# 9.6 UPnP Screen

Use this screen to enable UPnP on your EMG2881-T20A.

Click Configuration > Applications > UPnP to display the screen shown next.

Figure 46 Configuration > Applications > UPnP

UPnP		Apply	Cancel
UPnP :	Enable O Disable		

The following table describes the fields in this screen.

LABEL	DESCRIPTION
UPnP	Select <b>Enable</b> to activate UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the EMG2881-T20A's IP address (although you must still enter the password to access the web configurator).
Apply	Click <b>Apply</b> to save the setting to the EMG2881-T20A.
Cancel	Click Cancel to return to the previously saved settings.

Table 37 Configuration > Applications > UPnP

# 9.7 Technical Reference

The following section contains additional technical information about the EMG2881-T20A 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).

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".	

Table 38 IEEE 802.1 p Priority Level and Traffic Type

PRIORITY LEVEL	TRAFFIC TYPE
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.

Table 38 IEEE 802.1p Priority Level and Traffic Type

### 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.

DSCP (6 bits)	Unused (2 bits)
---------------	-----------------

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.

### **IP Precedence**

Similar to IEEE 802.1 p prioritization at layer-2, you can use IP precedence to prioritize packets in a layer-3 network. IP precedence uses three bits of the eight-bit ToS (Type of Service) field in the IP header. There are eight classes of services (ranging from zero to seven) in IP precedence. Zero is the lowest priority level and seven is the highest.

### Automatic Priority Queue Assignment

If you enable QoS on the EMG2881-T20A, the EMG2881-T20A can automatically base on the IEEE 802.1p priority level, IP precedence and/or packet length to assign priority to traffic which does not match a class.

The following table shows you the internal layer-2 and layer-3 QoS mapping on the EMG2881-T20A. On the EMG2881-T20A, traffic assigned to higher priority queues gets through faster while traffic in lower index queues is dropped if the network is congested.

	LAYER 2 LAYER 3			
Priority Queue	IEEE 802.1P USER PRIORITY (ETHERNET PRIORITY)	TOS (IP PRECEDENCE)	DSCP	IP PACKET LENGTH (BYTE)
0	1	0	000000	
1	2			
2	0	0	000000	>1100
3	3	1	001110	250~1100
			001100	
			001010	
			001000	
4	4	2	010110	
			010100	
			010010	
			010000	
5	5	3	011110	<250
			011100	
			011010	
			011000	
6	6	4	100110	
			100100	
			100010	
			100000	
		5	101110	
			101000	
7	7	6	110000	
		7	111000	

Table 39 Internal Layer2 and Layer3 QoS Mapping

### **Token Bucket**

The token bucket algorithm uses tokens in a bucket to control when traffic can be transmitted. The bucket stores tokens, each of which represents one byte. The algorithm allows bursts of up to *b* bytes which is also the bucket size, so the bucket can hold up to *b* tokens. Tokens are generated and added into the bucket at a constant rate. The following shows how tokens work with packets:

- A packet can be transmitted if the number of tokens in the bucket is equal to or greater than the size of the packet (in bytes).
- After a packet is transmitted, a number of tokens corresponding to the packet size is removed from the bucket.

- If there are no tokens in the bucket, the EMG2881-T20A stops transmitting until enough tokens are generated.
- If not enough tokens are available, the EMG2881-T20A treats the packet in either one of the following ways:

In traffic shaping:

• Holds it in the queue until enough tokens are available in the bucket.

In traffic policing:

- Drops it.
- Transmits it but adds a DSCP mark. The EMG2881-T20A may drop these marked packets if the network is overloaded.

Configure the bucket size to be equal to or less than the amount of the bandwidth that the interface can support. It does not help if you set it to a bucket size over the interface's capability. The smaller the bucket size, the lower the data transmission rate and that may cause outgoing packets to be dropped. A larger transmission rate requires a big bucket size. For example, use a bucket size of 10 kbytes to get the transmission rate up to 10 Mbps.

### Single Rate Three Color Marker

The Single Rate Three Color Marker (srTCM, defined in RFC 2697) is a type of traffic policing that identifies packets by comparing them to one user-defined rate, the Committed Information Rate (CIR), and two burst sizes: the Committed Burst Size (CBS) and Excess Burst Size (EBS).

The srTCM evaluates incoming packets and marks them with one of three colors which refer to packet loss priority levels. High packet loss priority level is referred to as red, medium is referred to as yellow and low is referred to as green.

The srTCM is based on the token bucket filter and has two token buckets (CBS and EBS). Tokens are generated and added into the bucket at a constant rate, called Committed Information Rate (CIR). When the first bucket (CBS) is full, new tokens overflow into the second bucket (EBS).

All packets are evaluated against the CBS. If a packet does not exceed the CBS it is marked green. Otherwise it is evaluated against the EBS. If it is below the EBS then it is marked yellow. If it exceeds the EBS then it is marked red.

The following shows how tokens work with incoming packets in srTCM:

- A packet arrives. The packet is marked green and can be transmitted if the number of tokens in the CBS bucket is equal to or greater than the size of the packet (in bytes).
- After a packet is transmitted, a number of tokens corresponding to the packet size is removed from the CBS bucket.
- If there are not enough tokens in the CBS bucket, the EMG2881-T20A checks the EBS bucket. The packet is marked yellow if there are sufficient tokens in the EBS bucket. Otherwise, the packet is marked red. No tokens are removed if the packet is dropped.

### **Two Rate Three Color Marker**

The Two Rate Three Color Marker (trTCM, defined in RFC 2698) is a type of traffic policing that identifies packets by comparing them to two user-defined rates: the Committed Information Rate (CIR) and the Peak Information Rate (PIR). The CIR specifies the average rate at which packets are admitted to the

86

network. The PIR is greater than or equal to the CIR. CIR and PIR values are based on the guaranteed and maximum bandwidth respectively as negotiated between a service provider and client.

The trTCM evaluates incoming packets and marks them with one of three colors which refer to packet loss priority levels. High packet loss priority level is referred to as red, medium is referred to as yellow and low is referred to as green.

The trTCM is based on the token bucket filter and has two token buckets (Committed Burst Size (CBS) and Peak Burst Size (PBS)). Tokens are generated and added into the two buckets at the CIR and PIR respectively.

All packets are evaluated against the PIR. If a packet exceeds the PIR it is marked red. Otherwise it is evaluated against the CIR. If it exceeds the CIR then it is marked yellow. Finally, if it is below the CIR then it is marked green.

The following shows how tokens work with incoming packets in trTCM:

- A packet arrives. If the number of tokens in the PBS bucket is less than the size of the packet (in bytes), the packet is marked red and may be dropped regardless of the CBS bucket. No tokens are removed if the packet is dropped.
- If the PBS bucket has enough tokens, the EMG2881-T20A checks the CBS bucket. The packet is marked green and can be transmitted if the number of tokens in the CBS bucket is equal to or greater than the size of the packet (in bytes). Otherwise, the packet is marked yellow.

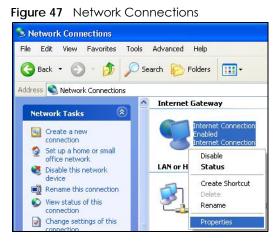
### 9.7.1 Using UPnP in Windows XP Example

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 EMG2881-T20A.

Make sure the computer is connected to a LAN port of the EMG2881-T20A. Turn on your computer and the EMG2881-T20A.

### 9.7.1.1 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.



3 In the Internet Connection Properties window, click Settings to see the port mappings there were automatically created.



Figure 48 Internet Connection Properties

4 You may edit or delete the port mappings or click Add to manually add port mappings.Figure 49 Internet Connection Properties: Advanced Settings



Figure 50 Internet Connection Properties: Advanced Settings: Add

Service Settings		? 🔀
Description of service:		
Test		
Name or IP address (for example 192 computer hosting this service on you		the
192.168.1.11		
External Port number for this service:		
143	TCP	C UDP
Internal Port number for this service:		
143		
	ОК	Cancel

Note: When the UPnP-enabled device is disconnected from your computer, all port mappings will be deleted automatically.



5 Select Show icon in notification area when connected option and click OK. An icon displays in the system tray.

Figure 51 System Tray Icon



6 Double-click on the icon to display your current Internet connection status.

igure 52 In	ternet Conne	ection Status
😼 Internet Conn	ection Status	? 🛛
General		
- Internet Gatewa	y	
Status:		Connected
Duration:		00:00:56
Speed:		100.0 Mbps
Activity	Internet Gateway	My Computer
<b>()</b> —	🧐	
Packets:		
Sent: Received:	8 5,943	618 746
Properties	Disable	
		Close

### 9.7.2 Web Configurator Easy Access

With UPnP, you can access the web-based configurator on the EMG2881-T20A without finding out the IP address of the EMG2881-T20A first. This comes helpful if you do not know the IP address of the EMG2881-T20A.

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.

89

Figure 53 Network Connections

e Edit View Favorites	Tools Adv	anced Help	
🕽 Back 🝷 🕥 - 🏂	Search	6 Folders	-
iress 🔇 Network Connections	8		
	(A) In	ternet Gatewa	у
Network Tasks Create a new connection Set up a home or small office network		Disable	t Connection d t Connection
	LA	N or High-Spe	ed Internet
<ul> <li>Network Troubleshooter</li> <li>Other Places</li> <li>Control Panel</li> <li>My Network Places</li> <li>My Documents</li> <li>My Computer</li> </ul>	<ul> <li></li> <li></li> </ul>	5 Enabled	rea Connection EN1207D-TX PCI Fast
Details	۲		
Network Connections System Folder			

- 4 An icon with the description for each UPnP-enabled device displays under Local Network.
- 5 Right-click on the icon for your EMG2881-T20A and select **Invoke**. The web configurator login screen displays.



Figure 54 Network Connections: My Network Places

6 Right-click on the icon for your EMG2881-T20A and select **Properties**. A properties window displays with basic information about the EMG2881-T20A.

90

Figure 55 Network Connections: My Network Places: Properties: Example

XEL Internet S General	iharing Gateway
<u>ě</u>	ZyXEL Internet Sharing Gateway
Manufacturer:	ZyXEL
Model Name:	ZyXEL Internet Sharing Gateway
Model Number:	Model Number:
Description:	ZyXEL Internet Sharing Gateway
Device Address:	http://192.168.1.1/
	Close Cancel

# CHAPTER 10 Security

# 10.1 Overview

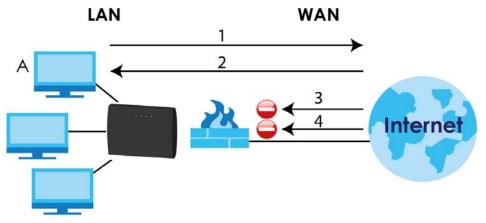
Use these screens to enable and configure the firewall that protects your EMG2881-T20A and your LAN from unwanted or malicious traffic.

Enable the firewall to protect your LAN computers from attacks by hackers on the Internet and control access between the LAN and WAN. By default the firewall:

- allows traffic that originates from your LAN computers to go to all of the networks.
- blocks traffic that originates on the other networks from going to the LAN.

The following figure illustrates the default firewall action. User **A** can initiate an IM (Instant Messaging) session from the LAN to the WAN (1). Return traffic for this session is also allowed (2). However other traffic initiated from the WAN is blocked (3 and 4).





### 10.1.1 What You Can Do

- Use the IPv4 Firewall screen to enable or disable the EMG2881-T20A's IPv4 firewall (Section 10.2 on page 93).
- Use the IPv6 Firewall screen to enable or disable the EMG2881-T20A's IPv6 firewall (Section 10.3 on page 95).

### 10.1.2 What You Need To Know

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

92

### About the EMG2881-T20A Firewall

The EMG2881-T20A's firewall feature physically separates the LAN and the WAN and acts as a secure gateway for all data passing between the networks.

It is a stateful inspection firewall and is designed to protect against Denial of Service attacks when activated (click the **IPv4 Firewall** or **IPv6 Firewall** tab under **Security** and then click the **Enable Firewall** check box). The EMG2881-T20A's purpose is to allow a private Local Area Network (LAN) to be securely connected to the Internet. The EMG2881-T20A can be used to prevent theft, destruction and modification of data, as well as log events, which may be important to the security of your network.

The EMG2881-T20A is installed between the LAN and a broadband modem connecting to the Internet. This allows it to act as a secure gateway for all data passing between the Internet and the LAN.

The EMG2881-T20A has one Ethernet WAN port and four Ethernet LAN ports, which are used to physically separate the network into two areas. The WAN (Wide Area Network) port attaches to the broadband (cable or DSL) modem to the Internet.

The LAN (Local Area Network) port attaches to a network of computers, which needs security from the outside world. These computers will have access to Internet services such as e-mail, FTP and the World Wide Web. However, "inbound access" is not allowed (by default) unless the remote host is authorized to use a specific service.

### **Guidelines For Enhancing Security With Your Firewall**

- 1 Change the default password via Web Configurator.
- 2 Think about access control before you connect to the network in any way, including attaching a modem to the port.
- 3 Limit who can access your router.
- 4 Don't enable any local service (such as NTP) that you don't use. Any enabled service could present a potential security risk. A determined hacker might be able to find creative ways to misuse the enabled services to access the firewall or the network.
- 5 For local services that are enabled, protect against misuse. Protect by configuring the services to communicate only with specific peers, and protect by configuring rules to block packets for the services at specific interfaces.
- 6 Protect against IP spoofing by making sure the firewall is active.
- 7 Keep the firewall in a secured (locked) room.

## 10.2 IPv4 Firewall Screen

Use this screen to enable or disable the EMG2881-T20A's IPv4 firewall. Click **Configuration** > **Security** > **IPv4 Firewall** to open the firewall setup screen.

Figure 57	Configuration > Security > IPv4 Firewall
riguie 37	

v4 Firewall		Apply Can
ICMP Respond to Ping on:	LAN	
Firewall Setup	Ø	
	۲	
Enable Firewall Rule		
Enable Firewall Rule	✓	
Filter table type	● DROP ◎ ACCEPT	
Add Firewall Rule		
Service Name :		
MAC Address :		
Dest IP Address :		
Source IP Address :		
Protocol :	TCP	
Dest Port Range :	-	
Source Port Range :		
5	Add Rule	
Firewall Rule (Maximum: 64)		

The following table describes the labels in this screen.

LABEL	DESCRIPTION
ICMP	Internet Control Message Protocol is a message control and error-reporting protocol betweer a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the TCP/IP software and directly apparent to the application user.
Respond to Ping on	The EMG2881-T20A will not respond to any incoming Ping requests when <b>Disable</b> is selected. Select LAN to reply to incoming LAN Ping requests. Select WAN to reply to incoming WAN Ping requests. Otherwise select LAN&WAN to reply to all incoming LAN and WAN Ping requests.
Firewall Setup	
Enable Firewall	Select this check box to activate the firewall. The EMG2881-T20A performs access control and protects against Denial of Service (DoS) attacks when the firewall is activated.
Enable Firewall Rul	e
Enable Firewall Rule	Select this check box to activate the firewall rules that you define (see Add Firewall Rule below).
Filter table type	Select <b>DROP</b> to silently discard the packets which meet the firewall rules. The others are accepted.
	Select ACCEPT to allow the passage of the packets which meet the firewall rules. The others are blocked.
Add Firewall Rule	
Service Name	Enter a name that identifies or describes the firewall rule.
MAC Address	Enter the MAC address of the computer for which the firewall rule applies.

LABEL	DESCRIPTION
Dest IP Address	Enter the IP address of the computer to which traffic for the application or service is entering.
	The EMG2881-T20A applies the firewall rule to traffic initiating from this computer.
Source IP Address	Enter the IP address of the computer that initializes traffic for the application or service.
	The EMG2881-T20A applies the firewall rule to traffic initiating from this computer.
Protocol	Select the protocol ( <b>TCP</b> , <b>UDP</b> or <b>ICMP</b> ) used to transport the packets for which you want to apply the firewall rule.
Dest Port Range	This is the port number/range of the destination that define the traffic type, for example TCP port 80 defines web traffic.
Source Port Range	This is the port number/range of the source that define the traffic type, for example TCP port 80 defines web traffic.
Add Rule	Click Add Rule to save the firewall rule.
Firewall Rule	
#	This is your firewall rule number. The ordering of your rules is important as rules are applied in turn.
Service Name	This is a name that identifies or describes the firewall rule.
MAC address	This is the MAC address of the computer for which the firewall rule applies.
Dest IP	This is the IP address of the computer to which traffic for the application or service is entering.
Source IP	This is the IP address of the computer from which traffic for the application or service is initialized.
Protocol	This is the protocol (TCP, UDP or ICMP) used to transport the packets for which you want to apply the firewall rule.
Dest Port Range	This is the port number/range of the destination that define the traffic type, for example TCP port 80 defines web traffic.
Source Port Range	This is the port number/range of the source that define the traffic type, for example TCP port 80 defines web traffic.
Delete	Click 🍵 to remove the firewall rule.
Apply	Click Apply to save the settings.
Cancel	Click <b>Cancel</b> to start configuring this screen again.

Table 40 Configuration > Security > IPv4 Firewall (continued)

# 10.3 IPv6 Firewall Screen

This chapter shows you how to enable and create IPv6 firewall rules to filter IPv6 traffic.

Click Configuration > Security > IPv6 Firewall. The IPv6 Firewall screen appears as shown.

Figure 58	Configuration :	> Security >	IPv6 Firewall

v6 Firewall			Apply	Cancel
Enable Firewall Rule	8			
Filter table type	DROP      ACCEPT			
Add Firewall Rule				
Service Name :				
MAC Address :				
Dest IP Address :				
Source IP Address :				
Protocol :	TCP			
Dest Port Range :	-			
Source Port Range :	-			
	Add Rule			
Firewall Rule (Maximum: 64)				
# Service Name MAC Address	Dest IP Source IP Protocol	Dest Port Range	Source Port Range	

The following table describes the labels in this screen.

LABEL	DESCRIPTION
Enable Firewall Rule	
Enable Firewall Rule	Select this check box to activate the firewall rules that you define (see Add Firewall Rule below).
Filter table type	Select <b>DROP</b> to silently discard the packets which meet the firewall rules. The others are accepted.
	Select <b>ACCEPT</b> to allow the passage of the packets which meet the firewall rules. The others are blocked.
Add Firewall Rule	
Service Name	Enter a name that identifies or describes the firewall rule.
MAC Address	Enter the MAC address of the computer for which the firewall rule applies.
Dest IP Address	Enter the IPv6 address of the computer to which traffic for the application or service is entering.
	The EMG2881-T20A applies the firewall rule to traffic destined for this computer.
Source IP Address	Enter the IPv6 address of the computer that initializes traffic for the application or service.
	The EMG2881-T20A applies the firewall rule to traffic initiating from this computer.
Protocol	Select the protocol (TCP, UDP or ICMPv6) used to transport the packets for which you want to apply the firewall rule.
Dest Port Range	Enter the port number/range of the destination that defines the traffic type, for example TCP port 80 defines web traffic.
Source Port Range	Enter the port number/range of the source that defines the traffic type, for example TCP port 80 defines web traffic.
Add Rule	Click Add Rule to save the firewall rule.
Firewall Rule	

Table 41 Configuration > Security > IPv6 Firewall

LABEL	DESCRIPTION
#	This is your firewall rule number. The ordering of your rules is important as rules are applied in turn.
ServiceName	This is a name that identifies or describes the firewall rule.
MAC Address	This is the MAC address of the computer for which the firewall rule applies.
Dest IP	This is the IP address of the computer to which traffic for the application or service is entering.
Source IP	This is the IP address of the computer to which traffic for the application or service is initialized.
Protocol	This is the protocol ( <b>TCP</b> , <b>UDP</b> or <b>ICMPv6</b> ) used to transport the packets for which you want to apply the firewall rule.
Dest Port Range	This is the port number/range of the destination that defines the traffic type, for example TCP port 80 defines web traffic.
Source Port Range	This is the port number/range of the source that defines the traffic type, for example TCP port 80 defines web traffic.
Delete	Click 😑 to remove the firewall rule.
Apply	Click Apply to save the settings.
Cancel	Click Cancel to restore your previously saved settings.

# CHAPTER 11 Maintenance

# 11.1 Overview

This chapter provides information on the Maintenance screens.

# 11.2 What You Can Do

- Use the **General** screen to set the timeout period of the management session (Section 11.3 on page 98).
- Use the **Password** screen to change your EMG2881-T20A's system password (Section 11.4 on page 99).
- Use the Time screen to change your EMG2881-T20A's time and date (Section 11.5 on page 100).
- Use the Firmware Upgrade screen to upload firmware to your EMG2881-T20A (Section 11.6 on page 101).
- Use the **Backup/Restore** screen to view information related to factory defaults, backup configuration, and restoring configuration (Section 11.8 on page 104).
- Use the **Restart** screen to reboot the EMG2881-T20A without turning the power off (Section 11.8 on page 104).
- Use the Log screen to see the logs for the activity on the EMG2881-T20A (Section 11.9 on page 104).
- Use the **ROMD** screen to save and/or clean the configuration to/from the ROMD file which can store customized default settings.

# 11.3 General Screen

Use this screen to set the management session timeout period. Click **Maintenance** > **General**. The following screen displays.

#### Figure 59 Maintenance > General

General			Apply		Cancel
System Name :	EMG2881-T20A				
Domain Name :	local				
Administrator Inactivity Timer :	60	(minutes, 0 mea	ns no timeou	t)	



The following table describes the labels in this screen.

LABEL	DESCRIPTION
System Name	System Name is a unique name to identify the EMG2881-T20A in an Ethernet network.
Domain Name	Enter the domain name you want to give to the EMG2881-T20A.
Administrator Inactivity Timer	Type how many minutes a management session can be left idle before the session times out. The default is 5 minutes. After it times out you have to log in with your password again. Very long idle timeouts may have security risks. A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended).
Apply	Click <b>Apply</b> to save your changes back to the EMG2881-T20A.
Cancel	Click Cancel to exit this screen without saving.

 Table 42
 Maintenance > General

# 11.4 Password Screen

It is strongly recommended that you change your EMG2881-T20A's password.

If you forget your EMG2881-T20A's password (or IP address), you will need to reset the device. See Section 11.8 on page 104 for details.

Click Maintenance > Password. The screen appears as shown.

Figure 60	Maintenance > Password
-----------	------------------------

Password		Apply	Cancel
User :	admin <b>T</b>		
Old Password :			
New Password :	Please enter password at 8 ~ 30 characters		
Retype to Confirm :			

The following table describes the labels in this screen.

LABEL	DESCRIPTION
User	This field displays the name of the admin account.
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 an asterisk (*) for each character you type.
Retype to Confirm	Type the new password again in this field.
Apply	Click Apply to save your changes back to the EMG2881-T20A.
Cancel	Click Cancel to begin configuring this screen afresh.

Table 43Maintenance > Password

# 11.5 Time Screen

Use this screen to configure the EMG2881-T20A's time based on your local time zone. To change your EMG2881-T20A's time and date, click **Maintenance** > **Time**. The screen appears as shown.

Figure 61 Maintenance > Time

Time		Apply	Cancel
Current Time and Date Current Time : Current Date :	02:42:18 2017-12-18		
Time and Date Setup Manual New Time (hh:mm:ss): New Date (yyyy/mm/dd): Get from Time Server	00 : 00 : 00 2014 / 01 / 01		
User Defined Time Server Address :	pool.ntp.org		
Time Zone Setup			
Time Zone :	auto (GMT)		۲

The following table describes the labels in this screen.

LABEL	DESCRIPTION	
Current Time and	Date	
Current Time	This field displays the time of your EMG2881-T20A.	
	Each time you reload this page, the EMG2881-T20A synchronizes the time with the time server.	
Current Date	This field displays the date of your EMG2881-T20A.	
	Each time you reload this page, the EMG2881-T20A synchronizes the date with the time server.	
Time and Date Se	etup	
Manual	Select this radio button to enter the time and date manually. If you configure a new time and date, Time Zone and Daylight Saving at the same time, the new time and date you entered has priority and the Time Zone and Daylight Saving settings do not affect it.	
New Time	This field displays the last updated time from the time server or the last time configured manually.	
(hh:mm:ss)	When you select Manual, enter the new time in this field and then click Apply.	
New Date	This field displays the last updated date from the time server or the last date configured manually.	
(yyyy/mm/dd)	When you select Manual, enter the new date in this field and then click Apply.	
Get from Time Server	Select this radio button to have the EMG2881-T20A get the time and date from the time server you specified below.	
User Defined Time Server Address	Enter the IP address or URL (up to 20 extended ASCII characters in length) of your time server. Check with your ISP/network administrator if you are unsure of this information.	
Time Zone Setup		
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).	

LABEL	DESCRIPTION
Daylight Savings	Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.
	Select this option if you use Daylight Saving Time.
Start Date	Configure the day and time when Daylight Saving Time starts if you selected <b>Daylight Savings</b> . The <b>o'clock</b> field uses the 24 hour format. Here are a couple of examples.
	Daylight Saving Time starts in most parts of the United States on the first Sunday of April. Each time zone in the United States starts using Daylight Saving Time at 2 A.M local time. So in the United States you would select <b>First</b> , <b>Sunday</b> , <b>April</b> and type 2 in the <b>o'clock</b> field.
	Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.m. GMT or UTC). So in the European Union you would select <b>Last</b> , <b>Sunday</b> , <b>March</b> . The time you type in the <b>o'clock</b> field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
End Date	Configure the day and time when Daylight Saving Time ends if you selected <b>Daylight Savings</b> . The <b>o'clock</b> field uses the 24 hour format. Here are a couple of examples.
	Daylight Saving Time ends in the United States on the last Sunday of October. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select <b>Last</b> , <b>Sunday</b> , <b>October</b> and type 2 in the <b>o'clock</b> field.
	Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select <b>Last, Sunday, October</b> . The time you type in the <b>o'clock</b> field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT + 1).
Apply	Click Apply to save your changes back to the EMG2881-T20A.
Cancel	Click <b>Cancel</b> to exit this screen without saving.

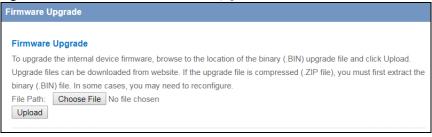
Table 44 Maintenance > Time (continued)

# 11.6 Firmware Upgrade Screen

Find firmware at <u>www.zyxel.com</u> in a file that (usually) uses the system model name with a "\*.bin" extension, e.g., "EMG2881-T20A.bin". The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot.

Click **Maintenance** > **Firmware Upgrade**. Follow the instructions in this screen to upload firmware to your EMG2881-T20A.

Figure 62	Maintenance > Firmware Upgrade
-----------	--------------------------------



The following table describes the labels in this screen.

LABEL	DESCRIPTION
Firmware Upgrad	le
File Path	Type in the location of the file you want to upload in this field or click <b>Choose File</b> to find it.
Choose File	Click <b>Choose File</b> to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click <b>Upload</b> to begin the upload process. This process may take up to two minutes.

Table 45	Maintenance > Firmware Upgrade
	indimensioned - infinite opgrade

### Do not turn off the EMG2881-T20A while firmware upload is in progress!

After you see the **Firmware Upload In Process** screen, wait two minutes before logging into the EMG2881-T20A again.

The EMG2881-T20A automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 63 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, an error message appears.

# 11.7 Configuration Backup/Restore Screen

Backup configuration allows you to back up (save) the EMG2881-T20A's current configuration to a file on your computer. Once your EMG2881-T20A 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.

Restore configuration allows you to upload a new or previously saved configuration file from your computer to your EMG2881-T20A.

Click **Maintenance** > **Backup/Restore**. Information related to factory defaults, backup configuration, and restoring configuration appears as shown next.

#### Figure 64 Maintenance > Backup/Restore

Backup/Restore
Backup Configuration Click Backup to save the current configuration of your system to your computer. Backup
Restore Configuration To restore a previously saved configuration file to your system, browse to the location of the configuration file and click Upload. File Path : Choose File No file chosen
Upload
Back to Factory Defaults
Click Reset to clear all user-entered configuration information and return to factory defaults. After resetting, the
- Password will be reset to default
- LAN IP address will be 192.168.1.1
- DHCP will be reset to server
Reset

The following table describes the labels in this screen.

LABEL	DESCRIPTION	
Backup Configu	ration	
Backup	Click <b>Backup</b> to save the EMG2881-T20A's current configuration to your computer.	
Restore Configu	ration	
File Path	Click Choose File to browse to the location of the configuration file in your computer.	
Upload	Click <b>Upload</b> to begin the upload process.	
	Note: Do not turn off the EMG2881-T20A while configuration file upload is in progress.	
	After you see a "configuration upload successful" screen, you must then wait one minute before logging into the EMG2881-T20A again. The EMG2881-T20A automatically restarts in this time causing a temporary network disconnect.	
	If you see an error screen, click Back to return to the Backup/Restore screen.	
Reset	Pressing the <b>Reset</b> button in this section clears all user-entered configuration information and returns the EMG2881-T20A to its factory defaults.	
	You can also press the <b>RESET</b> button on the rear panel to reset the factory defaults of your EMG2881-T20A. Refer to the chapter about introducing the Web Configurator for more information on the <b>RESET</b> button.	

#### Table 46 Maintenance > Backup/Restore

Note: 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 EMG2881-T20A IP address (192.168.1.1). See Appendix B on page 121 for details on how to set up your computer's IP address.

# 11.8 Restart Screen

System restart allows you to reboot the EMG2881-T20A without turning the power off.

Click Maintenance > Restart to open the following screen.

Figure 65 Maintenance > Restart

Restart
System Restart
Click Restart to have the device perform a software restart. The SYS(or PWR) LED blinks as the device restarts and
then stays steady on if the restart is successful.
Restart

Click Restart to have the EMG2881-T20A reboot. This does not affect the EMG2881-T20A's configuration.

# 11.9 Log Screen

The Web Configurator allows you to look at all of the EMG2881-T20A's logs in one location.

You can configure which logs to display in the Log screen. Select the logs you wish to display. Click **Apply** to save your settings. Click **Cancel** to start the screen afresh.

Use this screen to see the logged messages for the EMG2881-T20A. The log wraps around and deletes the old entries after it fills. Select what logs you want to see from the **Display** drop list. The log choices depend on your settings above this screen. Click **Refresh** to renew the log screen. Click **Clear Log** to delete all the logs.

Figure 66 Maintenance > Log

Log		Apply	Cancel
Active Log and Alert			
Log			
Access Control			
Display : All Logs V	Refresh Clear Log		
Summary			
<u>#</u> <u>Time</u> ▽	Message		

## 11.10 The ROMD Screen

Click Maintenance > ROMD to open the following screen.

#### Figure 67 Maintenance > ROMD

ROMD
Save ROMD Click Save to Save Configuration to ROMD. Save
Clean ROMD Click Clean to Clean Confuguration to ROMD. Clean

Click **Save** to save the EMG2881-T20A's current configuration to the ROM-D file. Click **Clear** to reset the customized settings in the ROM-D file to factory defaults.

# CHAPTER 12 Troubleshooting

# 12.1 Overview

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
- EMG2881-T20A Access and Login
- Internet Access
- Resetting the EMG2881-T20A to Its Factory Defaults
- Wireless Connections

## 12.2 Power, Hardware Connections, and LEDs

The EMG2881-T20A does not turn on. None of the LEDs turn on.

- 1 Make sure you are using the power adaptor or cord included with the EMG2881-T20A.
- 2 Make sure the power adaptor or cord is connected to the EMG2881-T20A and plugged in to an appropriate power source. Make sure the power source is turned on.
- 3 Disconnect and re-connect the power adaptor or cord to the EMG2881-T20A.
- 4 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 1.5 on page 12.
- 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 Disconnect and re-connect the power adaptor to the EMG2881-T20A.
- 5 If the problem continues, contact the vendor.

# 12.3 EMG2881-T20A Access and Login

### I don't know the IP address of my EMG2881-T20A.

- 1 The default IP address of the EMG2881-T20A in Router Mode is 192.168.1.1.
- 2 If you changed the IP address and have forgotten it, you might get the IP address of the EMG2881-T20A in Router Mode 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 EMG2881-T20A (it depends on the network), so enter this IP address in your Internet browser.
- 3 Reset your EMG2881-T20A to change all settings back to their default. This means your current settings are lost. See Section 12.5 on page 109 in the **Troubleshooting** for information on resetting your EMG2881-T20A.

I forgot the password.

- 1 The default password is the factory default (see the device label).
- 2 If this does not work, you have to reset the device to its factory defaults. See Section 12.5 on page 109.

I cannot see or access the Login screen in the Web Configurator.

- 1 Make sure you are using the correct IP address.
  - The default IP address of the EMG2881-T20A in Router Mode is 192.168.1.1.
  - If you changed the IP address (Section 8.4 on page 71), use the new IP address.
  - If you changed the IP address and have forgotten it, see the troubleshooting suggestions for I don't know the IP address of my EMG2881-T20A.
- 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 JavaScript and Java enabled. See Appendix A on page 112.
- 4 Make sure your computer is in the same subnet as the EMG2881-T20A. (If you know that there are routers between your computer and the EMG2881-T20A, skip this step.)
  - If there is a DHCP server on your network, make sure your computer is using a dynamic IP address. See Section 8.4 on page 71.
  - If there is no DHCP server on your network, make sure your computer's IP address is in the same subnet as the EMG2881-T20A. See Section 8.4 on page 71.

- 5 Reset the device to its factory defaults, and try to access the EMG2881-T20A with the default IP address. See Section 1.5.6 on page 14.
- 6 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

#### **Advanced Suggestions**

- Try to access the EMG2881-T20A using another service, such as Telnet. If you can access the EMG2881-T20A, check the remote management settings and firewall rules to find out why the EMG2881-T20A does not respond to HTTP.
- If your computer is connected to the **WAN** port or is connected wirelessly, use a computer that is connected to a **LAN/ETHERNET** port.

I can see the Login screen, but I cannot log in to the EMG2881-T20A.

- 1 Make sure you have entered the password correctly. The default password is the factory default (see the device label). This field is case-sensitive, so make sure [Caps Lock] is not on.
- 2 This can happen when you fail to log out properly from your last session. Try logging in again after 10 minutes.
- 3 Disconnect and re-connect the power adaptor or cord to the EMG2881-T20A.
- 4 If this does not work, you have to reset the device to its factory defaults. See Section 12.5 on page 109.

# 12.4 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.
- 2 Make sure the WAN port is connected to a broadband modem or router with Internet access. Your computer and the EMG2881-T20A should be in the same subnet.
- 3 Make sure you entered your ISP account information correctly in the wizard or the WAN screen. These fields are case-sensitive, so make sure [Caps Lock] is not on.
- 4 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.
- 5 Disconnect all the cables from your device, and follow the directions in the Quick Start Guide again.
- 6 If the problem continues, contact your ISP.

I cannot access the Internet anymore. I had access to the Internet (with the EMG2881-T20A), 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 1.5 on page 12.
- 2 Reboot the EMG2881-T20A.
- 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 1.5 on page 12. If the EMG2881-T20A 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 the EMG2881-T20A closer to the AP 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** Reboot the EMG2881-T20A.
- 4 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

#### Advanced Suggestion

• Check the settings for QoS. If it is disabled, you might consider activating it.

# 12.5 Resetting the EMG2881-T20A to Its Factory Defaults

If you reset the EMG2881-T20A, you lose all of the changes you have made. The EMG2881-T20A re-loads its default settings. You have to make all of your changes again.

You will lose all of your changes when you push the **RESET** button.

To reset the EMG2881-T20A:

- 1 Make sure the power LED is on.
- 2 Press the **RESET** button for one to four seconds to restart/reboot the EMG2881-T20A.

**3** Press the **RESET** button for longer than five seconds to set the EMG2881-T20A back to its factory-default configurations.

If the EMG2881-T20A restarts automatically, wait for the EMG2881-T20A to finish restarting, and log in to the Web Configurator. The password is reset to the factory default (see the device label).

If the EMG2881-T20A does not restart automatically, disconnect and reconnect the EMG2881-T20A's power. Then, follow the directions above again.

# **12.6 Wireless Connections**

I cannot access the EMG2881-T20A or ping any computer from the WLAN.

- 1 Make sure the wireless LAN is enabled on the EMG2881-T20A.
- 2 Make sure the wireless adapter on your computer 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 EMG2881-T20A.
- 4 Make sure your computer (with a wireless adapter installed) is within the transmission range of the EMG2881-T20A.
- 5 Check that both the EMG2881-T20A and the wireless adapter on your computer are using the same wireless and wireless security settings.
- 6 Make sure traffic between the WLAN and the LAN is not blocked by the firewall on the EMG2881-T20A.
- 7 Make sure you allow the EMG2881-T20A to be remotely accessed through the WLAN interface. Check your remote management settings.
  - See the chapter on Wireless LAN in the User's Guide for more information.

# What factors may cause intermittent or unstabled wireless connection? How can I solve this problem?

The following factors may cause interference:

- Obstacles: walls, ceilings, furniture, and so on.
- Building Materials: metal doors, aluminum studs.
- Electrical devices: microwaves, monitors, electric motors, cordless phones, and other wireless devices.

To optimize the speed and quality of your wireless connection, you can:

• Move your wireless device closer to the AP if the signal strength is low.

- Reduce wireless interference that may be caused by other wireless networks or surrounding wireless electronics such as cordless phones.
- Place the AP where there are minimum obstacles (such as walls and ceilings) between the AP and the wireless client.
- Reduce the number of wireless clients connecting to the same AP simultaneously, or add additional APs if necessary.
- Try closing some programs that use the Internet, especially peer-to-peer applications. If the wireless client is sending or receiving a lot of information, it may have too many programs open that use the Internet.
- Position the antennas for best reception. If the AP is placed on a table or floor, point the antennas upwards. If the AP is placed at a high position, point the antennas downwards. Try pointing the antennas in different directions and check which provides the strongest signal to the wireless clients.

# APPENDIX A Pop-up Windows, JavaScript and Java Permissions

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

- Web browser pop-up windows from your device.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

Note: The screens used below belong to Internet Explorer version 6, 7 and 8. Screens for other Internet Explorer versions may vary.

### Internet Explorer Pop-up Blockers

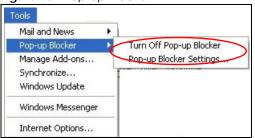
You may have to disable pop-up blocking to log into your device.

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 68 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 69 Internet Options: Privacy

nternet	Options					?
General	Security	Privacy	Content	Connections	Programs	Advanced
Settin	56	he slider ti	o select a	privacy setting	for the Interr	net
- [	_ Me	dium				
-	- priv - Blo ⊡- info Re	acy policy ocks third- mation wi estricts first	party cook thout your t-party coo	ties that do not ties that use pe implicit consen kies that use p cit consent	rsonally iden t	itifiable
	Sites		mport	Advanced.	Del	ault
Pop-u		t most pop ck pop-up	<u> </u>	ows from appea		ngs
			OK	Ca	ncel	Apply

**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 70 Internet Options: Privacy

Internet O	ptions					?
General	Security	Privacy	Content	Connection	s Programs	Advanced
- Settings		he slider to	o select a j	privacy setting	g for the Inter	met
- [	_ Me	dium				
	- priv - Blo - info Re	acy policy ocks third-j mation wil estricts first	party cook thout your -party coo	ies that do no ies that use p implicit conse kies that use cit consent	ersonally ide nt	ntifiable
	Sites		mport	Advanced	<b>1</b> De	efault
Pop-up				ws from appe	$\langle$	
	Elo	ck pop-up:	s		Sett	tings
			OK		ancel	Apply

- **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://192.168.167.1.
- 4 Click Add to move the IP address to the list of Allowed sites.

Pop-up Blocker Settings Exceptions Pop-ups are currently blocked. You can allow pop-ups from specific Web sites by adding the site to the list below. Address of Web site to allow: http://192.168.1.1 Add Allowed sites: Remove Remove All Notifications and Filter Level Play a sound when a pop-up is blocked. Show Information Bar when a pop-up is blocked. Filter Level: Medium: Block most automatic pop-ups Y Pop-up Blocker FAQ Close

Figure 71 Pop-up Blocker Settings

EMG2881-T20A User's Guide

- 5 Click Close to return to the Privacy screen.
- 6 Click Apply to save this setting.

### JavaScript

If pages of the web configurator do not display properly in Internet Explorer, check that JavaScript are allowed.

1 In Internet Explorer, click Tools, Internet Options and then the Security tab.

Figure 72 Internet Options: Security Internet Options ? X General Security Privacy Content Connections Programs Advanced Select a Web content zone to specify its security settings. Internet Local intranet Trusted sites Restricted sites Internet This zone contains all Web sites you haven't placed in other zones Security level for this zone-Move the slider to set the security level for this zone. Medium Safe browsing and still functional Prompts before downloading potentially unsafe content - Unsigned ActiveX controls will not be downloaded - Appropriate for most Internet sites Custom Level. Default Level ΩK. Cancel

- 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 73 Security Settings - Java Scripting

Security Settings		? ×
Settings:		
<ul> <li>Scripting</li> <li>Active scripting</li> <li>Disable</li> <li>Enable</li> <li>Prompt</li> <li>Allow paste operations via so</li> <li>Disable</li> <li>Enable</li> <li>Prompt</li> <li>Scripting of Java applets</li> <li>Disable</li> <li>Enable</li> <li>Prompt</li> <li>Scripting of Java applets</li> <li>Disable</li> <li>Enable</li> <li>Prompt</li> <li>Prompt</li> </ul>	ript	
Reset custom settings	<b>_</b>	Reset
	ОК	Cancel

### **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 74 Security Settings - Java

ecurity Settings				?>
Settings:				
O Disable				<b></b>
• Enable				
Font download				
O Disable				_
<ul> <li>Enable</li> </ul>				
O Prompt				_
Microsoft VM				
📑 Java permission	5			
O Custom				
Disable Jawa				
• High safety				
O Low safety				
Q Medium safe	ty			-
				•
Reset custom settings				
Reset to: Medium			•	R <u>e</u> set
		Oł		Cancel

## 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.

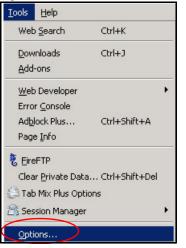
Internet Options	?
General Security Privacy Content Connections Programs	Advanced
<u>S</u> ettings:	
Use inline AutoComplete     Use Passive FTP (for firewall and DSL modem compatibil     Use smooth scrolling     HTTP 1.1 settings     Use HTTP 1.1     Use HTTP 1.1     Use HTTP 1.1 through proxy connections     Java (Sun)     Use Java 2 v1.4.1_07 for <applet> (requires restart)     Microsoft VM     Java console enabled (requires restart)     Java logging enabled     JIT compiler for virtual machine enabled (requires restart)     Multimedia     Always show Internet Explorer (5.0 or later) Radio toolbar</applet>	ity)
<ul> <li>Don't display online media content in the media bar</li> <li>Enable Automatic Image Resizing</li> </ul>	
<u></u> estore D	efaults
OK Cancel	Apply

### **Mozilla Firefox**

Mozilla Firefox 2.0 screens are used here. Screens for other versions may vary slightly. The steps below apply to Mozilla Firefox 3.0 as well.

You can enable Java, Javascript and pop-ups in one screen. Click **Tools**, then click **Options** in the screen that appears.

Figure 76 Mozilla Firefox: TOOLS > Options



Click Content to show the screen below. Select the check boxes as shown in the following screen.

✓ Load images automatically     Except       ✓ Enable JavaScript     Adyan       ✓ Enable Java     Fonts & Colors	ed eptions eptions (anced
✓ Block pop-up windows     Except       ✓ Load images automatically     Except       ✓ Enable JavaScript     Adyan       ✓ Enable Java     Fonts & Colors	eptions
✓ Load images automatically     Except       ✓ Enable JavaScript     Adyan       ✓ Enable Java     Fonts & Colors	eptions
✓ Enable JavaScript     Adyan       ✓ Enable Java     Fonts & Colors	
Fonts & Colors	anced
Fonts & Colors	
Default font: Times New Roman Size: 16 💌 Advar	
	vanced
Colo	jolors
- File Types	
	anage
<u>.</u>	

Figure 77 Mozilla Firefox Content Security

# Opera

Opera 10 screens are used here. Screens for other versions may vary slightly.

# **Allowing Pop-Ups**

From Opera, click Tools, then Preferences. In the General tab, go to Choose how you prefer to handle pop-ups and select Open all pop-ups.

Figure 78 Opera: Allowing Pop-Ups

Opera cap star	at with the second second to the second second terms from the times	
	rt with your favorite Web pages or continue from last time	
Startup	Continue from last time	
Home page	http://portal.opera.com Use Current	1
Choose how yo	ou prefer to handle pop-ups	
Choose how yo	Open all pop-ups	
	Open all pop-ups Open all pop-ups Open pop-ups in background	
	Open all pop-ups Open pop-ups  Open pop-ups in background Block unwanted pop-ups	
Pop-ups	Open all pop-ups Open all pop-ups Open pop-ups in background	

# **Enabling Java**

From Opera, click **Tools**, then **Preferences**. In the **Advanced** tab, select **Content** from the left-side menu. Select the check boxes as shown in the following screen.

Figure 79 Opera: Enabling Java

Pre	ferences		x
G	ieneral   Forms   Sear	ch   Web Pages Advanced	
C	Tabs Browsing Notifications Content Fonts Downloads Programs	Enable animated images     Enable sound in Web pages     Enable JavaScript     DavaScript     Enable plug-ins	
	History Cookies Security	Style Options	_
	Network Toolbars Shortcuts	Content settings can be adapted to each site           Manage Site Preferences           Blocked Content	
	Voice	OK Cancel Help	

To customize JavaScript behavior in the Opera browser, click JavaScript Options.

Figure 80 Opera: JavaScript Options

Ja	ivaS	cript Options X
	R	Allow resizing of windows
	☑	Allow moving of windows
		Allow raising of windows
		Allow lowering of windows
	•	Allow changing of status field
	◄	Allow scripts to detect context menu events
	•	Allow script to hide address bar
		Open console on error
	V.	er JavaScript folder
		Choose
		OK Cancel

Select the items you want Opera's JavaScript to apply.

# APPENDIX B Setting Up Your Computer's IP Address

Note: Your specific EMG2881-T20A 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 121
- Windows Vista on page 124
- Windows 7 on page 127
- Mac OS X: 10.3 and 10.4 on page 132
- Mac OS X: 10.5 and 10.6 on page 135
- Linux: Ubuntu 8 (GNOME) on page 138
- Linux: openSUSE 10.3 (KDE) on page 142

#### 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.



2 In the Control Panel, click the Network Connections icon.



3 Right-click Local Area Connection and then select Properties.



4 On the General tab, select Internet Protocol (TCP/IP) and then click Properties.

Local	Area Conne	ction	Proper	ies			?
General	Authentication	Adv	anced				
Connec	t using:						
<b>III)</b> /	ccton EN1207	D-TX F	PCI Fast E	thernet	Adap	oter	
						Configur	e
This co	nnection uses tl	he follo	wing item	s:			
	QoS Pookot 9 Internet Proto	col (TC	ler :P/IP) Uninstall	)		Propertie	
Desc			ormiotal			Поронае	
Tran wide	smission Contro area network p ss diverse interc	rotoco	I that prov	ides co			ult
Sho	w icon in notific	ation a	rea when	connec	cted		

5 The Internet Protocol TCP/IP Properties window opens.

meral Alternate Configur	ation
	signed automatically if your network supports ou need to ask your network administrator for
<ul> <li>Obtain an IP address</li> </ul>	automatically
OUse the following IP a	ddress:
IP address:	
Subnet mask:	
Default gateway:	
Obtain DNS server ad	ddress automatically
OUse the following DN	S server addresses:
Preferred DNS server:	
Alternate DNS server:	
	Advanced

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.

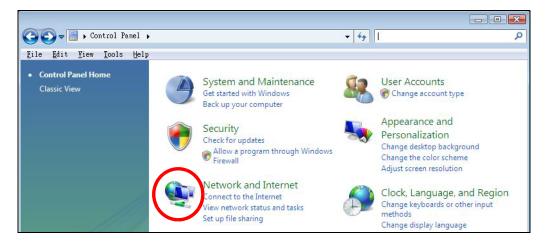
#### Windows Vista

This section shows screens from Windows Vista Professional.

1 Click Start > Control Panel.



2 In the Control Panel, click the Network and Internet icon.



3 Click the Network and Sharing Center icon.



4 Click Manage network connections.



5 Right-click Local Area Connection and then select Properties.

LAN or High-Spec	Collapse group	Left Arrow
Netwo Intel	Expand all groups Collapse all groups	
	Disable Status Diagnose	
	Bridge Connections	
	Create Shortcut Delete Rename	
<	Properties	

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.

working		
onnect using:		
🛐 Intel(R) PRO/1	000 MT Desktop Connection	
	Con	figure
nis connection uses	the following items:	
🗹 👥 Client for Mic	rosoft Networks	
🛛 县 Network Mor	nitor3 Driver	
	사망 방법 방법 방법 방법	
🗹 📇 File and Print	ter Sharing for Microsoft Networks	
The second s	ter Sharing for Microsoft Networks <u> pcol Version 6 (TCP/IPv6)</u>	
🖌 📥 Internet Prote	4 Y C G 11 C 2 C C T C C C C C C C C C C C C C C C	
<ul> <li>Internet Prote</li> <li>Internet Prote</li> </ul>	acol Version 6 (TCP/IPv6)	/er
<ul> <li>Internet Prote</li> <li>Internet Prote</li> <li>Internet Prote</li> <li>Link-Layer To</li> </ul>	ocol Version 6 (TCP/IPv6) ocol Version 4 (TCP/IPv4)	/er
<ul> <li>Internet Prote</li> <li>Internet Prote</li> <li>Internet Prote</li> <li>Link-Layer To</li> </ul>	peol Version 6 (TCP/IPv6) peol Version 4 (TCP/IPv4) opology Discovery Mapper I/O Driv	/er
<ul> <li>Internet Prote</li> <li>Internet Prote</li> <li>Internet Prote</li> <li>Link-Layer To</li> </ul>	ocol Version 6 (TCP/IPv6) ocol Version 4 (TCP/IPv4) opology Discovery Mapper I/O Driv opology Discovery Responder	
<ul> <li>✓ Internet Prote</li> <li>✓ Internet Prote</li> <li>✓ Link-Layer Tr</li> <li>✓ Link-Layer Tr</li> <li>✓ Link-Layer Tr</li> </ul>	ocol Version 6 (TCP/IPv6) ocol Version 4 (TCP/IPv4) opology Discovery Mapper I/O Driv opology Discovery Responder	ver
<ul> <li>Internet Prote</li> <li>Internet Prote</li> <li>Internet Prote</li> <li>Link-Layer To</li> <li>Link-Layer To</li> <li>Install</li> <li>Description</li> </ul>	ocol Version 6 (TCP/IPv6) ocol Version 4 (TCP/IPv4) opology Discovery Mapper I/O Driv opology Discovery Responder Uninstall Prop	perties
<ul> <li>Internet Prote</li> <li>Internet Prote</li> <li>Internet Prote</li> <li>Link-Layer To</li> <li>Link-Layer To</li> <li>Install</li> <li>Description</li> <li>Transmission Control</li> </ul>	ocol Version 6 (TCP/IPv6) ocol Version 4 (TCP/IPv4) opology Discovery Mapper I/O Driv opology Discovery Responder Uninstall Prop ol Protocol/Internet Protocol. The o	berties default
<ul> <li>Internet Prote</li> <li>Internet Prote</li> <li>Ink-Layer Tr</li> <li>Link-Layer Tr</li> <li>Install</li> <li>Description</li> <li>Transmission Contr</li> <li>wide area network</li> </ul>	ocol Version 6 (TCP/IPv6) ocol Version 4 (TCP/IPv4) opology Discovery Mapper I/O Driv opology Discovery Responder Uninstall Prop	berties default
<ul> <li>Internet Prote</li> <li>Internet Prote</li> <li>Install</li> <li>Description</li> <li>Transmission Contrivide area network</li> </ul>	opol Version 6 (TCP/IPv6) opology Discovery Mapper I/O Driv opology Discovery Responder Uninstall Prop ol Protocol/Internet Protocol. The o protocol that provides communicati	berties default

7 The Internet Protocol Version 4 (TCP/IPv4) Properties window opens.

Seneral You car	Alternate Configuration		dia i Fin		otwork .	supports
this cap	ability. Otherwise, you appropriate IP settings	need to ask				
0	otain an IP address auto	omatically				
_ () Uş	e the following IP addre	ess:				
<u>I</u> P ad	ldress:		3	5	÷	
Sybr	iet mask:		3	12	12	
<u>D</u> efa	ult gateway:		-1	2		
<b>o</b> ol	otain DNS server addres	ss automatica	lly			
O Us	e the following DNS ser	ver addresse	s:			
Pref	erred DNS server:		0		1.	
Alter	nate DNS server:		13	12	i.	
					Adv	anced

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**

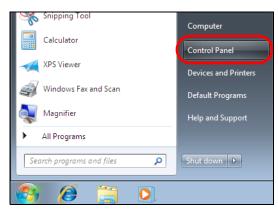
- 1 Click Start > All Programs > Accessories > Command Prompt.
- 2 In the Command Prompt window, type "ipconfig" and then press [ENTER].

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.



2 In the Control Panel, click View network status and tasks under the Network and Internet category.



3 Click Change adapter settings.



4 Double click Local Area Connection and then select Properties.

🚱 🔵 🗢 🖳 🕨 Control Panel 🕨 Net	work and Internet   Network	Connections
Organize 🔻 Disable this network d	evice Diagnose this conn	ection Rename this
Local Area Connection Unidentified network Broadcom NetXtreme Gigabit	ZyXEL_RT3	etwork Connection 062_AP1 4 reless USB Adapter
Local Area Connection Status		
Connection IPv4 Connectivity:	No network access	
IPv6 Connectivity:	No network access	
Media State:	Enabled	
Duration:	00:04:36	
Speed:	100.0 Mbps	
Details		
Activity		
Sent —	Received	
Packets: 432	0	
Properties 🛞 Disable	Diagnose	
	Close	
·		

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.

🕌 Local Area Connection Properties 🛛 💽
Networking Sharing
Connect using:
Broadcom NetXtreme Gigabit Ethemet
<u>C</u> onfigure This c <u>o</u> nnection uses the following items:
<ul> <li>Client for Microsoft Networks</li> <li>QoS Packet Scheduler</li> <li>File and Printer Sharing for Microsoft Networks</li> <li>Internet Protocol Version 6 (TCP/IPv6)</li> <li>Internet Protocol Version 4 (TCP/IPv4)</li> <li>Ink-Layer Topology Discovery Mapper I/O Driver</li> <li>Link-Layer Topology Discovery Responder</li> </ul>
Install Uninstall Properties
Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
OK Cancel

6 The Internet Protocol Version 4 (TCP/IPv4) Properties window opens.

Internet Protocol Version 4 (TCP/IPv4)	Properties							
General								
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.								
Obtain an IP address automatical	y							
Use the following IP address:								
IP address:	192.168.1.7							
S <u>u</u> bnet mask:	255 . 255 . 255 . 0							
Default gateway:								
Obtain DNS server address autom	natically							
• Us <u>e</u> the following DNS server add	resses:							
Preferred DNS server:								
<u>A</u> lternate DNS server:	· · ·							
Valjidate settings upon exit	Ad <u>v</u> anced							
	OK Cancel							

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.

X C:\WINNT\system32\cmd.exe	
::\>ipconfig	<u> </u>
Findows 2000 IP Configuration	
Sthernet adapter Local Area Connection:	
Connection-specific DNS Suffix . : P-2612HNU-F3v	2
IP Address	
Default Gateway : 192.168.1.1	
	-

# 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.



2 In the System Preferences window, click the Network icon.



3 When the Network preferences pane opens, select Built-in Ethernet from the network connection type list, and then click Configure.

	Location:	Automatic
	Show	Network Status
θ	Built-in Ethernet	Built-in Ethernet is currently active and has the IP address 10.0.1.2. You are connected to the internet via Built-in Ethernet.
•		Internet Sharing is on and is using AirPort to share the connection.
		Configure) (Disconnect)

4 For dynamically assigned settings, select Using DHCP from the Configure IPv4 list in the TCP/IP tab.

	Ne	etwork		
Show All			Q	
L	ocation: Automatio	c	•	
	Show: Built-in Et	thernet	•	
ТСР	/IP PPPoE Appl	eTalk Proxies	Ethernet	
Configure IPv4:			•	
IP Address:		1	Renew DH	Please
Subnet Mask:	0.0.0.0	DHCP Client ID	-	
Router:		brier chent ib	(If required	)
DNS Servers:				1
Divs Servers.				
Search Domains:				(Optiona
IPv6 Address:				
	Configure IPv6	)		(

- **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.

0	Network		
Show All		Q	
U	ocation: Automatic	;	
	Show: Built-in Ethernet	;	
TCP	IP PPPoE AppleTalk P	roxies Ethernet	
Configure IPv4:	Manually	;	
IP Address:	0.0.0.0		
Subnet Mask:	0.0.0.0		
Router:	0.0.0.0		
DNS Servers:			
Search Domains:			(Optiona
IPv6 Address:			
	Configure IPv6		(

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.

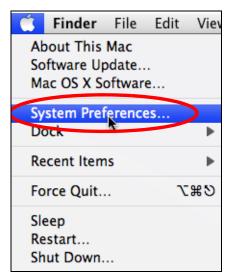


O O Network I			Utility				
Info Netstat App	leTalk	Ping	Lookup	Traceroute	Whois	Finger	Port Scan
lease select a network	interfac	e for in	formation				
Network Interface (er	0)	:					
Interface Informatio	n			Transfer	Statistics		
Hardware Address	00:16:c	b:8b:50	:2e	Sent Packets 20607			
IP Address(es)	118.169	9.44.20	3	Send Errors 0			
Link Speed	100 Mb			Recv Pack	ets 2262	6	
Link Status	Active			Recv Err	ors 0		
Vendor	Marvell			Collisio	ons 0		
Model	Yukon C 88E805	Contraction of the second	Adapter				

#### 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.



2 In System Preferences, click the Network icon.



3 When the Network preferences pane opens, select Ethernet from the list of available connection types.

00		Network		-	
Show All				٩	
	Location: (	Automatic		•	
Internal Modem Not Connected	Con	Status:	Not Connected		
PPPoE     Not Connected	§		The cable for Etherne your computer does	et is connected, but not have an IP address.	
Ethernet Not Connected	<···>	Configure:	Using DHCP	÷	
FireWire Not Connected	¥				
AirPort     Off					
		DNS Server:			
		Search Domains:			
		802.1X:	WPA: ZyXEL04	Connect	
+ - *-				Advanced	?
Click the lock to	prevent further	changes.	Assist me	(Revert) (Appl	y

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 EMG2881-T20A.

00		Network		
Show All				٩
	Location: Automat	tic		•
<ul> <li>Internal Modem Not Connected</li> <li>PPPoE Not Connected</li> </ul>	Cor.	1	Not Connected The cable for Ethernet Your computer does n	t is connected, but iot have an IP address.
Ethernet     Not Connected	Cc	onfigure:	Manually	•
<ul> <li>FireWire Not Connected</li> <li>AirPort Off</li> </ul>	Subn	Address: net Mask: Router: IS Server: Domains: 802.1X:	0.0.0.0 WPA: ZyXEL04	Connect
+ - \$.				Advanced) ?
Click the lock to	prevent further changes.	(	Assist me	Revert Apply

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.

O Network Util	lity			
<mark>nfo</mark> Netstat AppleTalk Ping Lookup T	Fraceroute	Whois	Finger	Port Scar
ease select a network interface for information				
Network Interface (en1)	Transfer	Statistics		
Hardware Address: 00:30:65:25:6a:b3	Sent Packets: 1230			
IP Address(es): 10.0.2.2	Send Errors: 0			
Link Speed: 11 Mbit/s	Recv Pac	kets: 119	7	
Link Status: Active	Recv Er	rors: 0		
Vendor: Apple	Collis	ions: 0		
Model: Wireless Network Adapter				

Figure 82 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.



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.

5	Network Settings	×			
Location:					
Connections Genera	I DNS Hosts				
-	d connection g mode enabled	<b>P</b> roperties			
	to point connec work interface is not c				
<u> H</u> elp		lock <u>C</u> lose			

3 In the Authenticate window, enter your admin account name and password then click the Authenticate button.

-	Authenticate 🛛 🗙
R	System policy prevents modifying the configuration
	An application is attempting to perform an action that requires privileges. Authentication as one of the users below is required to perform this action.
	🕒 C.J.,,,, (chris) 📫
	Password for chris:
þ <u>D</u> eta	ils
	Cance Authenticate

4 In the Network Settings window, select the connection that you want to configure, then click Properties.

Network Settings	×
Location:	•
Connections General DNS Hosts	
Wired connection     Roaming mode enabled	Properties
Point to point connec.     This network interface is not c	
🕜 Help	Unlock

5 The **Properties** dialog box opens.

( <u>5</u>	th0 Properties 🛛 🗙					
□ E <u>n</u> able roaming mo	Enable roaming mode					
Connection Settings						
Con <u>fi</u> guration:						
<u>I</u> P address:						
<u>S</u> ubnet mask:						
<u>G</u> ateway address:						
	Cancel					

- 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.

Network S	ettings X
Location:	
Connections General DNS Host	S
DNS Servers	
10.0.2.3	<u>루 A</u> dd
Search Domains	
	- Add ☐ Delete
C Help	Unlock Close

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.

nfigure

#### Figure 83 Ubuntu 8: Network Tools

#### Linux: openSUSE 10.3 (KDE)

This section shows you how to configure your computer's TCP/IP settings in the K 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).

Search:			•	
			Applica	tions 🔺
	dministrator Settings aST			
👰 In	stall Software			
	ystem Information ysinfo:/			
			System Fo	Iders
	ome Folder nome/zyxel			
	<b>y Documents</b> nome/zyxel/Docum	ents		
	etwork Folders emote:/			
			ħ	1edia
	4G Media (2.0 GB ava	ilable)		•
$\stackrel{\frown}{\simeq}$			$\bigotimes$	•2
<u>F</u> avorites	Applications	<u>C</u> omputer	History	Leave
User zyxel on linux-h2oz			open <b>S</b>	iUSE <sup>®</sup>

2 When the Run as Root - KDE su dialog opens, enter the admin password and click OK.

💥 Run as root - KDE su 🎱 🛛 🛛 🗶				
R	Please enter the Administra password to continue.	ator (root)		
Command:	/sbin/yast2			
<u>P</u> assword:	rd: 🛛 🕶 🕶			
	Ignore 🖌 OK	X <u>C</u> ancel		

3 When the YaST Control Center window opens, select Network Devices and then click the Network Card icon.

🥘 YaST Control Center @ lir	iux-h2oz 🎱			×
<u>E</u> ile <u>E</u> dit <u>H</u> elp				
Software	DSL		ISDN	
Hardware				
Software Hardware System	Modem 🚰	3	Network Card	
Network Services				
Movell AppArmor				
Security and Users				
Network Devices          Network Services         Novell AppArmor         Security and Users         Miscellaneous         Search				
Search	۹ <u></u>			

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.

	A Notwork Sottings	
Network Card Overview	Network Settings	
Obtain an overview of		
nstalled network cards.	Global Options Overview Hostname/DNS Routing	
Additionally, edit their		]
configuration.	Name         IP Address           AMD PCnet - Fast 79C971 DHCP         IP Address	
Adding a Network	AMD PChet - Fast 790971 DHCP	
Card:		
ress Add to configure a		
nanually.		
Configuring or		
eleting: hoose a network card		
change or remove.		
hen press Configure or		
elete as desired.		
	AMD PCnet - Fast 79C971	
	MAC: 08:00:27:96:ed:3d	
	Device Name: eth-eth0	
	<ul> <li>Started automatically at boot</li> <li>IP address assigned using DHCP</li> </ul>	
	• IF address assigned using DHCF	
	Add <u>C</u> onfigure delete	
	Add <u>C</u> onfigure Jele <u>t</u> e	

5 When the Network Card Setup window opens, click the Address tab

Address Setup 🔺	Network Ca	rd Setup		
Select <b>No Address</b> Setup if you do not want any IP address for this device. This is particularly useful for bonding ethernet devices.		Hardware onfiguration Name th0 r Bonding Devices)		
Select Dynamic	O Dynamic Address	DHCP		
address if you do not	Statically assigned	d IP Address		
address assigned by	IP Address	<u>S</u> ubnet Mask	<u>H</u> ostname	
he system				
administrator or your cable or DSL provider.	Additional Addresses	1 <del>-</del>		
You can choose one of	Alias Name IP.	Address Netmask		
he dynamic address		innerst mensee Uperstandig internet of the		5
assignment method. Select <b>DHCP</b> if you				
nave a DHCP server				
running on your local				
network. Network addresses are then				
obtained automatically from the server. To automatically				
rom the server. Fo automatically search for free IP and				
rom the server. To automatically			elete	

#### Figure 84 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.

Enter the name for Anis computer and the	Network Settings	
DNS domain that it belongs to.	Global Options Overview Hostn	ame/DNS Routing
Optionally enter the name server list and	Hostname and Domain Name	Domain Name
domain search list.	linux-h2oz	site
Note that the hostname is globalit applies to all	<u>C</u> hange Hostname via DHCP <u>W</u> rite Hostname to /etc/hosts	
interfaces, not just this one. The domain is	Ch <u>a</u> nge /etc/resolv.conf manually     Name Servers and Domain Search L     Name Server 1	st
especially important if	10.0.2.3	
this computer is a mail server.	Name Server 2	
If you are using DHCP to get an IP address, check whether to get	Name Server <u>3</u>	
a hostname via DHCP. The hostname of your host (which can be	Update DNS data via DHCP	
seen by issuing the hostname command) will be set automatically by the DHCP client. You may want to disable this option if you connect to different networks		

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 submenu, select Show Connection Information.

Figure 85 openSUSE 10.3: KNetwork Manager

🕅 Enable Wireless		
🗊 Disable Wireless	🥪 KNetworkManager	
🖌 Switch to Online Mode	🔍 Wired Devices	
🐼 Switch to Offline Mode	🗙 Wired Network	
🝸 Show Connection Information	🔜 Dial-Up Connections	•
💫 Configure	🔦 Options	•
	🕢 🕜 <u>H</u> elp	•
	0 Quit	Ctrl+Q

When the **Connection Status - KNetwork Manager** window opens, click the **Statistics tab** to see if your connection is working properly.

rigare ee operie					
💫 Connection Status - KNetworkManager 🥯 🛜 🗖 🗙					
<u>D</u> evice	🔌 <u>A</u> ddresse 🛛 🔇 S	tatistics			
	Received	Transmitted			
Bytes	2317441	841875			
MBytes	2.2	0.8			
Packets	3621	3140			
Errors	0	0			
Dropped	0	0			
KBytes/s	0.0	0.0			
		<b>₩</b> OK			

Figure 86 openSUSE: Connection Status - KNetwork Manager

# APPENDIX C 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.

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	7648	A popular videoconferencing solution from White
	UDP	24032	Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (for example <u>www.zyxel.com</u> ) to IP numbers.
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
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	20	File Transfer Program, a program to enable fast
	ТСР	21	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.

#### Table 47 Commonly Used Services

Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the

PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the

A streaming audio service that enables real time

The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the

Simple Mail Transfer Protocol is the message-

control channel.

data channel.

Remote Login.

Remote Telnet.

Internet.

Remote Command Service.

Remote Execution Daemon.

Simple File Transfer Protocol.

sound over the web.

NAME	PROTOCOL	PORT(S)	DESCRIPTION
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	ТСР	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).

1723

47

512

7070

514

513

107

554

115

25

PPTP

RCMD

REXEC

RLOGIN

RTELNET

RTSP

SFTP

SMTP

REAL AUDIO

PPTP\_TUNNEL (GRE)

TCP

TCP

TCP

TCP

TCP

TCP

TCP

TCP

TCP/UDP

User-Defined

			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.

NAME	PROTOCOL	PORT(S)	DESCRIPTION
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.
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.

Table 47 Commonly Used Services (continued)

# APPENDIX D Customer Support

In the event of problems that cannot be solved by using this manual, you should contact your vendor. If you cannot contact your vendor, then contact a Zyxel office for the region in which you bought the device.

See http://www.zyxel.com/homepage.shtml and also http://www.zyxel.com/about\_zyxel/zyxel\_worldwide.shtml for the latest information.

Please have the following information ready when you contact an office.

# **Required Information**

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

# Corporate Headquarters (Worldwide)

#### Taiwan

- Zyxel Communications Corporation
- http://www.zyxel.com

#### Asia

#### China

- Zyxel Communications (Shanghai) Corp.
   Zyxel Communications (Beijing) Corp.
   Zyxel Communications (Tianjin) Corp.
- http://www.zyxel.cn

#### India

- Zyxel Technology India Pvt Ltd
- http://www.zyxel.in

#### Kazakhstan

- Zyxel Kazakhstan
- http://www.zyxel.kz

#### Korea

- Zyxel Korea Corp.
- http://www.zyxel.kr

# Malaysia

- Zyxel Malaysia Sdn Bhd.
- http://www.zyxel.com.my

#### Pakistan

- Zyxel Pakistan (Pvt.) Ltd.
- http://www.zyxel.com.pk

# Philippines

- Zyxel Philippines
- http://www.zyxel.com.ph

# Singapore

- Zyxel Singapore Pte Ltd.
- http://www.zyxel.com.sg

#### Taiwan

- Zyxel Communications Corporation
- http://www.zyxel.com/tw/zh/

# Thailand

- Zyxel Thailand Co., Ltd
- http://www.zyxel.co.th

# Vietnam

- Zyxel Communications Corporation-Vietnam Office
- http://www.zyxel.com/vn/vi

# Europe

# Austria

- Zyxel Deutschland GmbH
- http://www.zyxel.de

# Belarus

- Zyxel BY
- http://www.zyxel.by

#### Belgium

- Zyxel Communications B.V.
- http://www.zyxel.com/be/nl/
- http://www.zyxel.com/be/fr/

#### Bulgaria

- Zyxel България
- http://www.zyxel.com/bg/bg/

# **Czech Republic**

- Zyxel Communications Czech s.r.o
- http://www.zyxel.cz

#### Denmark

- Zyxel Communications A/S
- http://www.zyxel.dk

#### Estonia

- Zyxel Estonia
- http://www.zyxel.com/ee/et/

# Finland

- Zyxel Communications
- http://www.zyxel.fi

#### France

- Zyxel France
- http://www.zyxel.fr

#### Germany

- Zyxel Deutschland GmbH
- http://www.zyxel.de

#### Hungary

- Zyxel Hungary & SEE
- http://www.zyxel.hu

#### Italy

- Zyxel Communications Italy
- http://www.zyxel.it/

# Latvia

- Zyxel Latvia
- http://www.zyxel.com/lv/lv/homepage.shtml

# Lithuania

- Zyxel Lithuania
- http://www.zyxel.com/lt/lt/homepage.shtml

# Netherlands

- Zyxel Benelux
- http://www.zyxel.nl

# Norway

- Zyxel Communications
- http://www.zyxel.no

# Poland

- Zyxel Communications Poland
- http://www.zyxel.pl

# Romania

- Zyxel Romania
- http://www.zyxel.com/ro/ro

# Russia

- Zyxel Russia
- http://www.zyxel.ru

# Slovakia

- Zyxel Communications Czech s.r.o. organizacna zlozka
- http://www.zyxel.sk

# Spain

- Zyxel Communications ES Ltd
- http://www.zyxel.es

# Sweden

- Zyxel Communications
- http://www.zyxel.se

# Switzerland

• Studerus AG

• http://www.zyxel.ch/

### Turkey

- Zyxel Turkey A.S.
- http://www.zyxel.com.tr

# UK

- Zyxel Communications UK Ltd.
- http://www.zyxel.co.uk

### Ukraine

- Zyxel Ukraine
- http://www.ua.zyxel.com

# Latin America

### Argentina

- Zyxel Communication Corporation
- http://www.zyxel.com/ec/es/

### Brazil

- Zyxel Communications Brasil Ltda.
- https://www.zyxel.com/br/pt/

### Ecuador

- Zyxel Communication Corporation
- http://www.zyxel.com/ec/es/

### Middle East

### Israel

- Zyxel Communication Corporation
- http://il.zyxel.com/homepage.shtml

# Middle East

- Zyxel Communication Corporation
- http://www.zyxel.com/me/en/

# North America

# USA

- Zyxel Communications, Inc. North America Headquarters
- http://www.zyxel.com/us/en/

# Oceania

# Australia

- Zyxel Communications Corporation
- http://www.zyxel.com/au/en/

# Africa

# South Africa

- Nology (Pty) Ltd.
- http://www.zyxel.co.za

# **APPENDIX E** Legal Information

#### Copyright

Copyright © 2018 by Zyxel Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of Zyxel Communications Corporation.

Published by Zyxel Communications Corporation. All rights reserved.

#### Disclaimer

Zyxel does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. Zyxel further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

#### **Regulatory Notice and Statement**

#### UNITED STATES of AMERICA



The following information applies if you use the product within USA area.

#### FCC EMC Statement

• The device complies with Part 15 of 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.

- Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the device.
- This product has been tested and complies with the specifications 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 according to 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 or television reception, which is found 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:
  - Reorient or relocate the receiving antenna
  - Increase the separation between the devices
  - Connect the equipment to an outlet other than the receiver's
  - Consult a dealer or an experienced radio/TV technician for assistance

The following information applies if you use the product with RF function within USA area.

#### FCC Radiation Exposure Statement

- This device complies with FCC RF radiation exposure limits set forth for an uncontrolled environment.
- This transmitter must be at least 23 cm from the user and must not be co-located or operating in conjunction with any other antenna or transmitter.
- Operation of this device is restricted to indoor use only, except for relevant user's manual mention that this device can be installed into the
  external environment.

#### CANADA

The following information applies if you use the product within Canada area.

#### Industry Canada ICES Statement

CAN ICES-3 (B)/NMB-3(B)

157

#### Industry Canada RSS-GEN & RSS-247 statement

- This device complies with Industry Canada license-exempt RSS standard(s). 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 radio transmitter (2468C-EMG2881T20A) has been approved by Industry Canada to operate with the antenna types listed below with the maximum permissible gain and required antenna impedance for each antenna type indicated. Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.

#### Antenna Information

TYPE	MANUFACTURER	GAIN	CONNECTOR
РСВ	CINGXIN	2.97 dBi (2.4~2.4835GHz)	i-pex(MHF)
		2.99 dBi (5.15~5.85GHz)	
РСВ	CINGXIN	2.75 dBi (2.4~2.4835GHz)	i-pex(MHF)
		2.97 dBi (5.15~5.85GHz)	

If the product with 5G wireless function operating in 5150-5250 MHz and 5725-5850 MHz, the following attention must be paid,

- The device for operation in the band 5150-5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems.
- For devices with detachable antenna(s), the maximum antenna gain permitted for devices in the band 5725-5850 MHz shall be such that the equipment still complies with the e.i.r.p. limits specified for point-to-point and non-point-to-point operation as appropriate; and The worst-case tilt angle(s) necessary to remain compliant with the e.i.r.p. elevation mask requirement set forth in Section 6.2.2(3) of RSS 247
- shall be clearly indicated.

If the product with 5G wireless function operating in 5250-5350 MHz and 5470-5725 MHz , the following attention must be paid.

- For devices with detachable antenna(s), the maximum antenna gain permitted for devices in the bands 5250-5350 MHz and 5470-5725 MHz
- shall be such that the equipment still complies with the e.i.r.p. limit. Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.
- Le présent émetteur radio (2468C-EMG2881T20A) de modèle s'il fait partie du matériel de catégoriel) a été approuvé par Industrie Canada pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal et l'impédance requise pour chaque type d'antenne. Les types d'antenne non inclus dans cette liste, ou dont le gain est supérieur au gain maximal indiqué, sont strictement interdits pour l'exploitation de l'émetteur.

#### Informations Antenne

TYPE	FABRICANT	GAIN	CONNECTEUR
РСВ	CINGXIN	2.97 dBi (2.4~2.4835GHz)	i-pex(MHF)
		2.99 dBi (5.15~5.85GHz)	
РСВ	CINGXIN	2.75 dBi (2.4~2.4835GHz)	i-pex(MHF)
		2.97 dBi (5.15~5.85GHz)	

Lorsque la fonction sans fil 5G fonctionnant en 5150-5250 MHz and 5725-5850 MHz est activée pour ce produit , il est nécessaire de porter une attention particulière aux choses suivantes

- Les dispositifs fonctionnant dans la bande 5150-5250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux:
- Pour les dispositifs munis d'antennes amovibles, le gain maximal d'antenne permis (pour les dispositifs utilisant la bande de 5 725 à 5 850 MHz) doit être conforme à la limite de la p.i.r.e. spécifiée pour l'exploitation point à point et l'exploitation non point à point, selon le cas;
- Les pires angles d'inclinaison nécessaires pour rester conforme à l'exigence de la p.i.r.e. applicable au masque d'élévation, et énoncée à la section 6.2.2 3) du CNR-247, doivent être clairement indiqués.

Lorsque la fonction sans fil 5G fonctionnant en 5250-5350 MHz et 5470-5725 MHz est activée pour ce produit , il est nécessaire de porter une attention particulière aux choses suivantes.

Pour les dispositifs munis d'antennes amovibles, le gain maximal d'antenne permis pour les dispositifs utilisant les bandes de 5 250 à 5 350 MHz et de 5 470 à 5 725 MHz doit être conforme à la limite de la p.i.r.e.

#### Industry Canada radiation exposure statement

This device complies with IC radiation exposure limits set forth for an uncontrolled environment. This device should be installed and operated with a minimum distance of 25 cm between the radiator and your body.

#### Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 25 cm de distance entre la source de ravonnement et votre corps.

#### **EUROPEAN UNION**



The following information applies if you use the product within the European Union.

#### Declaration of Conformity with Regard to EU Directive 2014/53/EU (Radio Equipment Directive, RED)

- Compliance information for 2.4GHz and/or 5GHz wireless products relevant to the EU and other Countries following the EU Directive 2014/53/ EU (RED). And this product may be used in all EU countries (and other countries following the EU Directive 2014/53/EU) without any limitation except for the countries mentioned below table:
- In the majority of the EU and other European countries, the 5GHz bands have been made available for the use of wireless local area networks (LANs). Later in this document you will find an overview of countries in which additional restrictions or requirements or both are applicable. The requirements for any country may evolve. Zyxel recommends that you check with the local authorities for the latest status of their national regulations for the 5GHz wireless LANs. If this device for operation in the band 5150-5350 MHz, it is for indoor use only.
- If this device for operation in the band 5150-5350 MHz, it is for indoor use only.
  This equipment should be installed and operated with a minimum distance of 20cm between the radio equipment and your body.

Български (Bulgarian)	С настоящото Zyxel декларира, че това оборудване е в съответствие със съществените изисквания и другите приложими разпоредбите на Директива 2014/53/ЕС.			
	National Restrictions			
	<ul> <li>The Belgian Institute for Postal Services and Telecommunications (BIPT) must be notified of any outdoor wireless link having a range exceeding 300 meters. Please check http://www.bipt.be for more details.</li> <li>Draadloze verbindingen voor buitengebruik en met een reikwijdte van meer dan 300 meter dienen aangemeld te worden bij het Belgisch Instituut voor postdiensten en telecommunicatie (BIPT). Zie http://www.bipt.be voor meer gegevens.</li> <li>Les liaisons sans fil pour une utilisation en extérieur d'une distance supérieure à 300 mètres doivent être notifiées à l'Institut Belge des services Postaux et des Télécommunications (IBPT). Visitez http://www.ibpt.be pour de plus amples détails.</li> </ul>			
Español (Spanish)	Por medio de la presente Zyxel declara que el equipo cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 2014/53/UE			
Čeština (Czech)	Zyxel tímto prohlašuje, že tento zařízení je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 2014/53/EU.			
Dansk (Danish)	Undertegnede Zyxel erklærer herved, at følgende udstyr udstyr overholder de væsentlige krav og øvrige relevante krav i direktiv 2014/53/EU.			
	National Restrictions			
	<ul> <li>In Denmark, the band 5150 - 5350 MHz is also allowed for outdoor usage.</li> <li>I Danmark må frekvensbåndet 5150 - 5350 også anvendes udendørs.</li> </ul>			
Deutsch (German)	Hiermit erklärt Zyxel, dass sich das Gerät Ausstattung in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 2014/53/EU befindet.			
Eesti keel (Estonian)	Käesolevaga kinnitab Zyxel seadme seadmed vastavust direktiivi 2014/53/EL põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.			
Ελληνικά (Greek)	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ ΖΥΧΘΙ ΔΗΛΩΝΕΙ ΟΤΙ εξοπλισμός ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 2014/53/ΕΕ.			
English	Hereby, Zyxel declares that this device is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU.			
Français (French)	Par la présente Zyxel déclare que l'appareil équipements est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 2014/53/UE.			
Hrvatski (Croatian)	Zyxel ovime izjavljuje da je radijska oprema tipa u skladu s Direktivom 2014/53/UE.			
Íslenska (Icelandic)	Hér með lýsir, Zyxel því yfir að þessi búnaður er í samræmi við grunnkröfur og önnur viðeigandi ákvæði tilskipunar 2014/53/ UE.			
Italiano (Italian)	Con la presente Zyxel dichiara che questo attrezzatura è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 2014/53/UE.			
	National Restrictions			
	<ul> <li>This product meets the National Radio Interface and the requirements specified in the National Frequency Allocation Table for Italy. Unless this wireless LAN product is operating within the boundaries of the owner's property, its use requires a "general authorization." Please check http://www.sviluppoeconomico.gov.it/ for more details.</li> <li>Questo prodotto è conforme alla specifiche di Interfaccia Radio Nazionali e rispetta il Piano Nazionale di ripartizione delle frequenze in Italia. Se non viene installato all 'interno del proprio fondo, l'utilizzo di prodotti Wireless LAN richiede una "Autorizzazione Generale". Consultare http://www.sviluppoeconomico.gov.it/ per maggiori dettagli.</li> </ul>			

Latviešu valoda	Ar šo Zyxel deklarē, ka iekārtas atbilst Direktīvas 2014/53/ES būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.		
(Latvian)	National Restrictions		
	<ul> <li>The outdoor usage of the 2.4 GHz band requires an authorization from the Electronic Communications Office. Please check http://www.esd.lv for more details.</li> <li>2.4 GHz frekvenèu joslas izmantoðanai ârpus telpâm nepiecieðama atïauja no Elektronisko sakaru direkcijas. Vairâk informâcijas: http://www.esd.lv.</li> </ul>		
Lietuvių kalba (Lithuanian)	Šiuo Zyxel deklaruoja, kad šis įranga atitinka esminius reikalavimus ir kitas 2014/53/ES Direktyvos nuostatas.		
Magyar (Hungarian)	Alulírott, Zyxel nyilatkozom, hogy a berendezés megfelel a vonatkozó alapvető követelményeknek és az 2014/53/EU irányelv egyéb előírásainak.		
Malti (Maltese)	Hawnhekk, Zyxel, jiddikjara li dan tagħmir jikkonforma mal-ħtiģijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 2014/53/UE.		
Nederlands (Dutch)	Hierbij verklaart Zyxel dat het toestel uitrusting in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 2014/53/EU.		
Polski (Polish)	Niniejszym Zyxel oświadcza, że sprzęt jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 2014/53/UE.		
Português (Portuguese)	Zyxel declara que este equipamento está conforme com os requisitos essenciais e outras disposições da Directiva 2014/53/ UE.		
Română (Romanian)	Prin prezenta, Zyxel declară că acest echipament este în conformitate cu cerințele esențiale și alte prevederi relevante ale Directivei 2014/53/UE.		
Slovenčina (Slovak)	Zyxel týmto vyhlasuje, že zariadenia spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 2014/53/EÚ.		
Slovenščina (Slovene)	Zyxel izjavlja, da je ta oprema v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 2014/53/EU.		
Suomi (Finnish)	Zyxel vakuuttaa täten että laitteet tyyppinen laite on direktiivin 2014/53/EU oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.		
Svenska (Swedish)	Härmed intygar Zyxel att denna utrustning står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 2014/53/EU.		
Norsk (Norwegian)	Erklærer herved Zyxel at dette utstyret er I samsvar med de grunnleggende kravene og andre relevante bestemmelser I direktiv 2014/53/EU.		

#### Notes:

Although Norway, Switzerland and Liechtenstein are not EU member states, the EU Directive 2014/53/EU has also been implemented in those countries.

The regulatory limits for maximum output power are specified in EIRP. The EIRP level (in dBm) of a device can be calculated by adding the gain of the antenna used (specified in dBi) to the output power available at the connector (specified in dBm).

COUNTRY	ISO 3166 2 LETTER CODE	COUNTRY	ISO 3166 2 LETTER CODE
Austria	AT	Liechtenstein	LI
Belgium	BE	Lithuania	LT
Bulgaria	BG	Luxembourg	LU
Croatia	HR	Malta	MT
Cyprus	СҮ	Netherlands	NL
Czech Republic	CZ	Norway	NO
Denmark	DK	Poland	PL
Estonia	EE	Portugal	PT
Finland	FI	Romania	RO
France	FR	Serbia	RS
Germany	DE	Slovakia	SK
Greece	GR	Slovenia	SI
Hungary	HU	Spain	ES
Iceland	IS	Switzerland	СН
Ireland	IE	Sweden	SE
Italy	IT	Turkey	TR
Latvia	LV	United Kingdom	GB

#### List of national codes

#### **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 obstruct the device ventilation slots as insufficient airflow may harm your device. For example, do not place the device in an enclosed space such as a box or on a very soft surface such as a bed or sofa.
- 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.
- Do not remove the plug and connect it to a power outlet by itself; always attach the plug to the power adaptor first before connecting it to a power outlet.
- 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.
- Please use the provided or designated connection cables/power cables/ adaptors. Connect it to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe). If the power adaptor or cord is damaged, it might cause electrocution. Remove it from the device and the power source, repairing the power adapter or cord is prohibited. 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.
  CAUTION: Risk of explosion if battery is replaced by an incorrect type, dispose of used batteries according to the instruction. Dispose them at the applicable collection point for the recycling of electrical and electronic devices. For detailed information about recycling of this
- product, please contact your local city office, your household waste disposal service or the store where you purchased the product.
  The following warning statements apply, where the disconnect device is not incorporated in the device or where the plug on the power supply cord is intended to serve as the disconnect device,

- For permanently connected devices, a readily accessible disconnect device shall be incorporated external to the device;

- For pluggable devices, the socket-outlet shall be installed near the device and shall be easily accessible.

#### **Environment Statement**

#### ErP (Energy-related Products)

Zyxel products put on the EU market in compliance with the requirement of the European Parliament and the Council published Directive 2009/ 125/EC establishing a framework for the setting of ecodesign requirements for energy-related products (recast), so called as "ErP Directive (Energy-related Products directive) as well as ecodesign requirement laid down in applicable implementing measures, power consumption has satisfied regulation requirements which are:

- Network standby power consumption < 8W, and/or
- Off mode power consumption < 0.5W, and/or</li>
- Standby mode power consumption < 0.5W.</li>

(Wireless setting, please refer to "Wireless" chapter for more detail.)

#### **European Union - Disposal and Recycling Information**

The symbol below means that according to local regulations your product and/or its battery shall be disposed of separately from domestic waste. If this product is end of life, take it to a recycling station designated by local authorities. At the time of disposal, the separate collection of your product and/or its battery will help save natural resources and ensure that the environment is sustainable development.

Die folgende Symbol bedeutet, dass Ihr Produkt und/oder seine Batterie gemäß den örtlichen Bestimmungen getrennt vom Hausmüll entsorgt werden muss. Wenden Sie sich an eine Recyclingstation, wenn dieses Produkt das Ende seiner Lebensdauer erreicht hat. Zum Zeitpunkt der Entsorgung wird die getrennte Sammlung von Produkt und/oder seiner Batterie dazu beitragen, natürliche Ressourcen zu sparen und die Umwelt und die menschliche Gesundheit zu schützen.

El símbolo de abajo indica que según las regulaciones locales, su producto y/o su batería deberán depositarse como basura separada de la domástica. Cuando este producto alcance el final de su vida útil, llévelo a un punto limpio. Cuando llegue el momento de desechar el producto, la recogida por separado éste y/o su batería ayudará a salvar los recursos naturales y a proteger la salud humana y medioambiental.

Le symbole ci-dessous signifie que selon les réglementations locales votre produit et/ou sa batterie doivent être éliminés séparément des ordures ménagères. Lorsque ce produit atteint sa fin de vie, amenez-le à un centre de recyclage. Au moment de la mise au rebut, la collecte séparée de votre produit et/ou de sa batterie aidera à économiser les ressources naturelles et protéger l'environnement et la santé humaine.

Il simbolo sotto significa che secondo i regolamenti locali il vostro prodotto e/o batteria deve essere smaltito separatamente dai rifiuti domestici. Quando questo prodotto raggiunge la fine della vita di servizio portarlo a una stazione di riciclaggio. Al momento dello smaltimento, la raccolta separata del vostro prodotto e/o della sua batteria aiuta a risparmiare risorse naturali e a proteggere l'ambiente e la salute umana.

Symbolen innebär att enligt lokal lagstiftning ska produkten och/eller dess batteri kastas separat från hushållsavfallet. När den här produkten når slutet av sin livslängd ska du ta den till en återvinningsstation. Vid tiden för kasseringen bidrar du till en bättre miljö och mänsklig hälsa genom att göra dig av med den på ett återvinningsställe.







以下訊息僅適用於產品具有無線功能且銷售至台灣地區

- 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,指依電信法規定作業之無線電通信。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。
- 無線資訊傳輸設備忍受合法通信之干擾且不得干擾合法通信;如造成干擾,應立即停用,俟無干擾之虞,始得繼續使用。
- 無線資訊傳設備的製造廠商應確保頻率穩定性,如依製造廠商使用手冊上所述正常操作,發射的信號應維持於操作頻帶中
- 使用無線產品時,應避免影響附近雷達系統之操作。
- 若使用高增益指向性天線,該產品僅應用於固定式點對點系統。

以下訊息僅適用於產品屬於專業安裝並銷售至台灣地區

• 本器材須經專業工程人員安裝及設定,始得設置使用,且不得直接販售給一般消費者。

安全警告 - 為了您的安全,請先閱讀以下警告及指示:

- 請勿將此產品接近水、火焰或放置在高溫的環境。
- 避免設備接觸:
  - 任何液體 切勿讓設備接觸水、雨水、高濕度、污水腐蝕性的液體或其他水份。
     灰塵及污物 切勿接觸灰塵、污物、沙土、食物或其他不合適的材料。
- 雷雨天氣時,不要安裝,使用或維修此設備。有遭受電擊的風險。
- 切勿重摔或撞擊設備,並勿使用不正確的電源變壓器。
- 若接上不正確的電源變壓器會有爆炸的風險。
- 請勿隨意更換產品內的電池。
- 如果更換不正確之電池型式,會有爆炸的風險,請依製造商說明書處理使用過之電池。
- 請將廢電池丟棄在適當的電器或電子設備回收處。
- 請勿將設備解體。
- 請勿阻礙設備的散熱孔,空氣對流不足將會造成設備損害。
- 請插在正確的電壓供給插座(如:北美/台灣電壓110VAC,歐洲是230VAC)。

EMG2881-T20A User's Guide

- 假若電源變壓器或電源變壓器的纜線損壞,請從插座拔除,若您還繼續插電使用,會有觸電死亡的風險。
- 請勿試圖修理電源變壓器或電源變壓器的纜線,若有毀損,請直接聯絡您購買的店家,購買一個新的電源變壓器。
- 請勿將此設備安裝於室外,此設備僅適合放置於室內。
- 請勿隨一般垃圾丟棄。
- 請參閱產品背貼上的設備額定功率。
- 請參考產品型錄或是彩盒上的作業溫度。
- 產品沒有斷電裝置或者採用電源線的插頭視為斷電裝置的一部分,以下警語將適用:
  - 對永久連接之設備, 在設備外部須安裝可觸及之斷電裝置;
  - 對插接式之設備, 插座必須接近安裝之地點而且是易於觸及的。

#### About the Symbols

Various symbols are used in this product to ensure correct usage, to prevent danger to the user and others, and to prevent property damage. The meaning of these symbols are described below. It is important that you read these descriptions thoroughly and fully understand the contents.

#### Explanation of the Symbols

SYMBOL	EXPLANATION	
	Alternating current (AC):	
$\sim$	AC is an electric current in which the flow of electric charge periodically reverses direction.	
	Direct current (DC):	
	DC if the unidirectional flow or movement of electric charge carriers.	
$\frown$	Earth; ground:	
	A wiring terminal intended for connection of a Protective Earthing Conductor.	
	Class II equipment:	
	The method of protection against electric shock in the case of class II equipment is either double insulation or reinforced insulation.	

#### Viewing Certifications

Go to http://www.zyxel.com to view this product's documentation and certifications.

#### **Zyxel Limited Warranty**

Zyxel warrants to the original end user (purchaser) that this product is free from any defects in material or workmanship for a specific period (the Warranty Period) from the date of purchase. The Warranty Period varies by region. Check with your vendor and/or the authorized Zyxel local distributor for details about the Warranty Period of this product. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials. Zyxel will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product of equal or higher value, and will be solely at the discretion of Zyxel. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

#### Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. Zyxel shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at http://www.zyxel.com/web/support\_warranty\_info.php.

#### Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

#### **Open Source Licenses**

This product contains in part some free software distributed under GPL license terms and/or GPL like licenses. Open source licenses are provided with the firmware package. You can download the latest firmware at www.zyxel.com. To obtain the source code covered under those Licenses, please contact support@zyxel.com.tw to get it.

# Index

# A

Address Assignment 38 AP 10 AP Mode menu 23 AP+Bridge 10

# В

Bridge/Repeater 10

# С

certifications 161 viewing 163 Channel 20 channel 54 Configuration restore 103 contact information 151 copyright 157 CoS 84 CoS technologies 76 CPU usage 20 customer support 151

# D

DDNS service providers 95 DHCP 35 DHCP server see also Dynamic Host Configuration Protocol DHCP server 71 Differentiated Services, see DiffServ 84 DiffServ 84 marking rule 84 disclaimer 157 DNS Server 38 Domain Name System. See DNS. DS field 84 DS, dee differentiated services DSCP 84 DynDNS 95 DynDNS see also DDNS 95

# Ε

```
encryption 55
and local (user) database 56
key 56
WPA compatible 56
ESSID 110
```

# F

Firewall guidelines 93 ICMP packets 95 firewall stateful inspection 92 Firmware upload 101 file extension using HTTP firmware version 19

# G

General wireless LAN screen 57 Guest WLAN 56 Guest WLAN Bandwidth 56

#### 164

# I

IGMP 39 see also Internet Group Multicast Protocol version IGMP version 39 Internet Group Multicast Protocol 39 IP Address 71

# L

LAN 70 LAN overview 70 LAN setup 70 Language 104 Link type 20 local (user) database 55 and encryption 56 Local Area Network 70

# Μ

MAC 64 MAC address 38, 54 cloning 38 MAC address filter 54 MAC address filtering 64 MAC filter 64 managing the device good habits 11 using the web configurator. See web configurator. using the WPS. See WPS. MBSSID 10 Media access control 64 Memory usage 20 mode 10 Multicast 39 IGMP 39

# Ν

NAT Traversal 77 Navigation Panel 21 navigation panel 21

# 0

operating mode 10

# Ρ

Per-Hop Behavior, see PHB 84 PHB 84 Point-to-Point Protocol over Ethernet 40 port speed 21 PPPoE 40 dial-up connection push button 14

# Q

QoS 75, 84 marking 76 setup 75 tagging 76 versus CoS 76 Quality of Service, see QoS

# R

RADIUS server 55 Reset button 14 Reset the device 14 Restore configuration 103 Roaming 65 Router Mode status screen 18 RTS/CTS Threshold 54, 65

# S

Scheduling 68 Service Set 58, 63 Service Set IDentification 58, 63 Service Set IDentity. See SSID. Single Rate Three Color Marker, see srTCM srTCM 86 SSID 20, 54, 58, 63 stateful inspection firewall 92 Status 18 Subnet Mask 71 Summary DHCP table 35 System General Setup 98 System restart 104

# Т

Time setting **100** trTCM **86** Two Rate Three Color Marker, see trTCM

# U

Universal Plug and Play Application 77 Security issues 77 user authentication 55 local (user) database 55 RADIUS server 55

# V

VPN Passthrough 49

### W

WAN (Wide Area Network) 37

WAN MAC address 38 warranty 163 note 163 Web Configurator how to access 16 Overview 16 web configurator 11 WEP Encryption 61 wireless channel 110 wireless LAN 110 WPS push button 14 wireless LAN scheduling 68 Wireless network basic guidelines 54 channel 54 encryption 55 example 53 MAC address filter 54 overview 53 security 54 SSID 54 Wireless security 54 overview 54 type 54 wireless security 110 Wireless tutorial 24 WPA compatible 56 WPS 11 push button 14