

WRP400 Firmware Version 1.00.06

This document describes the updates that have been made since version 1.00.04.c and provides instructions for downloading and installing the new firmware.

- [“Changes since WRP400 Firmware Version 1.00.04.c” on page 1](#)
- [“Upgrading the Firmware for the WRP400” on page 3](#)

Changes since WRP400 Firmware Version 1.00.04.c

New features have been added, existing features have been upgraded, and bugs have been fixed.

New Features

The following new features were added:

- Added the ability to configure a wireless “guest network” to allow guests to connect to the Internet while preventing access to your local network. For instructions, see the *WRP400 User Guide*.
- Added provisioning support for configuring router/data parameters via open (XML-style) format .
- Added VLAN support through a VLAN ID that is included in all outgoing packets. You can configure this VLAN ID through remote provisioning.

NOTE: For information about the new provisioning parameters that support these features, see [“New Provisioning Parameters” on page 5](#).

Enhancements and Bug Fixes

- Upgraded the wireless driver to version 2.0.7-1.
- Upgraded the voice module version 1.0.12(20080529a).
- Updated all Help content in the web-based utility.
- Edited the GUI to address minor issues.
- Modified the IGMP Proxy switch control mechanism to enhance Triple Play performance. Now the router directs multicast packets to the respective LAN ports without using the CPU’s multicast routing.
- Added support for router syslog and debug log.
- Added support for WPS in the web-based utility.
- Added PPPoE Relay in the Advanced Routing page.
- Added DNS Proxy to the Basic Setup page.
- Added ability to detect active LAN clients through the Diagnostics page.
- Fixed an issue with the Internet Access Restriction feature.
- Fixed an issue with DMZ by MAC with a static LAN IP.
- Fixed an issue with incoming logging when Port Range Triggering is enabled.
- Fixed a DHCP lease time issue.
- Fixed an issue with the wireless channel display.
- Resolved an issue with the MS-CHAP protocol.

- Resolved an issue with MAC clone while using remote management.
- Resolved an issue with relay of T.38 packets.
- Fixed an issue with display of time zone settings.
- Resolved an issue with factory reset through the web GUI.
- Resolved an issue with Internet Access Restriction when NAT is disabled.
- Resolved an issue with wireless connectivity after running the setup wizard.
- Resolved an issue with the web GUI firmware login.
- Resolved issue with wireless broadcast under the WPA encryption type.
- Resolved an issue with security LED behavior.
- Improved DTMF detection during a call.
- Improved Voice QoS.
- Fixed an issue with phones displaying incorrect status (fast flashing) when taken off hook.
- Fixed an issue with custom settings not being saved during configuration backup.
- Resolved an issue with the restore configuration function.
- Replaced an expired embedded router certificate.

Upgrading the Firmware for the WRP400

You need to download the firmware from Linksys.com and then install it on the WRP400.

Downloading the Firmware from Linksys.com

1. Start Internet Explorer, and enter the following URL: <http://www.linksys.com>
2. From the menu at the top of the page, select **Support > Technical Support**.
3. Click **Choose a Product**.

NOTE: If you are visiting the site for the first time, you may be prompted to choose your location before continuing.

4. On the *Select Product Category* page, find the *Routers and Access Points* drop-down list. Choose **Wireless Routers**.



5. On the *Choose The Device Wireless Routers* page, scroll down to the end of the page, and then choose **WRP400** from the drop-down list on the left side of the page.



6. On the *WRP400 Downloads* page, choose the hardware version for your device.
7. Under *Firmware*, click the link for the latest version of the firmware.
NOTE: If you are using Windows XP Service Pack 2 (SP2) and Internet Explorer, you may see the “*Pop-up blocked*” message in your browser information bar. If you see this message, click the information bar and select **Temporarily Allow Pop-ups**. Then click the link again.
8. Click **Save** in the *File Download* dialog box that appears.
9. In the *Save As* dialog box, choose a location for the file and then click **Save**.
10. When the download is complete, if prompted, click **Close**.
11. Open the file in WinZip and extract it to a temporary location.

Installing the Firmware

1. Start Internet Explorer, and connect to the web-based utility for the router.

NOTE: The default IP address is 192.168.15.1. When prompted, enter the user name and password. The factory default user name and password are **admin**.

2. During a firmware upgrade, the router may lose the settings that you have customized. To back up your configuration, complete the following steps:

- a. Click **Administration > Config Management**.
- b. Click **Backup** to back up the configuration. Follow the on-screen instructions.

3. Click **Administration > Firmware Upgrade**.

NOTE: The service provider may require a separate login before a firmware upgrade. If you see the *Username & Password* screen, enter the user name and password provided by your service provider. The factory default user name and password are **admin**. After you enter the user name and password, click **OK**.

4. Click **Browse**, and then select the extracted firmware upgrade file.
5. Click **Start to Upgrade**. Follow the on-screen instructions.

New Provisioning Parameters

This section describes the new parameters that are now available for provisioning.

NOTE: A sample XML profile can be generated by using the Linksys profile compiler tool (SPC). For instructions about provisioning, see the *Linksys SPA Provisioning Guide* (available to partners through the Linksys Partner Connection).

Feature/XML Tag	Parameters	Examples
Wireless QoS <WL_QOS>	<WL_QOS>wl_wme,wl_wme_no_ack</WL_QOS> wl_wme: WMM support (Wi-Fi Multimedia); on (enabled) or off (disabled) wl_wme_no_ack: No-acknowledgement option; on (enabled) or off (disabled)	To enable WMM with the No-acknowledgement option turned off: <WL_QOS>wl_wme=on,wl_wme_no_ack=off</WL_QOS>
Internet Access Priority <RT_QOS>	<RT_QOS>QoS,rate_mode>manual_rate</RT_QOS> QoS: Internet access priority; 1 (enabled) or 0 (disabled) rate_mode: Upstream bandwidth type; 0 (manual) or 1 (automatic) manual_rate: Upstream bandwidth rate; numerals from 64 to 50000	To enable Manual QoS and specify the upstream bandwidth rate: <RT_QOS>QoS=1,rate_mode=0,manual_rate=5000</RT_QOS> To enable Auto QoS: <RT_QOS>QoS=1,rate_mode=1</RT_QOS> To disable QoS: <RT_QOS>QoS=0</RT_QOS>
QoS Category Priority Rule <QOS_PRIORITY_RULE>	<QOS_PRIORITY_RULE>category_number,name,priority,port_range</QOS_PRIORITY_RULE> category_num: QoS Category number; 1 (application), 2 (online game), 3 (MAC address), 4 (Ethernet port) name: Name string, corresponding to the selected category Application: The name of the application Online Games: The name of the game MAC Address: The MAC address in the format xx:xx:xx:xx:xx:xx Ethernet Port: The port; Ethernet Port 1, Ethernet Port 2, Ethernet Port 3, or Ethernet Port 4 priority: Priority; 0 (Low), 1 (Normal), 2 (Medium), 3 (High) port_range: The port range; start;end;protocol start: The first port number in the range end: The final port number in the range protocol: 0 (Both), 1 (TCP), 2 (UDP)	To configure a rule for an application: <QOS_PRIORITY_RULE>category_num=1,name=ap1,priority=3,port_range=111;222;0;333;444;1</QOS_PRIORITY_RULE> To configure a rule for an online game: Format 1 (default game): <QOS_PRIORITY_RULE>category_number=2,name,priority</QOS_PRIORITY_RULE> Example: <QOS_PRIORITY_RULE>category_num=2,name=Age of Empires,priority=2</QOS_PRIORITY_RULE> Format 2 (with port range): <QOS_PRIORITY_RULE>category_number=2,name,priority,port_range</QOS_PRIORITY_RULE><QOS_PRIORITY_RULE>category_num=2,name=game1,priority=1,port_range=555;666;1</QOS_PRIORITY_RULE> To configure a rule for a MAC Address: <QOS_PRIORITY_RULE>category_num=3,name=mac1,priority=1,mac=00:02:03:04:05:06</QOS_PRIORITY_RULE> To configure a rule for an Ethernet port: <QOS_PRIORITY_RULE>category_num=4,name=Ethernet Port 1,priority=0</QOS_PRIORITY_RULE> To delete all rules: <QOS_PRIORITY_RULE></QOS_PRIORITY_RULE>
Basic Wireless Settings for Primary Network <WL_BASIC_SET_1>	<WL_BASIC_SET_1>wl_net_mode,wl_closed,wl_ssid</WL_BASIC_SET_1> wl_net_mode: Network mode; mixed, b-only, g-only, or disabled wl_closed: SSID broadcast status; 1 (disabled) or 0 (enabled) wl_ssid: Wireless network name; enter 1 to 32 ASCII characters (backslash character not allowed)	To enable SSID-1 and specify the SSID name: <WL_BASIC_SET_1>wl_net_mode=g-only,wl_closed=0,wl_ssid=aaabbb</WL_BASIC_SET_1> To configure SSID-1 as a Wireless B network: <WL_BASIC_SET_1>wl_net_mode=b-only,wl_ssid=aaabbb</WL_BASIC_SET_1> To disable SSID-1: <WL_BASIC_SET_1>wl_net_mode=disabled</WL_BASIC_SET_1>

Feature/XML Tag	Parameters	Examples
Basic Wireless Settings for Secondary or Guest Network <WL_BASIC_SET_2>	<WL_BASIC_SET_2>wl1_net_mode_tmp,wl1_closed,wl1_ssid,ap_isolation</WL_BASIC_SET_2> IMPORTANT: The secondary network can be enabled only when when wl_net_mode is enabled for the primary network. wl1_net_mode_tmp: Network mode; 1 (enabled), 0 (disabled) wl1_closed: SSID broadcast status; 1 (disabled) or 0 (enabled) wl1_ssid: Wireless network name; enter 1-32 ASCII characters (backslash character not allowed) ap_isolation: For Internet Only Access (Guest Network); 1 (disabled) or 0 (enabled) ctrl_ssid2: Allows Service Provider to lock SSID2; when enabled, user will not be able to configure SSID2 from the device GUI; 1 (enabled) or 0 (disabled)	To enable SSID-2 and specify the SSID name, with guest network: <WL_BASIC_SET_2>wl1_net_mode_tmp=1,wl1_closed=0,wl1_ssid=cccd,ap_isolation=1</WL_BASIC_SET_2> To disable SSID-2: <WL_BASIC_SET_2>wl1_net_mode_tmp=0</WL_BASIC_SET_2> To enable SSID-2 guest network: <WL_BASIC_SET_2>ap_isolation=1</WL_BASIC_SET_2> To prevent SSID-2 configuration from the device GUI: <WL_BASIC_SET_2>ctrl_ssid2=0</WL_BASIC_SET_2>
Wireless Security for SSID1 <WL_SECURITY_SET_1> Wireless Security for SSID2 <WL_SECURITY_SET_2>	<WL_SECURITY_SET_1>wl_security_mode2=[mode],[parameters]</WL_SECURITY_SET_1> <WL_SECURITY_SET_2>wl1_security_mode2=[mode],[parameters]</WL_SECURITY_SET_1> wl_security_mode2: Security mode for SSID1 wl1_security_mode2: Security mode for SSID2 Acceptable values are WEP, WPA Personal, WPA2 Personal, WPA Enterprise, WPA2 Enterprise, or Disabled	To disable Wireless Security 1: <WL_SECURITY_SET_1>wl_security_mode2=disabled</WL_SECURITY_SET_1> To disable Wireless Security 2: <WL_SECURITY_SET_1>wl1_security_mode2=disabled</WL_SECURITY_SET_1>
	WEP Parameters wl_wep_bit: WEP encryption; 64 (64 bits 10 hex digits) or 128 (128 bits 26 hex digits) wl_passphrase: WEP passphrase; enter 1 to 16 ASCII characters wl_key1: Key 1; 10 or 26 hex wl_key2: Key 2; 10 or 26 hex wl_key3: Key 3; 10 or 26 hex wl_key4: Key 4; 10 or 26 hex wl_key: WEP transmission key; numerals from 1 to 4	To enable Wireless WEP 1 and specify the passphrase and keys: <WL_SECURITY_SET_1>wl_security_mode2=wep,wl_wep_bit=64,wl_passphrase=test1,wl_key1=81461A688C,wl_key2=A8B0AFDB8F,wl_key3=B99D3E230B,wl_key4=B9EF3E6ACD,wl_key=4</WL_SECURITY_SET_1> To enable Wireless WEP 2 and specify the passphrase and keys: <WL_SECURITY_SET_2>wl1_security_mode2=wep,wl1_wep_bit=64,wl1_passphrase=test2,wl1_key1=8542E268D6,wl1_key2=FFD9405B8B,wl1_key3=25C9B8C5BB,wl1_key4=73B13791B2,wl1_key=4</WL_SECURITY_SET_2>
	WPA Personal and WPA2 Personal Parameters wl_crypto: WPA personal and WPA Enterprise algorithms; tkip (TKIP) or aes (AES) wl1_crypto: WPA2 personal and WPA2 Enterprise algorithms; tkip+aes (TKIP+AES) or aes (AES) wl_wpa_psk: WPA shared key; enter from 8 to 63 ASCII characters wl_wpa_gtk_rekey: WPA group key renewal; numerals from 600 to 7200	To enable Wireless WPA Personal, specify the keys and set the renewal rate: <WL_SECURITY_SET_1>wl_security_mode2=wpa_personal,wl_crypto=aes,wl_wpa_psk=personal,wl_wpa_gtk_rekey=700</WL_SECURITY_SET_1> To enable Wireless WPA2 Personal, specify the keys and set the group key renewal: <WL_SECURITY_SET_1>wl_security_mode2=wpa2_personal,wl_crypto=aes,wl_wpa_psk=personal,wl_wpa_gtk_rekey=700</WL_SECURITY_SET_1>

Feature/XML Tag	Parameters	Examples
Wireless Security, continued	WPA Enterprise and WPA2 Enterprise Parameters wl_crypto: WPA algorithms; tkip (TKIP) or aes (AES) wl_radius_ipaddr: RADIUS server address wl_radius_port: RADIUS port number; numerals from 1 to 65535 wl_radius_key: RADIUS shared key; enter from 1 to 79 ASCII characters wl_wpa_gtk_rekey: Key renewal timeout; numerals from 600 to 7200	To enable WPA Enterprise and specify the RADIUS information: <WL_SECURITY_SET_1>wl_security_mode2=wpa_enterprise,wl_crypto=aes,wl_radius_ipaddr= 192.168.15.111,wl_radius_port=6666,wl_radius_key=enterprise,wl_wpa_gtk_rekey=666</WL_SECURITY_SET_1> To enable WPA2 Enterprise and specify the RADIUS information: <WL_SECURITY_SET_1>wl_security_mode2=wpa2_enterprise,wl_crypto=aes,wl_radius_ipaddr=192.168.15.111,wl_radius_port=6666,wl_radius_key=enterprise,wl_wpa_gtk_rekey=666</WL_SECURITY_SET_1>
RTSP <RTSP>	<RTSP>rtsp_enable</RTSP> rtsp_enable: Real Time Streaming Protocol (RTSP); 1 (enabled) or 0 (disabled)	To enable RTSP: <RTSP>rtsp_enable=1</RTSP> To disable RTSP: <RTSP>rtsp_enable=0</RTSP>
IGMP <IGMP>	<IGMP>force_igmp_version,multicast_pass,multicast_immediate_leave</IGMP> force_igmp_version: Specifies the version of IGMP that is supported; 1 (IGMP v1, RFC 1112), 2 (IGMP v2, RFC 2236) or 3 (IGMP v3, RFC 3376) multicast_pass: IGMP proxy, allows multicast traffic through the router for your multimedia application devices; 1 (enabled) or 0 (disabled) multicast_immediate_leave: Allows immediate channel swapping or flipping without lag or delays; 1 (enabled) or 0 (disabled)	To specify IGMP version 1 with multicast pass through and immediate leave: <IGMP>force_igmp_version=1,multicast_pass=1,multicast_immediate_leave=1</IGMP>
UPnP <UPNP>	<UPNP>upnp_enable,upnp_config,upnp_keep_portmap,upnp_internet_dis</UPNP> upnp_enable: UPnP status; 1 (enabled) or 0 (disabled) upnp_config: Allows configuration of UPnP; 1 (enabled) or 0 (disabled) upnp_keep_portmap: Keeps UPnP configurations after system reboot; 1 (enabled) or 0 (disabled) NOTE: This parameter applies only if upnp_config is enabled. upnp_internet_dis: Prevents Internet access; 1 (Internet access is disabled) or 0 (Internet access is allowed)	To allow users to config UPnP: <UPNP>upnp_enable=1,upnp_config=1</UPNP> To allow user to config UPnP ,and save this config even after system reboot: <UPNP>upnp_enable=1,upnp_config=1,upnp_keep_portmap=1</UPNP> To allow user to enable or disable Internet access through Enable/Stop "upnp Device": <UPNP>upnp_enable=1,upnp_internet_dis=1</UPNP> To allow user to do any UPnP function: <UPNP>upnp_enable=1,upnp_config=1,upnp_keep_portmap=1,upnp_internet_dis=1</UPNP>
LAN DHCP <LAN_DHCP>	<LAN_DHCP>dhcp_lease,dhcp_default_lease</LAN_DHCP> dhcp_lease: Client lease time in minutes; numerals from 1 to 9999 dhcp_default_lease: Default lease time in minutes; numerals from 1 to 9999 NOTE: Dhcp_default_lease allows the Service Provider to configure the length of the "default lease time." By default, the client lease time is set to "0," meaning 1 day.	To set the client lease time: <LAN_DHCP>dhcp_default_lease=888</LAN_DHCP> To set lease time and default lease time: <LAN_DHCP>dhcp_lease=777,dhcp_default_lease=888</LAN_DHCP>

Feature/XML Tag	Parameters	Examples
Switch Rate <SWITCH_RATE>	<SWITCH_RATE>mv_switch_total_rate_limit</SWITCH_RATE> mv_switch_total_rate_limit: Limits the switch throughput; numerals from 1 to 200 (default is 4) NOTE: The switch rate is set by dividing 200 by the mv_switch_total_rate_limit. With the default value of 4, the throughput is limited to 50Mbps. IMPORTANT: It is highly recommended to keep the default switch rate settings. Default settings have been tested to support the appropriate Quality of Service for the IPTV video transmission towards the set-top box, in addition to maintaining the appropriate Quality of Service of the Voice Telephony transmission.	To set the switch rate limit to 40 Mbps: <SWITCH_RATE>mv_switch_total_rate_limit=5</SWITCH_RATE>
WAN Type <WAN_TYPE>	<WAN_TYPE>wan_proto=[mode],[parameters]</WAN_TYPE> wan_proto: Internet connection type; dhcp, static, pppoe, pptp, l2tp, heartbeat DHCP Parameters No other settings are required.	To configure a DHCP connection: <WAN_TYPE>wan_proto=dhcp</WAN_TYPE>
	Static IP Parameters wan_ipaddr: WAN IP address wan_netmask: WAN subnet mask wan_gateway: Gateway IP address	To configure a Static IP connection: <WAN_TYPE>wan_proto=static,wan_ipaddr=192.168.0.11,wan_netmask=255.255.255.128,wan_gateway=192.168.0.252</WAN_TYPE>
	PPPoE (Point-to-Point Protocol over Ethernet) Parameters ppp_username: User name; enter from 1 to 63 ASCII characters ppp_passwd: Password; enter from 1 to 63 ASCII characters ppp_service: Service name; enter from 0 to 63 ASCII characters	To configure a PPPoE connection: <WAN_TYPE>wan_proto=pppoe,ppp_username=adc,ppp_passwd=def</WAN_TYPE> To configure a PPPoE connection type and specify a service name: <WAN_TYPE>wan_proto=pppoe,ppp_username=adc,ppp_passwd= def,ppp_service=aaa</WAN_TYPE>
	PPTP (Point-to-Point Tunneling Protocol) Parameters wan_ipaddr: WAN IP address wan_netmask: WAN subnet mask pptp_server_ip: PPTP server IP address ppp_username: User name; enter from 1 to 63 ASCII characters ppp_passwd: Password; enter from 1 to 63 ASCII characters	To configure a PPTP connection: <WAN_TYPE>wan_proto=pptp,ppp_username=adc,ppp_passwd=def,wan_ipaddr=192.168.0.18,wan_netmask=255.255.255.0,pptp_server_ip=192.168.0.251</WAN_TYPE>
	L2TP (Layer 2 Tunneling Protocol) Parameters l2tp_server_ip: Server IP address ppp_username: User name; enter from 1 to 63 ASCII characters ppp_passwd: Password; enter from 1 to 63 ASCII characters	To configure an L2TP connection: <WAN_TYPE>wan_proto=l2tp,ppp_username=adc,ppp_passwd=def,l2tp_server_ip=192.168.0.15</WAN_TYPE>

Feature/XML Tag	Parameters	Examples
WAN Type, <i>continued</i>	Heartbeat for Telstra Cable Network Parameters hb_server_ip: Heartbeat server IP address ppp_username: User name; enter from 1 to 63 ASCII characters ppp_passwd: Password; enter from 1 to 63 ASCII characters	To configure a Telstra Cable connection: <code><WAN_TYPE>wan_proto=heartbeat,ppp_username=adc,ppp_passwd=def,hb_server_ip=192.168.0.16</WAN_TYPE></code>
		Fail Pattern: <code><WAN_TYPE>wan_proto=dhcpd</WAN_TYPE></code> <code><WAN_TYPE>wan_proto=static,wan_ipaddr=192.168.0.11,wan_netmask=255.255.255.128</WAN_TYPE></code> <code><WAN_TYPE>wan_proto=l2tp,ppp_passwd=def,l2tp_server_ip=192.168.0.15</WAN_TYPE></code> <code><WAN_TYPE>wan_proto=heartbeat,ppp_username=adc,ppp_passwd=def</WAN_TYPE></code> <code><WAN_TYPE>wan_proto=static,wan_ipaddr=aaabbb,wan_netmask=255.255.255.128,wan_gateway=192.168.0.252</WAN_TYPE></code>
PPP Demand <code><PPP_DEMAND></code>	<code><PPP_DEMAND>ppp_demand,ppp_redialperiod</PPP_DEMAND></code> ppp_demand: PPP Demand Type; 1 (Connect on Demand) or 0 (Keep Alive) ppp_idletime: Maximum idle time in minutes; numerals from 1 to 9999 ppp_redialperiod: Redial period in seconds; numerals from 2 to 180	To configure PPP to connect on demand: <code><PPP_DEMAND>ppp_demand=1,ppp_idletime=666</PPP_DEMAND></code>
		To configure PPP to keep alive: <code><PPP_DEMAND>ppp_demand=0,ppp_redialperiod=77</PPP_DEMAND></code> Fail Pattern: <code><PPP_DEMAND>ppp_demand=1,ppp_idletime=66666</PPP_DEMAND></code> <code><PPP_DEMAND>ppp_demand=0,ppp_redialperiod=777</PPP_DEMAND></code> <code><PPP_DEMAND>ppp_demand=1</PPP_DEMAND></code> <code><PPP_DEMAND>ppp_demand=0</PPP_DEMAND></code> <code><PPP_DEMAND>ppp_demand=1,ppp_redialperiod=77</PPP_DEMAND></code> <code><PPP_DEMAND>ppp_demand=0,ppp_idletime=666</PPP_DEMAND></code>
WAN Host <code><WAN_HOST></code>	<code><WAN_HOST>wan_hostname=host_test,wan_domain=domain</WAN_HOST></code> wan_hostname: WAN hostname; enter from 0 to 39 ASCII characters wan_domain: WAN domain name; enter from 0 to 63 ASCII characters	To specify a WAN hostname and WAN domain name: <code><WAN_HOST>wan_hostname=host_test,wan_domain=domain_test</WAN_HOST></code> To specify a WAN hostname only: <code><WAN_HOST>wan_hostname=host_test</WAN_HOST></code> To specify a WAN domain name only: <code><WAN_HOST>wan_domain=domain_test</WAN_HOST></code>

Feature/XML Tag	Parameters	Examples
WAN MTU <WAN_MTU>	<WAN_MTU>mtu_enable</WAN_MTU> mtu_enable: MTU mode; 0 (automatic) or 1 (manual) wan_mtu: MTU size; if MTU mode is manual, enter a numeral from 576 to 1500 NOTE: The default size depends on the Internet Connection Type: - DHCP or Static IP: 1500 - PPPoE: 1492 - PPTP or L2TP: 1460 - Telstra Cable: 1500	To enable MTU in Auto mode: <WAN_MTU>mtu_enable=0</WAN_MTU> To enable MTU in Manual mode and specify the MTU size: <WAN_MTU>mtu_enable=1,wan_mtu=888</WAN_MTU> To enable MTU in Manual mode without specifying the MTU size: <WAN_MTU>mtu_enable=1</WAN_MTU> Fail Pattern <WAN_MTU>mtu_enable=0,wan_mtu=999</WAN_MTU> <WAN_MTU>wan_mtu=777</WAN_MTU>
WAN DNS <WAN_DNS>	<WAN_DNS>wan_dns</WAN_DNS> wan_dns: DNS IP address; separate multiple addresses with a space	To specify one DNS address: <WAN_DNS>wan_dns=192.168.0.21</WAN_DNS> To specify multiple DNS addresses: <WAN_DNS>wan_dns=192.168.0.21 192.168.0.22</WAN_DNS><WAN_DNS>wan_dns=192.168.0.21 192.168.0.22 192.168.0.23</WAN_DNS> Fail Pattern <WAN_DNS>wan_dns=aaabbb</WAN_DNS> <WAN_DNS>wan_dns=192.168.0.21 192.168.0.aa</WAN_DNS> <WAN_DNS>wan_dns=192.168.0.21 192.168.0.22 192.168.0.23 192.168.0.23</WAN_DNS>
DHCP Reservation <DHCP_RESERVATION>	<DHCP_RESERVATION>dhcp_statics=name;mac;ip</DHCP_RESERVATION> dhcp_statics: Identifies the client name: A name for this reservation mac: The MAC address of the client; enter the MAC address without hyphens ip: The IP address of the client	To create two reservations (R51 and R52) for two clients: <DHCP_RESERVATION>dhcp_statics=R51;00:0E:35:6B:56:78;100</DHCP_RESERVATION><DHCP_RESERVATION>dhcp_statics=R52;00:0E:35:6B:34:56;101</DHCP_RESERVATION> To delete all reservations: <DHCP_RESERVATION></DHCP_RESERVATION>

Feature/XML Tag	Parameters	Examples
Single Port Forwarding <SINGLE_PORT_FORWARDING>	<SINGLE_PORT_FORWARDING>forward_single=name:on off:both tcp udp:external-port:internal-port:ip</SINGLE_PORT_FORWARDING> NOTE: To configure port forwarding, you also should configure a DHCP reservation for the designated server. forward_single: Supports port forwarding on the specified port name: Application name on off: on (enabled) or off (disabled) both tcp udp: Selected protocol; tcp, udp, or both external-port: The external port number internal-port: The internal port number ip: The IP address of the PC that should receive the requests.	To forward FTP to 192.168.15.18: <SINGLE_PORT_FORWARDING>forward_single=FTP:on:tcp:21:21:18</SINGLE_PORT_FORWARDING> To configure port forwarding for non-standard applications: <SINGLE_PORT_FORWARDING>forward_single=fw1:on:both:1111:2222:28</SINGLE_PORT_FORWARDING> <SINGLE_PORT_FORWARDING>forward_single=fw2:off:tcp:3333:4444:29</SINGLE_PORT_FORWARDING> <SINGLE_PORT_FORWARDING>forward_single=fw3:on:udp:5555:6666:30</SINGLE_PORT_FORWARDING> To delete all: <SINGLE_PORT_FORWARDING></SINGLE_PORT_FORWARDING> To configure port forwarding for default standard applications such as FTP, Telnet, SMTP, and others: <SINGLE_PORT_FORWARDING>forward_single=FTP:on:tcp:21:21:18</SINGLE_PORT_FORWARDING> <SINGLE_PORT_FORWARDING>forward_single=Telnet:on:tcp:23:23:19</SINGLE_PORT_FORWARDING> <SINGLE_PORT_FORWARDING>forward_single=SMTP:on:tcp:25:25:20</SINGLE_PORT_FORWARDING> <SINGLE_PORT_FORWARDING>forward_single=DNS:on:udp:53:53:21</SINGLE_PORT_FORWARDING> <SINGLE_PORT_FORWARDING>forward_single=TFTP:on:udp:69:69:22</SINGLE_PORT_FORWARDING> <SINGLE_PORT_FORWARDING>forward_single=Finger:on:tcp:79:79:23</SINGLE_PORT_FORWARDING> <SINGLE_PORT_FORWARDING>forward_single=HTTP:on:tcp:80:80:24</SINGLE_PORT_FORWARDING> <SINGLE_PORT_FORWARDING>forward_single=POP3:on:tcp:110:110:25</SINGLE_PORT_FORWARDING> <SINGLE_PORT_FORWARDING>forward_single=NNTP:on:tcp:119:119:26</SINGLE_PORT_FORWARDING>

Feature/XML Tag	Parameters	Examples
Port Range Forwarding <PORT_RANGE_FORWARDING>	<PORT_RANGE_FORWARDING>forward_single=name:on off:both tcp udp:port range start:port range end:ip</PORT_RANGE_FORWARDING> NOTE: To configure port forwarding, you also should configure a DHCP reservation for the designated server. forward_port: Supports port forwarding on a range of ports name: Application name on off: On (Enabled or off (Disabled both tcp udp: Selected protocol; tcp, udp, or both external-port: The external port number internal-port: The internal port number ip: The IP address of the PC running the specific application.	To allow forwarding on two specified port ranges: <PORT_RANGE_FORWARDING>forward_port=prf1:on:tcp:555:666:18</PORT_RANGE_FORWARDING> <PORT_RANGE_FORWARDING>forward_port=prf2:on:both:777:888:19</PORT_RANGE_FORWARDING> To delete all: <PORT_RANGE_FORWARDING></PORT_RANGE_FORWARDING>
Port Range Triggering <PORT_RANGE_TRIGGERING>	<PORT_RANGE_TRIGGERING>port_trigger=name:on off:trigger start:trigger end:forward start:forward end</PORT_RANGE_TRIGGERING> port_trigger: Supports port range triggering name: Application name on off: On (enabled) or Off (disabled) trigger start:trigger end: Triggered range forward start:forward end: Forwarded range	To configure two port range triggers: <PORT_RANGE_TRIGGERING>port_trigger=prt1:on:111:222:333:444</PORT_RANGE_TRIGGERING> <PORT_RANGE_TRIGGERING>port_trigger=prt2:on:555:666:777:888</PORT_RANGE_TRIGGERING> To delete all: <PORT_RANGE_TRIGGERING></PORT_RANGE_TRIGGERING>
VLAN <WAN_VLAN>	<WAN_VLAN>wan_vlan_enable,wan_vlan_id</WAN_VLAN> wan_vlan_enable: VLAN status; 1 (enabled) 0 (disabled) wan_vlan_id: VLAN ID number	To enable VLAN and specify the VLAN ID: <WAN_VLAN>wan_vlan_enable=1,wan_vlan_id=123</WAN_VLAN> To disable VLAN: <WAN_VLAN>wan_vlan_enable=0</WAN_VLAN>
Router Syslog <ROUTER_SYSLOG>	<ROUTER_SYSLOG>log_provision</ROUTER_SYSLOG> log_provision: Type of log; 0 (console display), 1 (system log), or 2 (console display and system log)	To configure console display and system log: <ROUTER_SYSLOG>log_provision=2</ROUTER_SYSLOG>