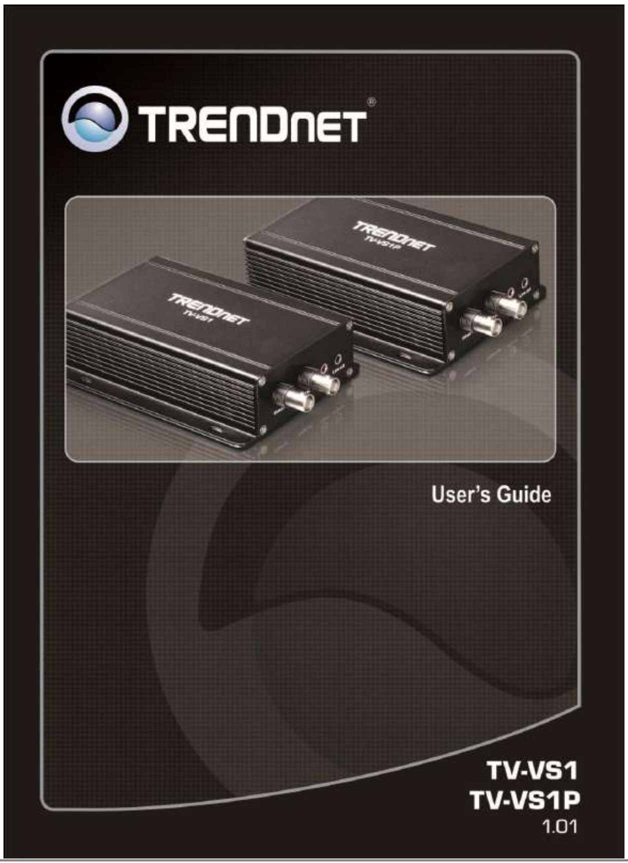
TRENDnet
User's Guide
TV-VS1
TV-VS1P
1.01

Manual abstract:

TV-VS1P Compliant with IEEE802.3af PoE (Power over Ethernet) standard, the Video Encoder provides you with more flexibility of device installation according to your application. The device can be powered by the Ethernet, so that you can place the device anywhere without a power outlet supported. The simple installation procedures and web-based interface allow you to integrate it into your network easily. With comprehensive applications supported, the Video Encoder is your best solution to transmit the realtime high-quality video images for monitoring. -1- This Advanced Installation Guide provides you with the instructions and illustrations on how to use your Video Encoder, which includes: Chapter 1 Knowing Your Video Encoder describes the component features of the device, as well as the applications of the device. Hardware Installation helps you install the device according to your application environment. You can use this device at home, at work, at any where you want. Accessing the Video Encoder lets you start using your device without problem. The device can be set up easily and work within your network environment instantly.

Configuring the Video Encoder guides you through the configuration of the device using the Web browser on your PC. Appendix provides the specification of the device and some useful information for using your device. Chapter 2 Chapter 3 Chapter 4 Chapter 5 NOTE The illustrations and configuration values in this guide are for reference only. The actual settings depend on your practical application of the Video Encoder. -2- Contents PREFACE .

-4- CHAPTER 1 KNOWING YOUR VIDEO ENCODER 1.1 Checking the Package Contents Check the items contained in the package carefully. You should have the following: NOTE TV-VS1 or TV-VS1P Multi-Language Quick Installation Guide CD-ROM (Utility & User's Guide) GPIO Connector Network Cable (RJ-45) Audio Y cable (3.
5mm Jack) Power Adapter (12VDC, 1.5A) Mounting Kit Any content is damaged or missing, please contact the local authorized dealer for replacement. -5- 1.2 Component Features Front Panel NO. Item Video In Video Out Function Connect an analog camera with the composite video output (BNC type). Connect an external video device with the composite video input (BNC type) to display the camera's image on a conventional monitor. Connect CCTV camera's audio out to Video Encoder's Line In. Connect an external active speaker to broadcast on-thespot sound of the connected CCTV camera. Line In Line Out -6- Rear Panel NO. Item DC Power Connector LED Function Connect one end of power plug into the power source and the other end to the device. Power LED (upper) will light a steady amber light to indicate the device is powered on. Link LED (lower) will blink a green light to indicate the device's network connectivity. Connect the external devices for trigger and advanced functions. For more information, refer to the Appendix, GPIO Terminal Application. Connect the network cable. The connector supports the NWay protocol so that the device can detect the network speed automatically. Insert the SD card to expand the storage space for the device (up to 32GB) Press to restart the device when it is pressed quickly; press and hold for five seconds to restore the factory default settings. -7- GPIO and RS485 Ethernet Connector SD Card Slot Reset Button 1.3 Features and Benefits H.264/MPEG4/MJPEG Multi-codec Supported The device provides you with excellent images by the H.

264/MPEG4/ MJPEG multi-codec selectable technology, allowing you to adjust image size and quality, and bit rate according to the networking environment. Flexible Audio Capability The device allows you to connect the external microphone to receive on-the-spot audio via the Internet, allowing you to monitor the on-site voice. In addition, you can connect an external active speaker to the device to broadcast the received sound through the connected camera. Supports RTSP The device supports RTSP (Real Time Streaming Protocol), which is a technology that allows you to view streaming media via the network. You can view the real-time video with the Quick Time player or RealPlayer. To view the real-time streaming image on your computer, open the Web browser and enter the RTSP link: MPEG4 stream: rtsp://(IP address of the device)/mpeg4 H.264 stream: rtsp://(IP address of the device)/h264 I/O Connectors and RS-485 Provided The I/O connectors (IN/OUT) of the device provide the physical interface to send and receive digital signals to a variety of external alarm devices (such as motion detection, event triggering, alarm notification, and a variety of external control functions). The pins TX+ & TX- of the I/O connectors are used for RS-485 data transmission, which allow you to connect a special featured device (such as an external device stand with rotation function) and then configure the settings and control the device from the GPIO Trigger window of Web Configuration. -8- Remote Control Supported By using a standard Web browser, the administrator can easily change the configuration of the device via Intranet or Internet. In addition, the device can be upgraded remotely when a *new firmware is available.*

The users are also allowed to monitor the image and take snapshots via the network. Multiple Profiles Supported The device supports multiple profiles simultaneously, so that you can separately set up different image settings (such as image quality and frame rate) for the three video types of the device: H.264, MPEG4, MJPEG, and 3GPP. Multiple Platforms Supported The device supports multiple network protocols, including TCP/IP, SMTP e-mail, HTTP, and other Internet related protocols. Therefore, you can use the device in a mixed operating system environment, such as Windows® 7/Vista/XP.

Multiple Applications Supported Through the remote access technology, you can use the device to monitor various objects and places for your own purposes. For example, babies at home, patients in the hospital, offices and banks, and more. The device can capture both still images and video clips, so that you can keep the archives and restore them at any time. PoE Supported (TV-VS1P only) PoE (Power over Ethernet) standard enables the device to be powered by the Ethernet, which simplifies your surveillance system by eliminating the need of power outlet. The PoE device features both stability and security, providing a cost-saving solution to your application of Internet surveillance.

-9- 1.4 System Requirement Networking LAN 10Base-T Ethernet or 100Base-TX Fast Ethernet; Auto-MDIX IEEE 802.3af PoE (TV-VS1P only) Accessing the Device using Web Browser Platform CPU RAM Resolution User Interface Microsoft® Windows® 7/Vista/XP Intel Pentium III 800MHz or above 512MB 800x600 or above Microsoft® Internet Explorer 6.0 or above; - 10 - CHAPTER 2 HARDWARE INSTALLATION 2.1 Mounting the Device on the Wall The provided mounting Kit is used to mount the device on the wall or ceiling. The example below is wall mounting installation. You can place the device flexibly according to your need. a. Drill four mounting holes into the wall. b.

Hammer the plastic anchors into the holes. c. Mount the device onto the wall with four screws. - 11 - 2.2 Connecting the Cables 1. Connecting the device to power source Use the provided power adapter to connect the device to the power source, such as the electrical outlet on the wall, and connect the other end to the device. You can verify the power status from the Power LED on the rear panel of the device. Connecting the device to LAN Use the provided Network cable to connect the device to your local area network (LAN). Once connected, the Link LED starts flashing green light. Connecting the camera to the device Connects a CCTV analog camera to the Video Encoder so that the Video Encoder can work within your surveillance solution.

To connect the camera, plug one end of the BNC cable to the Video in connector of the device and the other end to the Video out connector of the camera. 2. 3. - 12 - 2.3 Applications of the Video Encoder The video encoder can be applied in multiple applications, including: Monitor local and remote places and objects via Internet or Intranet.

Capture still images and video clips remotely. Upload images or send email messages with the still images attached. The following diagram explains one of the applications for your Video Encoder and provides a basic example for above the Live View image. Zoom buttons: Click the zoom button (in the live view image by 1x, 2x, 3x, or Full-screen. date & time.

The information can be modified in the Web Configuration.) to zoom Device Information: Displays the device's location and the current NOTE If your computer use Microsoft® Windows® 7/Vista platform, you may not find the recorded files that are saved by Snapshot or Manual Record. You need to disable the protected mode of Security in the IE Browser through the following steps: 1. Open IE Browser 2. Select ToolsInternet Options 3. Select Security 4. Uncheck the "Enable Protected Mode" then press OK - 20 - 3.3 Configuring the IP Address of the Computer If you are failed to access to the Video Encoder, please check the IP address of your computer. When you connect the device to your computer directly to proceed with configuration of the device, you need to set up the IP addresses to be in the same segment for the two devices to communicate. 1.

2. 3. 4. 5. 6. On your computer, click Start > Control Panel to open the Control Panel window. Double-click Network Connection to open the Network Connection window. Right-click Local Area Connection and then click Properties from the shortcut menu. When the Local Area Connection Properties window appears, select the General tab. Select Internet Protocol [TCP/IP] and then click Properties to bring up the Internet Protocol [TCP/IP] Properties window.

To configure a fixed IP address that is within the segment of the device, select the Use the following IP address option. Then, enter an IP address into the empty field. The suggested IP address is 192.168.10.

x (x is 1~254 except 30), and the suggested Subnet mask is 255.255.255.0. When you are finished, click OK.

7. - 21 - CHAPTER 4 CONFIGURING THE VIDEO ENCODER 4.1 Using the Web Configuration You can access and manage the Video Encoder through the Web browser. This chapter describes the Web Configuration, and guides you through the configuration of the device by using the Web browser. To configure the device, click on the Main screen of Web Configuration. The Web Configuration will start from the Basic page. The Web Configuration contains the settings that are required for the device in the left menu bar, including Smart Wizard, Basic, Network, Video/Audio, Event Server, Motion detect, Event Config, Tools, RS-485, SD Card, and Information. - 22 - 4.2 Using Smart Wizard The device's Smart Wizard lets you configure your device easily and quickly. The wizard will guide you through the necessary settings with detailed instructions on each step.

To start the wizard, click Smart Wizard in the left menu bar. Step 1. Basic Settings By default, the server name is set as model number. Change the server name if necessary. Enter the location, administrator password twice. - 23 - Step 2. IP Settings Setup the IP setting, DHCP, Static IP or PPPoE. Step 3. Email Settings Enter the mail server information. If you are using a free mails server, select the SSL and/or STARTTLS according to the mail server requirement. - 24 - Step 4. Confirm Settings - 25 - 4.3 Basic Setup The Basic menu contains three sub-menus that provide the system settings for the device, such as the Server Name, Location, Date & Time, and User management. - 26 - 4.3.

1 Basic >> System Basic: This item allows you to assign the device name and location information. Server Name: Enter a descriptive name for the Video Encoder, which is helpful to identify the device easily while multiple devices are connected within the network. Location: Enter a descriptive name for the location where is monitored by the connected camera. Language Default: Select your preferred language for the system. Indication LED: This item allows you to set the LED illumination as desired.

There available options include: Normal, and OFF. - 27 - 4.3.2 Basic >> Date & Time Date and Time: Enter the correct date and time for the system. TimeZone: Select the proper time zone for the region from the pull-down menu. Synchronize with PC: Select this option and the date & time settings of the device will be synchronized with the connected computer. Synchronize with NTP Server: Select this option and the time will be synchronized with the NTP Server.

You need to enter the IP address of the server and select the update interval in the following two boxes. Manual: Select this option to set the date and time manually. - 28 - 4.

3.3 Basic >> User Administrator: To prevent unauthorized access to the device's Web Configuration, you are strongly recommend to change the default administrator password. Type the administrator password twice to set and confirm the password. General User User Name: Enter the user's name you want to add to use the device. Password: Enter the password for the new user. UserList: Display the existing users of the device. To delete a user, select the one you want to delete and click Delete. When you are finished, click Add/Modify to add the new user to the device. To modify the user's information, select the one you want to modify from UserList and click Add/Modify. Guest User Name: Enter the guest's name you want to add to use the device.

- 29 - Password: Enter the password for the new guest. UserList: Display the existing guests of the device. To delete a user, select the one you want to delete and click Delete. NOTE The "General User" can access the device and control the Function buttons of the device's Web Configuration; the "Guest' can only view the live view image from the Main screen of the Web Configuration while accessing the device. Only the "Administrator" is allowed to configure the device through the Web Configuration.

- 30 - 4.4 Network Settings The Network menu contains two sub-menus that provide the network settings for the device, such as the IP Setting, DDNS Setting, and IP Filter. - 31 - 4.4.1 Network >> Network IP Setting: This item allows you to select the IP address mode and set up the related configuration.

The default setting is DHCP mode enabled. DHCP: Select this option when your network uses the DHCP server. When the device starts up, it will be assigned an IP address from the DHCP server automatically. Static IP: Select this option to assign the IP address for the device directly. You can use IPSetup to obtain the related setting values. - 32 - IP Subnet Mask Default Gateway Primary/ Secondary DNS Enter the IP address of the device. The default setting is 192.168.10.30.

Enter the Subnet Mask of the device. The default setting is 255.255.255.0. Enter the Default Gateway of the device. The default setting is 192.168.10.1. DNS (Domain Name System) translates domain names into IP addresses. Enter the Primary DNS and Secondary DNS that are provided by ISP. PPPoE: Select this option when you use a direct connection via the ADSL modem. You should have a PPPoE account from your Internet service provider. Enter the User Name and Password.

The device will get an IP address from the ISP as starting up. NOTE Once the device get an IP address from the ISP as starting up, it automatically sends a notification email to you. Therefore, when you select PPPoE as your connecting type, you have to set up the email or DDNS configuration in advance. DDNS Setting: With the Dynamic DNS feature, you can assign a fixed host and domain name to a dynamic Internet IP address. To set up the DDNS: 1.

2. 3. Select the Enable option to enable this feature. Select the Provider from the pull-down list. Enter the required information in the Host Name, User Name, and Password boxes. NOTE You have to sign up for DDNS service with the service provider before configuring this feature. UPnP: The device supports UPnP (Universal Plug and Play), which is a set of computer network protocols that enable the device-todevice interoperability. In addition, it supports port auto mapping function so that you can access the device if it is behind an NAT router or firewall. Select the Enable option to enable this feature. - 33 - Ports Number HTTP Port: The default HTTP port is 80.

If the device is behind an NAT router of firewall, the suggested to be used is from 1024 to 65535. NOTE 4.4.2 Network >> Network >> Advanced HTTPS Enable: Select this option to enable HTTPS, which is a secure protocol to provide authenticated and encrypted communication within your network. - 34 - HTTPS Port: Assign a HTTPS port in the text box. The default HTTPS port is 443. Bonjour: The devices with Bonjour will automatically broadcast their own services and listen for services being offered for the use of others. If your browser with Bonjour, you can find the device on your local network without knowing its IP address. The Apple Safari is already with Bonjour. You can download the complete Bonjour for Internet Explorer browser from Apple's web site by visiting http://www.

apple.com/bonjour/. RTSP RTSP Streaming: Selection the Authentication as Disable or Enable to configure the transmission of streaming data within the network. The default RTSP Port (Real Time Streaming Protocol) is 554. Multicast settings: Configure the following settings so that you can deliver information from your device to a set of receivers.

Group IP H.264 Port MPEG4 Port Audio Port TTL Assign a category of IP addresses to receive the information from the device. Assign a multicast port for H.264 in the text box. The default port is 1234.

Assign a multicast port for MPEG4 in the text box. The default port is 1236. Assign a multicast port for audio in the text box. The default port is 1238. Set the TTL value from 1 to 255, which is used to modify the time to live field in the IP header. QoS Live Video DSCP: Assign the DSCP (DiffServ Code Point) of the stream video from the device. Live Audio DSCP: Assign the DSCP (DiffServ Code Point) of the stream audio from the device. - 35 - 4.4.3 Network >> IP Filter The IP Filter setting allows the administrator of the device to limit the users within a certain range of IP addresses to access the device.

To disable this feature, select the Disable option; otherwise, select the Accept option to assign the range of IP addresses that are allowed to access the device, or select the Deny option to assign the range of IP addresses that are blocked to access the device. Disable: Select this option to disable the IP Filter function of the device. Accept IPv4: Assign a range of IP addresses that are allowed to access the device by entering the Start IP address and End IP address options. When you are finished, click Add to save the range setting. You can repeat the action to assign multiple ranges for the device. IPv6: Enter the IP Address that is allowed to access the device. - 36 - Deny IPv4: Assign a range of IP addresses that are blocked to access the device by entering the Start IP address and End IP address options. When you are finished, click Add to save the range setting. You can repeat the action to assign multiple ranges for the device. IPv6: Enter the IP Address that is not allowed to access the device.

For example, when you enter 192.168.10.50/192.168.

10.80 in Start/End IP Address of Accept > IPv4, the user whose IP address located within 192.

168.10.50 ~ 192.

168.10.80 will be allowed to access the device. On the other hand, if you enter the IP range in Start/End IP Address of Deny > IPv4, the user whose IP address located within the range will not be allowed to access the device. - 37 - 4.5 Setting up Video & Audio The Video & Audio menu contains four sub-menus that provide the video and audio settings for the device. - 38 - 4.5.1 Video & Audio >> Image Setting Image Setting Brightness: Adjust the brightness level from 0 ~ 100. Saturation: Adjust the colors level from 0 ~ 100.

Sharpness: Adjust the sharpness level from 0 ~ 100. Hue: Adjust the hue level from 0 ~ 100. WDRC: Adjust value of WDRC (Wide Dynamic Range Correction) to provide clear images even when the background light varies excessively. TIP Click Default then Apply to restore the default settings of the options above - 39 - 4.5.2 Video & Audio >> Video H.264 Video Resolution: Select the desired video resolution from the pull-down menu. Please note that higher setting obtains better video quality while it uses more resource within your network. Video Quality: Select the desired image quality from five levels: Lowest, Low, Medium, High, and Highest. Frame Rate: Select a proper setting depending on your network status.

MPEG4 Video Resolution: Select the desired video resolution from the pull-down menu. Please note that higher setting obtains better video quality while it uses more resource within your network. - 40 - Video Quality: Select the desired image quality from five levels: Lowest, Low, Medium, High, and Highest. Frame Rate: Select a proper setting depending on your network status. MJPEG Video Resolution: Select the desired video resolution from the three formats: VGA, QVGA and QQVGA.

The higher setting (VGA) obtains better video quality while it uses more resource within your network. Video Quality: Select the desired image quality from five levels: Lowest, Low, Medium, High, and Highest. Frame Rate: Select a proper setting depending on your network status. None IE Browser Viewer: Select Java Applet, Still Image, or Server Push for the viewers who use the none IE browser. 3GPP: The device supports 3GPP specification.

Select the Disable option to disable this feature. Otherwise, select 3GPP Without Audio or 3GPP With Audio to transfer the video clips without or with audio. If you use a mobile phone that supports 3GPP, you can also view the real-time streaming image captured by the connected camera on your phone (with the default player on the phone) by entering the RTSP link: rtsp://(IP address of the device)/3gp. NOTE Your mobile phone and the service provider must support 3GPP function. Please contact your service provider when you are failed to use this service. - 41 - 4.5.3 Video & Audio >> Audio Line In: Select the Enable option to enable the device's audio function, so that you can receive the on-site sound and voice from the connected camera. Line Out: Select the Enable option to enable the device's external speaker function, so that the connected speaker can play the sound and voice through the connected camera. You can set the speaker's volume by entering the proper value in the Volume option.

The default setting is 90. - 42 - 4.5.4 Video & Audio >> Overlay / Mask This sub-menu is used to set the image overlay and mask feature of the device. Image Overlay: This item allows you to set the image overlay. In the Image File option, click Browse to select the image file from your computer, and then click Upload. You can click Preview to check the image size and adjust the image position before clicking Upload. The preview image area is displayed with red dotted line. If you want to remove the preview image before uploading, click Delete. Since you click Upload, the preview image area is displayed with white dotted line.

Click Enable and set the transparency setting by whether selecting the Transparent option or not. When done, click Apply. You can see the image overlay on the live view image when you click Live View. - 43 - NOTE The width and height of the input overlay graphic should be multiple of 4 at a maximum size of 38400 pixels each, and in JPG or BMP (24bit RGB) format. Privacy Mask: This item allows you to configure up to two mask areas.

Select the area 1 or 2 from the Window pull-down list, and then click Enable. You can change the size and position of the area by holding and dragging the mouse. You can also change the color of the mask area by clicking the Color box and then selecting the color you want. When done, click Apply. You can see the mask area(s) on the live view image when you click Live View.

4.5.6 Video & Audio >> Overlay / Mask >> Text Overlay This page is used to set the text overlay feature of the device, including the following three options: date & time, heading text, and background transparency setting. Include Date & Time: Select this option to display the date & time information on the live view image. Include Text: Select this option and enter your heading text in the box to display the text information on the live view image. Enable Opaque: Select this option to display the overlay text with a background color. - 44 - 4.6 Event Server Configuration The Event Server menu contains four sub-menus that allow you to upload images to FTP, send emails that include still images, store the images to a NAS system, and send instant message When you complete the required settings (such as FTP server configuration), click Test to test the related configuration is correct or not. Once the device connects to the server successfully, click Apply. - 45 - 4.

6.1 Event Server Setting >> HTTP HTTP Notify For Motion Trigger Send the query parameter via an HTTP notification when an event is triggered. Host: Enter the IP of the HTTP server Port: Enter the Port number of the HTTP server User Name: Enter the username of the HTTP server - 46 - Password: Enter the password of the HTTP server Query: Enter the query parameter for the request if necessary Example: Host: 192.168.10.1 Port: 80 Query: xxx.cgi?name1=value1&name2=value2 Ex: cgi/event.cgi?status=#s&time=#t&model=modelname Result: http://192.168.10.

1:80/cgi/event.cgi?status=#s&time=#t&model= modelname 4.6.2 Event Server Setting >> FTP FTP Host Address: Enter the IP address of the target FTP server. Port Number: Enter the port number used for the FTP server.

User Name: Enter the user name to login into the FTP server. Password: Enter the password to login into the FTP server. - 47 - Directory Path: Enter the destination folder for uploading the images. For example, test. Passive Mode: Select the Enable option to enable passive mode.

FTP Upload with: Select upload to FTP with one snapshot image or a series image in pre-event/post-event time when event triggered. NOTE Depending on the network environment, your network may not be able to upload all the screen shots that was set to FTP server.

4.6.3 Event Server Setting >> Email Email SMTP Server Address: Enter the mail server address. For example, mymail.com. If you are using a free mail service (e.g. - 48 - Google Gmail®, Yahoo®, Hotmail®), please enter the SMTP server address from the service provider.

Sender Email Address: Enter the email address of the user who will send the email. For example, John@mymail.com. SMTP Port: Assign the SMTP port in the text box. The default SMTP port is 25. If the mail server requires an encrypted connection, you should check the SSL option. SSL / STARTTLS: Most free email services require an encrypted connection. If you are using a free email service, please check the mail server requirement and select the options that apply to the server. Authentication Mode: Select None or SMTP according to the mail server configuration. Sender User Name: Enter the user name to login the mail server.

Sender Password: Enter the password to login the mail server. Receiver #1 Email Address: Enter the first email address of the user who will receive the email. @@@@@@@@@@For example, test. @@@@@@@@@@@@@@@@@@@Jabber Server Address: Enter the Jabber server address manually. Jabber Port: Assign the Jabber port manually in the text box.

@@@@Receiver: Enter the receiver's information. @@@@@@ Name: Assign a name to the detecting area. @@Otherwise, leave this option blank to use the default setting. @@@@To customize the profile, click Add and then enter a descriptive name for the profile in the prompt dialog window. After entering the profile name, click OK and the profile is added to the Schedule Profiles list.

To delete the profile, select the profile in the list and click Delete. Profile Name: Display the profile name that you select in the Schedule Profiles list. Weekdays: Select the weekday(s) that you want to separately assign in the schedule profile. The weekday that has been assigned will be displayed with green color. Time List: Display the time period that you have assigned within the selected weekday. To assign the same time period to every - 56 - weekday, click Copy this to all weekdays; click Delete this from all weekdays to remove the selected time period from every weekday. Click Delete to remove the selected time period. Start/End Time: Enter the start and end time and then click Add to assign a time period within in the selected weekday. 4.8.

3 Event Configuration >> Motion Detect Trigger Motion Detect Trigger: Select the Enable option to enable the trigger function of the device, so that you can send captured images within the detecting area to the FTP server, email receiver, or the Network Storage server. You have to configure corresponding settings, such as FTP server and email server, to enable this feature. Please note that you have to configure the related settings before enabling these features. Schedule Profile: Select a schedule profile from the pull-down list. Action: Set the Trigger Out function or select the destination that the captured images will be sent to: , or Record to SD Card, Record to Network Storage, Send Email, FTP Upload, or Instant Message. - 57 - 4.8.4 Event Configuration >> Schedule Trigger You can separately configure the schedule for trigger function of the device by Email Schedule, FTP Schedule, or Network Storage Schedule. Select the Enable option on each item, and then select a Schedule Profile from the pull-down list and set the Interval time. NOTE If the setting value of the Storage Recording Time Per Event option in General Setting is longer than the Interval time in Network Storage Schedule, the recorded file will be a continuous video clip.

For example, if you set the Storage Recording Time Per Event as 10 seconds and the Interval as 5 seconds, recorded file becomes a non-stop video clip because the device will record a 10-second video clip every 5 seconds. - 58 - 4.8.5 Event Configuration >> GPIO Trigger GPIO Trigger: Select the Enable Trigger In 1/2 option to enable the GPIO trigger function of the device, so that you can set Trigger Out function or send captured images within the detecting area to the SD card, FTP server, email receiver, Network Storage server, or send an instant message. You have to configure corresponding settings, such as FTP server and email server, to enable this feature.

Schedule Profile: Select a schedule profile from the pull-down list. Action: Set the Trigger Out function or select the destination that the captured images will be sent to: Record to SD Card, Record to Network Storage, Send Email, FTP Upload, or Instant Message. - 59 - 4.9 Tools The Tools menu provides the commands that allow you to restart or reset the device. You can also backup and restore your configuration, and upgrade the firmware for the device. Factory Reset: Click Reset to restore all factory default settings for the device. System Reboot: Click Reboot to restart the device just like turning the device off and on. The device configuration will be retained after rebooting. Configuration: You can save your device configuration as a backup file on your computer. Whenever you want to resume the original settings, you can restore them by retrieving the backup file. - 60 - Backup: Click Get the backup file to save the current configuration of the device. Restore: Click Browse to locate the backup file and then click Restore. Update Firmware: You can upgrade the firmware for your device once you obtained a latest version of firmware. Current Firmware Version: This item displays the current firmware version. Select the firmware: Click Browse to locate the backup file and then click Update.

NOTE Make sure to keep the device connected to the power source during the process of upgrading firmware. Otherwise, the device might be damaged because of failure upgrading the firmware. - 61 - 4.10 RS-485 The RS-485 menu provides the control settings for external device through the I/O port. - 62 - 4.10.1 RS-485 >> RS-485 Setting Select the Enable option and complete the required configuration to use the RS-485 function of the device. When you enable the RS-485 function of the device, the PTZ Control button will be displayed on the Live View screen. Popular Protocol Setting: Select a Protocol (Pelco-D or Pelco-P) and then select a Camera ID. Custom Protocol Setting: Select this option to configure the commands protocol manually.

You can click Test to test each command that you have assigned. In the Name and Command - 63 - string boxes, you can customize more buttons for your needs. Please note that the setting values in the Command string boxes should be from the connected external device (please refer to the manual of the connected device). 4.10.

2 RS-485 >> Patrol The Patrol function provides the patrol control settings for the connected camera. Preset Position To set the preset position for the connected camera: - 64 - 1. 2. 3. 4.

Use the Navigation buttons to move the camera lens to the desired position.

Select a Position number (Home, 2~32) from the Preset Position pull-down list. Enter the descriptive name for the location in the text box. Click Apply. To move the camera lens to the preset position immediately, select the position number (Home, 2~32) from the pull-down list and then clicking Go. Pan Speed: Adjust the moving speed (1 ~ 10) while panning the lens. Tilt Speed: Adjust the moving speed (1 ~ 10) while tilting the lens. Zoom Speed: Adjust the speed (1 ~ 10) while zooming the lens. Focus Speed: Adjust the speed (1 ~ 10) while focusing the lens. Zoom In/Zoom Out: Click to zoom in/out the live view image.

Focus Far/Focus Near: Click to adjust the focus by far/near. Patrol Position This field allows you to set the positions for camera's patrolling: 1. Select a preset position from the Preset Position pull-down list, and then click Add to be Patrol Position. The preset position will be added to the Patrol Path list. From the Patrol Path list, you can change the patrolling order by selecting a position and clicking Up or Down. You can also delete a position by clicking Remove. You can change the stay time for each position when the camera is patrolling. Select a position in the Patrol Path list and then enter a time setting in the text box below the Stay Time list. Click Update to save the setting. The Stay Time list displays the current setting for each position.

When done, click Save. - 65 - 2. 3. 4. 4.

11 Setting up SD Card The SD Card menu allows you to set up the SD card. SD Card Dismount: Click Dismount to safely remove the SD card that is installed in the device. Note: You must disable the event trigger in order to dismount the SD Card. SD Card Information: Displays the information of the installed SD card, including the Total space and Free space. SD Card Setting When Storage Full: Select Stop Recording or Recycle Delete Oldest Folder when the storage space on the SD card is full.

- 66 - File Format: Select MP4 or AVI as the file format while recording. 4.12 Information The Information menu displays the current configuration and events log of the device. - 67 - 4.12.1 System Information >> Device Information Display the Basic, Video & Audio, and Network settings of the device. 4.12.2 System Information >> Log The Logs table displays the events log recorded by the system. - 68 - CHAPTER 5 How to access the Video Encoder behind a Router You can either setup the Dynamic DNS connection via video encoder itself or your home router.

An account from any of the listed DDNS providers is required prior to this operation. Configure DDNS on your Video Encoder 1. Go to Video Encoder's DDNS Setting page, click Enable to activate the feature. Then select a DDNS provider from the list. 2. Enter your DDNS's the Host Name, User Name and Password. - 69 - 3. In the Port Number section, assign an HTTP port of the video encoder. The default HTTP Port on the video encoder is 80. The example shows above is using port number 9000.

Open another web browser and go to your Router's Web Configuration page. (In the example, TRENDnet's TEW-651BR Wireless N router is used) 4. 5. Go to Virtual Server section and create a new entry. Enable: Click Enable Name: Enter the application name (eg.*

*Video Encoder Name) Protocol: Select TCP Private Port: The HTTP port that you assign on your video encoder. - 70 - Public Port: The port used on remote side to access to your video encoder. LAN Server: The local IP address of your video encoder. Then click Add to add the application. * Please refer to your router's user's manual for detail Virtual Server setting.*

Some router might use Port Forwarding or Special applications for this function. The setup steps should be very similar. - 71 - 6. Open another web browser and enter your DDNS domain and video encoder's port number. http://yourDomainName:PortNumber 7. Video encoder's login page will appear. Configure DDNS on your router 1. Go to Video Encoder's DDNS Ports Number section, assign a HTTP port for your video encoder and click Apply. 2. Login to your router's web configuration page.

- 72 - 3. Find the Dynamic DNS configuration section. 4. Enable DDNS, fill out the following information and then click Apply. - 73 - 5. Go to Virtual Server section and create a new entry. Enable: Click Enable Name: Enter the application name (eg. Video Encoder Name) Protocol: Select TCP Private Port: The HTTP port that you assign on your video encoder. Public Port: The port used on remote side to access to your video encoder. LAN Server: The local IP address of your video encoder.*

*Click Add to add the application. * Please refer to your router's user's manual for detail Virtual Server setting. Some router might use Port Forwarding or Special applications for this function. The setup steps should be very similar. 6.*

Open another web browser and enter your DDNS domain and video encoder's port number. http://yourDomainName:PortNumber 7. The video encoder login page will appear. - 74 - Appendix A.1 Specification General Video Video In: CVBS / 1 Vp-p±0.

2 / 75 Ohms ; BNC connecter Video Out: CVBS /1 Vp-p /75 Ohms; BNC connecter Line Input: 3.5mm jack (CCTV Camera Audio) Line Output: 3.5mm jack (Speaker) S/N Ratio: < 60dB Format: PCM/AMR 2 Way audio supported Ground, GPIO in/out, DC12V output, RS485 TX+/TXSupports SD/SDHC (up to 32GB) Protocol: Pelco D, Pelco P 32 presets Auto Patrol IEEE 802.3u 10/100Mbps Fast Ethernet, Auto-MDIX IEEE 802.3af PoE (TV-VS1P only) Power, Link Push and release to reboot Push and hold for 5 seconds to restore to factory default 7 Watts 12V, 1.5A external power adapter (for non-PoE installation) 160 x 109 x 36 mm (6.3 x 4.3 x 1.4 in.) TV-VS1: 430 g (15.

2 oz.) - 75 - Audio GPIO SD Slot Pan/Tilt/Zoom Hardware Network LED Reset Button Power Consumption Power Dimension Weight Temperature Humidity Certifications Requirement Management Interface To run Utility Network Protocols Management Remote Backup / Restore Settings Image Video Encoder TV-VS1P: 445 g (15.7 oz.) Operating: 0C ~ 45C (32F ~ 113F) Storage: -15C ~ 60C (5F ~ 140F) Max. 85% (non-condensing) CE, FCC Internet Explorer 6.0 or above Windows 7(32/64-bit), Vista(32/64-bit), XP(32/64bit) TCP/IP, IPv4/IPv6, UDP, ICMP, DHCP, NTP, DNS, DDNS, SMTP, FTP, HTTP, HTTPs, Samba, PPPoE, UPnP, Bonjour, RTP, RTSP, RTCP Remote management supported Save/retrieve configuration files Brightness, contrast, saturation, Hue WDRC (Wide Dynamic Range Correction) Encoding type: H.264, MPEG4, MJPEG Resolution/frame rate(auto-sensing) 704 x 480, 352 x 240, 176 x 120, up to 30 fps (NTSC) 704 x 576, 352 x 288, 176 x 144, up to 25 fps (PAL) Compression: 5 levels Recording type: continuous, schedule, or motion detection HTTP port: 80 (default), RTSP (554) 3x Yes Synchronize with NTP server or set time/date manually Supported up to 2 destination accounts 100 entries - 76 - Recording Port Settings Digital Zoom Dynamic DNS Time SMTP System Log A.

2 GPIO Terminal Application Typically used in association with programming scripts for developing applications for motion detection, event triggering, alarm notification via e-mail, and a variety of external control functions. The 8-pin I/O Terminal Block is located on the rear panel and provides the interface to: a photocoupled switch output, a photo-coupled input, and RS-485 interface. The RS-485 is typically used for pan/tilt control.

Connector Pin Assignment PIN 1 Ground 2 IN1 Photo-Relay INPUT (+) 3 IN2 FUNCTION (common) SPECIFICATION GND Active High voltage 9~40VDC Dropout voltage 0 VDC. Close circuit current maximum 70mA AC or 100mA DC. 4 OUT+ Photo-Relay OUTPUT (Normal Open) Output resistance 30 Ohm. Open circuit voltage maximum 240V AC or 350V DC. 5 Ground 6 DC 12V 7 TX+ 8 TX(common) DC +12V output RS-485 (+) or (A) Compliant to RS-485. RS-485 (-) or (B) GND Power distribution: 250mA max. - 77 - Interface Schematic - 78 - A.4 Glossary of Terms NUMBERS 10BASE-T 100BASE-TX 10BASE-T is Ethernet over UTP Category III, IV, or V unshielded twisted-pair media. The two-pair twisted-media implementation of 100BASE-T is called 100BASE-TX. A ADPCM Adaptive Differential Pulse Code Modulation, a new technology improved from PCM, which encodes analog sounds to digital form.

AMR (Adaptive Multi-Rate) is an audio data compression scheme optimized for speech coding, which is adopted as the standard speech codec by 3GPP. Applets are small Java programs that can be embedded in an HTML page. The rule at the moment is that an applet can only make an Internet connection to the computer form that the applet was sent. American Standard Code For Information Interchange, it is the standard method for encoding characters as 8-bit sequences of binary numbers, allowing a maximum of 256 characters. Address Resolution Protocol. ARP is a protocol that resides at the TCP/IP Internet layer that delivers data on the same network by translating an IP address to a physical address. Audio Video Interleave, it is a Windows platform audio and video file type, a common format for small movies and videos. AMR Applet ASCII ARP AVI B BOOTP Bootstrap Protocol is an Internet protocol that can automatically configure a network device in a diskless workstation to give its own IP address. C - 79 - Communication Communication has four components: sender, receiver, message, and medium. In networks, devices and application tasks and processes communicate messages to each other over media.

They represent the sender and receivers. The data they send is the message. The cabling or transmission method they use is the medium. In networking, two devices establish a connection to communicate with each other. Connection D DHCP Developed by Microsoft, DHCP (Dynamic Host Configuration Protocol) is a protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network. In some systems, the device's IP address can even change while it is still connected. It also supports a mix of static and dynamic IP addresses. This simplifies the task for network administrators because the software keeps track of IP addresses rather than requiring an administrator to manage the task. A new computer can be added to a network without the hassle of manually assigning it a unique IP address.

DHCP allows the specification for the service provided by a router, gateway, or other network device that automatically assigns an IP address to any device that requests one. Domain Name System is an Internet service that translates domain names into IP addresses. Since domain names are alphabetic, they're easier to remember. The Internet however, is really based on IP addresses every time you use a domain name the DNS will translate the name into the corresponding IP address. For example, the domain name www.

network_camera.com might translate to 192.167.222.8.

DNS E Enterprise network An enterprise network consists of collections of networks connected to each other over a geographically dispersed area. The enterprise network serves the needs of a widely - 80 - distributed company and operates the company's missioncritical applications. Ethernet The most popular LAN communication technology. There are a variety of types of Ethernet, including 10Mbps (traditional Ethernet), 100Mbps (Fast Ethernet), and 1,000Mbps (Gigabit Ethernet). Most Ethernet networks use Category 5 cabling to carry information, in the form of electrical signals, between devices. Ethernet is an implementation of CSMA/CD that operates in a bus or star topology. F Fast Ethernet Firewall Fast Ethernet, also called 100BASE-T, operates at 10 or 100Mbps per second over UTP, STP, or fiber-optic media. Firewall is considered the first line of defense in protecting private information. For better security, data can be encrypted. A system designed to prevent unauthorized access to or from a private network.

Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially Intranets all messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria. G Gateway Group A gateway links computers that use different data formats together. Groups consist of several user machines that have similar characteristics such as being in the same department. H HEX Short for hexadecimal refers to the base-16 number system, which consists of 16 unique symbols: the numbers 0 to 9 and the letters A to F. For example, the decimal number 15 is represented as F in the hexadecimal numbering system. The hexadecimal system is useful because it can represent every byte (8 bits) as two consecutive hexadecimal digits. It - 81 - is easier for humans to read hexadecimal numbers than binary numbers. I Intranet This is a private network, inside an organization or company that uses the same software you will find on the public Internet. The only difference is that an Intranet is used for internal usage only. The Internet is a globally linked system of computers that are logically connected based on the Internet Protocol (IP).

The Internet provides different ways to access private and public information worldwide. To participate in Internet communications and on Internet Protocol-based networks, a node must have an Internet address that identifies it to the other nodes. All Internet addresses are IP addresses Internet Protocol is the standard that describes the layout of the basic unit of information on the Internet (the packet) and also details the numerical addressing format used to route the information. Your Internet service provider controls the IP address of any device it connects to the Internet. The IP addresses in your network must conform to IP addressing rules.

In smaller LANs, most people will allow the DHCP function of a router or gateway to assign the IP addresses on internal networks.

IP address is a 32-binary digit number that identifies each sender or receiver of information that is sent in packets across the Internet. For example 80.80.80.69 is an IP address. When you "call" that number, using any connection methods, you get connected to the computer that "owns" that IP address. ISP (Internet Service Provider) is a company that maintains a network that is linked to the Internet by way of a dedicated communication line. An ISP offers the use of its dedicated communication lines to companies or individuals who can't afford the high monthly cost for a direct connection. Internet Internet address IP IP address ISP - 82 - J JAVA Java is a programming language that is specially designed for writing programs that can be safely downloaded to your computer through the Internet without the fear of viruses. It is an object-oriented multi-thread programming best for creating applets and applications for the Internet, Intranet and other complex, distributed network. L LAN Local Area Network a computer network that spans a relatively small area sharing common resources. Most LANs are confined to a single building or group of buildings. M MJPEG MJPEG (Motion JPEG) composes a moving image by storing each frame of a moving picture sequence in JPEG compression, and then decompressing and displaying each frame at rapid speed to show the moving picture. MPEG4 is designed to enable transmission and reception of high-quality audio and video over the Internet and nextgeneration mobile telephones.

MPEG4 N NAT Network Address Translator generally applied by a router that makes many different IP addresses on an internal network appear to the Internet as a single address. For routing messages properly within your network, each device requires a unique IP address. But the addresses may not be valid outside your network. NAT solves the problem. When devices within your network request information from the Internet, the requests are forwarded to the Internet under the router's IP address. NAT distributes the responses to the proper IP addresses within your network. A network consists of a collection of two or more devices, people, or components that communicate with each other over physical or virtual media. The most common types of - 83 - Network network are: LAN (local area network): Computers are in close distance to one another. They are usually in the same office space, room, or building. WAN (wide area network): The computers are in different geographic locations and are connected by telephone lines or radio waves.

NWay Protocol A network protocol that can automatically negotiate the highest possible transmission speed between two devices. P PCM PING PCM (Pulse Code Modulation) is a technique for converting analog audio signals into digital form for transmission. Packet Internet Groper, a utility used to determine whether a specific IP address is accessible. It functions by sending a packet to the specified address and waits for a reply. It is primarily used to troubleshoot Internet connections.

Point-to-Point Protocol over Ethernet. PPPoE is a specification for connecting the users on an Ethernet to the Internet through a common broadband medium, such as DSL or cable modem. All the users over the Ethernet share a common connection. Communication on the network is governed by sets of rules called protocols. Protocols provide the guidelines devices use to communicate with each other, and thus they have different functions.

Some protocols are responsible for formatting and presenting and presenting data that will be transferred from file server memory to the file server's net work adapter Others are responsible for filtering information between networks and forwarding data to its destination. Still other protocols dictate how data is transferred across the medium, and how servers respond to workstation requests and vice versa. Common network protocols responsible for the presentation and formatting of data for a network operating system are the Internetwork Packet Exchange (IPX) protocol or the Internet Protocol (IP). - 84 - PPPoE Protocol Protocols that dictate the format of data for transferors the medium include token-passing and Carrier Sense Multiple Access with Collision Detection (CSMA/CD), implemented as token-ring, ARCNET, FDDI, or Ethernet. The Router Information Protocol (RIP),a part of the Transmission Control Protocol/Internet Protocol (TCP/IP) suite, forwards packets from one network to another using the same network protocol. R RJ-45 Router RTP RJ-45 connector is used for Ethernet cable connections. A router is the network software or hardware entity charged with routing packets between networks. RTP (Real-time Transport Protocol) is a data transfer protocol defined to deliver live media to the clients at the same time, which defines the transmission of video and audio files in real time for Internet applications. RTSP (Real-time Streaming Protocol) is the standard used to transmit stored media to the client(s) at the same time, which provides client controls for random access to the content stream. RTSP S Server SIP It is a simple computer that provides resources, such as files or other information.

SIP (Session Initiated Protocol) is a standard protocol that delivers the real-time communication for Voice over IP (VoIP), which establishes sessions for features such as audio and video conferencing. The Simple Mail Transfer Protocol is used for Internet mail. Simple Network Management Protocol. SNMP was designed to provide a common foundation for managing network devices. In LANs, a station consists of a device that can communicate data on the network. In FDDI, a station includes both physical nodes and addressable logical devices. - 85 - SMTP SNMP Station Workstations, single-attach stations, dual-attach stations, and concentrators are FDDI stations. Subnet mask In TCP/IP, the bits used to create the subnet are called the subnet mask. T (TCP/IP) Transmission Control Protocol/Internet Protocol is a widely used transport protocol that connects diverse computers of various transmission methods. It was developed y the Department of Defense to connect different computer types and led to the development of the Internet.

A transceiver joins two network segments together. Transceivers can also be used to join a segment that uses one medium to a segment that uses a different medium. On a 10BASE-5 network, the transceiver connects the network adapter or other network device to the medium. Transceivers also can be used on 10BASE-2 or 10BASE-T networks to attach devices with AUI ports. Transceiver U UDP User Name Utility UTP The User Datagram Protocol is a connectionless protocol that resides above IP in the TCP/IP suite The USERNAME is the unique name assigned to each person who has access to the LAN. It is a program that performs a specific task. Unshielded twisted-pair. UTP is a form of cable used by all access methods.

It consists of several pairs of wires enclosed in an unshielded sheath. W WAN Wide-Area Network. A wide-area network consists of groups of interconnected computers that are separated by a wide distance and communicate with each other via common carrier telecommunication techniques. WEP is widely used as the basic security protocol in Wi-Fi networks, which secures data transmissions using 64-bit or - 86 - WEP 128-bit encryption. Windows WPA Windows is a graphical user interface for workstations that use DOS. WPA (Wi-Fi Protected Access) is used to improve the security of Wi-Fi networks, replacing the current WEP standard. It uses its own encryption, Temporal Key Integrity Protocol (TKIP), to secure data during transmission. Wi-Fi Protected Access 2, the latest security specification that provides greater data protection and network access control for Wi-Fi networks. WPA2 uses the governmentgrade AES encryption algorithm and IEEE 802.1X-based authentication, which are required to secure large corporate networks. WPA2 - 87 - Limited Warranty TRENDnet warrants its products against defects in material and workmanship, under normal use and service, for the following lengths of time from the date of purchase. @@@@@@All products that are replaced become the property of TRENDnet.

Replacement products may be new or reconditioned. TRENDnet does not issue refunds or credit. Please contact the point-of-purchase for their return policies. @@There are no user serviceable parts inside the product. Do not remove or attempt to service the product by any unauthorized service center. This warranty is voided if (i) the product has been modified or repaired by any unauthorized service center, (ii) the product was subject to accident, abuse, or improper use (iii) the product was subject to conditions more severe than those specified in the manual. Warranty service may be obtained by contacting TRENDnet within the applicable warranty period and providing a copy of the dated proof of the purchase. Upon proper submission of required documentation a Return Material Authorization (RMA) number will be issued. An RMA - 88 - number is required in order to initiate warranty service support for all TRENDnet products. Products that are sent to TRENDnet for RMA service must have the RMA number marked on the outside of return packages and sent to TRENDnet prepaid, insured and packaged appropriately for safe shipment.

Customers shipping from outside of the USA and Canada are responsible for return shipping fees. Customers shipping from outside of the USA are responsible for custom charges, including but not limited to, duty, tax, and other fees. WARRANTIES EXCLUSIVE: IF THE TRENDNET PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, THE CUSTOMER'S SOLE REMEDY SHALL BE, AT TRENDNET'S OPTION, REPAIR OR REPLACE. THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESSED OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. TRENDNET NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION MAINTENANCE OR USE OF TRENDNET'S PRODUCTS.

TRENDNET SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLECT, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR OR MODIFY, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, OR OTHER HAZARD. LIMITATION OF LIABILITY: TO THE FULL EXTENT ALLOWED BY LAW TRENDNET ALSO EXCLUDES FOR ITSELF AND ITS SUPPLIERS ANY LIABILITY, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE OR PROFITS, LOSS OF BUSINESS, LOSS OF INFORMATION OR DATE, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE - 89 - SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF THE POSSIBILITY OF SUCH DAMAGES, AND LIMITS ITS LIABILITY TO REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT TRENDNET'S OPTION. THIS DISCLAIMER OF LIABILITY FOR DAMAGES WILL NOT BE AFFECTED IF ANY REMEDY PROVIDED HEREIN SHALL FAIL OF ITS ESSENTIAL PURPOSE. Governing Law: This Limited Warranty shall be governed by the laws of the state of California. Some TRENDnet products include software code written by third party developers.

These codes are subject to the GNU General Public License ("GPL") or GNU Lesser General Public License ("LGPL"). Go to http://www.trendnet.com/gpl or http://www.trendnet.com Download section and look for the desired TRENDnet product to access to the GPL Code or LGPL Code. These codes are distributed WITHOUT WARRANTY and are subject to the copyrights of the developers. TRENDnet does not provide technical support for these codes. Please go to http://www.gnu.

org/licenses/gpl.txt or http://www.gnu.org/licenses/lgpl.txt for specific terms of each license. - 90 - - 91 - .