

DES-1032 SWITCH
CONFIGURATION UTILITY
USER MANUAL

Version 2.20
February 21, 2000

Printed In Taiwan



RECYCLABLE

LIMITED WARRANTY

D-Link Systems, Inc. ("D-Link") provides this limited warranty for its product only to the person or entity who originally purchased the product from D-Link or its authorized reseller or distributor.

Limited Hardware Warranty: D-Link warrants that the hardware portion of the D-Link products described below ("Hardware") will be free from material defects in workmanship and materials from the date of original retail purchase of the Hardware, for the period set forth below applicable to the product type ("Warranty Period") if the Hardware is used and serviced in accordance with applicable documentation; provided that a completed Registration Card is returned to an Authorized D-Link Service Office within ninety (90) days after the date of original retail purchase of the Hardware. If a completed Registration Card is not received by an authorized D-Link Service Office within such ninety (90) period, then the Warranty Period shall be ninety (90) days from the date of purchase.

<i>Product Type</i>	<i>Warranty Period</i>
Product (excluding power supplies and fans), if purchased and delivered in the fifty (50) United States, or the District of Columbia ("USA")	As long as the original purchaser still owns the product
Product purchased or delivered outside the USA	One (1) Year
Power Supplies and Fans	One (1) Year
Spare parts and spare kits	Ninety (90) days

D-Link's sole obligation shall be to repair or replace the defective Hardware at no charge to the original owner. Such repair or replacement will be rendered by D-Link at an Authorized D-Link Service Office. The replacement Hardware need not be new or of an identical make, model or part; D-Link may in its discretion may replace the defective Hardware (or any part thereof) with any reconditioned product that D-Link reasonably determines is substantially equivalent (or superior) in all material respects to the defective Hardware. The Warranty Period shall extend for an additional ninety (90) days after any repaired or replaced Hardware is delivered. If a material defect is incapable of correction, or if D-Link determines in its sole discretion that it is not practical to repair or replace the defective Hardware, the price paid by the original purchaser for the defective Hardware will be refunded by D-Link upon return to D-Link of the defective Hardware. All Hardware (or part thereof) that is replaced by D-Link, or for which the purchase price is refunded, shall become the property of D-Link upon replacement or refund.

Limited Software Warranty: D-Link warrants that the software portion of the product ("Software") will substantially conform to D-Link's then current functional specifications for the Software, as set forth in the applicable documentation, from the date of original delivery of the Software for a period of ninety (90) days ("Warranty Period"), if the

Software is properly installed on approved hardware and operated as contemplated in its documentation. D-Link further warrants that, during the Warranty Period, the magnetic media on which D-Link delivers the Software will be free of physical defects. D-Link's sole obligation shall be to replace the non-conforming Software (or defective media) with software that substantially conforms to D-Link's functional specifications for the Software. Except as otherwise agreed by D-Link in writing, the replacement Software is provided only to the original licensee, and is subject to the terms and conditions of the license granted by D-Link for the Software. The Warranty Period shall extend for an additional ninety (90) days after any replacement Software is delivered. If a material non-conformance is incapable of correction, or if D-Link determines in its sole discretion that it is not practical to replace the non-conforming Software, the price paid by the original licensee for the non-conforming Software will be refunded by D-Link; provided that the non-conforming Software (and all copies thereof) is first returned to D-Link. The license granted respecting any Software for which a refund is given automatically terminates.

What You Must Do For Warranty Service:

Registration Card. The Registration Card provided at the back of this manual must be completed and returned to an Authorized D-Link Service Office for each D-Link product within ninety (90) days after the product is purchased and/or licensed. The addresses/telephone/fax list of the nearest Authorized D-Link Service Office is provided in the back of this manual. FAILURE TO PROPERLY COMPLETE AND TIMELY RETURN THE REGISTRATION CARD MAY AFFECT THE WARRANTY FOR THIS PRODUCT.

Submitting A Claim. Any claim under this limited warranty must be submitted in writing before the end of the Warranty Period to an Authorized D-Link Service Office. The claim must include a written description of the Hardware defect or Software nonconformance in sufficient detail to allow D-Link to confirm the same. The original product owner must obtain a Return Material Authorization (RMA) number from the Authorized D-Link Service Office and, if requested, provide written proof of purchase of the product (such as a copy of the dated purchase invoice for the product) before the warranty service is provided. After an RMA number is issued, the defective product must be packaged securely in the original or other suitable shipping package to ensure that it will not be damaged in transit, and the RMA number must be prominently marked on the outside of the package. The packaged product shall be insured and shipped to D-Link, 53 Discovery Drive, Irvine CA 92618, with all shipping costs prepaid. D-Link may reject or return any product that is not packaged and shipped in strict compliance with the foregoing requirements, or for which an RMA number is not visible from the outside of the package. The product owner agrees to pay D-Link's reasonable handling and return shipping charges for any product that is not packaged and shipped in accordance with the foregoing requirements, or that is determined by D-Link not to be defective or non-conforming.

What Is Not Covered:

This limited warranty provided by D-Link does not cover:

Products that have been subjected to abuse, accident, alteration, modification, tampering, negligence, misuse, faulty installation, lack of reasonable care, repair or service in any way that is not contemplated in the documentation for the product, or if the model or serial number has been altered, tampered with, defaced or removed;

Initial installation, installation and removal of the product for repair, and shipping costs;

Operational adjustments covered in the operating manual for the product, and normal maintenance;

Damage that occurs in shipment, due to act of God, failures due to power surge, and cosmetic damage; and

Any hardware, software, firmware or other products or services provided by anyone other than D-Link.

Disclaimer of Other Warranties: EXCEPT FOR THE LIMITED WARRANTY SPECIFIED HEREIN, THE PRODUCT IS PROVIDED “AS-IS” WITHOUT ANY WARRANTY OF ANY KIND INCLUDING, WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. IF ANY IMPLIED WARRANTY CANNOT BE DISCLAIMED IN ANY TERRITORY WHERE A PRODUCT IS SOLD, THE DURATION OF SUCH IMPLIED WARRANTY SHALL BE LIMITED TO NINETY (90) DAYS. EXCEPT AS EXPRESSLY COVERED UNDER THE LIMITED WARRANTY PROVIDED HEREIN, THE ENTIRE RISK AS TO THE QUALITY, SELECTION AND PERFORMANCE OF THE PRODUCT IS WITH THE PURCHASER OF THE PRODUCT.

Limitation of Liability: TO THE MAXIMUM EXTENT PERMITTED BY LAW, D-LINK IS NOT LIABLE UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY OR OTHER LEGAL OR EQUITABLE THEORY FOR ANY LOSS OF USE OF THE PRODUCT, INCONVENIENCE OR DAMAGES OF ANY CHARACTER, WHETHER DIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, LOSS OF INFORMATION OR DATA CONTAINED IN, STORED ON, OR INTEGRATED WITH ANY PRODUCT RETURNED TO D-LINK FOR WARRANTY SERVICE) RESULTING FROM THE USE OF THE PRODUCT, RELATING TO WARRANTY SERVICE, OR ARISING OUT OF ANY BREACH OF THIS LIMITED WARRANTY, EVEN IF D-LINK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE SOLE REMEDY FOR A BREACH OF THE FOREGOING LIMITED WARRANTY IS REPAIR, REPLACEMENT OR REFUND OF THE DEFECTIVE OR NON-CONFORMING PRODUCT.

GOVERNING LAW: This Limited Warranty shall be governed by the laws of the state of California.

Some states do not allow exclusion or limitation of incidental or consequential damages, or limitations on how long an implied warranty lasts, so the foregoing limitations and

exclusions may not apply. This limited warranty provides specific legal rights and the product owner may also have other rights which vary from state to state.

CONTENTS

INTRODUCTION	1
<i>Broadcast Issues</i>	1
<i>Benefits of VLANs</i>	3
<i>Link Trunking</i>	4
SYSTEM REQUIREMENTS.....	5
INSTALLATION	5
MAIN FUNCTION DESCRIPTIONS	6
1. Port Based Security Option:.....	6
2. SuperMAC option:	6
3. Aging Control:	7
4. Broadcast Storm Control:.....	7
5. Address Learning:	7
6. Full Duplex Flow Control (802.3X):.....	8
7. Auto-Negotiation:	8
8. Trunk Settings:	8
9. VLAN settings:	9
10. Flood Control:	9
11. Explicit Address Table Entry:	10
PROGRAM DESCRIPTIONS.....	11
<i>Main Window</i>	11
<i>Properties Window System Page</i>	14
<i>Properties Window Port Page</i>	16
<i>Properties Window Trunk Assignment Page</i>	19
<i>Properties Window VLAN Page</i>	23
<i>Properties Window Explicit Address Table Page</i>	27
<i>Default Configuration</i>	29
TYPICAL STEPS TO USE SWITCH CONFIGURATION UTILITY	30
<i>To Edit a Configuration File</i>	30
<i>To Transmit Current Configuration to the Switch</i>	32
<i>To Assign Trunks and Set VLAN Groups</i>	33
TROUBLESHOOTING	40

Introduction

The DES-1032 has all the functions of a Fast Ethernet switch as well as many useful features such as VLAN, port trunking, broadcast storm control, secure mode traffic filtering and flow control are provided by the device. The user can take advantage of these features by using the DES-1032 Switch Configuration Utility. The utility is a Windows based program with a comprehensive user interface running on Windows 95, Windows 98, Windows SE and Windows 2000. Once the Switch Configuration Utility has been loaded onto a PC and connected to the device through the parallel port, the user can easily reconfigure the device. The system configurations are stored on EEPROMs. During start-up or device reset, the device will read the EEPROMs and initialize the system. Users may use the utility to make changes to their systems while retaining their preferences.

Broadcast Issues

Broadcast packets are used for tasks such as presence or service announcements, searching for servers, and other tasks that need to be forwarded to every device in the node. Broadcasts normally form less than 1% of the traffic sent by each networked device and rarely exceed 5% of network traffic. However, as the network grows and more devices are connected the amount of bandwidth consumed is greater because broadcast packets are being sent to every device on the network.

Depending on the applications used, when too many devices are connected to a network, broadcasts can occupy more than 50% of the bandwidth each device receives. In such situation, it is likely that most of the broadcast traffic will be useless for most of the receiving devices, resulting in bandwidth loss. To limit the damage of broadcast affection, the solution is to separate group of devices in a single network segment beyond which broadcasts are not

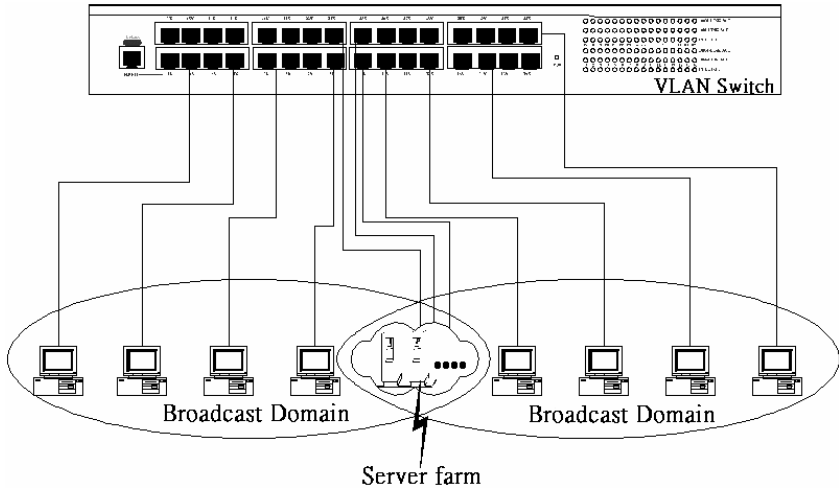
transmitted. All the devices grouped in such a segment share the same broadcast domain.

Traditionally, routers were used to isolate the different segments of a large network. Routers are Layer 3 network equipment that use the IP protocol to forward unicast packets toward the broadcast domain of the segments while containing the broadcast packets inside that domain. The extra manipulation performed on each packet and the necessary configuration and management make the router a complex and expensive solution.

VLAN switching is a simple solution to protect your network against broadcast storms by creating segments based on Layer 2 Ethernet information. By avoiding the complexity and the heavy processing requirements of Layer 3 IP based routers.

As a result, each group of stations connected to separate Segmented Ports forms different isolated Broadcast Domains. The Broadcast Sharing Ports should be used to connect servers and other common services, such as Internet access, that are used by all the stations connected to the different Segmented Ports.

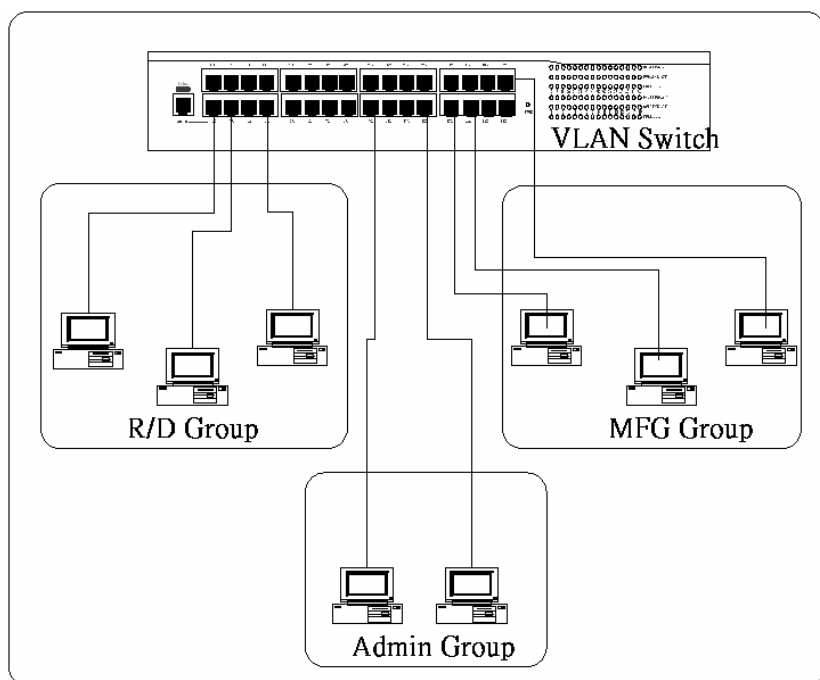
Virtual LAN, or VLAN, is generally defined as a broadcast domain. VLAN can be viewed as a group of end nodes, possibly on different physical network segments, which can communicate with each other.



Benefits of VLANs

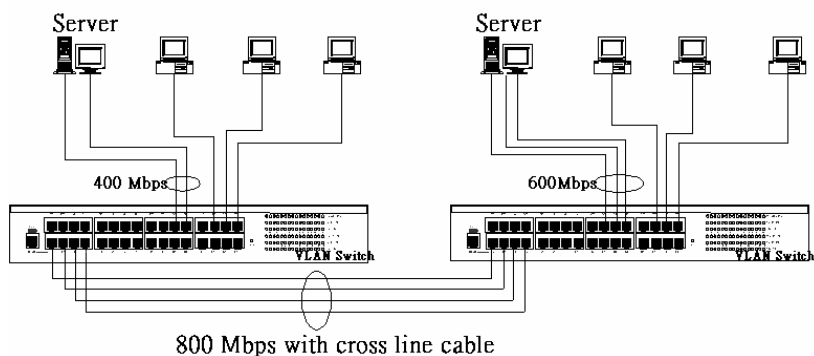
- ❑ Grouping users into logical networks for performance enhancement.
- ❑ Provides effective broadcast containment between Segmented Ports, which prevents flooding of a network.
- ❑ Offers security by isolating each Broadcast Domain on separate Segmented Ports.
- ❑ Preserving current investment in equipment and cabling.
- ❑ Providing an easy, flexible, economic way to modify logical groups when needed.
- ❑ Network administrators can easily "fine tune" the network.
- ❑ Keeping network structure from the physical topology of the cabling.
- ❑ Making large networks more manageable.

You can group users according to some shared characteristic, such as a common business function or a common protocol. A single switch may have several independent VLANs within it.



Link Trunking

Link trunking allows you to increase the available bandwidth between switches by grouping ports into a trunk. Trunking groups can be used to connect servers to switches for higher bandwidth. You can link Trunking groups to improve the throughput between network segments.



System Requirements

- ❑ IBM PC 80486 compatible or higher
- ❑ Windows 95 or Windows 98, Windows 98 SE and Windows 2000
- ❑ Configuration Cable

Installation

- ❑ Start Windows 95, Windows 98, Windows 98 SE or Windows 2000 and insert the Switch Configuration Utility diskette into drive A.
- ❑ Click **Start** on the **Taskbar** and select **Run**.

- From the **Run** dialog box, select (or type) A:\SETUP or B:\SETUP and click OK. Follow the on-screen instructions.

Main Function Descriptions

1. Port Based Security Option:

- A security violation occurs when a packet from an unknown MAC address is received.
- Enabled ports will not learn source MAC address. You must build explicit addresses for the corresponding port(s) for proper operation.
- When violations occur, the violating port discards the packets that caused the violation.

2. SuperMAC option:

- When this option is disabled, the switch will perform standard back-off algorithm when collisions occur.
- When enabled, the collision port will perform back-off on up to 3 slots, thus the switch can gain the network usage more easily.
- When the setting is enabled the DES-1032 has a higher priority. The result is that data will move more quickly.

3. Aging Control:

- When disabled, the switch will keep the learned source MAC address from each port.
- When enabled, user can change the aging time from 1 to 510 seconds for the learned MAC address.
- For the learned MAC address, when aging time is expired, that MAC address will be discarded.
- The aging control function is device wide.

4. Broadcast Storm Control:

- The DES-1032 supports Broadcast Storm Control to limit the number of consecutive broadcast packets for each port. The broadcast packets are stored in the buffer and sent to ports individually. The buffer discards excess packets when the number reaches the specified threshold. The threshold can be 16, 32, 48, or 64.
- Broadcast Storm Control must be enabled in order for the DES-1032 control Broadcast Storms.

5. Address Learning:

- When enabled, the source MAC address of the packet sent to this port will be learned.
- When disabled, the source MAC address of the packet sent to this port will not be learned.

6. Full Duplex Flow Control (802.3X):

- When enabled, the DES-1032 will perform full duplex flow control mechanism (802.3X) in full duplex transmission mode.
- When disabled, the DES-1032 will not perform full duplex flow control (802.3X) in full duplex transmission mode.

7. Auto-Negotiation:

- When enabled, the auto-negotiation capability for data rate and duplex mode will be performed.
- When disabled, the auto-negotiation capability is turned off. The user should specify the data rate (10M / 100M) and duplex mode (half / full-duplex) for proper operation.

8. Trunk Settings:

- The DES-1032 supports link aggregation/trunking. Trunking is a method to treat multiple physical links as a single logical link. The benefit of trunking is that trunked ports are able to group multiple lower speed links into one higher speed link. For example, four full-duplex 100Mbps links, such as Port 1 to Port 4, can be grouped as one single 800Mbps link as Trunk 1.
- For any port switch, users may specify 4 trunks. Each trunk may have two to four ports as its members. For example, Port 1 to Port 4, any two, three, or all four ports can be grouped as one trunk (TRUNK1). The same situation can be applied to the other ports. But remember that only Port 1 to Port 4, Port 5 to Port 8, Port 9 to Port 12, and Port 13 to Port 16 can be set as above. Port 4 and Port 5 CANNOT be grouped as one trunk.

- There are two load-balancing methods for trunking: MAC based and port based. For MAC based method, only 4-port trunk is allowed. The device will check the designated two bits of the source and destination MAC addresses of the incoming packet, and determine which trunk port the packet will be switched to. For port-based method, two, three, or four ports can be assigned to one trunk. The user can manually assign which trunk port to be linked to the non-trunk ports. Using this method, the user is responsible for balancing the traffic load among the trunk.

9. VLAN settings:

- VLAN (Virtual Local Area Network) basically is a broadcast domain. In a switched network system, a broadcast packet or an unknown destination MAC address packet will broadcast to ALL the other ports, which will decrease the whole network system performance dramatically. By grouping some ports into one VLAN, broadcast packets will only be sent to the ports within the same VLAN without affecting the traffic of other ports outside the VLAN.
- In the device, any two or more ports/trunks can be grouped as one VLAN, and ports/trunks can be shared among different VLANs.

10. Flood Control:

- Within a VLAN, the flood control function is provided to decide what to do with the incoming unicast packets with unknown destination MAC addresses.
- When enabled, packets received with unknown unicast addresses are forwarded to the out-link specified in the same VLAN. But if the source port (trunk) belongs several VLAN, the packet will be only forwarded to one of the out-links.

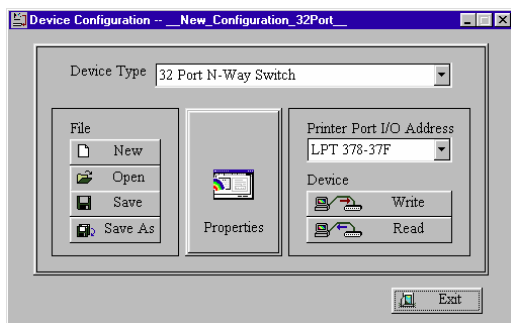
- When disabled, packets received with unknown unicast addresses are forwarded to all ports (except the receiving port) within the VLAN groups that the received port (trunk) belongs to.
- When flood control is enabled, each VLAN group must choose a member as its out-link. If some VLAN groups have overlapped members, user should choose one of these members as their out-link. Because if a port (trunk) belongs to more than one VLAN, packets it received with unknown DA will be only forwarded to one of the out-links of those VLAN groups it belongs to.

11. Explicit Address Table Entry:

- In general, the ports learn the source address through the received packets. The device also allows ports to have the source address assigned manually. Which is applicable in, e.g., security function. This is called explicit address table.
- There are totally 10 static addresses that can be assigned to Port 1 – 8, Port 9-16, Port 17 – 24, and Port 25 – 32 group, respectively.

Program Descriptions

Main Window



In the beginning, user should select the correct device type to start configuring. The program always keeps a current editing configuration during run time. It may save as a configuration file in disk. The file format is dedicated for this program. Its extension name is **s08** for 8 port switch, **s16**, **s24**, and **s32** for 16, 24, and 32 port switch respectively. The title of **Main Window** would show the name of the current configuration file name if it had ever been opened or saved, otherwise, display the name like “Device Configuration -- __New_Configuration_XXPort__”.

User may press **Properties** button to start to set the current configuration properties. A five page property-sheet window would popup for user to specify his/her preference in detail. Descriptions of these pages are given at next sections. When user has finished settings, the current configuration can be written into the device to achieve its reconfiguration. In the opposite direction, the configuration data inside the device can also be retrieved to the program for user to view and edit its properties.

- File | New

Reset to do a new configuration editing. According to the selected device type, all values will reset to its default, and the current name will become, for example, **__New_Configuration_16Port__** for *16 Port N-Way Switch*, **__New_Configuration_24Port_1FX_On_Borad__** for the device *24 Port Switch with 1-FX On Board*, ... etc.

□ File | Open

Open an existed device configuration file to configure.

□ File | Save

Save the current configuration to a switch configuration file.

□ File | Save As

Save as other file name.

□ Device Type

Choose the type of the device that user is ready to configure. There are twelve types to be selected. The first four types are common N-Way switches including *8 Port N-Way Switch*, *16 Port N-Way Switch*, *24 Port N-Way Switch*, and *32 Port N-Way Switch*. And others are switches with fiber interface, which including '*24 Port Switch, 1-FX On Board*', '*24 Port Switch, 2-FX On Board*', and 1-FX or 2-FX option module for 16/24/32 port switch, such as '*32 Port Switch, 2-FX Option Module*'.

□ Properties

Popup the multiple-page **Properties Window** to begin the configuration settings.

□ Printer Port I/O Address

User may choose *LPT 378-37F*, *LPT 278-27F*, or *LPT 3BC-3BF* to connect to the device. The value behind *LPT*, such as *378-37F*, means the I/O addresses of the printer port that host PC specified. This program will transmit configuration data to the device through the specified I/O ports.

□ Device | Write

Write the currently configuration data into the device. If write successfully, the device will auto-reset and be initialized by this new configuration.

If write failed, first, please check whether the Configuration Cable is well connected, then check the host PC whether the drivers for the Printer Port (LPT) are installed correctly, or whether the selection of **Printer Port I/O Address** meets host's setting.

Note: The Configuration Cable should be connected to the PC's printer port directly. If there is any device, such as key-pro or printer buffer, attached on the printer port, please remove it before connecting the Configuration Cable.

□ Device | Read

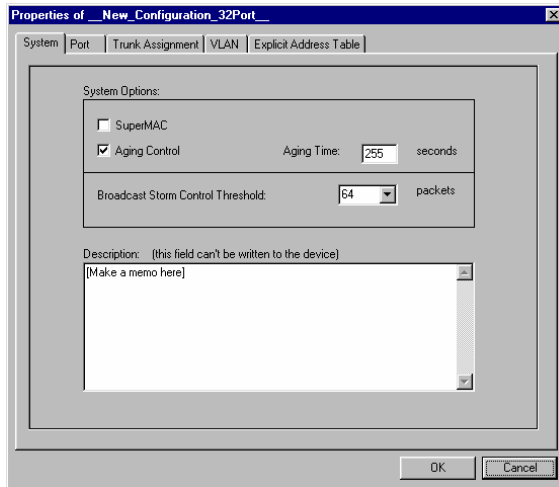
Read the configuration data from the device. If read successfully, the current configuration name will become __Inside_Device_Configuration__.

Note: If the configuration data inside the device was written by earlier versions of the program, it can't be read back as current configuration.

□ Exit

Leave this program.

Properties Window | System Page



User sets the system-wise configuration in this page. Options selected here will affect the overall system operation if user modify or choose the parameters. The default selection of each option is typed as underlined.

❑ SuperMAC

Enable -- When collision occurs, the device will use a more aggressive back off algorithm (back off up to 3 slots).

Disable -- When collision occurs, the device will perform the IEEE802.3 standard exponential back off algorithm.

❑ Aging Control

Enable -- The table aging process will be running to age all dynamically learned table entries.

Disable -- The table aging process will be stopped.

Only the dynamically learned address will be aged. All explicit (static) entry will not be aged out.

□ Aging Time

The address-aging timer is built in the table aging process. The minimum time is 1 second and the maximum is 510 seconds, and it must be an even number if it is larger than 256. The default value is 255 seconds.

□ Broadcast Storm Control Threshold

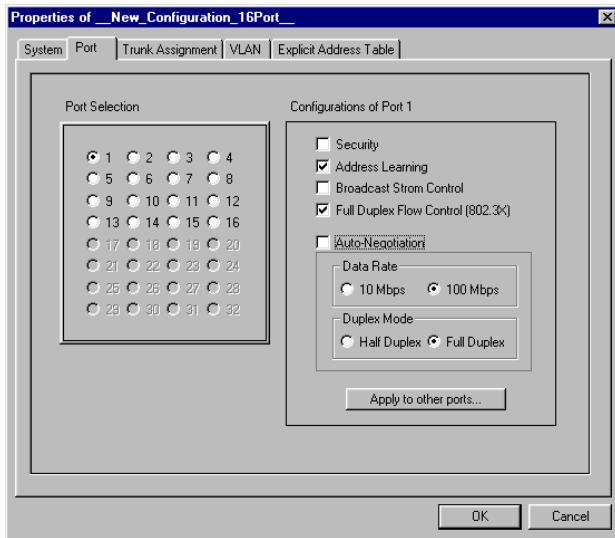
This sets the threshold of number of consecutive broadcast packets allowed from the input buffer of the port that has enabled the option **Broadcast Storm Control**. This value could be 16, 32, 48 or 64 packets. The default selection is 64 packets.

□ Description

User can make a memo here. At most 2048 characters can be written in this edit box.

Note: The description can only be saved to and read from the disk file. It can't be saved to the device.

Properties Window | Port Page



User may set each port-based configuration in this page. Just choose a port number from the left radios and set its properties on right options. Instead of configuring one by one port, the dialog **Apply to Other Ports** can be used to accelerate these settings. The default selection of each option is typed as underlined.

- Port Selection

Select a port to set its configuration.

- Security

Enable -- The packet which results in security violation at this port will be discarded.

Disable -- The forwarding decision made about packets received from the port will not involve the source MAC address checking.

The device is able to provide the security for the intrusion protection. If enabled, any packet results in security violation at this port will be discarded. The security violation would happen only if a packet received from this port with unknown source MAC address or with source MAC address learned previously from another port. After user enables this option, the device will disable address learning and disable aging process of this port. User should explicitly add to the address table the MAC address of the workstation connected to this port.

□ Address Learning

Enable -- The source MAC address of the packet from this port will be learned.

Disable -- The source MAC address of the packet from this port will not be learned.

□ Broadcast Storm Control

Enable -- If the accumulated consecutive broadcast packets in the input buffer of a port is over the threshold specified by the value of **Broadcast Storm Control Threshold** on the **System Page**, new incoming broadcast packets will be discarded until the number has been reduced below the threshold.

Disable -- The broadcast packet will not be throttled.

□ Full Duplex Flow Control (802.3X)

Enable -- Enable full duplex flow control by method 802.3X.

Disable -- Do not support flow control for full duplex mode.

□ Auto-Negotiation

Enable -- Turn on the auto-negotiation capability for data rate and duplex mode.

Disable -- Turn off the auto-negotiation capability. Without auto-negotiation, user should specify the data rate and duplex mode.

Note: If this port is with fiber (FX) interface, this option is fixed disabled.

□ Data Rate

User may specify 10 or 100 Mbps data transmission rate for this port.

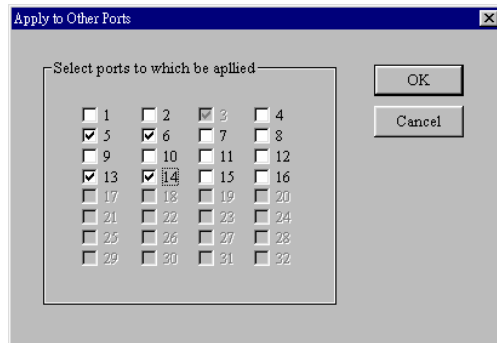
Note: If this port is with fiber (FX) interface, the data rate is fixed 100 Mbps.

□ Duplex Mode

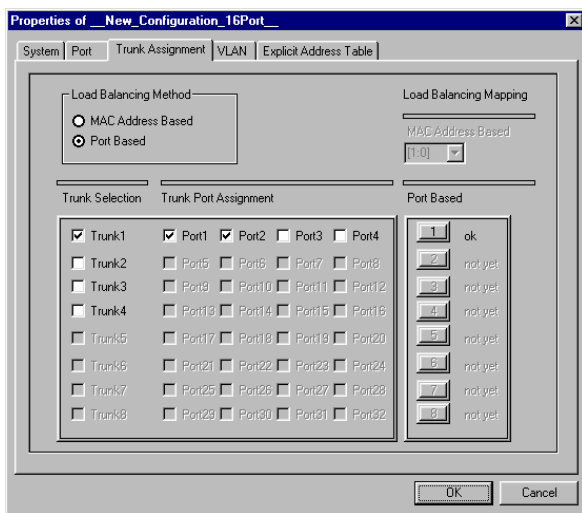
User may specify full duplex or half duplex mode of this port.

□ Apply to other Ports

The dialog **Apply to Other Ports** below will popup after the button being pressed. User may use this dialog to automatically apply the current port's configurations to another ports selected here.



Properties Window | Trunk Assignment Page



The device supports link aggregation/trunking. Trunking is basically a method to bundle multiple physical links as a single logical link. The benefit is to be able to group multiple lower speed links into one higher speed link for bandwidth aggregation. For example, four full duplex 100Mbps links, such as Port 1 to Port 4, can be grouped as one single 800Mbps link for

Trunk 1. As the need of higher bandwidth, trunking is usually used between switch and server, or two switches.

For n port switch, user may at most specify $n/4$ trunks at most. Each trunk may have two to four ports as its members. User may just click checkboxes **Trunk Selection** and **Trunk Port Assignment** to decide the link aggregation of the system. The port has been assigned to a trunk is called trunk port, otherwise individual port.

□ Load Balancing Method

In a multiple link trunk, the links within a trunk should have equal amount of traffic in order to achieve maximum efficiency. Therefore, some sort of load balancing among the links of trunk has to be deployed. The device supports **MAC address-based and port-based**, two alternative load balancing methods. By such method, any packet with trunk destination received by the switch can be forwarded to a proper trunk port. After choosing one method, user has to specify the relative load-balancing mapping to complete the configuration of the trunk port load balancing.

□ Trunk Selection, Trunk Port Assignment

User may just click checkboxes of **Trunk Selection** and **Trunk Port Assignment** to decide the link aggregation of the system. For MAC address based load-balancing mode, each trunk must consist of four trunk ports. But the port-based load-balancing trunk may consist of two, three, or four trunk ports.

□ Load Balancing Mapping – MAC Address Based

When the switch receives a packet with a trunk destination, it will automatically forward the packet to a trunk port based on the source MAC address (SA) and destination MAC address (DA) of the packet. The device uses two bits from SA and DA to map to four trunk ports. User may choose which two bits used for mapping:

- [1:0] -- Choose bit 1 and 0 for mapping.
- [3:2] -- Choose bit 3 and 2 for mapping.
- [5:4] -- Choose bit 5 and 4 for mapping.
- [7:6] -- Choose bit 7 and 6 for mapping.

The mapping rule is described as below:

1. *Exclusive Or (XOR)* the designated two bits of SA and DA respectively.
2. Four combinations of the result are mapped to four trunk ports, where the left value is for SA and the right for DA:

- [Odd, Odd] -- trunk port 1
- [Odd, Even] -- trunk port 2
- [Even, Odd] -- trunk port 3
- [Even, Even] -- trunk port 4

For example, if user specifies bit 1 and 0 for mapping and trunk 2 is assigned, any packet ready to be forwarded to trunk 2 will be transmitted as following:

- a) If a packet's SA is 00:C0:A7:98:FE:81 and DA is 00:C0:A7:98:FE:9B, it will be forwarded to port 6 (trunk port 2). Because for SA it is "0 XOR 1 = Odd", and for DA it is "1 XOR 1 = Even".
- b) If a packet's SA is 00:C0:A7:98:FE:80 and DA is 00:C0:A7:98:FE:9A, it will be forwarded to port 7 (trunk port 3). Because for SA it is "0 XOR 0 = Even", and for DA it is "1 XOR 0 = Odd".

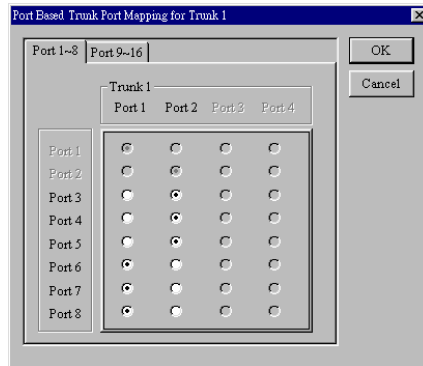
Note: some device's trunk port mapping is different. The following is its mapping rule, where TPx is for Trunk Port x.

<i>SA \ DA</i>	<i>00</i>	<i>01</i>	<i>10</i>	<i>11</i>
<i>00</i>	<i>TP4</i>	<i>TP3</i>	<i>TP2</i>	<i>TP1</i>
<i>01</i>	<i>TP3</i>	<i>TP4</i>	<i>TP1</i>	<i>TP2</i>
<i>10</i>	<i>TP2</i>	<i>TP1</i>	<i>TP4</i>	<i>TP3</i>
<i>11</i>	<i>TP1</i>	<i>TP2</i>	<i>TP3</i>	<i>TP4</i>

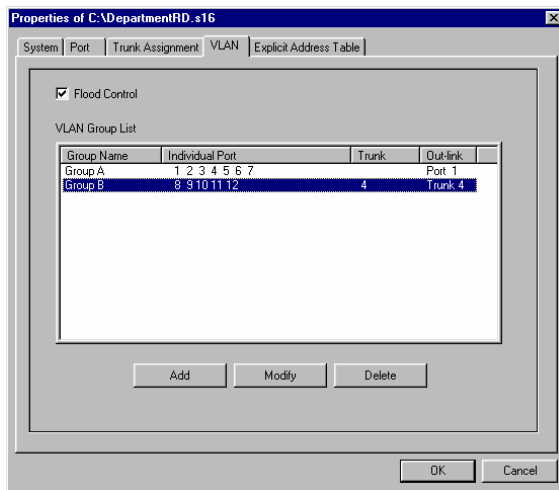
□ Load Balancing Mapping – Port Based

The port-based load balancing method is an explicit port assignment scheme. It requires each other port to be assigned to a specific link (trunk port) in the trunk. When the switch receives a packet with a trunk destination, it will automatically forward the packet to a trunk port based on the port it came from.

After selecting a trunk, user should click its **Port Based** button under **Load Balancing Mapping** to invoke the dialog **Port Based Trunk Port Mapping for Trunk x** as below to do port based load-balancing mapping. Like the selections in this dialog to do trunk port mapping for trunk1, port3 to port5 are mapped to trunk port2, and port6 to port8 are mapped to trunk port1. User may just click radios to decide the mapping from all other ports to one of the trunk ports. User must assign all mappings then to leave the dialog. After that, the status will become **ok** on the right side of the button **Port Based**. Otherwise, the status **not yet** means the load-balancing mapping has not been completed.



Properties Window | VLAN Page



This page allows user to define VLAN membership by groups of device's ports. Any individual port or trunk can be a member of a VLAN group. A VLAN group is basically a broadcast domain, but any port/trunk is not limited to belong to only one VLAN group. The forwarding rule is that packets from the source port/trunk will be only forwarded to destination port/trunk within the same VLAN group. That is, a broadcast/multicast

packet will be forwarded to all ports/trunks within the same VLAN group(s) of the source port/trunk except the source port/trunk itself. An unicast packet will be forwarded to the destination port/trunk only if the destination port/trunk is in the same VLAN group as the source port/trunk.

□ Flood Control

Enable -- Packets received with unknown unicast DA will be forwarded to the specified out-link in the same VLAN group. But if the source port (trunk) does not only belong to one VLAN group, then the packet will be only forwarded to one of the out-links.

Disable -- Packets received with unknown unicast DA will be forwarded to all ports (except the receiving port) within the same VLAN groups that the received port (trunk) belongs to.

The flood control is available only when at least one VLAN group is assigned. And the out-link port **must** be assigned when flood control is enabled for proper operation.

When the flood control is enabled, each VLAN group must choose a member as its out-link. If some VLAN groups have overlapped members, user should choose one of these members as their out-link. Because, if a port (or trunk) does not only belong to one VLAN group, packets that it receives with unknown DA will be only forwarded to one of the out-links of those VLAN groups that it belongs to.

Note: The out-link described here is definitely not the same as the Uplink on the front panel of the switch.

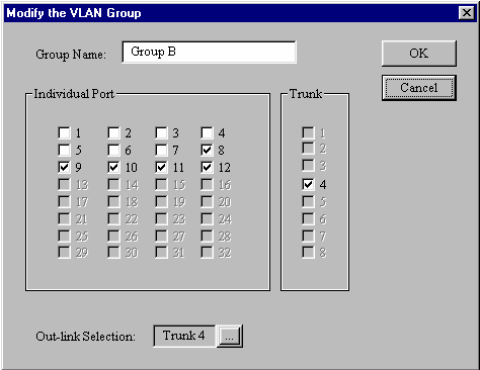
□ VLAN Group

The list box shows all defined VLAN groups of the system, and each row is a group. Any individual port or trunk can be a member of a VLAN group, and each group comprises at least two members. One of the members is to be chosen as its out-link. But if the flood control is disabled, the column of **Out-link** will not show up.

User may press **Delete** button to remove the current highlighted group, or press **Add** button to add a new group. User may also press **Modify** button or double click the current highlighted group to modify its content. While adding or modifying a VLAN group, the dialog **Modify the VLAN Group** (or **Add a New VLAN Group**) as below will popup for user to specify its content.

The group count is not limited. User may specify n VLAN groups or even more groups for any n port switch. But note that after writing to the device, only the information of the first $n/2$ added VLAN groups can be read back from the device of n port switch.

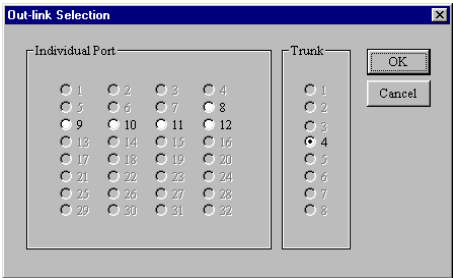
Note: Once at least one VLAN group has been added, the system will automatically gather all un-selected members as an implicit VLAN group. Users are recommended to explicitly assign all groups they need, although they know that there exists an implicit VLAN group.



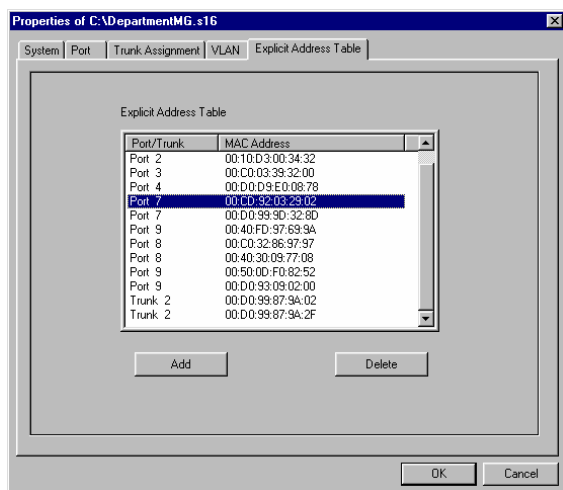
Group Name -- User may give a name, at most 8 characters, to the group.

Individual Port / Trunk -- Both individual port and trunk can be the member of a VLAN group. All light checkboxes are qualified members of VLAN. User must select at least two members to consist of a VLAN group.

Out-link Selection -- If the flood control is enabled, user should click the button to choose one port or trunk as the out-link of this VLAN group. When clicking the button, the dialog **Out-link Selection** as below would popup for user to choose the out-link.



Properties Window | Explicit Address Table Page



The address table of the switch is set up through automatic address learning (dynamic) or manual entry (static). This page is for user to explicitly give static entries to the address table in the device. All static address entries will not be aged or updated by the switch's address learning.

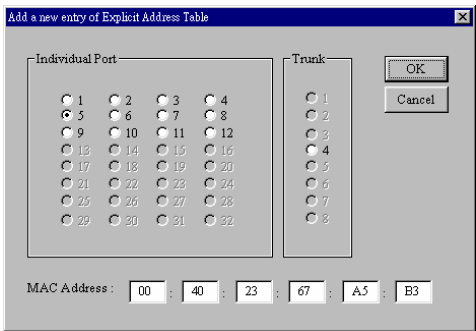
□ Explicit Address Table

The list box shows all explicit (static) entries for the address table. Each row is an entry for a MAC address to an individual port or a trunk. There are totally 10 static addresses that can be assigned to Port 1 – 8, Port 9-16, Port 17 – 24, and Port 25 – 32 group, respectively.

User may press **Delete** button to remove the current highlighted entry, or press **Add** button to add a new entry. While adding an entry, the dialog **Add**

a new entry of **Explicit Address Table** as below will popup for user to specify its content.

Note: Normally, the device has static entry capacity of 10 per each group. Each group is consisted of consecutive 8 ports and 2 trunks, that is, Port 1-8 and Trunk 1-2 belong to a group, Port 9-16 and Trunk 3-4 belong to another group, ...etc. But if a static address is assigned for Trunk3-8, it will occupy an entry for all groups not only the group it belongs to. That is, if there is any static address assigned for Trunk 3-8, it will reduce the entry capacity of each group. Anyway, the dialog **Add a new entry of Explicit Address Table** will gray those ports and trunks when there is no capacity to give a static entry for them.



In this dialog, just give the MAC address of a workstation, and choose an individual port or a trunk to which the workstation is connected.

Default Configuration

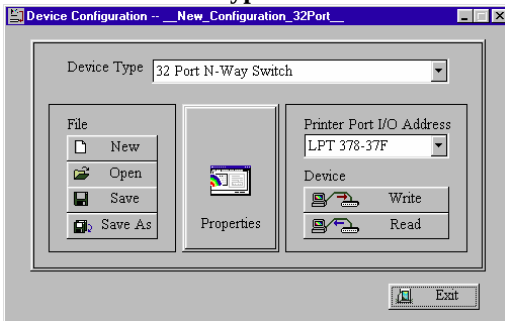
The following table shows the default configuration:

Page	Options	Default Settings
System	SuperMAC	<i>Disabled</i>
	Aging Control	<i>Enabled</i>
	Aging Time	<i>255 seconds</i>
	Broadcast Storm Control Threshold	<i>64 packets</i>
Port	Security	<i>Disabled</i>
	Address Learning	<i>Enabled</i>
	Broadcast Storm Control	<i>Disabled</i>
	Full-Duplex Flow Control	<i>Enabled</i>
	Auto-Negotiation	<i>Enabled,</i>
* Port (FX Interface)	Auto-Negotiation	<i>Disabled</i>
	Data Rate	<i>100 Mbps</i>
	Duplex Mode	<i>Full Duplex</i>
Trunk Assignment	Load Balancing Method	<i>Port Based</i>
	Trunk Selection	<i>None</i>
VLAN	Flood Control	<i>Disabled</i>
	VLAN Group List	<i>None</i>
Explicit Address Table	Explicit Address Table	<i>None</i>

Typical Steps to Use Switch Configuration Utility

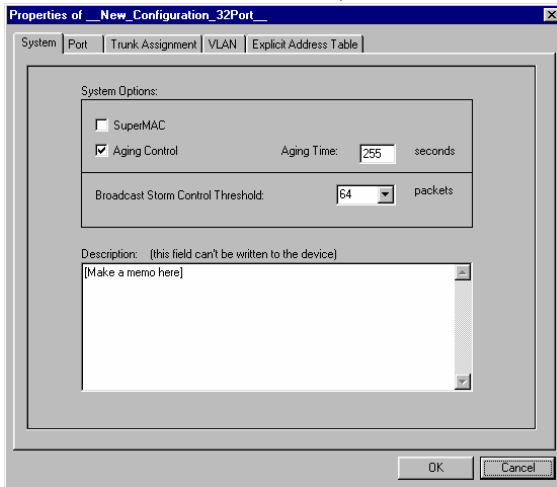
To Edit a Configuration File

1. From the **Start** menu, choose the **Programs** submenu and the **Switch Configuration** submenu, then click the **Switch Configuration** item within it.
2. In the main window, choose the correct device type of switch in the combo box **Device Type**.

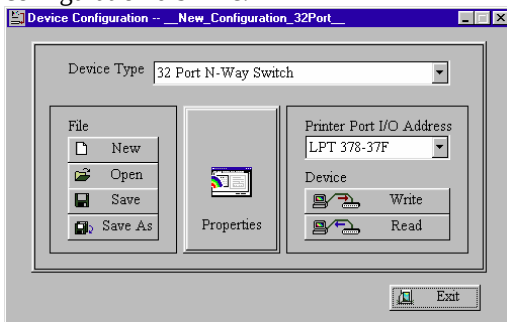


3. Click the button **Open** to open an existed configuration file, if necessary.
4. Click the button **Properties** to invoke the **Properties Window** to start or modify configuration settings.

5. Click **OK** to leave this window, if finished these settings.

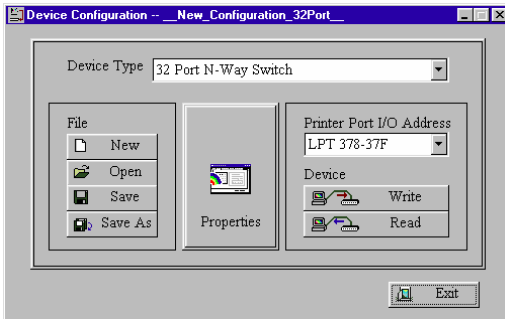


6. Click the button **Save** or **Save As** to save current settings as a configuration disk file.



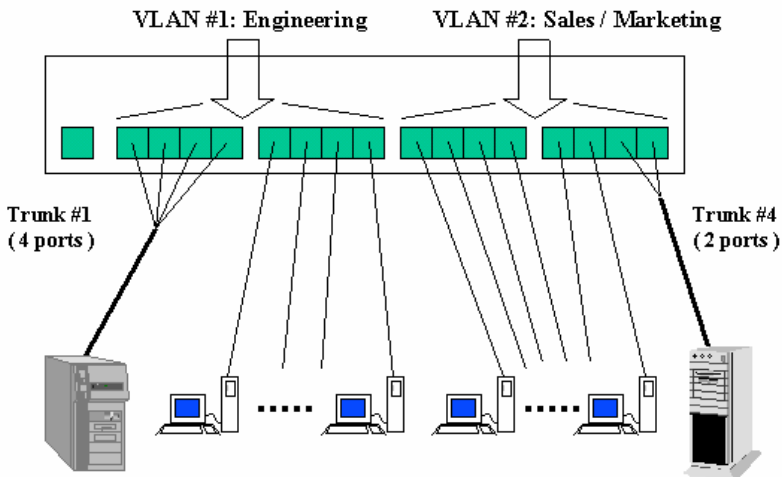
To Transmit Current Configuration to the Switch

1. Connect the Configuration Cable directly to the printer port of host PC and the switch.
2. Power on the switch.
3. From the **Start** menu, choose the **Programs** submenu and the **Switch Configuration** submenu, then click the **Switch Configuration** item within it.
4. In the main window, choose the correct device type of switch in the combo box **Device Type**.



5. Choose the correct printer port in the combo box **Printer Port I/O Address**. You had better make sure whether the drivers for Printer Port (LPT) are installed correctly in the host system.
6. Click the button **Open** to open an existed configuration file if necessary.
7. Click the button **Write** to start to write current configuration data to the switch via the cable.
8. If successful to write data, the switch will be auto reset immediately and initialized by the current configuration.

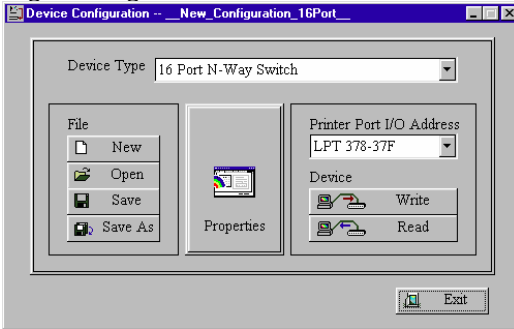
To Assign Trunks and Set VLAN Groups



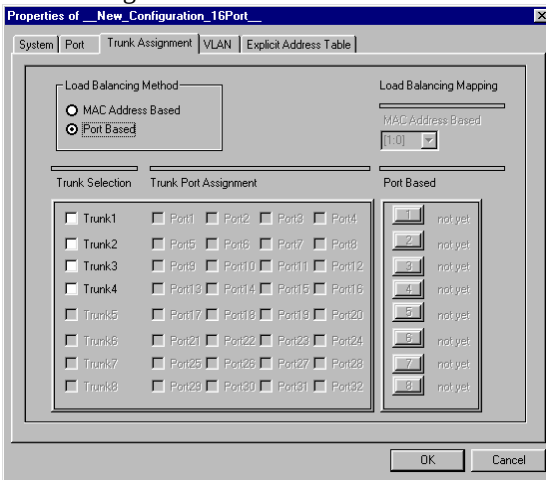
Here we give an example to show how to assign trunks and set VLAN groups. From the figure above, user plans to configure a 16 port switch into two VLAN groups, one for Engineering and the other for Sales/Marketing. There are four stations connected to Port 5 to Port 8 respectively used by engineers, and a server shared by them which is connected to Trunk 1 by using four trunk ports. On the other side, there are six stations connected to Port 9 to Port 14 respectively used by Sales/Marketing department, and a server shared by them which is connected to Trunk 4 by using two trunk ports.

To achieve the goal above, just follow steps below:

1. Press the button **Properties** to invoke **Properties Window** and begin settings.

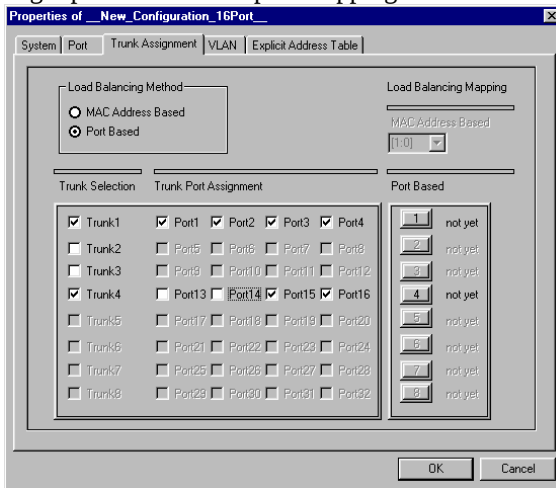


2. Select the page **Trunk Assignment** in the **Properties Window** to start to assign trunks.

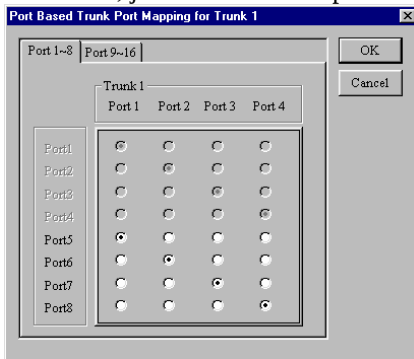


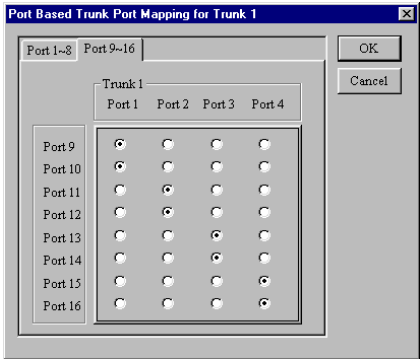
3. Click checkboxes to select Trunk 1 and Trunk 4, and assign their trunk ports. Then click the relative **Port Based** buttons **1** and **4** to

begin port-based trunk port mapping.

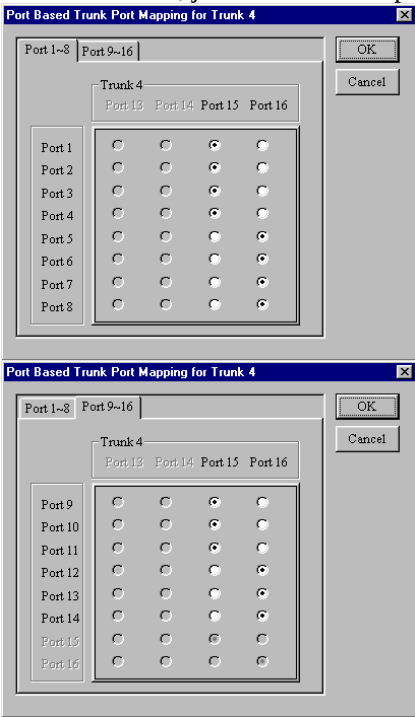


- Click radio boxes to give trunk port mapping for Trunk 1. For Port 5 to Port 8, just make them map to different trunk ports.

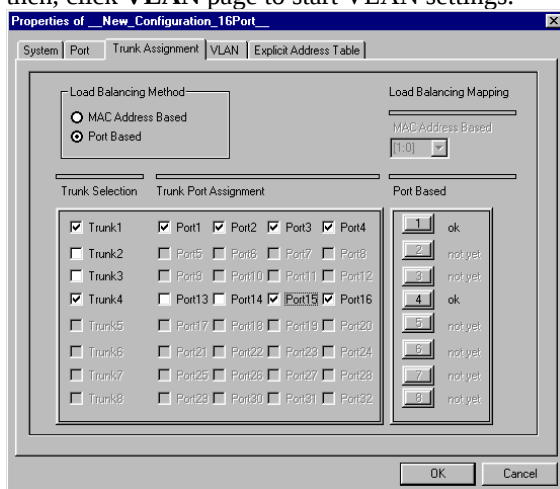




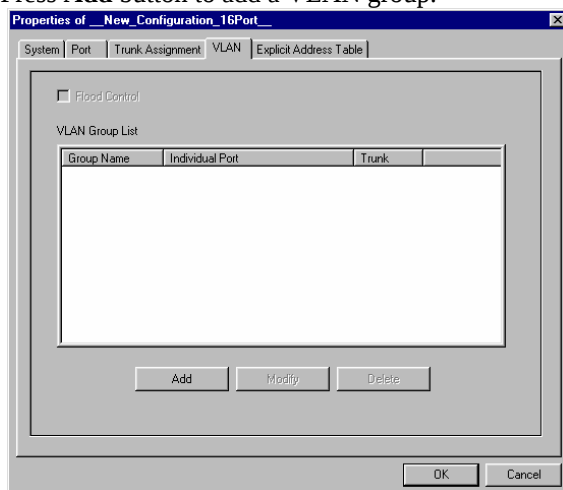
5. Click radio boxes to give trunk port mapping for Trunk 4. from Port 9 to Port 14, just make them map to both trunk ports evenly.



6. After finishing trunk port mapping, it shows **ok** besides the relative **Port Based** buttons. Now, all trunk assignments are finished. And then, click **VLAN** page to start VLAN settings.



7. Press **Add** button to add a VLAN group.



8. Give the name 'Engineer' in the edit box and select Trunk 1 and Port 5 to Port 8 to be members of this group.

Add a new VLAN Group

Group Name:

Individual Port

☐ 1	☐ 2	☐ 3	☐ 4
☒ 5	☒ 6	☒ 7	☒ 8
☐ 9	☐ 10	☐ 11	☐ 12
☐ 13	☐ 14	☐ 15	☐ 16
☐ 17	☐ 18	☐ 19	☐ 20
☐ 21	☐ 22	☐ 23	☐ 24
☐ 25	☐ 26	☐ 27	☐ 28
☐ 29	☐ 30	☐ 31	☐ 32

Trunk

☒ 1
☐ 2
☐ 3
☐ 4
☐ 5
☐ 6
☐ 7
☐ 8

Out-link Selection:

9. Press **Add** button to add another VLAN group.

Properties of _New_Configuration_16Port_

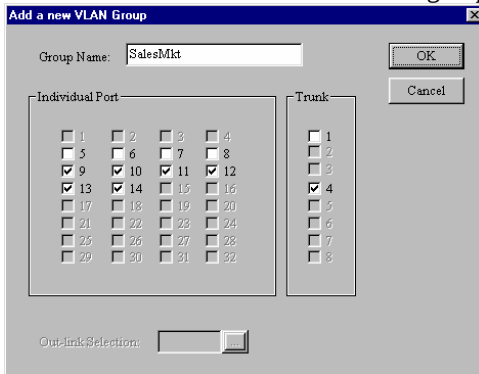
System | Port | Trunk Assignment | **VLAN** | Explicit Address Table

☐ Flood Control

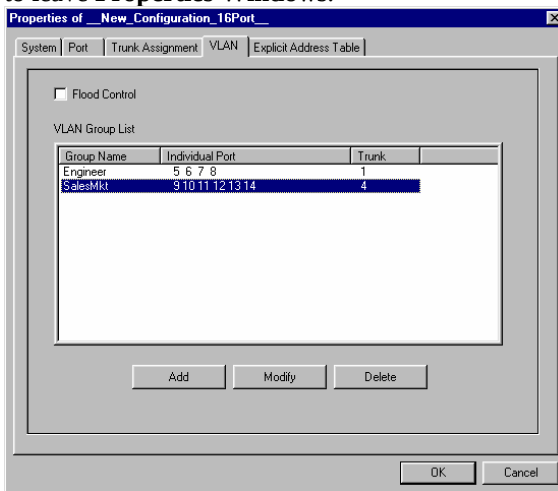
VLAN Group List

Group Name	Individual Port	Trunk
Engineer	5 6 7 8	1

10. Give the name 'SalesMkt' in the edit box and select Trunk 4, click Port 9 to Port 14 to be members of this group.

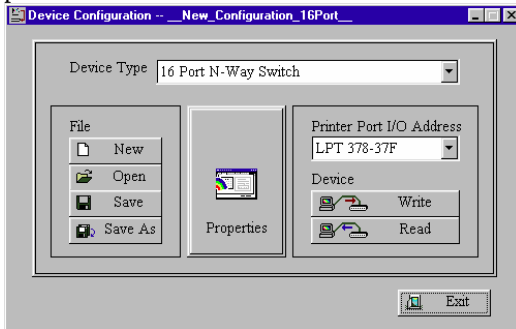


11. Till now, two VLAN group settings are completed. Just click **OK** to leave **Properties Windows**.



12. User may press **Save** button to save current configuration as a file, and press **Write** button to download it into device to realize this

plan.



Troubleshooting

□ Problem 1:

If failed to write data to the switch or read from?

□ Solution 1:

1. Make sure the switch is powered on.
2. Make sure the Configuration Cable is well connected. It should be connected to the PC's printer port directly. If there is any device, such as key-pro or printer buffer, attached on the printer port, please remove it before connecting the Configuration Cable.
3. Examine host PC whether the drivers for Printer Port (LPT) are installed correctly. Open the **System** item in **Control Panel**, and select **Device Manager** tag. Check out whether the item **Printer Port** exists under submenu **Ports (Com & LPT)**. If it does not exist, the drivers for LPT have to be installed. If it

exists, check out its properties. Select the **Resource** tag and make sure whether its **Input/Output Range** is **0378-037F**, **0278-027F**, or **03BC-03BF**

4. Examine the **Parallel Port Mode** in the host PC's BIOS settings, if it is **SPP**, please change it into **EPP** or **ECP** mode.
5. Make sure the selection of the combo box **Printer Port I/O Address** in the main window meets Printer Port Input/Output Range setting.
6. Make sure the selection of the combo box **Device Type** in the main window is correct.