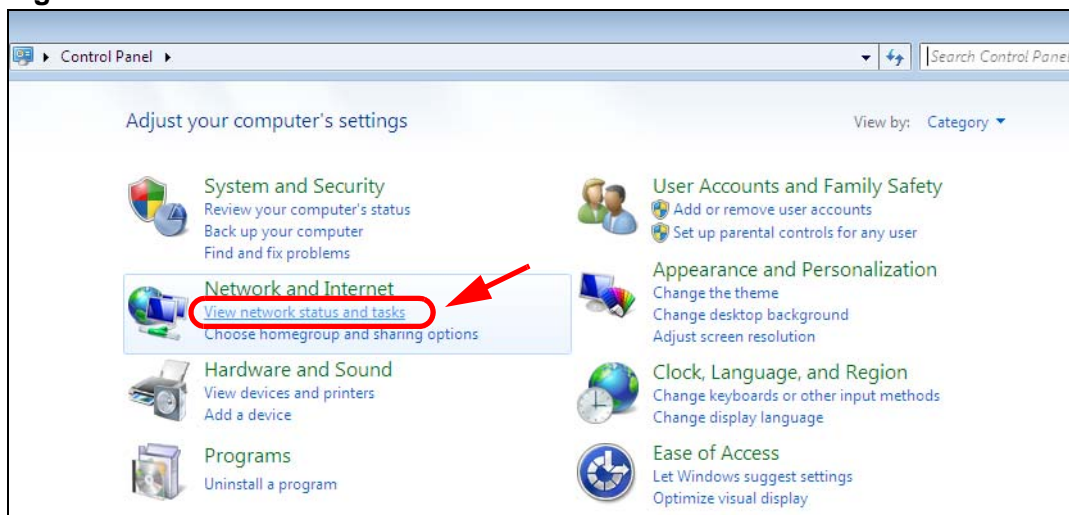
- 1 Click **Start > Control Panel**.

Figure 155 Windows 7: Start Menu



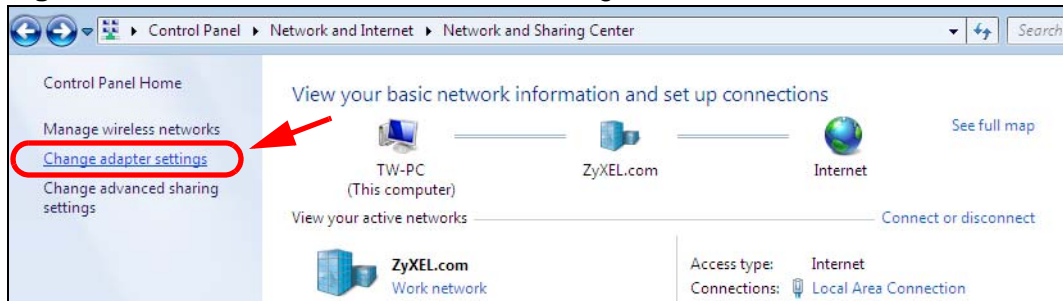
- 2 In the **Control Panel**, click **View network status and tasks** under the **Network and Internet** category.

Figure 156 Windows 7: Control Panel



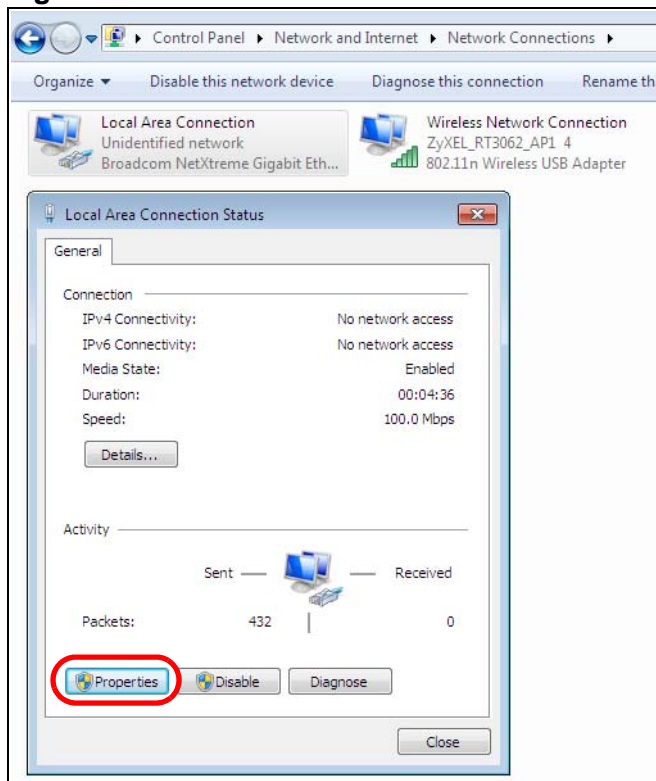
- 3 Click **Change adapter settings**.

Figure 157 Windows 7: Network And Sharing Center



- 4 Double click **Local Area Connection** and then select **Properties**.

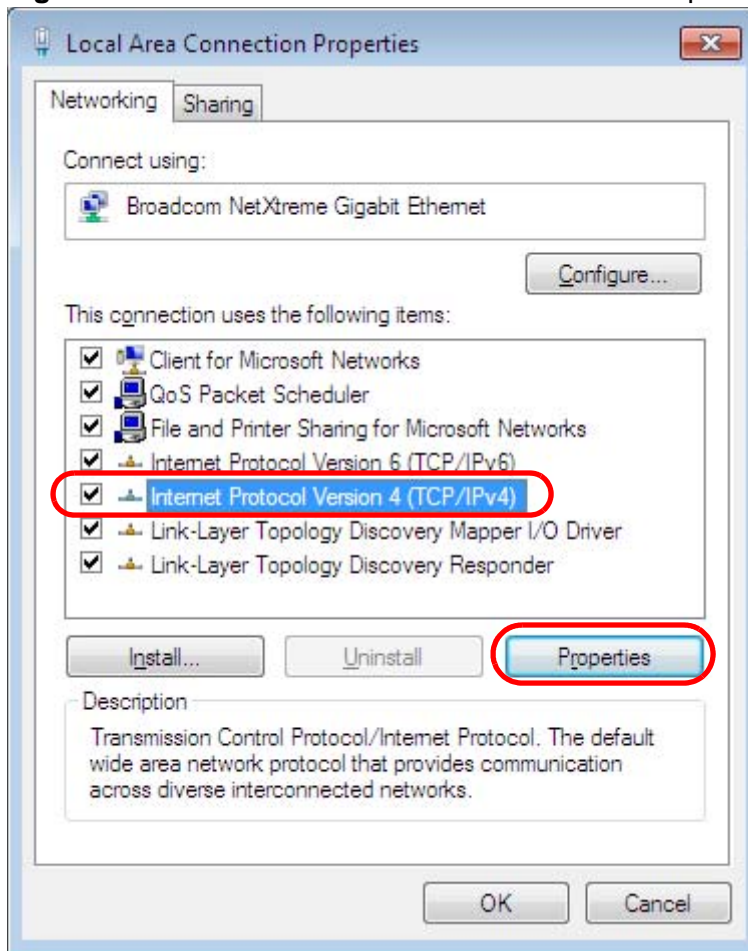
Figure 158 Windows 7: Local Area Connection Status



Note: During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.

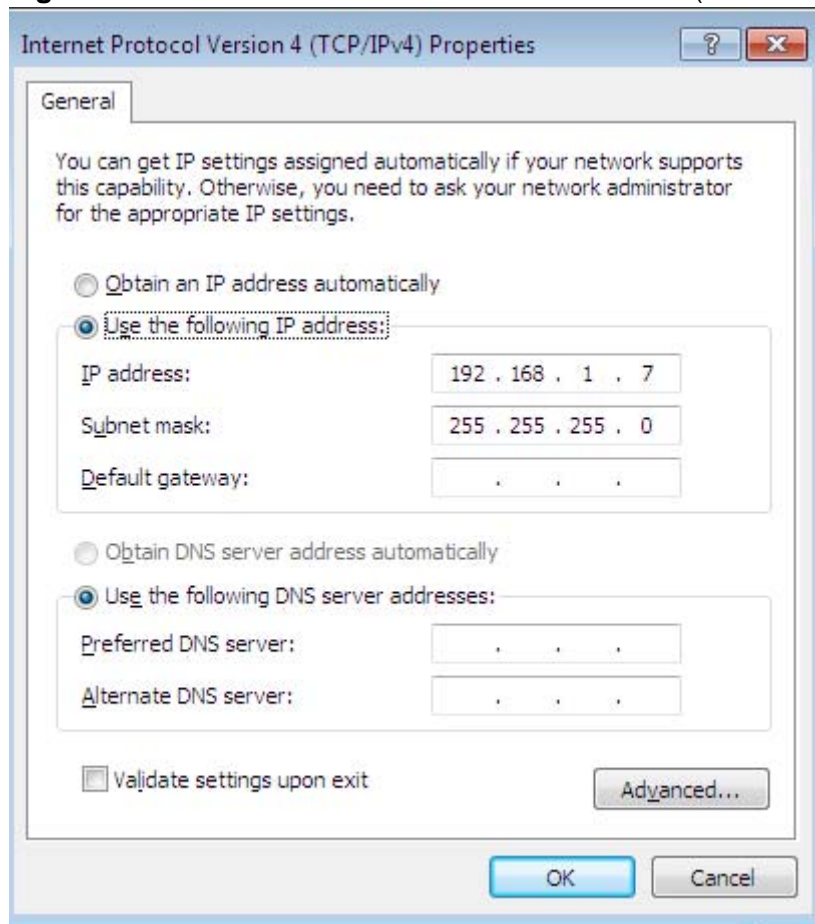
- 5 Select **Internet Protocol Version 4 (TCP/IPv4)** and then select **Properties**.

Figure 159 Windows 7: Local Area Connection Properties



- 6 The **Internet Protocol Version 4 (TCP/IPv4) Properties** window opens.

Figure 160 Windows 7: Internet Protocol Version 4 (TCP/IPv4) Properties



- 7 Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.

Select **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields if you have a static IP address that was assigned to you by your network administrator or ISP. You may also have to enter a **Preferred DNS server** and an **Alternate DNS server**, if that information was provided. Click **Advanced** if you want to configure advanced settings for IP, DNS and WINS.

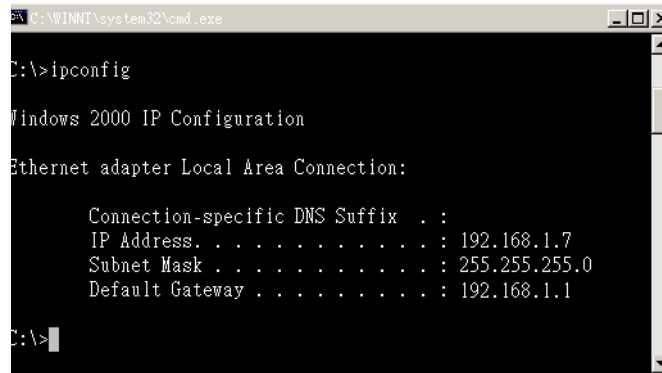
- 8 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.
- 9 Click **OK** to close the **Local Area Connection Properties** window.

Verifying Settings

- 1 Click **Start > All Programs > Accessories > Command Prompt**.
- 2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

- 3 The IP settings are displayed as follows.

Figure 161 Windows 7: Internet Protocol Version 4 (TCP/IPv4) Properties



```
C:\WINNT\system32\cmd.exe
C:\>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . . . :
    IP Address . . . . . : 192.168.1.7
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

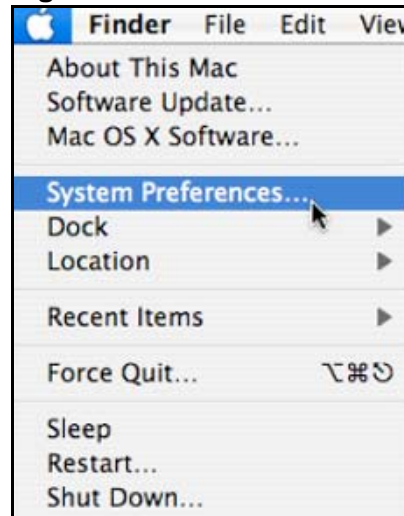
C:\>
```

Mac OS X: 10.3 and 10.4

The screens in this section are from Mac OS X 10.4 but can also apply to 10.3.

- 1 Click **Apple > System Preferences**.

Figure 162 Mac OS X 10.4: Apple Menu



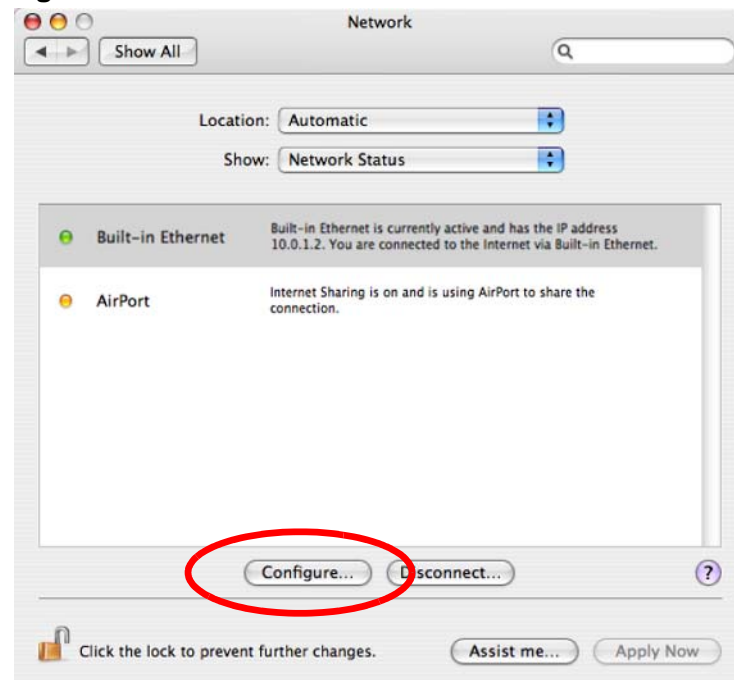
- 2 In the **System Preferences** window, click the **Network** icon.

Figure 163 Mac OS X 10.4: System Preferences



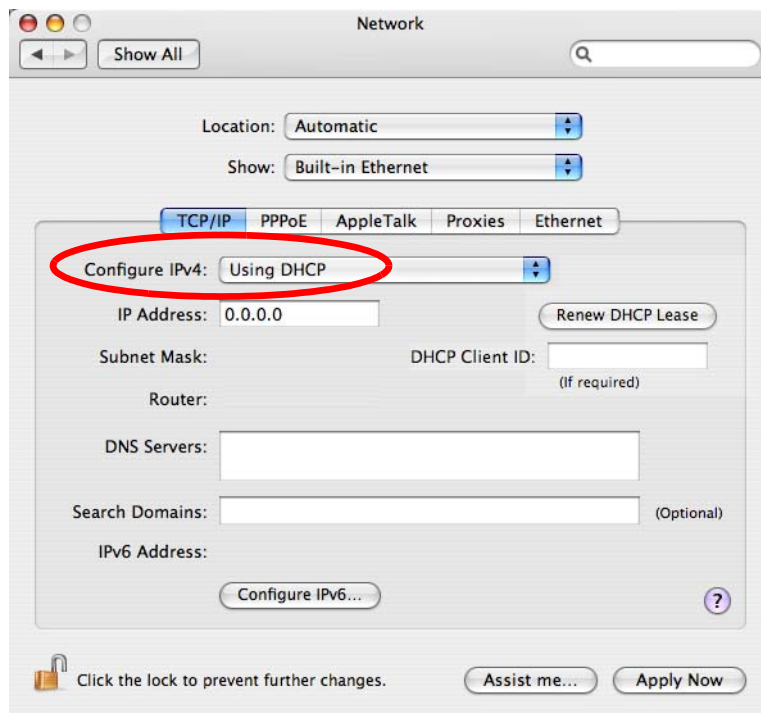
- 3 When the **Network** preferences pane opens, select **Built-in Ethernet** from the network connection type list, and then click **Configure**.

Figure 164 Mac OS X 10.4: Network Preferences



- 4 For dynamically assigned settings, select **Using DHCP** from the **Configure IPv4** list in the **TCP/IP** tab.

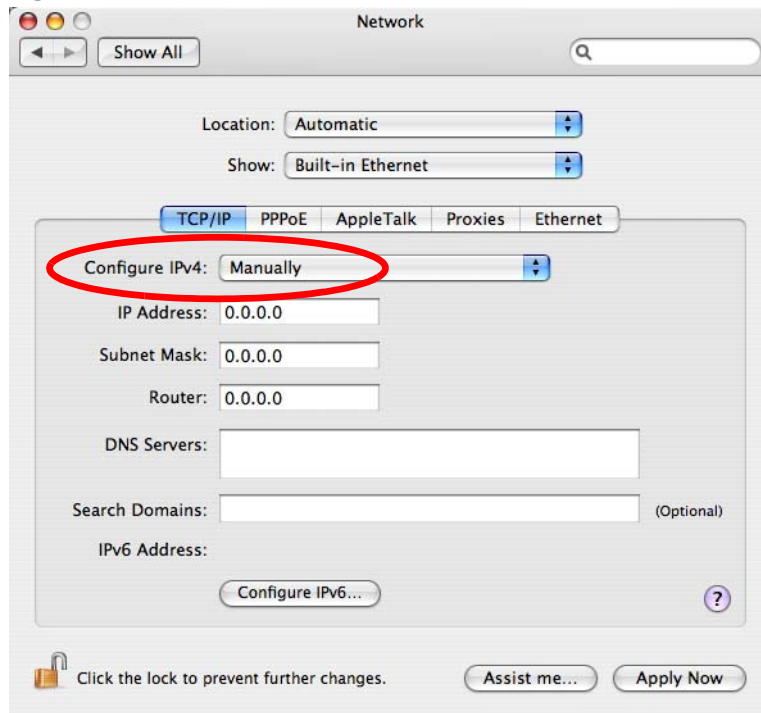
Figure 165 Mac OS X 10.4: Network Preferences > TCP/IP Tab.



- 5 For statically assigned settings, do the following:
 - From the **Configure IPv4** list, select **Manually**.
 - In the **IP Address** field, type your IP address.
 - In the **Subnet Mask** field, type your subnet mask.

- In the **Router** field, type the IP address of your device.

Figure 166 Mac OS X 10.4: Network Preferences > Ethernet

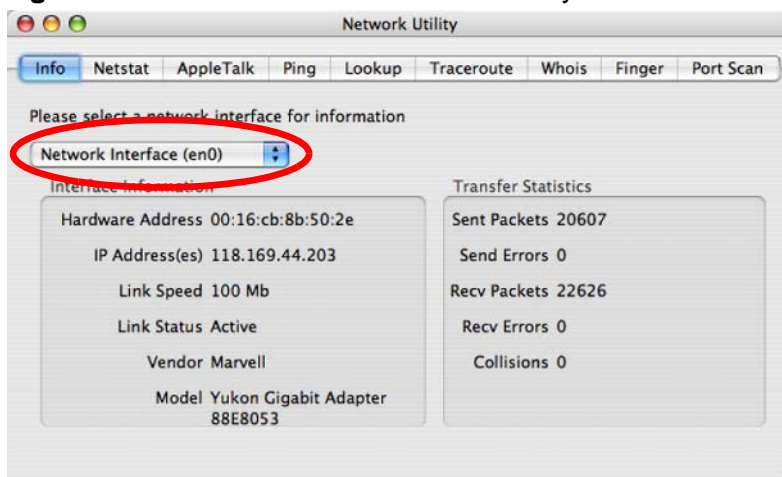


- 6 Click **Apply Now** and close the window.

Verifying Settings

Check your TCP/IP properties by clicking **Applications > Utilities > Network Utilities**, and then selecting the appropriate **Network Interface** from the **Info** tab.

Figure 167 Mac OS X 10.4: Network Utility

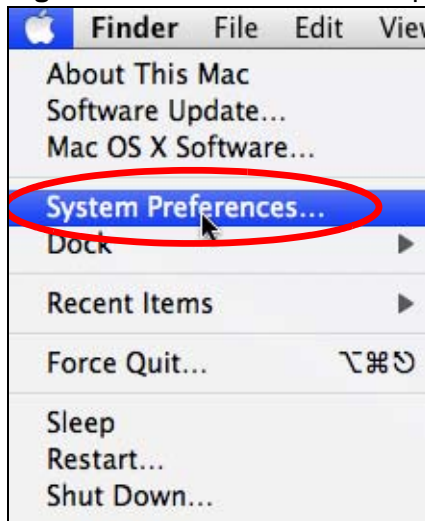


Mac OS X: 10.5 and 10.6

The screens in this section are from Mac OS X 10.5 but can also apply to 10.6.

- 1 Click **Apple** > **System Preferences**.

Figure 168 Mac OS X 10.5: Apple Menu



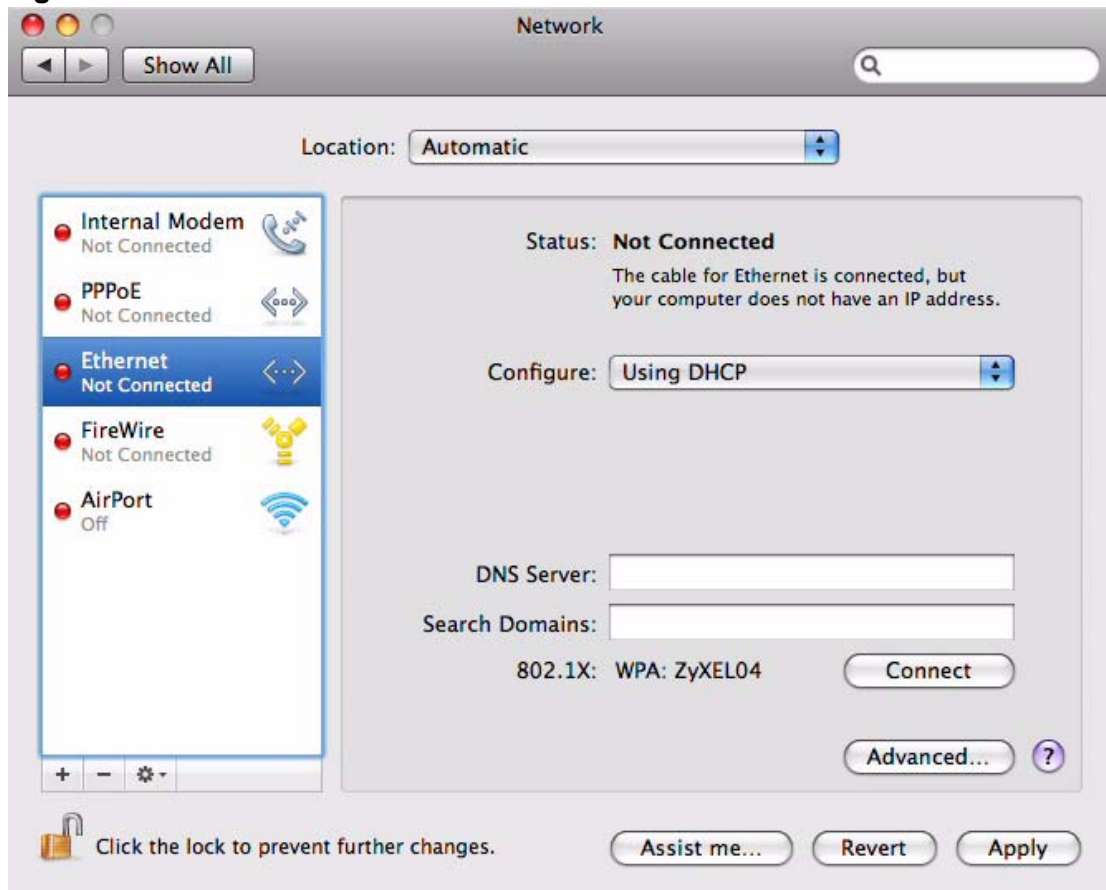
- 2 In **System Preferences**, click the **Network** icon.

Figure 169 Mac OS X 10.5: Systems Preferences



- 3 When the **Network** preferences pane opens, select **Ethernet** from the list of available connection types.

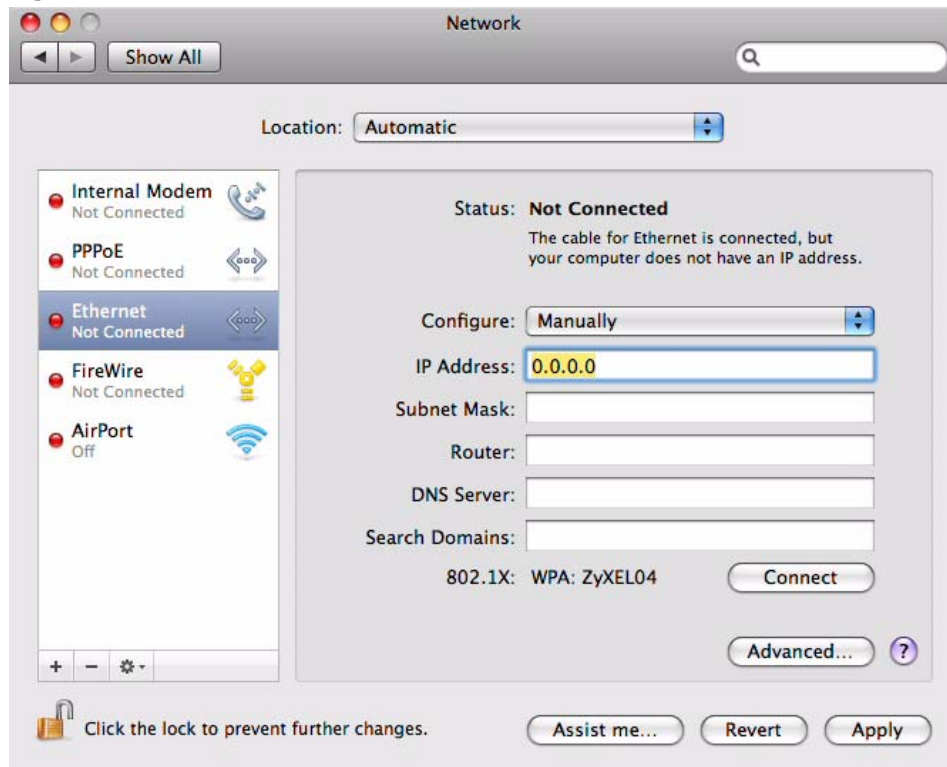
Figure 170 Mac OS X 10.5: Network Preferences > Ethernet



- 4 From the **Configure** list, select **Using DHCP** for dynamically assigned settings.
- 5 For statically assigned settings, do the following:
 - From the **Configure** list, select **Manually**.
 - In the **IP Address** field, enter your IP address.
 - In the **Subnet Mask** field, enter your subnet mask.

- In the **Router** field, enter the IP address of your CellPipe 7130 RG.

Figure 171 Mac OS X 10.5: Network Preferences > Ethernet

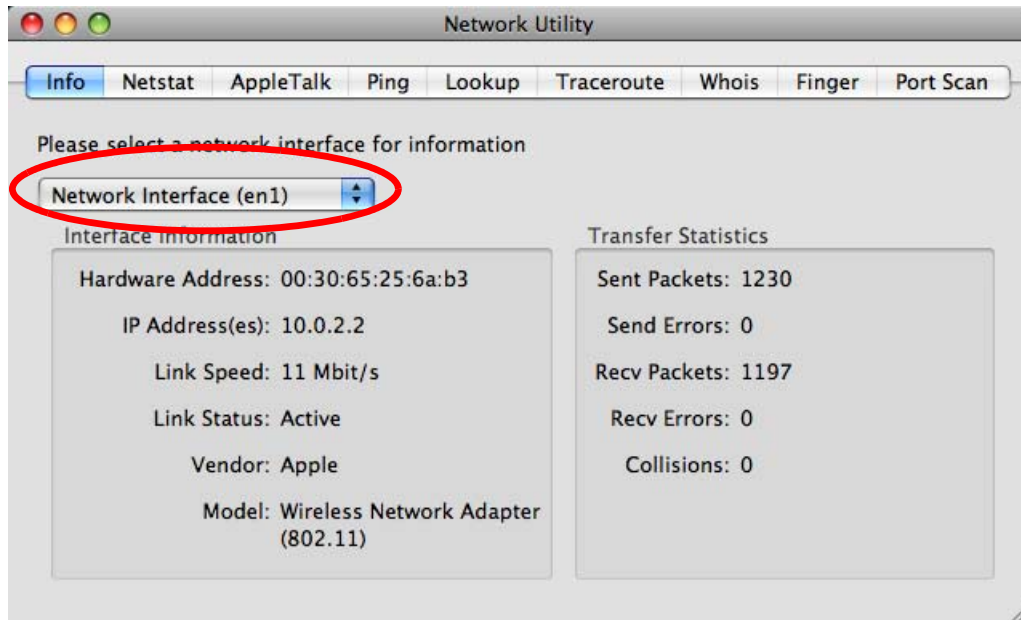


- 6 Click **Apply** and close the window.

Verifying Settings

Check your TCP/IP properties by clicking **Applications > Utilities > Network Utilities**, and then selecting the appropriate **Network interface** from the **Info** tab.

Figure 172 Mac OS X 10.5: Network Utility



Linux: Ubuntu 8 (GNOME)

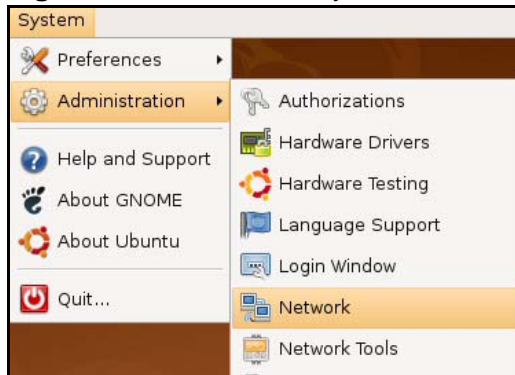
This section shows you how to configure your computer's TCP/IP settings in the GNU Object Model Environment (GNOME) using the Ubuntu 8 Linux distribution. The procedure, screens and file locations may vary depending on your specific distribution, release version, and individual configuration. The following screens use the default Ubuntu 8 installation.

Note: Make sure you are logged in as the root administrator.

Follow the steps below to configure your computer IP address in GNOME:

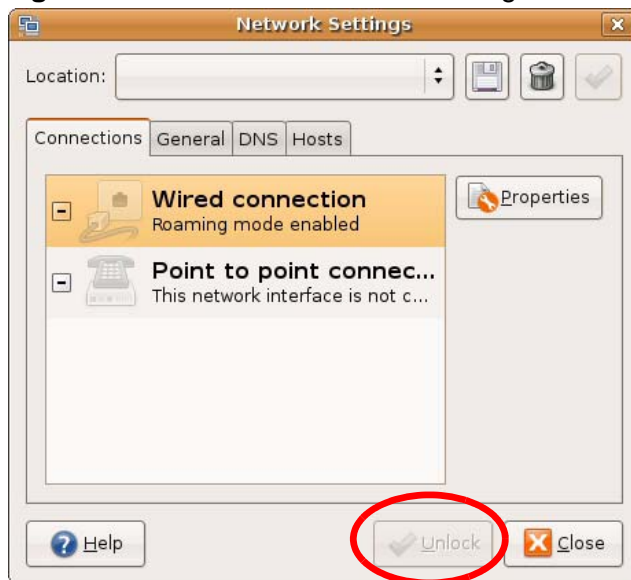
- 1 Click **System > Administration > Network**.

Figure 173 Ubuntu 8: System > Administration Menu



- 2 When the **Network Settings** window opens, click **Unlock** to open the **Authenticate** window. (By default, the **Unlock** button is greyed out until clicked.) You cannot make changes to your configuration unless you first enter your admin password.

Figure 174 Ubuntu 8: Network Settings > Connections



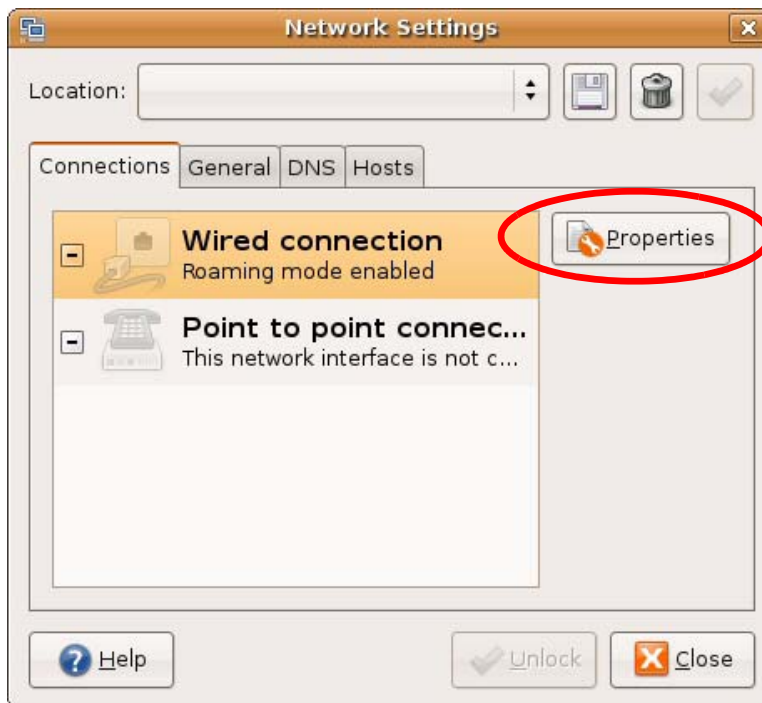
- 3 In the **Authenticate** window, enter your admin account name and password then click the **Authenticate** button.

Figure 175 Ubuntu 8: Administrator Account Authentication



- 4 In the **Network Settings** window, select the connection that you want to configure, then click **Properties**.

Figure 176 Ubuntu 8: Network Settings > Connections



- 5 The **Properties** dialog box opens.

Figure 177 Ubuntu 8: Network Settings > Properties



- In the **Configuration** list, select **Automatic Configuration (DHCP)** if you have a dynamic IP address.
 - In the **Configuration** list, select **Static IP address** if you have a static IP address. Fill in the **IP address**, **Subnet mask**, and **Gateway address** fields.
- 6 Click **OK** to save the changes and close the **Properties** dialog box and return to the **Network Settings** screen.

- 7 If you know your DNS server IP address(es), click the **DNS** tab in the **Network Settings** window and then enter the DNS server information in the fields provided.

Figure 178 Ubuntu 8: Network Settings > DNS



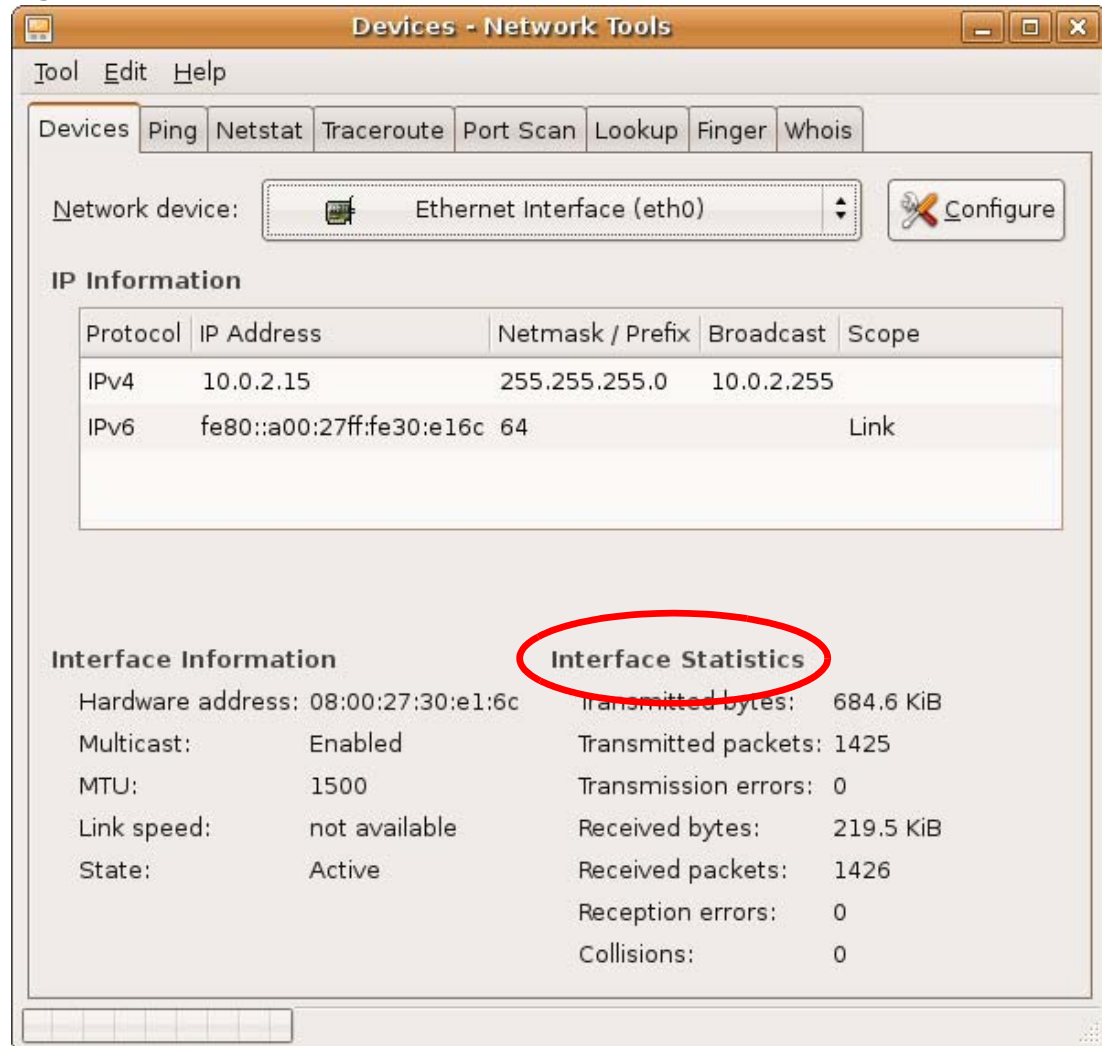
- 8 Click the **Close** button to apply the changes.

Verifying Settings

Check your TCP/IP properties by clicking **System > Administration > Network Tools**, and then selecting the appropriate **Network device** from the **Devices**

tab. The **Interface Statistics** column shows data if your connection is working properly.

Figure 179 Ubuntu 8: Network Tools



Linux: openSUSE 10.3 (KDE)

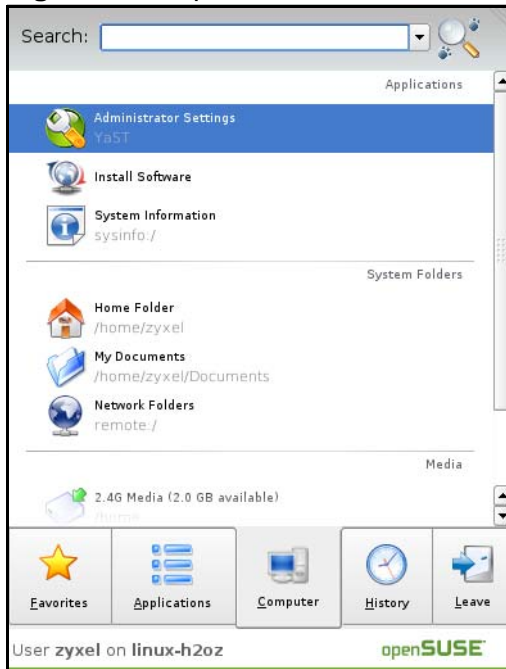
This section shows you how to configure your computer's TCP/IP settings in the KDE Desktop Environment (KDE) using the openSUSE 10.3 Linux distribution. The procedure, screens and file locations may vary depending on your specific distribution, release version, and individual configuration. The following screens use the default openSUSE 10.3 installation.

Note: Make sure you are logged in as the root administrator.

Follow the steps below to configure your computer IP address in the KDE:

- 1 Click **K Menu > Computer > Administrator Settings (YaST)**.

Figure 180 openSUSE 10.3: K Menu > Computer Menu



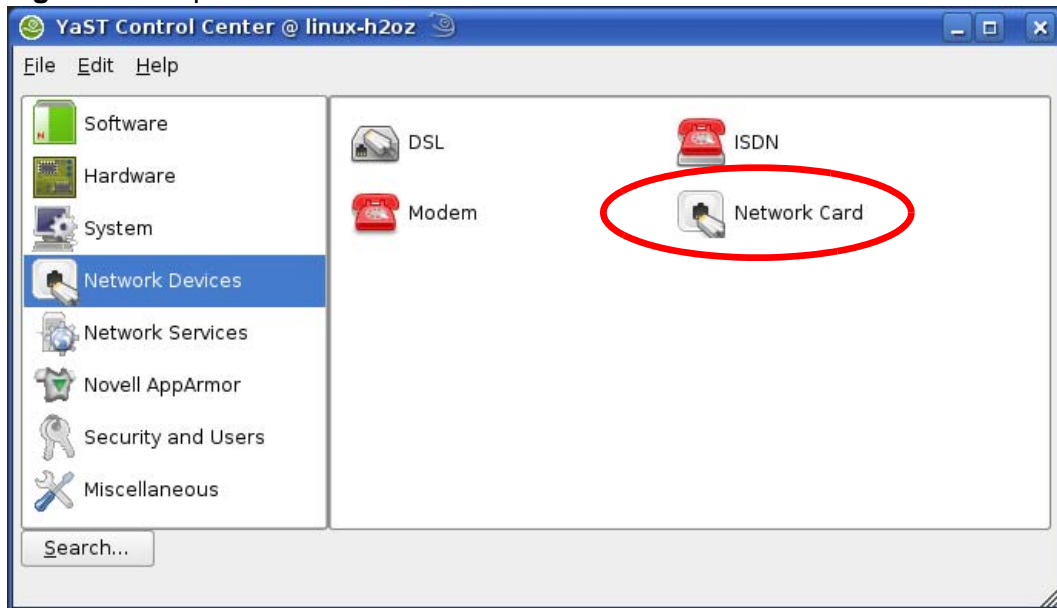
- 2 When the **Run as Root - KDE su** dialog opens, enter the admin password and click **OK**.

Figure 181 openSUSE 10.3: K Menu > Computer Menu



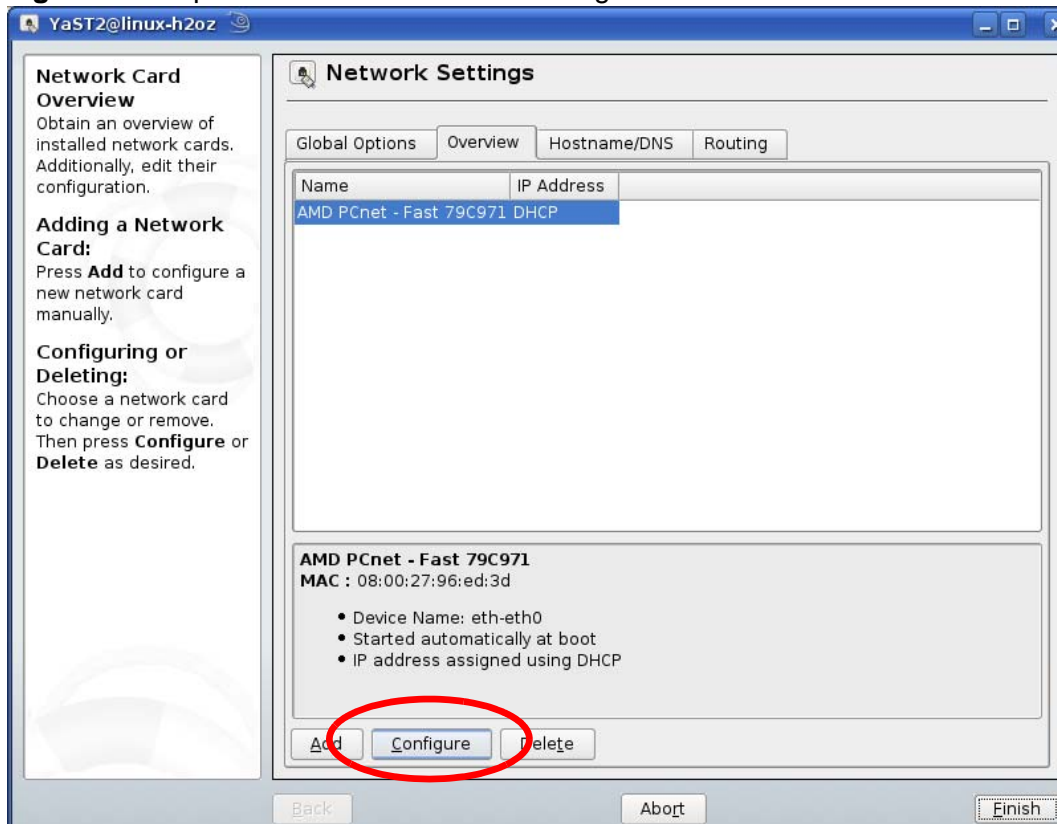
- 3 When the **YaST Control Center** window opens, select **Network Devices** and then click the **Network Card** icon.

Figure 182 openSUSE 10.3: YaST Control Center



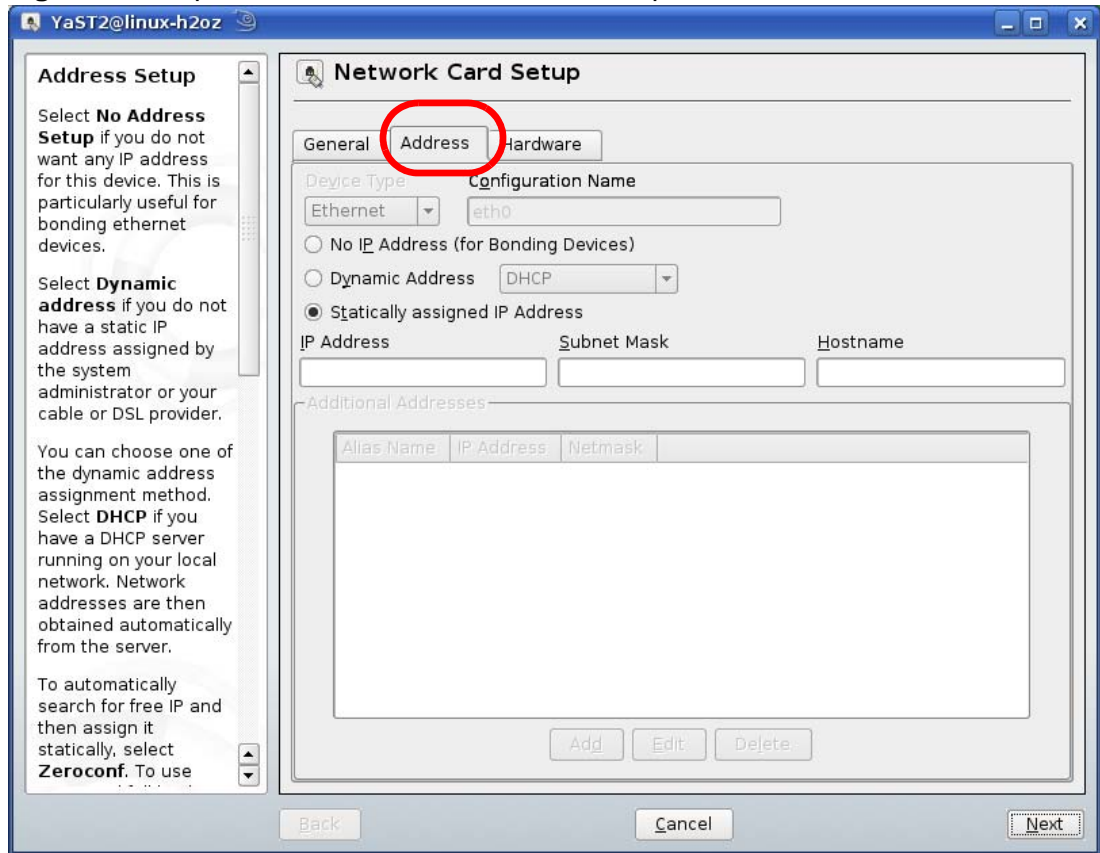
- 4 When the **Network Settings** window opens, click the **Overview** tab, select the appropriate connection **Name** from the list, and then click the **Configure** button.

Figure 183 openSUSE 10.3: Network Settings



- 5 When the **Network Card Setup** window opens, click the **Address** tab

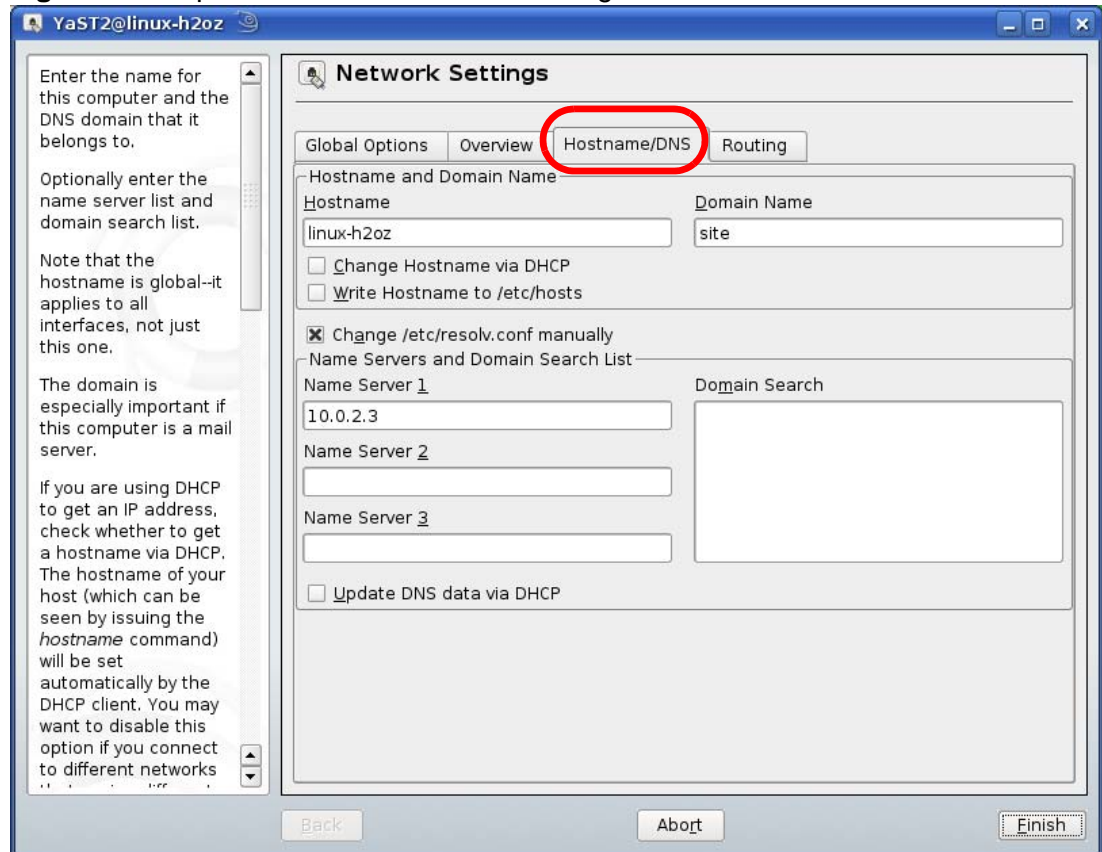
Figure 184 openSUSE 10.3: Network Card Setup



- 6 Select **Dynamic Address (DHCP)** if you have a dynamic IP address.
Select **Statically assigned IP Address** if you have a static IP address. Fill in the **IP address**, **Subnet mask**, and **Hostname** fields.
- 7 Click **Next** to save the changes and close the **Network Card Setup** window.

- 8 If you know your DNS server IP address(es), click the **Hostname/DNS** tab in **Network Settings** and then enter the DNS server information in the fields provided.

Figure 185 openSUSE 10.3: Network Settings

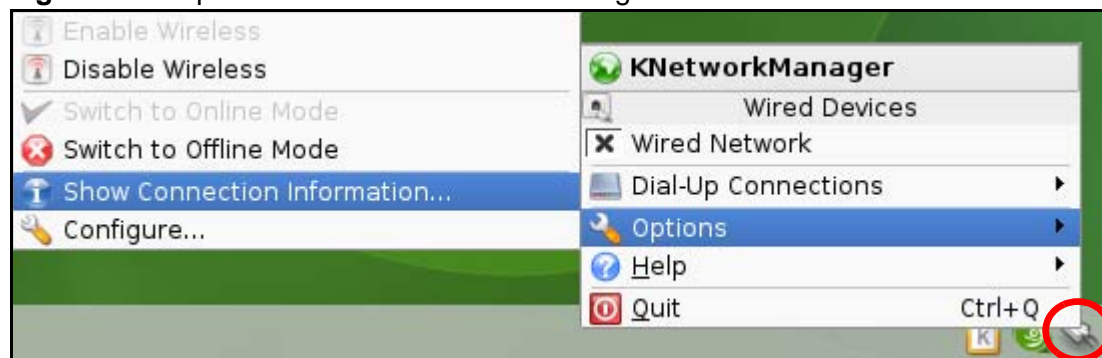


- 9 Click **Finish** to save your settings and close the window.

Verifying Settings

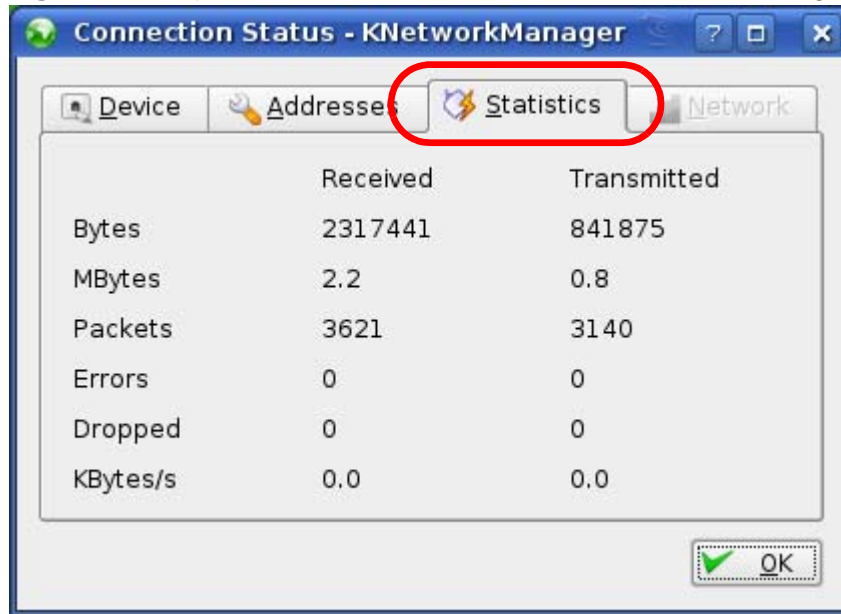
Click the **KNetwork Manager** icon on the **Task bar** to check your TCP/IP properties. From the **Options** sub-menu, select **Show Connection Information**.

Figure 186 openSUSE 10.3: KNetwork Manager



When the **Connection Status - KNetwork Manager** window opens, click the **Statistics tab** to see if your connection is working properly.

Figure 187 openSUSE: Connection Status - KNetwork Manager



Pop-up Windows, JavaScripts and Java Permissions

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

Note: Internet Explorer 6 screens are used here. Screens for other Internet Explorer versions may vary.

Internet Explorer Pop-up Blockers

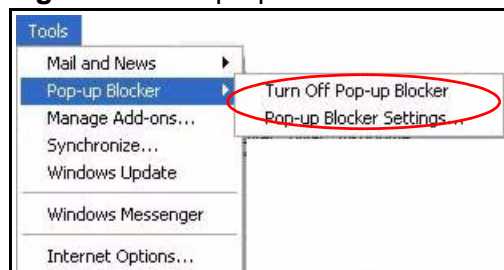
You may have to disable pop-up blocking to log into your device.

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or allow pop-up blocking and create an exception for your device's IP address.

Disable Pop-up Blockers

- 1 In Internet Explorer, select **Tools, Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

Figure 188 Pop-up Blocker



You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

- 1 In Internet Explorer, select **Tools, Internet Options, Privacy**.
- 2 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

Figure 189 Internet Options: Privacy



- 3 Click **Apply** to save this setting.

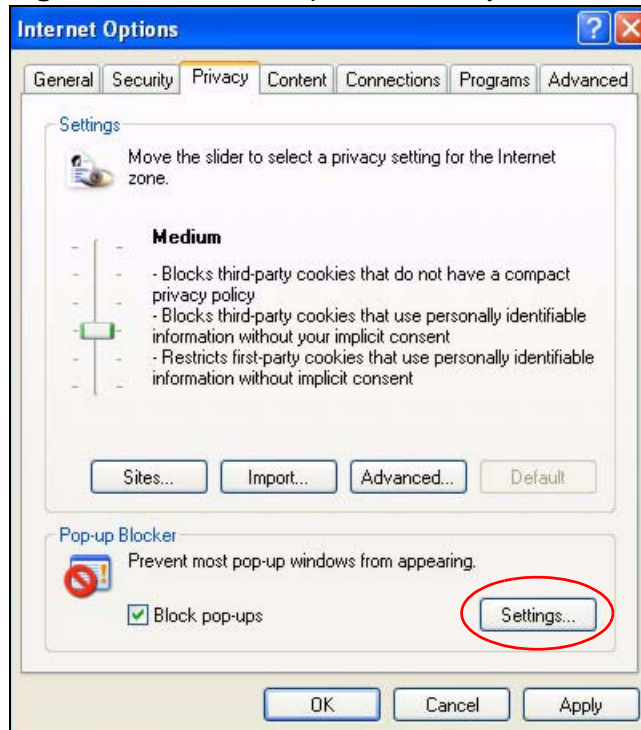
Enable Pop-up Blockers with Exceptions

Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

- 1 In Internet Explorer, select **Tools, Internet Options** and then the **Privacy** tab.

- 2 Select **Settings...** to open the **Pop-up Blocker Settings** screen.

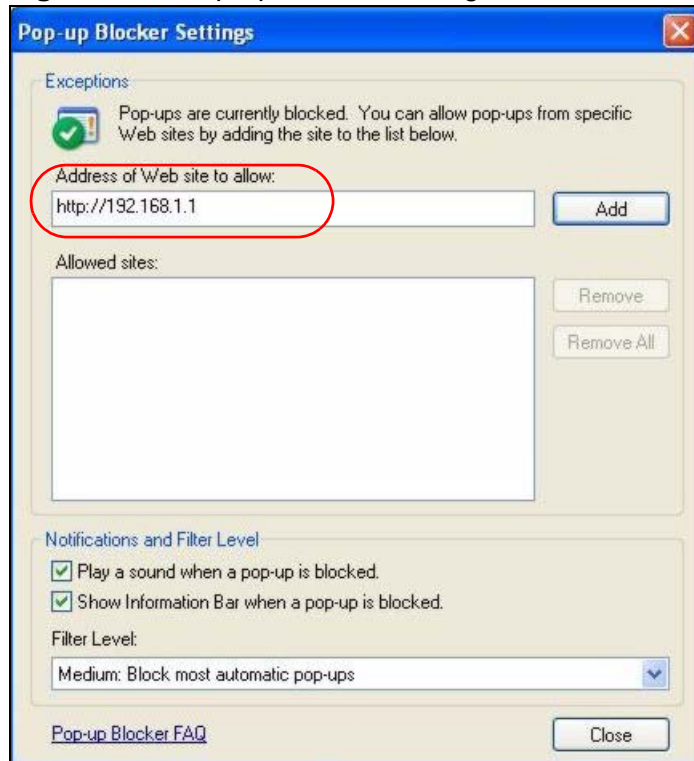
Figure 190 Internet Options: Privacy



- 3 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix "http://". For example, http://192.168.1.1.

- 4 Click **Add** to move the IP address to the list of **Allowed sites**.

Figure 191 Pop-up Blocker Settings



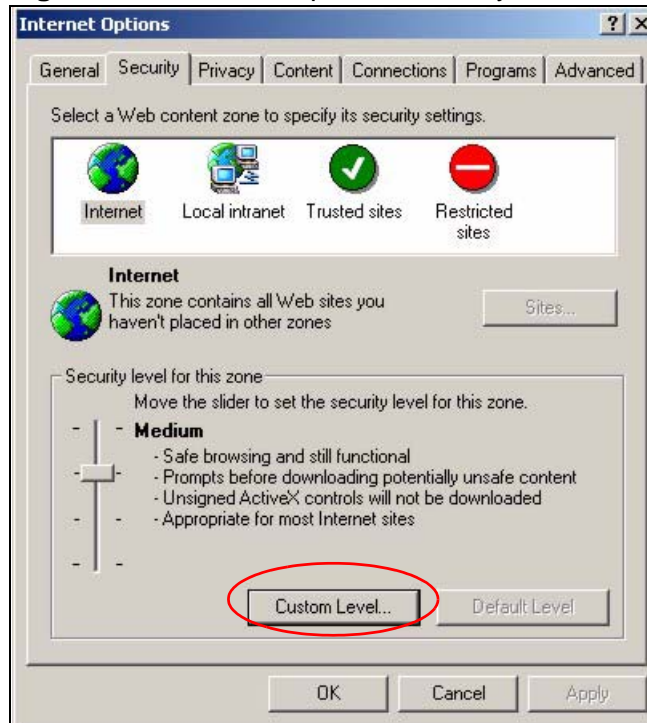
- 5 Click **Close** to return to the **Privacy** screen.
- 6 Click **Apply** to save this setting.

JavaScripts

If pages of the web configurator do not display properly in Internet Explorer, check that JavaScripts are allowed.

- 1 In Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

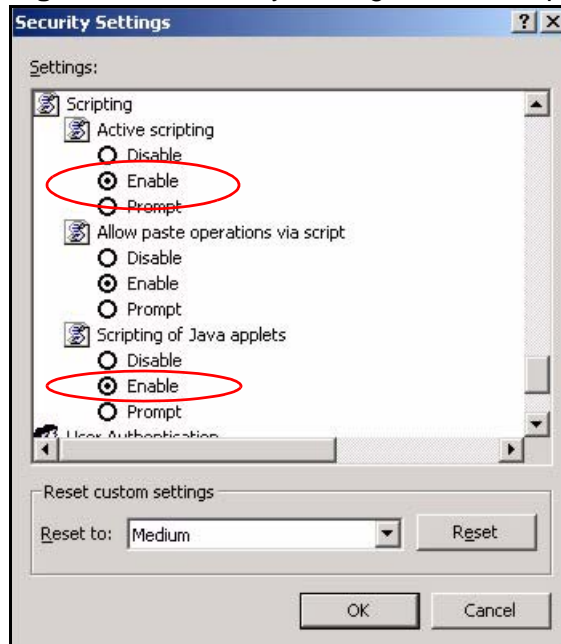
Figure 192 Internet Options: Security



- 2 Click the **Custom Level...** button.
- 3 Scroll down to **Scripting**.
- 4 Under **Active scripting** make sure that **Enable** is selected (the default).
- 5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).

- 6 Click **OK** to close the window.

Figure 193 Security Settings - Java Scripting

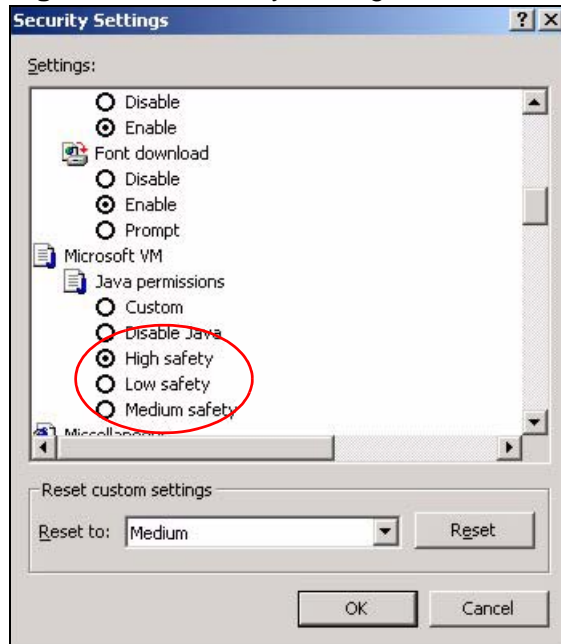


Java Permissions

- 1 From Internet Explorer, click **Tools, Internet Options** and then the **Security** tab.
- 2 Click the **Custom Level...** button.
- 3 Scroll down to **Microsoft VM**.
- 4 Under **Java permissions** make sure that a safety level is selected.

- 5 Click **OK** to close the window.

Figure 194 Security Settings - Java

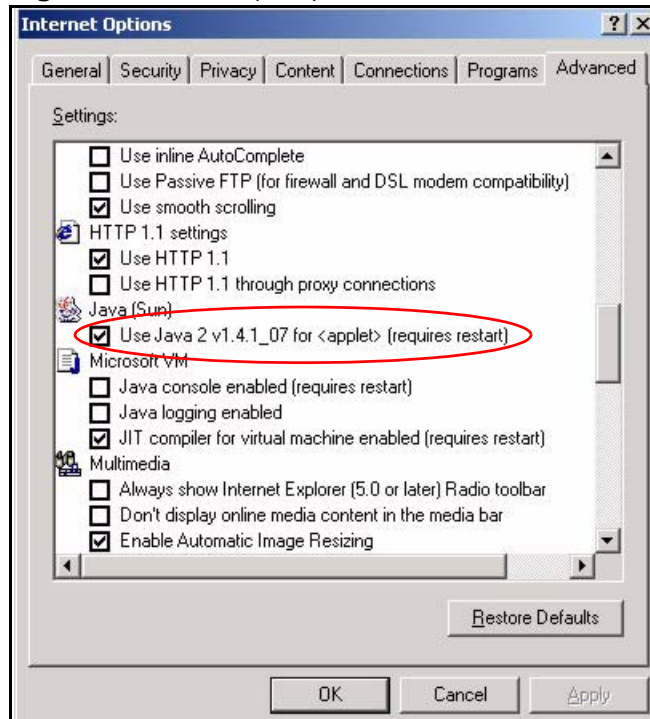


JAVA (Sun)

- 1 From Internet Explorer, click **Tools, Internet Options** and then the **Advanced** tab.
- 2 Make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.

- 3 Click **OK** to close the window.

Figure 195 Java (Sun)

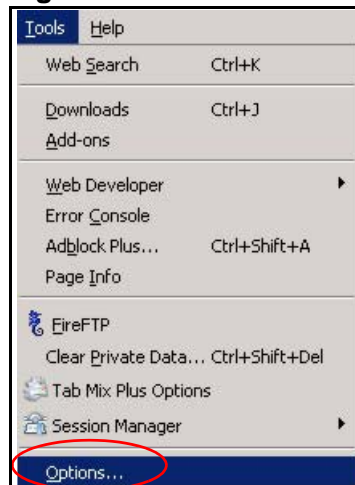


Mozilla Firefox

Mozilla Firefox 2.0 screens are used here. Screens for other versions may vary.

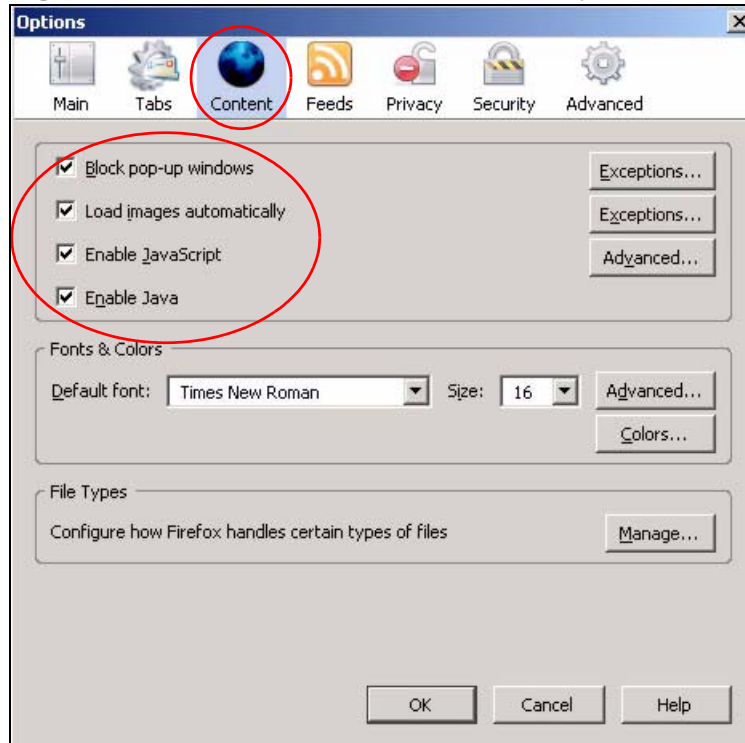
You can enable Java, Javascripts and pop-ups in one screen. Click **Tools**, then click **Options** in the screen that appears.

Figure 196 Mozilla Firefox: Tools > Options



Click **Content** to show the screen below. Select the check boxes as shown in the following screen.

Figure 197 Mozilla Firefox Content Security



IP Addresses and Subnetting

This appendix introduces IP addresses and subnet masks.

IP addresses identify individual devices on a network. Every networking device (including computers, servers, routers, printers, etc.) needs an IP address to communicate across the network. These networking devices are also known as hosts.

Subnet masks determine the maximum number of possible hosts on a network. You can also use subnet masks to divide one network into multiple sub-networks.

Introduction to IP Addresses

One part of the IP address is the network number, and the other part is the host ID. In the same way that houses on a street share a common street name, the hosts on a network share a common network number. Similarly, as each house has its own house number, each host on the network has its own unique identifying number - the host ID. Routers use the network number to send packets to the correct network, while the host ID determines to which host on the network the packets are delivered.

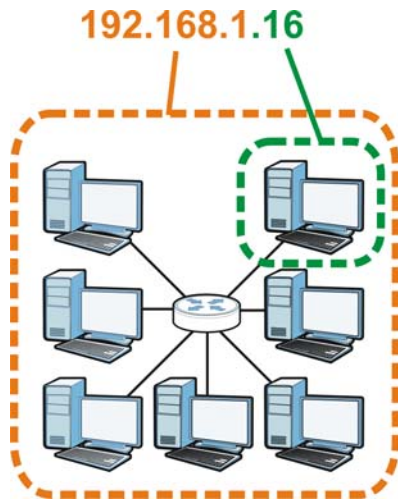
Structure

An IP address is made up of four parts, written in dotted decimal notation (for example, 192.168.1.1). Each of these four parts is known as an octet. An octet is an eight-digit binary number (for example 11000000, which is 192 in decimal notation).

Therefore, each octet has a possible range of 00000000 to 11111111 in binary, or 0 to 255 in decimal.

The following figure shows an example IP address in which the first three octets (192.168.1) are the network number, and the fourth octet (16) is the host ID.

Figure 198 Network Number and Host ID



How much of the IP address is the network number and how much is the host ID varies according to the subnet mask.

Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). The term “subnet” is short for “sub-network”.

A subnet mask has 32 bits. If a bit in the subnet mask is a “1” then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is “0” then the corresponding bit in the IP address is part of the host ID.

The following example shows a subnet mask identifying the network number (in bold text) and host ID of an IP address (192.168.1.2 in decimal).

Table 105 IP Address Network Number and Host ID Example

	1ST OCTET: (192)	2ND OCTET: (168)	3RD OCTET: (1)	4TH OCTET (2)
IP Address (Binary)	11000000	10101000	00000001	00000010
Subnet Mask (Binary)	11111111	11111111	11111111	00000000
Network Number	11000000	10101000	00000001	
Host ID				00000010

By convention, subnet masks always consist of a continuous sequence of ones beginning from the leftmost bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

Subnet masks can be referred to by the size of the network number part (the bits with a “1” value). For example, an “8-bit mask” means that the first 8 bits of the mask are ones and the remaining 24 bits are zeroes.

Subnet masks are expressed in dotted decimal notation just like IP addresses. The following examples show the binary and decimal notation for 8-bit, 16-bit, 24-bit and 29-bit subnet masks.

Table 106 Subnet Masks

	BINARY				DECIMAL
	1ST OCTET	2ND OCTET	3RD OCTET	4TH OCTET	
8-bit mask	11111111	00000000	00000000	00000000	255.0.0.0
16-bit mask	11111111	11111111	00000000	00000000	255.255.0.0
24-bit mask	11111111	11111111	11111111	00000000	255.255.255.0
29-bit mask	11111111	11111111	11111111	11111000	255.255.255.248

Network Size

The size of the network number determines the maximum number of possible hosts you can have on your network. The larger the number of network number bits, the smaller the number of remaining host ID bits.

An IP address with host IDs of all zeros is the IP address of the network (192.168.1.0 with a 24-bit subnet mask, for example). An IP address with host IDs of all ones is the broadcast address for that network (192.168.1.255 with a 24-bit subnet mask, for example).

As these two IP addresses cannot be used for individual hosts, calculate the maximum number of possible hosts in a network as follows:

Table 107 Maximum Host Numbers

SUBNET MASK		HOST ID SIZE		MAXIMUM NUMBER OF HOSTS
8 bits	255.0.0.0	24 bits	$2^{24} - 2$	16777214
16 bits	255.255.0.0	16 bits	$2^{16} - 2$	65534
24 bits	255.255.255.0	8 bits	$2^8 - 2$	254
29 bits	255.255.255.248	3 bits	$2^3 - 2$	6

Notation

Since the mask is always a continuous number of ones beginning from the left, followed by a continuous number of zeros for the remainder of the 32 bit mask, you can simply specify the number of ones instead of writing the value of each octet. This is usually specified by writing a "/" followed by the number of bits in the mask after the address.

For example, 192.1.1.0 /25 is equivalent to saying 192.1.1.0 with subnet mask 255.255.255.128.

The following table shows some possible subnet masks using both notations.

Table 108 Alternative Subnet Mask Notation

SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.0	/24	0000 0000	0
255.255.255.128	/25	1000 0000	128
255.255.255.192	/26	1100 0000	192
255.255.255.224	/27	1110 0000	224
255.255.255.240	/28	1111 0000	240
255.255.255.248	/29	1111 1000	248
255.255.255.252	/30	1111 1100	252

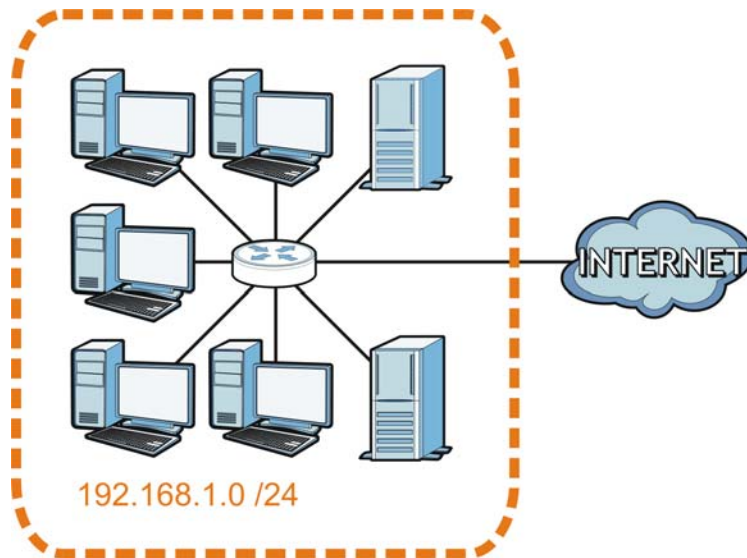
Subnetting

You can use subnetting to divide one network into multiple sub-networks. In the following example a network administrator creates two sub-networks to isolate a group of servers from the rest of the company network for security reasons.

In this example, the company network address is 192.168.1.0. The first three octets of the address (192.168.1) are the network number, and the remaining octet is the host ID, allowing a maximum of $2^8 - 2$ or 254 possible hosts.

The following figure shows the company network before subnetting.

Figure 199 Subnetting Example: Before Subnetting

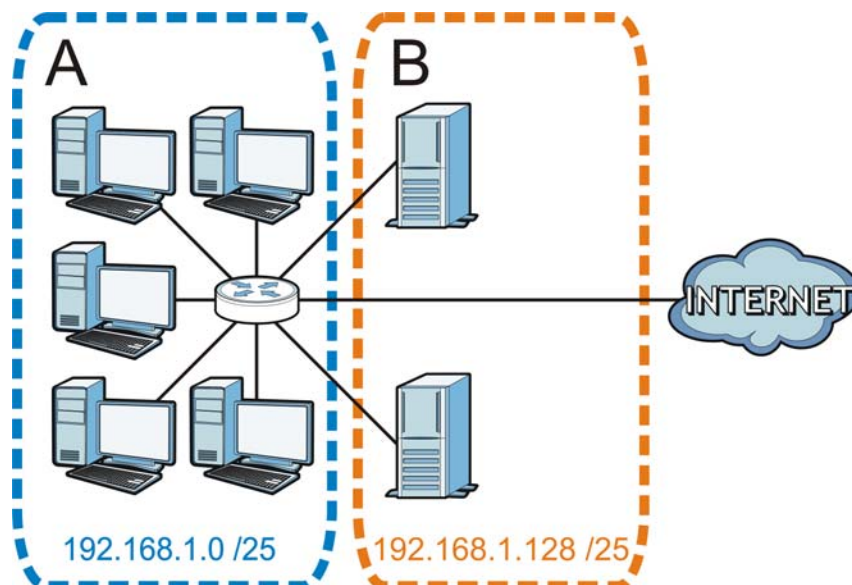


You can “borrow” one of the host ID bits to divide the network `192.168.1.0` into two separate sub-networks. The subnet mask is now 25 bits (`255.255.255.128` or `/25`).

The “borrowed” host ID bit can have a value of either 0 or 1, allowing two subnets; `192.168.1.0 /25` and `192.168.1.128 /25`.

The following figure shows the company network after subnetting. There are now two sub-networks, **A** and **B**.

Figure 200 Subnetting Example: After Subnetting



In a 25-bit subnet the host ID has 7 bits, so each sub-network has a maximum of $2^7 - 2$ or 126 possible hosts (a host ID of all zeroes is the subnet's address itself, all ones is the subnet's broadcast address).

192.168.1.0 with mask 255.255.255.128 is subnet **A** itself, and 192.168.1.127 with mask 255.255.255.128 is its broadcast address. Therefore, the lowest IP address that can be assigned to an actual host for subnet **A** is 192.168.1.1 and the highest is 192.168.1.126.

Similarly, the host ID range for subnet **B** is 192.168.1.129 to 192.168.1.254.

Example: Four Subnets

The previous example illustrated using a 25-bit subnet mask to divide a 24-bit address into two subnets. Similarly, to divide a 24-bit address into four subnets, you need to "borrow" two host ID bits to give four possible combinations (00, 01, 10 and 11). The subnet mask is 26 bits (11111111.11111111.11111111.11000000) or 255.255.255.192.

Each subnet contains 6 host ID bits, giving $2^6 - 2$ or 62 hosts for each subnet (a host ID of all zeroes is the subnet itself, all ones is the subnet's broadcast address).

Table 109 Subnet 1

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address (Decimal)	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	00000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

Table 110 Subnet 2

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	01000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.64	Lowest Host ID: 192.168.1.65	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Table 111 Subnet 3

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	10000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.191	Highest Host ID: 192.168.1.190	

Table 112 Subnet 4

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	11000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.192	Lowest Host ID: 192.168.1.193	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

Example: Eight Subnets

Similarly, use a 27-bit mask to create eight subnets (000, 001, 010, 011, 100, 101, 110 and 111).

The following table shows IP address last octet values for each subnet.

Table 113 Eight Subnets

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	225	254	255

Subnet Planning

The following table is a summary for subnet planning on a network with a 24-bit network number.

Table 114 24-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.255.128 (/25)	2	126
2	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

The following table is a summary for subnet planning on a network with a 16-bit network number.

Table 115 16-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14
13	255.255.255.248 (/29)	8192	6
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

Configuring IP Addresses

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP

addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. You must also enable Network Address Translation (NAT) on the CellPipe 7130 RG.

Once you have decided on the network number, pick an IP address for your CellPipe 7130 RG that is easy to remember (for instance, 192.168.1.1) but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your CellPipe 7130 RG will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the CellPipe 7130 RG unless you are instructed to do otherwise.

Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet (running only between two branch offices, for example) you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP, or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, Address Allocation for Private Internets and RFC 1466, Guidelines for Management of IP Address Space.

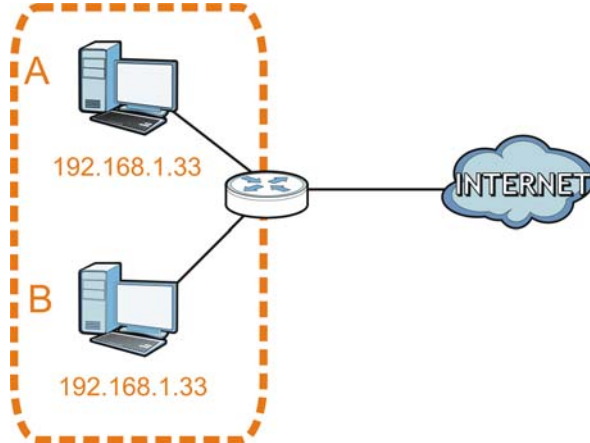
IP Address Conflicts

Each device on a network must have a unique IP address. Devices with duplicate IP addresses on the same network will not be able to access the Internet or other resources. The devices may also be unreachable through the network.

Conflicting Computer IP Addresses Example

More than one device can not use the same IP address. In the following example computer **A** has a static (or fixed) IP address that is the same as the IP address that a DHCP server assigns to computer **B** which is a DHCP client. Neither can access the Internet. This problem can be solved by assigning a different static IP address to computer **A** or setting computer **A** to obtain an IP address automatically.

Figure 201 Conflicting Computer IP Addresses Example

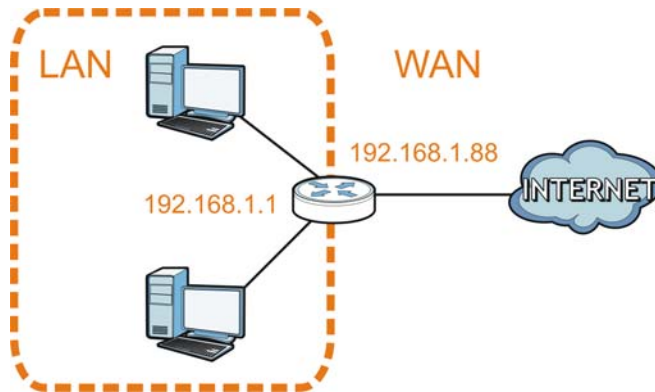


Conflicting Router IP Addresses Example

Since a router connects different networks, it must have interfaces using different network numbers. For example, if a router is set between a LAN and the Internet (WAN), the router's LAN and WAN addresses must be on different subnets. In the

following example, the LAN and WAN are on the same subnet. The LAN computers cannot access the Internet because the router cannot route between networks.

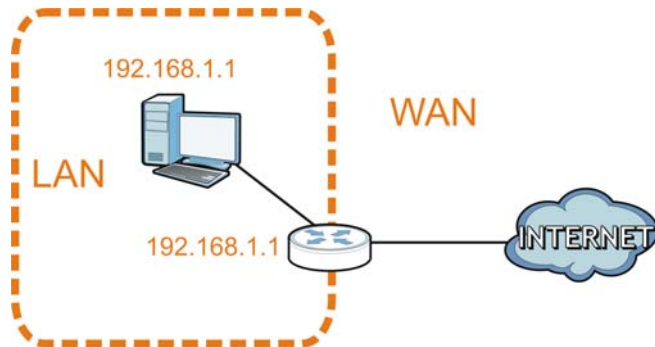
Figure 202 Conflicting Router IP Addresses Example



Conflicting Computer and Router IP Addresses Example

More than one device can not use the same IP address. In the following example, the computer and the router's LAN port both use 192.168.1.1 as the IP address. The computer cannot access the Internet. This problem can be solved by assigning a different IP address to the computer or the router's LAN port.

Figure 203 Conflicting Computer and Router IP Addresses Example



Wireless LANs

Note: Your specific CellPipe 7130 RG may not support all of the wireless security types described in this appendix. See the product specifications for more information about which wireless security types are supported.

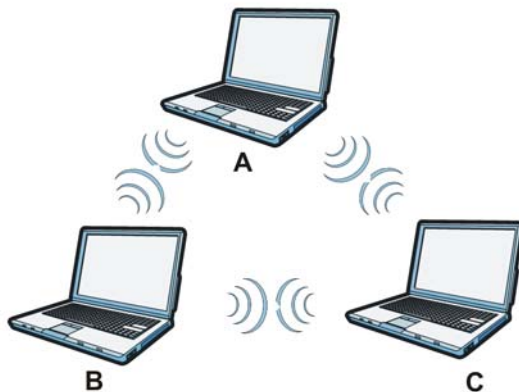
Wireless LAN Topologies

This section discusses ad-hoc and infrastructure wireless LAN topologies.

Ad-hoc Wireless LAN Configuration

The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless adapters (A, B, C). Any time two or more wireless adapters are within range of each other, they can set up an independent network, which is commonly referred to as an ad-hoc network or Independent Basic Service Set (IBSS). The following diagram shows an example of notebook computers using wireless adapters to form an ad-hoc wireless LAN.

Figure 204 Peer-to-Peer Communication in an Ad-hoc Network

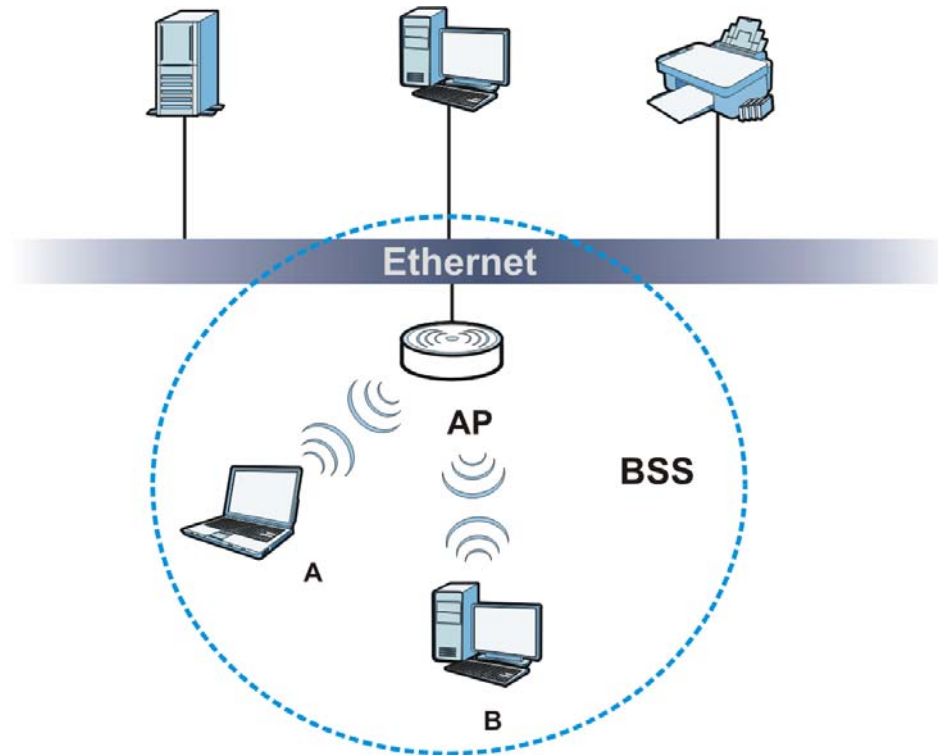


BSS

A Basic Service Set (BSS) exists when all communications between wireless clients or between a wireless client and a wired network client go through one access point (AP).

Intra-BSS traffic is traffic between wireless clients in the BSS. When Intra-BSS is enabled, wireless client **A** and **B** can access the wired network and communicate with each other. When Intra-BSS is disabled, wireless client **A** and **B** can still access the wired network but cannot communicate with each other.

Figure 205 Basic Service Set



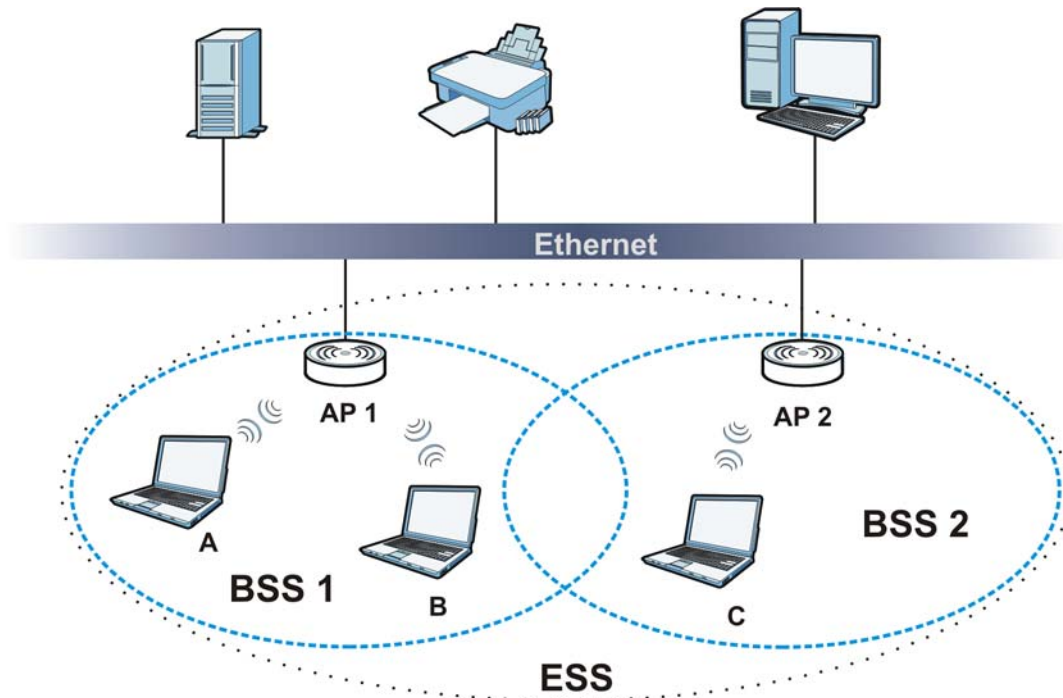
ESS

An Extended Service Set (ESS) consists of a series of overlapping BSSs, each containing an access point, with each access point connected together by a wired network. This wired connection between APs is called a Distribution System (DS).

This type of wireless LAN topology is called an Infrastructure WLAN. The Access Points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood.

An ESSID (ESS IDentification) uniquely identifies each ESS. All access points and their associated wireless clients within the same ESS must have the same ESSID in order to communicate.

Figure 206 Infrastructure WLAN



Channel

A channel is the radio frequency(ies) used by wireless devices to transmit and receive data. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a channel different from an adjacent AP (access point) to reduce interference. Interference occurs when radio signals from different access points overlap causing interference and degrading performance.

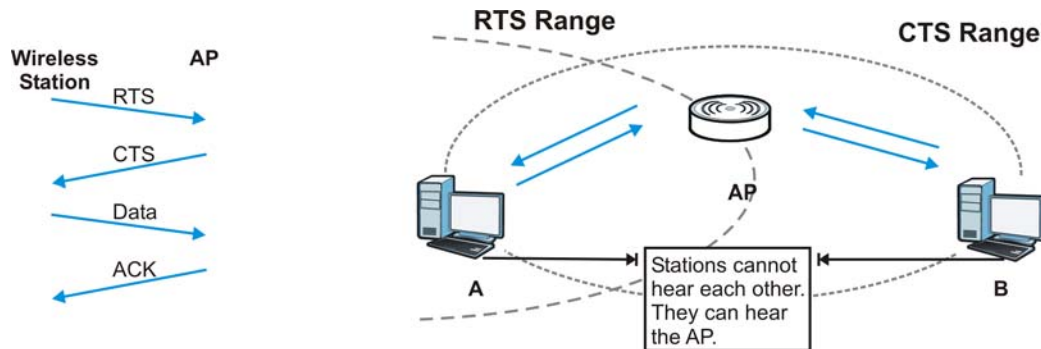
Adjacent channels partially overlap however. To avoid interference due to overlap, your AP should be on a channel at least five channels away from a channel that an adjacent AP is using. For example, if your region has 11 channels and an adjacent AP is using channel 1, then you need to select a channel between 6 or 11.

RTS/CTS

A hidden node occurs when two stations are within range of the same access point, but are not within range of each other. The following figure illustrates a

hidden node. Both stations (STA) are within range of the access point (AP) or wireless gateway, but out-of-range of each other, so they cannot "hear" each other, that is they do not know if the channel is currently being used. Therefore, they are considered hidden from each other.

Figure 207 RTS/CTS



When station **A** sends data to the AP, it might not know that the station **B** is already using the channel. If these two stations send data at the same time, collisions may occur when both sets of data arrive at the AP at the same time, resulting in a loss of messages for both stations.

RTS/CTS is designed to prevent collisions due to hidden nodes. An **RTS/CTS** defines the biggest size data frame you can send before an RTS (Request To Send)/CTS (Clear to Send) handshake is invoked.

When a data frame exceeds the **RTS/CTS** value you set (between 0 to 2432 bytes), the station that wants to transmit this frame must first send an RTS (Request To Send) message to the AP for permission to send it. The AP then responds with a CTS (Clear to Send) message to all other stations within its range to notify them to defer their transmission. It also reserves and confirms with the requesting station the time frame for the requested transmission.

Stations can send frames smaller than the specified **RTS/CTS** directly to the AP without the RTS (Request To Send)/CTS (Clear to Send) handshake.

You should only configure **RTS/CTS** if the possibility of hidden nodes exists on your network and the "cost" of resending large frames is more than the extra network overhead involved in the RTS (Request To Send)/CTS (Clear to Send) handshake.

If the **RTS/CTS** value is greater than the **Fragmentation Threshold** value (see next), then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

Note: Enabling the RTS Threshold causes redundant network overhead that could negatively affect the throughput performance instead of providing a remedy.

Fragmentation Threshold

A **Fragmentation Threshold** is the maximum data fragment size (between 256 and 2432 bytes) that can be sent in the wireless network before the AP will fragment the packet into smaller data frames.

A large **Fragmentation Threshold** is recommended for networks not prone to interference while you should set a smaller threshold for busy networks or networks that are prone to interference.

If the **Fragmentation Threshold** value is smaller than the **RTS/CTS** value (see previously) you set then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

Preamble Type

Preamble is used to signal that data is coming to the receiver. Short and long refer to the length of the synchronization field in a packet.

Short preamble increases performance as less time sending preamble means more time for sending data. All IEEE 802.11 compliant wireless adapters support long preamble, but not all support short preamble.

Use long preamble if you are unsure what preamble mode other wireless devices on the network support, and to provide more reliable communications in busy wireless networks.

Use short preamble if you are sure all wireless devices on the network support it, and to provide more efficient communications.

Use the dynamic setting to automatically use short preamble when all wireless devices on the network support it, otherwise the CellPipe 7130 RG uses long preamble.

Note: The wireless devices **MUST** use the same preamble mode in order to communicate.

IEEE 802.11g Wireless LAN

IEEE 802.11g is fully compatible with the IEEE 802.11b standard. This means an IEEE 802.11b adapter can interface directly with an IEEE 802.11g access point (and vice versa) at 11 Mbps or lower depending on range. IEEE 802.11g has

several intermediate rate steps between the maximum and minimum data rates. The IEEE 802.11g data rate and modulation are as follows:

Table 116 IEEE 802.11g

DATA RATE (MBPS)	MODULATION
1	DBPSK (Differential Binary Phase Shift Keyed)
2	DQPSK (Differential Quadrature Phase Shift Keying)
5.5 / 11	CCK (Complementary Code Keying)
6/9/12/18/24/36/ 48/54	OFDM (Orthogonal Frequency Division Multiplexing)

Wireless Security Overview

Wireless security is vital to your network to protect wireless communication between wireless clients, access points and the wired network.

Wireless security methods available on the CellPipe 7130 RG are data encryption, wireless client authentication, restricting access by device MAC address and hiding the CellPipe 7130 RG identity.

The following figure shows the relative effectiveness of these wireless security methods available on your CellPipe 7130 RG.

Table 117 Wireless Security Levels

SECURITY LEVEL	SECURITY TYPE
Least Secure	Unique SSID (Default)
	Unique SSID with Hide SSID Enabled
	MAC Address Filtering
	WEP Encryption
	IEEE802.1x EAP with RADIUS Server Authentication
Most Secure	Wi-Fi Protected Access (WPA)
	WPA2

Note: You must enable the same wireless security settings on the CellPipe 7130 RG and on all wireless clients that you want to associate with it.

IEEE 802.1x

In June 2001, the IEEE 802.1x standard was designed to extend the features of IEEE 802.11 to support extended authentication as well as providing additional

accounting and control features. It is supported by Windows XP and a number of network devices. Some advantages of IEEE 802.1x are:

- User based identification that allows for roaming.
- Support for RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile and accounting management on a network RADIUS server.
- Support for EAP (Extensible Authentication Protocol, RFC 2486) that allows additional authentication methods to be deployed with no changes to the access point or the wireless clients.

RADIUS

RADIUS is based on a client-server model that supports authentication, authorization and accounting. The access point is the client and the server is the RADIUS server. The RADIUS server handles the following tasks:

- Authentication
Determines the identity of the users.
- Authorization
Determines the network services available to authenticated users once they are connected to the network.
- Accounting
Keeps track of the client's network activity.

RADIUS is a simple package exchange in which your AP acts as a message relay between the wireless client and the network RADIUS server.

Types of RADIUS Messages

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user authentication:

- Access-Request
Sent by an access point requesting authentication.
- Access-Reject
Sent by a RADIUS server rejecting access.
- Access-Accept
Sent by a RADIUS server allowing access.
- Access-Challenge
Sent by a RADIUS server requesting more information in order to allow access. The access point sends a proper response from the user and then sends another Access-Request message.

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user accounting:

- Accounting-Request
Sent by the access point requesting accounting.
- Accounting-Response
Sent by the RADIUS server to indicate that it has started or stopped accounting.

In order to ensure network security, the access point and the RADIUS server use a shared secret key, which is a password, they both know. The key is not sent over the network. In addition to the shared key, password information exchanged is also encrypted to protect the network from unauthorized access.

Types of EAP Authentication

This section discusses some popular authentication types: EAP-MD5, EAP-TLS, EAP-TTLS, PEAP and LEAP. Your wireless LAN device may not support all authentication types.

EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE 802.1x transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, an access point helps a wireless station and a RADIUS server perform authentication.

The type of authentication you use depends on the RADIUS server and an intermediary AP(s) that supports IEEE 802.1x. .

For EAP-TLS authentication type, you must first have a wired connection to the network and obtain the certificate(s) from a certificate authority (CA). A certificate (also called digital IDs) can be used to authenticate users and a CA issues certificates and guarantees the identity of each certificate owner.

EAP-MD5 (Message-Digest Algorithm 5)

MD5 authentication is the simplest one-way authentication method. The authentication server sends a challenge to the wireless client. The wireless client 'proves' that it knows the password by encrypting the password with the challenge and sends back the information. Password is not sent in plain text.

However, MD5 authentication has some weaknesses. Since the authentication server needs to get the plaintext passwords, the passwords must be stored. Thus someone other than the authentication server may access the password file. In addition, it is possible to impersonate an authentication server as MD5 authentication method does not perform mutual authentication. Finally, MD5

authentication method does not support data encryption with dynamic session key. You must configure WEP encryption keys for data encryption.

EAP-TLS (Transport Layer Security)

With EAP-TLS, digital certifications are needed by both the server and the wireless clients for mutual authentication. The server presents a certificate to the client. After validating the identity of the server, the client sends a different certificate to the server. The exchange of certificates is done in the open before a secured tunnel is created. This makes user identity vulnerable to passive attacks. A digital certificate is an electronic ID card that authenticates the sender's identity. However, to implement EAP-TLS, you need a Certificate Authority (CA) to handle certificates, which imposes a management overhead.

EAP-TTLS (Tunneled Transport Layer Service)

EAP-TTLS is an extension of the EAP-TLS authentication that uses certificates for only the server-side authentications to establish a secure connection. Client authentication is then done by sending username and password through the secure connection, thus client identity is protected. For client authentication, EAP-TTLS supports EAP methods and legacy authentication methods such as PAP, CHAP, MS-CHAP and MS-CHAP v2.

PEAP (Protected EAP)

Like EAP-TTLS, server-side certificate authentication is used to establish a secure connection, then use simple username and password methods through the secured connection to authenticate the clients, thus hiding client identity. However, PEAP only supports EAP methods, such as EAP-MD5, EAP-MSCHAPv2 and EAP-GTC (EAP-Generic Token Card), for client authentication. EAP-GTC is implemented only by Cisco.

LEAP

LEAP (Lightweight Extensible Authentication Protocol) is a Cisco implementation of IEEE 802.1x.

Dynamic WEP Key Exchange

The AP maps a unique key that is generated with the RADIUS server. This key expires when the wireless connection times out, disconnects or reauthentication times out. A new WEP key is generated each time reauthentication is performed.

If this feature is enabled, it is not necessary to configure a default encryption key in the wireless security configuration screen. You may still configure and store keys, but they will not be used while dynamic WEP is enabled.

Note: EAP-MD5 cannot be used with Dynamic WEP Key Exchange

For added security, certificate-based authentications (EAP-TLS, EAP-TTLS and PEAP) use dynamic keys for data encryption. They are often deployed in corporate environments, but for public deployment, a simple user name and password pair is more practical. The following table is a comparison of the features of authentication types.

Table 118 Comparison of EAP Authentication Types

	EAP-MD5	EAP-TLS	EAP-TTLS	PEAP	LEAP
Mutual Authentication	No	Yes	Yes	Yes	Yes
Certificate – Client	No	Yes	Optional	Optional	No
Certificate – Server	No	Yes	Yes	Yes	No
Dynamic Key Exchange	No	Yes	Yes	Yes	Yes
Credential Integrity	None	Strong	Strong	Strong	Moderate
Deployment Difficulty	Easy	Hard	Moderate	Moderate	Moderate
Client Identity Protection	No	No	Yes	Yes	No

WPA and WPA2

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA.

Key differences between WPA or WPA2 and WEP are improved data encryption and user authentication.

If both an AP and the wireless clients support WPA2 and you have an external RADIUS server, use WPA2 for stronger data encryption. If you don't have an external RADIUS server, you should use WPA2-PSK (WPA2-Pre-Shared Key) that only requires a single (identical) password entered into each access point, wireless gateway and wireless client. As long as the passwords match, a wireless client will be granted access to a WLAN.

If the AP or the wireless clients do not support WPA2, just use WPA or WPA-PSK depending on whether you have an external RADIUS server or not.

Select WEP only when the AP and/or wireless clients do not support WPA or WPA2. WEP is less secure than WPA or WPA2.

Encryption

WPA improves data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x. WPA2 also uses TKIP when

required for compatibility reasons, but offers stronger encryption than TKIP with Advanced Encryption Standard (AES) in the Counter mode with Cipher block chaining Message authentication code Protocol (CCMP).

TKIP uses 128-bit keys that are dynamically generated and distributed by the authentication server. AES (Advanced Encryption Standard) is a block cipher that uses a 256-bit mathematical algorithm called Rijndael. They both include a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

WPA and WPA2 regularly change and rotate the encryption keys so that the same encryption key is never used twice.

The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients. This all happens in the background automatically.

The Message Integrity Check (MIC) is designed to prevent an attacker from capturing data packets, altering them and resending them. The MIC provides a strong mathematical function in which the receiver and the transmitter each compute and then compare the MIC. If they do not match, it is assumed that the data has been tampered with and the packet is dropped.

By generating unique data encryption keys for every data packet and by creating an integrity checking mechanism (MIC), with TKIP and AES it is more difficult to decrypt data on a Wi-Fi network than WEP and difficult for an intruder to break into the network.

The encryption mechanisms used for WPA(2) and WPA(2)-PSK are the same. The only difference between the two is that WPA(2)-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA(2)-PSK susceptible to brute-force password-guessing attacks but it's still an improvement over WEP as it employs a consistent, single, alphanumeric password to derive a PMK which is used to generate unique temporal encryption keys. This prevent all wireless devices sharing the same encryption keys. (a weakness of WEP)

User Authentication

WPA and WPA2 apply IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database. WPA2 reduces the number of key exchange messages from six to four (CCMP 4-way handshake) and shortens the time required to connect to a network. Other WPA2 authentication features that are different from WPA include key caching and pre-

authentication. These two features are optional and may not be supported in all wireless devices.

Key caching allows a wireless client to store the PMK it derived through a successful authentication with an AP. The wireless client uses the PMK when it tries to connect to the same AP and does not need to go with the authentication process again.

Pre-authentication enables fast roaming by allowing the wireless client (already connecting to an AP) to perform IEEE 802.1x authentication with another AP before connecting to it.

Wireless Client WPA Supplicants

A wireless client supplicant is the software that runs on an operating system instructing the wireless client how to use WPA. At the time of writing, the most widely available supplicant is the WPA patch for Windows XP, Funk Software's Odyssey client.

The Windows XP patch is a free download that adds WPA capability to Windows XP's built-in "Zero Configuration" wireless client. However, you must run Windows XP to use it.

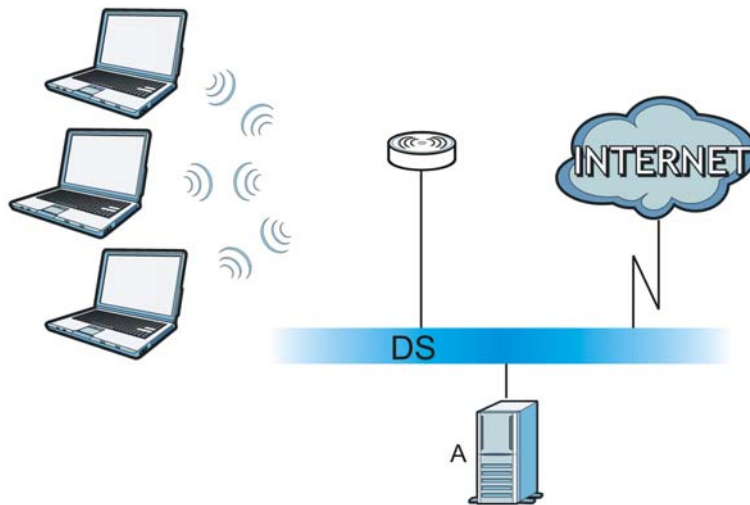
WPA(2) with RADIUS Application Example

To set up WPA(2), you need the IP address of the RADIUS server, its port number (default is 1812), and the RADIUS shared secret. A WPA(2) application example with an external RADIUS server looks as follows. "A" is the RADIUS server. "DS" is the distribution system.

- 1 The AP passes the wireless client's authentication request to the RADIUS server.
- 2 The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.
- 3 A 256-bit Pairwise Master Key (PMK) is derived from the authentication process by the RADIUS server and the client.

- 4 The RADIUS server distributes the PMK to the AP. The AP then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys. The keys are used to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients.

Figure 208 WPA(2) with RADIUS Application Example



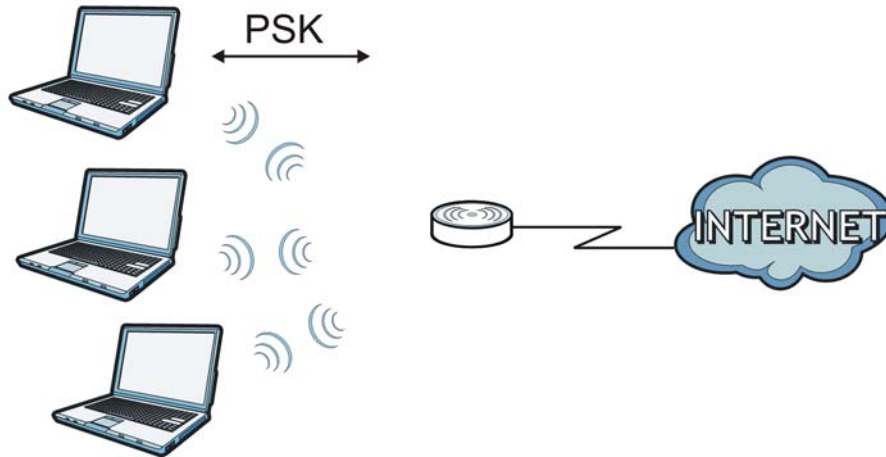
WPA(2)-PSK Application Example

A WPA(2)-PSK application looks as follows.

- 1 First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must consist of between 8 and 63 ASCII characters or 64 hexadecimal characters (including spaces and symbols).
- 2 The AP checks each wireless client's password and allows it to join the network only if the password matches.
- 3 The AP and wireless clients generate a common PMK (Pairwise Master Key). The key itself is not sent over the network, but is derived from the PSK and the SSID.

- 4 The AP and wireless clients use the TKIP or AES encryption process, the PMK and information exchanged in a handshake to create temporal encryption keys. They use these keys to encrypt data exchanged between them.

Figure 209 WPA(2)-PSK Authentication



Security Parameters Summary

Refer to this table to see what other security parameters you should configure for each authentication method or key management protocol type. MAC address filters are not dependent on how you configure these security features.

Table 119 Wireless Security Relational Matrix

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL	ENCRYPTION METHOD	ENTER MANUAL KEY	IEEE 802.1X
Open	None	No	Disable
		Yes	Enable without Dynamic WEP Key
Open	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
Shared	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
WPA	TKIP/AES	No	Enable
WPA-PSK	TKIP/AES	Yes	Disable
WPA2	TKIP/AES	No	Enable
WPA2-PSK	TKIP/AES	Yes	Disable

Antenna Overview

An antenna couples RF signals onto air. A transmitter within a wireless device sends an RF signal to the antenna, which propagates the signal through the air. The antenna also operates in reverse by capturing RF signals from the air.

Positioning the antennas properly increases the range and coverage area of a wireless LAN.

Antenna Characteristics

Frequency

An antenna in the frequency of 2.4GHz (IEEE 802.11b and IEEE 802.11g) or 5GHz (IEEE 802.11a) is needed to communicate efficiently in a wireless LAN

Radiation Pattern

A radiation pattern is a diagram that allows you to visualize the shape of the antenna's coverage area.

Antenna Gain

Antenna gain, measured in dB (decibel), is the increase in coverage within the RF beam width. Higher antenna gain improves the range of the signal for better communications.

For an indoor site, each 1 dB increase in antenna gain results in a range increase of approximately 2.5%. For an unobstructed outdoor site, each 1dB increase in gain results in a range increase of approximately 5%. Actual results may vary depending on the network environment.

Antenna gain is sometimes specified in dBi, which is how much the antenna increases the signal power compared to using an isotropic antenna. An isotropic antenna is a theoretical perfect antenna that sends out radio signals equally well in all directions. dBi represents the true gain that the antenna provides.

Types of Antennas for WLAN

There are two types of antennas used for wireless LAN applications.

- Omni-directional antennas send the RF signal out in all directions on a horizontal plane. The coverage area is torus-shaped (like a donut) which makes these antennas ideal for a room environment. With a wide coverage area, it is possible to make circular overlapping coverage areas with multiple access points.
- Directional antennas concentrate the RF signal in a beam, like a flashlight does with the light from its bulb. The angle of the beam determines the width of the coverage pattern. Angles typically range from 20 degrees (very directional) to 120 degrees (less directional). Directional antennas are ideal for hallways and outdoor point-to-point applications.

Positioning Antennas

In general, antennas should be mounted as high as practically possible and free of obstructions. In point-to-point application, position both antennas at the same height and in a direct line of sight to each other to attain the best performance.

For omni-directional antennas mounted on a table, desk, and so on, point the antenna up. For omni-directional antennas mounted on a wall or ceiling, point the antenna down. For a single AP application, place omni-directional antennas as close to the center of the coverage area as possible.

For directional antennas, point the antenna in the direction of the desired coverage area.

Common Services

The following table lists some commonly-used services and their associated protocols and port numbers. For a comprehensive list of port numbers, ICMP type/code numbers and services, visit the IANA (Internet Assigned Number Authority) web site.

- **Name:** This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol:** This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **USER-DEFINED**, the **Port(s)** is the IP protocol number, not the port number.
- **Port(s):** This value depends on the **Protocol**. Please refer to RFC 1700 for further information about port numbers.
 - If the **Protocol** is **TCP, UDP, or TCP/UDP**, this is the IP port number.
 - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description:** This is a brief explanation of the applications that use this service or the situations in which this service is used.

Table 120 Commonly Used Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM/New-ICQ	TCP	5190	AOL's Internet Messenger service. It is also used as a listening port by ICQ.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP UDP	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names to IP numbers.
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.

Table 120 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP	TCP TCP	20 21	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323	TCP	1720	NetMeeting uses this protocol.
HTTP	TCP	80	Hyper Text Transfer Protocol - a client/server protocol for the world wide web.
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic or routing purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Management Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.
NFS	UDP	2049	Network File System - NFS is a client/server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING	User-Defined	1	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).

Table 120 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.
RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
REXEC	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.
RTELNET	TCP	107	Remote Telnet.
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP	TCP	115	Simple File Transfer Protocol.
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC: 1215).
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSH	TCP/UDP	22	Secure Shell Remote Login Program.
STRM WORKS	UDP	1558	Stream Works Protocol.
SYSLOG	UDP	514	Syslog allows you to send system logs to a UNIX server.
TACACS	UDP	49	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET	TCP	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.

Table 120 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
TFTP	UDP	69	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE	TCP	7000	Another videoconferencing solution.

Legal Information

Certifications

Federal Communications Commission (FCC) Interference Statement

The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

This device 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 device 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 device does cause harmful interference to radio/television reception, which can be determined by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- 1 Reorient or relocate the receiving antenna.
- 2 Increase the separation between the equipment and the receiver.
- 3 Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- 4 Consult the dealer or an experienced radio/TV technician for help.



FCC Radiation Exposure Statement

- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
- IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.
- To comply with FCC RF exposure compliance requirements, a separation distance of at least 20 cm must be maintained between the antenna of this device and all persons.

Industry Canada Statement

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions:

- 1) this device may not cause interference and
- 2) this device must accept any interference, including interference that may cause undesired operation of the device

This device has been designed to operate with an antenna having a maximum gain of 2dBi.

Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the EIRP is not more than required for successful communication.

IMPORTANT NOTE

Device for the band 5150-5250 MHz is only for indoor usage to reduce potential for harmful interference to co-channel mobile satellite systems; users should also be cautioned to take note that high-power radars are allocated as primary users (meaning they have priority) of the bands 5250-5350 MHz and 5650-5850 MHz and these radars could cause interference and/or damage to LE-LAN devices.

IC Radiation Exposure Statement

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. End users must follow the specific operating instructions for satisfying RF exposure compliance.

注意 !

依據 低功率電波輻射性電機管理辦法

第十二條 經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前項合法通信，指依電信規定作業之無線電信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

本機限在不干擾合法電臺與不受被干擾保障條件下於室內使用。減少電磁波影響，請妥適使用。

Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device has been designed for the WLAN 2.4 GHz network throughout the EC region and Switzerland, with restrictions in France.

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two 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.

For a Class B digital device or peripheral, the instructions furnished the user shall include the following or similar statement, placed in a prominent location in the text of the manual:

NOTE: 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.

(c) The provisions of paragraphs (a) and (b) do not apply to digital devices exempted from the technical standards under the provisions of Section 15.103.

(d) For systems incorporating several digital devices, the statement shown in paragraph (a) or (b) needs to be contained only in the instruction manual for the main control unit.

(e) In cases where the manual is provided only in a form other than paper, such as on a computer disk or over the Internet, the information required by this section may be included in the manual in that alternative form, provided the user can reasonably be expected to have the capability to access information in that form.

RF exposure warning

This equipment must be installed and operated in accordance with provided instructions and the antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter. End-users and installers must be provide with antenna installation instructions and transmitter operating conditions for satisfying RF exposure compliance.

Index

A

ACS [239](#)
ADSL
 compliance [301](#)
 dual latency [301](#)
 EOC [301](#)
 multi-mode [301](#)
 TPS-TC [301](#)
 vendor ID [301](#)
Advanced Encryption Standard
 See AES.
AES [383](#)
ALG [177](#)
alternative subnet mask notation [364](#)
antenna [297](#)
 directional [388](#)
 gain [387](#)
 omni-directional [388](#)
AP (access point) [375](#)
Application Layer Gateway [177](#)
applications
 Internet access [20](#)
 media server [187](#)
 iTunes server [23](#)
arp [313](#)
ATM Adaptation Layer 5 (AAL5) [124](#)
Auto Configuration Server, see ACS [239](#)

B

backup [278](#)
Basic Service Set, See BSS [373](#)
blinking LEDs [26](#)
broadcast [129](#)
BSS [373](#)

C

CA [197](#), [381](#)
Canonical Format Indicator See CFI
CBR (Continuous Bit Rate) [109](#)
CCMs [283](#)
certificate
 details [202](#)
 factory default [198](#)
Certificate Authority
 See CA.
certificates [197](#)
 authentication [197](#)
 CA
 creating [199](#)
 importing [200](#), [203](#)
 public key [197](#)
 replacing [198](#)
 storage space [198](#)
Certification Authority [197](#)
Certification Authority. see CA
certifications [393](#)
 notices [395](#)
CFI [129](#)
CFM [283](#)
 CCMs [283](#)
 link trace test [284](#)
 loopback test [284](#)
 MA [283](#)
 MD [283](#)
 MEP [283](#)
 MIP [283](#)
channel [375](#)
 interference [375](#)
channel ID [143](#)
CIFS [182](#)
CIFS (Common Internet File System) [183](#), [188](#),
 [189](#)
command parameters [306](#)
command syntax [306](#)

Common Internet File System (CIFS) [183](#), [188](#), [189](#)
Common Internet File System, see CIFS
compliance [300](#)
configuration [132](#), [135](#)
Connectivity Check Messages, see CCMs
copyright [393](#)
CoS [234](#)
CoS technologies [221](#)
CPU usage [93](#)
creating certificates [199](#)
CTS (Clear to Send) [376](#)

D

date and time [93](#)
default [280](#)
default LAN IP address [84](#)
DHCP [99](#), [132](#), [135](#), [237](#)
DHCP client [99](#)
DHCP client list [99](#)
DHCP relay [299](#)
DHCP server [299](#)
diagnostic [284](#), [287](#)
Differentiated Services, see DiffServ [234](#)
DiffServ [234](#)
 marking rule [235](#)
digital IDs [197](#)
DLNA [23](#)
DNS [132](#)
DNS server address assignment [129](#)
Domain Name [178](#)
domain name system
 see DNS
Domain Name System. See DNS.
DS field [235](#)
DS, dee differentiated services
DSCP [234](#)
DSL interface [104](#)
dynamic DNS [237](#)
Dynamic Host Configuration Protocol. See DHCP.
dynamic WEP key exchange [381](#)

DYNDNS wildcard [237](#)

E

EAP Authentication [380](#)
ECHO [178](#)
Encapsulation [123](#)
 MER [123](#)
 PPP over Ethernet [123](#)
 PPPoA [124](#)
encapsulation
 RFC 1483 [124](#)
encryption [382](#)
 WEP [147](#)
end-to-end loopback test [287](#)
ESS [374](#)
ESSID [93](#)
Extended Service Set IDentification [144](#)
Extended Service Set, See ESS [374](#)

F

F4 cells [287](#)
F5 cells [287](#)
FCC interference statement [393](#)
file sharing [23](#), [183](#), [188](#), [189](#)
Finger [178](#)
firmware
 upload [276](#)
 upload error [277](#)
firmware version [92](#)
fragmentation threshold [377](#)
FTP [172](#), [178](#)

H

hidden node [375](#)
host [268](#)
host name [92](#)
HTTP [178](#), [191](#), [192](#)
HTTP (Hypertext Transfer Protocol) [276](#)

humidity [297](#)

I

IANA [136](#), [369](#)

IBSS [373](#)

IEEE 802.11g [377](#)

IEEE 802.1Q [128](#)

IGMP [129](#), [132](#)

version [129](#)

IGMP proxy [301](#)

IGMP snooping [262](#)

IGMP v1 [301](#)

IGMP v2 [301](#)

importing certificates [200](#), [203](#)

Independent Basic Service Set

See IBSS [373](#)

initialization vector (IV) [383](#)

install UPnP [247](#)

Windows Me [247](#)

Windows XP [248](#)

internal routing table [96](#)

Internet access [20](#)

Internet Assigned Numbers Authority

See IANA [369](#)

internet mode [102](#), [104](#)

DSL

ATM [102](#)

PTM [102](#)

ethernet [103](#)

IP Address [176](#)

IP address [135](#)

IP Address Assignment [126](#)

IP filter

basics [191](#)

creating or editing rules [194](#)

introduction [191](#)

policies [192](#)

IP multicasting [301](#)

IP pool [134](#)

IP pool setup [135](#)

ipconfig [307](#)

ipconfig, release [308](#)

ipconfig, renew [308](#)

iTunes server [23](#)

L

LAN statistics [98](#)

LAN TCP/IP [135](#)

LAN-Side DSL CPE Configuration [241](#)

LBR [284](#)

link trace [284](#)

Link Trace Message, see LTM

Link Trace Response, see LTR

logs [271](#)

overview [271](#)

settings [272](#)

Loop Back Response, see LBR

loopback [284](#)

LTM [284](#)

LTR [284](#)

M

MA [283](#)

MAC [92](#)

MAC address [92](#)

MAC address filter action [151](#)

MAC filter [150](#), [151](#)

Maintenance Association, see MA

Maintenance Domain, see MD

Maintenance End Point, see MEP

managing the device

good habits [20](#)

Maximum Burst Size (MBS) [110](#), [125](#)

MD [283](#)

media server [187](#)

DLNA [187](#)

enable [189](#)

memory usage [93](#)

MEP [283](#)

Message Integrity Check (MIC) [382](#)

MTU (Multi-Tenant Unit) [128](#)

multicast [129](#), [132](#)

multiplexing [124](#)

- LLC-based [124](#)
- VC-based [124](#)
- multiprotocol encapsulation [124](#)

N

- NAT [136](#), [171](#), [369](#)
 - default server [176](#)
 - DMZ host [176](#)
 - external port [173](#)
 - internal port [173](#)
 - port forwarding [172](#)
 - port number [172](#), [178](#)
 - services [178](#)
 - Symmetric [127](#)
- NAT example [179](#)
- NAT traversal [245](#)
- netstat [317](#)
- Network Address Translation, see NAT
- network troubleshooting [305](#)
 - arp [313](#)
 - ipconfig [307](#)
 - netstat [317](#)
 - ping [309](#)
 - route [314](#)
 - tracert [311](#)
- NNTP [178](#)

O

- OAM [287](#)
- OAM ping test [287](#)
- operation humidity [297](#)
- operation temperature [297](#)
- Operation, Administration and Maintenance, see OAM

P

- Packet Transfer Mode [104](#)
- Pairwise Master Key (PMK) [383](#), [385](#)
- Peak Cell Rate (PCR) [109](#), [125](#)

- Per-Hop Behavior, see PHB [235](#)
- PHB [235](#)
- ping [309](#)
 - timeout [310](#)
- Point to Point Protocol over ATM Adaptation Layer 5 (AAL5) [124](#)
- Point-to-Point Tunneling Protocol [178](#)
- POP3 [178](#), [191](#), [192](#)
- ports [26](#)
- power adaptor [302](#)
- power specifications [297](#)
- PPP (Point-to-Point Protocol) Link Layer Protocol [301](#)
- PPPoE [124](#)
 - Benefits [124](#)
- PPPoE (Point-to-Point Protocol over Ethernet) [299](#)
- PPTP [178](#)
- preamble mode [377](#)
- print server [23](#)
- PSK [383](#)
- PTM [104](#)

Q

- QoS [219](#), [234](#)
 - marking [221](#)
 - setup [219](#)
 - tagging [221](#)
 - versus CoS [221](#)
- Quality of Service, see QoS
- Quick Start Guide [84](#)

R

- RADIUS [379](#)
 - message types [379](#)
 - messages [379](#)
 - shared secret key [380](#)
- related documentation [3](#)
- remote management
 - TR-069 [239](#)
- Remote Procedure Calls, see RPCs [239](#)

restore [278](#)
 RFC 1058. See RIP.
 RFC 1389. See RIP.
 RFC 1483 [124](#)
 RFC 1631 [171](#)
 RFC 2131. See DHCP.
 RFC 2132. See DHCP
 RFC 2516 [299](#)
 RIP [132](#), [217](#)
 Routing Information Protocol
 see RIP
 route [314](#)
 route status [96](#)
 router features [20](#)
 routing information [96](#)
 Routing Information Protocol. See RIP
 RPPCs [239](#)
 RTS (Request To Send) [376](#)
 threshold [375](#), [376](#)

S

safety warnings [6](#)
 segment loopback test [287](#)
 service access control [242](#)
 Service Set [144](#)
 Services [178](#)
 sharing files [183](#), [188](#), [189](#)
 SIP ALG [177](#)
 SIP Application Layer Gateway [177](#)
 SMTP [178](#)
 SNMP [178](#), [301](#)
 SNMP trap [178](#)
 static route [209](#), [213](#), [217](#)
 static VLAN
 status indicators [26](#)
 storage humidity [297](#)
 storage temperature [297](#)
 subnet [361](#)
 subnet mask [135](#), [362](#)
 subnetting [364](#)
 Sustain Cell Rate (SCR) [110](#)

Sustained Cell Rate (SCR) [125](#)
 Symmetric NAT [127](#)
 Symmetric NAT, Outgoing [128](#)
 syntax conventions [4](#)
 system name [92](#)

T

Tag Control Information See TCI
 Tag Protocol Identifier See TPID
 TCI
 TCP/IP [191](#)
 temperature [297](#)
 Temporal Key Integrity Protocol (TKIP) [382](#)
 TPID [128](#)
 TR-064 [241](#)
 TR-069 [239](#)
 ACS setup [239](#)
 authentication [240](#)
 tracertr [311](#)
 traffic shaping [125](#)
 transparent bridging [301](#)

U

unicast [129](#)
 Universal Plug and Play [245](#)
 application [246](#)
 UPnP [245](#)
 forum [246](#)
 security issues [246](#)
 USB device removal [188](#)
 USB features [23](#)
 USB printer [23](#)
 user levels [83](#)
 admin [83](#)
 installer [83](#)
 privileged [83](#)
 root [83](#)
 subscriber [83](#)
 tech [83](#)

VVCI [287](#)VDSL [300](#)band plans [300](#)HDLC [300](#)INP [300](#)MCM [300](#)profiles [300](#)SNR [300](#)SNRM [300](#)SRA [300](#)tone spacing [300](#)TPS-TC [300](#)USO types [300](#)

VID

virtual channel [287](#)Virtual Circuit (VC) [124](#)virtual circuits [287](#)terminology [287](#)

Virtual Local Area Network See VLAN

virtual path [287](#)VLAN [128](#)Introduction [128](#)

number of possible VLANs

priority frame

static

VLAN ID [128](#)

VLAN Identifier See VID

VLAN tag [128](#)VPI [287](#)ping [309](#)route [314](#)tracert [311](#)wireless client WPA supplicants [384](#)wireless security [378](#)wireless station list [97](#)Wireless tutorial [29](#)

WLAN

interference [375](#)security parameters [386](#)WLAN button [28](#)WPA [382](#)key caching [384](#)pre-authentication [384](#)user authentication [383](#)vs WPA-PSK [383](#)wireless client supplicant [384](#)with RADIUS application example [384](#)WPA2 [382](#)user authentication [383](#)vs WPA2-PSK [383](#)wireless client supplicant [384](#)with RADIUS application example [384](#)WPA2-Pre-Shared Key [382](#)WPA2-PSK [382](#), [383](#)application example [385](#)WPA-PSK [382](#), [383](#)application example [385](#)

WPS

status [93](#)**W**WAN (Wide Area Network) [101](#)WAN interface [95](#)WAN statistics [94](#)Web Configurator [83](#), [84](#)WEP encryption [148](#)Wi-Fi Protected Access [382](#)Windows Command Prompt [306](#)arp [313](#)command parameters [306](#)ipconfig [307](#)netstat [317](#)

