Gemtek systems

P380

Wi-Fi Inter-Building Router

User's Guide

. Wireless Broadband Anywhere. Wireless Broadband Anywhere. Wireless Broadband Anywhere.

Contents

Overview

The AP router, P380, is a standalone wireless client, which provides IP routing functionality between a Local Area Network (LAN) and a Wide Area Network (WAN). It uses an Ethernet interface to connect to LAN, and wireless 802.11b-based interface to connect to a Wireless Networking System, which provides miscellaneous WAN access.

Wireless Networking System

P380 is part of the Wireless Internet Service Provision System. It provides access for locally connected computers to WAN, such as the Internet. In Figure 1 shown below, P380 client devices are connected to P380 access points (please refer to P380 specification).

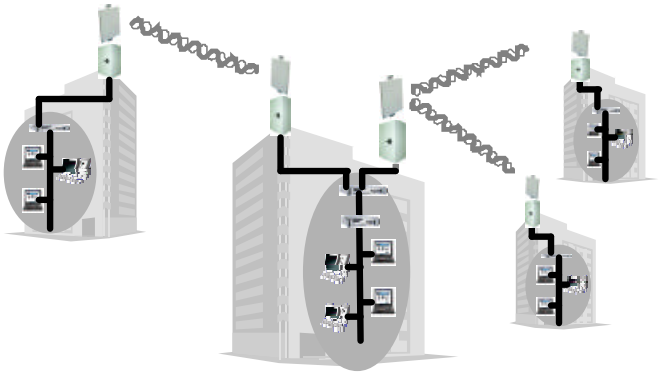


Figure 1: P380 Solution

Features

P380 is based on indoor architecture. An indoor unit with 2.4 GHz antennas is placed on the mast or the ceiling of the construction elements. It is connected to a UTP cable. An individual computer or an entire local network can gain access to the Internet by simply connecting the P380 indoor unit to the switch/hub. P380 is a full featured IP router with extensive firewall capabilities and a user-friendly web interface.

Features:

- Wireless Access Point or Client (configurable)
- Router/Bridge (configurable) and Firewall
- Telecom features Built-in
- Web management Interface

P380 can be managed via:

- FTP
- Telnet
- WWW
- SNMP (v1, v2)

It is possible to modify the following information through a web interface:

- General information
- Network LAN and WAN interfaces settings
- Wireless device settings
- DHCP server configuration
- IP Firewall
- Port forwarding
- Static routing

3 Operating Modes

The P380 Router supports 3 different kind of operating modes: AP-Router, AP and Bridge.

AP-Router Mode

In this mode, the P380 wireless unit plays the roles of the wireless network Access point and a router.

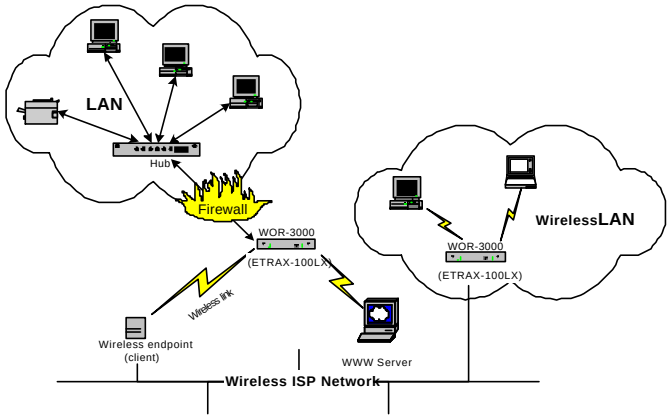


Figure 2: AP-Router mode

AP Mode

In this mode, P380 acts as conventional wireless Access point. The routing function is disabled. Local Network Area is automatically set up to Wireless.

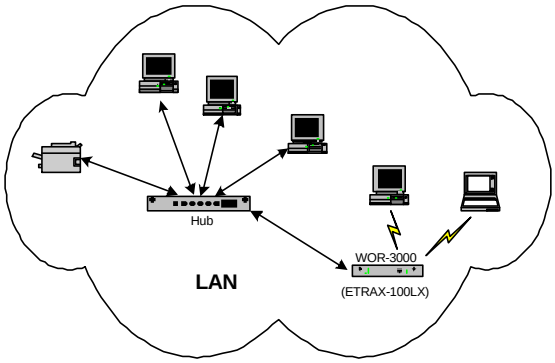


Figure 3: AP mode

Bridge Mode

When operating in this mode, one P380 device can connect with another P380 device and form wireless "bridge" interconnecting two or more local networks. Note that all these devices must work in the same frequency channel and must have the same SSID string. Please also note that wireless "bridge" DOES NOT retransmits packets.

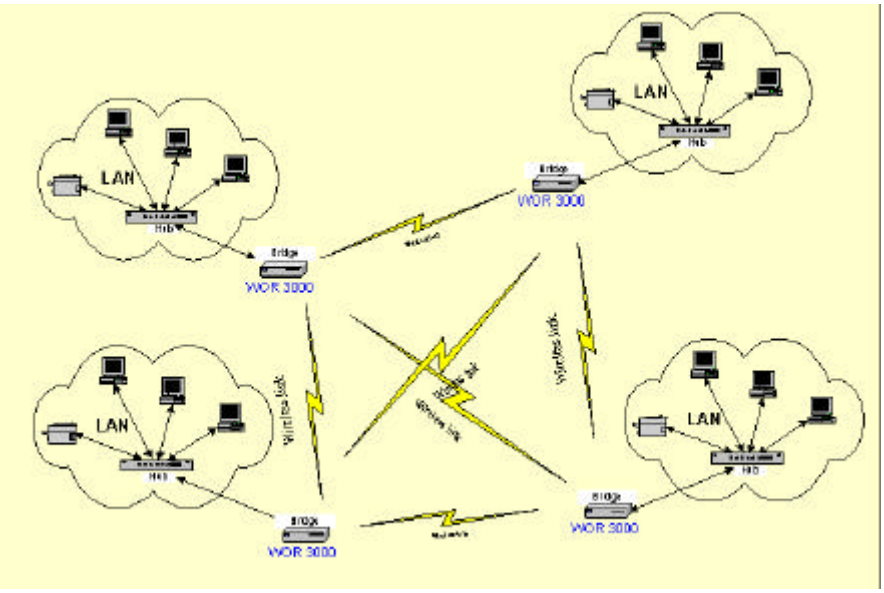


Figure 4: Bridge mode

Starting Up

To setup P380 for the first time can be performed through a web browser on a computer connected to the local network. The administrator can use one of standard browsers available (e.g., Netscape Navigator, or Microsoft Internet Explorer versions 4.0 or later). Once the setup process is completed, P380 can be managed from any computer on the network that has a web browser.

The steps to setup P380 using a web browser are listed below:

1. Launch a standard web browser on a computer connected to the network.
2. Enter the P380 IP address given to you from the ISP into the URL field of your web browser (the default setting is 192.168.2.2). P380 device provides SSL (Secure Sockets Layer) feature, so use https://192.168.2.2 to connect.

If local network settings were configured correctly, then a login screen should appear:

Input the username (the default username is "*root*") and correct password (the default password is "*pass*") and click the "***OK***" button to pass the security control screen. Once the correct username and password combination is entered, a P380 welcome screen should appear as below:

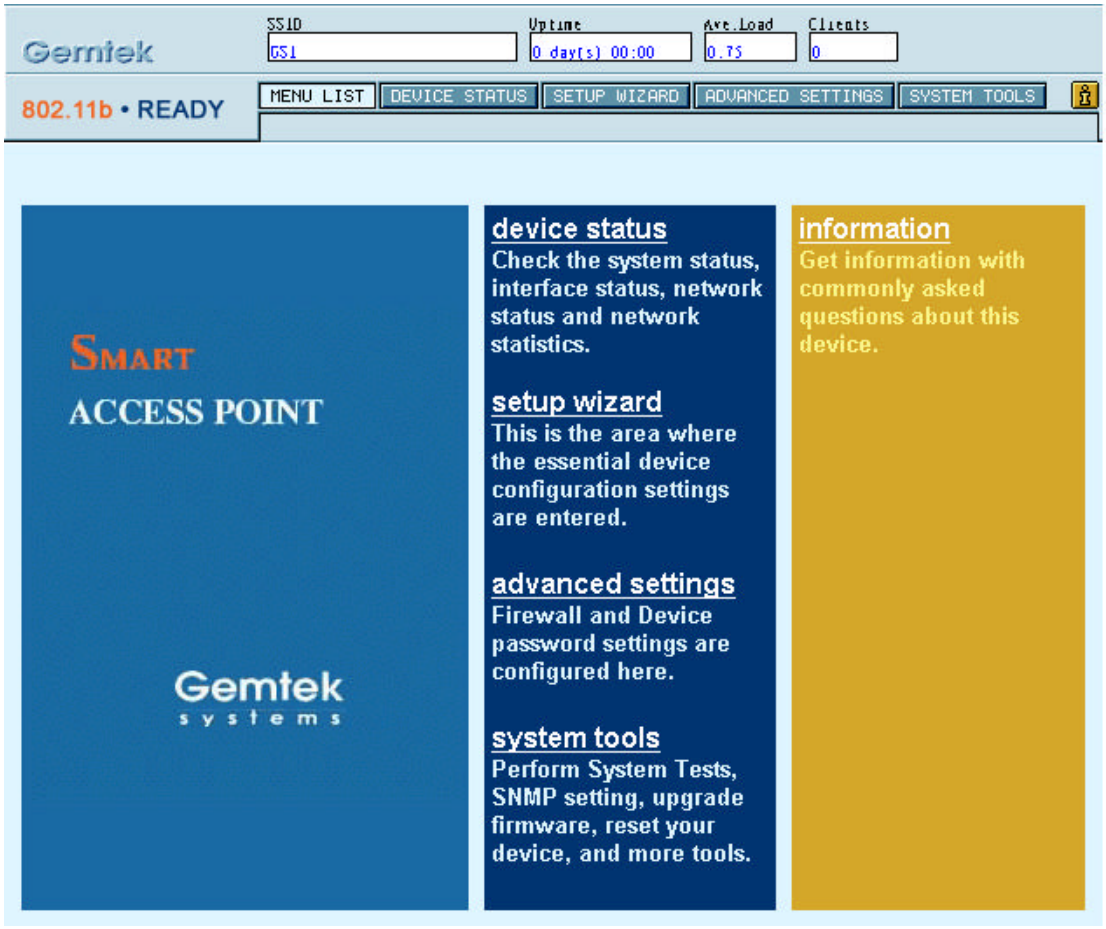
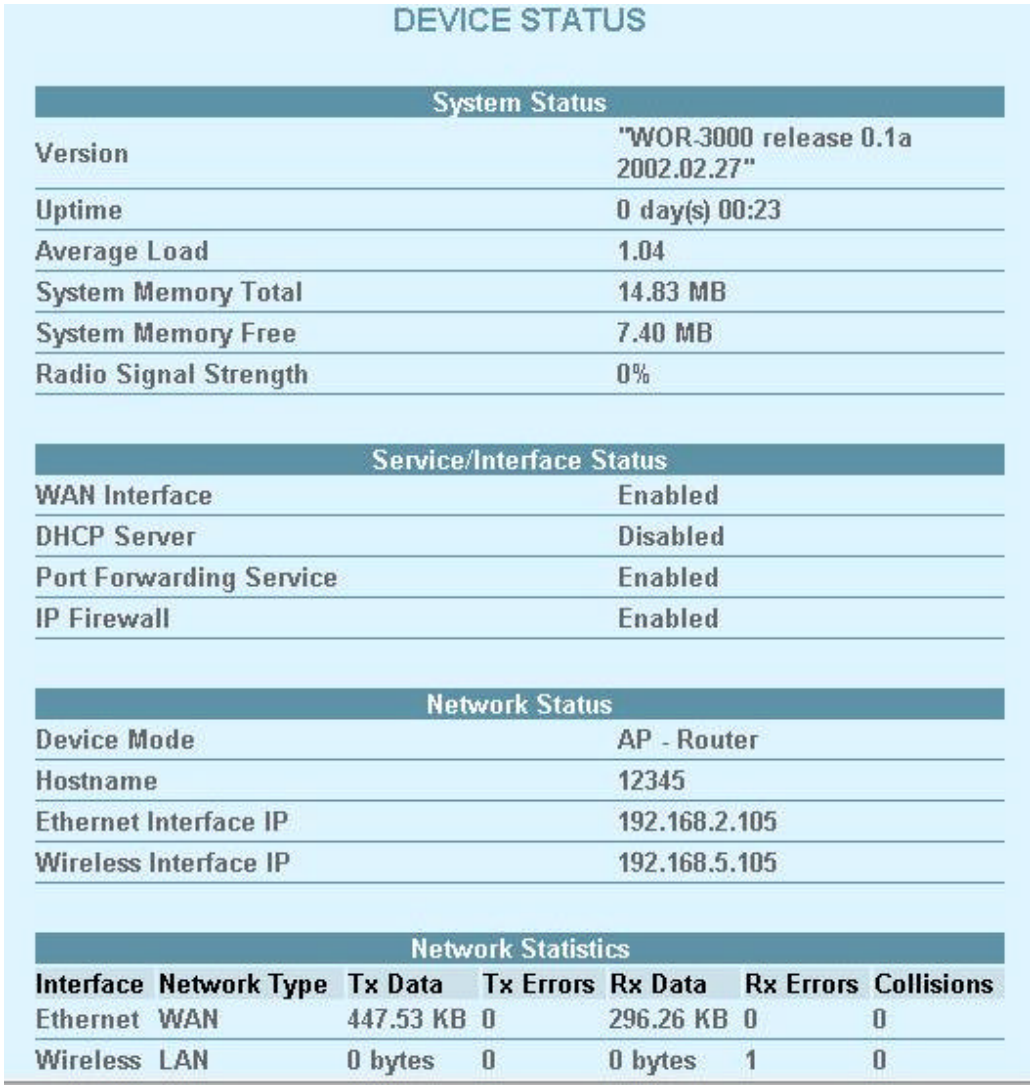


Figure 5: Welcome screen

Click on the "***Setup Wizard***" button on the menu bar to begin P380 device configuration (described in the following section).

Device Status page

Device status page displays all information includes system, interface and network status.



DEVICE STATUS

System Status	
Version	"WOR-3000 release 0.1a 2002.02.27"
Uptime	0 day(s) 00:23
Average Load	1.04
System Memory Total	14.83 MB
System Memory Free	7.40 MB
Radio Signal Strength	0%

Service/Interface Status	
WAN Interface	Enabled
DHCP Server	Disabled
Port Forwarding Service	Enabled
IP Firewall	Enabled

Network Status	
Device Mode	AP - Router
Hostname	12345
Ethernet Interface IP	192.168.2.105
Wireless Interface IP	192.168.5.105

Network Statistics

Interface	Network Type	Tx Data	Tx Errors	Rx Data	Rx Errors	Collisions
Ethernet	WAN	447.53 KB	0	296.26 KB	0	0
Wireless	LAN	0 bytes	0	0 bytes	1	0

Figure 6: Device Status table

The Device Status page is divided into to four parts:

System Status table - This table shows P380 software version, system uptime (after last reboot), average load, memory usage and radio signal strength (RSSI).

System service and interfaces status is shown in "**Service/Interface Status**" table - This table shows wireless interface and system services state. Possible values in this table can be Enabled/Disabled for appropriate interface/service state.

Network status is shown in the "**Network Status**" table - This table shows operating mode of the device, which can be "Router" for AP-Router mode, "AP" – for access point mode and "Bridge" for bridge mode.

Network statistics are shown in separate table - This table contains statistics for both interfaces of the P380 – wired and wireless. The wired interface is called LAN, and the wireless interface is called WLAN. Each column corresponds to the statistics value of the interfaces:

TxData – amount of data transferred
TxErrors – amount of transmit errors
RxData – amount of data received
RxErrors – amount of receive errors
Collisions – amount of network collisions

Setup Wizard

Operation Mode Settings Page

The first page of the P380 configuration wizard is dedicated to the device operating mode selection:

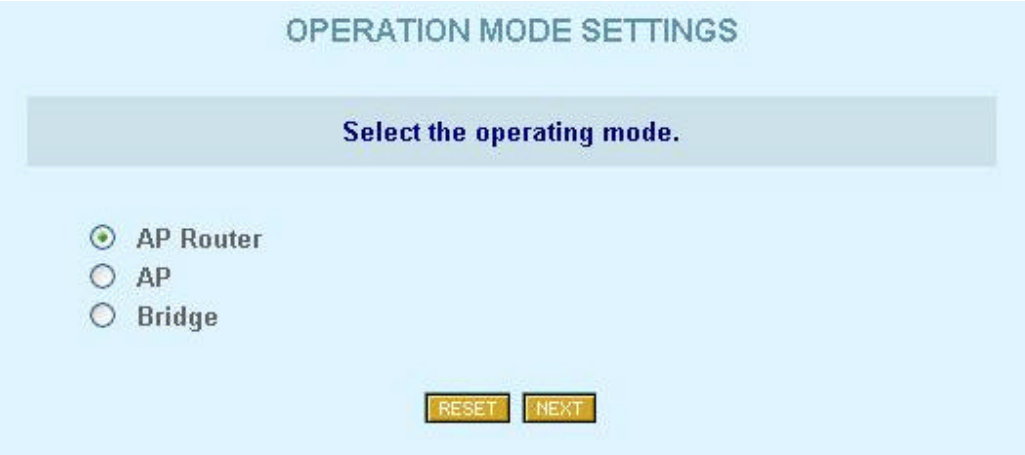


Figure 7: Device Mode Settings page

This enables a user to select the operating mode of the device.

Click on the "***Reset***" button to reset the page fields to their default values. Select one of the three device modes and click on the "***Next***" button to continue the configuration wizard (For a detailed explanation of the wizard settings, please refer to the P380 Quick Installation Guide).

General Configuration Settings Page

Various general device parameters can be set in this page. All of those parameters are optional.

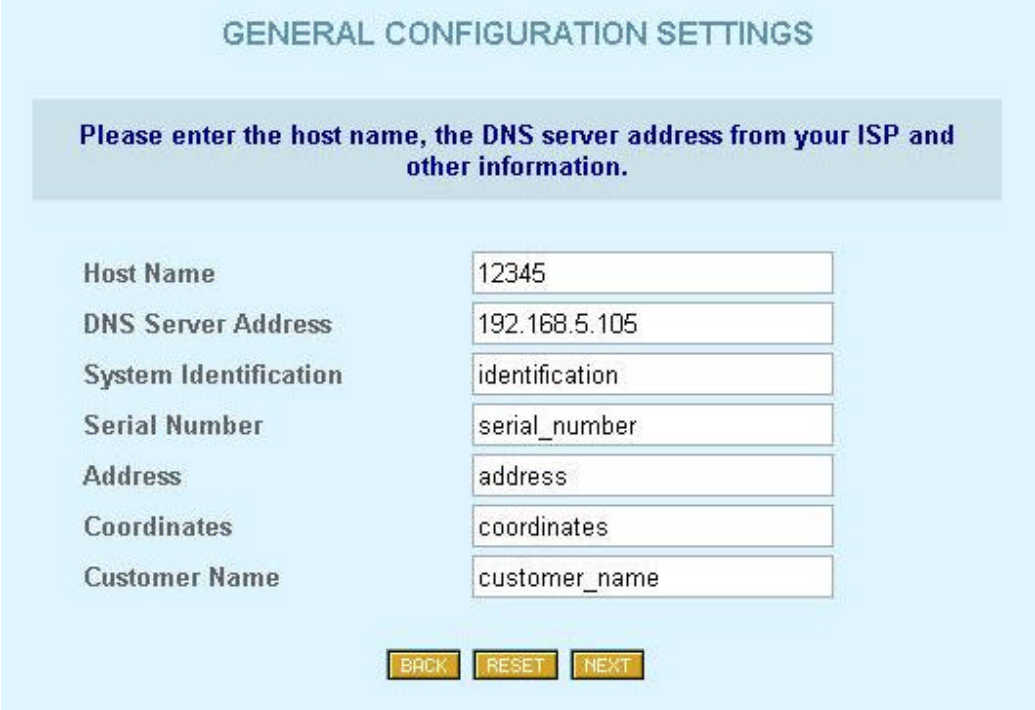


Figure 8: General Configuration Settings page

These parameters include:

Hostname – a general network parameter returned in statistics routines
DNS Server address – this Domain Name Server address is assigned to the PCs requesting DNS address through DHCP (Dynamic Host Configuration Protocol).
System Identification – free form system identification code for easier device identification by the service staff.
Serial Number – A unique serial number of the P380 device. Users should not change this number.
Address – The location of the device.
Coordinates – GPS coordinates. Service staff fills this field when deploying device.
Customer Name – customer name, which is used for easy identification of P380

Click on the "***Back***" button to go to the previous page, Operating Mode Settings. Click on the "***Reset***" button to reset all page fields to their previous values and click on the "***Next***" button to continue the configuration wizard.

Network Configuration Settings page

❖ **Router Mode**

In Router mode, LAN (Local Area Network) and WAN (Wide Area Network – For P380, this can be the enterprise networks on the Internet) configurations can be modified using the LAN Settings and the WAN Settings tables shown as followed:

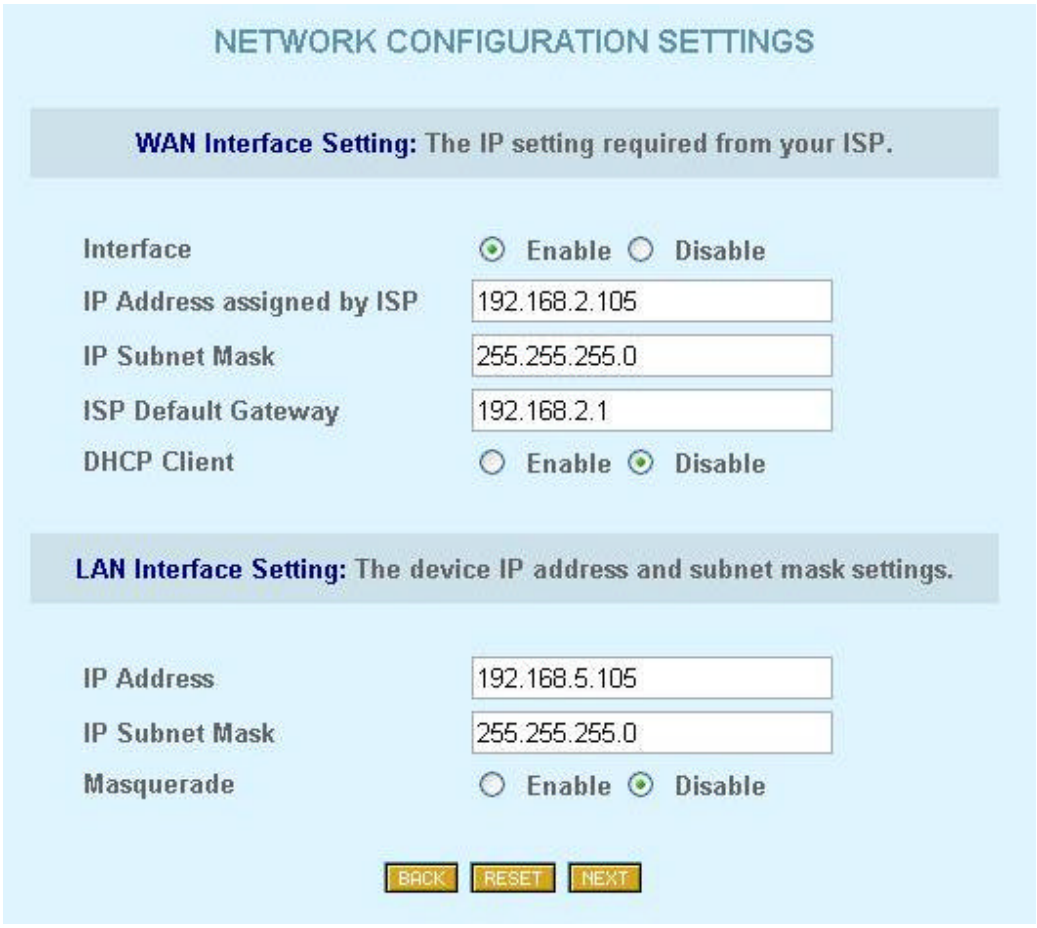


Figure 9: Network Configuration Settings page -1 (Router mode)

WAN settings must be set up according to the information provided by the ISP. There is no such restriction on LAN settings. WAN access can be disabled to restrict LAN users access to this network.

The masquerade setting enables the users to use the NAT (Network Address Translation) feature of P380. When this option is enabled, P380 "hides" LAN addresses to the "external world". Access to the services, such as web services, provided by servers in the LAN, can be achieved by using the port forwarding feature.

ⓘ **Hint:** *Use known private IP addresses for the local network, because if you use public addresses, you will not be able to connect to WAN. It is recommended to use IANA (Internet Assigned Numbers Authority) reserved private address space (10.0.0.0/8, 172.16.0.0/12 and 192.168.0.0/16) .*

❖ **AP Mode**

In AP and Bridge mode, P380 does not require an active LAN (Local Area Network) interface, so the "LAN Interface Settings" table is not displayed.

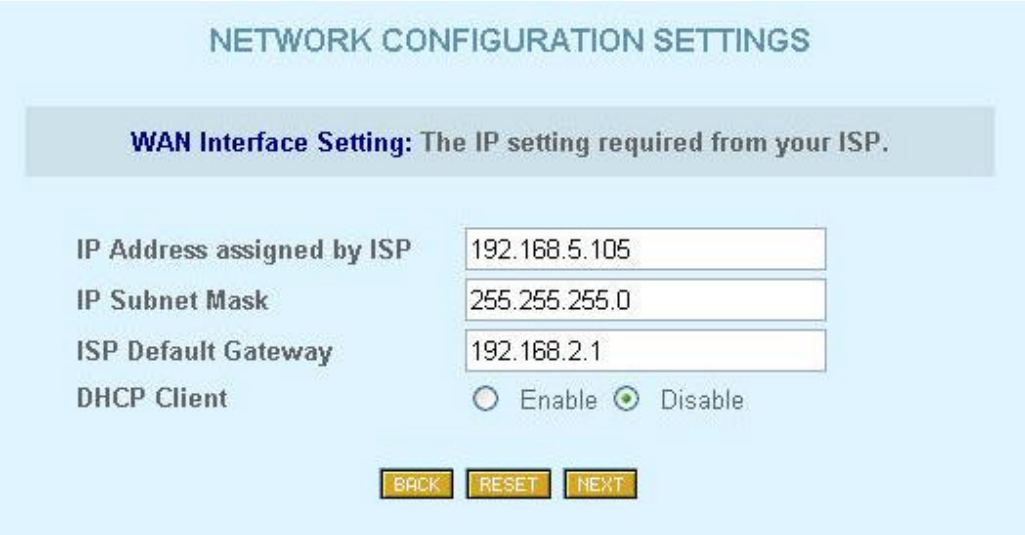


Figure 10: Network Configuration Settings page -2 (non-Router mode)

Click on the "***Back***" button to go back to the previous page, which is General Configuration Settings. Click on the "***Reset***" button to reset all current page fields to their previous values and click on the "***Next***" button to continue wizard.

Wireless Configuration Settings page

Wireless device is configured as shown below:

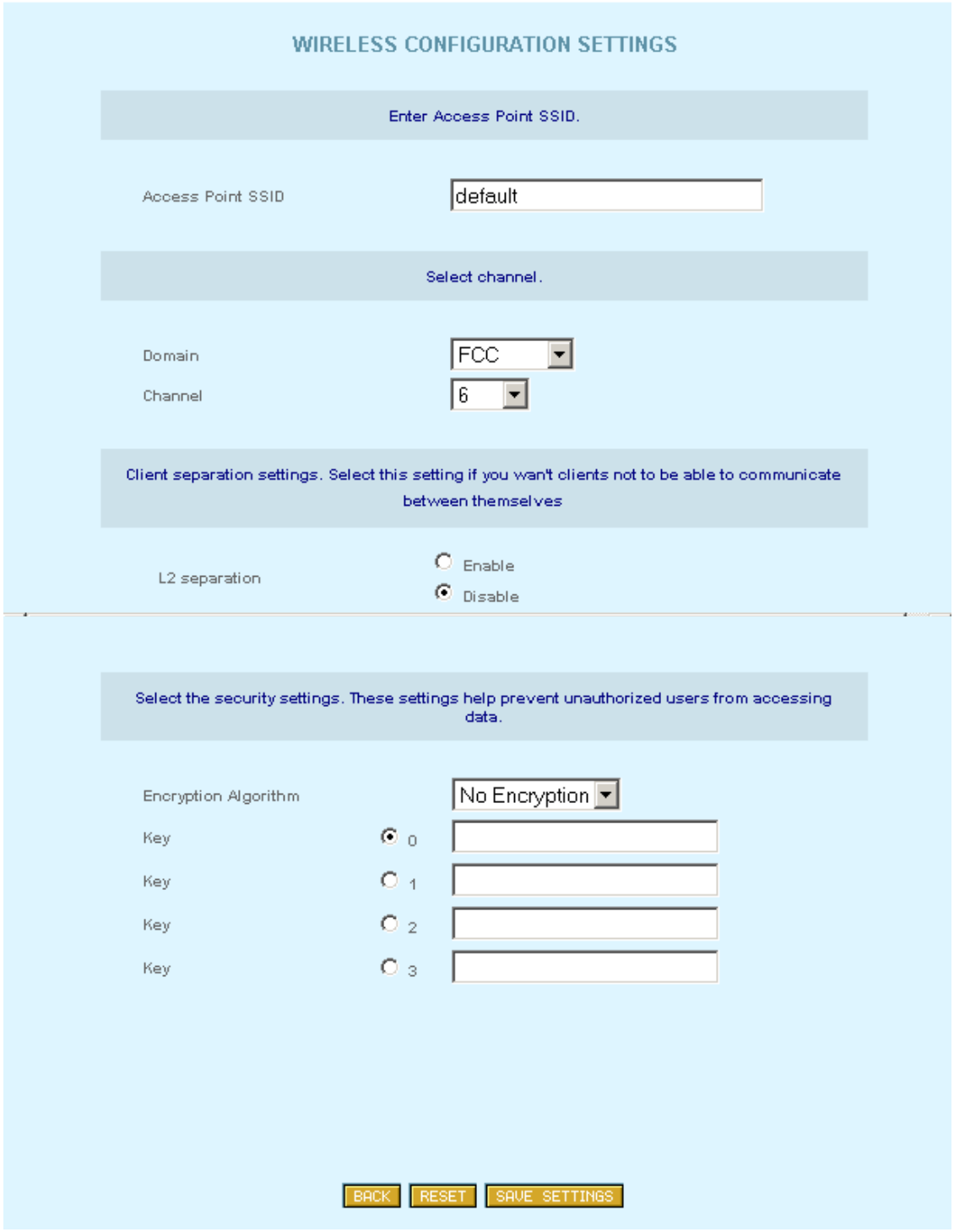


Figure 11: Wireless Configuration Settings page

At lease two essential parameters are required to setup:

- **Access Point SSID** (Service Set Identifier): This is a case-sensitive parameter to uniquely identify your radio network.

- **Default Channel for BSS**: It can be set up by selecting a fixed channel or have the channel automatically assigned.

ⓘ **Hint:** *Use the site survey utility in System Tools to verify a fixed channel selection. This utility will help the administrator to discover unused channels, or to check the signal strengths of other Access points of the selected channel.*

In Bridge mode, there is a column field called "Access Point ID". This value should be assigned with different for all bridges connected to the same LAN as a bridge ID. The value itself has no meaning if it's less or greater than other's bridge ID. It can be from 0 to 255. For example, it could be assigned value "20" to the first bridge and "25" to the second.

You may desire additional security on your wireless network, which can be achieved by using WEP (Wired Equivalent Privacy) encryption. P380 offers 64/128 bit WEP securities on wireless transmissions. Encryption keys are combined by 5 (for 64 bit WEP) or 13 (for 128 bit WEP) pairs of hexadecimal digit and separated by colon (e.g., 01:23:45:67:89 for 64 bit WEP encryption keys). WEP encrypts each frame transmitted from the radio using one of the keys from this table.

When an encrypted frame is received, it will only be accepted if it is decrypted correctly, therefore the receiver must have the same WEP key used by the transmitter. Each key must consist of hex digits, which is composed of digits 0-9 and letters A-F.

ⓘ **Hint:** *Network traffic encryption requires a significant amount of resources, so its usage is recommended only when security is crucial. Usually it is not used in simple commercial networks transmitting everyday data. Also usually is more efficient to protect sensitive documents before transmitting over network e.g., use archive program with password protection, than encrypt all network traffic.*

Click on the "***Back***" button to return to the previous page, the Network Configuration Settings page. Click on the "***Reset***" button to reset all page fields to their previous values. Click on the "***Save settings***" to save and to close the configuring window.

Redirection Service

If a new IP was assigned and the "***Save Settings***" button was click to save the network setting, a waiting and redirection message pops up as shown below:

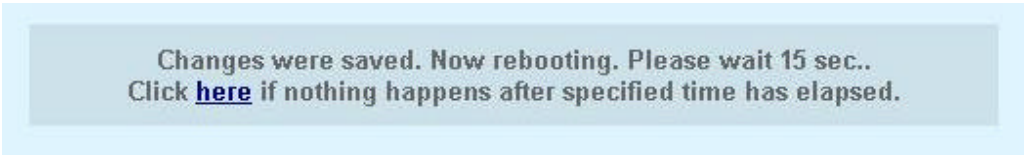


Figure 12: Waiting and redirection message

It indicates that the browser will be redirected to a new site (new IP). If the new site is in a different subnet from the old one (e.g., from 192.168.2.218/24 to 168.20.1.10/24), the redirection function will not work. The IP of the local connected computer must change to the same subnet of the new site (168.20.1.x/24) first. And then re-click the redirection message above or re-enter the new IP of P380 into URL field of browser, to reconnect to the site.

If the new site is in the same subnet as the old site (e.g., from 192.168.2.218 to 192.168.2.100), and the redirection function did not redirect to new site automatically, please re-click the redirection message or refresh button in the browser.

Advanced Settings

Setting up advanced P380 settings requires some advanced knowledge of the TCP/IP network structure and functionalities. It is recommended that only skilled network administrators should use these settings.

Firewall configuration

IP firewall configuration page provides user firewall services control. User can add, modify or delete customized firewall rules. Main firewall page view is shown as followed:

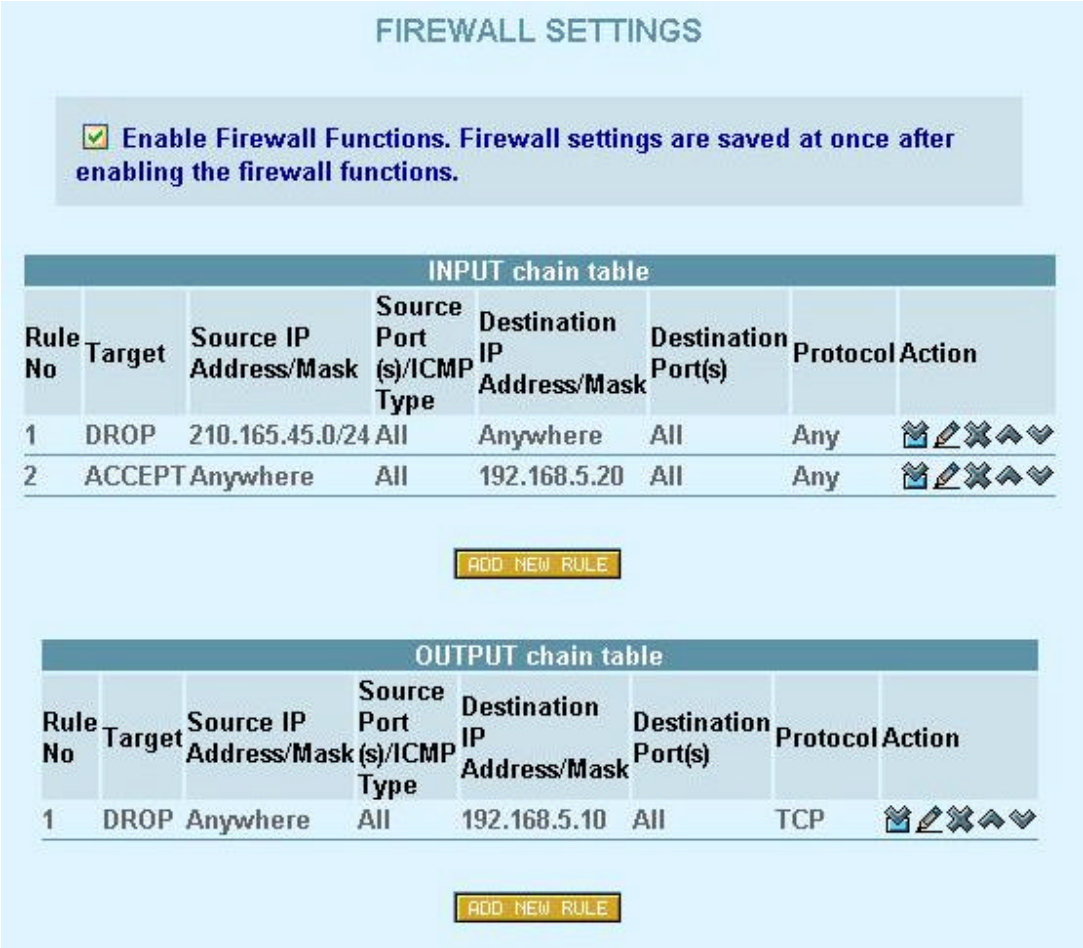


Figure 13: IP Firewall Settings page

Note: *In AP and Bridge mode P380 has no active LAN (Local Area Network) interface, so the "Firewall configuration" page is not displayed*

This page shows service state and firewall rules list. Rules are divided in two parts – Input rules, which apply to the incoming packets, and the Output rules, which apply to the outgoing packets. User can change these rule lists by editing existing rules, deleting unnecessary ones, and adding new rules. Modification and addition of the rules is shown below:

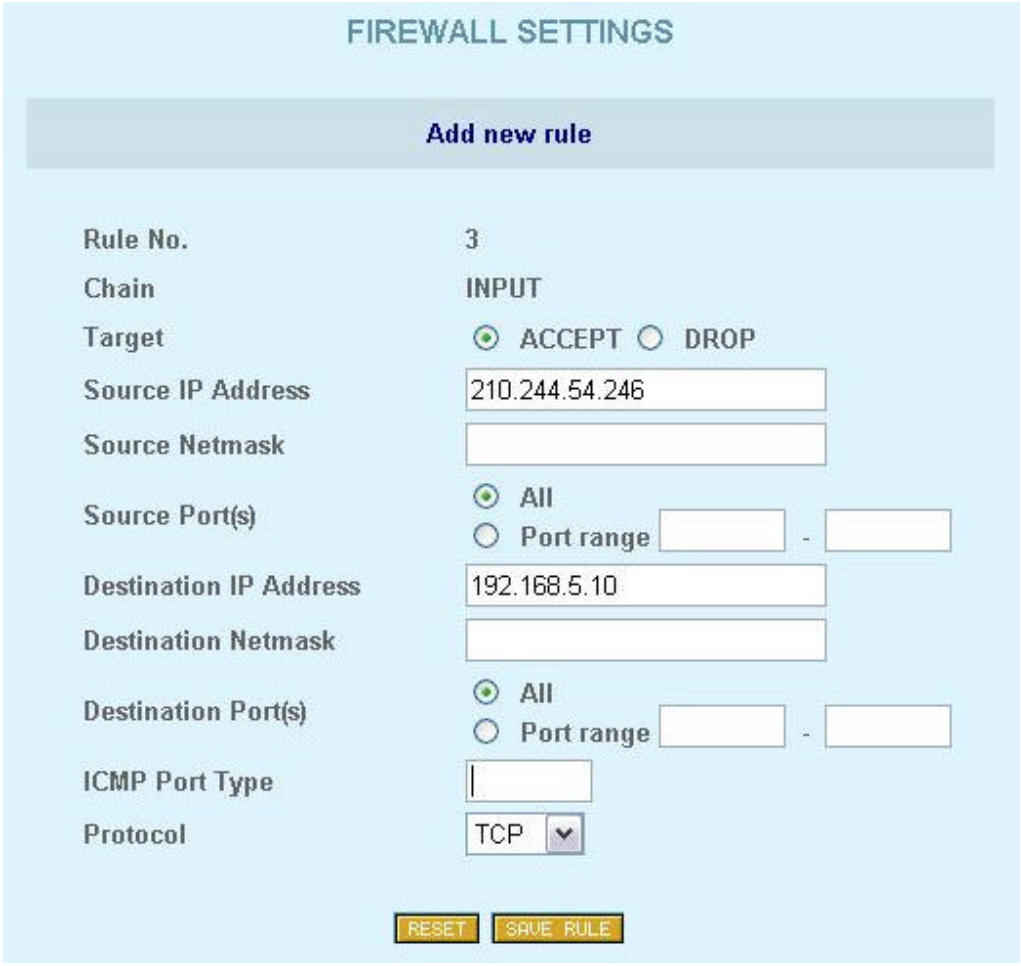


Figure 14: Firewall rule edit

The main firewall rule parameters are:

Target – this implementation of firewall control supports only two types of rules – *ACCEPT* and *DROP*. The appropriate policy defines what to do if packet matches rule.

Source IP Address – source IP address, can be specified as ***any***

Source Netmask – source subnet, can be specified as ***any***

Source port(s) – can be specified in two ways: **All** or a given port range

Destination IP Address – specified the same as Source IP

Destination Netmask – specified the same as Source Netmask

Destination port(s) – specified the same as Source port

Network protocol – network protocol which the rule affects. Can be specified as one of ***TCP/UDP/ICMP*** or ***any***

ⓘ **Hint:** *If an exact port is specified, use of "any" protocol setting makes no sense (different protocols use their own port ranges). Use exact protocol, or use several rules to specify traffic filtering on required ports.*

Note: When defining rules, avoid DENY type rules using "any" as the address class, which can cause loss of web management connection (e.g., deny traffic from any to any IP address). In such case, only connection via serial console, manually disabling the firewall or hardware reset the device to factory default to disable the firewall setting, can rectify this problem.

ACL Configuring

All clients MAC are set by acceptable as default in Access Control List function. To deny the MAC address, just click "Add New Rule" button to add the new record. Access Control List setting is shown below:

Figure 15: ACL Settings page

Static routing configuration

Static routing service lets user specify static routes, which is present in system routing table form system startup. This service is needed, when local computers are divided into different subnets, using external router, etc. Static routing page is shown as followed:

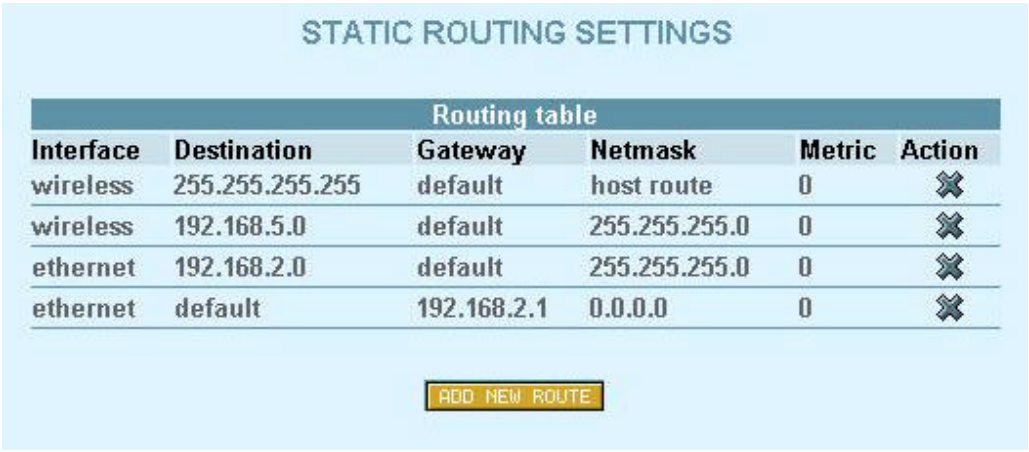


Figure 16: Static Routing Settings page

ⓘ **Hint:** *above figure shows default system routes, which are added automatically, and restored after any network configuration. However these routes can be edited for temporary needs.*

This page provides a user static route list (present on the system), and ability to edit, delete and add routes. Rule editing and adding is done in the following page:

Note: *In AP and Bridge mode P380 has no active LAN (Local Area Network) interface, so the "Static Routes" page is not displayed*

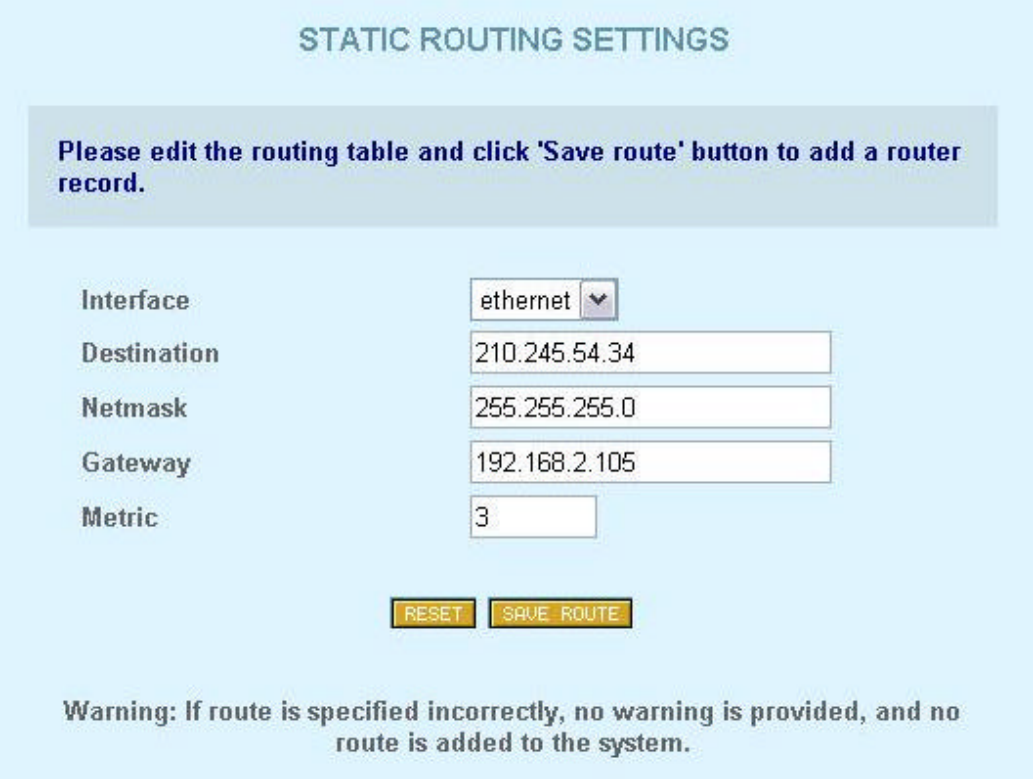


Figure 17: Route editing table

Each rule in the route list consists of Device (interface) selection (can be wireless or Ethernet), Destination address (depending on netmask, can be a host or subnet), Gateway address (if not specified, program uses default interface gateway), Metric (route priority), and Netmask. If netmask is specified as 255.255.255.255, then routing program assumes that it is the "host" route type; otherwise route specifies "net". Note that routes are automatically enabled when the "**Save Route**" button is pressed. If a rule is specified incorrectly, no warning is provided, but rule is not added to the system. Only skilled network administrator with in-depth knowledge of the network topology should use the static routing feature.

DHCP Service Configuration

The Dynamic Host Configuration Protocol (DHCP) provides IP configuration parameters to hosts in a client-server model. DHCP servers assign network addresses and deliver the configuration parameters to other (client) hosts.

DHCP server feature is offered only in AP Router mode. This server set up is done in the DHCP Settings table, which is shown below.

Figure 18: DHCP Server Settings page

DHCP server service can be enabled or disabled from this page. Service state is altered, and new configuration is loaded after ***"Save Settings"*** button is clicked. The IP Address range entered must be in the same subnet the LAN interface of P380.

ⓘ **Hint:** *Remember to set up local computers as DHCP client, when the DHCP server is enabled. If the server detects that some computers already have addresses from the defined range, the address is not given to the computers.*

Note: *In AP and Bridge mode P380 has no active LAN (Local Area Network) interface, so "DHCP Settings" page is not displayed.*

Click on the "***Reset***" button to reset all page fields to their previous values and click on the "***Save Settings***" button to save the DHCP server setting.

Port forwarding configuration

Port forwarding service provides access to locally connected computers with dedicated services by overriding the firewall' s NAT (Network Address Translation) feature. Example of such services can be chat programs, online games, etc. Port forwarding

administrator can define local computer, to which data from specified ports of firewall are automatically redirected to ports of this local computer. Port Forwarding Settings page is shown below:

Figure 19: Port Forwarding Settings table

Note: *In AP and Bridge mode P380 has no active LAN (Local Area Network) interface, so the "Port Forwarding Settings" page is not displayed*

From this page, administrator can modify port forwarding rule list by adding new, delete and edit existing rules. Also the service can be enabled or disabled from this page. When editing existing rule, or adding new one – the following page is displayed:

Figure 20: Port Forwarding Rule editing table

As shown in Figure 20, a port forwarding rule consists of protocol specification – UDP or TCP protocol, port on the P380 needed for application, the local IP address and port to which arriving data will be redirected.

ⓘ **Hint:** *Sometimes games, chat programs and other applications may need to change their network settings to something like "Use Firewall" or "Use proxy" to work properly. This setting may and sometimes should be used with Port Forwarding service. When remote server desires to define IP address to communicate, you should specify not your local IP address, but IP address of P380.*

Setting up administrator password

Administrator password is a key used to access P380 configuration functions in administrator security required login screen (please refer section "**Starting Up"**). It will be requested when setting up or maintaining P380. This password is set up in the Administrator Settings table shown in following:

Figure 21: Administrator Settings table

To change the password, you must enter the current password in "Old Password" field, then enter a new password in the "New Password" field. Re-enter the same value in the "Retype New Password" field. Use hard-to-guess password, i.e. more than five characters, containing both letters and numbers, and is not a dictionary word. Be sure to remember this password (or write it down at a safe location) to access the P380 management administration features in the future. Default factory password setting is "pass" (password is case-sensitive). This password should be changed frequently to prevent unauthorized user access to P380.

Click on the "***Reset***" button to reset all page fields to their previous values and click on the "***Save Settings***" button to save the administrator settings.

System Tools

Clients page

Connected Clients page shows connected wireless clients list (AP and AP-Router modes only). This list is shown in the form of a table:

Figure 22: Connected Clients page

In the "**Client MAC address**" column, connected wireless card MAC (hardware) addresses are shown.
Signal and **Noise** columns show radio signal and noise levels.
The column, "**Rate**", shows connection bit rate (connection speed) in hundreds of kilobits. This rate can be easily converted in to megabits by dividing this number by 10. For example 110 corresponds to 11Mbits, 55 correspond to 5.5Mbits and so on.

Loopback Test

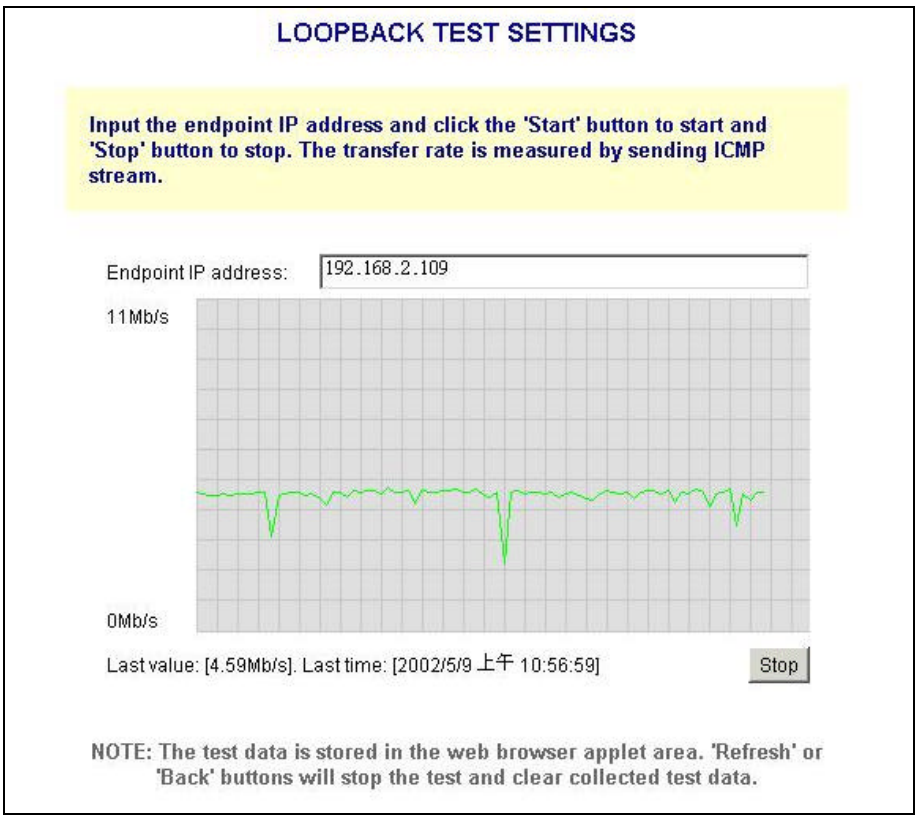


Figure 23: Loopback Test page

Loopback test is used for wireless link diagnostics. This page shows data transfer rate between P380 and endpoint device (PC running endpoint program). This transfer rate is

measured by sending ICMP (Internet diagnostics protocol) stream to the end point device. Data is refreshed every second.

To start loopback testing, enter endpoint IP address in the "**Endpoint IP address**" field and click on the "***Start***" button in the lower right corner of the page. Status line will show last measured data transfer rate, and the time when this data was received from the endpoint. To stop loopback-testing, click on the "***Stop***" button.

Note: *Due to the nature of this test, test data is stored in the web browser applet area. Clicking the "**Refresh**" or "**Back**" buttons when test is running will stop the test and clear the collected test data.*

Configuring SNMP management

SNMP (Simple Network Management Protocol) service is configured in the SNMP Settings page. This page is used for setting up read-only and read-write communities:

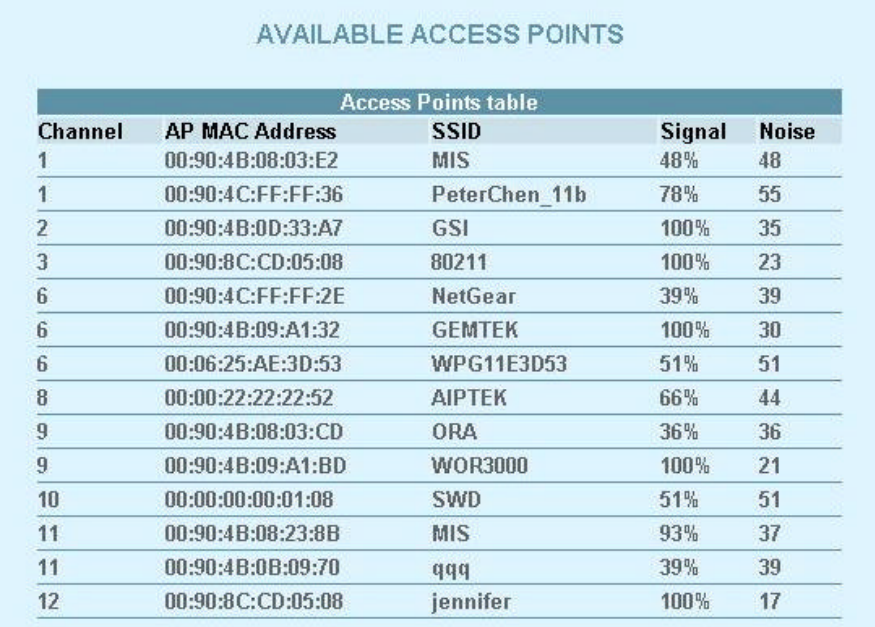
Figure 24: SNMP Settings

Community strings are used for SNMP authentication purposes. It is possible to allow or deny IP address groups from accessing P380 using SNMP. IP address and netmask combination 0.0.0.0/32 means "ANY" IP address. It could be setup by a specified IP, ex 192.168.2.100/32, or by a group, ex 192.168.2.0/24.

ⓘ **Hint:** *For security purposes, use only local IP addresses for Read/Write access*

Click on the "***Reset***" button to reset all page fields to their default values and click on the "***Save Settings***" button to save the SNMP setting.

Site survey page



AVAILABLE ACCESS POINTS

Access Points table

Channel	AP MAC Address	SSID	Signal	Noise
1	00:90:4B:08:03:E2	MIS	48%	48
1	00:90:4C:FF:FF:36	PeterChen_11b	78%	55
2	00:90:4B:0D:33:A7	GSI	100%	35
3	00:90:8C:CD:05:08	80211	100%	23
6	00:90:4C:FF:FF:2E	NetGear	39%	39
6	00:90:4B:09:A1:32	GEMTEK	100%	30
6	00:06:25:AE:3D:53	WPG11E3D53	51%	51
8	00:00:22:22:22:52	AIPTEK	66%	44
9	00:90:4B:08:03:CD	ORA	36%	36
9	00:90:4B:09:A1:BD	WOR3000	100%	21
10	00:00:00:00:01:08	SWD	51%	51
11	00:90:4B:08:23:8B	MIS	93%	37
11	00:90:4B:0B:09:70	qqq	39%	39
12	00:90:8C:CD:05:08	jennifer	100%	17

Figure 25: Site Survey Test Results page

Site survey test shows the load situation in the wireless network. Using this test, user can scan for active Access Points; check the operating channels and their respective signal/noise levels.

ⓘ **Hint:** *Because wireless card is scanning through all radio frequency channels, the page loading time is much longer when compared to the other P380 management pages. Use the rescan button to check signal/noise levels when deploying new Access Points in the existing wireless network.*

Monitoring page

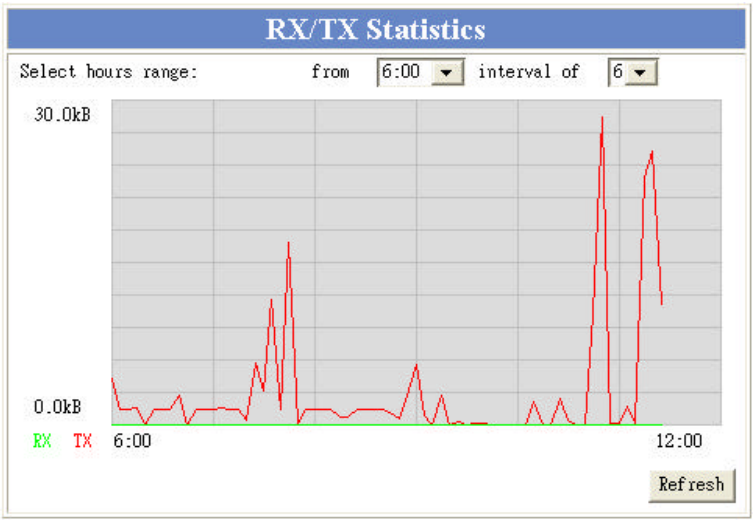


Figure 26: Monitoring page

The Monitoring menu shows TX/RX statistics graph. These statistics show a five-minute average traffic rate over the last 24 hours period. RX (green) indicates incoming (Received) traffic and TX (red) indicates outgoing (Transmitted) traffic.
The TX/RX monitoring is restarted on every P380 reboot. The reason is that P380 has no real time clock, and the time used is relative to P380 restart. The first statistics appear as 2 points after 5 minutes after P380. Normal view is acquired 10 minutes and later after P380 reboot. Click on the 'Show' button is needed when first time the TX/RX statistics applet appears in browser window. Next time click 'Refresh' button which appears instead of 'Show' button to get newer TX/RX statistics.
You can also manipulate on TX/RX graph time interval. There are two drop-down menus used for this purpose. The first one is used to choose the interval starting hour. It is possible to choose any hour from the last 24 hours, but choice can be limited to fewer hours because of P380 reboot. The second drop-down is used to choose time interval duration in hours. The possible choices are from 1 to 25 hours, but it also can be limited to fewer hours because of P380 reboot. Sometimes you can get 24 instead of 25 hours limit because relative time is even to hour range.

✎ **Note:** *On older firmware versions, only 'Refresh' or 'Show' buttons are available, but they have the same behaviour.*

Upgrade page

✎ **Important!** *When clicking on the "Upgrade button" in the main menu, a warning message box will pop up. Do not enter this page if there is no need to upgrade P380. Simply click on the "**Reset**" button, if no upgrade is necessary.*

Entering this page will put the device into UPGRADE mode. ***All of the device functions will be SUSPENDED****. Once the device enters the UPGRADE mode, it can only be upgraded or rebooted.*

ⓘ **Hint:** *Because upgrade is done using the WEB management screen, all management pages still work, so it is still possible to configure P380 before rebooting it.*

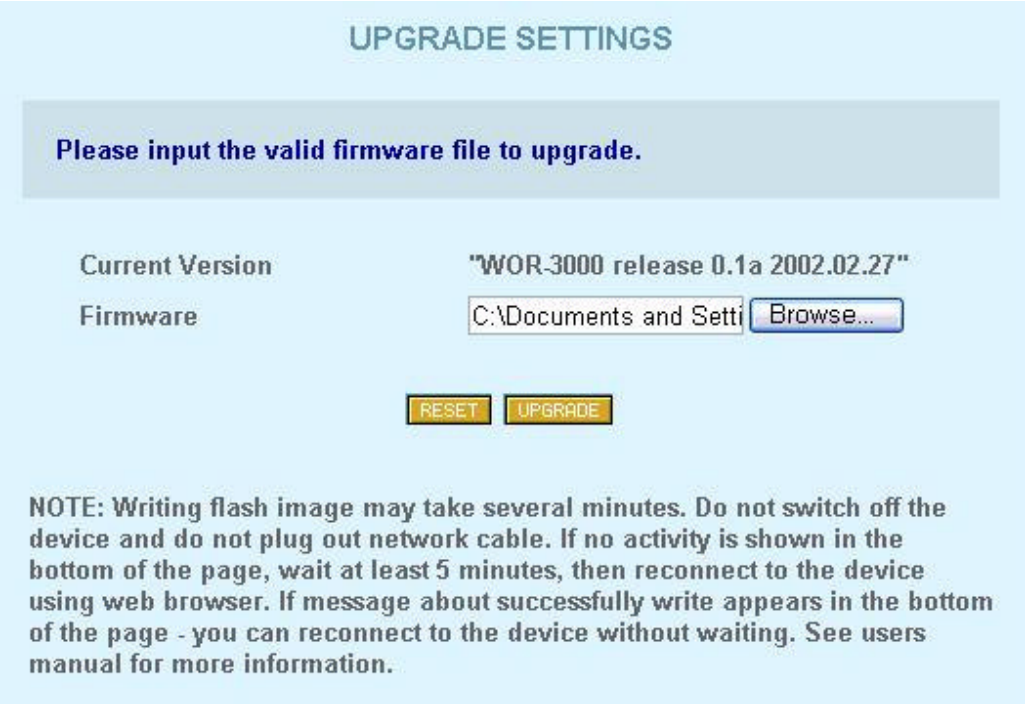


Figure 27: Upgrade page

P380 firmware is upgraded using the "***Upgrade***" page. In this page, the current firmware version is shown. If there is a need to change this firmware, a valid firmware file must be selected first. Click on the "Browse" button to do this. After clicking this button – a file selection dialog should appear:

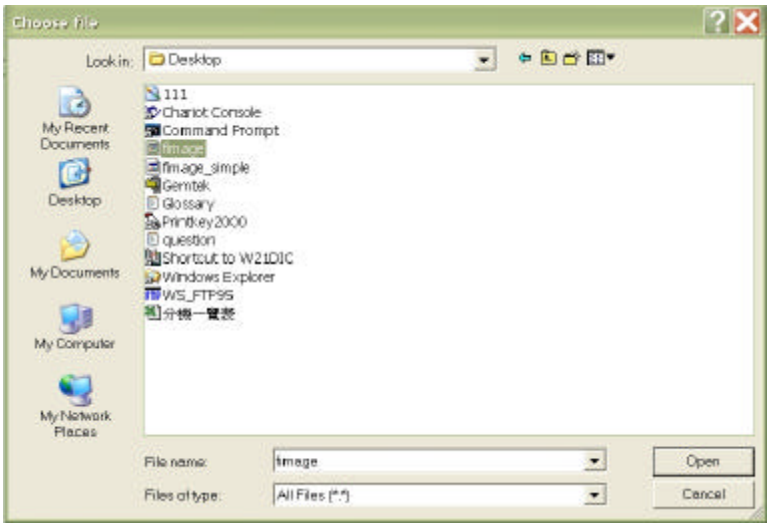


Figure 28: Firmware file selection dialog

When firmware file is selected, its name is shown in the "**Firmware**" field. Then click on the "Upgrade" button to upgrade firmware.

A "System Firmware Upgrade Process" screen will be displayed and firmware should be upgraded as shown below:

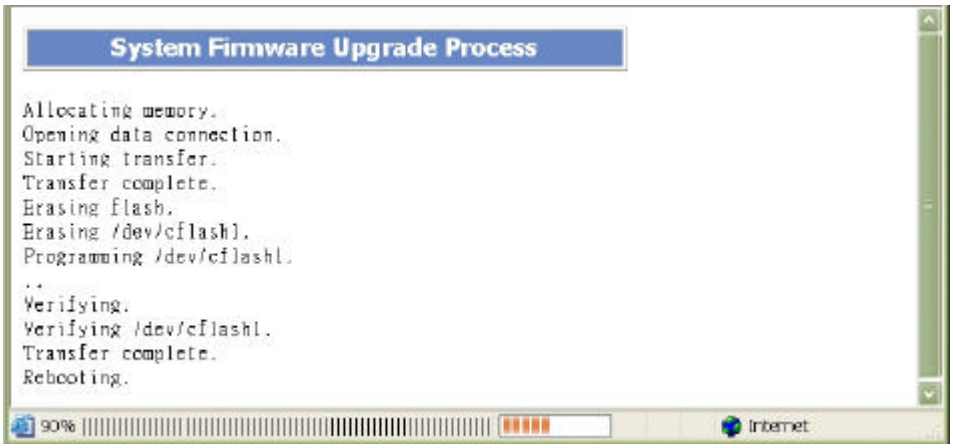


Figure 29: System Firmware Upgrade Process Status

A percentage will be showed on the status bar to indicate the upgrade status. After completed the firmware upgrade, the P380 device will be rebooted automatically.

Note: *The new firmware file overwrites the old one completely. All custom P380 configuration settings will be reset to the default values. Write down all configuration settings to be preserved, and set up them, when P380 starts after firmware upgrade. Initial P380 setup is described in the "Starting Up" chapter of this manual.*

Upgrade Utility

P380 can also be configured as a wireless station, but the unit requires full firmware upgrade, which can not be done in the web site. Therefore the P380 comes with an upgrade utility, "**upgrade.exe**", to allow the user to perform the task. The program runs under MS Windows 2000 family and MS Windows XP. Before the program is executed, the firmware should be located first. It can be found under the root directory in the CD.

When executing the program, the following screen should appear:

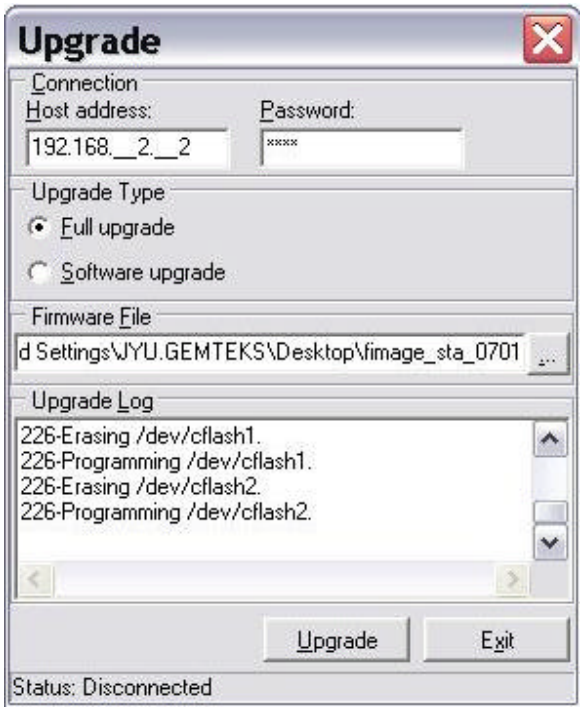


Figure 30: Upgrade utility

In the Host address field, enter the P380 IP address for which the firmware is to be upgraded. Enter the root password and choose Full upgrade. Specify the P380 station firmware file, before clicking on the "**Upgrade**" button. When the process is completed, it will be indicated in the upgrade log window.

Reboot Page

Click on the "***Reboot***" button to reboot P380 device via web management. All functions will be stopped while the device is rebooted.

Reset page

To reset the P380 device to the factory setting, click on the "***Reset***" button. A waiting & redirection message should be shown as below (for the redirection service, please refer to the redirection service section for detail):

Note: *All customized P380 configuration settings will be reset to the default values. Write down any configuration changes to be preserved, and set up them, when P380 starts after reset. Initial P380 setup is described in the "Starting Up" chapter of this manual.*

Hardware Reset

To reset the P380 device back to factory settings, except for web management, hardware reset will be another choice. There is no any physical button offered in hardware reset. For convenience sake, P380 offers the hardware reset processes as followed.

1. Unplug the power cable.
2. Re-connect the power cable.
3. Please wait for 5 to 6 seconds. At this moment, please disconnect the power cable.
4. Reconnect the cable on again and device will restart. This procedure will reset the settings back to default configuration. The device IP will be reset to the default IP.

Note: The length of the time allowed for hardware reset is only around two seconds. If it is missed, please restart the process.

Note: *All custom P380 configuration settings will be reset to the default values. Write down any configuration settings, which should be preserved, and set up them, when P380 starts after reset. Initial P380 setup is described in the "Starting Up" chapter of this manual.*

Specifications

Hardware

CPU	ETRAX-100LX
RAM	16 MB
Flash Memory	4 MB
Ethernet	10/100 Mbit
Wireless	IEEE 802.11b

Operating system

Linux version 2.4.14.

Network Subsystem

TCP/IP protocol suite

Firewall
Packet filtering
Masquerading (NAT)
Port forwarding

DHCP
DHCP server for one interface (Ethernet)

SNMP
802.11 MIB support (read write)
MIB-I, MIB2 support (read only)

Routing
Static routing only

Wireless
Wireless client mode support.
Wireless access point mode support
Wireless bridge mode support
WEP-48, WEP-128 encryption support

Administration

Web
Access to all user functions through web browsers (Java Script must be enabled)
Dynamic configuration changes (no reboot necessary)

Telnet
All console features

Scripting
User script support (available on the Pro version)

SNMP
802.11 MIB support (read write)
MIB-I, MIB-II support (read only)
Separate community strings for read and write support, standard SNMP trap support.

Glossary

Symbols:

10BaseT 10 Mbps/baseband/twisted pair. The IEEE standard for twisted pair Ethernet.

IEEE 802.11b The IEEE standards for the definition of the Wireless high speed (11Mbit) protocol for wireless communication.

A

Authorization the process of determining what types of activities a user is permitted to undertake. Usually, authorization is in the context of authentication: once you have authenticated a user, they may be authorized for different types of access or activity.

B

Backbone The primary connectivity mechanism of a hierarchical distributed system. All systems, which have connectivity to an intermediate system on the backbone, are assured of connectivity to each other. This does not prevent systems from setting up private arrangements with each other to bypass the backbone for reasons of cost, performance, or security.

Bandwidth Technically, the difference, in Hertz (Hz), between the highest and lowest frequencies of a transmission channel. However, as typically used, the amount of data that can be sent through a given communications circuit. For example, typical Ethernet has a bandwidth of 100Mbps.

bps *bits per secon*d. A measure of the data transmission rate.

D

DHCP *Dynamic Host Configuration Protocol.* A service that lets clients on a LAN request configuration information, such as IP host addresses, from a server.

DNS *Domain Name Syste*m. The distributed name/address mechanism used in the Internet. It comprises distributed online databases that contain mappings between human-readable names and IP addresses, and servers, which provide translation services to client applications.

Domain A part of the DNS naming hierarchy. Syntactically, an Internet domain name consists of a sequence of names (labels) separated by periods (dots), e.g., “machine.company.com”. See DNS.

E

Ethernet A common, 10Mbps local area network technology invented by Xerox Corporation at the Palo Alto Research Center. Ethernet is a best-effort delivery system that uses CSMA/CD technology. Ethernet can be run over thinwire coaxial cable (10BASE2), thickwire coaxial cable (10BASE5), twisted pair cable (10BASET), or fibre optic cable.

F

Filter Within the router, a filter is a process used to select which packets will be processed by the router, and which will be ignored or discarded. Selection may be based on addresses or protocol type.

Firewall A system or combination of systems that enforces a boundary between two or more networks.

FLASH A new memory technology, which combines the nonvolatile features of EPROMs with the easy in-system reprogramming of conventional volatile RAM. See EPROM.

G

Gateway The original Internet term for what is now called router or more precisely, IP router. In modern usage, the term “gateway” and “application gateway” refers to systems, which perform translation from some native protocol, or physical data format to another. Examples include electronic mail gateways, which translate between X.400 and RFC 822 mail message formats. See router.

H

Host An (end-user) computer system that connects to a network, such as a PC, minicomputer of mainframe.

I

ICMP *Internet Control Message Protoco*l. The TCP/IP protocol used to handle errors and control messages at the IP layer. ICMP is part of the IP protocol. Gateways, routers and hosts use ICMP to send reports of problems about datagrams back to the original source that sent the datagram.

Interface One of the physical ports on the router, including the Ethernet and asynchronous ports.

Interface type The type (Ethernet or Point-to-Point) of one of the interfaces on the router.

Internet A collection of networks interconnected by a set of routers, which allow them to function as a single, large virtual network.

Internet (note the capital "I") The largest internet in the world consisting of large national backbone networks (such as MILNET, NSFNET, and CREN) and a myriad of regional and local campus networks all over the world. The Internet is a multiprotocol network, but generally carries TCP/IP.

Internet address See IP address.

Internet Protocol See IP.

ISP *Internet service provider*. A company that provides Internet - related services. Most importantly, an ISP provides Internet access services and products to other companies and consumers.

IP *Internet Protoco*l. The network layer protocol for the TCP/IP protocol suite. It is a connectionless, best-effort packet switching protocol.

IP address A 32-bit address assigned to hosts using TCP/IP. The address specifies a specific connection to a network, not the host itself. See dotted decimal notation.

L

LAN *Local Area Networ*k. Any physical network technology (such as Ethernet) that operates at high speed (typically 10 Mbit per second or more) over short distances (up to a few kilometers). See WAN.

LED *Light Emitting Diod*e. A luminous indicator.

M

MAC address. The hardware address of a device connected to a shared media. For example, the MAC address of a PC on an Ethernet is its Ethernet address.

Metric A concept used to describe the cost of a route across a network, the distance to the destination at the remote end of the route, or the capacity of the route.

N

Name resolution The process of mapping a name into the corresponding address. See DNS.

NAT *Network Address Translation*, an Internet standard that enables a local-area network (LAN) to use one set of IP addresses for internal traffic and a second set of addresses for external traffic. A NAT box located where the LAN meets the Internet makes all

necessary IP address translations. NAT is used for two main tasks – to provide a type of firewall by hiding internal IP addresses and enable a company to use more internal IP addresses. Since they're used internally only, there's no possibility of conflict with IP addresses used by other companies and organizations.

Network A computer network is a data communications system which interconnects computer systems at various different sites. A network may be composed of any combination of LANs or WANs.

Network address The network portion of an IP address. For a class A network, the network address is the first byte of the IP address. For a class B network, the network address is the first two bytes of the IP address. For a class C network, the network address is the first three bytes of the IP address. In each case, the remainder is the host address. In the Internet, assigned network addresses are globally unique. See IP address.

Node An addressable device attached to a computer network. See host, router.

P

Packet The unit of data sent across a network. “Packet” is a generic term used to describe units of data at all levels of the protocol stack, but it is most correctly used to describe application data units. See datagram, frame.

Policy Organization-level rules governing acceptable use of computing resources, security practices, and operational procedures.

Port The abstraction used by Internet transport protocols to distinguish among multiple simultaneous connections to a single destination host. A port is a transport layer demultiplexing value. Each application has a unique port number associated with it. It is also used to refer to one of the physical network connectors on the router.

Protocol A formal description of message formats and the rules two computers must follow to exchange those messages. Protocols can describe low-level details of machine-to-machine interfaces (e.g., the order in which bits and bytes are sent across a wire) or high-level exchanges between allocation programs (e.g., the way in which two programs transfer a file across the Internet).

Q

QOS *Quality of Servic*e. Transmission system qualities measure in terms of reliability and availability.

R

Route The path that network traffic takes from the source to the destination. It may include many gateways, routers, hosts and physical networks.

Route table A table listing information about routes to other hosts or networks, such as the remote network or host address, the interface down which the route exists, the distance to the remote address and the cost of sending data over the route.

Router A system responsible for making decisions about which of several paths network (or Internet) traffic will follow. To do this it uses a routing protocol to gain information about the network, and algorithms to choose the best route based on several criteria known as “routing metrics”.

S

Server A network device that provides services to client stations. Examples include file servers and print servers.

Service A term used with the router to refer to a connection to another port on (another) router, used to access dialup modems, hosts that do not support TCP/IP and other asynchronous devices.

SNMP *Simple Network Management Protoco*l. The Internet standard protocol developed to manage nodes on an IP network. See MIB.

Subnet A portion of a network, which may be a physically independent network segment, which shares a network address with other portions of the network and is distinguished by a subnet number. A subnet is to a network what a network is to an internet.

Subnet Address The subnet portion of an IP address. In a subnetted network, the host portion of an IP address is split into a subnet portion and a host portion using an address or subnet mask. See subnet mask, IP address and network address.

Subnet Mask A bit mask used to select bits from an Internet address for subnet addressing. The mask is 32 bits long and selects the network portion of the Internet address and one or more bits of the local portion. Sometimes called address mask.

T

TCP *Transmission Control Protoco*l. The TCP/IP standard transport layer protocol in the Internet suite of protocols, providing reliable, connection-oriented, full-duplex streams. It uses IP for delivery.

TCP/IP Protocol Suite *Transmission Control Protocol over Internet Protoco*l. This is common shorthand, which refers to the suite of transport and application protocols that runs over IP. See IP, ICMP, TCP, UDP, FTP, Telnet, and SNMP.

Telnet The virtual terminal protocol in the TCP/IP suite of protocols, which allows users of one host to log into a remote host and interact as normal terminal users of that host.

Topology A network topology shows the computers and the links between them. A network layer must know the current network topology to be able to route packets to their final destination.

U

UDP *User Datagram Protoco*l. A transport layer protocol in the TCP/IP suite of protocols. UDP, like TCP, uses IP for delivery; however, unlike TCP, UDP provides for exchange of datagrams without acknowledgements or guaranteed delivery.

URL *Uniform Resource Locato*r. A standard format for specifying the name, type and location of documents and resources on an Internet. The syntax is type://host.domain[:port]/path/filename, where type specifies the type of document or resource (e.g. http is a file on a WWW server; file is a file on an anonymous FTP server; telnet is a connection to a Telnet-based service). See WWW.

W

WAN *Wide Area Networ*k. Any physical network technology that spans large geographic distances. WANs usually operate a slower speeds than LANs. See LAN.

WWW *World Wide We*b. A hypertext-based, distributed information system based on client - server architecture. Web browsers (client applications) request documents from Web servers. Documents may contain text, graphics and audiovisual data, as well as links to other documents and services. Web servers and documents are identified by URLs (Uniform Resource Locators). See URL.

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: To assure continued compliance, any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

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