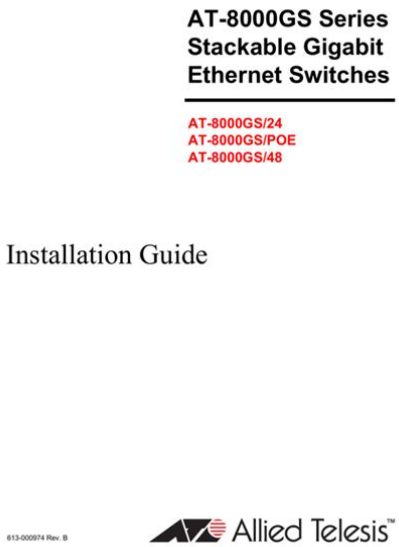
8000gs manual



File Name: 8000gs manual.pdf
Size: 3810 KB
Type: PDF, ePub, eBook
Category: Book
Uploaded: 26 May 2019, 20:35 PM
Rating: 4.6/5 from 794 votes.

Status: AVAILABLE

Last checked: 9 Minutes ago!

In order to read or download 8000gs manual ebook, you need to create a FREE account.

Download Now!

eBook includes PDF, ePub and Kindle version

Register a free 1 month Trial Account.
Download as many books as you like (Personal use)
Cancel the membership at any time if not satisfied.
Join Over 80000 Happy Readers

Book Descriptions:

We have made it easy for you to find a PDF Ebooks without any digging. And by having access to our ebooks online or by storing it on your computer, you have convenient answers with 8000gs manual . To get started finding 8000gs manual , you are right to find our website which has a comprehensive collection of manuals listed.
Our library is the biggest of these that have literally hundreds of thousands of different products represented.

Book Descriptions:

8000gs manual

Information in this document is subject to change without notice. All company names, logos, and product designs that are trademarks or registered trademarks are the property of their respective owners. Link can then either be shut down automatically, or an operator can be alerted to manually intervene.Firmware upgrades are automatic too and help to reduce the burden and cost of network administration.CPoE lets switches perform actions such as software upgrades without forcing the powered devices to power cycle.EPSR offers. The following topics are included in this document Caution Insure that the latest Boot Loader Version 2.0.0.1 is installed on your AT8000GS switch or stack of switches before upgrading the management software to Version 2.0.0.27. Next Page 2 ATS95 Version 2.0.0.27 Software Release NotesPage 4 ATS95 Version 2.0.0.27 Software Release Notes. Upgrade Procedure. This section describes how to upgrade the ATS95 bootloader and software. Page 5 ATS95 Version 2.0.0.27 Software Release NotesPage 6 ATS95 Version 2.0.0.27 Software Release NotesSee Figure 2 on page 6.Page 8 ATS95 Version 2.0.0.27 Software Release NotesProduct Documentation. For hardware. Page 9 ATS95 Version 2.0.0.27 Software Release NotesPage 10 ATS95 Version 2.0.0.27 Software Release Notes. Contacting Allied Telesis. If you need assistance with this product, you may contact. Page 11 ATS95 Version 2.0.0.27 Software Release Notes. The switch is rebooted. Contacting Allied Telesis This section provides Allied Teles is contact information for technical support as well as sales and corporate information. Online Support You can request technical support online by accessing the Allied Tel esis Knowledge Base www. These userfriendly products are able to irrigate in seconds using a cycle of preset minutes. All 8000 controllers are connected to switchtype sensor for optimal performance. These controllers are especially suited for greenhouses and misting applications.http://aiswaryamatrimonials.com/fck_uploads/calculate-antilog-manually.xml

- **at-8000gs manual, allied telesis 8000gs manual, 8000gs manual.**

Designed by UNI Developed by EOI Web Like This! Well assume youre ok with this, but you can optout if you wish. We delete comments that violate our policy, which we encourage you to read. Discussion threads can be closed at any time at our discretion. Please check your inbox, and if you can’t find it, check your spam folder to make sure it didnt end up there. Please also check your spam folder. The web pages are easytouse and easytonavigate. A product sent to Allied Telesis without a RMA number will be returned to the sender at the sender’s expense. Enter “anonymous” as the user name and your email address for the password. The login information is configured with a default user name and password. The default password is friend; the default user name is manager. Passwords are both case sensitive and alphanumeric. Additional user names can be added. The Login Page opens The System General Page opens The Port Settings Page displays an example of the Zoom View with a detailed graphical representation of the device ports. The Port Settings Page opens Indicator legend descriptions are provided with each context of the specific Zoom View. The configuration change is The configuration Resets the information for all parameters in Userdefined information can be added, modified or deleted in specific WBI pages. A configuration is saved as permanent by copying the current Running Configuration file to the Startup Configuration file. To log out. The current management session is ended and the Login Page opens This prevents the current device configuration from being lost.You are prompted to confirm. Resetting the device ends the web browser management session. You must restart the session to continue managing the device. After the device is reset, a prompt for a user name and password displays. The default settings are restored and the device is reset. The System General Page opens The Administration

section of the System General Page contains the following fields.http://domholidays.com/userfiles/calculate-amortization-schedule-manually.xml

This is a required field. The field range is 0159 characters. The field range is 0159 characters. The address must be entered in the format xxx.xxx.xxx.xxx. The default value is 0.0.0.0. The configured IP address must belong to the same subnet as one of the IP interfaces. With dynamic addressing, a device can have a different IP address every time it connects to the network. If the DHCP client software is activated, the device immediately begins to query the network for a DHCP server. The device continues to query the network for its IP configuration until it receives a response. If the device and IP address are manually assigned, that address is deleted and replaced by the IP address received from the DHCP server. The default time is 300 seconds, and the range is 0300. During the period of Daylight Saving Time, Brazilian clocks go forward one hour in most of the Brazilian southeast. In the rest of the country, from the first Sunday in March or after 9th March. Daylight Saving Time is usually regulated by provincial and territorial governments. Exceptions may exist in certain municipalities. If the system time is kept using an external SNTP clock, and the external SNTP clock fails, the system time reverts to the local hardware clock. Daylight Savings Time can be enabled on the device. The System Time Page opens The possible field values are. The field format is HHMMSS. For example 211503. The local system clock settings are saved, and the device is updated. SNTP assures accurate network device clock time synchronization up to the millisecond. Time synchronization is performed by a network SNTP server. The device operates only as an SNTP client, and cannot provide time services to other systems. The device can poll the following server types for the server time The higher the stratum where zero is the highest, the more accurate the clock. The device receives time from stratum 1 and above.

The following is an example of stratums Stratum 1 time servers provide primary network time standards. For example, a Stratum 2 server receives the time over a network link, via NTP, from a Stratum 1 server. T1 T4 are used to determine the server time. This is the preferred method for synchronizing device time. The first Anycast server to return a response is used to set the time value. Time levels T3 and T4 are used to determine the server time. Using Anycast time information for synchronizing device time is preferred to using Broadcast time information. When a broadcast message is sent from an SNTP server, the SNTP client listens for the response. The SNTP client neither sends time information requests nor receives responses from the Broadcast server. MD5 is an algorithm that produces a 128bit hash. MD5 is a variation of MD4, and increases MD4 security. MD5 verifies the integrity of the communication, authenticates the origin of the communication. The System Time Page opens. The possible field values are. The Poll Interval default is 1024 seconds. The System Time Page opens There are two types of daylight settings, either by a specific date in a particular year or a recurring setting irrespective of the year. For a specific setting in a particular year complete the Daylight Savings area, and for a recurring setting, complete the Recurring area. The possible field values are. The European option applies to EU members, and other European countries using the EU standard. If Custom is selected, the From and To fields must be defined. The default time is 60 minutes. The range is 11440 minutes. The possible field range is 131. The possible field range is Jan.Dec. The field format is HHMM. For example 0530. The possible field range is JanDec. In the example, DST begins locally every first Sunday in April at midnight. The possible field range is SundaySaturday. The possible field range is 15. The possible field range is Jan.Dec. The field format is HourMinute.

http://www.drupalitalia.org/node/77098

For example 0210. In the example, DST ends locally every first Sunday in October at midnight. The possible field range is SundaySaturday. For example 0530. If you select Other, you must define its From and To fields. To configure DST parameters that will recur every year, select Recurring and define its From and To fields. This section contains the following topics Access to management

functions can be limited to user groups. User groups are defined for interfaces according to IP addresses or IP subnets. Access profiles contain management methods for accessing and managing the device. The device management methods include For example, User Group 1 can access the device module only via an HTTPS session, while User Group 2 can access the device module via both HTTPS and Telnet sessions. The Access Profile Page contains the currently configured access profiles and their activity status. If an access profile is assigned to any interface, the device can be accessed by all interfaces. The Access Profile Page opens The access profile name can contain up to 32 characters. The possible field values are Access Profiles cannot be deleted when active. When the packet is matched to a rule, user groups are either granted permission or denied device management access. The rule number is essential to matching packets to rules, as packets are matched on a firstfit basis. The rule priorities are assigned in the Profile Rules Page. Users with this access profile can access the device using the management method selected. If selected, users accessing the device using Telnet meeting access profile criteria are permitted or denied access to the device. If selected, users accessing the device using HTTP meeting access profile criteria are permitted or denied access to the device. If selected, users accessing the device using HTTPS meeting access profile criteria are permitted or denied access to the device.

If selected, users accessing the device using SNMP meeting access profile criteria are permitted or denied access to the device. The Source IP Address field is valid for a subnetwork. The possible field values are. This is the default. Users can also be blocked from accessing the device. Rules are composed of filters including When the packet is matched to a rule, user groups are either granted permission or denied device management access. The possible field values are Users with this access profile can access the device using the management method selected. This is the default. User authentication can be performed either locally or on an external server. User authentication occurs in the order the methods are selected. If the first authentication method is not available, the next selected method is used. For example, if the selected authentication methods are RADIUS and Local, and the RADIUS server is not available, then the user is authenticated locally. The Authentication Profiles Page opens The default configuration displays as Console Default, and Network Default. The possible authentication methods are The device checks the user name and password for authentication. For more information, see Defining RADIUS Server Settings. If authentication cannot be verified locally, the RADIUS server authenticates the management method. If the RADIUS server cannot authenticate the management method, the session is blocked. If authentication cannot be verified at the RADIUS server, the session is authenticated locally. If the session cannot be authenticated locally, the session is blocked. If the RADIUS server cannot authenticate the management method, the session is permitted. If the session cannot be authenticated locally, the session is permitted. If the session cannot be authenticated locally, the session is permitted. The profile is added to the profiles table and the device is updated. The Authentication Profiles Page opens.

For example, console users can be authenticated by Authentication Profile List 1, while Telnet users are authenticated by Authentication Profile List 2. Authentication methods are selected using arrows. The order in which the methods are selected is the order by which the authentication methods are used. The Authentication Mapping Page opens SSH provides clients secure and encrypted remote connections to a device. The possible methods are Possible methods are User authentication can be performed locally, or on an external server. Once the authentication session is completed, an authorization session starts using the authenticated user name. The field range is 160 seconds and the default is 10 seconds. The field range is 065535. The default is 0. The field range is 160 seconds and the default is 10 seconds. The possible field values are RADIUS servers provide a

centralized authentication method for web access. To configure RADIUS security settings. The RADIUS Configuration Page opens Possible field values are 110. The range is 02000. The possible values are 165535, where 1 is the highest value. The RADIUS server priority is used to configure the server query order. The authentication port is used to verify the RADIUS server authentication. The authenticated port default is 1812. Possible field values are 110. The field range is 160 seconds and the default is 10 seconds. The default is 0 minutes. This key must match the RADIUS encryption. The default value is All. The possible field values are To configure local users and passwords. The Local Users Page opens The lowest user access level is 1 and the highest is 15. User assigned a access level of 15 have readonly access. The possible field values are Local user passwords can contain up to 159 characters. The Local Users Page opens. This section contains the following topics Guest VLANs limited network access to authorized ports.

If a port is denied network access via portbased authorization, but the Guest VLAN is enabled, the port receives limited network access. For example, a network administrator can use Guest VLANs to deny network access via portbased authentication, but grant Internet access to unauthorized users. The MAC addresses can be dynamically learned or statically configured. Locked port security monitors both received and learned packets that are received on specific ports. Access to the locked port is limited to users with specific MAC addresses. These addresses are either manually defined on the port, or learned on that port up to the point when it is locked. When a packet is received on a locked port, and the packet DLink source MAC address is not tied to that port either it was learned on a different port, or it is unknown to the system, the protection mechanism is invoked, and can provide various options. Unauthorized packets arriving at a locked port are either The MAC address list can be restored after the device has been reset. Disabled ports are activated from the Port Security Page. To define port security The Port Security Page opens The possible port indicators are The port indicator changes to selected. The Learning Mode field is enabled only if Locked is selected in the Set Port field.The possible field values are. The port is immediately locked, regardless of the number of addresses that have already been learned. The port learns up to the maximum addresses allowed on the port. Both relearning and aging MAC addresses are enabled. The possible values are. The possible field range is 11,000,000 seconds, and the default is 10 seconds. Indicates the action to be applied to packets arriving on a locked port. This is the default value. The port remains shut down until reactivated, or until the device is reset. The field range is 1128. The default is 1. The possible values are.

If the port is not authenticated, then no authentication method is used, and the session is permitted. If a port is denied network access via portbased authorization, but the Guest VLAN field is enabled, the port receives limited network access. No part o f this pub lication may be repro duced without prior wr itten permission from Al lied Telesis, Inc. Allied Telesis is a t rademark of Allied Tele sis, Inc. Microsoft and Internet Explorer are regist ered tradem arks of Microsoft Co rporation. Netscape Navigator is a register ed trademark of Netscape Communi cations Corporation. All other pr od uct names, co mpany names, lo gos or other designations mentioned herein are t rademarks o r registered t r ademarks of their respective owners. Allied Telesis, Inc.The informa tion provided herein is subject to change without notice. In no event shall Allied Telesis, Inc.This preface contains the following sections “Safety Symbols Used in this Document” o n page 4 “Where to Find W ebbased Guides” on p age 5 “Contacting Allie d T elesis” on p age 6 W arning Performing or omi tting a specific action may result in electrical shock. A product sent to Allied Te lesis without an RMA number will be returned to the sender at t he sender’s expense. Management Software Updates New releases of management softwar e for our managed products are available from either of the following Internet sites. Enter “an onymous” for the user name and your email address for the password. A stack of six units maximum is supp orted. In each stack, at any given point of ti me, there is a single Stack unit that is the stack’s “Master”; all other units are “Slaves”. One of the slaves can act as a backup master, so that in t he event of failure of the master unit, the backup takes over.

The Stack architec ture provides for dynamic learning of the topology, and dynamic det ection at stack startup.

Device configuration is performe d through an Embedded Web Server EWS or through a Command Line interface CLI. The de vice management is performed through an RS232 interface. Jumbo frames 802.1d, 1w, 1s priority tags supported. Broadcast storm control IEEE 802.1Q tagged VLANs supported. Ingress rate limiting. RFC 2618 RADIUS Authentication. Industry standard CL I. Browser based manageme nt interface HTTP. T elnet access supported. SNMP v1, v2 and v3. RFC1757 RMON support. Port Mirroring support. PVE Port Security DHCP support S tatic IP Multicast support. IGMP Snooping These ports are associated with the RJ45 copper ports 21, 22, 23 and 24. Select Button — Se lects the port LED indications.These ports are associat ed with the RJ45 copper ports 21, 22, 23 and 24.These ports are associated with the RJ45 copper ports 45, 46, 47, and 48. Select Button — Se lects the port LED indications.Table 1 lists the supported SFPs RJ45 Console Port The RJ45 port on the rear panel is an asynchrono us serial console port supporting the RS232 electrical specifica tion. The port is used to connect the device to a console managing the device. This in terface configuration is as follows. Eight data bit s. One stop bit. No parity. Baud rate is 1 15,200 default.The different LED types are as follows “System LEDS” on pag e 16 — These LEDs indicate the switch power supply and diagnostic result sta tus and are are found on the front panel. “S tacking Port LEDs” on page 17 — These LEDs indicates the switch location in a st ack and are found on the front panel. “Mode LEDs” on pa ge 18 — These LEDs indicates the functional information that the RJ45 port LE D displays.The power supply port LED indications are described in th e following table SYS LED The SYS LED on the front panel of the de vice indicates the diagnostic results. The diagnostics LED indica tions are described in the following table Stacking Port LEDs The stacking LED indicates the position of the switch in a stack.

The following figure illustrates the stacking LEDs. Figure 8 Stacking LEDs Table 2 Power Supply LED Indicat ions LED Description LED Indication Description Power Green System powered up power on Off System not powered up power off Table 3 System LED Indications LED Description LED Indication Description SYS Flashing Green System diagnostics has failed. Solid Green System diagnostics successfully completed. S1 Green The device is in stacking mode, and is either the master or backup of the stack, which is determined by the master election algorithm. S2 Green The device is masterenabled, and is either the master or backup of the stack, which is determined by the master election algorithm. S3 Green The device is operating as Stack Member 3 in the stack. S4 Green The device is operating as Stack Member 4 in the stack. S5 Green The device is operating as Stack Member 5 in the stack. S6 Green The device is operating as Stack Member 6 in the stack. Note Please refer to Table 5, “Mo de LED Indication Non POE Only” on page 19 for the selection of th e Mode using the front panel MODE switch Table 5 Mode LED Indication Non POE Only LED Description LED Indication Functional Description COL Green Indicates that Collision status is displayed on right port LED. Off Another Mode is displayed. SPD Green Indicates that Speed status is displayed on right port LED. FDX Green Indicates that Duplex status is displayed on right port LED. ACT Blinking Green Indicates that Activity status is displayed on right port LED. Off Another Mode is displayed. Right LED COL Solid Green Data collisions are occurring on the port. Off No data co llisions are occurring on the port. SPD Solid Green Link is established at 1000Mbps. Solid Amber Link is established at 100Mbps. Off Link is established in 10Mbps. FDX Solid Green A Full Duplex mode connection is established. Off A Half Du plex mode connection is established. Off No activity is estab lished.

Solid Amber An overload, a terminal short or e xternal forced voltage feeds into the p ort. Flashing amber PD is detected but power exceeds the max switch POE power budget. Off No PD is connected, and subsequen tly there is no power feeding. Figure 12 SFP Port LEDs The SFP ports have one LEDs for lin k and activity. Flashing Green Activity is detected on the port. Off No link is established on

the port. The following figure illustrates the Stacking port LEDs. Figure 13 St acking Port LEDs The HDMI ports have two LEDs, one is for Link and one is for Activity. The Stacking LEDs indications are described in the following tab l e Table 9 Stacking Ports LEDs Indications Port Description LED Indication Description Left LED Link Green A link is established on port Off No link is established on port Right LED Act Green There is data transmission on port Off There is no data transmission on po rt Note The indicates that a translation of the safety state ment is available in a PDF document titled “Tra nslated Safety Statements” 613000990 on the Allied Telesis website a t www.alliedtelesis.com. W arning Class 1 Laser product. L1 W arning Do not st are into the laser beam. L2 W arning T o prevent electric shock, do not remove the cover. No userserviceable pa rts inside. This unit contains hazardous voltages and sh ould only be opened by a trained and qualified technician. T o avoid the possibili ty of electric shock, disconnect electric power to the product before connecting or disconnecting the LAN cables. E1 W arning Do not work on equipment o r cables during periods of lightning activity. E2 W arning Power cord is used as a di sconnection device. T o d e energize equipment, disconnect the power cord. E3 W arning Class I Equipment. This equipmen t must be earthed. The power plug must be connected to a properly wired earth ground socket outlet. An improperly wired socket outlet could place hazardous voltages on a ccessible metal part s. E4 Pluggable Equipment.

The socke t outlet shall be installed near the equipment and shall be easily accessible. E5 Caution Air vent s must not be blocked and must have free access to the room ambient air for cooling. E6 Appropriate consideration of equipme nt nameplate ratings should be used when addressing this concern. E21 Caution Risk of explosion if battery is replaced by an incorrect type. Replace only with t he same or equivalent type recommended by the manufacturer. Dispose of use d batteries according to the manufacturer’s instructions. Attention Le remplacement de la batterie par une batterie de type incorrect peut provoquer un dan ger d’explosion. La remplacer uniquement p ar une batterie du meme type ou de type equivalent recommandee p ar le constructeur. Les batteries doivent etre eliminees conformement aux instruction s du constructeur. E22 W arning Mounting of the equipment in the rack shou ld be such that a hazardous condition is not created d ue to uneven mechanical loading. E25 If installed in a closed or multiunit rack assembly, the operating ambient temperature of the rack environment may be gre ater than the room ambient temperature. The refore, consideration should be given to inst alling the equipment in an environment compatible with the manufactu rer ’s maximum rated ambient temperature Tmra. E35 Caution Installation of t he equipment in a rack should be such that the amount of air flow required for safe op eration of the equipment is not compromised. E36 W arning Reliable earthing of rackmounte d equipment should be maintained. Particular att ention should be given to supply connections other than direct connections to th e branch circuits e.g., use of power strips. E37 Please return damaged unit s for servicing.Opening or removing covers marked with a triangular symbol and a lighting bolt may cause electrical shock.

T o determi ne the possib ility of overloading the supply circuits, a dd together the ampere ratin gs of all devices inst alled on the same circuit as the device being installed. Comp are this total with the rating limit for the circuit. The maximum ampere ratings are usually printed on the switch, near their AC power connectors. Ensure the air flow around the front, sides, and back of t he switch is not restricted. Ensure the cooling vent s are not blocked. Do not install th e switch in an environment where the operating ambient temperature might exceed 40.Before installing the unit, verify that the location chosen for installation meets the following site requirements. General — Ensure that t he power supply is correctly installed. Power — The unit is installed within 1.5 m 5 feet of a grounded, easily accessible outlet 100250V AC, 5060Hz. Clearance — There is adequate frontal clearance for operator access. Allow clearance for cabling, power connections, and ventilation. Cabling — The cablin g is routed to avoid sources of electrical noise such as radio transmitters, br oadcast amplifiers, p ower lines, and fluorescent lighting fixtures. Ambient Requirement s — The ambient

unit operating t emperature range is 0 to 40. C 32 to 104 F a t a relative humidity of up to 95%, noncondensing. V erify that water or moisture cannot enter the device casing. Unpacking This section contains information for unpacking the device, and includes the following topics “Package Contents” on page 30 “W arranty” on page 30 “Unpacking Essentials” on p age 30 Package Contents While unpacking the device, ensure that the following items are included. Rubber Feet for desktop inst allation. Rackmount kit hardware accessories. An AC power cable S tacking cab le Y ellow color. Console RS232 cable with RJ45 connector. Unpacking Essentials Note Before unpacking th e device, inspect the package and report any eviden ce of damage immediately.

An ESD strap is not suppl ied with the device. 2. Place the container on a clean flat surface and cut all straps securing the container. 3. Open t he container. 4. Carefully remove the device from th e container and place it on a secure and clean surface. 5. Remove all packing material. 6. Inspect the product for damage. Report any damage immediately. If any item is found missing or damaged, please contact your local A TI reselle r for a replacement. This section includes the following topics “Desktop or Shelf Inst allation” on page 32 “Rack Installation” on p age 32 Desktop or Shelf Installation When installing the switch on a desktop or sh elf, the rubber feet incl uded with the d evice should first be at tached. Attach th ese cushioni ng feet on the bottom a t each corner of the device. Ensure the surface is be able to support th e weig ht of the device and the device cables. T o install the device on a surface, perform the following 1. Attach the rubber feet on the bottom of th e device. The following fig ure illustrates the rubber feet in stallation on the device. Figure 1 Inst alling Rubber Feet 2. Set device down on a flat surface, while leaving 2 inches on each side and 5 inches at the back. 3. Ensure that the device has proper v entilation by allo wing adequate space for ventilation between the device a nd th e objects around the device. Rack Installation The device can be moun ted in an EIA standardsized, 19inch rack, which can be plac ed in a wiring closet with other equipment. T o insta ll the device the mounting brackets must first be attached to the device’s sides. An ESD strap is not suppl ied with the device. 2. Place the device on a flat and stable surface. 3. Place the supplied rackmounti ng bracket on one side of the device ensuring the mounting holes on the device line up to t he mountin g holes on the rack mounting bracket. The following figu re illustrates w here the mounting brackets are placed on the device.