GS108T Smart Switch
Software Administration
Manual

NETGEAR

NETGEAR, Inc.
4500 Great America Parkway
Santa Clara, CA 95054 USA

202-10337-01
December 2007

Manual abstract:

@@@@@@NETGEAR does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein. Information is subject to change without notice. Certificate of the Manufacturer/Importer It is hereby certified that the GS108T Gigabit Smart Switch has been suppressed in accordance with the conditions set out in the BMPT-AmtsblVfg 243/1991 and Vfg 46/1992. The operation of some equipment (for example, test transmitters) in accordance with the regulations may, however, be subject to certain restrictions. Please refer to the notes in the operating instructions. The Federal Office for Telecommunications Approvals has been notified of the placing of this equipment on the market and has been granted the right to test the series for compliance with the regulations. Voluntary Control Council for Interference (VCCI) Statement This equipment is in the first category (information equipment to be used in commercial and/or industrial areas) and conforms to the standards set by the Voluntary Control Council for Interference by Data Processing Equipment and Electronic Office Machines that are aimed at preventing radio interference in commercial and/or industrial areas. Consequently, when this equipment is used in a residential area or in an adjacent area thereto, radio interference may be caused to equipment such as radios and TV receivers. Federal Communications Commission (FCC) Compliance Notice: Radio Frequency Notice This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: This device may not cause harmful interference.

This device must accept any interference received, including interference that may cause undesired operation. NOTE: This equipment has been tested and found to comply with the limits for a Class A 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. ii v1. 0, December 2007 • • Connect the equipment into an outlet on a circuit different from that which the receiver is connected. Consult the dealer or an experienced radio/TV technician for help.

In a domestic environment, this product may cause radio interference, in which case the user may be required to take appropriate measures. Canadian Department of Communications Radio Interference Regulations This digital apparatus (NETGEAR GS108T Gigabit Smart Switch) does not exceed the Class A limits for radio-noise emissions from digital apparatus as set out in the Radio Interference Regulations of the Canadian Department of Communications. règlement sur le brouillage radioélectrique du ministère des Communications Cet appareil numérique (NETGEAR GS108T Gigabit Smart Switch) respecte les limites de bruits radioélectriques visant les appareils numériques de classe A prescrites dans le Règlement sur le brouillage radioélectrique du ministère des Communications du Canada. Customer Support For assistance with installing and configuring your NETGEAR system or for questions or problems following installation: • • • • Check the NETGEAR Web page at http://www. If you are outside North America, please refer to the phone numbers listed on the Support Information Card that was included with your switch. Defective or damaged merchandise can be returned to your point-of-purchase representative. Internet/World Wide Web NETGEAR maintains a World Wide Web home page that you can access at the uniform resource locator (URL) http:// www. A direct connection to the Internet and a Web browser such as Internet Explorer or Netscape are required. FCC Requirements for Operation in the United States FCC Information to User: This product does not contain any user-serviceable components and is to be used with approved antennas only. Any product changes or modifications will invalidate all applicable regulatory certifications and approvals FCC Guidelines for Human Exposure: This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment.

This equipment should be installed and operated with a minimum distance of 20 cm iii v1. 0, December 2007 between the radiator and your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter. fCC Declaration Of Conformity: We , NETGEAR , Inc. , 4500 Great America Parkway, Santa Clara, CA 95054, declare under our sole responsibility that the model GS108T: ProSafe™ 8 Port 10/100/1000 smart switch complies with Part 15 of FCC Rules. Operation is subject to the following two conditions: a) This device may not cause harmful interference and b) This device must accept any interference received, including interference that may cause undesired operation. 1-5 NIC Setting on the Host That Accesses the GS108T Gigabit Smart Switch . 1-9 Chapter 2 Introduction to the Web Browser Interface Logging In to the NETGEAR Home Page . 0, December 2007 ix About This Manual The NETGEAR® GS108T Smart Switch Software Administration Manual describes how to install, configure, operate, and troubleshoot the GS108T Gigabit Smart Switch using its included software. This book describes the software configuration procedures and explains the options available within those procedures.

Who Should Use This Book The information in this manual is intended for readers with intermediate to advanced system management skills. This document was created primarily for the system administrator who wishes to install and configure the GS108T Smart Switch in a network. it assumes that the reader has a general understanding of switch platforms and a basic knowledge of Ethernet and networking concepts. To install this switch, it is not necessary to understand and use all of its capabilities. Once basic configuration is performed, it will function in a network using its remaining factory default settings. However, a greater level of configuration—anywhere from the basic up to the maximum possible—will allow your network the full benefit of the switch's features. The Web interface simplifies this configuration at all levels. How to Use This Book This document describes configuration menu commands for the GS108T Smart Switch software. The commands can all be accessed from the Web interface.

Chapter 1, “Getting Started with Switch Management,” describes how to use the Smart Wizard Discovery utility to set up your switch so that you can communicate with it.

Chapter 2, “Introduction to the Web Browser Interface,” introduces the Web browser interface. • • Chapter 3, “Managing System Settings,” describes how to configure the system functions. Chapter 4, “Configuring Switching,” describes how to configure the switching functions. Chapter 5, “Configuring QoS and Security,” describes how to configure QoS and security functions. x v1. 0, December 2007 GS108T Smart Switch Software Administration Manual • • • • Chapter 6, “Monitoring, Maintenance, and Help,” describes the logs, the reset functions, the firmware upgrade procedure, and the help options. Appendix C, “Network Cabling,” gives cabling requirements and describes some details of port cabling connections. Note: See the product release notes for the GS108T Smart Switch Software application level code. The release notes detail the platform-specific functionality of the Switching, SNMP, Config, and Management packages. Conventions, Formats, and Scope The conventions, formats, and scope of this manual are described in the following paragraphs: • Typographical conventions.

This manual uses the following typographical conventions: Italics Bold Fixed Italics Emphasis, books User input, IP addresses, GUI screen text Command prompt, CLI text, code URL links • Formats. This manual uses the following formats to highlight special messages: Note: This format is used to highlight information of importance or special interest. Tip: This format is used to highlight a procedure that will save time or resources. Warning: Ignoring this type of note might result in a malfunction or damage to the equipment. Failure to take heed of this notice might result in personal injury or death. • Scope. This manual is written for the GS108T Smart Switch according to these specifications: Product Version Manual Publication Date . GS108T Gigabit Smart Switch December 2007 Note: Product updates are available on the NETGEAR, Inc. How to Use This Manual The HTML version of this manual includes the following: • • Buttons a time. And for browsing forward or backward through the manual one page at A button that displays the table of contents and a button that displays an index.

Double-click a link in the table of contents or index to navigate directly to where the topic is described in the manual. Online knowledge base for the product • • Links to PDF versions of the full manual and individual chapters. How to Print This Manual To print this manual, choose one of the following options: • • Printing a page from HTML. Each page in the HTML version of the manual is dedicated to a major topic. Select File > Print from the browser menu to print the page contents.

printing from PDF. Your computer must have the free Adobe Acrobat Reader installed in order for you to view and print PDF files. The Acrobat Reader is available on the Adobe website at http://www. Click the PDF of This Chapter link at the top left of any page in the chapter you want to print. The PDF version of the chapter you were viewing opens in a browser window.

Click the print icon in the upper left of your browser window. • – Printing a PDF version of the Complete Manual. • Click the Complete PDF Manual link at the top left of any page in the manual. The PDF version of the complete manual opens in a browser window. Click the print icon in the upper left of your browser window. Tip: If your printer supports printing two pages on a single sheet of paper, you can save paper and printer ink by selecting this feature. 0, December 2007 About This Manual Chapter 1 Getting Started with Switch Management This chapter provides an overview of switch management, including the methods you can choose to start managing your NETGEAR GS108T Gigabit Smart Switch. It also leads you through the steps necessary to get started, using the Smart Wizard Discovery utility. The information is discussed in the following sections: • “System Requirements” • “Switch Management Interface” • “Network with a DHCP Server” • “Network without a DHCP Server” • “Web Access” • “Additional Utilities” System Requirements The following hardware and software facilities are required to run the applications described in this manual: • Network facilities: – Ethernet network with or without DHCP server as appropriate – Ethernet cable to connect the switch to a PC For running the Smart Wizard Discovery utility and local or remote Web management: – IBM-type PC with CD drive. RAM size and disk specification are not critical.

Note: For complete hardware installation instructions, see the GS108T Smart Switch Hardware Installation Guide included on your Resource CD, or go to http://www. This switch functions as a simple switch without the management software. However, you can use the management software to configure more advanced features and consequently improve switch efd (NIC) under the MS Windows OS in Windows screens similar to the following one. For comparison, the settings screens of the switch are also shown, although they do not appear in the Windows view. Getting Started with Switch Management v1. 0, December 2007 1-5 GS108T Smart Switch Software Administration Manual Figure 1-4 You need Windows administrator privileges to change these settings. 1. On your PC, access the MS Windows operating system TCP/IP Properties. 2. Set the IP address and subnet mask appropriately.

The subnet mask value should be identical to that set in the switch. The PC IP address must be different from that of the switch but must be in the same subnet. 3. Click Web Access in the Smart Wizard Discovery utility to enable the management screens described in the following section. Web Access For Web access, you do either of the following: • • Using the Smart Wizard Discovery utility, click Web Access (see “Network with a DHCP Server” or “Network without a DHCP Server”).

Access the switch directly, without using the Smart Wizard Discovery utility. You must work from the same network segment that contains the switch (that is, the subnet mask values of switch and PC host must be the same), and you must point your browser using the switch IP address. If you used the Smart Wizard Discovery utility to set up IP address and subnet mask, either with or without DHCP server, use that IP address in your browser window. 1-6 Getting Started with Switch Management v1. 0, December 2007 GS108T Smart Switch Software Administration Manual If you are starting with an “out-of-the-box” switch and are not using the Smart Wizard Discovery utility, you must initially configure your host PC to be on a network segment to match the default settings of the switch, which are as follows: • IP address: 192.

0 Later, you might want to change the network settings to match those of your network (this procedure is described in "IP Configuration" on page 3-3). Your host PC network settings must then also be set back to match your network. Clicking Web Access on the Smart Wizard Discovery utility or accessing the switch directly displays the following screen. . Figure 1-5 Use this screen to proceed to management of the switch, as covered in Chapter 2, "Introduction to the Web Browser Interface. □ Additional Utilities Alternatively, from the main screen shown in Figure 1-1 on page 1-3 you can access additional functions as described in the following sections: • "Password Change" • "Firmware Upgrade" Getting Started with Switch Management v1. 0, December 2007 1-7 GS108T Smart Switch Software Administration Manual Password Change You can set a new password of up to 20 ASCII characters. You can set a new password. Enter the new password, and enter is again to confirm it. Note: You can also upgrade the firmware using the File Download screen of the switch (see "File Download" on page 6-20).

If you click Firmware Upgrade in the main screen (see Figure 1-1 on page 1-3), after you have selected the switch to upgrade, the following screen displays: . Figure 1-6 1-8 Getting Started with Switch Management v1. 0, December 2007 GS108T Smart Switch Software Administration Manual The application software for the GS108T Smart Switch is upgradeable, so you can take advantage of improvements to your switch and additional features as they become available. The upgrade procedure and the required equipment are described as follows. This procedure assumes that you have downloaded or otherwise obtained the firmware upgrade and that you have it available as a binary file on your computer. For information about downloading firmware, see "File Download" on page 6-20. □ This procedure uses the TFTP protocol to implement the transfer from computer to switch. 1. Enter the following values into the appropriate places in the form: • • • Firmware Path. The location of the new firmware.
If you do not know the location, you can click Browse to locate the file. password. Enter your password; the default password is password. When the process is complete, the switch automatically reboots. Exit Click Exit in the Switch Setting section to close the Smart Wizard Discovery utility.
Getting Started with Switch Management v1. 0 , December 2007 1-9 GS108T Smart Switch Software Administration Manual 1-10 Getting Started with Switch Management v1. 0, December 2007 Chapter 2 Introduction to the Web Browser Interface This section introduces the browser interface that lets you configure and manage your NETGEAR GS108T Gigabit Smart Switch. Your GS108T Smart Switch provides a built-in browser interface that lets you configure and manage it remotely using a standard Web browser such as Microsoft Internet Explorer or Netscape Navigator. Online help is also provided for many of the basic functions and features of the switch.
Note: When a screen displays, click the help icon the screen settings. For additional information about This section introduces the areas of the browser interface and includes the following topics: • • "Logging In to the NETGEAR Home Page" "Navigation Tabs" Logging In to the NETGEAR Home Page Begin your overview of the GS108T Smart Switch browser interface by logging in: 1. Start the application, either through the Smart Wizard Discovery utility or directly by entering the switch's IP address, as described in Chapter 1, "Getting Started with Switch Management. Enter the password (the factory default is password), and click Login. The first screen of the GS108T Smart Switch browser interface is displayed. Figure 2-2 2-2 Introduction to the Web Browser Interface v1. 0, December 2007 GS108T Smart Switch Software Administration Manual The navigation tabs across the top provide access to all the configuration functions of the switch, and remain constant. The menu items in the blue bar change according to the navigation tab that is selected. For further description of the functions, see the appropriate section of this manual: • • • • Chapter 3, "Managing System Settings," describes how to configure the system functions. Chapter 4, "Configuring Switching," describes how to configure the switching functions.

Chapter 5, "Configuring QoS and Security," describes how to configure the QoS and security functions. Chapter 6, "Monitoring, Maintenance, and Help," describes how to display statistics, how to reset the switch, how to upload and download files such as firmware, and how to obtain further help. Click the Logout button to log out of the browser interface. 0, December 2007 Chapter 3 Managing System Settings Using the System Tab The navigation tabs on the top of the home page include a System tab that lets you manage your GS108T Gigabit Smart Switch using features under the following main menu commands and subcommnands: • "Management" • "System Information" • "IP Configuration" • "Time" "SNMP" • "SNMP V1/V2" "LLDP" • "Basic—LLDP Configuration" • "Advanced—LLDP Configuration" • "Advanced—LLDP Port Settings" • "Advanced—Local Information" • "Advanced—Neighbors Information" • • The sections that follow in this chapter cover these features and tell you how to set them in the GS108T Smart Switch. Management This section describes how to display the switch status and specify some basic switch information, how to configure the system IP address source, and how to configure the system clock source. 3-1 v1. 0, December 2007 GS108T Smart Switch Software Administration Manual System Information The System Information screen displays the system settings and lets you to change some of the configurable settings of the switch: 1. You can also change some of the configurable fields of the switch: • Product Name. Shows the switch model name. You can assign a system name for the switch.
This name lets you track your switch. You can assign a location name for the switch. This field assists you in keeping track of which switch you are connected to when you are connected to your switch remotely. You can assign a duration for login time-out. Users are automatically logged out when the login session remains idle after the specified duration.
This allows other users to access the switch if one forgets to log out. Shows the IP address of the switch. subnet mask. Shows the subnet mask of the IP address. default gateway.
Shows the IP address of the gateway for the remote manager. mAC address. Shows the MAC address of the switch. system UpTime.

Shows the switch up time after bootup. 3. Click Apply if you have made any change to the System Name, System Location, or Idle Timeout setting. 4. View the system hardware and software version information under the Versions heading: • Model Name. Shows the switch model name.

Shows the boot code version of the switch. • Software Version. Shows the software version of the switch. IP Configuration The IP Configuration screen lets you set the system IP address source and optional management VLAN: 1. Select the appropriate radio button for your IP configuration: • Get Dynamic IP from DHCP Server. Specifies that the switch must obtain the IP address through a DHCP server. • Get Dynamic IP from BootP Server. Specifies that the switch must obtain the IP address through a BootP server. • Static IP Address. Specifies that the IP address, subnet mask, and default gateway must be manually configured.

Enter this information in the fields below this radio button. 3. Select the management VLAN ID (the default is 0 for all VLANs). The management VLAN is used to establish an IP connection to the switch from a workstation that is connected to a port in the VLAN. If not specified, the active management VLAN ID is 0 (default), which allows an IP connection to be established through any port.

When the management VLAN is configured, an IP connection can be made only through a port that is part of the management VLAN. It is also mandatory that the port VLAN ID (PVID) of the port to be connected in that management VLAN be the same as the management VLAN ID. • • • Only one management VLAN can be active at a time. When a new management VLAN is configured, connectivity through the existing management VLAN is lost. The management station should be reconnected to the port in the new management VLAN.

Note: Make sure that the VLAN to be configured as the management VLAN exists. And make sure that the PVID of at least one port that is a port of the VLAN is the same as the management VLAN ID. Time Simple Network Time Protocol (SNTP) synchronizes time across the network. □ The time interval at which the switch polls for time is called the polling time and is set to 30 minutes. As long as the NTP/SNTP server is reachable, the switch polls for time every 30 minutes and updates the system time. 3-4 v1. 0, December 2007 Managing System Settings GS108T Smart Switch Software Administration Manual • The time-out period is the time duration for which the switch waits for a reply from the server. time-out is set to 15 seconds. If two NTP/SNTP servers are specified and neither one is available, then the total time-out is 30 seconds. You can specify whether to set the system time manually or with an SNTP server: 1.

Date and time are calculated through a local clock source that is based on CPU cycles. Date and time are selected through an SNTP server. go to step 5 3. When setting the date and time through a local clock source, enter the following: a. date. Specify the date to which the switch is set in the DD/MM/YYYY format. Specify the switch time in the HH:MM:SS format. Select the local time zone in which the switch is operating. 5. When setting the date and time through an SNTP server, enter the following settings: a.

In the NTP Server IP - 1 field, specify the IP address of the primary NTP/SNTP server for the switch to use when synchronizing time. b. In the NTP Server IP - 2 field, specify the IP address of alternate NTP/SNTP server for the switch to use when synchronizing time. SNMP V1/V2 The SNMP V1/V2 screen lets you limit the IP addresses that can access the management information base (MIB) of the switch and to which the switch sends the traps. The switch responds only to requests from management stations that have their IP address in the management station list.

You can also select the traps that the switch sends to the management station after a trap event. The setting of a management station is not active until you set the Status field to Enable. Under Community Configuration & Trap Flags, view or specify the SNMP settings for up to four management stations: • Management Station. The community string provides an authentication mechanism to the SNMP protocol. The switch processes requests from the management station only if the community string in the request packet matches the community string that is specified in the Community String field. • Access Mode. Sets the access privilege (Read Only or Read Write) state of the management station. • Trap (T2). Enables the switch to generate an SNMP trap when it reboots. Enables the switch to generate an SNMP trap when one of its ports changes its link status. If you have selected one or more management stations for removal, click Remove. If you have made any changes to an existing management station, click Apply. 4. Under Authentication Fail Trap, select the Enable Authentication Fail Trap check box to enable the switch to generate an SNMP trap for all management stations when a computer attempts to gain access to the switch through SNMP but the computer's IP address is not in the SNMP management station table. 5.

If you have made changes to the Enable Authentication Fail Trap check box, click Apply. LLDP Link Layer Discovery Protocol (LLDP) is a one-way protocol that provides the following capabilities: • • An LLDP agent can transmit information about the capabilities and current status of the switch associated with its MAC Service Access Point (MSAP) identifier. An LLDP agent can also receive information about the capabilities and current status of the switch associated with a remote MSAP identifier. LLDP agents do not solicit information from other LLDP agents using LLDP. Basic—LLDP Configuration The Basic LLDP Configuration screen lets you to enable or disable LLDP and configure the basic LLDP settings: 1. When LLDP is disabled, select how LLDP packets are processed from the LLDPDU Handling drop-down list: • Flooding. lLDPDU packet flooding is enabled. LLDP packets that are received from another LLDP device are flooded, that is, the packets are forwarded to all devices that are attached to the switch. LLDP packets that are received from another LLDP device are dropped. 4.

When LLDP is enabled, the following configurable LLDP settings are displayed: • TLV Advertised Interval (5–32768 sec). The interval at which LLDP frames are transmitted on behalf of this LLDP agent. The result is the time-tolive (TTL) value for the information that is advertised. The minimum delay period from the time a port becomes disabled until its reinitialization. The delay between successive LLDP frame transmissions that are initiated by a value or status changes in the local system.

The interval at which notifications are generated when remote MSAP information changes. The number of successive LLDP frame transmissions for one complete fast-start interval. Advanced—LLDP Port Settings When LDDP is enabled, you can view the LLDP port settings in the LDDP Port Settings screen: 1.

You can make changes to the LLDP settings for an individual port, for a group of ports, or for all ports simultaneously: • To change the LLDP settings for an individual port, select the check box to the left of its port number, and then select the LLDP port settings. managing System Settings v1. 0, December 2007 3-9 GS108T Smart Switch Software Administration Manual • • To change the LLDP settings for a group of ports, select the check boxes to the left of their port numbers, and then select the LLDP port settings. To change the LLDP settings for all ports simultaneously, select the check box at the top of the column of check boxes, and then select the LLDP port settings. The following information about the LLDP configuration for a port is displayed: • Ports. The administratively assigned status of the local LLDP agent. The possible field values are: – TX Only. Specifies that transmission of local LLDP information only is enabled. – RX Only. Specifies that reception of remote LLDP information only is enabled. – TX and RX. Specifies that both transmission and reception of LLDP information are enabled.

– Disable. Specifies that both transmission and reception of LLDP information are disabled. • Notification. Specifies whether or not transmission notifications are enabled. • MED Notification. Specifies whether or not Media Endpoint Discovery (MED) transmission notifications are enabled. • Optional TLVs. Specifies whether or not the transmission of threshold limit values (TLVs) is enabled. 0, December 2007 Managing System Settings GS108T Smart Switch Software Administration Manual Advanced—Local Information When LDDP is enabled, you can view the LLDP local information in the Local Information screen, which is also referred to as the LLDP Local Device Information screen: Select System > LLDP > Advanced > LLDP Port Settings. Shows the basis for the chassis ID entity.

chassis ID. Shows the identifier for the particular chassis in the system. Shows a textual description of the network entity, including the full name and version identification of the system's hardware type. system Capabilities. Shows the primary functions of the system.

enabled Capabilities. Shows which of the primary functions are enabled. mED Device Type. Shows whether the device is a MED device. management Address.

Shows the address that is associated with the LLDP agent that can be used to reach higher-layer entities to assist discovery by network management. table 3-1. Management Address Item Address Sub-type Address Interface Sub-type Interface Number OID Description Shows the type of address that is listed in the management address field. shows the management IP address. Shows the numbering method used for defining the interface number. Shows the specific address associated with the management address. Shows the type of hardware component or protocol entity that is associated with the management address. Shows the basis for the identifier that is listed in the Port ID field. • Port ID. Shows the identifier for the port from which the LLDPDU was transmitted.

0, December 2007 Managing System Settings GS108T Smart Switch Software Administration Manual Under Port Information, click a port number in the Port column. a screen similar to the following displays. Figure 3-8 The following LLDP local port information is displayed: Table 3-2. MSAP Details Item Port ID SubType Port ID Description The basis for the identifier that is listed in the Port ID field. Identifier for the port from which LLDPDU was transmitted. 3 Set Details Item Auto-Negotiation Aggregator Status Aggregator Id Maximum Frame Size Description If autonegotiation supported and enabled in both the systems, there should be no speed difference. Whether the port through which LLDPDU is transmitted is aggregated or not. port ID information for the aggregated port. Maximum size of a frame that can be transmitted. Advertisement of this TLV by endpoints enables LLDP-MED-capable network connectivity devices to determine support of LLDP-MED by endpoints that they are connecting to.

Device Type A specific type of LLDP-MED device, which can be either a network connectivity device or a specific class of endpoint device. Location Format Location ID Shows the specific Location ID data format being delivered in the Location ID field. Three Location ID data formats are defined: • Coordinate-based LCI data format • Civic Address LCI data format • ECS ELIN data format Shows whether LLDP-MED device transmitting the LLDPDU is a Power Sourcing Entity (PSE) or Power Device (PD). The power source being utilized by a PSE or PD device. The priority of the PD type device to the power being supplied by the PSE type device, or the power priority associated with the PSE type device's port that is sourcing the power through MDI.

MED Set Details (continued) Item Description Power Value Shows the total power in watts required by a PD device from a PSE device, or the total power a PSE device is capable of sourcing over a maximum-length cable based on its current configuration. Network Policies Network policy is associated with multiple sets of application types supported on a given port. • Application Type. Integer value indicating the primary function of the applications defined for this network policy, advertised by an endpoint or network connectivity device. • Unknown Policy.

Shows that an endpoint device wants to explicitly advertise that this policy is required by the device but is currently unknown. • Tagged. Shows whether the specified application type is using a tagged or an untagged VLAN. • VLAN ID. Contains the VLAN identifier (VID) for the port. • L2 Priority. Shows the Layer 2 priority to be used for the specified application type. • DSCP. Contains the DSCP value to be used to provide Diffserv node behavior for the specified application type. Advanced—Neighbors Information When there are local LLDP neighbors, you can view the remote information in the Neighbors Information screen: Select System > LLDP > Advanced > Neighbors Information.

Figure 3-9 Under Neighbors Information, the following information is displayed: • MSAP Entry. Shows the MSAP identifier from which the LLDPPU was transmitted. • Local Port. Shows the local port on which the LLDPDU was received. Shows the basis for the chassis ID that is listed in the Chassis ID field. chassis ID. Shows the chassis ID of the system from which the LLDPPU was transmitted. port ID SubType. Shows the basis for the identifier that is listed in the Port ID field. port ID.

Shows the port from which the LLDPDU was transmitted. 3-16 v1. 0, December 2007 Managing System Settings Chapter 4 Configuring Switching Using the Switching Tab The navigation tabs on the top of the home page include a Switching tab that lets you manage your GS108T Gigabit Smart Switch using features under the following main menu commands and subcommnands: • • "Ports" • "Port Configuration" "LAG" • "Basic—LAG Configuration" • "Basic—LAG Membership" • "Advanced—LAG Configuration" • "Advanced—LAG Membership" • "Advanced—LACP Configuration" • "Advanced—LACP Port Configuration" "VLAN" • "Basic—VLAN Configuration" • "Advanced—VLAN Configuration" • "Advanced—VLAN Membership" • "Advanced—Port PVID Configuration" "STP" • "Basic—RSTP Configuration" • "Advanced—RSTP Configuration" • "Advanced—Port Configuration" "Multicast" • "IGMP Snooping" • "Static Multicasting" • "Multicast Group Membership" 4-1 v1.

0, December 2007 • • • GS108T Smart Switch Software Administration Manual • • "Switch Configuration" • "Jumbo Frame Configuration" "Address Table" • "Static Address" • "Dynamic Address" The sections that follow in this chapter cover these features and tell you how to configure them in the GS108T Smart Switch. Ports You can define speed, duplexing, and flow control operation for a port when autonegotiation is off.

When autonegotiation is on, those data are negotiated from the link partner. Otherwise, you can enable or disable ports to control packet forwarding. Port Configuration The Port Configuration screen lets you to define the port switching settings: 1. You can make changes to the port switching settings for an individual port, for a group of ports, or for all ports simultaneously: • To change the port switching settings for an individual port, select the check box to the left of its port number, and then select the port switching settings. Note: You can also enter the interface number (that is, the port number) in the GO TO INTERFACE field, and then click GO.

□ • To change the port switching settings for a group of ports, select the check boxes to the left of their port numbers, and then select the port switching settings. To change the port switching settings for all ports simultaneously, select the check box at the top of the column of check boxes, and then select the port switching settings. The following port switching settings are displayed for all ports. Except for the Interface and Link Status fields, all fields are configurable. Shows whether the link is up or down. • Port Speed. Specifies the speed for the port. the possible fields values are: – 100M. Specifies that the port speed is 100 Mbps. – 10M.

Specifies that the port speed is 10 Mbps. Select this mode when you want the port speed to function at 1000 Mbps. – Disable. Specifies that the port speed is disabled. This mode can be enabled only when the port speed is 10 Mbps or 100 Mbps. • Flow Control. Specifies whether flow control support is enabled or disabled: – Enable. If the port receives a pause frame, it halts for a certain period before sending out a frame. Specifies the packet priority for packets arriving at the port without tagging. the possible fields values are: 0–7.

If packet arrives with a tag or priority tag, the priority is retrieved from the priority field of the tag. 3ad) that allows several physical ports to be bundled together to form a single logical channel. Link aggregation allows one or more links to be aggregated together to form a LAG, such that a MAC client can treat the LAG as if it were a single link. Link aggregation can be used on 10-Mbps, 100-Mbps, or 1000-Mbps Ethernet full-duplex ports. Example: A network administrator could combine a group of five 100-Mbps ports into a logical link that will function as a single 500-Mbps port (the actual throughput, however, will be less than the total sum of the links).

Basic—LAG Configuration The Basic LAG Configuration screen lets you define the status and administration settings for up to two available LAGs. However, you first have to define the members of the LAGs. You can make changes to the LAG settings for an individual LAG or for both LAGs simultaneously: • To change the LAG settings for an individual LAG, select the check box to the left of its LAG ID, and then select the LAG settings. □ To change the LAG settings for both LAGs simultaneously, select the check box at the top of the column of check boxes, and then select the LAG settings. The following LAG settings are displayed for both LAGs.

Except for the LAG ID and LAG State fields, all fields are configurable. Shows whether the LAG is enabled or disabled. • LACP. Specifies whether LACP enabled or disabled for the LAG. (If the administrative mode is disabled, LACP cannot be up. This implies that static trunking is enabled. Note: In order for you to successfully apply a LAG configuration, all members of the trunk must be selected before you enable the LAG configuration, must have the same speed and duplex modem, and must be either linked or unlinked. Basic—LAG Membership The Basic LAG Membership screen lets you define the ports that are aggregated together to form a single LAG. There are certain requirements for a LAG: • Each port can belong to only one LAG. • Each LAG can have up to four ports.

□ Ports in a LAG must have the same speed and be in the same VLAN group. Select up to four ports for membership in the LAG by selecting the check boxes below the port numbers. 0, December 2007 Configuring Switching GS108T Smart Switch Software Administration Manual Advanced—LACP Configuration The LACP Configuration screen lets you set the LACP system priority, which specifies the device's link aggregation priority relative to the devices at the other ends of the links on which link aggregation is enabled. Figure 4-5 The LACP System Setting field is the only configurable field in this screen: • LACP System Setting. lACP Port priority ranges from 0 to 65536. A higher value indicates a lower priority. Advanced—LACP Port Configuration The LACP Port Configuration screen, which is also referred to as the LACP Port Priority screen, lets you set the LACP port priority and time-out value: 1. You can make changes to the LACP port priority settings for an individual port, for a group of ports, or for all ports simultaneously: • To change the LACP port priority settings for an individual port, select the check box to the left of its port number, and then select the LACP port priority settings. Note: You can also enter the interface number (that is, the port number) in the GO TO INTERFACE field, and then click GO. □ • To change the LACP port priority settings for a group of ports, select the check boxes to the left of their port numbers, and then select the LACP port priority settings.

To change the LACP port priority settings for all ports simultaneously, select the check box at the top of the column of check boxes, and then select the LACP port priority settings. The following information about the LACP priority for a port is displayed. Both the LACP Priority and Timeout fields are configurable. Specifies the port priority value in a range from 1 to 65335. The possible field values are: – Long.

VLAN A virtual local area network (VLAN) is a way to electronically separate ports on the same switch (from a single broadcast domain) into separate broadcast domains so that broadcast packets are not sent to all the ports on a single switch. When you use a VLAN, users can be grouped by logical function instead of physical location. 1Q VLAN screen control the VLAN membership of each port for transmitting packets. Also, these settings determine if transmitted packets from each port are tagged with the VLAN ID and other information.

the switch supports 64 tag-based VLANs.

By default, every port is a member of VLAN 1, and so they have a port VLAN ID (PVID) of 1. □ Port-based VLANs Single or multiple ports are grouped into a smaller virtual network, which is independent of the other ports. the switch supports 8 port-based VLANs. Any user-assigned VLAN cannot have member ports that belong to different port groups. Basic—VLAN Configuration The Basic VLAN Configuration screen lets you select the VLAN type and create VLANs. You can select to create either IEEE 802. 1Q VLANs or port-based VLANs. The screen functions differently for IEEE 802. 1Q VLANs than it does for port-based VLANs. Warning: Changing the VLAN type erases all existing VLAN settings, static multicast groups, and trusted MAC addresses.

The following information about the VLAN configuration is displayed. Both the VLAN ID and VLAN Name fields are configurable: • • VLAN ID. Enter a number in the VLAN ID field. b. Enter a name in the VLAN Name field. Select the check box to the left of the VLAN ID that you want to remove. Select the check box to the left of the VLAN ID that you want to change. b. Enter a new name in the VLAN Name field. Select the Port-Based radio button to specify the port-based VLAN type.

Warning: Changing the VLAN type erases all existing VLAN settings, static multicast groups, and trusted MAC addresses. In the VLAN Name field, enter an optional VLAN name. Perform one of the following actions: • To add a VLAN: – – – • Select the check box to the left of one of the VLAN IDs. Enter a VLAN name in the VLAN Name field. click Add.

To delete a VLAN: – – Select the check box to the left of the VLAN ID that you want to remove. click Delete. □ To change a VLAN name: – – – Select the check box to the left of the VLAN ID that you want to change. Enter a new name in the VLAN Name field. Advanced—VLAN Membership The VLAN Membership screen lets you set the VLAN membership of each port.

The screen functions differently for port-based VLANs than it does for IEEE 802. 1Q VLAN Membership Note: By default, every port is a member of VLAN 1, which has a port VLAN ID (PVID) of 1. From the VLAN Identifier drop-down list, select the number that represents the VLAN you want to view or modify. You can either assign the same tag setting to or remove it from all ports in the VLAN in step 3, or assign a tag setting to or remove it from each individual port in the VLAN in step 4. These steps are mutually exclusive. 3. To assign the same tag setting to or remove it from all ports in the VLAN, toggle the check box to the left of Unit 1. The tag setting determines if packets that are transmitted from each port are tagged with the VLAN ID and other information. the possible tag settings are: – T. Specifies that the egress (outgoing) packet is tagged for all ports.

– U. Specifies that the egress packet is untagged for all ports. – Empty. Specifies that none of the ports are part of the VLAN. 4. To assign a tag setting to or remove it from an individual port in the VLAN: a. Assign a tag setting to or remove it from a port by toggling the check box under an individual port number. The tag settings determine if packets that are transmitted from the port are tagged with the VLAN ID and other information. the possible tag settings are: – – – T. Specifies that the egress packet is tagged for the port.

u. Specifies that the egress packet is untagged for the port. empty. Specifies that the port is not part of the VLAN. From the VLAN Identifier drop-down list, select the number that represents the VLAN you want to view or modify.

You can either assign all ports to or remove them from the VLAN in step 3, or assign individual ports to or remove them from the VLAN in step 4. These steps are mutually exclusive. 3. To assign all ports to or remove them from the VLAN, select the check box to the left of Unit 1. 4.

To assign individual ports to or remove them from the VLAN: a. To assign a port to or remove it from the VLAN, select the check box under an individual port number. Note: When the port-based VLAN type is configured, an ingress (incoming) packet with an IEEE 802. There are certain requirements for a PVID: • All ports must have a defined PVID. □ If no other value is specified, the default VLAN PVID is used. □ If you want to change the port's default PVID, you must first create a VLAN group that includes the port. You can make changes to the port PVID settings for an individual port or for a group of ports: • To change the port PVID setting for an individual port, select the check box to the left of its port number, and then enter an existing VLAN ID in the PVID field. Note: You can also enter the interface number (that is, the port number) in the GO TO INTERFACE field, and then click GO. □ To change the port PVID settings for a group of ports, select the check boxes to the left of their port numbers, and then enter an existing VLAN ID in the PVID fields. The following information about the port PVID settings is displayed: • PVID.

0, December 2007 Configuring Switching GS108T Smart Switch Software Administration Manual STP The Rapid Spanning Tree Protocol (RSTP) provides rapid convergence of the spanning tree by assigning port roles and by determining the active topology. The RSTP builds upon the IEEE 802. 1D STP protocol to select the switch with the highest switch priority as the root switch. Reconfiguration of the spanning tree can occur in less than 1 second. This is the default setting. Advanced—RSTP Configuration In addition to the function of the Basic RSTP Configuration screen, The Advanced RSTP Configuration screen lets you view and modify the bridge settings: 1. Under Bridge Settings, view or modify the bridge settings. The following configurable fields are displayed with their possible ranges and default values: • Bridge Priority. Specifies the priority of the current bridge. After exchanging bridge protocol data units (BPDUs) with other STP-enabled devices, the device with the lowest priority value becomes the root bridge.

• Bridge Max Age. Specifies the maximum age of the current bridge in seconds. This is the maximum age of the STP information that is learned from the network before it is discarded. • Bridge Hello Time. Specifies the period in seconds that the switch waits before sending configuration PDUs when it is the root of the spanning tree or trying to become the root.

• Bridge Forward Delay. Indicates the period in seconds that the port stays in each of the listening and learning states that precedes the forward state. This period is also used to age all dynamic entries in the forwarding databases when a topology change has been detected and is underway. Advanced—Port Configuration The Port Configuration screen, also referred to as the Rapid Spanning Tree Port Configuration screen, lets you view and modify the RSTP settings: 1. You can make changes to the RSTP port settings for an individual port, for a group of ports, or for all ports simultaneously: • To change the RSTP port settings for an individual port, select the check box to the left of its port number, and then select the RSTP port settings.

Note: You can also enter the interface number (that is, the port number) in the GO TO INTERFACE field, and then click GO. □ • To change the RSTP port settings for a group of ports, select the check boxes to the left of their port numbers, and then select the RSTP port settings. To change the RSTP port settings for all ports simultaneously, select the check box at the top of the column of check boxes, and then select the RSTP port settings. Except for the Interface and State fields, all fields are configurable: • Interface. Specifies the cost of the port. Cost means the contribution of this port to the cost of paths toward the spanning tree root that include this port. The switch uses this value to determine which port is the forwarding port. If all other factors are equal, the path with the lowest cost to the root bridge is the active path. The possible values are between 1 and 65535. • Priority.

Specifies the priority of the port. This is the value of the priority field contained in the first octet of the port ID. The port with the lowest number has the highest priority. The possible values are 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, and 240. • Edge. Specifies whether the port is the edge port. Once configured as an edge port, the port immediately transitions to the forwarding state. the possible values are: – Yes. Specifies that the port is the edge port. – No.

Specifies that the port is not the edge port. If you connect a port to another port though a point-to-point link and the local port becomes a designated port, it negotiates a rapid transition with the other port to ensure a loop-free topology. Specifies that the port is not a point-to-point link. Multicast You can configure IGMP snooping, static multicasting, and multicast group membership. IGMP Snooping IGMP specifies how a host can register to a router to receive specific multicast traffic.

Configure the switch to use IGMP snooping in subnets that receive IGMP queries from either IGMP or the IGMP snooping querier. IGMP snooping constrains multicast traffic at Layer 2 by configuring Layer 2 LAN ports dynamically to forward multicast traffic only to those ports that want to receive it. IGMP is a standard defined in RFC1112 for IGMPv1 and in RFC2236 for IGMPv2. This is the default setting. When you enable IGMP snooping, the screen expands to display fields in which you can specify how IGMP leave packets are processed.

This is the default setting. When you enable IGMP snooping, the screen expands to display fields in which you can specify how IGMP leave packets are processed. in addition , dynamic multicast information is displayed. Select a radio button to specify how IGMP leave packets are processed: • Disable. Specifies that an incoming IGMP leave packet is forwarded to the multicast router, that is, the incoming IGMP leave packet is not blocked. When the multicast router receives the packet, it closes the channel. • Enable. Specifies that an incoming IGMP leave packet is filtered (also referred to as blocked) and, therefore, not forwarded to the multicast router. This is the default setting. Shows the Layer 2 group multicast address.

port Members. Shows the membership that is associated with the group. Static Multicasting Static multicast addressing provides a way to add or delete static multicast addresses that are related to a VLAN. The following information about static multicasting is displayed. Both the VID and Multicast Entry fields are configurable: • ID. Enter a multicast address in the 01:00:5E:XX:XX:XX format. Select the check box to the left of the static multicast ID that you want to remove. Select the VID of the static multicast ID that you want to change. From the ID drop-down list, select the static multicast ID that represents the multicast group that you want to view or modify. When you make your selection, the VID field and Multicast Entry fields change automatically.

You can either assign all ports to or remove them from the static group in step 3, or assign individual ports to or remove them from the static multicast group in step 4. These steps are mutually exclusive. 3. To assign all ports to or remove them from the static multicast group, select the check box to the left of Unit 1. 4.

To assign individual ports to or remove them from the static multicast group: a. To assign a port to or remove it from the static multicast group, select the check box under an individual port number. @@The default frame size is 1518 bytes. @@This is the default setting. @@@@The maximum number of trusted MAC addresses is 256 per system.

@@@@@@The following static MAC address information is displayed. all fields are configurable: • Interface. Specifies the interface (port) number to which the entry refers. • MAC Address. Specifies the MAC address to which the entry refers. • VLAN ID. Specifies the VLAN ID to which the entry refers. @@@@@@Select a check box to specify how the table is to be queried. The possible field types are: • Port. Specifies the interface for which the table is queried.

Specifies the VLAN ID for which the table is queried. Specifies the MAC address for which the table is queried. @@Shows the interface to which the address is assigned. • MAC Address. Shows the MAC address to which the address is assigned. • VLAN ID. Shows the VLAN ID to which the address is assigned. • Dynamic/Static. Shows whether the entry is dynamic or static. @@@@@@@@ 1p-based.

The eight priority tags that are specified in IEEE 802. 1p are p0 to p7. @@@@@@ 1p. Then, you can assign the IEEE 802. 1p priority level to one of the four internal hardware queues.

@@@@1p Based or the DSCP Based radio button to determine the QoS mode. @@@@Note: You can also enter the interface number (that is, the port number) in the GO TO INTERFACE field, and then click GO. □ • To change the bandwidth limits for a group of ports, select the check boxes to the left of their port numbers, and then select the bandwidth limits. To change the bandwidth limits for all ports simultaneously, select the check box at the top of the column of check boxes, and then select the bandwidth limits. Specifies the rate limitation of incoming traffic in this port.

The possible values in bits per second (bps) are: – 512K bps, 2M bps, 4M bbps, 10M bps, 20M bps, 40M bps, 60M bps, 100M bps, 200M bps, 400M bps, and 1000M bps. Specifies the rate limitation of outgoing traffic in this port. 1p to Queue Mapping screen lets you map priority values to the four hardware traffic queues: 1. The possible values are for the Queue field are Lowest, Low, Normal, and High. Assign a priority from 0 to 7 to a DSCP value by using the Priority drop-down lists. The following DSCP values are configurable: • CS. 0, December 2007 5-5 GS108T Smart Switch Software Administration Manual Using the Security Tab The navigation tabs on the top of the home page include a Security tab that lets you manage your GS108T Gigabit Smart Switch using features under the following main menu commands and subcommnands: • "Management Security" • "User Configuration—Change Password" • "RADIUS" • "Authentication Type" "Port Authentication" • "Basic—802.

1x Configuration" • "Advanced—802. 1x Configuration" • "Advanced—Port Authentication" "Traffic Control" • "Storm Control" • "Port Security" "Access" • "IP Access List" • "Trusted MAC" • • • The sections that follow in this chapter cover these features and tell you how to configure them in the GS108T Smart Switch. Management Security The Management Security menu lets you to manage your user configuration, RADIUS servers, and authentication type.

User Configuration—Change Password The User Configuration setting lets you to change the password for the switch. Enter the current password to access the switch. Enter the new password to access the switch. Note: It is good practice to select a password that is more than eight characters long and is a combination of numbers and letters. Names and simple words can be easy to guess. If you forget your password, you can always press the Factory Reset button on the switch, and the password will return to the default value of password. The server is used by ISPs to authenticate a user name and password before authorizing use of the network. You can configure both a primary server and a backup server: 1. The following fields are displayed, all of which are configurable: • Host IP Address. Specifies the IP address of the RADIUS server.
• Authentication Port. Specifies the User Datagram Protocol (UDP) port number of the Extensible Authentication Protocol (EAP) over LANs (EAPOL) control frame. The default UDP port number is 1812, but other numbers can be used if the RADIUS server can recognize them. • Number of Retries. Specifies the number of times the switch sends the RADIUS request to the server before giving up.
• Timeout for Reply. Specifies the number of seconds the switch waits for the RADIUS server to respond before resending the request. • Dead Time. Specifies the number of minutes a RADIUS server; that is not responding to authentication requests is to be skipped, thus avoiding the wait for the request to time out before trying the configured backup server. • Key String.
Specifies the string used by the RADIUS server as a password to identify EAPOL control frames. • Usage Type. Specifies the usage of the RADIUS server. The possible field values are: – Login. The RADIUS server is used for logging in to the switch. The RADIUS server is used for dot1x authentication. – All. The RADIUS server is used for both logging in and dot1x authentication. • Active Server. Specifies the RADIUS server (Primary or Backup) to which these settings apply.

Define all fields that are listed in step 2. Select the check box to the left of the host IP address of the RADIUS server that you want to remove. Select the check box to the left of the host IP address of the RADIUS server for which you want to make changes. b. Make changes to the authentication fields. Authentication Type The Authentication Type screen lets you specify the order in which authentication is performed: 1. Select the authentication type from the drop-down list. The possible field values are: • Local. Specifies that authentication occurs at the RADIUS server. Specifies that no authentication type is applied.
A user is allowed to log in without any authentication. Specifies that authentication occurs only on a local RADIUS server. The authentication procedure shows the order in which authentication is performed. If the first authentication type is not available, the second authentication type is used. Example: If RADIUS, Local is selected, the RADIUS server is used to authenticate a user.
If the RADIUS server is unavailable, or there is no RADIUS server on the network, then authentication is done locally. 1x Configuration screen lets you configure port authentication settings and guest VLANs, and lets you specify whether port authentication is applied to a port: 1. 1x Configuration, the following fields are displayed, all of which are configurable: • Port Based Authentication State. Specifies whether port authentication is enabled on the device. Specifies the authentication method that is used for port authentication.
Port authentication must be enabled to select an authentication method from the drop-down list. The possible field values are: – RADIUS, None. Specifies that port authentication occurs through the RADIUS server. However, if the port is not authenticated, then no authentication method is used, and the session is permitted. Specifies that port authentication occurs through the RADIUS server. – None. Specifies that no authentication method is used to authenticate the port. Guest VLAN: Specifies whether a guest VLAN is enabled on the device. At least one VLAN must exist to select one of the following radio buttons: – Disable. Specifies that a guest VLAN cannot be used for unauthorized ports.

This is the default value. – Enable. Specifies that a guest VLAN can be used for unauthorized ports. If a guest VLAN is enabled, the unauthorized port automatically joins the VLAN selected in the VLAN List field. Select an existing VLAN for the guest VLAN from the drop-down list. forward DOT1x EAPOL. When the port-based authentication state is disabled, you can enable or disable flooding EAPOL. This is the default value. Click Apply to confirm any settings changes to the 802. Under Port Settings, you can make changes to the port authentication setting for an individual port, for a group of ports, or for all ports simultaneously: • To change the port authentication setting for an individual port, select the check box to the left of its port number, and then select the authentication status.
Note: You can also enter the interface number (that is, the port number) in the GO TO INTERFACE field, and then click GO. □ • To change the port authentication setting for a group of ports, select the check boxes to the left of their port numbers, and then select the authentication status. To change the port authentication setting for all ports simultaneously, select the check box at the top of the column of check boxes, and then select the authentication status. The following port authentication settings are displayed. Only the Status field is configurable: • Port.
Specifies whether port authentication is enabled or disabled for the port. The possible field values are: 5-12 v1. 0 , December 2007 Configuring QoS and Security GS108T Smart Switch Software Administration Manual – – Disable. Specifies that port authentication is disabled for the port. No authentication process is required for the port; traffic can be forwarded normally.
This is the default value. enable. Specifies that port authentication is enabled for the port. The port must be authorized by a RADIUS server to forward traffic. Click Apply to confirm any settings changes to the port authentication settings. Advanced—Port Authentication The Advanced Port Authentication screen lets you configure global settings for port-based authentication: 1.