Virtual Local Area Network

(802.1Q Tag-based VLAN)

Ethernet Switch

ZyNOS 4.0

Support Notes

Version 4.00

Nov 2011

Separating a physical network into many virtual networks

What is Virtual LAN?

VLAN Overview

A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Stations on a logical network belong
to one group called VLAN Group. A station can belong to more than one group. The stations in the same VLAN group can communicate with each other. With VLAN, a station cannot directly talk to or hear from stations that are not in the same VLAN group(s); the traffic must first go through a router.

In MTU or IP-DSLAM applications, VLAN is vital for providing isolation and security among the subscribers. When properly configured, VLAN prevents one subscriber from accessing the network resources of another one on the
same LAN. Therefore, a user will not see the printers and hard disks of another user in the same building.

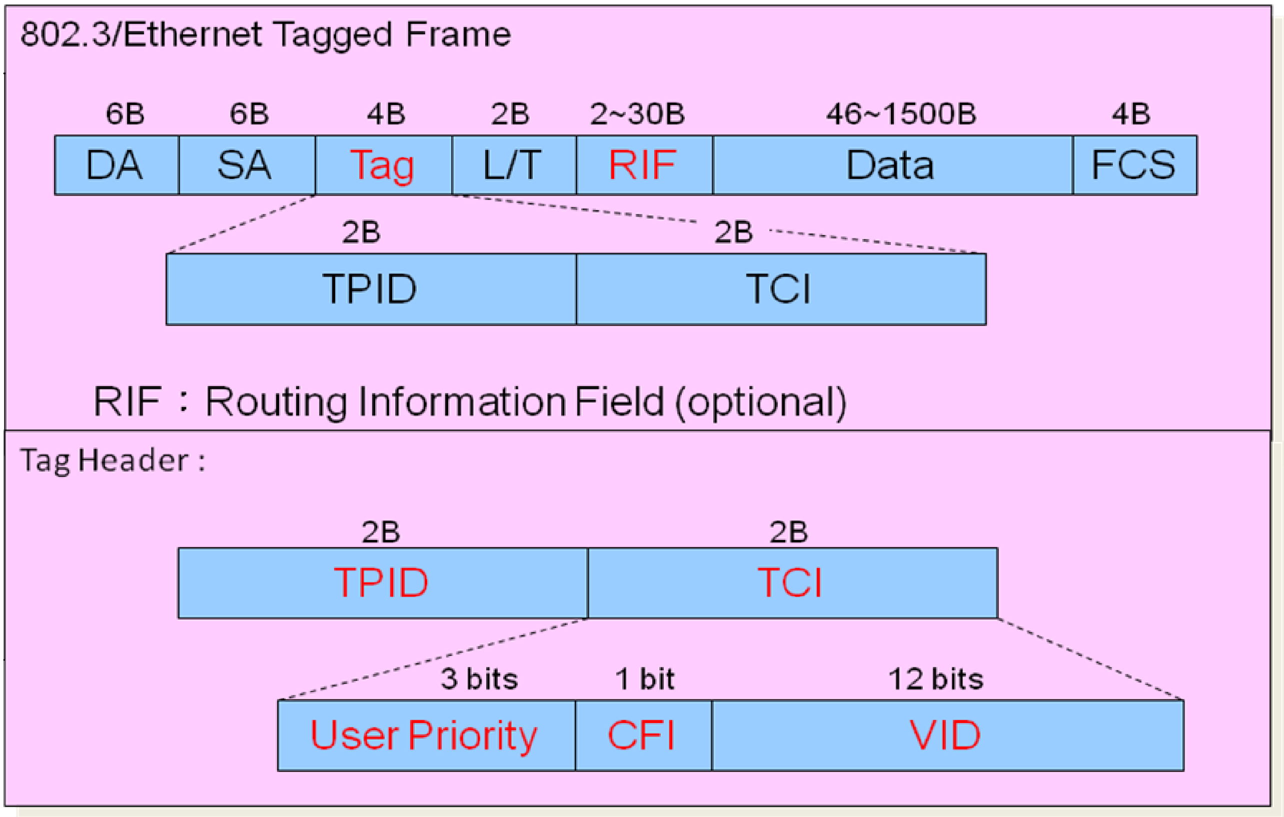
VLAN also increases network performance by limiting broadcasts to a smaller and more manageable logical broadcast domain. A VLAN group is a broadcast domain. In traditional Layer-2 switched environments, all broadcast packets go to each and every individual port. With VLAN, all broadcasts are confined to a specific broadcast domain.

There are two most popular VLAN implementations, Port-based VLAN and IEEE 802.1q Tagged VLAN. ZyXEL Managed Switch supports both VLAN implementations. The biggest difference between both VLAN implementations
is that Tagged VLAN can across Layer-2 switch but Port-based VLAN cannot.

What is IEEE 802.1Q Tag-based VLAN?

Tag-based VLAN Overview

Regarding the IEEE 802.1Q standard, Tag-based VLAN uses an extra tag in the MAC header to identify the VLAN membership of a frame going across the bridges. This tag is used for VLAN and QoS (Quality of Service) priority identification. The VLANs can be created statically by hand or dynamically through GVRP. The **VLAN ID** associates a frame with a specific VLAN and provides the information that switches need to process the frame across the network. A tagged frame is four bytes longer than an untagged frame and contains two bytes of TPID (Tag Protocol Identifier, residing within the type/length field of the Ethernet frame) and two bytes of TCI (Tag Control Information, starting behind the source address field of the Ethernet frame).



TPID: TPID has a defined value of 8100 in hex. When a frame has the EtherType equal to 8100, this frame carries the tag IEEE 802.1Q / 802.1P.
Priority: The first three bits of the TCI define user priority, giving eight (2^3) priority levels. IEEE 802.1P defines the operation for these 3 user priority bits.
CFI: Canonical Format Indicator is a single-bit flag, always set to zero for Ethernet switches. CFI is used for the reason of compatibility between Ethernet type network and Token Ring type network. If a frame received at

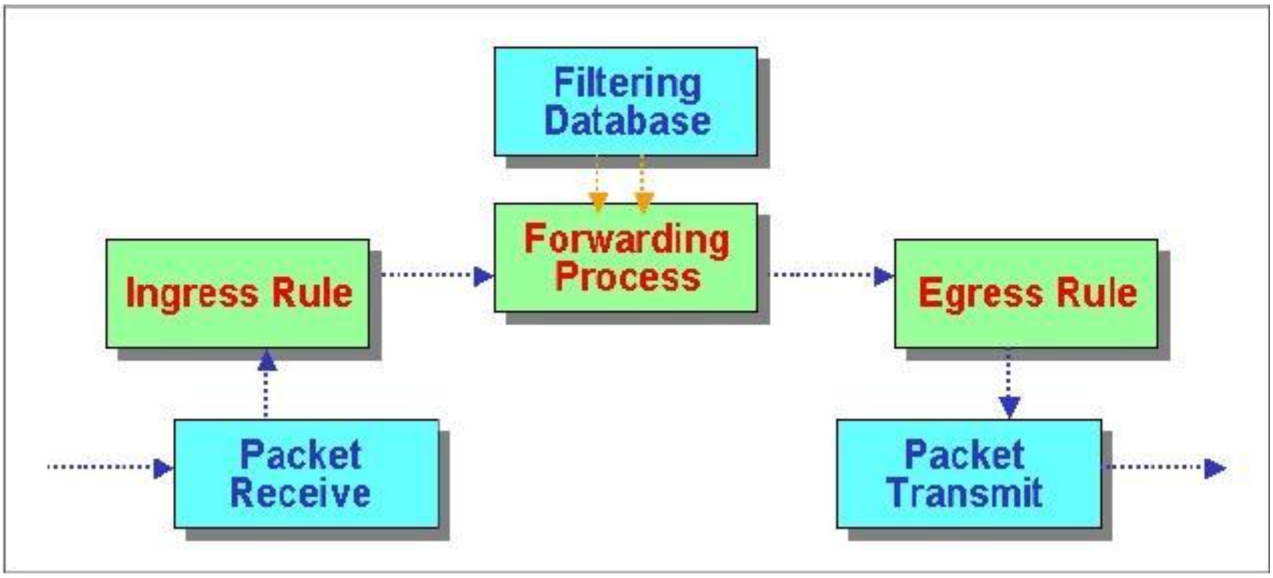
an Ethernet port has a CFI set to 1, then that frame should not be forwarded to an untagged port.

VID: VLAN ID is the identification of the VLAN, which is basically used by the 802.1Q standard. It has 12 bits and allows the identification of 4096 (2^12) VLANs. Of the 4096 possible VIDs, a VID of 0 is used to identify priority frames and value 4095 (FFF) is reserved, so the maximum possible VLAN configurations are 4,094.

Note that user priority and VLAN ID are independent of each other. A frame with VID (VLAN Identifier) of null (0) is called a priority frame, meaning that only the priority level is significant and the default VID of the ingress port is
given as the VID of the frame.

How 802.1Q VLAN works

According to the VID information in the tag, the switch forwards and filters the frames among ports. The ports with the same VID can communicate with each other. IEEE 802.1Q VLAN function contains the following three tasks, Ingress
Process, Forwarding Process and Egress Process.



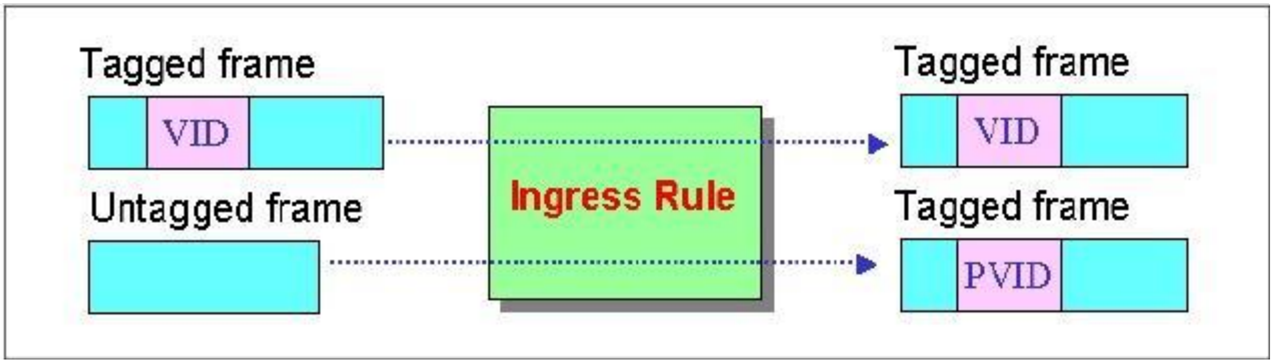
I. Ingress Process:

Each port is capable of passing tagged or untagged frames. Ingress Process identifies if the incoming frames contain tag and classifies the incoming frames belonging to a VLAN. Each port has its own Ingress rule. If Ingress rule accepts tagged frames only, the switch port will drop all incoming non-tagged frames. If Ingress rule accept all frame types, the switch port simultaneously allows the

incoming tagged and untagged frames:

When a tagged frame is received on a port, it carries a tag header that has explicit VID. Ingress Process directly passes the tagged frame to Forwarding Process.

An untagged frame doesn't carry any VID stating to which VLAN it belongs. When an untagged frame is received, Ingress Process inserts a tag containing the PVID into the untagged frame. Each physical port has a default VID called PVID (Port VID). PVID is assigned to untagged frames or priority tagged frames (frames with null (0) VID) received on this port.



After Ingress Process, all frames have 4-bytes tag and VID information, and then go to Forwarding Process.

II. Forwarding Process:

The Forwarding Process decides how to forward the received frames according to the Filtering Database. If you want to allow the tagged frames to be forwarded to certain port, this port must be the egress port of this VID. The egress port is an outgoing port for the specified VLAN, that is, frames with specified VID tag can go through this port. The Filtering Database stores and

organizes VLAN registration information useful for switching frames to and from the switch ports. It consists of static registration entries (Static VLAN or SVLAN table) and dynamic registration entries (Dynamic VLAN or DVLAN table). SVLAN table is manually added and maintained by the administrator. DVLAN table is automatically learned via GVRP protocol, and can't be neither created nor upgraded by the administrator.

The VLAN entries in Filtering Database contain the following information:

1. **VID:** VLAN ID
2. **Port:** The switch port number
3. **Ad Control:** Registration administration control. There are 3 types of ad control, including **forbidden** registration, **fixed** registration and **normal** registration.

    Forbidden registration: This port is forbidden to be the egress port of the specified VID.
    Fixed registration: When ad control is set to fixed registration, it means this is a static registration entry. This port is the egress port of the specified VID (a member port of the specified VLAN). The frames with specified VID tag can go through this port.
    Normal registration: When ad control is set to normal registration, it means this is a dynamic registration entry. The forwarding decision depends on Dynamic VLAN table.

4. **Egress tag Control:** This information is used for Egress Process. The value can be either tagged or untagged. If the value is tagged, the outgoing frame in the egress port is tagged. If the value is untagged, the
    tag will be removed before frame leaves the egress port.

VID	Port	Ad Control	Tag Control
10	1	Forbidden	Tag
10	2	Fixed	Tag
10	3	Normal	UnTag
20	1	Fixed	Tag
20	5	Fixed	UnTag

Filtering Database

VID	Egress Port
10	1
10	2
20	3

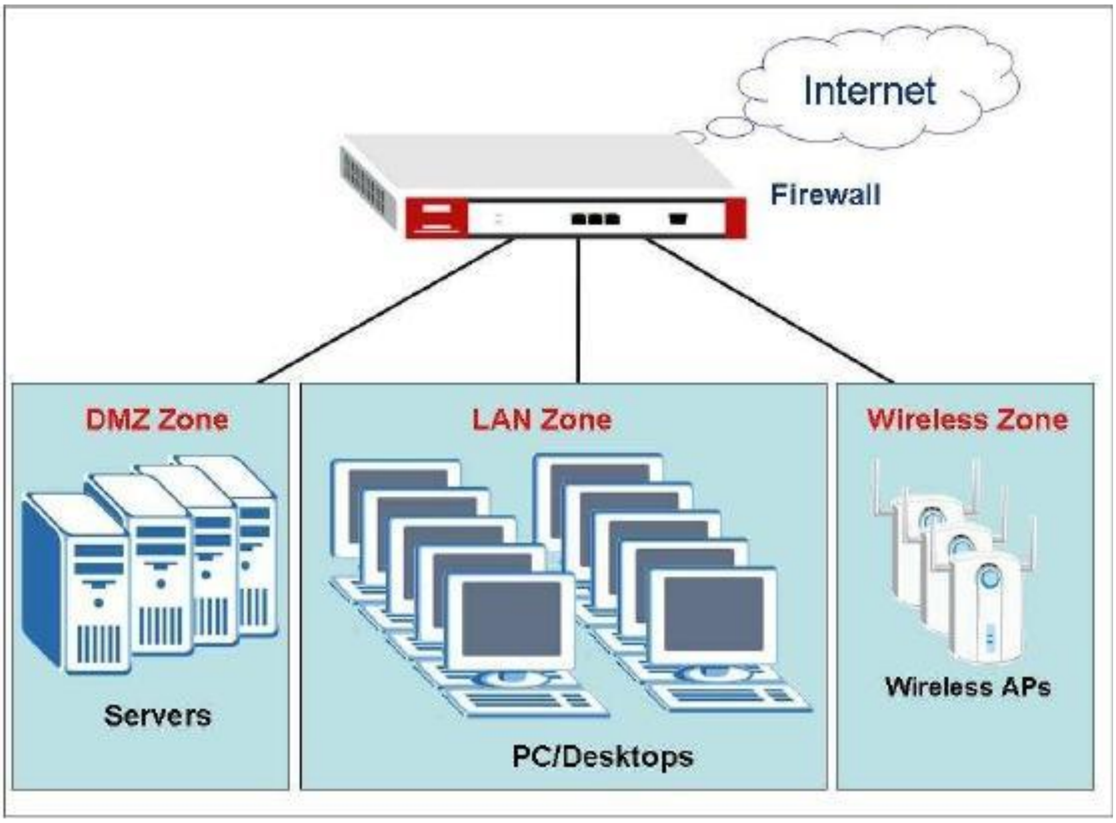
Dynamic VLAN (DVLAN) table

III. Egress Process:

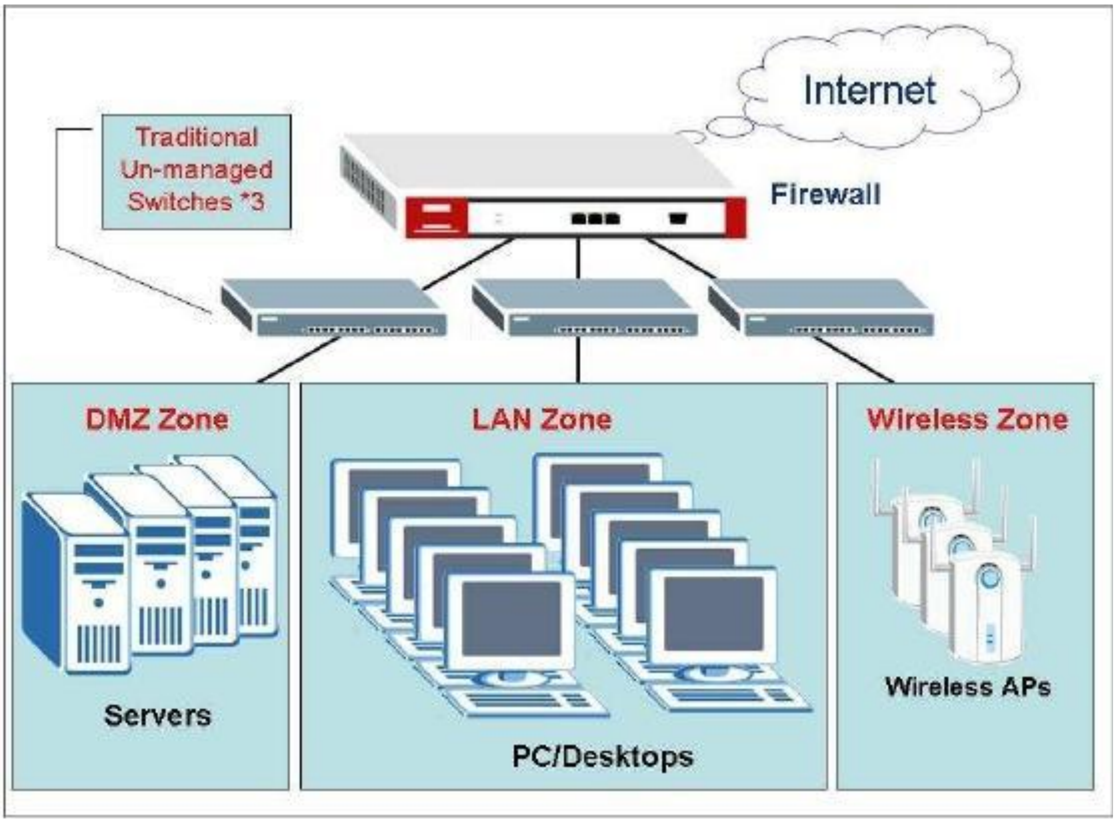
The Egress Process decides whether the outgoing frames will be sent tagged or untagged. The Egress Process refers to the egress tag control information in the Filtering Database. If the value is tagged, the outgoing frame on the egress port is tagged. If the value is untagged, the tag will be removed before
the frame leaves the egress port.

Application Scenario

There is a company which is going to implement 3 Zones (LAN, DMZ and the Wireless). The network administrator of the company has got a Firewall (ex: ZyWALL 1050) for the secure gateway. Also he has 4 servers in the DMZ zones, 10 PCs at the LAN Zone, 3 Access Points in the Wireless Zone. How many switches does he need to purchase?

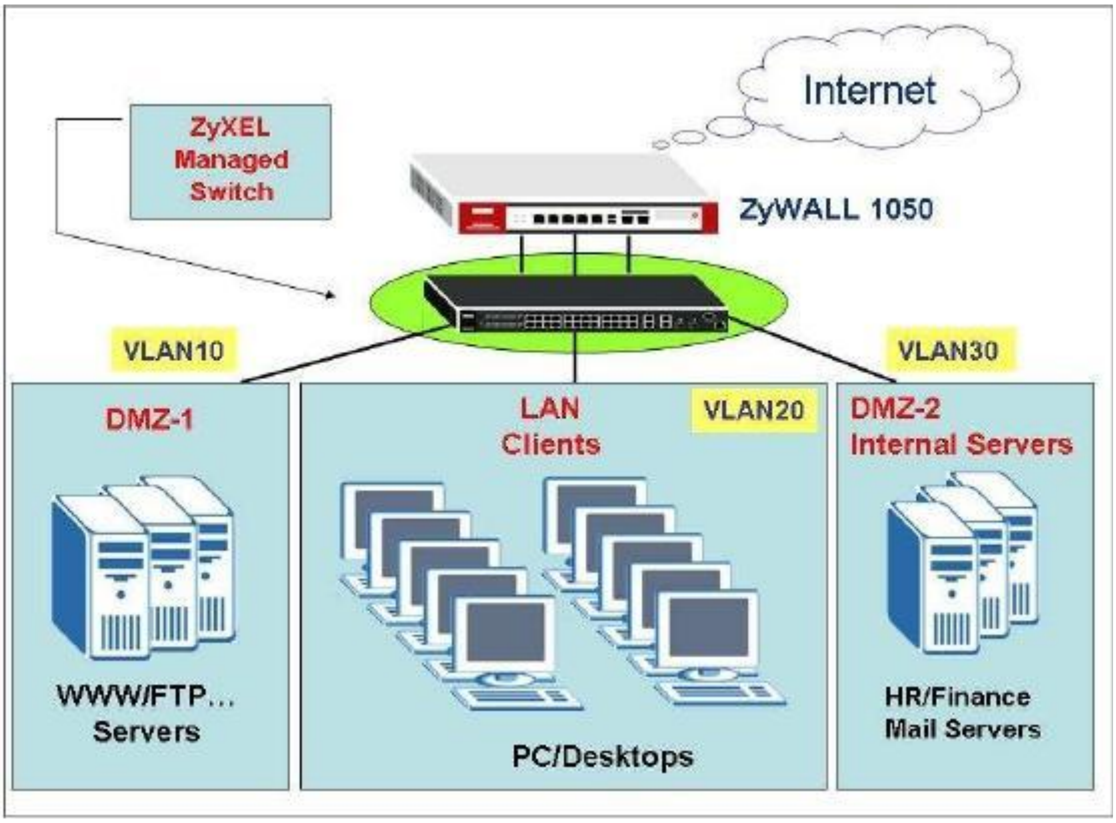


The answer is three for un-managed VLAN unaware Switch. (One for each zone)



However, if you got a VLAN aware ZyXEL Management Switch (e.g. ZyXEL ES-3124), you will just need one big Switch instead of the three Unmanageable Switches. Virtually cut the Switch into three smaller Switches and your job is done.

For example, VLAN10 for DMZ Zone, VLAN20 for the LAN Zone, VLAN30 for the Wireless Zone. Still, none of them can talk across Zones, although they are all physically connected to one Switch.



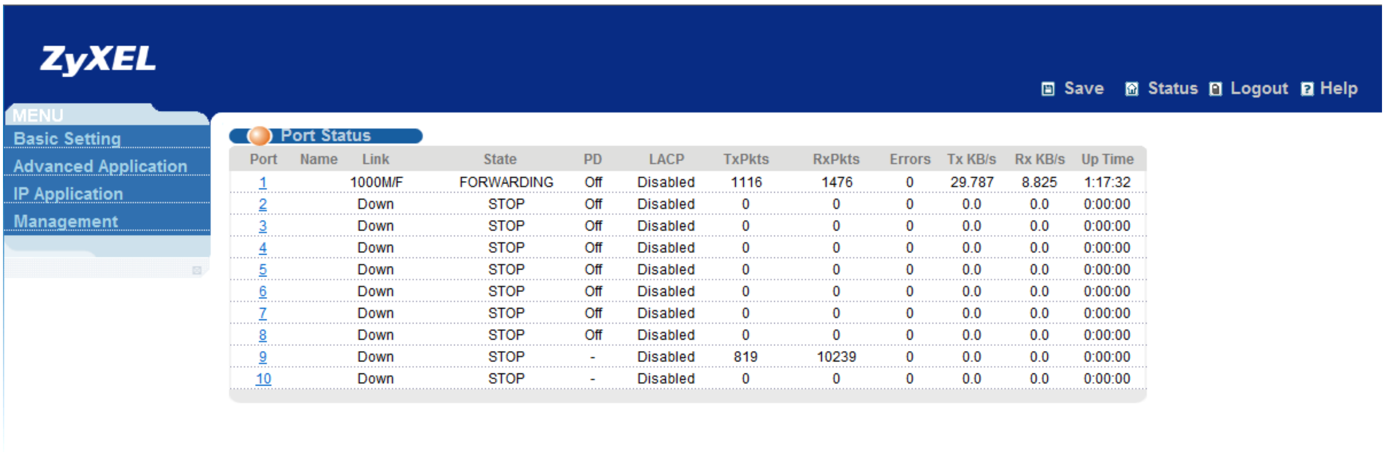
In a small/medium business, the IT infrastructure may consist three parts: DMZ (DMZ-1, to provide WWW and FTP server for external customer), Client LAN zone (for normal client users), and Server farm (DMZ-2, for internal server, e.g. Mail server, HR/Finance Server)

We'll use ZyXEL ZyWALL 1050 as a firewall device to setup this scenario. ZyWALL 1050 equips five configurable WAN/DMZ/LAN interfaces. Due to the physical port only have five, we need to use Switch(es) to extend the Ethernet ports. Here we use a ZyXEL Management Switch like ES-3124 to setup our scenario. Because it is a VLAN aware Switch, we can treat it as logically three Switches in our case.

The network topology is as the following picture shown. Based on this topology, we'll create three VLANs: VLAN 10, VLAN 20, and VLAN 30. Each VLAN mapping to DMZ-1, Clients LAN zone, and Server farm(DMZ-2) respectively.

Configuration via GUI on ZyXEL Management Switch

1. Connect PC or Notebook to the port 1 using the RJ45 Cable.
2. By default, the MGMT IP of every in-band port is 192.168.1.1/24
3. Set your NIC to 192.168.1.2/24
4. Open an Internet browser such as IE and enter http://192.168.1.1 in the URL field.
5. By default, you will need to insert “admin” as the username and “1234” as the password.
6. After you login successfully, you will see a screen similar to the one below.

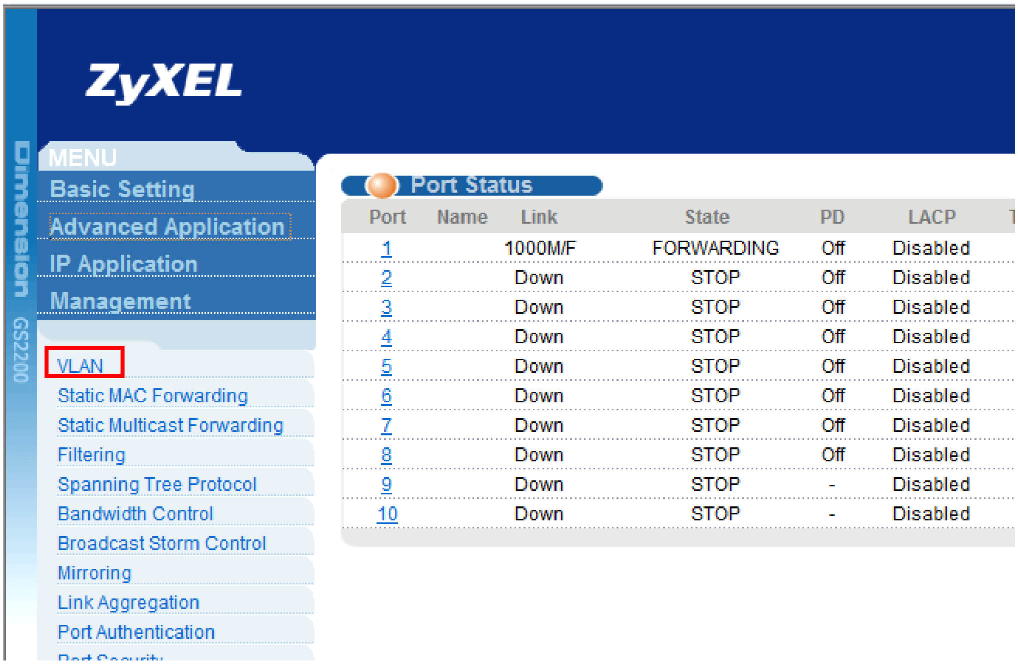


Port Status

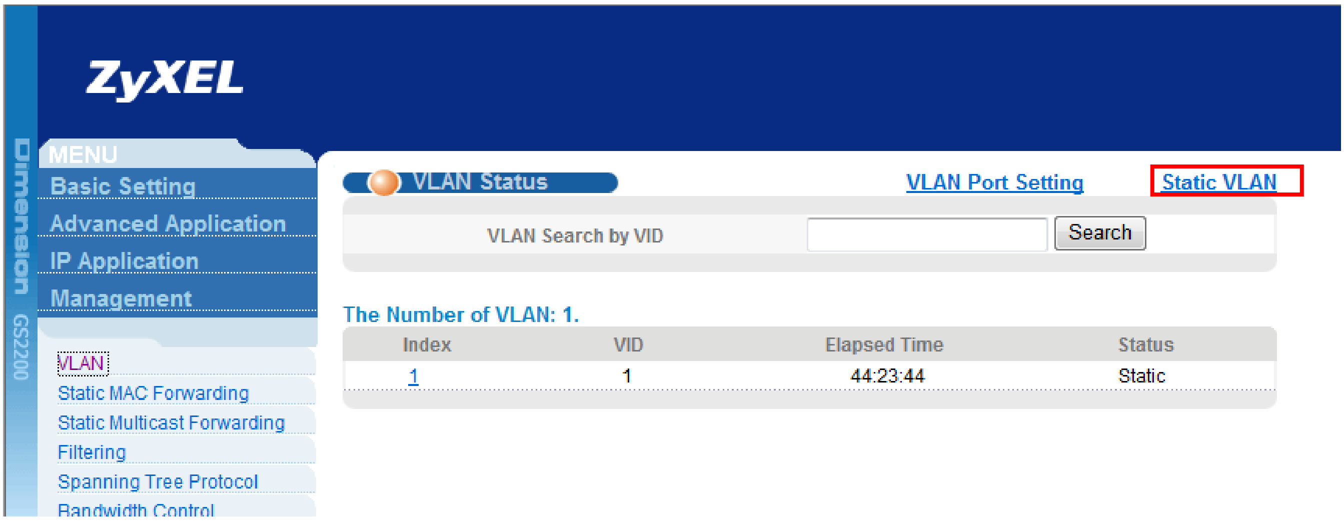
Port	Name	Link	State	PD	LACP	TxPkts	RxPkts	Errors	Tx KB/s	Rx KB/s	Up Time
1		1000M/F	FORWARDING	Off	Disabled	1116	1476	0	29.787	8.825	1:17:32
2		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
3		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
4		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
5		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
6		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
7		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
8		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
9		Down	STOP	-	Disabled	819	10239	0	0.0	0.0	0:00:00
10		Down	STOP	-	Disabled	0	0	0	0.0	0.0	0:00:00

7. Click “Advanced Application” on your left menu, and then choose “VLAN”.

8. Second, click “Static VLAN” to create VLAN 10, VLAN 20 and VLAN30.



Port	Name	Link	State	PD	LACP	T
1		1000M/F	FORWARDING	Off	Disabled	
2		Down	STOP	Off	Disabled	
3		Down	STOP	Off	Disabled	
4		Down	STOP	Off	Disabled	
5		Down	STOP	Off	Disabled	
6		Down	STOP	Off	Disabled	
7		Down	STOP	Off	Disabled	
8		Down	STOP	Off	Disabled	
9		Down	STOP	-	Disabled	
10		Down	STOP	-	Disabled	



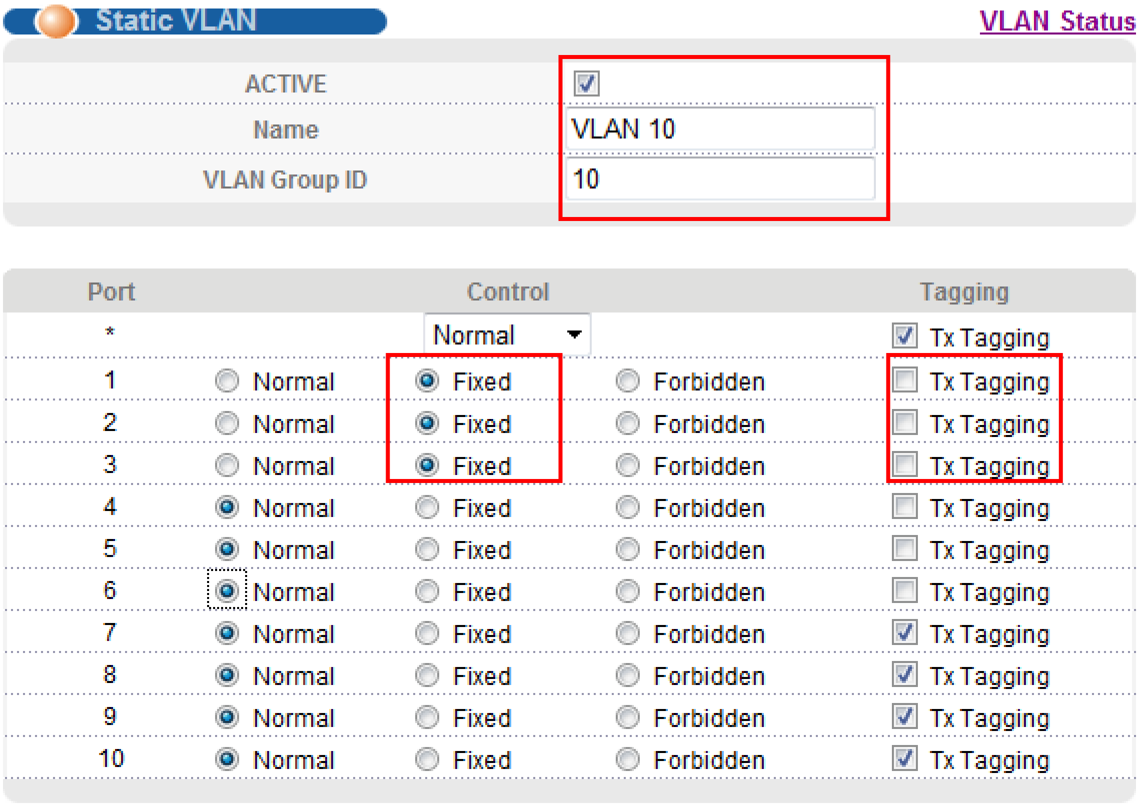
VLAN Search by VID

The Number of VLAN: 1.

Index	VID	Elapsed Time	Status
1	1	44:23:44	Static

9. First of all, we click the check box “ACTIVE” to enable this new VLAN. Then we need to give this VLAN a name and assign a VLAN ID to it. In this case, we are going to create VLAN10, thus we assign VLAN ID 10 to this VLAN. Moreover, we are going to make port 1~3 join VLAN10. Since all PCs connected to the Switch are VLAN unaware, all un-check the “Tx

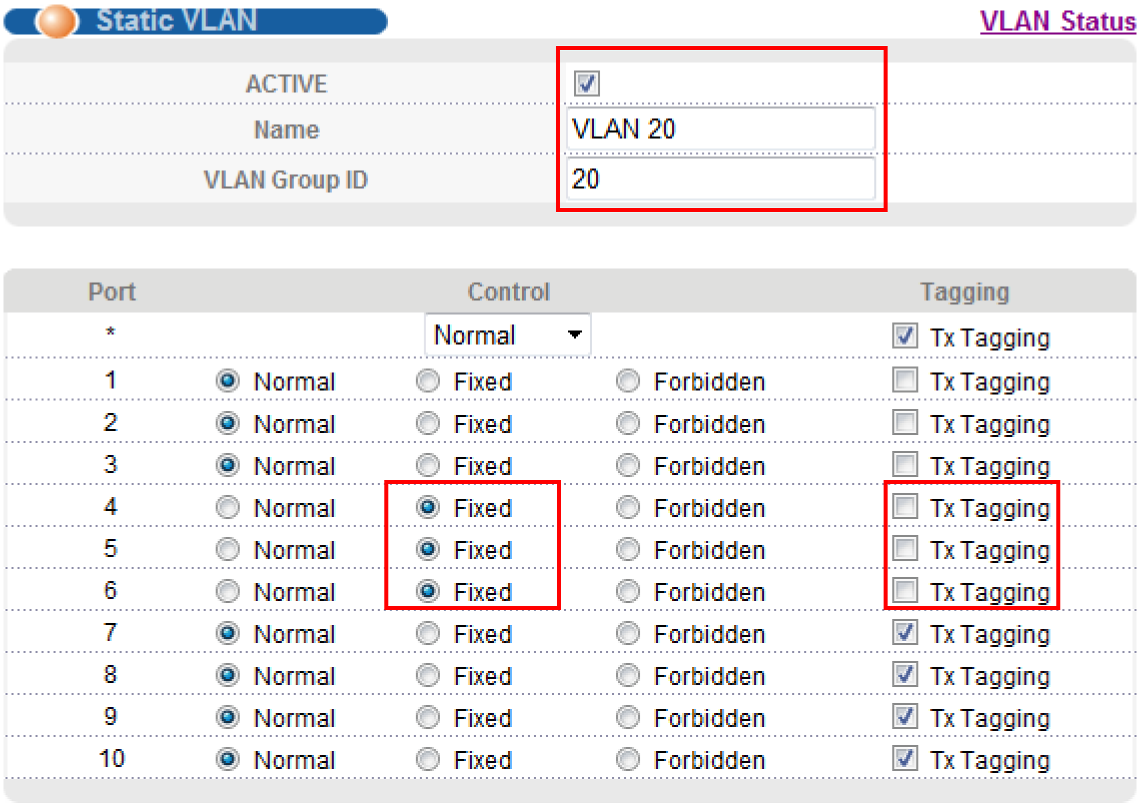
Tagging” to take away the VLAN tag during egress.



ACTIVE	☑
Name	VLAN 10
VLAN Group ID	10

Port	Control			Tagging
*	Normal			☑ Tx Tagging
1	○ Normal	● Fixed	○ Forbidden	□ Tx Tagging
2	○ Normal	● Fixed	○ Forbidden	□ Tx Tagging
3	○ Normal	● Fixed	○ Forbidden	□ Tx Tagging
4	● Normal	○ Fixed	○ Forbidden	□ Tx Tagging
5	● Normal	○ Fixed	○ Forbidden	□ Tx Tagging
6	● Normal	○ Fixed	○ Forbidden	□ Tx Tagging
7	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
8	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
9	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
10	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging

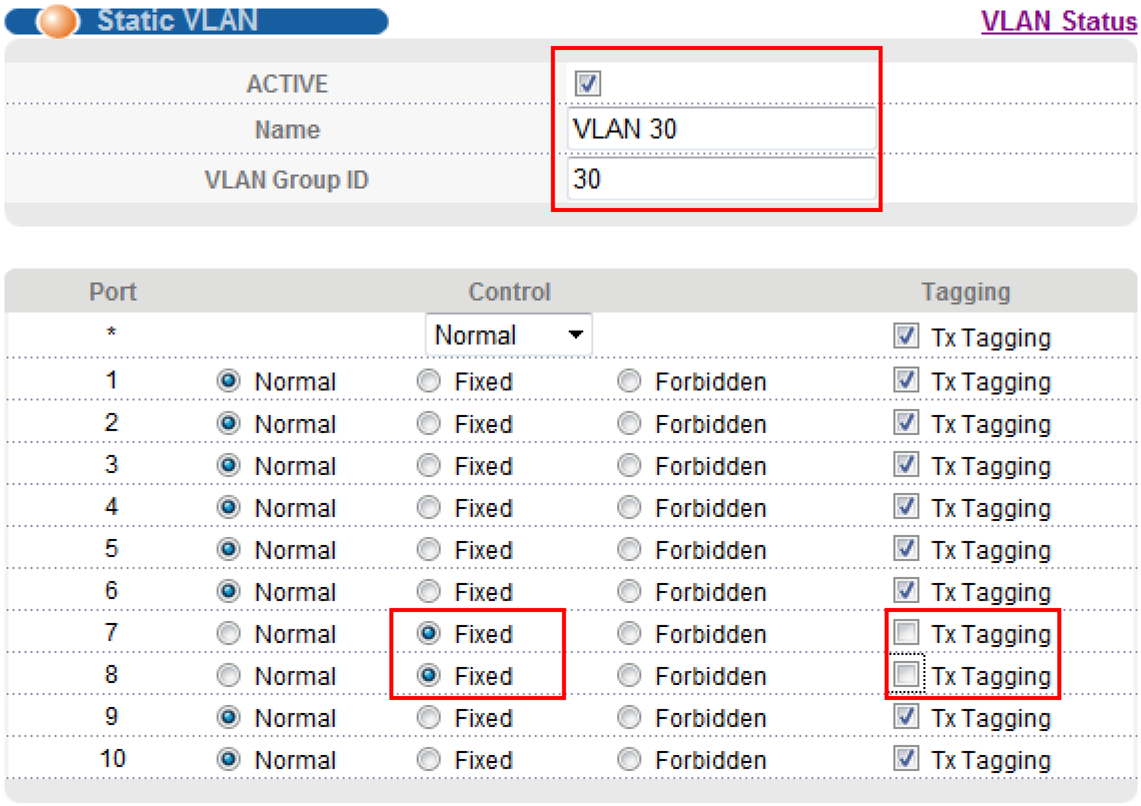
10. By following the above procedures, create VLAN 20 for port 4~6 and VLAN 30 for port 7 ~ 8.



Static VLAN — VLAN Status

ACTIVE	☑
Name	VLAN 20
VLAN Group ID	20

Port	Control			Tagging
*	Normal ▾			☑ Tx Tagging
1	● Normal	○ Fixed	○ Forbidden	□ Tx Tagging
2	● Normal	○ Fixed	○ Forbidden	□ Tx Tagging
3	● Normal	○ Fixed	○ Forbidden	□ Tx Tagging
4	○ Normal	● Fixed	○ Forbidden	□ Tx Tagging
5	○ Normal	● Fixed	○ Forbidden	□ Tx Tagging
6	○ Normal	● Fixed	○ Forbidden	□ Tx Tagging
7	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
8	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
9	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
10	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging

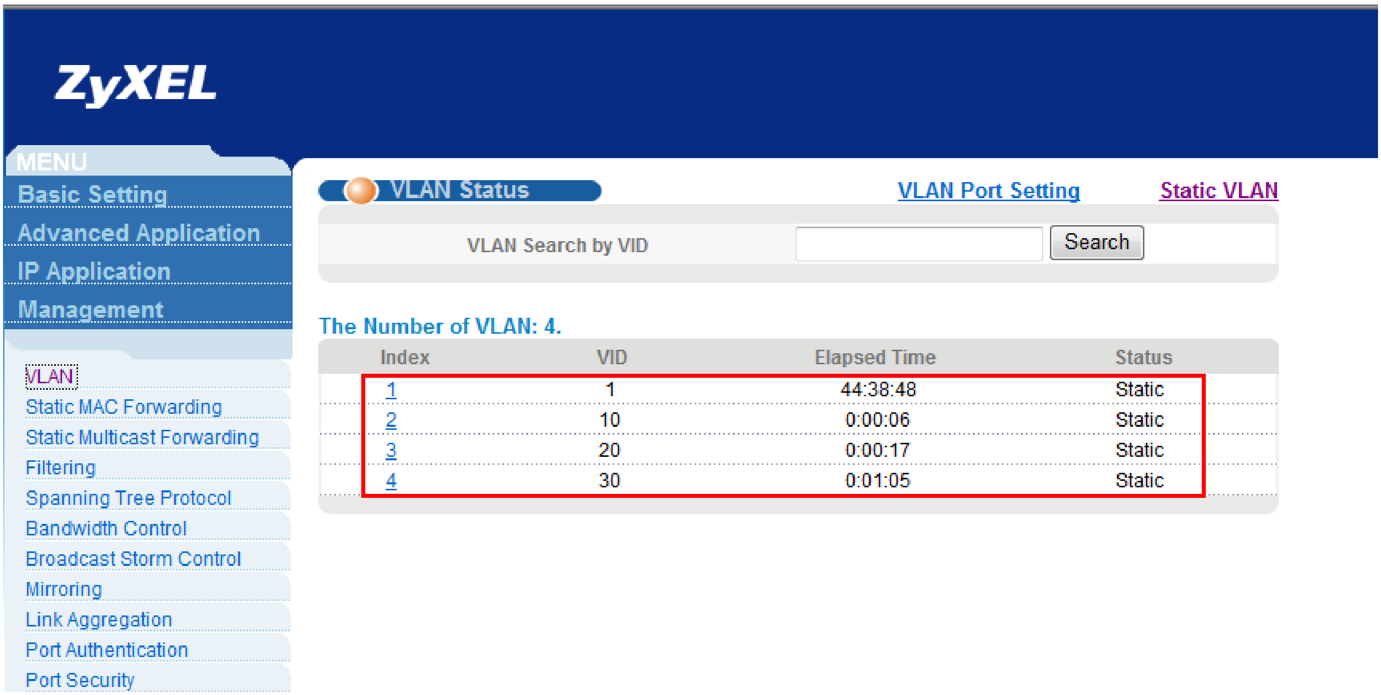


Static VLAN — VLAN Status

ACTIVE	☑
Name	VLAN 30
VLAN Group ID	30

Port	Control			Tagging
*	Normal ▾			☑ Tx Tagging
1	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
2	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
3	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
4	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
5	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
6	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
7	○ Normal	● Fixed	○ Forbidden	□ Tx Tagging
8	○ Normal	● Fixed	○ Forbidden	□ Tx Tagging
9	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
10	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging

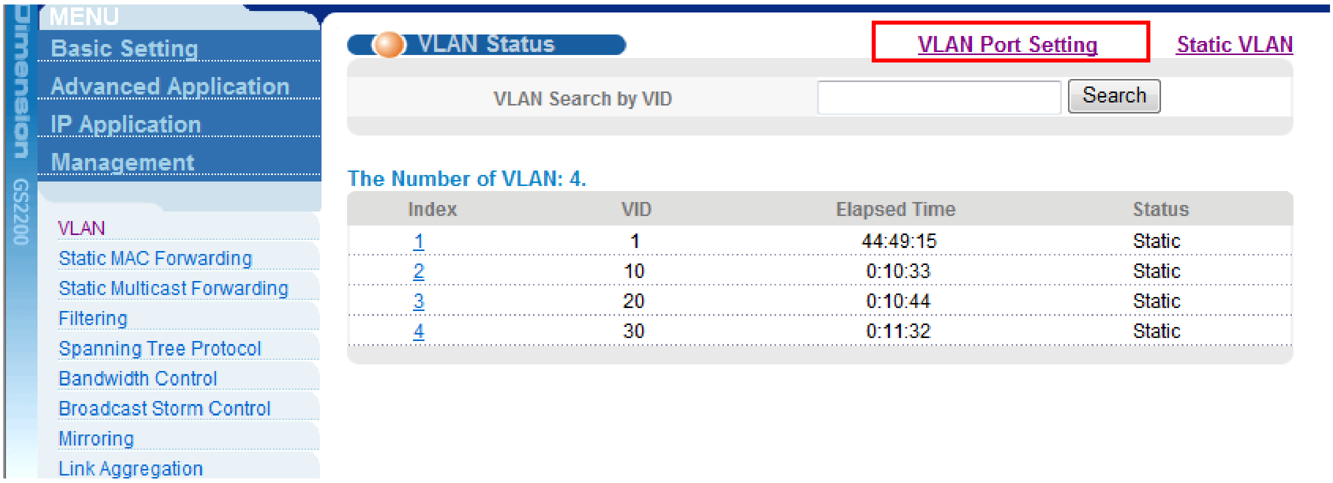
11. Now if you check the VLAN status, you should see a summary page like below. You can see VLAN10, 20 and 30 are there now.



The Number of VLAN: 4.

Index	VID	Elapsed Time	Status
1	1	44:38:48	Static
2	10	0:00:06	Static
3	20	0:00:17	Static
4	30	0:01:05	Static

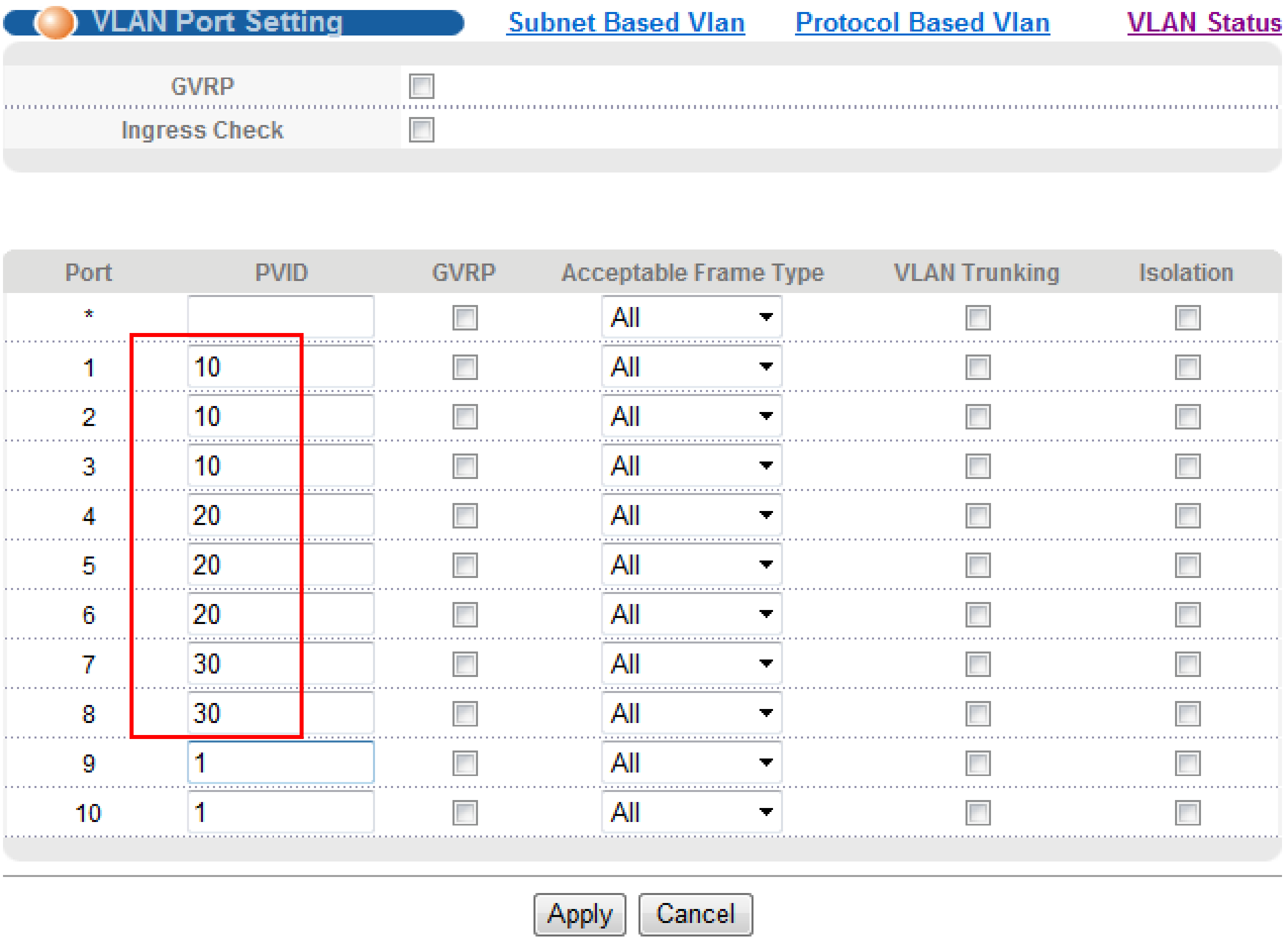
12. Now you need to define the PVID of VLAN10, 20 and 30 on the Switch. To do so, please click "VLAN Port Setting".



The Number of VLAN: 4.

Index	VID	Elapsed Time	Status
1	1	44:49:15	Static
2	10	0:10:33	Static
3	20	0:10:44	Static
4	30	0:11:32	Static

13. We put PVID 10 for port 1~6, PVID 20 for port 7~18, PVID 30 for port 19~24.



GVRP	□
Ingress Check	□

Port	PVID	GVRP	Acceptable Frame Type	VLAN Trunking	Isolation
*		□	All	□	□
1	10	□	All	□	□
2	10	□	All	□	□
3	10	□	All	□	□
4	20	□	All	□	□
5	20	□	All	□	□
6	20	□	All	□	□
7	30	□	All	□	□
8	30	□	All	□	□
9	1	□	All	□	□
10	1	□	All	□	□

14. At this point everything is done. The Switch is virtually cut into three.

For Security Appliance ZyWALL 1050's setting, we create three IP domains for the three separate zones, here is the example:

1. Configure physical port-1 as DMZ with IP subnet 192.168.1.0/24, and connect port-1 to the ZyXEL Management Switch port-01 to join the VLAN10

2. Configure physical port-2 as LAN with IP subnet 192.168.2.0/24, and

   connect port-2 to the ZyXEL Management Switch port-06 to join the VLAN20.

3. Configure physical port-3 as DMZ with IP subnet 192.168.3.0/24, and connect prot-3 to the ZyXEL Management Switch port-23 to join the VLAN30.

Configuration via CLI on ZyXEL Management Switch

Connect the Switch Console port with your PC or Notebook.

1. Open your Terminal program.(Ex, Hyper Terminal in Windows System)
2. Make sure that your port settings are

bps:9600

Data bits:8

Parity: None

Stop bits:1

Flow control: None:

3. After you connected successfully, give the correct user name and password.
4. Now you have already gotten into the enable mode. Then put “configure” to go into the configuration mode.

Issue the following commands to setup your Switch in this scenario.

To create VLAN 10, 20 and 30 on the Switch:

Issue the following commands.

```
vlan 10
   name VLAN10
   normal 7-28
   fixed 1-6
   forbidden ""
   untagged 1-6
exit
vlan 20
   name VLAN20
   normal 1-6,19-28
   fixed 7-18
   forbidden ""
   untagged 7-18
exit
vlan 30
```

```
   name VLAN30
   normal 1-18,25-28
   fixed 19-24
   forbidden ""
   untagged 19-24
exit
interface port-channel 1
   pvid 10
exit
interface port-channel 2
   pvid 10
exit
interface port-channel 3
   pvid 10
exit
interface port-channel 4
   pvid 10
exit
interface port-channel 5
   pvid 10
exit
interface port-channel 6
   pvid 10
exit
interface port-channel 7
   pvid 20
exit
interface port-channel 8
   pvid 20
exit
interface port-channel 9
   pvid 20
exit
interface port-channel 10
   pvid 20
exit
interface port-channel 11
```

```
    pvid 20
exit
interface port-channel 12
    pvid 20
exit
interface port-channel 13
    pvid 20
exit
interface port-channel 14
    pvid 20
exit
interface port-channel 15
    pvid 20
exit
interface port-channel 16
    pvid 20
exit
interface port-channel 17
    pvid 20
exit
interface port-channel 18
    pvid 20
exit
interface port-channel 19
    pvid 30
exit
interface port-channel 20
    pvid 30
exit
interface port-channel 21
    pvid 30
exit
interface port-channel 22
    pvid 30
exit
interface port-channel 23
    pvid 30
exit
```