ELTEK A7200-G1

Wireless
Broadband Router

User Manual

V1.1
20140505

INDEX

1. Introduction

The ELTEK A7200-G1 supports Annex A mode. It provides four 10/100 Base-T Ethernet ports for user. The device provides high-speed broadband connection to the Internet or Intranet for high-end users, such as net bars and office users.

It provides high performance access to the Internet, downstream up to 24 Mbps and upstream up to 1 Mbps. The device supports WLAN access to the Internet, such as WLAN AP or WLAN device. It complies with IEEE 802.11b/g, IEEE 802.11n specifications, WEP, WPA, and WPA2 security specifications.

You can configure the router by running the Setup Wizard in the CD-ROM provided in the package. The wizard provides quick setup for Internet and Wireless connection. When you start the Setup Wizard, Please follow the easy steps in Quick Installation Guide.

2. System Overview

2.1 General Description

Eltek A7200-G1/G2 is only a component of a hospital screen solution project.
The A7200-G1/G2 is just built-into the screen from customer.
Customer will later do the whole procedure for certification with their final product (such as hospital screen).

To ensure fully compatibility, the device was tested with all major AMs, and support standard 10/100 Mbps Base-T Ethernet interface Auto MDI/MDIx 10/100 Switch function allowing user easily to link to PC or other Switches/Hubs. The device is an idea solution for multi-users utilizing build-in channel mode (PPPoE/A, IPoA, IPoE), IP routing, NAT functionalities sharing the link. The device is also a perfect solution for the residential users, it supports the users with bridge mode in host based PPPoE Client.

2.2 Specifications

WLAN features

- Complies with IEEE 802.11b/g/n standards
- Backward compatible with 802.11b/g devices while operating at 802.11n data rate
- One Transmit and one Receive path (1T1R)
- 802.11b/g Data rates : 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54Mbps, 802.11n maximum Data rates :72.2Mbps receive/transmit PHY rate using 20MHz bandwidth, 150Mbps receive/transmit PHY rate using 40MHz bandwidth
- Burst-mode support for dramatically enhanced throughput
- DSSS with DBPSK and DQPSK, CCK modulations and demodulations supported with rate compatible punctured convolution coding with coding rate of 1/2, 2/3, 3/4 and 5/6
- OFDM with BPSK, QPSK, 16QAM and 64QAM modulations and demodulations supported with long and short preamble
- Complies with WMM, 802.11e, and CCX specifications
- Complies with 802.11h, 802.11i, 802.11j specifications
- Hardware-based IEEE 802.11i encryption/decryption engine, including 64-bit/128-bit WEP, TKIP, and AES
- Supports Wi-Fi alliance WPA and WPA2 security

Software features

- RFC-1483/2684 LLC/VC-Mux bridged/routed mode
- RFC-1577 Classical IP over ATM
- RFC-2516 PPPoE
- RFC-2364 PPPoA
- RFC-1661 PPP

- Bridge/Routing
  - DHCP Client/Sever/Relay
  - IP routing : RIP v1/v2
  - Static route
  - DNS Relay Agent
  - Dynamic DNS
  - IGMP Proxy
  - 802.1d Spanning-Tree Protocol
  - NAT (Network Address Translation)
  - NAPT port forwarding
  - DMZ support

- Security
  - User authentication for PPP
  - PAP (Password Authentication Protocol)
  - CHAP (Challenge Authentication Protocol)
- Firewall
  - IP/Port filtering
  - MAC filtering
  -
- ATM
  - ITU-T 1.610 F4/F5 OAM send and receiver loop-back
  - ATM QoS : CBR, rt-VBR, nrt-VBR and UBR
  - Multiple PVC : support 8 PVCs

- Management
  - Web-based configuration
  - Telnet remote management
  - SNMP v1/v2/Trap
  - Diagnostic tool
  - Firmware upgrade through FTP, TFTP and HTTP
  - UPnP support
  - ACL (Access Control List)

3. Hardware Installation

3.1 Hardware Requirements

DC15V Power Adapter

RJ-45 Ethernet cable

3.2 Hardware Setup Procedures

Step3: Connect your notebook / desktop computer to the LAN port of the router.

Step4: Power ON the router.

4. Software Configuration

The device is an wireless router. When you power on the device, the system will boot up. The system provides a PVC for bridge test by default. The default configurations for the system are listed below.

- LAN IP address: **192.168.10.1**, Netmask: **255.255.255.0**

User can change settings via WEB browser. The following sections describe the set up procedures.

Please set your PC's Ethernet port as follow:

- IP address: **192.168.10.XXX *(e.g. 192.168.10.10)***
- Netmask: **255.255.255.0**

Access the Web Console:

- Start your web browser.
- Type the Ethernet IP address of the modem/router on the address bar of the browser. Default IP address is 192.168.10.1.
- Enter Password in the dialog box when it appears. Default Username: **admin** Password: **mpnn01**

This page displays the router's current status and settings. This information is read-only except for the PPPoE/PPPoA channel for which user can connect/disconnect the channel on demand. Click the "Refresh" button to update the status

Function buttons in this page:

Connect / Disconnect

The two buttons take effect only when PVC is configured as PPPoE/PPPoA mode. Click Connect/Disconnect button to connect/disconnect the PPP dial up link.

5. Setup

5.1 WAN Configuration

There are three sub-menu for WAN configuration: [Channel Config], [ATM Settings]

Channel Config

modem/router supports 8 ATM Permanent Virtual Channels (PVCs). There are mainly three operations for each of the PVC channels: add, delete and modify. And there are several channel modes to be selected for each PVC channel. For each of the channel modes, the setting is quite different accordingly. Please refer to the section – Channel Mode Configuration for further details.

Function buttons in this page:

Add

Click Add to complete the channel setup and add PVC channel into configuration.

Modify

Select an existing PVC channel by clicking the radio button at the Select column of the Current ATM VC Table before we can modify the PVC channel. After selecting PVC channel, we can modify the channel configuration at this page. Click Modify to complete the channel modification and apply to the configuration.

Delete

Select an existing PVC channel to be deleted by clicking the radio button at the Select column of the Current ATM VC Table. Click Delete to delete this PVC channel from configuration.

5.1.1 ATM Settings

The page is for ATM PVC QoS parameters setting. The device support 4 QoS mode —CBR/rt-VBR/nrt-VBR/UBR.

Fields in this page:

Field	Description
VPI	Virtual Path Identifier. This is read-only field and is selected on the Select column in the Current ATM VC Table.
VCI	Virtual Channel Identifier. This is read-only field and is selected on the Select column in the Current ATM VC Table. The VCI, together with VPI, is used to identify the next destination of a cell as it passes through the ATM switch.
QoS	Quality of Service, a characteristic of data transmission that measures how accurately and how quickly a message or data is transferred from a source host to a destination host over a network. The four QoS options are: UBR (Unspecified Bit Rate): When UBR is selected, the SCR and MBS fields are disabled. CBR (Constant Bit Rate): When CBR is selected, the SCR and MBS fields are disabled. nrt-VBR (non-real-time Variable Bit Rate): When nrt-VBR is selected, the SCR and MBS fields are enabled. rt-VBR (real-time Variable Bit Rate): When rt-VBR is selected, the SCR and MBS fields are enabled.
PCR	Peak Cell Rate, measured in cells/sec, is the cell rate which the source may never exceed.
SCR	Sustained Cell Rate, measured in cells/sec, is the average cell rate over the duration of the connection.
MBS	Maximum Burst Size, a traffic parameter that specifies the maximum number of cells that can be transmitted at the peak cell rate.

Function buttons in this page:

Apply Changes

Set new PVC OoS mode for the selected PVC. New parameters will take effect after saving into flash memory and reboot the system. See section “Admin” for save details.

Undo
Discard your settings.

5.2 LAN Configuration

Click Setup -> LAN to configure the LAN Settings.

5.2.1 LAN Interface Setup

Following page shows the current setting of LAN interface. You can set IP address, subnet mask, and IGMP Snooping for LAN interface in this page.

Fields in this page:

Field	Description
IP Address	The IP address your LAN hosts use to identify the device's LAN port.
Subnet Mask	LAN subnet mask.
IGMP Snooping	Enable/disable the IGMP snooping function for the multiple bridged LAN ports.

Function buttons in this page:

Apply Changes
Click to save the setting. New parameters will take effect after saving into flash memory and reboot the system. See section "Admin" for save details.

Modify
Click to modify the setting.

5.2.2 DHCP Mode

You can configure your network and device to use the Dynamic Host Configuration Protocol (DHCP). This page provides DHCP instructions for implementing it on your network by selecting the role of DHCP protocol that this device wants to play. There are two different DHCP roles that this device can act as: DHCP Server and DHCP Relay. When acting as DHCP server, you can setup the server parameters at the DHCP Server page; while acting as DHCP Relay, you can setup the relay parameters at the DHCP Relay page.

5.2.2.1 DHCP Server Configuration

Fields in this page:

Field	Description
IP Pool Range	Specify the lowest and highest addresses in the pool.
Max Lease Time	The Lease Time is the amount of time that a network user is allowed to maintain a network connection to the device using the current dynamic IP address. At the end of the Lease Time, the lease is either renewed or a new IP is issued by the DHCP server. The amount of time is in units of seconds. The default value is 86400 seconds (1 day). The value –1 stands for the infinite lease.
Domain Name	A user-friendly name that refers to the group of hosts (subnet) that will be assigned addresses from this pool.
Subnet mask	A mask used to determine what subnet an IP address belongs to.
Default gateway	On a typical small home or office LAN, the existing routes that set up the default gateway for your LAN hosts and for the device provide the most appropriate path for all your Internet traffic
DNS server	It is used to select the way to obtain the IP addresses of the DNS servers.

5.2.2.2 DHCP Relay Configuration

Some ISPs perform the DHCP server function for their customers' home/small office network. In this case, you can configure this device to act as a DHCP relay agent. When a host on your network requests Internet access, the device contacts your ISP to obtain the IP configuration, and then forward that information to the host. You should set the DHCP mode to act as a DHCP relay.

Fields in this page:

Field	Description
Relay Server	If you are using the other DHCP server to assign IP address to your hosts on the LAN. You can set the DHCP server ip address.

5.2.3 DHCP Static Configuration

Static DHCP is as useful feature which makes the DHCP server on your router always assign the same IP address to a unique MAC address assigned to NIC.

Static IP is a manual way of obtaining an IP address for your computer, where the IP address is pre-determined and always the same.

5.3 Wireless Configuration

Click Setup -> WLAN to configure the Wireless settings.

This section provides the wireless network settings for your WLAN interface. The wireless interface enables the wireless AP function for modem.

5.3.1 Basic Setting

This page contains all of the wireless basic settings. Most users will be able to configure the wireless portion and get it working properly using the setting on this screen.

Fields in this page:

Field	Description
Disable Wireless LAN Interface	Check it to disable the wireless function for modem.
Band	Select the appropriate band from the list provided to correspond with your network setting.
Mode	The selections are: AP
SSID	The Service Set Identifier (SSID) or network name. It is case sensitive and must not exceed 32 characters, which may be any keyboard character. The mobile wireless stations shall select the same SSID to be able to communicate with your modem (or AP).
Channel Number	Select the appropriate channel from the list provided to correspond with your network settings. You shall assign a different channel for each AP to avoid signal interference.
Radio Power (mW)	The maximum output power: 15mW, 30mW or 60mW.
Channel Width	20MHz bandwidth : maximum Data rates = 72.2Mbps, 40MHz bandwidth : maximum Data rates = 150Mbps.
Associated Clients	It will show the Wireless clients currently associated with the modem

5.3.2 Wireless Security Setup

This screen allows you to setup the wireless security. Turn on WEP or WPA by using encryption keys to prevent any unauthorized access to your WLAN.

Fields in this page:

Field	Description
Encryption	There are 4 types of security to be selected. To secure your WLAN, it's strongly recommended to enable this feature. • **WEP:** Make sure that all wireless devices on your network are using the same encryption level and key. Click Set WEP Key button to set the encryption key. • **WPA (TKIP):** WPA uses Temporal Key Integrity Protocol (TKIP) for data encryption. TKIP utilized a stronger encryption method and incorporates Message Integrity Code (MIC) to provide protection against hackers. • **WPA2 (AES):** WPA2, also known as 802.11i, uses Advanced Encryption Standard (AES) for data encryption. AES utilized a symmetric 128-bit block data encryption. • **WAP2 Mixed:** The AP supports WPA (TKIP) and WPA2 (AES) for data encryption. The actual selection of the encryption methods will depend on the clients.
Use 802.1x Authentication	Check it to enable 802.1x authentication. This option is selectable only when the "Encryption" is choose to either None or WEP. If the "Encryption" is WEP, you need to further select the WEP key length to be either WEP 64bits or WEP 128bits.
WPA Authentication Mode	There are 2 types of authentication mode for WPA. • **WPA-RADIUS:** WPA RADIUS uses an external RADIUS server to perform user authentication. To use WPA RADIUS, enter the IP address of the RADIUS server, the RADIUS port (default is 1812) and the shared secret from the RADIUS server. Please refer to "Authentication RADIUS Server" setting below for RADIUS setting. The WPA algorithm is selected between TKIP and AES, please refer to "WPA cipher Suite" below. • **Pre-Shared Key:** Pre-Shared Key authentication is based on a shared secret that is known only by the parties involved. To use WPA Pre-Shared Key, select key format and enter a password in the "Pre-Shared Key Format" and "Pre-Shared Key" setting respectively. Please refer to "Pre-Shared Key Format" and "Pre-Shared Key" setting below.
Pre-Shared Key Format	• **PassPhrase:** Select this to enter the Pre-Shared Key secret as user-friendly textual secret. • **Hex (64 characters):** Select this to enter the Pre-Shared Key secret as hexadecimal secret.
Pre-Shared Key	Specify the shared secret used by this Pre-Shared Key. If the "Pre-Shared Key Format" is specified as PassPhrase, then it indicates a passphrase of 8 to 63 bytes long; or if the "Pre-Shared Key Format" is specified as Hex(64 characters), then it indicates a 64-hexadecimal number.
Authentication RADIUS Server	If the WPA-RADIUS is selected at "WPA Authentication Mode", the port (default is 1812), IP address and password of external RADIUS server are specified here.

Function buttons in this page:

Apply Changes

Change the settings. New parameters will take effect after saving current config into flash memory and reboot the system.

5.3.3 Wireless Multiple BSSID Setup

The SSID is a unique identifier that wireless networking devices use to establish and maintain wireless connectivity. You can configure up to 4 SSIDs on your AP router and assign different configuration settings to each SSID. All the SSIDs are active at the same time; that is, client devices can associate to the access point using any of the SSIDs. These are the settings you can assign to each SSID:

Enable VAP0~4

SSID

broadcast SSID

Relay Blocking

Authentication Type

5.3.4 Wireless Access Control

This page allows administrator to have access control by entering MAC address of client stations. MAC address can be added into access control list and only those clients whose wireless MAC address are in the access control list will be either allowed or denied to connect to the wireless AP as per the Access Control policy defined.

Fields in this page:

Field	Description
Wireless Access Control Mode	The Selections are: • **Disable:** Disable the wireless ACL feature. • **Allow Listed:** When this option is selected, no wireless clients except those whose MAC addresses are in the current access control list will be able to connect (to this device). • **Deny Listed:** When this option is selected, all wireless clients except those whose MAC addresses are in the current access control list will be able to connect (to this device).
MAC Address	Enter client MAC address and press “Add” button to add client MAC address into current access control list.

5.3.5 Wireless Advanced Settings

This page allows advanced users who have sufficient knowledge of wireless LAN to configure advanced settings. These setting shall not be changed unless you know exactly what will happen from the changes you made on your device.

Fields in this page:

Fragment Threshold	This value should remain at its default setting of 2346. It 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 increases the “Fragment Threshold” value within the value range of 256 to 2346. Setting this value too low may result in poor network performance. Only minor modifications of this value are recommended.
RTS Threshold	This value should remain at its default setting of 2347. If you encounter inconsistent data flow, only minor modifications are recommended. If a network packet is smaller than the preset “RTS threshold” size, the RTS/CTS mechanism will not be enabled. The modem (or AP) sends Request to Send (RTS) frames to a particular 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.
Beacon Interval	The Beacon Interval value indicates the frequency interval of the beacon. Enter a value between 20 and 1024. A beacon is a packet broadcast by the modem (or AP) to synchronize the wireless network. The default is 100.
Data Rate	The rate of data transmission should be set depending on the speed of your wireless network. You should select from a range of transmission speeds, or you can select Auto to have the modem (or AP) automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the AP and a wireless client. The default setting is Auto.
Preamble Type	The Preamble Type defines the length of the CRC (Cyclic Redundancy Check) block for communication between the AP and mobile wireless stations. Make sure to select the appropriate preamble type. Note that high network traffic areas should use the short preamble type. CRC is a common technique for detecting data transmission errors.
Broadcast SSID	If this option is enabled, clients can see the wireless network. This feature is intended to allow clients to dynamically discover and roam between WLANs; if this option is disabled, the device will hide its SSID. When this is done, the station cannot directly discover its WLAN and MUST be configured with the SSID. Note that in a home Wi-Fi network, roaming is largely unnecessary and the SSID broadcast feature serves no useful purpose. You should disable this feature to improve the security of your WLAN.
Relay Blocking	When Relay Blocking is enabled, wireless clients will not associate with other wireless clients.
Ethernet to Wireless Blocking	When enabled, traffic between Ethernet and wireless interfaces are not allowed.
DTIM Interval	The DTIM Interval determines the number of AP beacons between each Delivery Traffic Indication Message (DTIM). This informs clients of the next window for listening to broadcast and multicast messages. When the AP has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Clients for that AP hear beacons and awaken to receive the broadcast and multicast messages
WIFI Multicast to Unicast	For unicast transmissions, 802.11 implements layer2 acknowledgments and error checking to ensure frame delivery. Multicast traffic, on the other hand, has no link layer error or loss management in the 802.11 standard.

Aggregation	Frame aggregation is a process of packing multiple MSDUs or MPDUs together to reduce the overheads and average them over multiple frames, thus increasing the user level data rate.
Short GI	Guard Intervals (GI) are used to ensure that distinct transmissions do not interfere with one another. Short GI enable = 400ns, disable = 800ns.

5.3.6 WPS (Wi-Fi Pprotected Setup)

Although home Wi-Fi networks have become more and more popular, users still have trouble with the initial set up of network. This obstacle forces users to use the open security and increases the risk of eavesdropping. Therefore, The Wi-Fi Protected Setup (WPS) is designed to ease set up of security-enabled Wi-Fi networks and subsequently network management.

The largest difference between WPS-enabled devices and legacy devices is that users do not need the knowledge about SSID, channel and security settings, but they could still surf in a security-enabled Wi-Fi network.

This device supports Push Button method and PIN method for WPS. The following sub-paragraphs will describe the function of each item. The webpage is shown below.

Fields in this page:

Field	Description
Disable WPS	Check to disable the Wi-Fi protected Setup.
WPS Status	When AP's settings are factory default (out of box), it is set to open security and un-configured state. "WPS Status" will display it as "UnConfigured". If it already shows "Configured", some registrars such as Vista WCN will not configure AP. Users will need to go to the "Backup/Restore" page and click "Reset" to reload factory default settings.
Self-PIN Number	"Self-PIN Number" is AP's PIN. Whenever users want to change AP's PIN, they could click "Regenerate PIN" and then click " Apply Changes". Moreover, if users want to make their own PIN, they could enter four-digit PIN without checksum and then click " Apply Changes". However, this would not be recommended since the registrar side needs to be supported with four-digit PIN.
Push Button Configuration	Clicking this button will invoke the PBC method of WPS. It is only used when AP acts as a registrar.
Client PIN Number	It is only used when users want their station to join AP's network. The length of PIN is limited to four or eight numeric digits. If users enter eight-digit PIN with checksum error, there will be a warning message popping up. If users insist on this PIN, AP will take it.

Function buttons in this page:

Regenerate PIN
Click to regenerate the Self-PIN Number.

Start PBC
Click to start the Push Button method of WPS.

Apply Changes
Click to commit changes.

Reset
It restores the original values.

Start PIN
Click to start the PIN method of WPS.

6. Advanced Setup

The end user can configure the Advance Setup

Route Configuration

The Routing page enables you to define specific route for your Internet and network data. Most users do not need to define routes. On a typical small home or office LAN, the existing routes that set up the default gateways for your LAN hosts and for the device provide the most appropriate path for all your Internet traffic.

On your LAN hosts, a default gateway directs all Internet traffic to the LAN port(s) on the device. Your LAN hosts know their default gateway either because you assigned it to them when you modified your TCP/IP properties, or because you configured them to receive the information dynamically from a server whenever they access the Internet.

On the device itself, a default gateway is defined to direct all outbound Internet traffic to a route at your ISP. The default gateway is assigned either automatically by your ISP whenever the device negotiates an Internet access, or manually by user to setup through the configuration.

6.1 Route Setup

6.1.1 Static Route Setup

You may need to define routes if your home setup includes two or more networks or subnets, if you connect to two or more ISP services, or if you connect to a remote corporate LAN.

Fields in this page:

Field	Description
Enable	Check to enable the selected route or route to be added.
Destination	The network IP address of the subnet. The destination can be specified as the IP address of a subnet or a specific host in the subnet. It can also be specified as all zeros to indicate that this route should be used for all destinations for which no other route is defined (this is the route that creates the default gateway).
Subnet Mask	The network mask of the destination subnet. The default gateway uses a mask of 0.0.0.0.
Next Hop	The IP address of the next hop through which traffic will flow towards the destination subnet.
Metric	Defines the number of hops between network nodes that data packets travel. The default value is 0, which means that the subnet is directly one hop away on the local LAN network.
Interface	The WAN interface to which a static routing subnet is to be applied.

Function buttons in this page:

Add Route

Add a user-defined destination route.

Update

Update the selected destination route under the Static Route Table.

Delete Selected

Delete a selected destination route under the Static Route Table.

Show Routes

Click this button to view the device's routing table.

6.1.2 RIP Configuration

RIP is an dynamic routing Internet protocol. Here you can set up to share routing table information with other routing devices on your LAN, at your ISP's location, or on remote networks connected to your network via the line.

Most small home or office networks do not need to use RIP; they have only one router, such as the Router, and one path to an ISP. In these cases, there is no need to share routes, because all Internet data from the network is sent to the same ISP gateway.

You may want to configure RIP if any of the following circumstances apply to your network:

- Your home network setup includes an additional router or RIP-enabled router (other than the Router). The Router and the router will need to communicate via RIP to share their routing tables.
- Your network connects via the line to a remote network, such as a corporate network. In order for your LAN to learn the routes used within your corporate network, they should both be configured with RIP.
- Your ISP requests that you run RIP for communication with devices on their network.

Fields on the first setting block:

Field	Description
RIP	Enable/Disable RIP feature.

6.2 NAT Configuration

In computer networking, network address translation (NAT) is the process of modifying IP address information in IP packet headers while in transit across a traffic routing device.

6.2.1 DMZ Setup

A DMZ (Demilitarized Zone) allows a single computer on your LAN to expose ALL of its ports to the Internet. Enter the IP address of computer as a DMZ (Demilitarized

Zone) host with unrestricted Internet access. When doing this, the DMZ host is no longer behind the firewall.

Fields in this page:

Field	Description
Enable DMZ	Check this item to enable the DMZ feature.
DMZ Host IP Address	IP address of the local host. This feature sets a local host to be exposed to the Internet.

6.2.2 Virtual Server

Firewall keeps unwanted traffic from the Internet away from your LAN computers. Add a Virtual Server entry will create a tunnel through your firewall so that the computers on the Internet can communicate to one of the computers on your LAN on a single port.

Fields in this page:

Field	Description
Service Type	Select a service from pull-down menu or User-defined Service Name.
Protocol	There are 2 options available: TCP, UDP.
WAN Setting	There are 2 options available: create rules by interface or by IP address
WAN Interface	Select the WAN interface on which the Virtual Server rule is to be applied.
WAN Port	The destination port number that is made open for this application on the WAN-side
Local IP Address	IP address of your local server that will be accessed by Internet.
LAN Open Port	The destination port number that is made open for this application on the LAN-side.

Function buttons for the setting block:

Apply Changes

Click to save the rule entry to the configuration.

Function buttons for the Current Table:

Delete Selected

Delete the selected rules from the table. You can click Delete button from the Current virtual serve forwarding table.

Disable

Without deleting the rule you can make specific virtual server entry in the table as inactive. You can click Disable to de-activate the entry.

6.2.3 NAT ALG and Pass-Through

An application-level gateway (also known as **ALG** or application layer gateway) consists of a security component that augments a firewall or NAT employed in a computer network. It allows customized NAT traversal filters to be plugged into the gateway to support address and port translation for certain application layer "control/data" protocols such as IPSec, L2TP, PPTP, FTP, SIP, RTSP etc. In order for these protocols to work through NAT or a firewall, either the application has to know about an address/port number combination that allows incoming packets, or the NAT has to monitor the control traffic and open up port mappings (firewall pinhole) dynamically as required. Legitimate application data can thus be **passed through** the security checks of the firewall or NAT that would have otherwise restricted the traffic for not meeting its limited filter criteria.

6.3 QoS

6.3.1 IP QoS

The device provides a control mechanism that can provide different priority to different users or data flows. The QoS is enforced by the QoS rules in the QoS table. A QoS rule contains two configuration blocks: Traffic Classification and Action. The Traffic Classification enables you to classify packets on the basis of various fields in the packet and perhaps the physical ingress port. The Action enables you to assign the strict priority level and mark some fields in the packet that matches the Traffic Classification rule. You can configure any or all field as needed in these two QoS blocks for a QoS rule.

Fields on the first setting block of this page:

Field	Description
IP QoS	Enable/Disable the IP QoS function.
Source IP	The IP address of the traffic source.
Source Netmask	The source IP Netmask. This field is required if the source IP has been entered.
Destination IP	The IP address of the traffic destination.
Destination Netmask	The destination IP Netmask. This field is required if the destination IP has been entered.
Protocol	The selections are TCP, UDP, ICMP and the blank for none. This field is required if the source port or destination port has been entered.
Source Port	The source port of the selected protocol. You cannot configure this field without entering the protocol first.
Destination Port	The destination port of the selected protocol. You cannot configure this field without entering the protocol first.
Physical Port	The incoming ports. The selections include LAN ports, wireless port, and the blank for not applicable.

Fields on the second setting block of this page:

Field	Description
Outbound Priority	The priority level for the traffic that matches this classification rule. The possible selections are (in the descending priority): p0, p1, p2, p3.
IP Precedence	Select this field to mark the IP precedence bits in the packet that match this classification rule.
IP Type of Service	Select this field to mark the IP TOS bits in the packet that match this classification rule.

802.1p	Select this field to mark the 3-bit user-priority field in the 802.1p header of the packet that matches this classification rule. Note that this 802.1p marking is workable on a given PVC channel only if the VLAN tag is enabled in this PVC channel.

6.4 CWMP Setup

6.4.1 TR-069 Configuration

TR-069 is a protocol for communication between a CPE and Auto-Configuration Server (ACS). The CPE TR-069 configuration should be well defined to be able to communicate with the remote ACS.

Fields in this page:

ACS Field	Description
URL	ACS URL. For example, http://10.0.0.1:80 https://10.0.0.1:443
User Name	The username the device should use when connecting to the ACS.
Password	The password the device should use when connecting to the ACS.
Periodic Inform Enable	When this field is enabled, the device will send an Inform RPC to the ACS server at the system startup, and will continue to send it periodically at an interval defined in Periodic Inform Interval field; When this field is disabled, the device will only send Inform RPC to the ACS server once at the system startup.
Periodic Inform Interval	Time interval in second to send Inform RPC.

Connection Request Field	Description
User Name	The username the remote ACS should use when connecting to this device.
Password	The password the remote ACS should use when connecting to this device.
Path	The path of the device ConnectionRequestURL. The device ConnectionRequestURL should be configured based on the Device_IP, Path and Port as follows: http://Device_IP:Port/Path
Port	The port of the device ConnectionRequestURL.

6.5 Port Mapping Setup

The device provides multiple interface groups. Up to five interface groups are supported including one default group. The LAN and WAN interfaces could be included. Traffic coming from one interface of a group can only be flowed to the interfaces in the same interface group. Thus, the device can isolate traffic from group to group for some application. By default, all the interfaces (LAN and WAN) belong to the default group, and the other four groups are all empty. It is possible to assign any interface to any group but only one group.

6.5.1 Port Mapping Configuration

Fields in this page:

Field	Description
Enabled/Disabled	Radio buttons to enable/disable the interface group feature. If disabled, all interfaces belong to the default group.
“Interface groups	To manipulate a mapping group: • Select a group from the table. • Select interfaces from the available/grouped interface list and add it to the grouped/available interface list using the arrow buttons to manipulate the required mapping of the ports. • Click “Apply Changes” button to save the changes.

6.6 Others

6.6.1 Bridge Setting

You can enable/disable Spanning Tree Protocol and set MAC address aging time in this page.

Fields in this page:

Field	Description
Ageing Time	Set the Ethernet address ageing time, in seconds. After [Ageing Time] seconds of not having seen a frame coming from a certain address, the bridge will time out (delete) that address from Forwarding DataBase (fdb).
802.1d Spanning Tree	Enable/disable the spanning tree protocol

6.6.2 Client Limit Configuration

This page is used to configure the capability of force how many devices can access to Internet!

6.6.3 Other Advanced Configuration

Here you can set other miscellaneous advanced settings.

Half Bridge:

When the PPP Half Bridge is enabled the WAN IP address from the ISP is passed straight through the modem to the local client PC. Only one PC is able to access the Internet using half bridge mode as NAT is disabled. Half bridge mode can only be used when a single IP address has been assigned by the ISP, it is not suitable for services that provide multiple IP addresses. Half bridge mode is used when the use of NAT or NAPT is not desired and there is a single computer attached to the modem. When the half-bridged modem is used in conjunction with a router handling DHCP, only then multiple computers can connect to the Internet.

7. Service Setup

7.1 IGMP Configuration

Multicasting is useful when the same data needs to be sent to more than one hosts. Using multicasting as opposed to sending the same data to the individual hosts uses less network bandwidth. The multicast feature also enables you to receive multicast video stream from multicast servers.

IP hosts use Internet Group Management Protocol (IGMP) to report their multicast group memberships to neighboring routers. Similarly, multicast routers use IGMP to discover which of their hosts belong to multicast groups. This device supports IGMP proxy that handles IGMP messages. When enabled, this device acts as a proxy for a LAN host making requests to join and leave multicast groups, or a multicast router sending multicast packets to multicast group on the WAN side.

When a host wishes to join a multicast group, it sends IGMP REPORT message to the device's IGMP downstream interface. The proxy sets up a multicast route for the interface and host requesting the video content. It then forwards the Join to the upstream multicast router. The multicast IP traffic will then be forwarded to the requesting host. On a leave, the proxy removes the route and then forwards the leave to the upstream multicast router.

7.1.1 IGMP Proxy Configuration

The IGMP Proxy page allows you to enable multicast on WAN and LAN interfaces. The LAN interface is always served as downstream IGMP proxy, and you can configure one of the available WAN interfaces as the upstream IGMP proxy.

Upstream: The interfaces that IGMP requests from hosts are sent to the multicast router.

Downstream: The interface data from the multicast router are sent to hosts in the multicast group database.

Fields in this page:

Field	Description
IGMP Proxy	Enable/Disable IGMP proxy feature
Proxy Interface	The upstream WAN interface is selected here.

7.2 UPnP Setup

The device supports a control point for Universal Plug and Play (UPnP) version 1.0, and supports two key features: NAT Traversal and Device Identification. This feature requires one active WAN interface. In addition, the host should support this feature. In the presence of multiple WAN interfaces, select an interface on which the incoming traffic is present.

With NAT Traversal, when an UPnP command is received to open ports in NAT, the application translates the request into system commands to open the ports in NAT and the firewall. The interface to open the ports is given to UPnP when it starts up and is part of the configuration of the application.

For Device Identification, the application will send a description of the device as a control point back to the host making the request.

7.2.1 UPnP Configuration

Fields in this page:

Field	Description
UPnP Daemon	Enable/Disable UPnP feature.
Binded WAN Interface	Select WAN interface that will use UPnP from the drop-down lists.

7.3 SNMP Setup

Simple Network Management Protocol (SNMP) is a troubleshooting and management protocol that uses the UDP protocol on port 161 to communicate between clients and servers. The device can be managed locally or remotely by SNMP protocol.

7.3.1 SNMP Protocol Configuration

Fields in this page:

Field	Description
System Description	System description of the device.
System Contact	Contact person and/or contact information for the device.
System Name	An administratively assigned name for the device.
System Location	The physical location of the device.
System Object ID	Vendor objects identifier. The vendor's authoritative identification of the network management subsystem contained in the entity.
Trap IP Address	Destination IP address of the SNMP trap.
Community name (read-only)	Name of the read-only community. This read-only community allows read operation to all objects in the MIB.
Community name (write-only)	Name of the write-only community. This write-only community allows write operation to the objects defines as read-writable in the MIB.

7.4 DNS Setup

7.4.1 DNS Configuration

This page is used to select the way to obtain the IP addresses of the DNS servers.

Fields in this page:

Field	Description
Attain DNS Automatically	Select this item if you want to use the DNS servers obtained by the WAN interface via the auto-configuration mechanism.
Set DNS Manually	Select this item to configure up to three DNS IP addresses.

7.5 Dynamic DNS

Each time your device connects to the Internet, your ISP assigns a different IP address to your device. In order for you or other users to access your device from the WAN-side, you need to manually track the IP that is currently used. The Dynamic DNS feature allows you to register your device with a DNS server and access your device each time using the same host name. The Dynamic DNS page allows you to enable/disable the Dynamic DNS feature.

7.5.1 Dynamic DNS (DDNS) Configuration

On the Dynamic DNS page, configure the following fields:

Field	Description
Enable	Check this item to enable this registration account for the DNS server.
DDNS provider	There are two DDNS providers to be selected in order to register your device with: **DynDNS** and **TZO**. A charge may occur depends on the service you select.
Hostname	Domain name to be registered with the DDNS server.
Interface	This field defaults to your device's WAN interface over which your device will be accessed.
Username	User-name assigned by the DDNS service provider.
Password	Password assigned by the DDNS service provider.

8. Firewall Setup

Firewall contains several features that are used to deny or allow traffic from passing through the device.

8.1 MAC Filtering

The MAC filtering feature allows you to define rules to allow or deny frames through the device based on source MAC address, destination MAC address, and traffic direction.

Fields on the first setting block:

Field	Description
Outgoing Default Action	Specify the default action on the LAN to WAN bridging/forwarding path.
Incoming Default Action	Specify the default action on the WAN to LAN bridging/forwarding path.

Fields on the second setting block:

Field	Description
Rule Action	Deny or allow traffic when matching this rule.
Direction	Traffic bridging/forwarding direction.
Source MAC Address	The source MAC address. It must be xxxxxxxxxxxx format. Blanks can be used in the MAC address space and are considered as don't care.
Destination MAC Address	The destination MAC address. It must be xxxxxxxxxxxx format. Blanks can be used in the MAC address space and are considered as don't care.

8.2 IP/Port Filtering Setup

8.2.1 IP/Port Filtering

The IP/Port filtering feature allows you to deny/allow specific services or applications in the forwarding path.

Fields on the first setting block:

Field	Description
Outgoing Default Action	Specify the default action on the LAN to WAN forwarding path.
Incoming Default Action	Specify the default action on the WAN to LAN forwarding path.

Fields on the second setting block:

Field	Description

Rule Action	Deny or allow traffic when matching this rule.
Direction	Traffic forwarding direction.
Protocol	There are 3 options available: TCP, UDP and ICMP.
Source IP Address	The source IP address assigned to the traffic on which filtering is applied.
Source Subnet Mask	Subnet-mask of the source IP.
Source Port	Starting and ending source port numbers.
Destination IP Address	The destination IP address assigned to the traffic on which filtering is applied.
Destination Subnet Mask	Subnet-mask of the destination IP.
Destination Port	Starting and ending destination port numbers.

8.3 URL Filter

The URL Blocking is the web filtering solution. The firewall has the ability to block access to specific web URLs based on string matches. This can allow large numbers of URLs to be blocked by specifying only a FQDN (such as tw.yahoo.com). The URL Blocking enforces a Web usage policy to control content downloaded from, and uploaded to the Web.

8.3.1 URL Blocking Configuration

Fields in this page:

Field	Description
URL Blocking capability	Check this item to enable the URL Blocking feature.
Keyword	The filtered keyword such as yahoo. If the URL includes this keyword, the yahoo URL's will be blocked to access.

8.4 ACL Setup

The Access Control List (ACL) is a list of permissions for a packet to be matched. The list specifies who is allowed to access this device. If ACL is enabled, all hosts cannot access this device except for the hosts with IP address in the ACL table.

8.4.1 ACL Configuration

1. LAN – You can enable LAN ACS Switch to allow/block the PC to access the Modem.
2. WAN – You can enable web(http)/telenet/ftp/tftp/snmp/ping for WAN access.

8.5 DoS Setting

A denial-of-service attack (DoS attack) is an attempt to make a computer resource unavailable to its intended users. One common method of attack involves saturating the target machine with external communications requests, such that it cannot respond to legitimate traffic, or responds so slowly as to be rendered effectively unavailable. Such attacks usually lead to a server overload. In general terms, DoS attacks are implemented by either forcing the targeted computer(s) to reset, or consuming its resources so that it can no longer provide its intended service or obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately.

Enable DoS Prevention to detect and prevent denial of service attacks through automatic rate filtering or rules to protect legitimate users during the DoS attacks.

9. Maintenance Setup

9.1 Upgrade

9.1.1 Upgrade Firmware

To upgrade the firmware on the device:

- Click the Browse button to select the firmware file.
- Confirm your selection.
- Click the Upload button to start upgrading.

IMPORTANT!

Do not turn off your device or press the Reset button while this procedure is in progress.

9.1.2 Backup/Restore Settings

This page allows you to backup and restore your configuration into and from file on your host PC.

9.2 Password

The first time you log into the system, you use the default password. There are two-level for login: admin and user. The admin and user password configuration allows you to change the password for administrator and user.

9.2.1 User Account Configuration

Fields in this page:

Field	Description
User Name	Selection of user levels are: admin and user.
Old Password	Enter the old password for this selected login.
New Password	Enter the new password here.
Confirmed Password	Enter the new password here again to confirm.
Privilege	Selection of privilege levels are: root or user.

9.3 Reboot

Restart the router.

9.3.1 Commit/Reboot

Function buttons in this page:

1. Save Current Configuration >> Save changes.
2. Factory Default Configuration >> Restore router to factory default settings.
3. Commit Changes >> Save the changes into flash memory.
4. Reset >> Clear the changes from the setting.
5. Reboot >> Restart the modem.

9.4 Time Setup

Select a Network Time Server for synchronization. You can type in the address of a time server. If you have trouble using one server, enter another. Or, you can set the time manually.

9.4.1 System Time Configuration

Fields in this page:

Field	Description
System Time	The current time of the specified time zone. You can set the current time by yourself or configured by SNTP.
Time Zone Select	The time zone in which the device resides.
State	Enable the SNTP client to update the system clock.
Server	The IP address or the host name of the SNTP server. You can select from the list or set it manually.
NTP Start	Start to check the GMT time

9.5 Log Setup

You can setup the system log file.

9.5.1 Log Setting

This page shows the system log.

9.6 Diagnostic Setup

The device supports some useful diagnostic tools.

9.6.1 Ping Diagnostic

Ping operates by sending Internet Control Message Protocol (ICMP) echo request packets to the target host and waiting for an ICMP response. In the process it measures the time from transmission to reception (round-trip time) and records any packet loss.

9.6.2 Traceroute Diagnostic

Traceroute is a computer network diagnostic tool for displaying the route (path) and measuring transit delays of packets across an Internet Protocol (IP) network.

9.6.4 OAM Fault Management – Connectivity Verification

In order to isolate the ATM interface problems, you can use ATM OAM loopback cells to verify connectivity between VP/VC endpoints, as well as segment endpoints within the VP/VC.

OAM F4 cells operate at the VP level. They use the same VPI as the user cells, however, they use two different reserved VCIs, as follows:

VCI=3 Segment OAM F4 cells.

VCI=4 End-to-End OAM F4 cells.

OAM F5 cells operate at the VC level. They use the same VPI and VCI as the user cells. To distinguish between data and OAM cells, the PTI field is used as follows:

PTI=100 Segment OAM F5 cells processed by the next segment.

PTI=101 End-to-End OAM F5 cells which are only processed by end stations terminating an ATM link.

9.6.5 Diagnostic

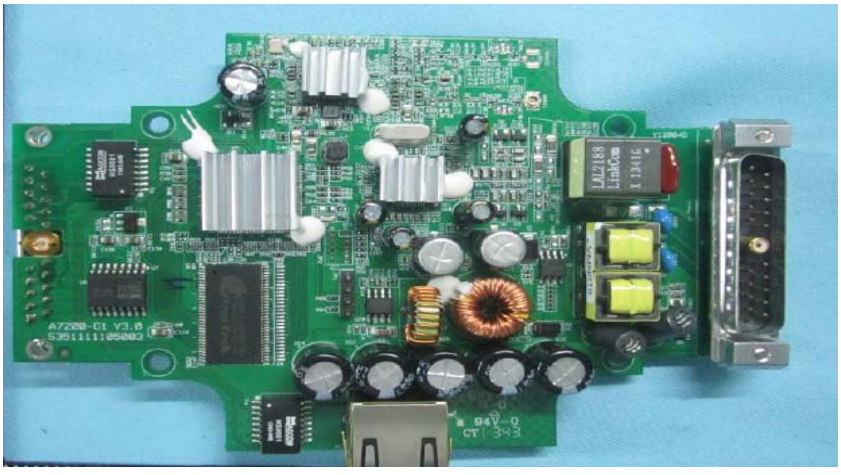
This page shows the diagnostic result. Click “Start” button to start the diagnostic.

9.6.6 Diagnostic Test

The Diagnostic Test page shows the test results for the connectivity of the physical layer and protocol layer for both LAN and WAN sides.

Fields in this page:

Field	Description
Select the Internet Connection	The available WAN side interfaces are listed. You have to select one for the WAN interface configured and run the Diagnostic test.



FCC Caution.

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

§ 15.21 Information to user.
Any Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

§ 15.105 Information to the user.
Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
-Reorient or relocate the receiving antenna.
-Increase the separation between the equipment and receiver.
-Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
-Consult the dealer or an experienced radio/TV technician for help.

The A7200-G1 module is designed to comply with the FCC statement.
FCC ID is 2AB3KA7200. The host system using A7200-G1, should have label indicated FCC ID 2AB3KA7200.

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