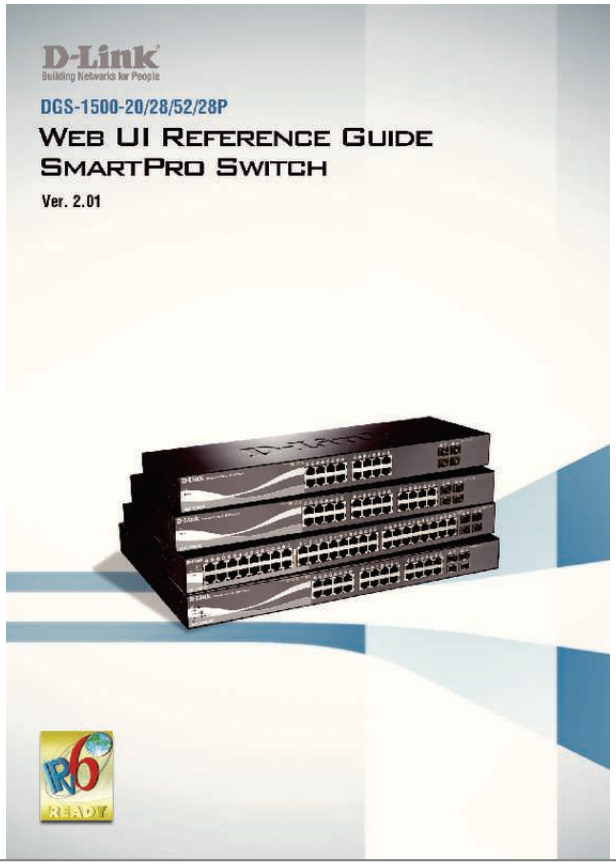

Manual abstract:

@@Terms/Usage In this guide, the term â□□Switchâ□□ (first letter capitalized) refers to the SmartPro Switch, and â□□switchâ□□ (first letter lower case) refers to other Ethernet switches. Some technologies refer to terms â□□switchâ□□, â□□bridgeâ□□ and â□□switching hubsâ□□ 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 SmartPro Switch Products. D-Link's next generation SmartPro 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 four 1000BASE-X SFP slots for fiber connection, network security, traffic segmentation, QoS and versatile management. flexible Port Configurations. Four port densities are available for selection: 16, 24, and 48 Gigabit Ethernet ports.

Supporting auto-detection of MDI/MDIX, these switches bring inexpensive and easy Ethernet connection to the desktops. DGS-1500 series provides 4 SFP slots, which supports 1000M fiber connections with appropriate fiber transceivers. DGS-1500-28P provides 4 combo SFP slots, which supports both 1000M and 100M fiber connections with appropriate fiber transceivers. The first 24 ports also support up to 15. 4 or 30 watts PoE power for the connections of wireless access points, IP phones and other PoE-supported devices, allowing them to be deployed at difficult places such as on high walls and ceilings, where AC power outlets are not readily available.

d-Link Green Technology. D-Link Green devices are about providing eco-friendly alternatives without compromising performance. D-Link Green Technology includes a number of innovations to reduce energy consumption on DGS-1500 series such as reducing power when a port does not have a device attached, or adjusting the power usage according to the Ethernet cable connected to it. For PoE model such as DGS1500-28P, D-Link Green Technology offers Time-based PoE feature to shut down per port power off working hours. extensive Layer 2 Features.

Implemented as complete L2 devices, these switches include functions such as IGMP snooping, port mirroring, Spanning Tree, 802. Implemented as complete L3 devices, these switches include functions such as IP interface, static route, IPv6 Static Route, ARP and single IP management to enhance performance and network resiliency. 1p priority queues, enabling users to run bandwidthsensitive applications such as streaming multimedia by prioritizing that traffic in network. These functions allow switches to work seamlessly with VLAN and 802. 1p traffic and IPv6 traffic class priority in the network. network Security. D-Linkâ□□s innovative Safeguard Engine function protects the switches against traffic flooding caused by virus attacks. Additional features Storm Control can help to keep the network from being overwhelmed by abnormal traffic. Port Security is another simple but useful authentication method to maintain the network device integrity. The new generation of D-Link Web Smart Switches provides growing businesses with a simple and easy management of their network, using an intuitive SmartConsole utility or a Web-Based management interface that allows administrators to remotely control their network down to the port level.

The SmartConsole easily allows customers to discover multiple D-Link web smart switches with the same L2 network segment connected to the userâ□□s local PC. With this utility, users do not need to change the IP address of the PC and provide easy initial settings of the smart switches. The switches within the same L2 network segment connected to the userâ□□s local PC are displayed on the screen for instant access. it allows extensive switch configuration settings , and basic configuration of discovered devices , such as a password change or firmware upgrade. Users can also access the switch via TELNET. Some basic tasks can be performed 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 by using the Command Line Interface (CLI). 2 1 Product Introduction D-Link Web Smart Switch User Manual In addition, users can utilize the SNMP MIB (Management Information Base) to poll the 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, and provides easy-to-use graphic interface and facilitates the operation efficiency. dGS-1500-20 16-Port 10/100/1000Mbps plus 4 1000Base-T/SFP ports SmartPro Switch.

Front Panel SFP ports for optical transceivers Figure 1. 1 â□□ DGS-1500-20 Front Panel Power LED : The Power LED lights up when the Switch is connected to a power source. Reset: By pressing the Reset button, the Switch will change back to the default configuration and all changes will be lost. port Link/Act/Speed LED (1-16 , 17F , 18F , 19F , 20F): The port LEDs indicate a network link through the corresponding port. Blinking indicates the Switch is either sending or receiving data to the port.

When the port LED glows in amber, it indicates the port is running on 10M or 100M. When the port LED glows in green, it is running on 1000Mbps. 2 â□□ DGS-1500-20 Rear Panel Power: The power port is where to connect the AC power cord. dGS-1500-28 24-Port 10/100/1000Mbps plus 4 1000Base-T/SFP ports SmartPro Switch. Front Panel SFP ports for optical transceivers Figure 1.

3 â□□ DGS-1500-28 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 (1-24, 25F, 26F, 27F, 28F): 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 an amber light, this indicates that the port is running on 10M or 100M. When it has a green light it is running on 1000M. Reset: By pressing the Reset button, the Switch will change back to the default configuration and all changes will be lost. rear Panel Figure 1. 4 â□□ DGS-1500-28 Rear Panel Power: The power port is where to connect the AC power cord.

dGS-1500-28P 24-Port 10/100/1000Mbps plus 4 1000Base-T/SFP ports SmartPro PoE Switch. Front Panel SFP ports for optical transceivers Figure 1.

5 â□□ DGS-1500-28P Front Panel Power LED : The Power LED lights up when the Switch is connected to a power source. Pwr Max: The Pwr Max LED lights up when the Switch reaches the maximum power budget defined by the administrator via PoE System Settings page of Web GUI or the default power budget of 78 Watts. Reset: By pressing the Reset button, the Switch will change back to the default configuration and all changes will be lost. Mode: By pressing the Mode button, the Port LED will switch between Link/Act and PoE modes. Port Link/Act/Speed LED (1-24, 25F, 26F, 27F, 28F): 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 an amber light, this indicates that the port is running on 10M or 100M. When it has a green light it is running on 1000Mbps. Fan: The Fan LED lights green when fans work well, and lights red when fans fail. NOTE: On DGS-1500-28P, the SFP ports are shared with normal RJ-45 ports 25 to 28.

When optical transceiver is inserted to SFP port and link up, the RJ-45 port cannot be used. 4 1 Product Introduction D-Link Web Smart Switch User Manual Port PoE LED (1-24): When mode LED lights up in PoE mode, the port LEDs indicate powering status over the corresponding port. rear Panel Figure 1. 6 â□□ DGS-1500-28P Rear Panel Power: The power port is where to connect the AC power cord. dGS-1500-52 48-Port 10/100/1000Mbps plus 4 100/1000FX SFP Slot SmartPro Switch.

Front Panel SFP ports for optical transceivers Figure 1. 7 â□□ DGS-1500-52 Front Panel Power LED : The Power LED lights up when the Switch is connected to a power source. Port Link/Act/Speed LED (1-48, 49F, 50F, 51F, 52F): 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 an amber light, this indicates that the port is running on 10M or 100M.

When it has a green light it is running on 1000M. Fan: The Fan LED lights green when fans work well, and lights red when fans fail. Reset: Press the Reset button to reset the Switch back to the default settings. 8 â□□ DGS-1500-52 Rear Panel Power: Connect the supplied AC power cable to this port. 5 2 Hardware Installation D-Link Web Smart Switch User Manual 2 Hardware Installation This chapter provides unpacking and installation information for the D-Link SmartPro 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 SmartPro 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 deviceâ□□s base. Allow enough ventilation space between the device and the objects around it. figure 2. 1 â□□ 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 switchâ□□s side panels (one on each side) and secure them with the screws provided (with 8 M3*6. 2 â□□ Attach the mounting brackets to the Switch Then, use the screws provided with the equipment rack to mount the switch in the rack. 6 2 Hardware Installation D-Link Web Smart Switch User Manual Figure 2. 3 â□□ 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 multi-unit rack assembly, the operating ambient temperature of the rable-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 supports 10 languages including English , Traditional Chinese , Simplified Chinese , German , Spanish , French , Italian , Portuguese , Japanese and Russian. By default, the password is admin and the language is English. figure 3. 3 â□□ Logon Dialog Box Smart Wizard After a successful login, the Smart Wizard will guide you through essential cation indicates where the message was 12 4 SmartConsole Utility D-Link Web Smart Switch User Manual received and IP Address denotes where it comes from. 3 â□□ 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. Time indicates when the trap message was received, Location indicates where the trap message was received, IP denotes where it comes from and Event shows the content of this trap message. 4 â□□ 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 Monitor List By clicking on this icon you will see below options: 13 4 SmartConsole Utility D-Link Web Smart Switch User Manual Figure 4. 5 â□□ SmartConsole Monitor List Save: Records the setting of the Device List as default for the next time the SmartConsole Utility is used. Save As: Records the setting of the Device List in an appointed filename and file path. restore: Manually reload a Device List setting file. About Click this icon to launch the SmartConsole Info window. figure 4. 6 â□□ SmartConsole About Device Configuration The Device Configuration in the SmartConsole Utility has five icons: Device Settings Password Settings 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, MAC Address, IPv4 Address, Subnet Mask, Gateway, System Name, Location, Trap IP, Group Interval, and DHCP Client Setting of the Switch.

To apply the configuration, insert the correct device password in the Confirm Password box and then click OK. Click on this icon to launch the Device Password Manager window. Here you can enter a new password and confirm it. figure 4. 8 â SmartConsole Password Settings Firmware Upgrade Select one or many switches of the 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 the device, and then click Upgrade. The state will show "OK" after completion, or âFailâ if the firmware upgrade fails or cannot be completed for any reason.

15 4 SmartConsole Utility D-Link Web Smart Switch User Manual Figure 4. 9 â Firmware Upgrade CAUTION: Do not disconnect the PC or remove the power cord from the device until the upgrade completes. The software may be corrupted because of 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 IPv4 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 IPv4 address from the DHCP server. 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 of 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 the Discover List, or select a device and click the â button to remove it. 12 â SmartConsole Delete device Device List This list displays all discovered Web-Smart devices on the network. figure 4. 13 â SmartConsole Device List Definitions of the Device List features: Select: Click the Select to choose a switch for configuration settings. Monitor: Click the Monitor button and the SmartConsole will collect the trap and log data from the device. In the monitor means the device was discovered by SmartConsole. Click the icon to have the The device to continue updating the information, such as system log or trap to the SmartConsole Utility. the icon .

When the device was detected as not reachable, the icon will change to will appear if the power or the cable of this device is disconnected. Subnet Mask: Displays the Subnet Mask setting of the device. Gateway: Displays the Gateway setting of the device. mAC Address: Displays the device MAC Addresses. Firmware version: Displays the current Firmware version of this device. system Name: Displays the appointed device system name. Location: Displays the location of the appointed device. SNMP: Displays the SNMP status of the device. Trap IP: Displays the IP address of the host where the Trap information will be sent. DHCP: Specify if the device gets the IP address from a DHCP server.

17 . Please check 4 SmartConsole Utility D-Link Web Smart Switch User Manual Group Interval: Displays the intervals (in seconds) that the Switch will be discovered in the SmartConsole Device List. NOTE: If the devices are marked red in the device list, it means that a firmware upgrade is required again. NOTE: If the IP address of device is showed with IPv6 address, then it can not be configured with Smartconsole Utility. The user needs to double click the selected device and login the web for configuration.

18 5 Configuration D-Link Web Smart Switch User Manual 5 Configuration The features and functions of the D-Link SmartPro 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 Donât show Smart Wizard next time for the next time you logon to the Webbased Management. IPv4 Information IPv4 Information will guide you to do basic configurations on 3 steps for the IP Information, access password, and SNMP.

Select Static, DHCP or BOOTP, and type the desired new IP Address, select the Netmask and type the Gateway address, then click the Apply button to enter the next Password setting page. (No need to enter IP Address, Netmask and Gateway of DHCP and BOOTP selection.) The IP address is allowed for IPv4 and IPv6 address. If you are not changing the settings, click Exit button to go back to the main page. Or you can click on Ignore the wizard next time to skip wizard setting when the switch boots up. Password Settings Type the desired new password in the Password box and again in the Confirm Password, then click the Next button to the SNMP setting page. 19 5 Configuration D-Link Web Smart Switch User Manual Figure 5. 2 â Password setting in Smart Wizard SNMP Settings The SNMP Setting allows you to quickly enable/disable the SNMP function. the default SNMP Setting is Disabled. Click Enabled and then click Apply to make it effective.

figure 5. 3 â SNMP Setting 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 a detailed description. 20 5 Configuration D-Link Web Smart Switch User Manual If you want to change the IP settings, click OK and start a new web browser. Figure 9 â Confirm the changes of IP address in Smart Wizard Web-based Management After clicking the Exit button in Smart Wizard you will see the screen below: Figure 5. 4 â Web-based Management The above image 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.

21 5 Configuration D-Link Web Smart Switch User Manual 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.

5 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 5. 6 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.

8 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 5. 9 â□□ Tool Menu > Reset Reset System Provide another safe reset option for the Switch. All configuration settings in non-volatile RAM will reset to factory default and the Switch will reboot. 22 5 Configuration D-Link Web Smart Switch User Manual Figure 5. 10 â□□ Tool Menu > Reset System Reboot Device Provide a safe way to reboot the system. 11 â□□ Tool Menu > Reboot Device Configuration Backup and 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 this file. Two methods can be selected: HTTP or TFTP. figure 5.

12 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. Select IPv4 or IPv6 and specify TFTP Server IP Address and TFTP File Name for the configuration file you want to save to / restore from. the maximum Telnet Server connection is 4. 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 Upgrade 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. 23 5 Configuration D-Link Web Smart Switch User Manual Figure 5. 13 â□□ Tool Menu > Firmware Backup and Upload HTTP: Backup or upgrade the firmware to or from your local PC drive. 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. Select IPv4 or IPv6 and specify TFTP Server IP Address and TFTP File Name for the configuration file you want to save to / restore from. the maximum Telnet Server connection is 4. 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 the upgrade completes. The Switch may crash if the Firmware upgrade is incomplete. 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. 15 â□□ User Guide Micro Site 25 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. 17 â□□ Device Information 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, and 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.

27 5 Configuration D-Link Web Smart Switch User Manual Figure 5. 18 â□□ System > System Settings System > Password The Password page allows user to change the login password of the device. figure 5. 19 â□□ System > Password To set the Password, set the following parameters and click Apply: Old Password: If a password was previously configured for this entry, enter it here in order to change it to a new password. New Password: Enter the new password that you wish to set on the Switch to authenticate users attempting to access Administrator Level privileges on the Switch.

The user may set a password of up to 20 characters. confirm Password: Confirm the new password entered above. Entering a different password here from the one set in the New Local Enabled field will result in a fail 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 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 the 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 a configurable MDI/MDIX function for users. The switches can be 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 â□□Autoâ□□ MDI/MDIX. Flow Control: You can enable this function to mitigate the traffic congestion. Ports configured for full-duplex use 802. 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. Server IP Address: Select IPv4 or IPv6 and specifies the IP address of the system log server. UDP Port (1 - 65535): Specifies the UDP port to which the server logs are sent. The possible range is 1 â□□ 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). System > Time Profile The Time Profile page allows users to configure the time profile settings of the device.

Date: Select Date and specifies the From Day and To Day of the time profile. Click Add to create a new time profile or click Delete to delete a time profile from the table. NOTE: The time must be set after current time, otherwise it will take effect on the next cycle time. 30 5 Configuration D-Link Web Smart Switch User Manual System > Power Saving The Power Saving mode feature reduces power consumption automatically when the RJ-45 port is link down or the connected devices are turned off. Less power will be consumed also when the short cable is used (less than 20 meters). By reducing power consumption, less heat is produced, resulting in extended product life and lower operating costs. By default, the Cable Length Detection and Link Status Detection are enabled. 24 â□□ System > Power Saving Advanced Power Saving Settings: Type: Specifies the Power Saving type to be LED Shut-off, Port Shut-off, Port Standby or System Hibernation. lED Shut-off - The LED Shut-off gets high priority. If the user select LED Shut-off, the profile function will not take effect.

It means the LED can not be turned on after Time Profile timeâ□□s up when the state is disabled. On the contrary, if the LED is enabled, the Time Profile function will work. Port Shut-off - The Port Shut-off state has high priority (the priority rule is the same as LED.) Therefore, if the Port Shut-off sate is already disabled the Time Profile function will not take effect. Port Standby - The system changes to standby state and wait for a wake up event. Each port on the system enters sleep state by schedule. System Hibernation - In this mode, switches get most power-saving figures since main chipsets (both MAC and PHY) are disabled for all ports, and energy required to power the CPU is minimal. state: Specifies the power saving state to be Enabled or Disabled. Time Profile 1: Specifies the time profile or None. Time Profile 2: Specifies the time profile or None.

Port: Specifies the ports to be configure of the Power Saving. click Select All configure all ports , or click Clear to uncheck all port. Then click Apply to implement changes made. 3 EEE standard defines mechanisms and protocols intended to reduce the energy consumption of network links during periods of low utilization, by transitioning interfaces into a low-power state without interrupting the network connection. The transmitted and received sides should be IEEE802.

3az EEE compliance. By default, the switch enabled the 802. 3az EEE function. Users can disable this feature by individual port via the IEEE802. 3az EEE settings From Port / To Port: A consecutive group of ports may be configured starting with the selected port.

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 â□□Untaggedâ□□ Delete: Click to delete the VLAN group. Add: 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. You may change the name accordingly to the desired groups, such as R&D, Marketing, email, etc. 1Q VLAN > VID Assignments VLAN > VLAN Status The VLAN Status page is for user to search the VLAN which has already existed by VLAN ID or VLAN Name. figure 5. 30 â□□ VLAN > VLAN Status 33 5 Configuration D-Link Web Smart Switch User Manual VLAN > GVRP > GVRP Global Settings The GVRP Global Settings page allows user to configure the GARP timer values for application join, leave, and leave_all GARP timer values.

Join Time (100-100000): Indicates the time in milliseconds that PDUs are transmitted. the default value is 200ms. Leave Time (100-100000): Indicates the amount of time in milliseconds that the device waits before leaving its GARP state. The leave time is activated by a leave all time message sent/received, and cancelled by the Join message. the default value is 600ms. Leave_All Time (100-100000): Used to confirm the port within the VLAN. The time in milliseconds between messages sent. NOTE: Leave time must be greater than or equal to three times the join time. Leave_all time must be greater than the leave time. VLAN > GVRP > GVRP Port Settings The GVRP Port Settings page allows user to determine whether the Switch will share its VLAN configuration information with other GARP VLAN Registration Protocol (GVRP) enabled switches.

In addition, Ingress Checking can be used to limit traffic by filtering incoming packets whose PVID does not match the PVID of the port.

Results can be seen in the table under the configuration settings, as seen below. figure 5. 32 â VLAN > GVRP > GVRP Port Settings 34 5 Configuration D-Link Web Smart Switch User Manual From Port/To Port: These two fields allow user to specify the range of ports that will be included in the Portbased VLAN that user is creating using the 802. 1Q Port Settings page.

PVID(1-4094): The read-only field in the 802. 1Q Port Table shows the current PVID assignment for each port, which may be manually assigned to a VLAN when created in the Settings table. The Switch's default is to assign all ports to the default VLAN with a VID of 1. The PVID is used by the port to tag outgoing, untagged packets, and to make filtering decisions about incoming packets. If the port is specified to accept only tagged frames - as tagging, and an untagged packet is forwarded to the port for transmission, the port will add an 802.

1Q tag using the PVID to write the VID in the tag. When the packet arrives at its destination, the receiving device will use the PVID to make VLAN forwarding decisions. If the port receives a packet, and Ingress filtering is enabled, the port will compare the VID of the incoming packet to its PVID. If the two are unequal, the port will drop the packet. If the two are equal, the port will receive the packet. GVRP: The Group VLAN Registration Protocol (GVRP) enables the port to dynamically become a member of a VLAN. gVRP is Disabled by default. Ingress Checking: This field can be toggled using the space bar between Enabled and Disabled. Enabled enables the port to compare the VID tag of an incoming packet with the PVID number assigned to the port. If the two are different, the port filters (drops) the packet.

Acceptable Frame Type: This field denotes the type of frame that will be accepted by the port. The user may choose between Tagged Only, which means only VLAN tagged frames will be accepted, and Admit_All, which mean both tagged and untagged frames will be accepted. VLAN > Voice VLAN > Voice VLAN Global Settings 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. If a VoIP packet comes with a VLAN tag, the Voice VLAN function wonât replace the original VLAN tag. 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 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.

priority: The 802. 1p priority levels of the traffic in the Voice VLAN. the default priority is highest. 35 5 Configuration D-Link Web Smart Switch User Manual Voice VLAN OUI Settings: this allows the user to configure the user-defined voice trafficâs OUI. An Organizationally Unique Identifier (OUI) is the first three bytes of the MAC address.

This identifier uniquely identifies a vendor, manufacturer, or other organization. default OUI: Pre-defined OUI values , including brand names of 3COM , Cisco , Veritel , Pingtel , Siemens , NEC/Philips , Huawei3COM , 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. 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 trafficâs 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 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, Huawei3COM, and Avaya is not common for all of their VoIP devices. VLAN > Voice VLAN > Voice VLAN Port Settings The Voice VLAN Port Settings page allows users 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. figure 5. 34 â VLAN > Voice VLAN > Voice VLAN Port Settings 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 36 5 Configuration D-Link Web Smart Switch User Manual Tagged / Untagged: tagged or untagged the ports. Click Apply to implement changes made and Refresh to refresh the voice vlan table. 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. Note: It is recommended setting the highest priority for Voice VLAN to guarantee the quality of VoIP traffic.

35 â VLAN > Voice VLAN > Voice Device List Select a port or all ports and click Search to display the Voice Device information in the table. VLAN > Auto Surveillance VLAN Similar as Voice VLAN, Auto Surveillance VLAN is a feature that allows you to automatically place the video traffic from D-Link 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 check the source OUI/MAC address / VLAN ID on the incoming packets. If it matches specified MAC address / VLAN ID, the packets will pass through switch with desired priority.

VLAN ID: By default, the VLAN ID 4094 was created as Auto Surveillance VLAN. You also can create another Auto 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 Auto Surveillance VLAN.
Priority: Specifies the priority level of Auto Surveillance VLAN on the Switch. The possible values are Highest, High, Medium and Low. the default priority is High. Tagged Uplink/Downlink Port: Specifies the port or ports to be tagged uplink port or downlink port for the Auto Surveillance VLAN. There are another five surveillance components that could be configured to be auto-detected by the Auto Surveillance VLAN. These five components are Video Management Server (VMS), VMS Client/Remote viewer, Video Encoder, Network Storage and Other IP Surveillance Devices. Description: Specifies the description for the component type. MAC/OUI: You can manually create an MAC or OUI address for the surveillance component. The maximum number of user defined MAC address is 5. System will auto generate an ACL profile (Profile ID: 56) for all the Auto Surveillance VLAN rules.

Click Add to create a new surveillance component and Refresh to refresh the Auto Surveillance VLAN summary table. L2 Functions > Jumbo Frame Jumbo Frame support is designed to enhance Ethernet networking throughput and significantly reduce the CPU utilization of large file transfers like large multimedia files or large data files by enabling more efficient larger payloads per packet. The Jumbo Frame page allows network managers to enable Jumbo Frames on the device. The Jumbo Frame default is disabled, Select Enabled then click Apply to turn on the jumbo frame support. figure 5. 37 â L2 Functions > Jumbo Frame Settings L2 Functions > 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. Target Port: Defines the target port. Source Port Selection: TX: Duplicates the data transmitted from the source port and forwards it to the Target Port. click âallâ to include all ports into port mirroring.
RX: Duplicates the data that received from the source port and forwards it to the Target Port. click âallâ to include all ports into port mirroring. TX/RX: Duplicate both the data transmitted from and data sent to the source port, and forwards all the data to the assigned Target Port. click âallâ to include all ports into port mirroring. None: Turns off the mirroring of the port.
L2 Functions > Loopback Detection The Loopback Detection function is used to detect the loop created by a specific port while Spanning Tree Protocol (STP) is not enabled in the network, especially when the down links are hubs or unmanaged switches. The Switch will automatically shutdown the port and sends a log to the administrator. The Loopback Detection port will be unlocked when the Loopback Detection Recover Time times out. The Loopback Detection function can be implemented on a range of ports at a time. You may enable or disable this function using the pull-down menu.
Recover Time (0 or 60-1000000): Time allowed (in seconds) for recovery when a Loopback is detected. The Loop Detection Recover Time can be set at 0 seconds, or 60 to 1000000 seconds. From Port: The beginning of a consecutive group of ports may be configured starting with the selected port. To Port: The ending of a consecutive group of ports may be configured starting with the selected port. State: Use the drop-down menu to toggle between Enabled and Disabled. default is Disabled. Click Apply to implement changes made or click Refresh to refresh the Loopback Detection table. l2 Functions > MAC Address Table > Static MAC This feature provides two distinct functions. The Disable Auto Learning table allows turning off the function of learning MAC address automatically, if a port isn't specified as an uplink port (for example, connects to a DHCP Server or Gateway). 40 â L2 Functions > MAC Address Table > Static MAC To initiate the removal of auto-learning for any of the uplink ports, enable this feature, and then select the port(s) for auto learning to be disabled.

The Static MAC Address Lists table displays the static MAC addresses connected, as well as the VID. Click Add to add a new MAC address, you also need to select the assigned Port number. Enter both the Mac Address and VID, and then Click Add. click Delete to remove one entry or click Delete all to clear the list. By disabling Auto Learning capability and specifying the static MAC addresses, the network is protected from potential threats like hackers, because traffic from illegal MAC addresses will not be forwarded by the Switch. L2 Functions > MAC Address Table > Dynamic Forwarding Table For each port, this table displays the MAC address learned by the Switch. To add a MAC address to the Static Mac Address List, click the Add to Static MAC checkbox, and then click Apply associated with the identified address. figure 5. 41 â L2 Functions > MAC Address Table > Dynamic Forwarding Table 40 5 Configuration D-Link Web Smart Switch User Manual L2 Functions > Spanning Tree > STP Bridge Global Settings The Switch implements three versions of the Spanning Tree Protocol, the Rapid Spanning Tree Protocol (RSTP) as defined by the IEEE 802. 1w specification , a version compatible with the IEEE 802.
1D STP and the Multiple Spanning Tree Protocol (MSTP) as defined by the IEEE802. 1 specification. 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. the IEEE 802. 1 Multiple Spanning Tree (MSTP) provides various load balancing scenarios by allowing multiple VLANs to be mapped to a single spanning tree instance, providing multiple pathways across the network.
For example, while port A is blocked in one STP instance, the same port can be placed in the Forwarding state in another STP instance. 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. by default Multiple Spanning Tree is enabled. It will tag BPDU packets to receiving devices and distinguish spanning tree instances, spanning tree regions and the VLANs associated with them. After enabling STP, setting the STP Bridge Global Setting includes the following options.

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. 41 5 Configuration D-Link Web Smart Switch User Manual 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 3. 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. 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. Forwarding BPDU: Bridges use Bridge Protocol Data Units (BPDU) to provide spanning tree information.

STP BPDUs filtering is useful when a bridge interconnects two regions; each region needing a separate spanning tree. BPDU filtering functions only when STP is disabled either globally or on a single interface. The possible field values are: Disabled â BPDU filtering is enabled on the port. enabled â BPDU forwarding is enabled on the port (if STP is disabled). Root Bridge: Displays the MAC address of the Root Bridge.

Root Cost: Displays the cost of the Root Bridge. the default is 0. Root Maximum Age: Displays the Maximum Age of the Root Bridge. the default is 20. Root Forward Delay: Displays the Forward Delay of the Root Bridge. 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. figure 5. 43 â L2 Functions > 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. Forwarding BPDU: Bridges use Bridge Protocol Data Units (BPDU) to provide spanning tree information. STP BPDUs filtering is useful when a bridge interconnects two regions; each region needing a separate spanning tree. BPDU filtering functions only when STP is disabled either globally or on a single interface. The possible field values are: Disabled â BPDU filtering is enabled on the port. enabled â BPDU forwarding is enabled on the port (if STP is disabled). Hello Time: The interval between two transmissions of BPDU packets sent by the Root Bridge to indicate to all other switches that it is indeed the Root Bridge. the default value is 2.

Click Apply for the settings to take effect. click Refresh to renew the page. L2 Functions > Spanning Tree > MST Configuration Identification Multiple Spanning Tree (MSTP) provides various load balancing scenarios by allowing multiple VLANs to be mapped to a single spanning tree instance, providing multiple pathways across the network. For example, while port A is blocked in one STP instance, the same port can be placed in the Forwarding state in another STP instance.

The MST Configuration Identification page is for defining global MSTP settings, including region names, MSTP revision level. 43 5 Configuration D-Link Web Smart Switch User Manual Figure 5. 44 â L2 Functions > Spanning Tree > MST Configuration Identification MST Configuration Identification Settings: Configuration Name: A configured name set on the switch to uniquely identify the MSTI (multiple spanning tree instance). If a configuration name is not set, this field shows the MAC address of the device running MSTP. Revision Level(0 - 65535): This value, together with the configuration name, and identical vlans mapped for STP instance IDs identifies the MST region configured on the switch. click Apply to define the configuration name and revision level.

Instance ID Settings: MSTI ID (1 - 15): Displays the MSTI ID associated with the VID List. The possible field range is 1-15. type: Defines the type of edit. The possible values are: Add VID - Indicates that edit type is add Remove VID - Indicates that edit type is removed. L2 Functions > Spanning Tree > STP Instance Settings The STP Instance Settings page display MSTIs currently set on the Switch and allows users to change the Priority of the MSTPs. figure 5. 45 â L2 Functions > Spanning Tree > STP Instance Settings To modify an entry on the table, click the Edit button. To view more information about and entry on the table at the top of the window, click the view button. The window above contains the following information: MSTI ID: Enter the MSTI ID in this field. an entry of 0 denotes the CIST (default MSTI).

Priority: Enter the new priority in the Priority field. The user may set a priority value between 0-61440. MSTP Port Setting: Instance ID: Lists the MSTP instances configured on the device. possible field range is 0-7. Internal Path Cost (0-200000000, 0=Auto): Indicates the port contribution to the Spanning Tree instance. The range should always be 1-200,000,000. The default value is automatically set cost, according to its speed. Selecting 0(zero) for this parameter will set the quickest route automatically and optimally for an interface. Priority: Defines the interface priority for the specified instance. the default value is 128.

A higher priority will designate the interface to forward packets first. A low number denotes a higher priority. Click Apply to implement the changes made or Edit to change the port settings. L2 Functions > Link Aggregation > Port Trunking The Trunking function enables the combining of two or more ports together to increase bandwidth. Up to eight Trunk groups may be created, and each group consists up to eight ports.

There are two types can be selected: Static - Static link aggregation. Select the ports to be grouped together, and then click Apply to activate the selected Trunking groups. 45 5 Configuration D-Link Web Smart Switch User Manual NOTE: Each combined trunk port must be connected to devices within the same VLAN group. L2 Functions > Link Aggregation > LACP Port Settings The LACP Port Settings is used to create port trunking groups on the Switch. The user may set which ports will be active and passive in processing and sending LACP control frames Figure 5.

48 â L2 Functions > Link Aggregation > LACP Port Settings From Port: The beginning of a consecutive group of ports may be configured starting with the selected port. To Port: The ending of a consecutive group of ports may be configured starting with the selected port. Activity: There are two different roles of LACP ports: Active - Active LACP ports are capable of processing and sending LACP control frames. This allows LACP compliant devices to negotiate the aggregated link so the group may be changed dynamically as needs require. In order to utilize the ability to change an aggregated port group, that is, to add or subtract ports from the group, at least one of the participating devices must designate LACP ports as active. Both devices must support LACP. Passive - LACP ports that are designated as passive cannot initially send LACP control frames. In order to allow the linked port group to negotiate adjustments and make changes dynamically, one end of the connection must have "active" LACP ports. timeout: Specify the administrative LACP timeout. The possible field values are: Short (3 Sec) - Defines the LACP timeout as 3 seconds.

long (90 Sec) - Defines the LACP timeout as 90 seconds. This is the default value. click Apply to implement the changes made. L2 Functions > Multicast > IGMP Snooping With Internet Group Management Protocol (IGMP) snooping, the Web Smart Switch can make intelligent multicast forwarding decisions by examining the contents of each frameâs Layer 2 MAC header. IGMP snooping can help reduce cluttered traffic on the LAN. With IGMP snooping enabled globally, the Web Smart Switch will forward multicast traffic only to connections that have group members attached. The settings of IGMP snooping is set by each VLAN individually. If enabled, the IGMP Global Settings will need to be entered: Host Timeout (130-153025 sec): This is the interval after which a learned host port entry will be purged. For each host port learned, a 'Port Purge Timer' runs for 'Host Port Purge Interval'. This timer will be restarted whenever a report message from host is received over that port.

If no report messages are received for 'Host Port Purge Interval' time, the learned host entry will be purged from the multicast group. If a subnet is expected to be lossy, the Robustness Variable may need to be increased. The Robustness Variable cannot be set to zero, and it SHOULD NOT be. default is 2 seconds. Query Interval (60-600 sec): The Query Interval is the interval between General Queries sent.

By adjusting the Query Interval, the number of IGMP messages can be increased or decreased; larger values will cause IGMP Queries to be sent less often. default value is 125 seconds. Router Timeout (60-600 sec): This is the interval after which a learned router port entry will be purged. For each router port learned, a 'Router Port Purge Timer' runs for 'Router Port Purge Interval'. This timer will be restarted whenever a Query control message is received over that port.

If there are no Query control messages received for 'Router Port Purge Interval' time, the learned router port entry will be purged. default is 260 seconds. 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.