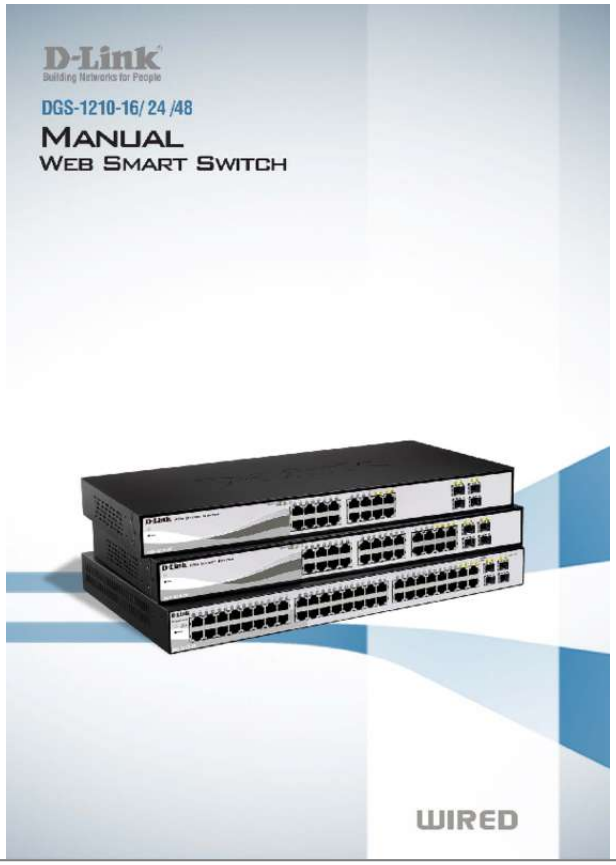

Manual abstract:

@@Terms/Usage In this guide, the term â□□Switchâ□□ (first letter capitalized) refers to the Smart 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 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 four combo 100/1000BASE-X SFP slots for fiber connection, network security, traffic segmentation, QoS and versatile management. choices of 16 , 24 , and 48 ports. Three 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. Each switch provides 4 combo SFP slots, which supports both 1000M and 100M fiber connections with appropriate fiber transceivers. 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-1210 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.

extensive Layer 2 Features. Implemented as complete L2 devices, these switches include functions such as IGMP snooping, port mirroring, Spanning Tree, 802. The switches support 802. 1Q VLAN standard tagging to enhance network security and performance. The switches also support 802. 1p priority queues, enabling users to run bandwidth-sensitive applications such as streaming multimedia by prioritizing that traffic in network. These functions allow switches to work seamlessly with VLAN and 802. 1p traffic in the network. Auto Voice VLAN will automatically place the voice traffic from IP phone to an assigned VLAN with higher priority, so it can be separated from normal data 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-Linkâ□□s innovative Safeguard Engine function protects the switches against traffic flooding caused by virus attacks. additional features like 802. 1X port-based authentication provides access control of the network with external RADIUS servers. aCL is a powerful tool to screen unwanted IP or MAC traffic.

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. versatile Management. 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).

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. 2 1 Product Introduction D-Link Web Smart Switch User Manual DGS-1210-16 16-Port 10/100/1000Mbps with 4 Combo SFP Slot Web Smart Switch Front Panel SFP ports for optical transceivers Figure 1 â□□ DGS-1210-16 Front Panel Power LED : The Power LED lights up when the Switch is connected to a power source. Port Link/Act/Speed LED (1-12, 13F, 14F, 15F, 16F, 13T, 14T, 15T, 16T): 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. NOTE: On DGS-1210-16, the SFP ports are shared with normal RJ-45 ports 13 to 16. When optical transceiver is inserted to SFP port and link up, 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 â□□ DGS-1210-16 Rear Panel Power: The power port is where to connect the AC power cord. DGS-1210-24 24-Port 10/100/1000Mbps with 4 Combo SFP Slot Web Smart Switch Front Panel Figure 3 â□□ DGS-1210-24 Front Panel SFP ports for optical transceivers Power LED : The Power LED lights up when the Switch is connected to a power source. Port Link/Act/Speed LED (1-20, 21F, 22F, 23F, 24F, 21T, 22T, 23T, 24T): The Link/Act/Speed LED flashes, which indicates a network link through the corresponding port. Blinking indicates that the Switch is either 3 1 Product Introduction D-Link Web Smart Switch User Manual 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: Press the Reset button to reset the Switch back to the default settings. all previous changes will be lost. NOTE: On the DGS-1210-24, the SFP ports are shared with normal RJ-45 ports 49 and 50.

When optical transceiver is inserted to SFP port and link up, the RJ-45 port cannot be used. Rear Panel Figure 4 â DGS-1210-24 Rear Panel Power: Connect the supplied AC power cable to this port. DGS-1210-48 48-Port 10/100/1000Mbps with 4 Combo SFP Slot Web Smart Switch Front Panel SFP ports for optical transceivers Figure 5 â DGS-1210-48 Front Panel Power LED : The Power LED lights up when the Switch is connected to a power source. Port Link/Act/Speed LED (1-44, 45F, 46F, 47F, 48F, 45T, 46T, 47T, 48T): 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 Err: The Fan Err LED lights red when the fan fails. It is off when all fans work normally. Reset: Press the Reset button to reset the Switch back to the default settings.

all previous changes will be lost. NOTE: On the DGS-1210-48, the SFP ports are shared with normal RJ-45 ports 49 and 50. When the optical transceiver is inserted to the SFP port and linked up, the RJ-45 port cannot be used. Rear Panel Figure 6 â DGS-1210-48 Rear Panel 4 1 Product Introduction D-Link Web Smart Switch User Manual 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 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 deviceâs base. Allow enough ventilation space between the device and the objects around it. Figure 7 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 switchâs 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 â 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 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 rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature (Tma) specified by the manufacturer. B) Reduced Air Flow - Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised.

C) Mechanical Loading - Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading. D) Circuit Overloading - Consideration should be given to the connection of the equipment to the supply circuit, and the effect that overloading of the circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern. e) Reliable Earthing - Reliable earthing of rack-mounted equipment should be maintained. Particular attenti only for computers running Windows 2000, Windows XP, or Windows Vista x64/86 operating systems. There are two options for the installation of the SmartConsole Utility; one is through the autorun program on the installation CD and the other is manual installation. NOTE: Please be sure to uninstall any existing SmartConsole Utility from your PC before installing the latest SmartConsole Utility. 10 3 Getting Started D-Link Web Smart Switch User Manual Option 1: Follow these steps to install the SmartConsole Utility via the autorun program on the installation CD. 1. Insert the Utility CD into your CD-Rom/DVD-Rom Drive.

Cl 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. To apply the configuration, insert the correct device password in the Confirm Password box and then click OK Figure 20 â 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 â SmartConsole Device Password Manager Multi 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. Figure 22 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 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 â 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 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. Figure 24 â SmartConsole Add device Figure 25 â SmartConsole Delete device Device List This list displays all discovered Web-Smart devices on the network. Figure 26 â SmartConsole Device List Definitions of the Device List features: Monitor: Checking the Monitor box 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 device The to continue updating the information, such as system log or trap to the SmartConsole Utility. the icon will .

When the device was detected as not reachable, the icon will change to appear power or the cable of this device is disconnected. Please check if the 4 SmartConsole Utility D-Link Web Smart Switch User Manual Protocol version: Displays the software version of the Utility. DHCP: Specify if the device gets the IP address from a DHCP server. Location: Displays the location of the appointed device. Trap IP: Displays the IP address of the host where the Trap information will be sent.

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. SNMP: Displays the SNMP status of the device.

NOTE: If the devices are marked red in the device list, it means that a firmware upgrade is required again. nOTE: The LLDP function is only provided by PoE models. For non-PoE models, the LLDP column will appear blank. 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 Donâ t show Smart Wizard next time for the next time you logon to the Webbased Management. 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 â Configure Password in Smart Wizard 19 5 Configuration D-Link Web Smart Switch User Manual SNMP Settings The SNMP Setting allows you to quickly enable/disable the SNMP function and configure the SNMP community name.

For the complete SNMP function, please check â Setup Menu > System > SNMP Settingsâ in the Web Interface. the default SNMP Setting is Disabled. Click Enabled, enter Community names, and then click Apply to make it effective. Figure 28 â 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 â Setup Menu > System > System Settingsâ . 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 â 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 a detailed description. If you want to change the IP settings, click OK and start a new web browser. Figure 30 â 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 â Web-based Management Main Configuration Screen 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.

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 reset to factory default and 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 this 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 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. 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 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. 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 âFunction Tree Device Information The Device Information provides an overview of the switch, including essential information such as firmware & hardware information, and IP address. 27 5 Configuration D-Link Web Smart Switch User Manual Figure 44 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. Figure 45 â System > System Setting 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. Figure 46 â System > Trap Setting You can select which event message(s) will be sent to the managing station 28 5 Configuration D-Link Web Smart Switch User Manual System Event: The system level messages, which contains: Device Bootup - System boot-up information.

Illegal Login - Events of incorrect password logins, recording the IP of the originating PC. 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. Figure 47 â System > Port Setting Speed: Gigabit Fiber connections can operate in 1000M Full Force Mode, Auto Mode or Disabled.

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. 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. Figure 48 â□□ System > SNMP Setting Community Setting: In support of SNMP version 1, the Web-Smart Switch accomplishes user authentication by using Community Settings that function as passwords. The remote user SNMP application and the Switch SNMP must use the same community string.
SNMP packets from a station that are not authenticated are ignored (dropped). The default community strings for the Switch used for SNMP v. Trap Setting: Traps are messages that alert network personnel of events that occur on the Switch. Such events can be as severe as a reboot (someone accidentally turned the Switch OFF), or less serious events such as a port status change. The Switch can generate traps and send them to the trap recipient (i.
Setting up a Trap: Select Enable, enter a Trap Name, add the IP of the device to be monitored, and select the event(s) to trap. The available trap Events to choose from include: SNMP Authentication Traps System Device Bootup Fiber Link Up / Link Down Twisted Pair Link Up / Link Down RSTP Port State Change Firmware Upgrade State 30 5 Configuration D-Link Web Smart Switch User Manual Note: Trap Name must be selected from a Community Name 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 twice, click Apply for the changes to take effect. Figure 49 â□□ 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 messages that will be sent. Click Enable so you can start to configure the related settings of the remote system log server, then press Apply for the changes to take effect. Figure 50 â□□ 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 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), Configuration > Jumbo Frame D-Link Gigabit Web Smart Switches support jumbo frames (frames larger than the Ethernet frame size of 1536 bytes) of up to 10,000 bytes (tagged). Default is disabled, Select Enabled then click Apply to turn on the jumbo frame support. 6 Figure 51 â□□ Configuration > Jumbo Frame 31 5 Configuration D-Link Web Smart Switch User Manual 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 â□□Untaggedâ□□ 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. 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 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 59 â□□ Configuration > 802. 1Q VLAN > Asymmetric VLAN â□□ Assign PVID 34 5 Configuration D-Link Web Smart Switch User Manual 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. If a VoIP packet comes with a VLAN tag, the Voice VLAN function wonâ□□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. 35 5 Configuration D-Link Web Smart Switch User Manual Aging Time: Enter a period of time (in hours) to remove a port from the 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 start. The port will be removed from the voice VLAN after the expiration of the 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 the 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 (including QoS). Therefore the voice traffic will be operated according to the Voice VLAN setting and not impacted by the QoS feature. Configuration > Voice VLAN > Voice VLAN OUI Setting This window allows the user to configure the user-defined voice traffic□□s OUI. @@@@@@@@@@The maximum number of user defined OUIs is 10.
@@@@@@@@@@@@@@@@@@@@@@@@@@@ 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.
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.
38 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. Press Apply for changes to take effect. A router port configured manually is a Static Router Port, and a Dynamic Router Port is dynamically configured by the Switch when a query control message is received. Figure 66 â□□ Configuration > IGMP Snooping > IGMP Router port Settings To view the Multicast Entry Table for a given VLAN, press the View button.

Figure 67 â□□ Configuration > IGMP Multicast Entry Table 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. 39 5 Configuration D-Link Web Smart Switch User Manual Figure 68 â□□ 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. click â□□allâ□□ to include all ports into port mirroring. RX (receive) mode: Duplicates the data that is received from the source port and forwards it to the Target Port. click â□□allâ□□ to include all ports into port mirroring. Both (transmit and receive) mode: Duplicate both the data transmitted from and data sent to the source port, and forwards all the data to the assigned Target Port. click â□□allâ□□ to include all ports into port mirroring. None: Turns off the mirroring of the port.

click â□□allâ□□ 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. @@The SNTP settings folders contain two windows: Time Settings and TimeZone Settings. 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 71 â□□ 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. 41 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 the primary SNTP server from which the system time is retrieved. SNTP Second Server: Specify the IP address of the 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 72 â□□ 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 must not be 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. 42 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 73 â□□ 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. 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 the 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 74 â□□ 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 75 â□□ QoS > 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 portâ□□s transmitting and receiving data rates. 45 5 Configuration D-Link Web Smart Switch User Manual Figure 76 â□□ 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. 1p 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. figure 77 â□□ QoS > 802.
1p Default Priority By selecting the DSCP priority, the web pages will changes as seen below: 46 5 Configuration D-Link Web Smart Switch User Manual Figure 78 â□□ QoS > DSCP Priority Settings Select QoS Mode: D-Link Smart Switch allows the user to prioritize the traffic based on the 802. 1p priority in the VLAN tag or the DSCP (Differentiated Services Code Point) priority in the IP header. Only one mechanism is selected to prioritize the packets at a time. Queuing Mechanism: Select Strict Priority to process the packets with the highest priority first. Select WRR (Weighted Round-Robin) to process packets according to the weight of each priority.
When a priority level has reached its egress weight, the system will process the packets in the next level even if there are remaining packets. 1p QoS mode, you can use From Port / To Port to specify the default priority of each port. In DSCP mode, you can configure the global default priority value by using From DSCP value / To DSCP value. Security > Trusted Host Use Trusted Host function to manage the switch from a remote station. You can enter up to ten designated management stations networks by defining the IP address/Subnet Mask as seen in the figure below.
Figure 79 Security > Trusted Host 47 5 Configuration D-Link Web Smart Switch User Manual To define a management station IP setting, click the Add Host button and type in the IP address and Subnet mask. Click the Apply button to save your settings. You may permit only single or a range of IP addresses by different IP mask settings, the format can either be 192. Please see the example below for permitting the IP range IP Address 192. 255 To delete the IP address, simply click the Delete button. Check the unwanted address, and then click Apply. Security > Safeguard Engine D-Linkâ□□s Safeguard Engine is a robust and innovative technology that automatically throttles the impact of packet flooding into the switch's CPU. This function helps protect the Web-Smart Switch from being interrupted by malicious viruses or worm attacks.

this option is enabled by default. Figure 80 â Security > Safeguard Engine Security > Port Security Port Security is a security feature that prevents unauthorized computers (with source MAC addresses) unknown to the Switch prior to stopping auto-learning processing from gaining access to the network.

A given portsâ (or a range of ports') dynamic MAC address learning can be stopped such that the current source MAC addresses entered into the MAC address forwarding table can not be changed once the port lock is enabled. Using the drop-down menu, change Admin State to Enabled, and then click Apply to confirm the setting. 1X Settings Network switches provide easy and open access to resources, by simply attaching a client PC. Unfortunately this automatic configuration also allows unauthorized personnel to easily intrude and possibly gain access to sensitive data. 48 5 Configuration D-Link Web Smart Switch User Manual IEEE-802. 1X provides a security standard for network access control, especially in Wi-Fi wireless networks. The switch uses Extensible Authentication Protocol over LANs (EAPOL) to exchange authentication protocol client identity (such as a user name) with the client, and forward it to another remote RADIUS authentication server to verify access rights. The EAP packet from the RADIUS server also contains the authentication method to be used. The client can reject the authentication method and request another, depending on the configuration of the client software and the RADIUS server. Depending on the authenticated results, the port is either made available to the user, or the user is denied access to the network.

The RADIUS servers make the network a lot easier to manage for the administrator by gathering and storing the user lists. To use EAP for security, select enabled and set the 802. 1X Global Settings for the Radius Server and applicable authentication information. RADIUS Server IP: The IP address of the external Radius Server. Confirm Key: Enter the Key a second time for confirmation.

TxPeriod (1 â 65535 sec): This sets the TxPeriod of time for the authenticator PAE state machine. This value determines the period of an EAP Request/Identity packet transmitted to the client. default is 24 seconds. ReAuthEnabled: This function is to determine whether regular re-authentication will take place on this port(s). QuietPeriod (0 â 65535 sec): Sets the number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client.

Default is 80 seconds SuppTimeout (1 â 65535 sec): This value determines timeout conditions in the exchanges between the Authenticator and the client. default is 12 seconds. ServerTimeout (1 â 65535 sec): Sets the amount of time the switch waits for a response from the client before resending the response to the authentication server. default is 16 seconds. MaxReq (1 â 10): This parameter specifies the maximum number of times that the switch retransmits an EAP request (md-5challnege) to the client before it times out the authentication session. default is 5 times. ReAuthPeriod (1 â 4294967295 sec): This command affects the behavior of the switch only if periodic reauthentication is enabled. 1X Port Access Control: Three type of Port Access Control State can be "Force Authorized", "Force UnAuthorized", and "Auto". 49 5 Configuration D-Link Web Smart Switch User Manual Select Force Authorized to disable 802. 1X and cause the port to transition to the authorized state without any authentication exchange required.

This means the port transmits and receives normal traffic without 802. 1X-based authentication of the client. If Force Unauthorized is selected, the port will remain in the unauthorized state ignoring all attempts by the client to authenticate. The Switch cannot provide authentication services to the client through the interface. if Auto is selected , it will enable 802. 1X and cause the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port transitions from down to up, or when an EAPOL-start frame is received. The Switch then requests the identity of the client and begins relaying authentication messages between the client and the authentication server. the default setting is Auto. Security > 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). by default , this feature is Off (disabled). Figure 83 â Security > Static Mac Address To initiate the removal of auto-learning for any of the uplink ports, click On to enable this feature, and then select the port(s) for auto learning to be disabled. The Static MAC Address Setting table displays the static MAC addresses connected, as well as the VID. Click Add Mac 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 Apply. click Delete to remove one entry or click Delete all to clear the list. You can also copy a learned MAC address from the Dynamic Forwarding Table (please refer to Security > MAC Address Table > Dynamic Forwarding Table for details). 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. Security > 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 checkbox, and then click Apply associated with the identified address. 50 5 Configuration D-Link Web Smart Switch User Manual Figure 84 â Security > Dynamic Forwarding Table Monitoring > Statistics The Statistics screen displays the status of each port packet count. Figure 85 â Monitoring > Statistics Refresh All: Renews the details collected and displayed. Clear All Counters: To reset the details displayed. To view the statistics of individual ports, click one of the linked port numbers for details. Figure 86 â Monitoring > Port Statistics 51 5 Configuration D-Link Web Smart Switch User Manual Previous Page: Go back to the Statistics main page. refresh: To renew the details collected and displayed. Clear Counter: To reset the details displayed. 52 5 Configuration D-Link Web Smart Switch User Manual Monitoring > Cable Diagnostics The Cable Diagnostics is designed primarily for administrators and customer service representatives to examine the copper cable quality. It rapidly determines the type of cable errors occurred in the cable.