APPENDIX B

Data Fields

This appendix describes the fields for the data parameters. After you log in, you can view or perform configuration from these tabs in the GUI:

- Quick Setup
- Interface Setup
- Network Setup
- Voice
- VPN
- Administration
- Diagnostics
- Status

Interface Setup module

The Interface Setup module includes these pages:

- Interface Setup > WAN
- Interface Setup > LAN
- Interface Setup > Wi-Fi Settings
- Interface Setup > Management Interface

Interface Setup > WAN page

Interface Setup > WAN > Internet Setup

From the **Interface Setup > WAN > Internet Setup** page, you can perform this configuration:

- Add a new WAN interface
- Edit an existing AN interface
- Configure a WAN interface

Add a New WAN Interface

Click the plus symbol to the right of the Ethernet WAN1 link.

Edit an Existing WAN Interface

Click the pen symbol to the right of the existing interface.

Configure WAN Interface

Either add or edit a WAN interface, The user sees a window with the fields that are described in the table that follows.

To save your settings, click the **Submit** button.

Field	Description
WAN	The interface ID (not applicable). This value cannot be changed.
VLAN ID	The ID for the VLAN (not applicable). VLAN 0, is used for the WAN interface, and this value cannot be changed.
Connection Type	Choose the connection type as required by your Internet Service Provider (ISP): • Automatic Configuration - DHCP • Static IP • PPPoE (for ADSLuser) • PPTP • L2TP
Automatic Configuration - DHCP	This type of connection is often used with cable modems. Select this option if your ISP did not assign a static IP address to your account and instead uses Dynamic Host Control Protocol (DHCP) to assign an IP address dynamically. No other information is required for this selection.
Static IP	Select this option if your ISP provides you with a static IP address. Enter the following required information as provided by your ISP: Internet IP Address, Subnet Mask, and Default Gateway IP address. Optionally, you can enter the IP addresses of up to three Domain Name System (DNS) servers, or leave the fields blank to allow a DNS server to be chosen dynamically. DNS servers translate website names such as www.cisco.com into routable IP addresses. • **Internet IP Address and Subnet Mask**–This is the router IP address and subnet mask as seen by external users on the Internet (including your ISP). If your Internet connection requires a static IP address, then your ISP will provide you with a Static IP Address and Subnet Mask. • **Default Gateway**–Your ISP will provide you with the Gateway IP Address. • **DNS 1-3**–The Domain Name System (DNS) is the method by which the Internet translates domain or website names into Internet addresses or URLs. Your ISP will provide you with at least one DNS Server IP Address. If you wish to use another, type that IP Address in one of these fields. You can enter up to three DNS Server IP Addresses here. The router will use these for quicker access to functioning DNS servers.

Field	Description
PPPoE (for ADSLuser)	Select this option if your ISP uses PPPoE (commonly with DSL services). Enter the User Name and Password for your ISP account. If required by your ISP, also enter the Service Name. Finally, choose either the Keep Alive or Connect On Demand option. With Connect on Demand, the router opens a connection only when a user attempts to connect to the Internet. The connection is automatically terminated if there is a period of inactivity longer than the specified Max Idle Time (in minutes). This option is recommended if your billing is based on the time that you are connected. Alternatively, the Keep Alive option enables the router to send messages to keep the connection permanently open, regardless of the level of Internet activity by your users. • **User Name and Password**–Enter the User Name and Password you use when you log on to your ISP through a PPPoE connection. • **Service Name**–If provided by your ISP, enter the Service Name. • **Connect on Demand**–You can configure the Router to terminate the Internet connection after a specified period of inactivity (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate Connect on Demand, click the radio button. If you want your Internet connection to remain active at all times, click the radio button next to Keep Alive. Otherwise, enter the number of minutes you want to elapse before your Internet connection terminates. • **Keep Alive**–This option keeps you connected to the Internet indefinitely, even when your connection sits idle. To use this option, click the radio button next to Keep Alive. The default Redial Period is 30 seconds (that is, the router checks the Internet connection every 30 seconds).
MTU	Size, in bytes, of the largest packet that can be sent through the network. This value is typically 1500 bytes, however it might need to be lower for some broadband services. Check with your service provider for specific requirements.

Interface Setup > WAN > Internet Option

Some ISPs may require the following information. Enter this information only if your ISP instructs you to do so.

Field	Description
Host Name	A host name for the WRP500. Some service providers, usually cable service providers, require a host name and a domain name as identification. In most cases, these fields can be left blank.
Domain Name	A domain name for the WRP500. Some service providers, usually cable service providers, require a host name and a domain name as identification. In most cases, these fields can be left blank.

Field	Description
IPv4 Static DNS 1 - 3	Optionally, enter the IP addresses for up to three Domain Name System (DNS) servers.
Scheduled WAN Reconnect	Enabled this feature will cause all WAN connections to be restarted at the specified Reconnect Time.
Reconnect Time	Set the reconnect time by hour and minute for Scheduled WAN Reconnect feature.

Internet Setup > WAN > Mobile Network

Field	Description
Global Settings	
Connect Mode	Select Auto to enable your 3G USB modem to establish a connection automatically. Select Manual to connect or disconnect your mobile connection manually. Please note that Ethernet Connection Recovery and Interface Connection Failover will work only if the Connection Mode is set to Auto. If you select Auto, you must select either Connect on Demand and Keep Alive. • Auto/Manual Select Auto to enable your modem to establish connection automatically. Select Manual to connect or disconnect your modem connection manually. Please note that Ethernet Connection Recovery and Interface Connection Failover will work only if the Connection Mode is set to Auto. • Connect on Demand Select this option to enable the router to terminate the Internet connection after it is inactive for a specified period of time (Max Idle Time). If your Internet connection is terminated due to inactivity, Connect on Demand enables the modem to automatically re-establish a terminated connection when a user attempts to access the Internet again. In the Max Idle Time field, enter the number of minutes of idle time that can elapse before your Internet connection terminates. The default Max Idle Time is 5 minutes. • Keep Alive Select this option to enable the router to check your Internet connection at the specified interval (Redial Period). If you are disconnected, then the router will automatically re-establish your connection. In the Redial Period field, specify how often you want the router to check the Internet connection. The default Redial Period is 30 seconds.

Field	Description
Tunnel Protocol	The Tunnel Protocol (PPTP/L2TP) could be supported via 3G USB modem by these simple instructions. • None Select this option to disable the Tunnel Protocol support. The option is used by default. • PPTP/L2TP Select one of the options to enable the PPTP or L2TP service you want to use. You will need to provide the server IP address, user name, and password. If you select 'None', the service would not be applied.
Card Status	This field shows the current modem connection status as Detecting, Connecting, or Connected. If your Connect Mode is Manual, there will be a button for you to click to connect or disconnect your Modem.
Mobile Network Setup	
Configure Mode	Select Auto to allow the router to automatically detect which card model was inserted and which carrier is available. Select Manual to set up the connection manually. To allow the router to automatically configure modem and mobile network settings, use the default setting, Auto.
Card Model	The data card model that is inserted in the USB drive. The mobile network service provider for Internet connection. This setting is required when you are using HSDPA/UMTS/GPRS Internet service.
Access Point Name (APN)	The Internet network to which the mobile device is connecting. Enter the access point name provided by your mobile network service provider.
Dial Number	The dial number for the Internet connection. Enter the dial number provided by your mobile network service provider.
User Name/ Password	Enter the user name and password provided by your mobile network service provider.
SIM PIN	The PIN code associated with your SIM card. Enter your SIM PIN number here.
Server Name	The name of the server for the Internet connection
Authentication	The type of authentication used by your service provider. Select your authentication type. If you do not know which type to use, use the default setting, Auto.
Service Type	Select the most commonly available type of mobile data service connection based on your area service signal. If your location supports only one mobile data service, you may set up for enhanced build up connection. The first selection will always search for HSPDA/3G/UMTS service or switch to GPRS automatically only when it is available.
LTE Service	LTE (Long-Term Evolution), commonly marketed as 4G LTE, is a standard for wireless communication of high-speed data for mobile phones and data terminals.Select your LTE service. If you do not know which service to use, use the default setting, Auto

Internet Setup > WAN > Multi-WAN Config

Field	Description
Failover	
Connection Failover	This feature ensures that the Internet connection is always connected through a stable WAN link. When this option is enabled, the WRP500 will first bring up the highest priority WAN interface. If the validation site associated with the WAN is unreachable, WRP500 will try to bring up the next priority WAN if available, and change system default route to that WAN. Once the validation site associated with higher priority WAN interface is reachable, WRP500 will change system default route back to the higher priority WAN interface and stop lower priority WAN connection. When this option is disabled, all WAN interfaces will try to establish the connection, and system default route will set to the highest priority WAN interface. Load balance feature is available at this time.
Failover Check Interval	Specify the time interval at which the WRP500 detects the status of the Internet connection. The default timeout interval is 60 seconds.
Failover Ping timeout	Specify the timeout value that WRP500 wait validation site response the ping request. The default timeout interval is 5 seconds.
Failover Ping Retries	Specify the retry value that validation site not respond the ping request. The default retry value is 1.
Failback after N Check Interval Successes	Specify how many successful responses from validation site the WRP500 recovery back to the high priority WAN.
Connection Validation Site	An IP address to use as a ping target to detect the status of the Internet connection. By default the WRP500 pings the gateway associated with the binding priority WAN. You may specify a different IP address as a target here.
WAN Interface	This summary provides information on the current status of the Ethernet Internet connection and the Mobile Network connection. You can click the hyperlink in the Status column to view the interface details. You may also configure the interface priority by using the Priority pull-down menu. If USB_Modem is the priority one and shows status **“Connected: Validation site unreachable,"** configure a valid IP address in the Priority 1 WAN field.
WAN Interface Detail	List WAN information related to WAN Interfaces table. The information includes WAN interface ID, IP address, net mask and gateway address.
Load Balance	
WAN Load Balancing	Enable or disable load balance. This feature is only available when Failover is disabled.
Weight	Specify the weight value associated with each WAN interface while running load balance. The valid value is between 0~99. 0 means the WAN interface will not join load balance.

Interface Setup > LAN page

Interface Setup > LAN > DHCP Server

Field	Description
DHCP Server	
Add Entry	After clicking the Add Entry button, you can create another DHCP Server Pool. To edit the settings for an existing DHCP server pool, click the pencil icon.
DHCP List	Name DHCP Name, Default is DHCPRule_1(Default LAN) and DHCPRule_voice. VLAN VLAN ID, The default is **1** and **100**.
DHCP Details	Click an entry in the DHCP List to see the details in the DHCP table
Router IP	
DHCP Name	Label which identifies this DHCP Server configuration and is used to assign the service to a VLAN interface.
Local IP Address/Subnet Mask	IP address and subnet mask used to configure the VLAN interface to which this DHCP rule is applied.
DHCP Server Setting	
DHCP Mode	To select this DHCP pool run as **DHCP Server** or **DHCP Relay** agent. Please note, DHCP Relay only works when the NAT function is disabled.
DHCP Server	
Show DHCP Reservation	Click this button to review and modify the DHCP reservations. Click the button again to hide the reservation tables.
Select Clients from DHCP Tables	Shows the clients that are currently receiving IP addresses from the DHCP server. If you want to reserve the currently assigned IP address for exclusive use by a client, check the Select box and click Add. The client appears in the Clients Already Reserved table.
Manually Adding Client	To reserve an IP address for a client, enter a client name and an IP address that you want to reserve for the client. Then enter the MAC address of the client and click Add. The client appears in the Clients Already Reserved table.
WAN Interface	Choose the WAN Interface from which the related DHCP information, specifically DNS, is obtained.
Default Gateway	Enter the IP address of the default gateway to be used by clients of this pool. If the field is 0.0.0.0. the VLAN Local IP Address is used as the default gateway.

Field	Description
Option 66	Provides provisioning server address information to hosts requesting this option. Server information can be defined in one of three ways: • Local TFTP Server: The WRP500 uses its own TFTP server to source provisioning files so it returns its own local IP address to the client. • Remote TFTP Server: If the WRP500 was configured by using this method, it uses the server information it received through option 66 on its WAN interface in response to local client requests. • Manual TFTP Server: Allows the manual configuration of a configuration server address. While this option is typically used to provide either an IP address or a fully qualified hostname, the WRP500 will also accept and offer a full URL including protocol, path and filename to meet to requirements of specific clients.
Option 67	Provides a configuration/bootstrap filename to hosts requesting this option. This is used in conjunction with option 66 to allow the client to form an appropriate TFTP request for the file.
Option 159	Provides a configuration URL to clients requesting this option. An option 159 URL defines the protocol and path information by using an IP address for clients that cannot use DNS. For example: **https://10.1.1.1:888/configs/bootstrap.cfg**
Option 160	Provides a configuration URL to clients requesting this option. An option 160 URL defines the protocol and path information by using a fully qualified domain name for clients that can use DNS. For example: **https://myconfigs.cisco.com:888/configs/bootstrap.cfg**
DNS Proxy	If DNS proxy is enabled, local clients are offered the WRP500 Local IP Address to use for DNS requests. The WRP500 then proxies these requests to the DNS servers it was configured with. If DNS proxy is disabled, then DHCP clients will be offered DNS server information based on the following: If the Static DNS field is configured, then that server alone will be offered to clients. If the Static DNS field is not configured up to three servers are offered, first from the global Internet Options static configuration and then from the WAN interface nominated above.
Starting IP Address	Enter an IP address of the first address in this pool.
Maximum DHCP Users	Enter the maximum number of devices that you want the DHCP server to assign IP addresses to.This number cannot be greater than 256.
Client Lease Time	Amount of time an address is leased to a client. Enter the amount of time, in minutes, for the lease. The default is 0 minutes, which means one day. Enter 9999 to assign an infinite lease.
WINS	The Window Internet Naming Service (WINS) manages the window's host name to address resolution. If you use a WINS server, enter the IP address of the server here. Otherwise, leave this field blank.
DHCP Relay	
Remote DHCP Server	Set the DHCP server IP address that DHCP message will be relayed to.

Interface Setup > LAN > VLAN Settings

Field	Description
VLAN Settings	
Add Entry	Click the **Add Entry** button to create another VLAN.
VLAN List	• Name—VLAN Name. The default is data_Lan and voice_Lan. • ID—VLAN ID, The default is data_Lan : 1 and voice_Lan : 100. • Address Type—LAN Address Type. The default is data_Lan and voice_Lan : DHCP Server Pool. • Voice—Voice, The default is data_Lan: disabled and voice_Lan : enabled. • Membership—Membership, The default is data_Lan: LAN Port 1-4 and SSID1, voice_Lan : LAN Port 1-4 and SSID2.
VLAN Details	Select one item the VLAN List, the Detail of VLAN table will show all VLAN information.
VLAN – Add	
VLAN Name	Enter your VLAN Name.
VLAN ID	Enter an identification number for the VLAN. Note that VLAN ID **0~2**, and **4080~4095** are reserved for internal interfaces, and cannot be set as the manual VLAN ID.
Voice VLAN	Click this box if you want voice applications to use this VLAN. **Note** All traffic from a voice VLAN follows the voice default route specified in WAN interface configuration unless there is policy based routing configured for the voice VLAN. Policy based routing takes precedence over the default route. There are no implicit QoS settings for voice VLAN. You will need to change these accordingly.
Role	When bridging LAN ports with a WAN interface, the VLAN role will control how the associated IP interface is created. • Select the WAN role to create the IP interface as a subinterface of the selected Ethernet WAN. The resulting VLAN will be a layer 2 broadcast domain on the outside of the firewall. • Select the LAN role to create the IP interface, if required, as a LAN VLAN. VLANs created without WAN interfaces are automatically created with the LAN role.

Field	Description
IPv4 Address Type	Address type determines the way in which the VLAN IP interface is configured. • Choose **None** if an IP interface is not required. This would typically be the case when bridging ports only. • Choose **Static IP Address** to manually define an address for the interface. • Choose **Dynamic IP Address** to request an address from a DHCP server on the local network. • Choose **DHCP server** to enable a previously configured DHCP Server service on this interface. In this case, the VLAN IP address will be derived from the DHCP Server configuration.
Available Interface	The interfaces that are available to be added to the VLAN. To move an interface to the Added Interface list, click the interface, and then click the right-arrow button (>). To move all of the interfaces at once, click the double right arrow button (>>).
Added Interface	The interfaces that were selected as members of the VLAN bridge. If you want to remove an interface from this list, click the interface and then click the left arrow button (<). To remove all of the interfaces at once, click the double left-arrow button (<<).

Interface Setup > LAN > Port Settings

Field	Description
Port Settings	
Port List	• Interface Show Port Interface. • Mode Describes the currently configured behavior of the port. • Desktop mode: Provides attached devices with access to a single data VLAN for which the WRP500 provides DHCP services. Incoming traffic from the host can be tagged or untagged. Outgoing traffic to the host will be untagged. • IP Phone + Desktop mode: The port is configured with a data VLAN for native access and a voice VLAN for use with an attached IP Phone. CDP is used to communicate voice VLAN information to the phone. • Switch/AP mode: The port is configured to be part of multiple VLANs (any combination other than 1 data and 1 voice VLAN) for the purposes of trunking to either a switch or wireless access point. • Generic: The port is configured for layer 2 bridging mode only. • Enabled Flow Control Mechanism for temporarily stopping the transmission of data on this physical interface. For example: A situation might arise where a sending station (computer) is transmitting data faster than some other part of the network (including the receiving station) can accept. The overwhelmed network element will send a PAUSE frame, which halts the transmission of the sender for a specified period of time. To enable this feature, check the box. The default setting is Enabled. • Speed Duplex (Ethernet Port 1~4) Choose the duplex mode. You can select from Autonegotiate, 10 Half, 10 Full, 100 Half,100 Full,1000 Half and 1000 Full. The default is Auto-negotiate.
Port	Defines the quality of service trust settings for the port. The default setting is untrusted. • If the port is not trusted, the queuing priority for incoming traffic is defined by the port priority setting. • If the port is trusted, the queuing priority for the traffic is determined by 802.1p priority (CoS to Queue) if present, or IP priority (DSCP to Queue) if not. If neither priority is available, the queuing priority is set based on the port setting.
Port/Access VLAN	Select the native VLAN (PVID) for this port. The dropdown list includes all VLAN IDs that were configured on the VLAN Settings page.

Field	Description
Voice VLAN	When the VLAN mode is IP Phone + Desktop, the voice VLAN ID is shown. This value is informational only.
Priority	Set a priority for unmarked, or untrusted traffic received on this port. By default, the priority is set to 0. A higher number indicates a higher priority.

Interface Setup > LAN > STP

Field	Description
STP	
Bridge Priority	Bridge priority is used to influence what bridge becomes the STP root. The bridge with the lowest value in the network will be elected as the root. Valid Bridge Priorities **range from 0 through 61440, in steps of 4096.** The default value is 32768.
Forward Delay	**Note** Forward Delay, Hello Time, and Max Age are configuration settings sent by the root bridge to all other bridges to define the current STP configuration. If the WRP500 is not elected as the root, the active timer values might be different to those configured here. Forward Delay is the time spent in the listening and learning state. This time is equal to **15** seconds by default, but you can adjust the time to be between **4** and **30** seconds. Base IEEE 802.1D Standard, to support interoperability with legacy Bridges, a Bridge shall enforce the following relationship: **2 x (Forward_Delay - 1.0 seconds) >= Max_Age** **Max_Age >= 2 x (Hello_Time + 1.0 seconds)**
Hello Time	The Hello Time is the time between each Bridge Protocol Data Unit (BPDU) that is sent by a bridge. This time is equal to **2** seconds by default, but you can adjust the time to be between **1** and **10** seconds. Base IEEE 802.1D Standard, to support interoperability with legacy Bridges, a Bridge shall enforce the following relationship: **2 x (Forward_Delay - 1.0 seconds) >= Max_Age** **Max_Age >= 2 x (Hello_Time + 1.0 seconds)**
Max Age	The Max Age timer defines how long bridges will wait after receiving the last hello message before assuming that the layer 2 topology has changed. At this point the current spanning tree configuration is discarded and the new topology is discovered. This time is **20** seconds by default, but you can adjust the time to be between **6** and **40** seconds. Base IEEE 802.1D Standard, to support interoperability with legacy Bridges, a Bridge shall enforce the following relationship: **2 x (Forward_Delay - 1.0 seconds) >= Max_Age** **Max_Age >= 2 x (Hello_Time + 1.0 seconds)**

Interface Setup > Wi-Fi Settings

Interface Setup > Wi-Fi Settings > Basic Wireless Settings

Field	Description
Wireless Network	
Operating Radio	Select Radio 1 (2.4 GHz) or Radio 2 (5 GHz) to specify which radio to configure. The rest of the settings on this tab apply to the radio you select in this field. Be sure to configure settings for both radios.
Wireless Table	
Wireless Network Name (SSID)	The default wireless network uses this name: "cisco-radio1-data" To rename the default wireless network, enter a unique Wireless Network Name, which is case-sensitive and must not exceed 32 characters (use any of the characters on the keyboard). To create a second wireless network, enter a unique Wireless Network Name in the SSID2 setting. (To activate this network, select Network Enabled.) Note: Your ISP or ITSP may control the SSID2 settings. Contact your ISP or ITSP for more information.
Broadcast Network Name	When wireless clients survey the local area for wireless networks to associate with, they detect the SSID broadcast by the Router. If you want to broadcast the SSID, leave the check box selected. If you do not want to broadcast the SSID, deselect the check box.
Enabled Network	To enable the wireless network, select the check box. To disable the wireless network, deselect the check box.
WPS Hardware Button	
Security	These settings configure the security of your wireless network.

Click "Edit" to configure SSID security

Wireless Security	
Security Mode	Select the security method for your wireless network. Proceed to the appropriate instructions. If you do not want to use wireless security, use the default, Disabled. • **WEP** • **WPA2 Personal** • **WPA/WPA2-Mixed Personal** • **WPA2 Enterprise** • **WPA/WPA2 Enterprise**

Interface Setup > Wi-Fi Settings > Wi-Fi Protected Setup

Field	Description
Select a SSID	From this drop-down menu, you can decide the WPS settings apply to which SSID. The default is SSID1.
Wi-Fi Protected Setup^{TM}	Select disabled if you don't want to use the Wi-Fi Protected Setup. The default is Disabled. There are three methods available. Use the method that applies to the client device; you are configuring. • Method 1 Use this method if your client device has a Wi-Fi Protected Setup button. a. Click or press the **Wi-Fi Protected Setup** button on the client device. b. Click the Wi-Fi Protected Setup button on this screen. c. After the client device has been configured, click d. **OK.** Then refer back to your client device or its documentation for further instructions. • Method 2 Use this method if your client device has a Wi-Fi Protected Setup PIN number. a. Enter the PIN number in the field on this screen. b. Click c. **Register.** d. After the client device has been configured, click e. **OK**. Then refer back to your client device or its documentation for further instructions. • Method 3 Use this method if your client device asks for the Router's PIN number. a. Enter the PIN number listed on this screen. (IT is also listed on the label on the bottom of the Router.) b. After the client device has been configured, click c. **OK**. Then refer back to your client device or its documentation for further instructions. The Wi-Fi Protected Setup Status, Network Name (SSID), Security are displayed at the bottom of the screen.

Interface Setup > Wi-Fi Settings > Advanced Wireless Settings

Field	Description
Operating Radio	Radio 1 and Radio 2 can be selected, after configure radio 1, you can select radio 2 to continue configuration.
RTS Threshold	The router sends Request to Send (RTS) frames to a receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission. If you encounter inconsistent data flow, you can adjust this threshold. Only minor reduction of the default value, **2347**, is recommended. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled. The RTS Threshold value should remain at its default value of **2347**.
AP Isolation	This feature isolates all wireless clients and wireless devices from one another. Wireless devices will be able to communicate with the router but not with other wireless devices on the network. To use this function, select Enabled. AP Isolation is disabled by default.
Basic Rate	The Basic Rate setting is not actually one rate of transmission but a series of rates at which the Router can transmit. The Router will advertise its Basic Rate to the other wireless devices in your network, so they know which rates will be used. The Router will also advertise that it will automatically select the best rate for transmission. The default setting is Default, which allows the Router to transmit at all standard wireless rates (1-2Mbps, 5.5Mbps, 11Mbps, 18Mbps, and 24Mbps). Other options are 1-2Mbps, for use with older wireless technology, and All, which allows the Router to transmit at all wireless rates.
DTIM Interval	This value, between 1 and 255, indicates the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the Router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Its clients hear the beacons and awaken to receive the broadcast and multicast messages. The default value is **1**
Fragmentation Threshold	This value specifies the maximum size for a packet before data is fragmented into multiple packets. If you experience a high packet error rate, you may slightly increase the Fragmentation Threshold. Setting the Fragmentation Threshold too low may result in poor network performance. Only minor reduction of the default value is recommended. In most case, it should remain at its default value of **2346**.
Beacon Interval	Enter a value between 20 and 1,024 milliseconds. The Beacon Interval value indicates the frequency interval of the beacon. A beacon is a packet broadcast by the router to synchronize the wireless network. The default value is 100.
Power Control	Form this drop-down menu, you can choose **high**, **middle**, or **low** value to specify the range of the wireless network. This option will determine the available distance. The default is **high** which is a normal power level.

Field	Description
PMF Capable	The 802.11w protocol applies only to a set of robust management frames that are protected by the Management Frame Protection **(PMF)** service. These include Disassociation, Deauthentication, and Robust Action frames. When PMF capable enabled, it is to be used if the client supports 802.11w.
PMF Required	Enabled PMF required will ensure that the clients that do not support 802.11w cannot associate with the WLAN.
PMF SHA256	Enable or Disable SHA-256 key derivation functionality.
Multicast Power Save	Enable or Disable Multicast Power Save.

Interface Setup > Wi-Fi Settings > WMM Setting

Field	Description
Wireless	
Operating Radio	Radio 1 and Radio 2 can be selected, after configure radio 1, you can select radio 2 to continue configuration.
WMM Support	WMM provides Quality of Service features to support voice and video applications. To enable WMM, keep the default setting, **Enabled**. Otherwise, choose **Disabled.**
No Acknowledgement	When this option is enabled, the router does not resend data if an error occurs. To enable this feature, keep the default setting, **Disabled**. Otherwise, choose **Enabled**.

Interface Setup > Management Interface

Field	Description
List of Management Interface	
IP Address	Enter the IP Address to use for the loopback test. If IP Address and WAN IP Address or LAN IP Address are the same, it is unavailable.

Network Setup module

The Network Setup module includes these pages:

- Network Setup > Routing
- Network Setup > NAT
- Network Setup > QoS
- Network Setup > Firewall
- Network Setup > PPPoE Relay
- Network Setup > DDNS
- Network Setup > DMZ

- Network Setup > IGMP
- Network Setup > UPnP
- Network Setup > CDP
- Network Setup > LLDP
- Network Setup > DNS Spoofing

Network Setup > Routing page

Network Setup > Routing > Static Routes > IPv4

Field	Description
Add Entry	After clicking the **Add Entry** button, it will create another Static Route.
Static Routing list	• Name Show all routes of name. • Interface Show all routes of interface.
Static Routing Details	Select one entry of Static Routing list, Defaults of Static Routing Details will show all Information. (Link Route Name, Destination IP Address, Subnet Mask, Gateway, Interface).
Enter Route Name	Enter a net Static Routing Name.
Destination	The Destination IP Address is the address of the network or host to which you want to assign a static route.
Subnet Mask	The Subnet Mask determines which portion of an IP address is the network portion, and which portion is the host portion.
Gateway	The IP address of the gateway device that allows for contact between the Router and the network or host.
Routing Table	• Destination LAN IP The Destination IP Address is the address of the network or host to which the static route is assigned. • Subnet Mask The Subnet Mask determines which portion of an IP address is the network portion, and which portion is the host portion. • Gateway This is the IP address of the gateway device that allows for contact between the Router and the network or host. • Interface This interface tells you whether the Destination IP Address is on the **LAN** (internal wired and wireless networks), the **Internet (WAN)**.

Network Setup > Routing > RIP > IPv4

Field	Description
RIP	Routing Information Protocol is used for dynamic routing. You can enable this protocol to allow the specified interfaces to automatically adjust to physical changes in the network's layout and to exchange routing tables with other router. The router determines the network packets' route based on the fewest number of hops between the source and destination. To enable the Dynamic Routing feature, select Enabled then enter the RIP settings, and enable RIP on the interfaces where you want to use this feature. To disable the Dynamic Routing feature for all data transmissions, use the default setting, **Disabled**.
RIP Version	To limit the types of packets that can be transmitted, choose Version 1 or Version 2. Alternatively, choose RIP v1/v2 to allow both Version 1 and Version 2 packets to be transmitted.
RIP Timer	RIP uses timers to regulate its performance. These include a routing-update timer, a route-timeout timer, and a route-flush timer. • Update Specify the rate at which the router sends routing updates. The default is 30 seconds • Timeout Specify the rate at which the router expects to receive routing updates from each router in the routing table. If this value is exceeded, the route is declared unreachable. The route is not removed from the routing table until the route flush timer expires. • Flush Specify the maximum period that the router will wait for an update before removing a route from the routing table.
RIP List	This list displays the RIP settings for the WAN interface (WAN1) and each VLAN. To edit the settings, click the pencil icon. • Interface Show RIP default interface. • RIP Enable • Passive • Authentication
RIP Network	• Network Address Specifies the IP Address and Subnet mask for the entry.

Network Setup > Routing > Intervlan Routing

Field	Description
Intervlan Routing	Configuring VLANs helps control the size of the broadcast domain and keeps local traffic local. However, when an end station in one VLAN needs to communicate with an end station in another VLAN, Intervlan communication is required. This communication is supported by Intervlan routing. To enable this feature, keep the default setting, **Enabled**. To disable this feature, choose **Disabled**.

Network Setup > Routing > Policy Routing

Field	Description
Add Entry	
Name	Specify the name for this policy route rule
Incoming Interface	Select LAN interface to apply for a rule. Any means the OUT Interface for this rule applied for all LAN interfaces
Source IP Address	Matches the source IP address from which packets are addressed to this rule.
Subnet Mask	Defines the source IP address wildcard mask. Masks specify which bits are used and which bits are ignored. A mask of 255.255.255.255 indicates that all the bits are important. A mask of 0.0.0.0 indicates that all the bits will be ignored. Therefore, if an Source IP Address is specified but source subnet mask specified to 0.0.0.0, the rule will regards it as 0.0.0.0/0 (all) address.
Destination IP Address	Matches the destination IP address to which packets are addressed to this rule.
Subnet Mask	Defines the destination IP address wildcard mask. Masks specify which bits are used and which bits are ignored. A mask of 255.255.255.255 indicates that all the bits are important. A mask of 0.0.0.0 indicates that all the bits will be ignored. Therefore, if a destination IP address is specified but destination subnet mask specified to 0.0.0.0, the rule will regards it as 0.0.0.0/0 (all) address.
Port	Defines the TCP/UDP destination port to match. "Any" means port field will not be inspected. "Single" means a port is specified. "Range" means that port range are specified
Protocol	Specify the interested protocol for this rule. Default is "Any", which, means protocol filed filter will be disabled and all kind of protocol are going to inspect. Beside, user can specify UDP, TCP

Field	Description
DSCP	Specify the DSCP number to match for this rule.
Route	Two possible output categories can be selected. One is existed VPN tunnel, and the other is existed WAN interface. When select WAN interface as output interface, an additional option can be checked: "Disable this rule if the interface is down". When this option is checked, the policy route rule will take no effect while the output interface is down (got no IP). The traffic will then fall through to match other policy route rules, or obey system's route (typically system default route).

Network Setup > NAT

Network Setup > NAT > NAT Setting

Field	Description
Address Translation	
NAT	Choose the correct working mode. Use the default setting, Enabled, if the Router is hosting your network's connection to the Internet (Enabled mode is recommended for most users). Select Disabled if the Router exists on a network with other routers
Application Layer Gateways	
SIP	SIP ALG can help to establish, modify, and terminate multimedia sessions (conferences) such as Internet telephony calls. The default is Enabled.
NetMeeting	NetMeeting ALG can modify RAS, Fast Start, H.245 Tunneling, Call Forwarding, RTP/RTCP and T.120 based audio, video, fax, chat, whiteboard, file transfer. Besides, it only support connected way from LAN hosts to WAN hosts at present. If you want to connected way from WAN to LAN, you need to set DMZ. The default is Enabled.
RTSP	RTSP ALG allows UDP transports to be setup properly, including RTP and RDT. The default is Enabled.
IRC	IRC ALG can allow users to send files to each other and user need connect to IRC server. The default is Enabled.

Network Setup > NAT > NAT Bypass

Field	Description
NAT Bypass	NAT Bypass Policy Setting which addressed a flexible and configurable rule matching criteria to set the matched traffic to perform pure routing while global NAT option is enabled.
Add Policy	Click the Add Policy button to create a NAT bypass rule

Field	Description
Policy List	• Policy Name User specified NAT bypass rule name • Inside Interface This field presents user specified inside interface, which will be VLAN interface, Host IP address or Indirect Network • Outside Interface This field presents user specified outside interface • Status This field presents this NAT bypass rule is enabled or disabled
Policy Details	All detailed information will be shown by selecting one entry from the list of NAT bypass rule.
Policy Name	Specify the rule name for this rule.
Enable	Enable/disable this rule.
Inside interface	Specify the traffic source rule • VLAN interface Specify the VLAN that to become the NAT bypass VLAN domain. The pull down menu contain all LAN (VLAN) collection. This is the either one option between Host and Indirect Network Domain options. • Host IP Address Specify a host IP address that to become a routed host. This is the either one option between VLAN and Indirect Network Domain options • Indirect Network Specify an indirect network domain (non-VLAN) to be a routed domain. This is the either one option between VLAN and Host options. • IP Address Specify source IP address associated with the indirect network domain when indirect network domain option selected. • Subnet Mask Specify the subnet mask associated with the source IP address when indirect network domain option is selected.
Outside Interface	Specify the traffic destination rule. • WAN interface Select the out interface. The pull down menu contains all WAN collection. • IP Address Specify destination IP address • Subnet Mask Specify the subnet mask associated with the destination IP address.

Network Setup > NAT > Port Forwarding

Port Forwarding	Use the Port Forwarding page if your network hosts network services (Internet applications) such as World Wide Web, email, FTP, videoconferencing or gaming. For each service, you need to configure the settings to forward Internet traffic to the servers that host these services. After clicking the Add Entry button, you can create another entry for another network service. To edit an entry, click the pencil icon. Before you perform this procedure, you should reserve a DHCP addresses for each server that hosts an Internet application. Use the Interface Setup > LAN > DHCP Server page. Click Add Entry, and then click Show DHCP Reservation. You can add the server from the Select Clients table, or manually enter the client information.
Add Entry	Click the **Add Entry** button to create another Single Port Forwarding or Port Range Forwarding
List of Port Forwarding	• Number • Type Show Port Forwarding entry type is Single Port Forwarding or Port Range Forwarding. • Status Show Enable or Disable the entry. • Application Show Entry Name.
Port Forwarding Details	Select one entry from the List of Port Forwarding Details of Port Forwarding will show all Information. (like Wan Interface Name, External Port, Internal Port, Protocol, IP Address).
Port Forwarding Type	Choose Single Port Forwarding to forward traffic to a single port on the specified server, or choose Port Range Forwarding to forward traffic to a range of ports.

	Single Port Forwarding • Application Name: Choose a standard application from the drop-down list. To enter an application that is not on the list, choose Add a new name, and then enter the name of a new application. • Enter a Name: Enter the name of the Internet application. • WAN Interface Name: Choose the WAN interface through which the traffic is transmitted • External Port: For single port forwarding, enter the external port number that is used by the server or Internet application. Check the Internet application's documentation for more information • Internal Port: For single port forwarding, enter the internal port number used by the server or Internet application. Check the Internet application's documentation for more information. • Protocol: Select the protocol TCP or UDP. • IP Address: Enter the IP address of the server that hosts this Internet application. The server must have a static IP address, which you can set on the Interface Setup > LAN > DHCP Server page. • Enabled: Check the box to enable the application you have defined. The default setting is unchecked (Disabled)
	Port Range Forwarding • Enter a Name: Enter the name of the Internet application • WAN Interface Name: Choose the WAN interface through which the traffic is transmitted • Start ~ End Port: For port range forwarding, specify the range of ports used by the server or Internet application. Enter the first port in the first box, and enter the final port in the second box to specify the range. Check the Internet application's documentation for more information. • Protocol: Select the protocol TCP or UDP. • IP Address: Enter the IP address of the server that hosts this Internet application. The server must have a static IP address, which you can set on the Interface Setup > LAN > DHCP Server page. • Enabled: Check the box to enable the application you have defined. The default setting is unchecked (Disabled).

Network Setup > NAT > Port Range Triggering

Field	Description
Port Range Triggering	Use the Port Range Triggering page to allow the router to dynamically open ports for network services (Internet applications) that are hosted by individual computers. When this feature is enabled, an outbound connection from specified ports triggers the router to open other specified ports for incoming traffic. Port Range Triggering does not require you to reserve an IP address (static IP address) for the computer that hosts the specified application. However, Port Range Triggering allows only one computer to host a service on the specified ports at one time.
Add Entry/Edit	After clicking **Add Entry** button, it can create another Port Range Triggering.
Port Range Triggering List	• Status Show Enable or Disable the entry. • Application Show Entry Name.
Port Range Triggering Details	Select one entry of Port Range Triggering List, Details of Port Triggering will show all Information, such as WAN Interface, LAN Interface, Triggered Range, Forwarded Range, Protocol.
Application Name	Enter a name to identify the application in the Port Range Triggering List
WAN	Choose the WAN Interface for the Internet traffic
LAN	Choose the LAN where the host computer is located
Triggered Range	Enter the starting and ending port numbers of the triggered port range. When a computer makes an outbound connection from these ports, the router will open the ports that are specified in the Forwarded Range fields. Check with the Internet application's documentation for the port number(s) needed.
Forwarded Range	Enter the starting and ending port numbers of the forwarded port range. These ports will be opened when an outbound connection is made from the ports that are specified in the Triggered Range fields. Check with the Internet application documentation for the port number(s) needed.
Protocol	Select the protocol TCP or UDP.
Enabled	Click the Enabled check box to enable the applications you have defined. This is disabled (unchecked) by default.

Network Setup > QoS

Network Setup > QoS > QoS Bandwidth Control

Field	Description
QoS Bandwidth Control	Set the bandwidth priority rule for a variety of interface.
Name	Show the interface name
Enabled	To use the QoS policies you have set, select the check box. Otherwise, deselect the check box.
Upstream Bandwidth	Show the maximum bandwidth for upstream data transmissions
Strict High/ High / Medium / Normal / Low	Show the bandwidth guarantees for each priority queues
Upstream Bandwidth	Set the maximum bandwidth for upstream data transmissions.
Priority	Set the bandwidth guarantees for the priority queues. • Strict High Enter the guaranteed bandwidth for the Strict High Priority queue. • High, Medium, Normal, Low Increase the rate and bandwidth for each queue by clicking the plus (+) button, or reduce the rate and bandwidth by clicking the minus (-) button.

Network Setup > QoS > QoS Policy

Field	Description
QoS Policy	Configures the Quality of Service (QoS) settings for specified applications, devices, ports, or VLANs. Quality of Service (QoS) ensures better service to high-priority types of network traffic, which may involve demanding, real-time applications, such as video conferencing. When you set priority, do not set all applications to High, because this will defeat the purpose of allocating the available bandwidth. If you want to select below normal bandwidth, select Low. Depending on the application, a few attempts may be needed to set the appropriate bandwidth priority.
Add Entry	Click the **Add Entry** button to create another QoS Policy.New create rule will have high priority than old one
List of QoS Policy	• Priority Show the priority of entry. • Name Show the name of entry
QoS Details	Select one entry of List of QoS Policy, Details of QoS will show all information about QoS

Field	Description
Category	There are five categories available. Select one of the following: **Application, MAC Address, Ethernet Port, VLAN** and **IP Address**, then complete the fields that appear, based on your selection.
	Application • Applications: Choose a standard application from the drop-down list. To enter an application that is not on the list, choose Add a New Application, and then enter the name. • Name: For most categories and applications, this field displays the name of the selected category or application. If you chose Add a New Application, enter the name of the application. • LAN: Choose the VLAN that is used for this traffic • Port Range: – Port Range: Enter the number or range of port(s) used by the server or Internet application. Check the Internet application's documentation for more information. Also select the protocol TCP or UDP, or select Both. – Protocol: Select the protocol **TCP** or **UDP**, or select **Both** • Priority: Choose the bandwidth priority for this traffic: **Strict**, **High**, **Medium**, **Normal**, or **Low**, **Medium** is recommended • Marking: Marking modifies the DiffServ or CoS field of the packet according to QoS Policy Rule (by Application port range, Mac, Ethernet port, VLAN and IP Address). Note: CoS value only valid when output interface is subwan (with 802.1Q tagging). • CoS and DiffServ: Setting Network Setup/QoS/Qos policy, this will classify the LAN to WAN packet. If traffic doesn't match these policy rules, it will use default priority setting by each Ethernet port if it is untrust mode, or classify by packet COS or DiffServ priority setting if it is trust mode.

Field	Description
	MAC Address • Name: Enter a name to describe this rule. • LAN: Choose the VLAN that is used for this traffic • MAC Address: Enter the MAC address of the device in the following format: xx:xx:xx:xx:xx:xx • Priority: Choose the bandwidth priority for this traffic: **Strict**, **High**, **Medium**, **Normal**, or **Low**, **Medium** is recommended. • Marking: Marking modifies the DiffServ or CoS field of the packet according to QoS Policy Rule (by Application port range, Mac, Ethernet port, VLAN and IP Address). **Note** CoS value only valid when output interface is subwan (with 802.1Q tagging). • CoS and DiffServ: Setting Network Setup/QoS/Qos policy, this will classify the LAN to WAN packet. If traffic doesn't match these policy rules, it will use default priority setting by each Ethernet port if it is untrust mode, or classify
	Ethernet Port • Name: Enter a name to describe this rule. • LAN: Choose the VLAN that is used for this traffic • Ethernet Choose the Ethernet port. • Priority: Choose the bandwidth priority for this traffic: **Strict**, **High**, **Medium**, **Normal**, or **Low**, **Medium** is recommended. • Marking: Marking modifies the DiffServ or CoS field of the packet according to QoS Policy Rule (by Application port range, Mac, Ethernet port, VLAN and IP Address). **Note** CoS value only valid when output interface is subwan (with 802.1Q tagging). • CoS and DiffServ: Setting Network Setup/QoS/Qos policy, this will classify the LAN to WAN packet. If traffic doesn't match these policy rules, it will use default priority setting by each Ethernet port if it is untrust mode, or classify by packet's COS or DiffServ priority setting if it is trust mode.

Field	Description
	VLAN • Name: Enter a name to describe this rule. • LAN: Choose the VLAN that is used for this traffic • Priority: Choose the bandwidth priority for this traffic: **Strict**, **High**, **Medium**, **Normal**, or **Low**, **Medium** is recommended. • Marking: Marking modifies the DiffServ or CoS field of the packet according to QoS Policy Rule (by Application port range, Mac, Ethernet port, VLAN and IP Address). **Note** CoS value only valid when output interface is subwan (with 802.1Q tagging). • CoS and DiffServ: Setting Network Setup/QoS/Qos policy, this will classify the LAN to WAN packet. If traffic doesn't match these policy rules, it will use default priority setting by each Ethernet port if it is untrust mode, or classify by packet's COS or DiffServ priority setting if it is trust mode.
	IP Address • Name: Enter a name to describe this rule. • Destination IP Address: Set the destination IP address of traffic flow that would apply QoS. • Destination Mask: Set the subnet mask to decide the destination IP address range. • Priority: Choose the bandwidth priority for this traffic: **Strict**, **High**, **Medium**, **Normal**, or **Low**, **Medium** is recommended. • Marking: Marking modifies the DiffServ or CoS field of the packet according to QoS Policy Rule (by Application port range, Mac, Ethernet port, VLAN and IP Address). **Note** CoS value only valid when output interface is subwan (with 802.1Q tagging). • CoS and DiffServ: Setting Network Setup/QoS/Qos policy, this will classify the LAN to WAN packet. If traffic doesn't match these policy rules, it will use default priority setting by each Ethernet port if it is untrust mode, or classify by packet's COS or DiffServ priority setting if it is trust mode.

Network Setup > QoS > CoS To Queue

Field	Description
VLAN CoS	Specifies the VLAN (CoS) priority tag values, where zero is the lowest and 7 is the highest.
Priority	Defines the traffic forwarding queue to which the CoS priority is mapped. Where five kinds of traffic priority queues are supported.

Network Setup > QoS > DSCP To Queue

Field	Description
DiffServ	Indicates the Differentiated Services Code Point (DSCP) value in the incoming packet
Priority	Defines the traffic forwarding queue to which the DSCP priority is mapped

Network Setup > Firewall

Network Setup > Firewall > Firewall Filter

Field	Description
SPI Firewall Protection	A firewall enhances network security and uses Stateful Packet Inspection (SPI) for more review of data packets entering your network. Select **Enabled** to use a firewall, or **Disabled** to disable it.
Filter Anonymous Internet Requests	When enabled, this feature keeps your network from being "pinged," or detected, by other Internet users. It also hides your network ports. Both to make it more difficult for outside users to enter your network. This filter is enabled by default. Select **Disabled** to allow anonymous Internet requests.
Filter Internet NAT Redirection	This feature uses port forwarding to block access to local servers from local networked computers. This filter is disabled by default. Select **Enabled** to filter Internet NAT redirection, or **Disabled** to disable this feature.
Filter IDENT (Port 113)	This feature keeps port 113 from being scanned by devices outside of your local network. This filter is enabled by default. Select **Enabled** to filter port 113, or **Disabled** to disable this feature.
Filter DoS Attack	When enabled, this feature wards off ICMP Ping flood (ICMP echo request) and TCP SYN flood (tcp_syn cookies) attacks. The default is disabled. Check the box to enable it. The maximum rate limit for both types of flood attacks is 50 packets per second Note: If an IP packet is destined to an IP broadcast or IP multicast destination address, your network can be used to execute a flooding DoS attack to other hosts.

Field	Description
Proxy	Use of WAN proxy servers may compromise your network security. Denying Filter Proxy will disable access to any WAN proxy servers. To enable proxy filtering, check the box.
Java	Java is a programming language for websites. If you deny Java, you run the risk of not having access to Internet sites created using this programming language. To enable Java filtering, check the box.
ActiveX	ActiveX is a programming language for websites. If you deny ActiveX, you run the risk of not having access to Internet sites that use this programming language. To enable ActiveX filtering, check the box.
Cookies	A cookie is data stored on your computer and used by Internet sites when you interact with them. To prevent the storage of cookies, check the box.
Filter Port	Set the Web service port for filtering Proxy/Java/ActiveX/Cookies, port 80 is used by default

Network Setup > Firewall > Firewall Filter

Field	Description
Internet Filter	• Filter Anonymous Internet Requests • Filter Internet NAT Redirection • Filter IDENT (Port 113 • Filter DoS Attack
Web Filter	• Proxy • Java • ActiveX • Cookies

Network Setup > Firewall > IPV4 > Internet Access Control

Field	Description
Internet Access Control	Configures rules controlling users' access to the Internet
Add Entry	Click the **Add Entry** button to create another Internet Access Control

Field	Description
Internet Access Policy list	- PolicyName Show the entry of name. - Status Show the entry of status. - From LAN Interface Show the entry of LAN interface. - To WAN Interface Show the entry of WAN interface.
Policy Details	Select an entry from the Internet Access Policy list, Details of Policy will show all information about Internet Access Policy.
Policy Name	Add Policy Name
Status	To enable this policy, click Enabled. To disable this policy, click **Disabled**. The default is **Disabled**
From LAN, To WAN	You can apply the rule to all traffic by choosing From All, To All, or you can limit the rule to apply only to particular interfaces, such as From VLAN1 to Ether_WAN1
Applied PCs	If you want the policy to apply only to specified PCs, click the Show Edit List button. Then you can specify individual PCs by entering the MAC address or the IP address. You can specify groups of PCs by entering up to two ranges of IP addresses
Days/Times	Choose the days and times when you want this policy to be enforced. Select the individual days, or select **Everyday**. Enter a range of hours by specifying the start time (From) and the end time (To), or select **24 Hours**.
Blocking Everything	Check this box to block all Internet traffic that meets the criteria that you specified on this page. Uncheck this box to choose one or more of the other filtering options.
Blocking by URL and Keyword	Check this box to prevent users from accessing specified URLs or URLs that contain specified keywords in HTTP session only, but HTTPS session is not supported. Enter up to four URLs and up to six keywords.

Field	Description
Blocking by destination IP address	Check this box to prevent users from accessing specified IP addresses. Enter up to four IP addresses.
Blocking by Services	Check this box to prevent users from accessing specified Internet services, such as FTP or telnet. (You can block up to three applications per policy.) From the Applications list, click the application that you want to block. Then click the right-arrow button to move the application to the Blocked List. To remove an application from the Blocked List, click it and then click the button left-arrow button. Application List: •DNS(53 - 53) •FTP(21 - 21) •HTTP(80 - 80) •HTTPS(443 - 443) •TFTP(69 - 69) •IMAP(143 - 143) •NNTP(119 - 119) •POP3(110 - 110) •SMTP(25 - 25) •SNMP(161 - 161) •TELNET(23 - 23)

Network Setup > Firewall > IPV4 > Inbound Access Control

Field	Description
Inbound Access Control	Configure rules controlling your users' access from the Internet (WAN to LAN).
Add Entry	Click the **Add Entry** button to create another Advanced Firewall Policy entry
Advanced Firewall Policy List	• Policy Name Show the entry of Policy Name • Status Show the entry of Status • IN Interface(WAN) Show the entry of IN Interface(WAN) • OUT Interface(LAN) Show the entry of OUT Interface(LAN) • Priority Show the entry of Priority

Field	Description
Rule Name	User specified rule name. Up to 31 characters are allowed to key-in.
Status	Enabled or disabled this rule entry.
IN Interface(WAN)	Select WAN interface to apply for a rule. ALL WAN means the IN Interface for this rule applied for all WAN interfaces.
OUT Interface(LAN)	Select LAN interface to apply for a rule. ALL LAN means the OUT Interface for this rule applied for all LAN interfaces.
Source IP Address	Matches the Source IP address to which packets are addressed to this rule.
Source Subnet Mask	Defines the source IP address wildcard mask. Masks specify which bits are used and which bits are ignored. A mask of 255.255.255.255 indicates that all the bits are important. A mask of 0.0.0.0 indicates that all the bits will be ignored. Therefore, if an Source IP Address is specified but source subnet mask specified to 0.0.0.0, the rule will regards it as 0.0.0.0/0 (all) address
Destination IP Address	Matches the destination IP address to which packets are addressed to this rule.
Destination Subnet Mask	Defines the destination IP address wildcard mask. Masks specify which bits are used and which bits are ignored. A mask of 255.255.255.255 indicates that all the bits are important. A mask of 0.0.0.0 indicates that all the bits will be ignored. Therefore, if an destination IP address is specified but destination subnet mask specified to 0.0.0.0, the rule will regards it as 0.0.0.0/0 (all) address.
Protocol	Specify the interested protocol for this rule. Default is "Any", which, means protocol filed filter will be disabled and all kind of protocol are going to inspect. Beside, user can specify UDP, TCP, or ICMP protocol
Source Port	Defines the TCP/UDP source port that this rule to match. “Any” means port field will not be inspected. “Single” means a port is specified. “Range” means that port range are specified.
Destination Port	Defines the TCP/UDP destination port that this rule to match. “Any” means port field will not be inspected. “Single” means a port is specified. “Range” means that port range are specified
Action	Deny or Permit the traffic associated with this rule.
Schedule	Selective week day schedule that this rule is going to apply.
Times	Specified time period that this rule is going to apply.

Network Setup > PPPoE Relay

Field	Description
Add Entry	Click the **Add Entry** button to create another PPPoE Relay
PPPoE Relay list	• Wan option Show the entry of wan option. • Lan option Show the entry of lan option. • PPPoE Relay Show the entry of status.
PPPoE Relay	Enable or Disable PPPoE Relay
WAN Interface	Select the WAN Interface for this rule
LAN Interface	Select the LAN Interface for this rule

Network Setup > DDNS

Field	Description
DDNS	Dynamic DNS (DDNS) is an Internet service that allows routers with varying public IP addresses to be located using Internet domain names. If your ISP has not provided you with a static IP, and your WAN connection is configured to use DHCP to get an IP address dynamically, then DDNS allows you to have a virtual static address for your website. To use DDNS, you must setup an account with a DDNS provider such as DynDNS.com or TZO.com Use the DDNS page to activate your service on the router.
DynDNS.org	
DynDNS.org	You must sign up for an account with DynDNS.org before you can use this service.
User Name	Enter the user name from DynDNS.org.
Password	Enter the password from DynDNS.org.
Host Name	Enter your host name. This should be in the format of name.dyndns.org.
System	Select the DynDNS service you use: **Dynamic**, **Static**, or **Custom**.
Mail Exchange (Optional)	Enter the address of your mail exchange server, so the email to your DynDNS address go to your mail server.
Mail Exchange (Backup MX)	This feature allows the mail exchange server to be a backup. To enable this feature, use the default setting, **Enabled**. To disable this feature, select **Disabled**. If you are not sure, which setting to select, use the default setting, **Enabled**.

Field	Description
Wildcard	This feature allows you to use a wildcard value in the DDNS address. For example, if your DDNS address is myplace.dyndns.org and you enable wildcard, then the x.myplace.dyndns.org will work as well (x is the wildcard). To enable wild cards, use the default setting, **Enabled**. To disable wildcard, select Disabled. If you are not sure which to select, use the default setting, **Enabled**.
Internet IP Address	Your current IP address.
Status	Your DDNS status.
Update	To manually trigger an update, click this button.
TZO.com	
TZO	You must sign up for an account with TZO before you can use this service.
E-Mail Address	Enter the email address for your TZO account.
TZO Key	Enter the key for your TZO account.
Domain Name	Enter your host name. This should be in the format of name.dyndns.org.
Internet IP Address	Your current IP address.
Status	TZO DDNS status.
Update	To manually trigger an update, click this button.

Network Setup > DMZ

Network Setup > DMZ > Software DMZ

Field	Description
Software DMZ	A DMZ (Demarcation Zone or Demilitarized Zone) is a sub-network that is behind the firewall but that is open to the public. By placing your public services on a DMZ, you can add an additional layer of security to the LAN. The public can connect to the services on the DMZ but cannot penetrate the LAN. You should configure your DMZ to include any hosts that must be exposed to the WAN (such as web or email servers)
Add Entry	Click the Add Entry button to create a software DMZ entry
Status	Select enable to activate this entry, or disable to deactivate it.
Public IP	Input an public IP address that this DMZ server will expose to the Internet
Private IP	The Subnet Mask Server's private IP address behind LAN corresponding to the Public IP address

Network Setup > DMZ > Hardware DMZ

Field	Description
Hardware DMZ	This feature will use new LAN port 4 as can be used for DMZ purposes for public access to the customer's web and other servers that are accessible from the Internet. The rest LAN network ports will continue to be used for private internal traffic.Please note that this feature only supported while WAN in static or DHCP mode. Hardware DMZ site can't be applied for a VPN connection site.
Hardware DMZ	When select enabled, LAN port 4 will act as DMZ port, or it acts as a normal LAN port for private internal traffic.
Add Entry	Click the Add Entry button to create a hardware DMZ IP matching.
Hardware DMZ Details	
Status	Select enable to activate this entry, or disable to deactivate it.
Public IP	Input an public IP address that equal to the server IP address that attached behind hardware DMZ port

Network Setup > IGMP

Field	Description
IGMP	Internet Group Management Protocol (IGMP) is a signaling protocol that supports IP multicasting for IPTV.
IGMP Proxy	Keep the default setting, **Enabled**, if you want to allow multicast traffic through the router for your multimedia application devices. Otherwise, select **Disabled**.
Support IGMP Version	Select the version you want to support, **IGMP v1**, **IGMP v2**,or **IGMP v3**. If you are not sure which version to select, keep the default setting, **IGMP v2**.
WAN Interface	Select WAN interface you want to forward, you can check **Internet Setup** to check its type. If you are not sure which WAN interface to select, keep the default setting [**AUTO**] to follow system default route interface.
Immediate Leave	Select **Enabled**, if you use IPTV applications and want to allow immediate channel swapping or flipping without lag or delays. Otherwise, use the default setting, **Disabled**.

Network Setup > UPnP

Field	Description
UPnP	UPnP (Universal Plug and Play) is a feature that allows for automatic discovery of devices that can communicate with the router.
UPnP	If you want to use UPnP, use the default setting, **Enabled**. Otherwise, select **Disabled**.

Field	Description
Allow Users to Configure	When this feature is enabled (the default setting), you can make manual changes while using the UPnP feature. Select Disabled, if you don't want to be able to make manual changes.
Keep UPnP Configurations After System Reboot	When this feature is enabled, the router saves UPnP configuration after a system reboot. The default is **Disabled**. When this feature is disabled, the router does not save UPnP configuration, but it does not remove the previous UPnP configuration.

Network Setup > CDP

Field	Description
CDP	Cisco Discovery Protocol (CDP) is a device discovery protocol that runs on all Cisco equipment. Each CDP-enabled device sends periodic messages to a multicast address and also listens to the periodic messages sent by others in order to learn about neighboring devices. Use the CDP page to choose the CDP settings for your network.
CDP Setting	
CDP	You can enable CDP on all ports, disable CDP on all ports, or configure CDP per port. Cisco recommends the default setting, Per Port. Enabling CDP is not recommended on the WAN port because it is connected to an insecure network.
CDP Timer	Specify the interval at which successive CDP packets can be sent. Valid values are from 5-900. The default is 60.
CDP Hold Timer	Specify the amount of time that the information sent in the CDP packet is cached by the device that receives the CDP packet. Valid values are from 10-255. The default is 180.
Interface List	Checked the enable check box to enable the interface.

Network Setup > DNS Spoofing

Field	Description
Enable	Enable DNS spoofing
Add Entry	Add DNS spoofing entry
DNS Spoofing Add Entry Setting	
Host Name	Enter one domain name field to spoofing.
IP Address	Enter one mapping IP address.

VPN module

The VPN module includes these pages:

- VPN > Site to Site IPSec VPN
- VPN > GRE Tunnel
- VPN > VPN Passthrough
- VPN > Cisco VPN Server

VPN > Site to Site IPSec VPN

VPN > Site to Site IPSec VPN > NAT Traversal

Field	Description
NAT Traversal	
NAT Traversal	IPSec NAT Traversal can support detecting the presence of NAT. The detecting packet not only detects the presence of NAT between the two IKE peers, but also detects where the NAT is. The location of the NAT device is important, as the keepalives have to initiate from the peer behind the NAT. Please refer RFC3947.To enable this feature, choose **Enabled**. To disable this feature, choose **Disabled**.

VPN > Site to Site IPSec VPN > IKE Policy

Field	Description
IKE Policy	
Add Entry	Click the **Add Entry** button to create another IKE policy.
List of IKE Policies	• Name Show entry of name.
IKE Details	Select an entry from the List of IKE Policies, Details of IKE will show all information about IKE Policy.
General	
Policy Name	Use a unique name which will be displayed in the list of VPN policies for the selection.
Exchange Mode	Choose the exchange mode based on your requirements for security and speed. Main: Choose this mode if you want higher security, but with a slower connection. Main Mode relies upon two-way key exchanges between the initiator and the receiver. The key-exchange process slows down the connection but increases security. Aggressive: Choose this mode if you want a faster connection, but with lowered security. In Aggressive Mode there are fewer key exchanges between the initiator and the receiver. Both sides exchange information even before there is a secure channel. This feature creates a faster connection but with less security than Main Mode.

Field	Description
Remote ID/Local ID	To set up remote and local identity, keep empty to remove identity setting. This can be an IP address (specified as dotted quad or as a Fully Qualified Domain Name, **which will be resolved immediately**) or as a Fully Qualified Domain Name itself (prefixed by "@" to signify that **it should not be resolved**)
IKE SA Parameters	
Encryption Algorithm	The available encryption algorithms are, **DES**, **3DES**, **AES128**, **AES192**, and **AES256**.
Authentication Algorithm	The available authentication algorithms are **MD5** and **SHA1**.
Diffie-Hellman (DH) Group	Choose a DH group to set the strength of the algorithm in bits: Group 1 (768 bits) and Group 2 (1024bits).
Pre Shared Key	Enter an alpha-numeric key to be shared with IKE peer.
Enable Dead Peer (DPD) Detection	This function is not necessary for an IKE rule, but it will help to keep the connection alive during periods when there is no traffic.
DPD Interval	DPD packet is sent periodically in interval seconds during no data traffic.
DPD Timeout	The connection will be disconnected if there is no DPD response after DPD timeout. Unit is second.
Extended Authentication	
XAUTH Client Enable	When this feature is enabled, the router can authenticate users from an external authentication server such as a RADIUS server. Enable this function only if the router is connected to a XAUTH server.
User Name/Password	Enter the credentials that the router uses to connect to the XAUTH server.

VPN > Site to Site IPSec VPN > IPSec Policy

Field	Description
IPSec Policy	A VPN policy contains IPSec Security Association parameters, which define the connection type and key type. Click the Add Entry button to add another VPN policy. To edit an existing policy, click the pencil icon.
Add Entry	Click the **Add Entry** button to create another IPSec policy.
List of VPN Policies	• Enable Select the enable check box to enable the VPN entry. • Number Show Entry of number. • NAME Show Entry of name
VPN Details	Select one entry of List of VPN Policies, Details of VPN will show all information about VPN Policy.
General	
Enable	Check to Enable IPSec Policy.

Field	Description
Policy Number	Enter an identification number for the policy.
Policy Name	Enter a unique name to be used to bring up the tunnel.
Policy Type	Choose Auto Policy or Manual Policy. The Auto Policy uses the IKE protocol to negotiate random keys for more security. You also must set an IKE policy on the Site to Site IPSec VPN > IKE Policy page The Manual Policy does not use IKE, which makes this policy more simple, but less secure.
Remote Endpoint	Choose how you want to identify the remote gateway for this site-to-site VPN tunnel. Choose IP Address to enter an IP address, choose FQDN to enter a Fully Qualified Domain Name, or choose Any (available only for an Auto Policy). Be aware that an FQDN requires that the router can connect to a DNS server to resolve the address before establishing the VPN tunnel.
Encryption Algorithm	Choose DES, 3DES, AES128, AES192, or AES256.
Integrity Algorithm	Choose MD5 or SHA1.
WAN Interface Name	Choose System Default Route, Ether_WAN1, USB_Modem.
Auto Policy Parameters	
PFS	When used in the memo Perfect Forward Secrecy (PFS) refers to the notion that compromise of a single key will permit access to only data protected by a single key. For PFS to exist the key used to protect transmission of data MUST NOT be used to derive any additional keys, and if the key used to protect transmission of data was derived from some other keying material, that material MUST NOT be used to derive any more keys.
SA Lifetime	Enter the IPSec SA life time in seconds. The default value is 7800, which is 130 minutes.
Local Traffic Selection	
Local IP	Choose the type of identifier that you want to use (IP Address or IP Address and Subnet Mask) for the local group that is allowed to pass through this tunnel then enter the identifier(s).
IP Address	Enter the IP Address.
Subnet Mask	
Remote Traffic Selection	
Remote IP	Choose the type of identifier that you want to use (IP Address or IP Address and Subnet Mask) for the local group that is allowed to pass through this tunnel then enter the identifier(s).
IP Address	Enter the IP Address.
Select IKE Policy	Choose an IKE policy to associate with this IPSec Policy. To view all IKE policies in a table, click the View IKE Table button.

VPN > GRE Tunnel

Field	Description
GRE Tunnel	Generic Routing Encapsulation (GRE) is a tunneling protocol developed by Cisco that can encapsulate a wide variety of network layer protocol packet type inside IP tunnels, creating a virtual point-to-point link to Cisco routers at remote points over an IP Internet network.
Add Entry	Click the **Add Entry** button to create another GRE tunnel
Summary GRE Tunnel	• Number Displayed here is the number which you selected. • Status Displayed here is the status of the tunnel. Tunnel Name Displayed here is the name of the tunnel.
GRE Details	Select one GRE tunnel of Summary GRE tunnel, GRE Details will show all Information about GRE. (like Status, Checksum, Sequence, Key, Key Value, Tunnel Name, Destination IP or HostName and Remote IP Address / Subnet mask)
GRE IP Tunnel	
Tunnel Number	Choose an identification number for this tunnel.
Tunnel Name	Enter a name to describe this tunnel.
Enable	Check the box to enable the tunnel, or uncheck the box to disable the tunnel.
Checksum	Choose **Input**, **Output**, **Both**, or **None**. **Input** requires that all inbound packets have the correct checksum. **Output** requires the checksums for outbound packets. **Both** require the checksum for all inbound and outbound packets. The default is **None**.
Sequence	Choose **None**, **Both**, **Input**, or **Output**. **Output** requires a sequence number for outbound packets. **Input** requires a sequence number for inbound packets. **Both** require a sequence number for inbound and outbound packets. The default is **None**. If sequence number check is set as **Input** or **Both** in receiver side, when sender side GRE session restart, the connection will be resumed after the sequence number reach the amount that record in previous session.
Key	Choose **Input**, **Output**, **Both**, or **None**. **Output** requires a key for outbound packets. **Input** requires a key for inbound packets. **Both** require a key for inbound and outbound packets. The default is **None**.
Key Value	If you chose **Input**, **Output**, or **Both** for the Key, specify the key by entering a number between 1 and 4294967295.
WAN Interface Name	Choose the WAN interface that is used to create the GRE Tunnel with the remote host.
Destination IP or HostName	Enter the Destination IP is the address of the remote network or host to which you want to build a tunnel with it.

Field	Description
Remote IP Address/Subnet Mask	Select the Remote IP Address/Subnet Mask for the remote host. You can use the below Add/Delete button to add/delete the pair
Modify Remote IP Address/Subnet Mask	You can input the pair of Remote IP Address and Subnet mask in this field. And then use the **Add** button to add it into the list of Remote IP Address/Subnet Mask. The following is example for this field: 192.168.2.0/24 or 192.168.3.0/32.

VPN > VPN Passthrough

Field	Description
VPN Passthrough	Configure IPSec passthrough if there are devices behind the router that need to set up IPSec tunnels independently, for example, to connect to another router on the WAN.
IPSec Passthrough	Internet Protocol Security (IPSec) is a suite of protocols used to implement secure exchange of packets at the IP layer. IPSec Passthrough is enabled by default. To disable IPSec Passthrough, select **Disabled**.
PPTP Passthrough	Point-to-Point Tunneling Protocol (PPTP) allows the Point-to-Point Protocol (PPP) to be tunneled through an IP network. PPTP Pass-Through is enabled by default. To disable PPTP Passthrough, select **Disabled**.
L2TP Passthrough	Layer 2 Tunneling Protocol is the method used to enable Point-to-Point sessions via the Internet on the Layer 2 level. L2TP Pass-Through is enabled by default. To disable L2TP Passthrough, select **Disabled**.

VPN > Cisco VPN Server

VPN > Cisco VPN Server > Group

Field	Description
Group	The Cisco VPN Server allows mobile users to access Intranet resource via an encrypted (IPSec) VPN tunnel by Cisco Systems VPN Client. The default values of IKE phase 1 and 2 are accepted by Cisco VPN client. Due to system restriction, “Cisco VPN Server” and “Site to Site VPN” are mutually exclusive.
Enable	Click Enable to activate the VPN server. The default is Disable. Enabling the VPN Server will deactivate any site-to-site VPN tunnels that have been defined.
Identify	
Group Name	Cisco VPN Group name used as an identifier for the VPN server. This name must match the group name specified the VPN Client profile. The length can contain up to 32 characters.

Field	Description
Password	Cisco VPN Group password. This password must match the group password specified the VPN Client profile. The length can contain up to 32 characters.
IKE Phase 1	
Exchange Mode	Aggressive mode is applied by default and cannot be changed. This mode is used for negotiating phase one ISAKMP Security Associations (SAs) when using preshared keys for authentication.
ESP Algorithm	Enter an encryption algorithm for the ISAKMP SA.Choices are AES, DES, and 3DES. The default is AES.
AH Algorithm	Hash algorithm for the ISAKMP SA. Choices are MD5 and SHA1. The default is MD5.
Auth Method	Method used to authenticate the remote user. Choices are PSK or PSK+XAUTH. If PSK is selected, then the client will be authenticated if it specifies the correct group name and password. If PSK+XAUTH is selected, then an additional username and password is required.
DH Group	Diffie-Hellman group options. Only 2 [modp 1024], The default is 2 [modp 1024]
IKE Phase 2	
PFS Group	Diffie-Hellman exponentiation group. Choices are: 1 [modp 768], 2 [modp 1024], 5 [modp 1536], 14 [modp 2048], or 15 [modp 3072].
SA Life Time	Defines how long an IPSec SA (security association) will be used. The default is 30 minutes.
Mode Configuration	
Starting IP Address	Starting IP address of the range of addresses that are assigned to the remote client. This range must not be in the same subnet as any VLAN.
Subnet Mask	Subnet mask for the address range assigned to remote clients.
DNS1	Primary DNS server to be used by remote clients.
DNS2	Secondary DNS server to be used by remote clients.
WINS1	Primary WINS server to be used by remote clients.
WINS2	Secondary WINS server to be used by remote clients
Banner	Message displayed to the remote user after they log on. The banner allows up to 500 printable ASCII characters on 1 line.

VPN > Cisco VPN Server > User

Field	Description
VPN Server Users	The Users page contains a list of usernames and passwords that can login to the Cisco VPN Server. Up to 15 unique users can be defined
Add Entry	Add User
List of VPN Server Users	List all the VPN users

Field	Description
User Account	
Username	Username to be provided by the VPN client when using PSK+XAUTH as the authentication method.
Password	Password to be provided by the VPN client when using PSK+XAUTH as the authentication method.
Confirm password	The contents of this field must match the Password field.

Administration module

The Administration module includes these pages:

- Administration > Web Access Management
- Administration > Remote Support
- Administration > Remote Management
- Administration > Time Setup
- Administration > Certificate Management
- Administration > User Management
- Administration > User Privilege Control
- Administration > Log
- Administration > Factory Defaults
- Administration > Firmware Upgrade
- Administration > Backup & Restore
- Administration > Reboot
- Administration > Switch Setting
- Administration > Status

Administration > Web Access Management

Field	Description
Web Access Management	Allows you to change the Router's access settings.
Web Utility Access	To access this web utility, you can use no security by selecting **HTTP** or security by selecting HTTPS. If you select **HTTPS**, be aware that you will need to include https in the address when you connect to the utility. Refer to the following example: https://xxx.xxx.xxx.xxx (the x's represent the Gateway's Internet IP address).
Web Utility Access via Wireless	This feature allows the administrator to access web utility from a wireless device.

Field	Description
Login Banner	
Banner Text	Input the Banner Text, the 1024 character left limitation
Remote Access	
Remote Management	This feature allows you to manage your Gateway from a remote location, via the Internet. If you enable this option and have not changed the router password from the default value, you will be prompted to change the password for security purposes.
Web Utility Access	To access this web utility, you can have no security **HTTP** or security **HTTPS**. For **HTTPS**, enter https://xxx.xxx.xxx.xxx (the x's represent the Gateway's Internet IP address) in your web browser's Address field.
Remote Upgrade	If enabled, the router firmware can be upgraded from Internet.
Allowed Remote IP Address	If you want to access the Router from any external IP address, select **Any IP Address**. If you want to specify an external IP address or range of IP addresses, then select the second option and complete the fields provided.
Remote Management Port	Enter the port number that will be open to outside access

Administration > Remote Support

Field	Description
Remote Support Access	
Collect Device Status Information	Click this button will collect system configuration and useful routing information that can help to debug this system.
Enable Remote Support	Turn on remote debug shell.
Access Port	The debug shell's port number. Default is port 22.

Administration > Remote Management

Administration > Remote Management > TR-069

Field	Description
TR-069	Some service providers can automatically provision your customer premises equipment from a central server. Use the TR-069 page to set up communication with an Auto Configuration Server (ACS).
Status	Click **Enabled** to allow auto-configuration of your router from a central server. Otherwise, click **Disabled**.

Field	Description
ACS URL	Enter the address and port of the ACS server. The format should be http(s)://xxx.xxx.xxx.xxx:port or xxx.xxx.xxx.xxx:port or http(s)://xxx.xxx.xxx.xxx:port/zzzz or xxx.xxx.xxx.xxx/zzz. The X's represent the IP address or domain name. The Z’s represent the URL location. After the colon, enter the port number.
ACS UserName	The default username is OUI-Serial Number; this value should be the same as configured at ACS side and must be filled.
ACS Password	This value should be the same as configured at ACS side and must be filled.
Connection Request Port	This port receives the Connection Request notification from the ACS
Connection Request Username	This value should be the same as configured at ACS side.
Connection Request Password	This value should be the same as configured at ACS side.
Periodic Inform Enable	Choose Enabled to allow the router to periodically initiate connections to the ACS. Otherwise, choose Disabled.
Periodic Inform Interval	Specify the interval (in seconds) at which the router will initiate connections to the ACS. The default value is 86400 seconds, which is 24 hours.
Binding with Loopback Interface	To check the Binding with Loopback Interface box and select a Loopback Interface to bind IP of the interface with TR-069 Connection request URL. The default is unchecked, which is to bind default WAN IP with Connection request URL.
Request Download	Click the Apply button if you want to immediately initiate a connection to the ACS. The ACS may call the Download RPC when it receives the request.
Provisioning Code	This value could be used by ACS to determine service provider-specific customization and provisioning parameters.

Administration > Remote Management > SNMP

Field	Description
SNMP	Simple Network Management Protocol (SNMP) is a popular network monitoring and management protocol that lets you monitor and manage your network from an SNMP manager. SNMP provides a remote means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.
SNMP Setting	
SNMP	To enable SNMP identification, click **Enabled**. To disable SNMP, click **Disabled**.
Trusted IP	Choose Any to allow access from any IP address (not recommended) or enter the IP address and subnet mask of a single SNMP manager or trap agent that can access this router via SNMP.
Get Community	Enter the password that allows read-only access to the Gateway's SNMP information.

Field	Description
Set Community	Enter the password that allows read/write access to the Gateway's SNMP information.
SNMPV3	To enable SNMPV3 function, click **Enabled**. To disable SNMPV3, click **Disabled**.
R/W User	Enter the user name for SNMPV3
Auth-Protocol	Choose SNMPV3 auth protocol, available protocol is “HMAC-MD5” and “HMAC-SHA”
Auth-Password	Enter password for Auth check.
PrivProtocol	Authentication is performed by using a users **privKey** to encrypt the data portion the message being sent.
Privacy Password	Enter the privKey for PrivProtocol to use.
SNMP Trap	To enable SNMP Trap, click **Enabled**. To disable SNMP Trap, click **Disabled**. SNMP Trap can be enabled only when SNMP is enabled
Trap Server	Enter the IP address that trap will be sent to.
Trap Community	Enter the password that allow read access to the SNMP Trap message.
Trap User	Enter the user name for SNMPV3 Trap
Trap Auth- Protocol	Choose SNMPV3 Trap auth protocol, available protocol is "HMAC-MD5" and “HMAC-SHA”.
Trap Auth- Password	Enter SNMPV3 Trap password for Auth check
Trap PrivProtocol	SNMPV3 Trap authentication is performed by using a users **privKey** to encrypt the data portion the message being sent.
Trap Privacy Password	Enter SNMPV3 Trap privKey for PrivProtocol to use.

Administration > Remote Management > Local TFTP

Field	Description
Local TFTP Control	
TFTP	Control TFTP enabled or disabled. Default Enabled.
Get Remote File	
URL	This shows where can get remote file.
Save As	Specify the file name to save
Session Timeout	Maximum time allowed for a connection session. A connection timeout for HTTP and FTP session will be 3 seconds, TFTP will be 1 seconds. For HTTP and FTP, a TCP reset response message will terminate a session.
Retry Sessions	Specify how many sessions are going to retry if transient problem occurred in a session

Field	Description
Status	The status of processing get remote file
File List	• Name This is the name of local file. • Size This is the size of local file.

Administration > Time Setup

Field	Description
Time Zone	Setup the time zone and configure the system time by synchronizing with time server (NTP) or set time manually (Manual Setting).
Time Zone	Select the time zone in which your network functions from this drop-down menu.Time zone is a region of the earth that has uniform standard time, usually referred to as the local time.
NTP	
Time Server Address	If you want to use the device's default Network Time Protocol (NTP) server, use the default setting, Auto. If you want to specify the NTP server, select Manual, and enter the URL or IP address of the NTP server you want to use.
Resync Timer	The timer controls how often the Device resyncs with the NTP server. Enter the number of seconds you want the interval to be, or use the default setting, 3600 seconds.
Enable Daylight Saving	Select this option if you want the device to automatically adjust for daylight saving time. This option is enabled by default
Manual Setting	
Date	date in format “Year/Month/Day”
Time	time in format “Hour:Min:Sec”
Auto Recovery After Reboot	
Auto Recovery After Reboot	When this feature is enabled, the device will recover system time after system reboot.

Administration > Certificate Management

Field	Description
Certificate Management	To support uploading certificate authority file through WEB GUI for TR069 and Provision. Up to 3 certificate authority files can be uploaded for T069 and 1 certificate authority file can be uploaded for Provision.

Field	Description
TR069 - Root CA File List	
Enabled	After uploading certificate authority file, click the check box to allow TR069 using the file in certification. Deselect all check boxes to disable all certificate authority file used by TR069. Please note, only one certificate authority file can be selected in the same time.
CA Name	To set the certificate authority file name in the system.
Select Certificate	To select a certificate authority file in client PC, and click Upload button to uploading the file. After uploading, you can click Enabled check box or click ✖ icon to delete the file.
Provision File List	
Enabled	After uploading certificate authority file, click the check box to allow Provision using the file in certification. Deselect all check boxes to disable all certificate authority file used by Provision.
CA Name	To set the certificate authority file name in the system.
Select Certificate	To select a certificate authority file in client PC, and click Upload button to uploading the file. After uploading, you can click Enabled check box or client ✖icon to delete the file.

Administration > User Management

Administration > User Management > Password Complexity Settings

Field	Description
Password Complexity Settings	
Password Complexity	Click **Enabled** to activate the User Password Complexity. The default is **Disabled**. Password Complexity check Level: • Low - Too Short Password • Low - Passwords cannot be repeated consecutively for three times • Low - Weak Password, use letters & numbers. • Medium - Medium Password, Use special charecters • High - Strong Password • Password is the same as username.

Administration > User Management > User List

Field	Description
User List	Use the User List page to manage the users who have access to the router configuration utility. There are two default accounts. The account with the default username of admin has administrator-level access. The account with the default username of cisco has guest-level access.
User Account	
Username	This is the name to login router.
Level	This shows user's level.
User List	
Username	Enter a new Username. The two default usernames cannot be changed.
Old Password	To ensure the device's security, you will be asked for your old password when you want to change the password. The default administrator password is admin. The default guest password is cisco. Cisco strongly recommends changing the password.
New Password	To ensure the device's security or WRP500's security, you will be asked for your password when you access the device's configuration utility. The default administrator password is admin. The default guest password is cisco. Cisco strongly recommends changing the password
Confirm New Password	Enter the new password again to confirm.
Level	The level of permission for this user: Admin or User. Admin has access to all settings as specified on the Privilege Control page. User has read-only access.

Administration > User Privilege Control

The privilege control provides three access types for all webpages: Read/Write, Read Only and Hidden. The Read/Write means to allow view and configure the items of the webpage. The Read Only means only allow view the webpage. The Hidden means the no any hyperlink to the webpage.

Administration > Log

Administration > Log > Log Setting

Field	Description
Local	
Local	To save log message in memory of router, after reboot, all the logs will disappear.
Log size	Up limit to save log message in memory, the allowed range is 128~1024KB.

Field	Description
USB	
USB	To save log message in external USB storage, if no USB storage plugs in, only “USB disconnect” shows. If USB storage is connected to, user can set
File Name	Filename to be saved into USB disk
Log size	Up limit to save log message in USB storage, the allowed range is 1~512MB
Syslog Server	
Syslog Server	Send out log message to remote syslog server.
IP Address	Enter IP address of remote syslog server
Port	Enter port number that syslog server listen on. Port 514 is chosen by default.
E-Mail	
E-Mail	Send out log message to specific E-Mail address.
Sender	Specify sender's E-Mail address.
Receiver	Specify receiver's E-Mail address.
SMTP Server	Enter mail server address.
SMTP Port	Enter port number that mail server listen on. Port 25 is chosen by default.
Subject	Specify mail subject to send log.
Number of logs	Enter a number to specify how many logs are collected in an E-Mail.
Interval	Enter a time interval to force send out E-Mail if the amount of logs doesn't reach Number of logs
User Name	Enter a user name for mail server authentication.
Password	Enter a password for mail server authentication.

Administration > Log > Log Module

Field	Description
Log Module Settings	
Status	To enable the collection of activity logs, select **Enabled**, and then click Submit. With logging enabled, you can choose to view temporary logs. Click the **Disabled** radio button to disable this function
Log	This drop-down list becomes available if you enable logging and choose log target to decide where the log save to. • Local Save log to system memory • USB Save log to USB disk, only work when USB disk is plugged in. • E-Mail Send log through E-Mail, please setup E-Mail related information in Log Setting page. • Syslog Server Send log to specific log server, please setup log server address in Log Setting page

Administration > Log > Log Viewer

Field	Description
Log Viewer	Allow user to see, download or clean log message save in system memory
Download All Log	Click to download log message in a file to local PC
Clear Log	Click to clean all log message saved in memory.
Display	Choose module to see related log message.
Filter	To filter log message with specific pattern.

Administration > Log > Firewall Log

Field	Description
Firewall Log	Firewall Log provides a functionality that can log certain specified traffic according to the current system firewall, such as SPI and DoS attacking. The traffic that matches the specified firewall rules will be logged. Firewall Log configuration page is shown as below. The description of each configured fields are explained as below.

Field	Description
Firewall Log Settings	
Firewall Log	Enable or disable firewall logging.
Log Level	Level of logging by using the specified syslog level: • 0 Emergency: system is unusable • 1 Alert: action must be taken immediately • 2 Critical: critical conditions • 3 Error: error conditions • 4 Warning: warning conditions • 5 Notice: normal but significant condition • 6 Info: Info messages • 7 Debug: debug-level messages
Log Category	Select which firewall module that is going to be logged and set how many events that generate one log.

Administration > Factory Defaults

Field	Description
Factory Defaults	The *Factory Defaults* screen allows you to restore the Router's Configuration to its Router and/or voice factory default settings. **Note** Restoring the voice defaults may require your login (the default user name and password are **admin**). If the defaults do not work, contact your ITSP for more information.
Factory Defaults	
Restore Router Factory Defaults	To reset the data (router) settings to the default values, select Yes, then click Submit. Any custom data (router) settings you have saved will be lost when the default settings are restored.
Restore Voice Factory Defaults	To reset the voice settings to the default values, select **Yes**, then click Submit. Any custom voice settings you have saved will be lost when the default settings are restored.

Administration > Firmware Upgrade

Field	Description
Firmware Upgrade	The *Firmware Upgrade* screen allows you to upgrade the Router's firmware. You do not need to upgrade the firmware unless you are experiencing problems with the Router or the new firmware has a feature you want to use. Before upgrading the firmware, download the Router's firmware upgrade file from the Cisco website, *www.cisco.com*. Then extract the file. **Note** The Router may lose the settings you have customized. Before you upgrade its firmware, write down all of your custom settings. After you upgrade the firmware, you will have to re-enter all of your configuration settings.
Firmware Upgrade Settings	
Please select a file to upgrade.	In the field provided, enter the name of the extracted firmware upgrade file, or click the **Browse** button to find this file.
Upgrade	After you have selected the appropriate file, click this button, and follow the on-screen instructions.

Administration > Backup & Restore

Administration > Backup & Restore > Default Configuration

Field	Description
Default Configuration	Specifies the Default Configuration settings.
Load Service Provider Default Configuration	Select **Yes** to load Service Provider default configure when do system factory default, select **No** to load Cisco factory default.

Administration > Backup & Restore > Backup Configuration

Field	Description
Backup Configuration	To back up the router's configuration settings
Backup	To back up the Router's configuration settings, click this button and follow the on-screen instructions.

Administration > Backup & Restore > Restore Configuration

Field	Description
Restore Configuration	To backup current configuration in case you need to reset the router back to its factory default settings.
Please select a file to restore	To restore the Router's configuration settings, click this button and follow the on-screen instructions. (You must have previously backed up the Router's configuration settings.)

Administration > Reboot

Click **Reboot** to power cycle the router.

Administration > Switch Setting

Administration > Switch Setting > Port Status

Field	Description
Port Status	Active/Inactive switch wire port. When deactivated, this port cannot do any network function until it is reactivated.
Port Status Setting	
Interface	The wire physical port that support on/off by administrator, don't include wireless or pvc interface.
Enabled	Click to allow network traffic input/output from this physical port. When administrator unclicks this port, LED will be off and traffic cannot pass.

Administration > Switch Setting > Bind MAC to Port

Field	Description
Bind MAC to Port	Enable this function will bind the assigned mac address to one of the LAN ports, and only allow this mac address can access this assigned LAN port but not others port.

Field	Description
Bind MAC to Port Setting	
Adding MAC address	Administrator add new entry to allow network traffic which source MAC come from which physical wire port. • LAN Port The physical wire port that support will bind to this mac address, not include wireless or PVC port. • MAC Address DUT will allow network traffic which source MACs (amount of 16) to match this setting. • Add Button that add this bind LAN Port/MAC address into filter table.
Enable Bind MAC to LAN Port 1	All MAC address entries that LAN Port 1 is relative • Enable click button to on/off Bind MAC address to LAN Port 1 function. • MAC Address address lists that administrator setting at LAN Port 1.
Enable Bind MAC to LAN Port 2	All MAC address entries that LAN Port 2 is relative. • Enable click button to on/off Bind MAC address to LAN Port 2 function. • MAC Address address lists that administrator setting at LAN Port 2.
Enable Bind MAC to LAN Port 3	All MAC address entries that LAN Port 3 is relative. • Enable click button to on/off Bind MAC address to LAN Port 3 function. • MAC Address address lists that administrator setting at LAN Port 3.
Enable Bind MAC to LAN Port 4	All MAC address entries that LAN Port 4 is relative. • Enable click button to on/off Bind MAC address to LAN Port 4 function. • MAC Address address lists that administrator setting at LAN Port 4.

Administration > Status

Field	Description
Status	
CPU	This shows CPU's MIPS, Loads and Uptime - Loads This shows CPU's Loads. - Uptime This shows CPU's Uptime.
Memory	This shows Memory's Total size(%), Free size(%), Used size(%), Buffer size(%), Cached size(%), active size and inactive size(%). - Total This shows Memory's total size(%). - Free This shows Memory's free size(%). - Used This shows Memory's used size(%). - Buffers This shows Memory's buffer size(%). - Cached This shows Memory's cached size(%). - Active This shows Memory's active size(%). - Inactive This shows Memory's inactive size(%).