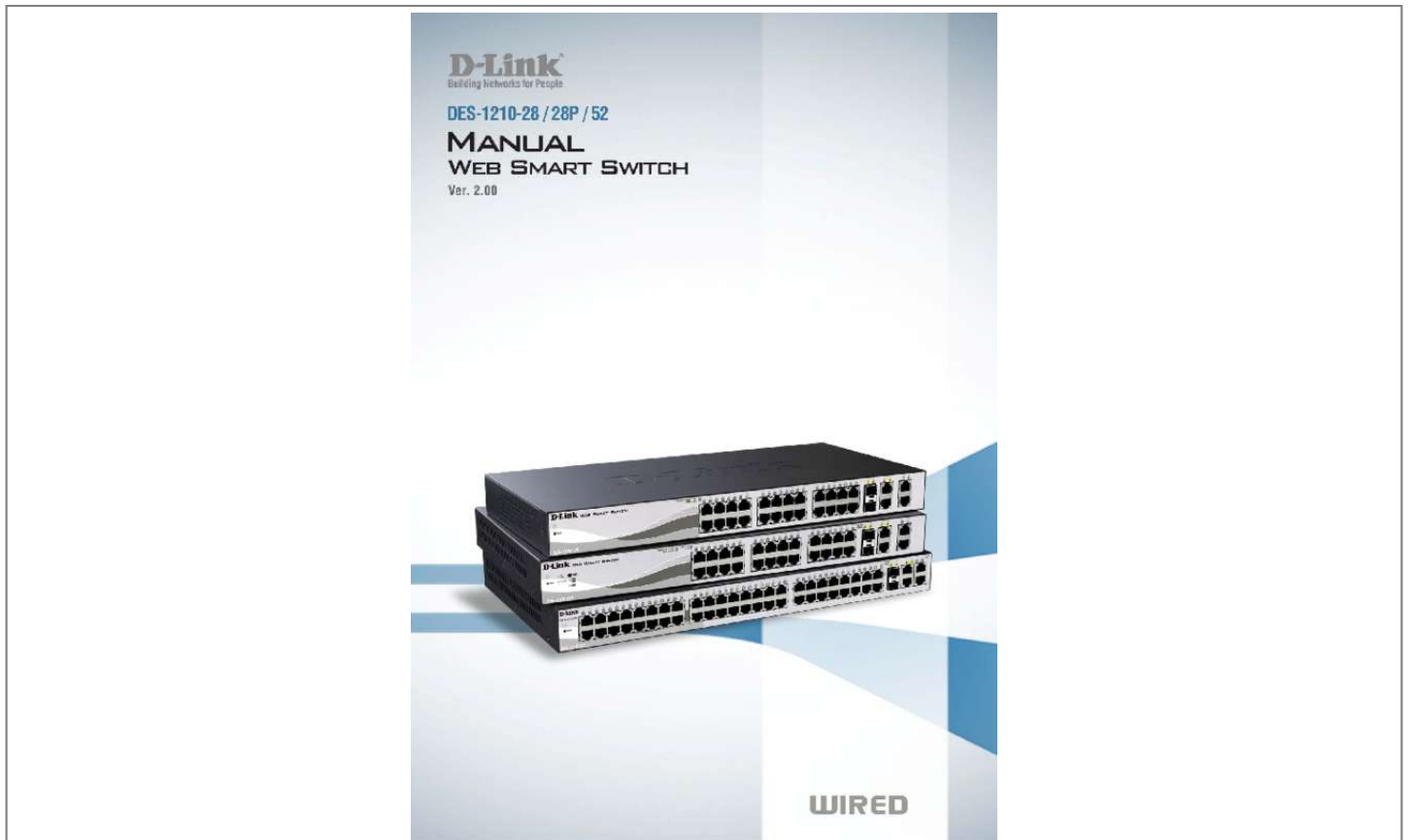




Your PDF Guides

You can read the recommendations in the user guide, the technical guide or the installation guide for D-LINK DES-1210-28P. You'll find the answers to all your questions on the D-LINK DES-1210-28P in the user manual (information, specifications, safety advice, size, accessories, etc.). Detailed instructions for use are in the User's Guide.

User manual D-LINK DES-1210-28P
User guide D-LINK DES-1210-28P
Operating instructions D-LINK DES-1210-28P
Instructions for use D-LINK DES-1210-28P
Instruction manual D-LINK DES-1210-28P



[You're reading an excerpt. Click here to read official D-LINK DES-1210-28P user guide](http://yourpdfguides.com/dref/5324783)
<http://yourpdfguides.com/dref/5324783>

Manual abstract:

@@Terms/Usage In this guide, the term Smart Switch (first letter capitalized) refers to the Smart Switch, and smart switch (first letter lower case) refers to other Ethernet switches. Some technologies refer to terms bridge and switching hubs interchangeably, and both are commonly accepted for Ethernet switches. A NOTE indicates important information that helps a better use of the device. a CAUTION indicates potential property damage or personal injury. Copyright and Trademarks Information in this document is subjected to change without notice. @@@@1 1 Product Introduction D-Link Web Smart Switch User Manual 1 Product Introduction Thank you and congratulations on your purchase of D-Link Web Smart Switch Products. D-Link's next generation Web Smart Ethernet switch series blends plug-and-play simplicity with exceptional value and reliability for small and medium-sized business (SMB) networking. All models are housed in a new style rack-mount metal case with easy-to-view front panel diagnostic LEDs, and provides advance features including two combo 1000BASE-T/SFP and two additional Gigabit uplinks, network security, traffic segmentation, QoS and versatile management. flexible Options with 24 and 48 ports. D-Link Web Smart Switches offer two port densities, 24 and 48 Ethernet ports that support auto MDI/MDIX feature which bring inexpensive and easy Ethernet connection to the desktops.

each switch provides 4 Gigabit uplinks connection to a Gigabit backbone or servers. Two of the Gigabit ports are SFP combo ports which support both 1000M and 100M fiber connections. extensive Layer 2 Features. Implemented as complete Layer 2 devices, these switches include functions such as IGMP Snooping, Port Mirroring, Spanning Tree, 802. The switches support 802. 1Q VLAN tagging to enhance network security and performance. The switches also support 802. Ip priority queues , enabling users to run bandwidthsensitive applications such as multimedia streaming by prioritizing traffic in network. These functions allow switches to work seamlessly with VLAN and 802. Ip traffic in the network.

Auto Voice VLAN automatically places the voice traffic from IP phone to an assigned VLAN with higher priority, separating from normal traffic. Asymmetric VLAN is implemented in these switches for a more efficient use of shared resources such as server or gateway devices. network Security. D-Link's innovative Safeguard Engine function protects the switches against traffic flooding caused by virus attacks. additional feature like 802. 1X port-based authentication provides access control of the network with external RADIUS servers. aACL is a powerful tool to screen unwanted IP or MAC traffic. Storm Control keeps the network from being overwhelmed by abnormal traffic. Port Security is another simple but useful authentication method to maintain the integrity of the network device. versatile Management.

The new generation of D-Link Web Smart Switches provides growing businesses simple and easy management of their network. The SmartConsole utility or a multi-language Web-Based management interface allows administrators to remotely control their network down to the port level. The intuitive SmartConsole easily allows customers to discover multiple D-Link web smart switches in the same L2 network segment. With this utility, users do not need to change the IP address of PC and provides easy initial setting of smart switches. The switches within the same L2 network segment connected to user's local PC are displayed on the screen for instant access. it allows extensive switch configuration setting , and basic configuration of discovered devices such as a password change or firmware upgrade. Users can also access the Switch via Telnet. Basic tasks such as changing the Switch IP address, resetting the settings to factory defaults, setting the administrator password, rebooting the Switch, or upgrading the Switch firmware can be performed using the Command Line Interface (CLI). In addition, users can utilize the SNMP MIB (Management Information Base) to poll switches for information about the status, or send out traps of abnormal events. SNMP support allows users to integrate the switches with other third-party devices for management in an SNMP-enabled environment. D-Link Web Smart Switches also come with the D-View plug-in module that works with D-View 6, SNMP Management Software which provides easy-to-use graphic interface and facilitates the operation efficiency. 2 1 Product Introduction D-Link Web Smart Switch User Manual DES-1210-28 24-Port 10/100Mbps with 4-Port 10/100/1000Mbps Copper and 2 Combo SFP Web Smart Switch Front Panel Figure 1 DES-1210-28 Front Panel Power LED : The Power LED lights up when the Switch is connected to a power source. Port Link/Act/Speed LED (1-24): The Link/Act/Speed LED flashes which indicates a network link through the corresponding port. Blinking indicates that the Switch is either sending or receiving data to the port. When a port has amber light indicates that port is running on 10M.

When it has a green light it is running on 100M. Port Link/Act/Speed LED (25F, 26F, 25T, 26T, 27, 28): The Link/Act/Speed LED flashes which indicates a network link through the corresponding port. Blinking indicates that the Switch is either sending or receiving data to the port. When a port has amber light indicates that port is running on 10M or 100M. When it has a green light it is running on 1000M.

NOTE: On DES-1210-28, the MiniGBIC ports are shared with normal RJ-45 ports 25 and 26. When MiniGBIC port is used, the RJ-45 port cannot be used. Reset: By pressing the Reset button the Switch will change back to the default configuration and all changes will be lost. Rear Panel Figure 2 DES-1210-28 Rear Panel Power: The power port is where to connect the AC power cord. DES-1210-52 48-Port 10/100Mbps Web Smart Switch with 4-Port 10/100/1000Mbps and 2 Combo SFPs Front Panel Figure 3 DES-1210-52 Front Panel 3 1 Product Introduction D-Link Web Smart Switch User Manual Power LED : The Power LED lights up when the Switch is connected to a power source. Port Link/Act/Speed LED (1-48): The Link/Act/Speed LED flashes which indicates a network link through the corresponding port. Blinking indicates that the Switch is either sending or receiving data to the port. When a port has amber light indicates that port is running on 10M. When it has a green light it is running on 100M. Port Link/Act/Speed LED (49F, 50F, 49T, 50T, 51, 52): The Link/Act/Speed LED flashes which indicates a network link through the corresponding port.

Blinking indicates that the Switch is either sending or receiving data to the port. When a port has amber light indicates that port is running on 10M or 100M. When it has a green light it is running on 1000M. Reset: Press the reset button to reset the Switch back to the default settings.



[You're reading an excerpt. Click here to read official D-LINK](http://yourpdfguides.com/dref/5324783)

[DES-1210-28P user guide](http://yourpdfguides.com/dref/5324783)

<http://yourpdfguides.com/dref/5324783>

all previous changes will be lost. NOTE: On the DES-1210-52, the MiniGBIC ports are shared with normal RJ-45 ports 49 and 50. When the MiniGBIC port is used, the RJ-45 port cannot be used. Rear Panel Figure 4

DES-1210-28P 24-Port 10/100Mbps PoE with 4-Port 10/100/1000Mbps Copper and 2 Combo SFP Web Smart Switch Front Panel Figure 5
DES-1210-28P Front Panel Power LED : The Power LED lights up when the Switch is connected to a power source. Power Max LED: The Power Max lights up when the system power resource remain

Fan OK/Fail LED: The FAN LED shows the status of the fans, the green light (OK) indicates that all fans work fine and the red light (Fail) indicate that on or multiple fans are working abnormally. Mode Select Button/LED: The Mode Select Button controls the mode of Port LED, and the current setting is indicated by the Mode LED under the button. Port LED (1-24): Link/Act/Speed Mode: When selecting the Link/Act/Speed Mode, the Port LED flashes which indicate a network link through the corresponding port. Blinking indicates that the Switch is either sending or receiving data to the port. When a port has amber light indicates that port is running on 10M.

When it has a green light it is running on 100M. PoE Mode: When selecting the PoE Mode, the port LED lights up with solid green indicates power device is connected to corresponding port. solid amber indicates a PoE error has occurred at this port. And light off indicates this port is not providing the power or no PD found. Port LED (25F, 26F, 25T, 26T, 27, 28): The Port LED flashes which indicates a network link through the corresponding port.

Blinking indicates that the Switch is either sending or receiving data to the port. When a port has amber light indicates that port is running on 10M or 100M.

When it has a green light it is running on 1000M. NOTE: On DES-1210-28P, the MiniGBIC ports are shared with normal RJ-45 ports 25 and 26. When MiniGBIC port is used, the RJ-45 port cannot be used. Reset: By pressing the Reset button the Switch will change back to the default configuration and all changes will be lost. Rear Panel Figure 6
DES-1210-28P Rear Panel Power: The power port is where to connect the AC power cord. 2 Hardware Installation D-Link Web Smart Switch User Manual 2 Hardware Installation This chapter provides unpacking and installation information for the D-Link Web-Smart Switch. Step 1: Unpacking Open the shipping carton and carefully unpack its contents. Please consult the packing list located in the User Manual to make sure all items are present and undamaged.

If any item is missing or damaged, please contact your local D-Link reseller for replacement. One D-Link Web-Smart Switch One AC power cord Four rubber feet Screws and two mounting brackets One Multi-lingual Getting Started Guide One CD with User Manual, SmartConsole Utility program, and D-View Module If any item is found missing or damaged, please contact the local reseller for replacement. Step 2: Switch Installation For safe switch installation and operation, it is recommended that you: Visually inspect the power cord to see that it is secured fully to the AC power connector. Make sure that there is proper heat dissipation and adequate ventilation around the switch. Do not place heavy objects on the switch. Desktop or Shelf Installation When installing the switch on a desktop or shelf, the rubber feet included with the device must be attached on the bottom at each corner of the device's base. Allow enough ventilation space between the device and the objects around it. Figure 7
Attach the adhesive rubber pads to the bottom Rack Installation The switch can be mounted in an EIA standard size 19-inch rack, which can be placed in a wiring closet with other equipment. To install, attach the mounting brackets to the switch's side panels (one on each side) and secure them with the screws provided (please note that these brackets are not designed for palm size switches). Figure 8
Attach the mounting brackets to the Switch 6 2 Hardware Installation D-Link Web Smart Switch User Manual Then, use the screws provided with the equipment rack to mount the switch in the rack.

Figure 9
Mount the Switch in the rack or chassis Please be aware of following safety Instructions when installing: A) Elevated Operating Ambient - If installed in a closed or mul NOTE: The switch's factory default IP address is 10. The web configuration can also be accessed through the SmartConsole Utility. Open the SmartConsole Utility and double-click the switch as it appears in the Monitor List. This will automatically load the web configuration in your web browser. When the following logon dialog box appears, enter the password and choose the language of the Webbased Management interface then click OK.

The switch support 9 languages including English, Traditional Chinese, Simplified Chinese, German, Spanish, French, Italian, Japanese and Russian. By default, the password is admin and the langus from and Status shows the content of this log message. Figure 16
SmartConsole Log Trap Click this icon to launch the Trap window. Click View Trap to show the events of the SmartConsole Utility and the device. Date/Time indicates when the trap message was received, IP denotes where it comes from and Status shows the content of this trap message.

click Clear Trap to clear all entries. Click OK to exit Figure 17
SmartConsole Trap The trap icon in the SmartConsole Settings will change while receiving new trap messages. Please see below for detailed description. Icon Description No new traps New traps was received File By clicking on this icon you will see below options: 13 4 SmartConsole Utility D-Link Web Smart Switch User Manual Figure 18
SmartConsole File Monitor Save: Records the setting of the Device List as default for the next time the SmartConsole Utility is used. Monitor Save As: Records the setting of the Device List in an appointed filename and file path. monitor Load: Manually load a Device List setting file. Help Click this icon to launch the SmartConsole Info window. Figure 19
SmartConsole Help 14 4 SmartConsole Utility D-Link Web Smart Switch User Manual Device Configuration The Device Configuration in the SmartConsole Utility has five icons: Device Settings Device Password Manager Multi Firmware Upgrade DHCP Refresh Web Access and the , , device buttons for the Device List. device Settings Select a switch from the Device List. Click on this icon to launch the Device Settings window.

Here you can configure the Product Name, IP Address, Gateway, Subnet Mask, System Name, Location, Trap Host IP, Switch Group Interval, and DHCP Client Setting of the Switch.



[You're reading an excerpt. Click here to read official D-LINK DES-1210-28P user guide](http://yourpdfguides.com/dref/5324783)
<http://yourpdfguides.com/dref/5324783>

To apply the configuration, insert the correct device password in the Confirm Password box and then click OK Figure 20 SmartConsole Device Settings
15 4 SmartConsole Utility D-Link Web Smart Switch User Manual Device Password Manager Select a switch from the Device List. Click on this icon to launch the Device Password Manager window. Here you can enter a new password and confirm it. Figure 21 SmartConsole Device Password Manager Multi Firmware Upgrade Select one or many switches of same model name from the Device List. Click on this icon to launch the Firmware Upgrade window. Specify the Firmware Path (or Browse for one) that you are going to use. Input the correct password of device, and then click Upgrade. The state will show "OK" after completion, and Fail is firmware upgrade fails or cannot be completed for any reason. Figure 22 Firmware Upgrade CAUTION:

Do not disconnect the PC or remove the power cord from device until upgrade completes.

The software may be corrupted because the incomplete firmware upgrade. DHCP Refresh: If a DHCP-client enabled switch in the Device List shows the default IP is still used, it means the device did not receive an IP address from the DHCP server successfully. Select that switch and click the DHCP refresh icon. Enter the correct Device Password and then click OK. The device will renew the IP address from the DHCP server.

16 4 SmartConsole Utility D-Link Web Smart Switch User Manual Figure 23 DHCP Refresh Web Access Select a switch from the Device List. Click this icon to launch your internet browser (eg. the Internet Explorer). Here you can configure the Switch through the Web-based Management utility. You may also get into the Web-based Management by double-clicking the device in the device list.

Add(+), Delete(-) and Discover the device Click the Discovery button to display all the Web-Smart devices located in the same domain with the management PC. Click the + and insert a device IP address to add a device into Discover List, or select a device and click the button to remove it. Figure 24 SmartConsole Add device Figure 25 SmartConsole Delete device Device List This list displays all discovered Web-Smart devices on the network. Figure 26 SmartConsole Device List Definitions of the Device List features: 17 4 SmartConsole Utility D-Link Web Smart Switch User Manual Monitor: Check the Monitor box and the SmartConsole will collect the trap and log data from the device. The in the monitor means the device was discovered by SmartConsole. Click the icon to have the device keep updating the information such as system log or trap to the SmartConsole Utility. The icon will become . When the device was detected as not reachable, the icon will change to . Please check if the power or the cable of this device is disconnected. Protocol version: Displays the software version of the Utility.

DHCP: Specify if the device gets the IP address from a DHCP server. location: Displays where the appointed device location. Trap IP: Displays the IP address of host where the Trap information will be sent to. Subnet Mask: Displays the Subnet Mask setting of the device. Gateway: Displays the Gateway setting of the device. Device Group Interval: Displays the intervals (in seconds) that the Switch will be discovered in the SmartConsole Device List Firmware version: Displays the current Firmware version of this device. LLDP: Displays the LLDP (Link Layer Discovery Protocol) status of the device. (Only for PoE model) SNMP: Displays the SNMP status of the device. NOTE: If the devices marked as red in the device list, it means the devices require to upgrade firmware again. 18 5 Configuration D-Link Web Smart Switch User Manual 5 Configuration The features and functions of the D-Link Web Smart Switch can be configured for optimum use through the Web-based Management Utility.

Smart Wizard Configuration After a successful login, the Smart Wizard will guide you through essential settings of the D-Link Web Smart Switch. If you do not plan to change anything, click Exit to leave the Wizard and enter the Web Interface. You can also skip it by clicking Don't show Smart Wizard next time for logon the Web-based Management next time. Password Settings Password setting allows you to change the login password of the device. Type the desired new password in the Switch Password box and again in the Confirm Switch Password, then click the Apply button to make it effective.

Figure 27 Configure Password in Smart Wizard 19 5 Configuration D-Link Web Smart Switch User Manual SNMP Settings The SNMP Settings feature allows you to quickly enable or disable the SNMP function and configure the SNMP community name. For the complete SNMP feature, please navigate to Setup Menu > System > SNMP Settings in the Web Interface. by default , the SNMP Setting is Disabled. Click Enabled, enter Community names, and then click Apply to activate SNMP Setting. Figure 28 Configure SNMP in Smart Wizard 20 5 Configuration D-Link Web Smart Switch User Manual System Settings You can manually change the system IP Address, Subnet Mask, and Gateway address by selecting Static and clicking Apply.

You can further configure and read more about the above settings in the Setup Menu > System > System Settings. The default setting of System IP address is Static. Select DHCP to have the switch obtain an IP address from a DHCP server in the network. Figure 29 Configure System IP address in Smart Wizard NOTE: Changing the system IP address will disconnect you from the current connection. Please enter the correct IP address in the Web browser again and make sure your PC is in the same subnet with the switch. See Login Webbased Management for detailed description. If you want to change the IP settings, click OK and start a new web browser. Figure 30 Confirm the changes of IP address in Smart Wizard 21 5 Configuration D-Link Web Smart Switch User Manual Web-based Management After clicking the Exit button in Smart Wizard you will see the screen below: Tool Bar Function Tree Figure 31 Web-based Management Main Configuration Screen Above is the Web-based Management screen. The three main areas are the Tool Bar on top, the Function Tree, and the Main Configuration Screen. The Tool Bar provides a quick and convenient way for essential utility functions like firmware and configuration management.

By choosing different functions in the Function Tree, you can change all the settings in the Main Configuration Screen. The main configuration screen will show the current status of your Switch by clicking the model name on top of the function tree. At the upper right corner of the screen the username and current IP address will be displayed. Under the username is the Logout button. Click this to end this session. NOTE: If you close the web browser without clicking the Logout button first, then it will be seen as an abnormal exit and the login session will still be occupied.



[You're reading an excerpt. Click here to read official D-LINK DES-1210-28P user guide](http://yourpdfguides.com/dref/5324783)
<http://yourpdfguides.com/dref/5324783>

Finally, by clicking on the D-Link logo at the upper-left corner of the screen you will be redirected to the local D-Link website. 22 5 Configuration D-Link Web Smart Switch User Manual Tool Bar > Save Menu The Save Menu provides Save Configuration and Save Log functions. Figure 32 â Save Menu Save Configuration Select to save the entire configuration changes you have made to the device to switchâs non-volatile RAM. Figure 33 â Save Configuration Save Log Save the log entries to your local drive and a pop-up message will prompt you for the file path.

You can view or edit the log file by using text editor (e. Figure 35 â Tool Menu Reset Provide a safe reset option for the Switch. All configuration settings in non-volatile RAM will be reset to factory default except for the IP address. Figure 36 â Tool Menu > Reset Reset System Provide another safe reset option for the Switch. All configuration settings in non-volatile RAM will be reset to factory default and then the Switch will reboot.

23 5 Configuration D-Link Web Smart Switch User Manual Figure 37 â Tool Menu > Reset System Reboot Device Provide a safe way to reboot the system. click Reboot to restart the switch. Figure 38 â Tool Menu > Reboot Device Configuration Backup & Restore Allow the current configuration settings to be saved to a file (not including the password), and if necessary, you can restore configuration settings from the file. Two methods can be selected: HTTP or TFTP. Figure 39 â Tool Menu > Configure Backup and Restore HTTP: Backup or restore the configuration file to or from your local drive. Click Backup to save the current settings to your disk. Click Browse to browse your inventories for a saved backup settings file. Click Restore after selecting the backup settings file you want to restore. TFTP: TFTP (Trivial File Transfer Protocol) is a file transfer protocol that allows you to transfer files to a remote TFTP server. Specify TFTP Server IP Address and File Name for the configuration file you want to save to / restore from. Click Backup to save the current settings to the TFTP server. Click Restore after selecting the backup settings file you want to restore. Note: Switch will reboot after restore and all current configurations will be lost Firmware Backup and Upload Allow for the firmware to be saved, or for an existing firmware file to be uploaded to the Switch. Two methods can be selected: HTTP or TFTP. 24 5 Configuration D-Link Web Smart Switch User Manual Figure 40 â Tool Menu > Firmware Backup and Upload HTTP: Backup or upgrade the firmware to or from your local drive of PC.

Click Backup to save the firmware to your disk. Click Browse to browse your inventories for a saved firmware file. Click Upgrade after selecting the firmware file you want to restore. TFTP: Backup or upgrade the firmware to or from a remote TFTP server. Specify TFTP Server IP Address and File Name for the configuration file you want to save to / restore from. Click Backup to save the firmware to the TFTP server. Click Upgrade after selecting the firmware file you want to restore. CAUTION: Do not disconnect the PC or remove the power cord from device until upgrade complete. switch may crash if Firmware upgrade incompletely. Tool Bar > Smart Wizard By clicking the Smart Wizard button, you can return to the Smart Wizard if you wish to make any changes there.

Tool Bar > Online Help The Online Help provides two ways of online support: Online Support Site will lead you to the D-Link website where you can find online resources such as updated firmware images; User Guide can offer an immediate reference for the feature definition or configuration guide. Figure 41 â Online Help 25 5 Configuration D-Link Web Smart Switch User Manual Figure 42 â User Guide Micro Site 26 5 Configuration D-Link Web Smart Switch User Manual Function Tree All configuration options on the switch are accessed through the Setup menu on the left side of the screen. Click on the setup item that you want to configure. The following sections provide more detailed description of each feature and function. Figure 43 â Function Tree Device Information The Device Information provides an overview of the switch, includes essential information such as firmware & hardware information, and IP address.

Figure 44 â Device Information 27 5 Configuration D-Link Web Smart Switch User Manual System > System Settings The System Setting allows the user to configure the IP address and the basic system information of the Switch. IP Information: There are two ways for the switch to obtain an IP address: Static and DHCP (Dynamic Host Configuration Protocol). When using static mode, the IP Address, Subnet Mask and Gateway can be manually configured. When using DHCP mode, the Switch will first look for a DHCP server to provide it with an IP address (including network mask and default gateway) before using the default or previously entered settings. By default the IP setting is static mode with IP address is 10.

System Information: By entering a System Name and System Location, the device can more easily be recognized through the SmartConsole Utility and from other Web-Smart devices on the LAN. Login Timeout: The Login Timeout controls the idle time-out period for security purposes, when there is no action for a specific time span in the Web-based Management. If the current session times out (expires), the user is required a re-login before using the Web-based Management again. Selective range is from 3 to 30 minutes, and the default setting is 5 minutes. Group Interval: The D-Link Web Smart Switch will routinely send report packets to the SmartConsole Utility in order to maintain the information integrity. The user can adjust the Group Interval to optimal frequency. Selective range is from 120 to 1225 seconds, and 0 means disabling the reporting function. Figure 45 â System > System Setting System > DHCP Auto Configuration This page allows you to enable the DHCP Auto Configuration feature on the Switch. When enabled, the Switch becomes a DHCP client and gets the configuration file from a TFTP server automatically on next boot up. To accomplish this, the DHCP server must deliver the TFTP server IP address and configuration file name information in the DHCP reply packet.

The TFTP server must be up and running and store the necessary configuration file in its base directory when the request is received from the Switch. Figure 46 â System > DHCP Auto Configuration System > Trap Settings (For SmartConsole) By configuring the Trap Setting, it allows SmartConsole Utility to monitor specified events on this Web-Smart Switch. by default , Trap Setting is disabled. When the Trap Setting is enabled, enter the Destination IP address of the managing station that will receive trap information. 28 5 Configuration D-Link Web Smart Switch User Manual Figure 47 â System > Trap Setting You can select which event message(s) to be sent to the managing station System Event: The system level messages, which contains: Device Bootup - System boot-up information.



[You're reading an excerpt. Click here to read official D-LINK](http://yourpdfguides.com/dref/5324783)

[DES-1210-28P user guide](http://yourpdfguides.com/dref/5324783)

<http://yourpdfguides.com/dref/5324783>

Illegal Login - Events of incorrect password logins, recording the IP of the originating PC. PoE Power On/Off: Status of power per port (only for DES-1210-28P) PoE Power Error: The four trap events are: power over loading, short circuit, thermal shutdown and power deny (only for DES-1210-28P). NOTE: The total PoE power budget is 193 watts and the remaining 7watts is reserved for the last PoE device to be connected to the switch. The Power Deny trap message is sent out when the switch hits the total power budget and when a new Power Device (PD) requests to connect to the switch at the same time. Over Max Power Budget: When the system supplies power to PDs and hits the max PoE power budget of 193watts, the system will send out this trap message. System > Port Settings In the Port Setting page, the status of all ports can be monitored and adjusted for optimum configuration. By selecting a range of ports (From Port and To Port), the Speed can be set for all selected ports, effective by clicking Apply. Press the Refresh button to view the latest information. The default setting for all ports is Auto. NOTE: Be sure to adjust port speed settings appropriately after changing connected cable media types.

MDI/MDIX: A medium dependent interface (MDI) port is an Ethernet port connection typically used on the Network Interface Card (NIC) or Integrated NIC port on a PC. switches and hubs usually use Medium dependent interface crossover (MDIX) interface. When connecting the Switch to end stations, user have to use straight through Ethernet cables to make sure the Tx/Rx pairs match up properly. When connecting the Switch to other networking devices, a crossover cable must be used. This switch provides configurable MDI/MDIX function for users.

The switches can set as an MDI port in order to connect to other hubs or switches without an Ethernet crossover cable. Auto MDI/MDIX is designed on the switch to detect if the connection is backwards and automatically chooses MDI or MDIX to properly match the connection. the default setting is Auto MDI/MDIX. Flow Control: You can enable this function to mitigate the traffic congestion. Ports configured for full-duplex use 802. SNMP enables network management stations to read and modify the settings of gateways, routers, switches, and other network devices. Use SNMP to configure system features for proper operation, monitor performance and detect potential problems in the Switch or LAN. Managed devices that support SNMP include software (referred to as an agent), which runs locally on the device. A defined set of variables (managed objects) is maintained by the SNMP agent and used to manage the device. These objects are defined in a Management Information Base (MIB), which provides a standard presentation of the information controlled by the on-board SNMP agent.

SNMP defines both the format of the MIB specifications and the protocol used to access this information over the network. 30 5 Configuration D-Link Web Smart Switch User Manual Figure 49 System > SNMP Settings > SNMP Global State Settings System > SNMP Settings > SNMP User Table This page is used to maintain the SNMP user table for the use of SNMPv3. SNMPv3 allows or restricts users using the MIB OID, and also encrypts the SNMP messages sent out between users and Switch. user Name: Enter a SNMP user name of up to 32 characters. Group Name: Specify the SNMP group of the SNMP user. SNMP Version: Specify the SNMP version of the user. Only SNMPv3 encrypts the messages. Auth-Protocol/Password: Specify either HMAC-MD5-96 or HMAC-SHA to be the authentication protocol. Enter a password for SNMPv3 encryption in the right column. Priv-Protocol/Password: Specify either no authorization or DES 56-bit encryption and then enter a password for SNMPv3 encryption in the right column.

Figure 50 System > SNMP Settings > SNMP User Table Click Apply to create a new SNMP user account, and click Delete to remove any existing data. System > SNMP Settings > SNMP Group Table State This page is used to maintain the SNMP Group Table associating to the users in SNMP User Table. SNMPv3 can control MIB access policy, security policy for a user group directly. Group Name: Specify the SNMP user group of up to 32 characters. Read View Name: Specify a SNMP group name for users that are allowed SNMP read privileges to the Switch's SNMP agent.

Write View Name: Specify a SNMP group name for users that are allowed SNMP write privileges to the Switch's SNMP agent. Security Model: Select the SNMP security model. SNMPv1 - SNMPv1 does not support the security features. sSNMPv2 - SNMPv2 supports both centralized and distributed network management strategies. It includes improvements in the Structure of Management Information (SMI) and adds some security features. SNMPv3 - SNMPv3 provides secure access to devices through a combination of authentication and encrypting packets over the network. Security Level: This function is only available when you select SNMPv3 security level. NoAuthNoPriv - No authorization and no encryption for packets sent between the Switch and SNMP manager. AuthNoPriv - Authorization is required, but no encryption for packets sent between the Switch and SNMP manager. 31 5 Configuration

D-Link Web Smart Switch User Manual AuthPriv Both authorization and encryption are required for packets sent between the Switch and SNMP manger. Notify View Name: Specify a SNMP group name for users that can receive SNMP trap messages generated by the Switch's SNMP agent. Figure 51 System > SNMP Settings > SNMP Group Table System > SNMP Settings > SNMP View Table This page allows you to maintain SNMP views to community strings that define the MIB objects which can be accessed by a remote SNMP manager. Figure 52 System > SNMP Settings > SNMP View Table View Name: Name of the view, up to 32 characters. subtree OID: The Object Identifier (OID) Subtree for the view. The OID identifies an object tree (MIB tree) that will be included or excluded from access by an SNMP manager.

oID Mask: The mask of the Subtree OID. 1 means this object number is concerned, 0 means do not concerned. View Type: Specify the configured OID is Included or Excluded that a SNMP manager can access. Click Apply to create a new view, Delete to remove an existing view. System > SNMP Settings > SNMP Community Table This page is used to maintain the SNMP community string of the. SNMP managers using the same community string are permitted to gain access to the Switch's SNMP agent. Community Name: Name of the community string User Name (View Policy): Specify the read/write or read-only level permission for the MIB objects accessible to the SNMP community. 32 5 Configuration D-Link Web Smart Switch User Manual Figure 53 System > SNMP Settings > SNMP Community Table Click Apply to create a new SNMP community, Delete to remove an existing community.



[You're reading an excerpt. Click here to read official D-LINK DES-1210-28P user guide](http://yourpdfguides.com/dref/5324783)
<http://yourpdfguides.com/dref/5324783>

system > SNMP Settings > SNMP Host Table This page is to configure the SNMP trap recipients. Host IP Address: Specify the IP address of SNMP management host.

SNMP Version: Specify the SNMP version to be used to the management host. Community String/SNMPv3 User Name: Specify the community string or SNMPv3 user name for the management host. Figure 54 [System > SNMP Settings > SNMP Host Table](#) Click Apply to create a new SNMP host, Delete to remove an existing host. System > SNMP Settings > SNMP Engine ID The Engine ID is a unique identifier used to identify the SNMPv3 engine on the Switch. Input the Engine ID then click Apply to apply the changes and click Default resets to default value.

Figure 55 [System > SNMP Settings > SNMP Engine ID](#) System > SNMP Settings > SNMP Trap Settings This page is to configure which traps will be sent to the SNMP manage hosts when event happens. Select the event and click Apply to submit the changes. 33 5 Configuration D-Link Web Smart Switch User Manual Figure 56 [System > SNMP Settings > SNMP Trap Setting](#) System > Password Access Control Setting a password is a critical tool for managers to secure the Web-Smart Switch. After entering the old password and the new password two times, click Apply for the changes to take effect. Figure 57 [System > Password Access Control System > System Log Settings](#) System Logs record and manage events, as well as report errors and informational messages.

message severity determines a set of event message will be sent. Click Enable so you can start to configure the related settings of remote system log server, then press Apply for the changes to take effect. Figure 58 [System > System Log Settings](#) Server IP Address: Specifies the IP address of the system log server. UDP Port: Specifies the UDP port to which the server logs are sent. The possible range is 1-65535, and the default value is 514. Time Stamp: Select Enable to time stamp log messages. Severity: Specifies the minimum severity from which warning messages are sent to the server. there are three levels. When a severity level is selected, all severity level choices above the selection are selected automatically. The possible levels are: Warning - The lowest level of a device warning.

Facility: Specifies an application from which system logs are sent to the remote server. Only one facility can be assigned to a single server. If a second facility level is assigned, the first facility is overwritten. There are up to eight facilities can be assigned (Local 0 ~ Local 7). Configuration > 802. 1Q VLAN A VLAN is a group of ports that can be anywhere in the network, but communicate as though they were in the same area. VLANs can be easily organized to reflect department groups (such as R&D, Marketing), usage groups (such as e-mail), or multicast groups (multimedia applications such as video conferencing), and therefore help to simplify network management by allowing users to move devices to a new VLAN without having to change any physical connections. The original settings have the VID as 1, no default name, and all ports as [Untagged](#) Rename: Click to rename the VLAN group. delete VID: Click to delete the VLAN group. Add New VID: Click to create a new VID group, assigning ports from 01 to 28 as Untag, Tag, or Not Member. A port can be untagged in only one VID.

To save the VID group, click Apply. 34 5 Configuration D-Link Web Smart Switch User Manual You may change the name accordingly to the desired groups, such as R&D, Marketing, email, etc. It allows devices in different VLANs to communicate with the servers, firewalls or other shared resources in the shared VLAN. This configuration is accomplished in three steps: Enabling Asymmetric VLAN function Creating shared VLAN and access VLAN Configuring the PVID of access VLAN Asymmetric VLAN is especially effective when used in a small network where a L3 routing device is absent, or if the resource to be shared is not capable of supporting tagged VLAN (for example, a printer). The example below is a typical application of Asymmetric VLAN.

Servers and firewall are located in shared VLAN (default VLAN), and PCs 1, 2 and 3 are located in different VLAN. Because VLANs remain separate, PCs 1, 2, and 3 cannot communicate with each other; but all of them need to access the servers or the Internet behind the firewall. The overlapping VLAN cannot be configured unless this function is enabled. Configure the shared VLAN (VLAN 1) and access VLANs (VLAN 2, 3, 4) In this case, the default VLAN is used as shared VLAN, and the ports that are shared in the network are: Ports 15-18 are connected to the server Port 20 is connected to the firewall The group of shared ports needs to be included for all the VLANs. Ports 15-18, 20 already belong to VLAN 1, therefore no changes are needed.

VLAN 2 is configured to include ports 15-18, 20 (shared VLAN ports) and the set of ports to be separated from the other VLANs (for example, port 5). VLAN 3 and 4 are then configured to include 36 5 Configuration D-Link Web Smart Switch User Manual shared ports and the set of ports to be separated from the other VLANs (for example, port 6 and 7 respectively). Therefore we have three VLANs that share some common ports, but their original membership ports are still separated from each other (for example, port 5, 6, and 7). The VLAN settings of this example are: VLAN 1: default VLAN 1, including all ports with untagged. Configuring the PVID of access VLAN Configure the PVID setting located at the bottom of the VLAN configuration page. The user needs to set the shared set of ports as PVID 1, and the other separated groups of ports (for example, port 5, 6, and 7) as PVID 2, 3 and 4 respectively. The purpose of assigning PVID is to make sure the untagged packets will be transmitted correctly. figure 66 [Configuration > 802. 1Q VLAN > Asymmetric VLAN](#) Assign PVID After configuration, the user will be able to share the network resources set on the shared group of ports (nominated as PVID 1), with both smaller subsets of VLANs (nominated PVID 2, 3 and 4). However, VLAN 2, 3 and 4 groups are incapable of sharing information with each other directly.

1Q Management VLAN setting allows you to transfer the authority of the switch from the default VLAN to others created by users. This allows managing the whole network more flexible. by default , the Management VLAN is disabled. You can select any existing VLAN as the management VLAN when this function is enabled. 1Q Management VLAN Configuration > Voice VLAN > Voice VLAN Setting Voice VLAN is a feature that allows you to automatically place the voice traffic from IP phone to an assigned VLAN to enhance the VoIP service. With a higher priority and individual VLAN, the quality and the security of VoIP traffic are guaranteed. The Voice VLAN function will only insert the Voice VLAN tag to untagged packets under corresponding ports.



[You're reading an excerpt. Click here to read official D-LINK DES-1210-28P user guide](#)
<http://yourpdfguides.com/dref/5324783>

If a VoIP packet comes with a VLAN tag, the Voice VLAN function won't replace the original VLAN tag. After you enabled Voice VLAN, you can configure the Voice VLAN Global Settings. VLAN ID: The ID of VLAN that you want to assign voice traffic to.

You must first create a VLAN from the 802.1Q VLAN page before you can assign a dedicated Voice VLAN. The member port you configured in 802.1Q VLAN setting page will be the static member port of voice VLAN. To dynamically add ports into the voice VLAN, please enable the Auto Detection function

Priority: The 802.

1p priority levels of the traffic in the Voice VLAN. Aging Time: Enter a period of time in hours to remove a port from voice VLAN if the port is an automatic VLAN member. When the last voice device stops sending traffic and the MAC address of this voice device is aged out, the voice VLAN aging timer will be started. The port will be removed from the voice VLAN after expiration of voice VLAN aging timer. Selectable range is from 1 to 120 hours and default is 1 hour.

From Port / To Port: A consecutive group of ports may be configured starting with the selected port. Auto Detection: Switch will add ports to the voice VLAN automatically if it detects the device OUI matches the Telephony OUI configured in Voice VLAN OUI Setting page. Use the drop-down menu to enable or disable the OUI auto detection function. The default is Disabled Click Apply to implement changes made. Note: Voice VLAN has higher priority than any other features even QoS. Therefore the voice traffic will be operated according to Voice VLAN setting and not impacted by QoS feature. 38 5 Configuration D-Link Web Smart Switch User Manual Configuration > Voice VLAN > Voice VLAN OUI Setting This window allows the user to configure the user-defined voice traffic's OUI. @@@@Figure 69 Configuration > Voice VLAN > Voice VLAN OUI Setting There are some pre-defined OUIs and when the user configures personal OUI, these pre-defined OUIs must be avoided. Below are the pre-defined voice traffic's OUI: OUI 00:E0:BB 00:03:6B 00:E0:75 00:D0:1E 00:01:E3 00:60:B9 00:0F:E2 00:09:6E Vendor 3COM Cisco Veritel Pingtel Siemens NEC/Philips Huawei-3COM Avaya Mnemonic Name 3com cisco veritel pingtel siemens nec&philips huawei&3com avaya Default OUI: Pre-defined OUI values, including brand names of 3COM, Cisco, Veritel, Pingtel, Siemens, NEC/Philips, Huawei-3COM, and Avaya. User defined OUI: You can manually create a Telephony OUI with a description.

The maximum number of user defined OUIs is 10. It will occupy one ACL rule when selecting user defined OUI by default, and to configure one user-defined OUI will take extra one ACL rule. System will auto generate an ACL profile (Profile ID: 51) for all the Voice VLAN rules. Select the OUI and press Add to the lower table to complete the Auto Voice VLAN setting. Note: The default OUI for 3COM, Cisco, Veritel, Pingtel, Siemens, NEC/Philips, Huawei-3COM, and Avaya is not common for all of their VoIP devices. Configuration > Auto Surveillance VLAN > Auto Surveillance VLAN Setting Similar as Voice VLAN, Auto Surveillance VLAN is a feature that allows you to automatically place the video traffic from IP cameras to an assigned VLAN to enhance the IP surveillance service. With a higher priority and individual VLAN, the quality and the security of surveillance traffic are guaranteed. The Auto Surveillance VLAN function will only insert the VLAN tag to untagged packets under corresponding ports. If a packet comes with a VLAN tag, the auto surveillance VLAN function won't replace the original VLAN tag. VLAN ID: By default, the VLAN ID 1 was created as Surveillance VLAN and all ports are member ports.

You also can create another Surveillance VLAN by selecting a VLAN ID that you have created a VLAN from the 802.1Q VLAN page. The member port you configured in 802.1Q VLAN setting page will be the static member port of surveillance VLAN. To dynamically add ports into the surveillance VLAN, please enable the Auto Detection function.

priority: The 802.1p priority levels of the traffic in the surveillance VLAN. Aging Time: Enter a period of time in hours to remove an automatic member port from surveillance VLAN. When the last IP camera stops sending traffic and its MAC address is aged out, the aging timer will be started. The port will be removed from the surveillance VLAN after expiration of the aging timer.

Selectable range is from 1 to 120 hours and default is 1 hour. From Port / To Port: A consecutive group of ports may be configured starting with the selected port. Auto Detection: Switch will add ports to the surveillance VLAN automatically if it detects the device OUI matches the Telephony OUI configured in Auto Surveillance VLAN OUI Setting page. Use the drop-down menu to enable or disable the OUI auto detection function. The default is Disabled Click Apply to implement changes made. @@@@The maximum number of user defined OUIs is 5. @@@@Disable - Remove all the member in this trunk group. @@@@ default is 128. @@@@Both devices must support LACP. @@@@ timeout: Specify the administrative LACP timeout.

@@ long (90 Sec) - Defines the LACP timeout as 90 seconds. This is the default value. click Apply to implement the changes made. @@IGMP snooping can help reduce cluttered traffic on the LAN. @@The settings of IGMP snooping is set by each VLAN individually. @@@@The Robustness Variable cannot be set to zero, and it SHOULD NOT be. default is 2 seconds. @@@@ default value is 125 seconds. @@@@This timer will be restarted whenever a Query control message is received over that port. If no Query control messages are received for 'Router Port Purge Interval' time, the learned router port entry will be purged.

default is 260 seconds. 42 5 Configuration D-Link Web Smart Switch User Manual Last Member Query Interval (1-25 sec): The Last Member Query Interval is the Max Response Time inserted into Group-Specific Queries sent in response to Leave Group messages, and is also the amount of time between Group-Specific Query messages. This value may be adjusted to modify the "leave latency" of the network. A reduced value results in reduced time to detect the loss of the last member of a group. default is 1 second.

Max Response Time (10-25 sec): The Max Response Time specifies the maximum allowed time before sending a responding report message. Adjusting this setting effects the "leave latency", or the time between the moment the last host leaves a group and when the multicast server is notified that there are no more members. It also allows adjustments for controlling the frequency of IGMP traffic on a subnet. default is 10 seconds. Querier State: D-Link Smart Switch is able to send out the IGMP Queries to check the status of multicast clients.

default is disabled. To enable IGMP snooping for a given VLAN, select enable and click on the Apply button. Then press the Edit button under Router Port Setting, and select the ports to be assigned as router ports for IGMP snooping for the VLAN, and press Apply for changes to take effect.



[You're reading an excerpt. Click here to read official D-LINK](http://yourpdfguides.com/dref/5324783)

[DES-1210-28P user guide](http://yourpdfguides.com/dref/5324783)

<http://yourpdfguides.com/dref/5324783>

A router port configured manually is a Static Router Port, and a Dynamic Router Port is dynamically configured by the Switch when query control message is received. Figure 75 Configuration > IGMP Router port Settings To view the Multicast Entry Table for a given VLAN, press the View button. Figure 76 Configuration > IGMP Multicast Entry Table Configuration > Multicast Filtering Mode The Multicast Filtering Mode function allows users to select the filtering mode for IGMP groups. Forward All Groups: The multicast stream will be flooded to all ports of the VLAN for both registered and unregistered groups. Forward Unregistered Groups: The multicast stream will be forwarded based on the register table in registered group, but will be flooded to all ports of the VLAN in unregistered group. Filter Unregistered Groups: The registered group will be forwarded based on the register table and the unregistered group will be filtered. 43 5 Configuration D-Link Web Smart Switch User Manual Figure 77 Configuration > Multicast Filtering Mode Configuration > Port Mirroring Port Mirroring is a method of monitoring network traffic that forwards a copy of each incoming and/or outgoing packet from one port of the Switch to another port where the packet can be studied.

This enables network managers to better monitor network performances. Figure 78 Configuration > Port Mirroring Selection options for the Source Ports are as follows: TX (transmit) mode: Duplicates the data transmitted from the source port and forwards it to the Target Port. RX (receive) mode: Duplicates the data that received from the source port and forwards it to the Target Port. None: Turns off the mirroring of the port. click All to remove all ports from mirroring. You may enable or disable this function using the pull-down menu. State: Use the drop-down menu to toggle between Enabled and Disabled. Users can configure the time settings for the switch, and the following parameters can be set or are displayed in the Time Settings page. Figure 80 Configuration > SNTP Settings > Time Settings Clock Source: Specify the clock source by which the system time is set. The possible options are: Local - Indicates that the system time is set locally by the device. SNTP - Indicates that the system time is retrieved from a SNTP server. 45 5 Configuration D-Link Web Smart Switch User Manual Current Time: Displays the current date and time for the switch. If choosing SNTP for the clock source, then the following parameters will be available: SNTP First Server: Specify the IP address of primary SNTP server from which the system time is retrieved. SNTP Second Server: Specify the IP address of secondary SNTP server from which the system time is retrieved. SNTP Poll Interval in Seconds (30-99999): Defines the interval (in seconds) at which the SNTP server is polled for Unicast information.

When selecting Local for the clock source, users can select from one of two options: Manually set current time: Users input the system time manually. Set time from PC: The system time will be synchronized from the local computer. Configuration > SNTP Settings > TimeZone Settings The TimeZone Setting Page is used to configure time zones and Daylight Savings time settings for SNTP. Figure 81 Configuration > SNTP Settings > TimeZone Settings Daylight Saving Time State: Use this drop-down menu to enable or disable the DST Settings. Daylight Saving Time Offset in Minutes: Use this drop-down menu to specify the amount of time that will constitute your local DST offset - 30, 60, 90, or 120 minutes. Time Zone Offset from GMT in +/- HH:MM: Use these drop-down menus to specify your local time zone's offset from Greenwich Mean Time (GMT.) DST Annual Settings: Using annual mode will enable DST seasonal time adjustment. Annual mode requires that the DST beginning and ending date be specified concisely is not in the same month. for example , specify to begin DST on March 8 and end DST on November 1. From: Month: Enter the month DST will start on, each year. From: Day: Enter the day of the week DST will start on, each year. From: Time in HH:MM: Enter the time of day DST will start on, each year. To: Month: Enter the month DST will end on, each year. To: Day: Enter the date DST will end on, each year. To: Time in HH:MM: Enter the time of day that DST will end on, each year.

click Apply to implement changes made. Configuration > Spanning Tree > STP Global Settings The Switch implements two versions of the Spanning Tree Protocol, the Rapid Spanning Tree Protocol (RSTP) as defined by the IEEE 802. 46 5 Configuration D-Link Web Smart Switch User Manual RSTP can operate with legacy equipment implementing IEEE 802. 1D, however the advantages of using RSTP will be lost. RSTP was developed in order to overcome some limitations of STP that impede the function of some recent switching innovations. The basic function and much of the terminology is the same as STP. Most of the settings configured for STP are also used for RSTP. This section introduces some new Spanning Tree concepts and illustrates the main differences between the two protocols. by default , Rapid Spanning Tree is disabled. If enabled, the Switch will listen for BPDU packets and its accompanying Hello packet.

BPDU packets are sent even if a BPDU packet was not received. Therefore, each link between bridges is sensitive to the status of the link. Ultimately this difference results in faster detection of failed links, and thus faster topology adjustment. After enabling STP, setting the STP Global Setting includes the following options: Figure 82 Configuration > Spanning Tree > STP Global Settings STP Version: You can choose RSTP or STP Compatible. the default setting is RSTP.

Bridge Priority: This value between 0 and 61410 specifies the priority for forwarding packets: the lower the value, the higher the priority. the default is 32768. TX Hold Count (1-10): Used to set the maximum number of Hello packets transmitted per interval. The count can be specified from 1 to 10. the default is 6.

Maximum Age (6-40 sec): This value may be set to ensure that old information does not endlessly circulate through redundant paths in the network, preventing the effective propagation of the new information. Set by the Root Bridge, this value will aid in determining that the Switch has spanning tree configuration values consistent with other devices on the bridged LAN. If the value ages out and a BPDU has still not been received from the Root Bridge, the Switch will start sending its own BPDU to all other switches for permission to become the Root Bridge. If it turns out that the Switch has the lowest Bridge Identifier, it will become the Root Bridge. A time interval may be chosen between 6 and 40 seconds. the default value is 20. (Max Age has to have a value bigger than Hello Time) Hello Time (1-10 sec): The user may set the time interval between transmissions of configuration messages by the root device, thus stating that the Switch is still functioning.



[You're reading an excerpt. Click here to read official D-LINK DES-1210-28P user guide](http://yourpdfguides.com/dref/5324783)
<http://yourpdfguides.com/dref/5324783>

the default is 2 seconds. Forward Delay (4-30 sec): This sets the maximum amount of time that the root device will wait before changing states. the default is 15 seconds.

Root Bridge: Displays the MAC address of the Root Bridge. Root Maximum Age: Displays the Maximum Age of the Root Bridge. Root Forward Delay: Displays the Forward Delay of the Root Bridge. root port: Displays the root port. Click Apply for the settings to take effect. In addition to setting Spanning Tree parameters for use on the switch level, the Switch allows for the configuration of groups of ports, each port-group of which will have its own spanning tree, and will require some of its own configuration settings. An STP Group spanning tree works in the same way as the switch-level spanning tree, but the root bridge concept is replaced with a root port concept. A root port is a port of the group that is elected based on port priority and port cost, to be the connection to the network for the group. Redundant links will be blocked, just as redundant links are blocked on the switch level. The STP on the switch level blocks redundant links between switches (and similar network devices).

The port level STP will block redundant links within an STP Group. it is advisable to define an STP Group to correspond to a VLAN group of ports. Figure 83 Configuration > Spanning Tree > STP Port Settings From Port/To Port: A consecutive group of ports may be configured starting with the selected port. External Cost: This defines a metric that indicates the relative cost of forwarding packets to the specified port list. 0 (auto) - Setting 0 for the external cost will automatically set the speed for forwarding packets to the specified port(s) in the list for optimal efficiency.

Value 1-200000000 - Define a value between 1 and 200000000 to determine the external cost. The lower the number, the greater the probability the port will be chosen to forward packets. Migrate: Setting this parameter as Yes will set the ports to send out BPDU packets to other bridges, requesting information on their STP setting. If the Switch is configured for RSTP, the port will be capable to migrate from 802. Migration should be set as yes on ports connected to network stations or segments that are capable of being upgraded to 802.

1w RSTP on all or some portion of the segment. Edge: Selecting the True parameter designates the port as an edge port. Edge ports cannot create loops, however an edge port can lose edge port status if a topology change creates a potential for a loop. Selecting the False parameter indicates that the port does not have edge port status. Selecting the Auto parameter indicates that the port have edge port status or not have edge port status automatically. Priority: Specify the priority of each port. Selectable range is from 0 to 240, and the default setting is 128. The lower the number, the greater the probability the port will be chosen as a root port. p2P: Choosing the True parameter indicates a point-to-point (P2P) shared link. P2P ports are similar to edge ports, however they are restricted in that a P2P port must operate in full-duplex.

like edge ports, P2P ports transition to a forwarding state rapidly thus benefiting from RSTP. A p2p value of false indicates that the port cannot have p2p status. Auto allows the port to have p2p status whenever possible and operate as if the p2p status were true. If the port cannot maintain this status, (for example if the port is forced to half-duplex operation) the p2p status changes to operate as if the p2p value were False. The default setting for this parameter is Auto. Restricted Role: Toggle between True and False to set the restricted role state of the packet. If set to True, the port will never be selected to be the Root port. the default value is False. Restricted TCN: Toggle between True and False to set the restricted TCN of the packet. Topology Change Notification (TCN) is a BPDU that a bridge sends out to its root port to signal a topology change.

If set to True, it stops the port from propagating received TCN and to other ports. the default value is False. Click Apply for the settings to take effect. click Refresh to renew the page. QoS > Storm Control The Storm Control feature provides the ability to control the receive rate of broadcast, multicast, and unknown unicast packets.

Once a packet storm has been detected, the Switch will drop packets coming into the Switch until the storm has subsided. Figure 84 Configuration > Storm Control Storm Control Type: User can select the different Storm type from Broadcast Only, Multicast & Broadcast, and Multicast & Broadcast & Unknown Unicast. Threshold (64Kbps * N): If storm control is enabled (default is disabled), the threshold is from of 64 ~ 1,024,000 Kbit per second, with steps (N) of 64Kbps. N can be from 1 to 16000. Click Apply for the settings to take effect.

QoS > Bandwidth Control The Bandwidth Control page allows network managers to define the bandwidth settings for a specified port's transmitting and receiving data rates. 49 5 Configuration D-Link Web Smart Switch User Manual Figure 85 Configuration > QoS > Bandwidth Control From Port / To Port: A consecutive group of ports may be configured starting with the selected port. Type: This drop-down menu allows you to select between RX (receive), TX (transmit), and Both. This setting will determine whether the bandwidth ceiling is applied to receiving, transmitting, or both receiving and transmitting packets. No Limit: This drop-down menu allows you to specify that the selected port will have no bandwidth limit. enabled disables the limit. Rate (64-1024000): This field allows you to enter the data rate, in Kbits per second, will be the limit for the selected port. The value is between 64 and 1024000. Click Apply to set the bandwidth control for the selected ports. NOTE: The TX rate for Gigabit ports can only be configured in multiples of 1850kbps.

If any other value is used, the system automatically rounds it down to the lower multiple of 1850. Ip standard that allows network administrators to reserve bandwidth for important functions that require a larger bandwidth or that might have a higher priority, such as VoIP (voice-over Internet Protocol), web browsing applications, file server applications or video conferencing. Thus with larger bandwidth, less critical traffic is limited, and therefore excessive bandwidth can be saved. The following figure displays the status of Quality of Service priority levels of each port, higher priority means the traffic from this port will be first handled by the switch. For packets that are untagged, the switch will assign the priority depending on your configuration. 50 5 Configuration D-Link Web Smart Switch User Manual Figure 86 Configuration > QoS > 802. 1p Default Priority By selecting the DSCP priority, the web pages will changes as seen below: Figure 87 Configuration > QoS > DSCP Priority Settings Select QoS Mode: D-Link Smart Switch allows the user to prioritize the traffic based on the 802.



[You're reading an excerpt. Click here to read official D-LINK](#)

[DES-1210-28P user guide](#)

<http://yourpdfguides.com/dref/5324783>