White Paper

Virtual Networks

SysKonnect

Virtual Networks

Table of Contents

1 Reasons for establishing a VLAN

VLANs reduce costs

Virtual networks offer the opportunity to separate physical from logical network structure.

Which virtual network a user is assigned to, no longer depends on the physical location of the network. Employees belonging to the same interest group can be joined in one virtual LAN group, regardless of their physical location. Under organizational aspects, all members of a department can, for example, form a network group, even if they are distributed over several buildings. Colleagues working on the same project can be united in a common VLAN, even if they belong to different departments in different buildings or even different locations.

By using virtual LANs, costs for network operations can be reduced, and overall competitiveness can be improved, if networks can be easily adapted to new organizational requirements.

VLANs ease network changes

Network administrators are forced to spend much of their time dealing with moving users and workstations. Although there are several tools that facilitate network management, costs for network management represent a considerable financial load for an average company. The costs for network management rise with each additional network user and with the demand for higher flexibility of the network.

With the introduction of virtual networks, operating costs can drastically be reduced. Whenever changes in operations or work assignments occur, staff members and network resources can quickly be restructured. The establishment of logical workgroups is carried out by software functions, while original subnet addresses are maintained. The network administrator need only reconfigure the new port to become part of a particular subnetwork. If the user belonged, for example, to VLAN “Marketing” before he moved, the new port need only be reassigned to VLAN “Marketing.”

VLANs enhance network security

In some networks, communications between individual workstations need to be prohibited at a relatively low level. Without VLANs all workstations belong to a single broadcast domain. By assigning the workstations to different VLANs, access can be denied or explicitly admitted by controlling devices such as routers. In general, this is referred to as First Level security.

VLANs help control network traffic

By establishing VLANs, broadcast traffic can be reduced considerably within backbones and individual subnetworks.

In a virtual network:

- Each packet sent from any workstation can be associated with exactly one VLAN.
- A workstation receives all multicast and broadcast packets within its associated VLAN.
- A workstation can receive unicast packets (packets addressed to an individual receiver) transmitted within its VLAN, if those packets are addressed to it.

VLANs thus divide the traffic, similar to routers. The broadcast feature important to many protocols for reaching all participants in a certain domain is maintained. For that reason, the term “VLAN” is sometimes synonymously used with “broadcast domain.”

2 Types of VLANs

In general, there are three basic models for determining how a packet gets assigned to a VLAN:

- Port-based VLANs
- MAC address-based VLANs
- Protocol-based VLANs (Layer 3 VLANs)

Port-based VLANs

In a port-based VLAN each port of a switch is assigned to a VLAN.

Example

	VLAN 1	VLAN 2
Switch No	Ports	Ports
1	2,3,7	--
2	2,3	1,5,8
3	1,2,3,6,7	--
4	2,3,7	4,5,8
5	--	1,2,5,7

VLAN 1 is built from the ports of switch No. 1 (2, 3, and 7), of switch No. 2 (2 and 3), of switch No. 3 (1, 2, 3, 6, and 7), and of switch No. 4 (2, 3, and 7). At switch No. 5, no port is assigned to VLAN 1.

VLAN 2 is built from the ports of switch No. 2 (1, 5, and 8), of switch No. 4 (4, 5, and 8), and of switch No. 5 (1, 2, 5, and 7). At switches No. 1 and No. 3, no port is assigned to VLAN 2.

When a workstation is moved to another port of the switch, the new port must be reassigned to the workstation’s old VLAN.

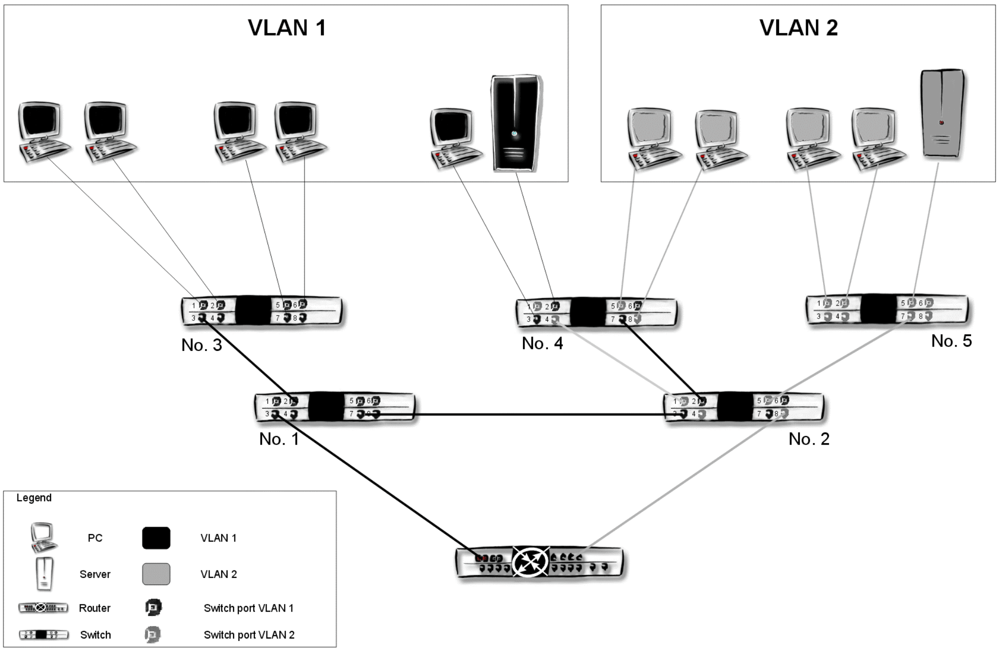

Figure 1. Port-based VLANs

It is a straight-lined model that virtualizes the physical LAN. Troubleshooting is eased since the assignment of the VLAN to the physical port is known.

If hubs are connected to the switches, the users assigned to a specific hub can only be assigned to a common VLAN.

MAC address-based VLANs

In MAC address-based VLANs, the MAC address of a workstation is assigned to a VLAN. Each switch maintains an assignment table of MAC addresses and their corresponding VLAN memberships. The source or destination MAC address determines to which VLAN a packet is passed.

Example

	VLAN 1	**VLAN 2**
Switch No	**MAC addresses**	**MAC addresses**
1	--	--
2	--	--
3	MAC_01, MAC_02, MAC_03, MAC_04	--
4	MAC_05, MAC_06	MAC_07, MAC_08
5	--	MAC_09, MAC_10, MAC_11

VLAN 1 is built from the MAC addresses MAC_01, MAC_02, MAC_03, and MAC_04 through switch No. 3, as well as from the MAC addresses MAC_05 and MAC_06 (server) through switch No. 4. Through switches No. 1, No. 2, and No. 5, no MAC address is assigned to VLAN 1.

VLAN 2 is built from the MAC addresses MAC_07 and MAC_08 through switch No. 4 as well as from the MAC addresses MAC_09, MAC_10, and MAC_11 (server) through switch No. 5. Through switches No. 1, No. 2, and No. 3, no MAC address is assigned to VLAN 2.

When a workstation is moved within the same VLAN it does not need to be reconfigured. Only if the workstation is moved to a different VLAN must the MAC address be reassigned to the new VLAN.

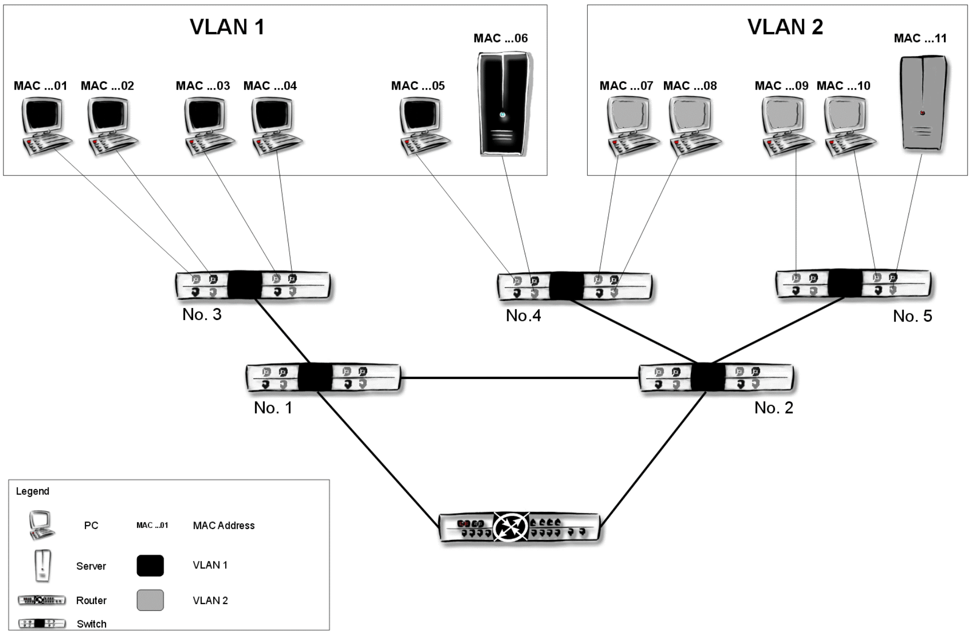

Figure 2. MAC address-based VLANs

The key advantage of this method is that the switch does not need to be reconfigured when a workstation is moved to another port. Another benefit of MAC-based VLANs is their excellent support of shared media hubs. This method permits users from different virtual networks to be on the same segment. Workstation moves can be handled automatically because each workstation is reassigned to its old VLAN as soon as it has been connected to the new port.

One drawback can be that MAC addresses have to be added manually during initial installation if auxiliary tools are not available. In addition, a single MAC address cannot easily be assigned to multiple VLANs. This may lead to a real limitation with respect to sharing server resources between more than one VLAN and result in serious problems when dealing with existing routers and bridges.

A major disadvantage is that this kind of network design places high demands upon the network management. An experienced user can simply reconfigure his workstation with a different MAC address, then directly access another VLAN. What is more, broadcasts can hardly be restricted, as the users of all the VLANs will soon be distributed over all the switch systems. In practice, then, all broadcasts are forwarded to all systems and therefore network traffic becomes quite complex.

Protocol-based VLANs

With this method, the delivery of packets depends on protocols (IP, IPX, NetBIOS, etc.) and Layer 3 addresses. It is the most flexible variant providing the most logical grouping of users. An IP subnetwork or an IPX network can be assigned its own VLAN. Protocol-based assignment also enables the administrator to use non-routable protocols, such as NetBIOS or DECnet, and assign them to larger VLANs than would be possible with IP or IPX. This leads to a considerable increase in efficiency. Another distinction to other VLAN implementations is the method used to indicate membership when a packet is transferred between switches. There are two different methods: implicit and explicit.

Implicit – The VLAN membership of a packet is indicated by the MAC address. In this case, all switches that support a particular VLAN must share a common table with MAC addresses and their assignments.

Explicit – The VLAN membership of a packet is indicated by a tag that is added to the packet (for the structure of a tag see below). This method is defined in the IEEE standard 802.1Q. When a packet arrives at its local switch, the VLAN membership can be determined as port-based, MAC address-based or protocol-based. When the packet is transferred to other switches the VLAN membership can either be detected implicitly (through the MAC address) or explicitly (through a tag that was added by the first switch). Port- and protocol-based VLANs prefer explicit tagging. MAC address-based VLANs are almost always implicit. The IEEE 802.1Q specification, approved in 1998, supports port-based assignment as well as explicit tagging.

Example

	VLAN 1	**VLAN 2**
Switch No	**IP addresses**	**IP addresses**
1	--	--
2	--	--
3	129.0.1.10, 129.0.1.11, 129.0.1.12, 129.0.1.13	--
4	129.0.1.14, 129.0.1.15	129.0.2.10, 129.0.2.11
5	--	129.0.2.12, 129.0.2.13, 129.0.2.14

VLAN 1 is built from the IP addresses 129.0.1.10, 129.0.1.11, 129.0.1.12, and 129.0.1.13 through switch No. 3, as well as from the IP addresses 129.0.1.14 and 129.0.1.15 (server) through switch No. 4. Through switches No. 1, No. 2, and No. 5, no IP address is assigned to VLAN 1.

VLAN 2 is built from the IP addresses 129.0.2.10 and 129.0.2.11 through switch No. 4 as well as from the IP addresses 129.0.2.12, 129.0.2.13, and 129.0.2.14 through switch No. 5. Through switches No. 1, No. 2, and No. 3, no IP address is assigned to VLAN 2.

When a workstation is moved within the same VLAN it does not need to be reconfigured. Only if the workstation is moved to another VLAN must the IP address be reassigned to the new VLAN.

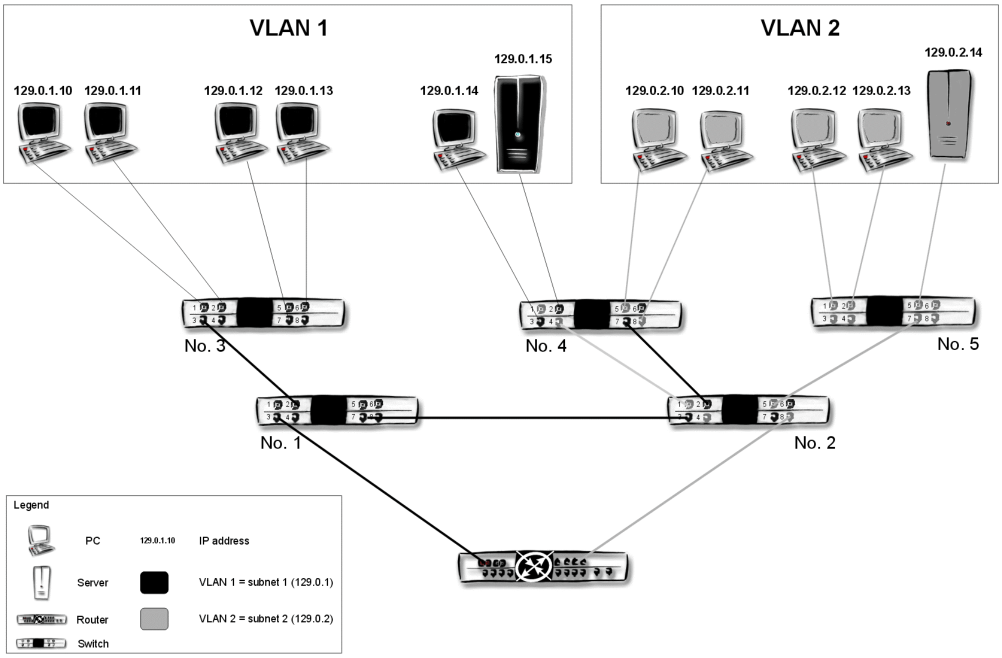

Figure 3. Protocol-based VLANs (here: via IP addresses)

One advantage of the protocol-based method is that it permits optimal traffic control. Any broadcast can be segmented according to the protocols used. Even workstations with multi-protocol stacks, or shared media segments with workstations using different protocols, can be supported by this procedure. Protocol/address-based variants support mixed networks.

One disadvantage is its high complexity, which places higher demands on network management. The network administrator must then have detailed knowledge regarding all the protocols in use. Another drawback is that dynamic address assignment procedures (e. g. DHCP) are incompatible with this method.

In the case of tagging, another drawback is that the maximum packet size increases compared to Standard Ethernet packets. In some devices, this may lead to counter errors. In addition, apart from the switches all routers and bridges must be able to manage the IEEE 802.1Q specification as well.

Layer 3 switching as a basis for VLANs

The benefits of VLANs – the independence of network membership from the physical workstation location – often lead to constellations that are less favorable for traffic flow.

Example

Let’s assume two terminal workstations were bound to different VLANs. If a workstation belonging to VLAN A wants to communicate with a workstation belonging to VLAN B all communication must go through a router due to their different VLAN/IP network. If a packet needs additionally to be passed on within one of the VLANs, then not only is the router needed for link establishment, but each packet sent by the first workstation of VLAN A to the second workstation of VLAN A must go through the router. Thus, every packet travels the link between the switch systems twice, and in addition must be processed by the router. If, on the other hand, the Layer 2 switch is upgraded with Layer 3 functionality, packet forwarding is performed as close as possible to the workstations involved. When a Layer 2/3 switch is used, the packets concerned are sent directly to the switch port where the destination workstation is connected.

In the following section, we will consider the establishment of a VLAN network in further detail using a tagged VLAN as the example.

3 Configuration of a VLAN

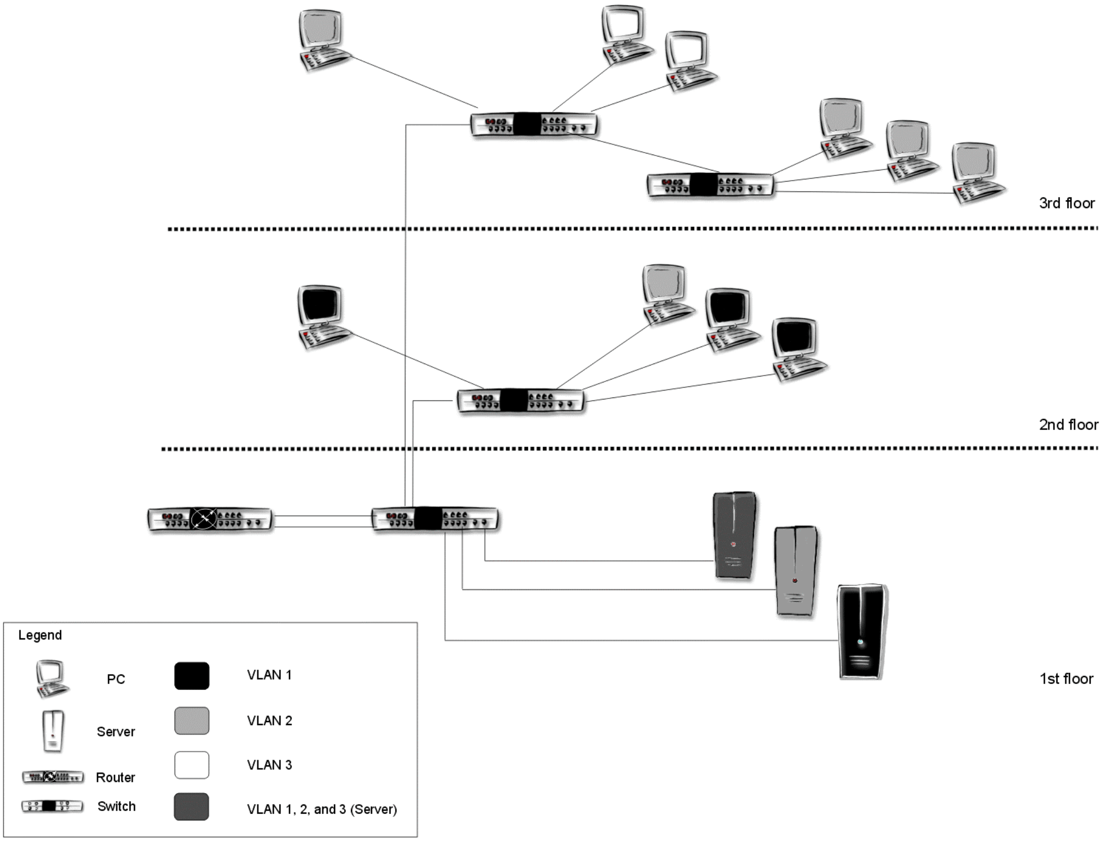

Figure 4. Structure of a network with virtual LANs

The above example of a simple-structured LAN network consists of a server center and networked participants on several floors. The switching components that serve to connect the workstations in the center and on the floors act as Layer 2 switches. In a VLAN, workstations can only communicate with other workstations belonging to the same VLAN. If a link to a workstation of another VLAN has to be established, the data must be distributed through a switch or a router, even if the destination station is located on the same floor. The switch acts as a filter. In the case of a broadcast packet, the switch makes sure that it is only sent to members of the respective VLAN. In the case of a unicast packet, it is sent only to the destination workstation. If members of a workgroup or department are distributed over several floors, unicast packets destined for a workstation belonging to the same VLAN but located on another floor must be passed over the respective switch-to-switch link to the destination workstation. Unicast packets that are destined for another member on the same floor are directly switched on that floor. Broadcast packets in the VLAN are, however, distributed over the respective feeders to the VLAN participants on the other floors.

Establishing a VLAN

Physical Connection

As soon all user/workstation-to-VLAN assignments have been executed the VLANs must be assigned to ports by configuring the ports to accept VLAN packets from its assigned VLAN. Each port receives a unique VLAN address. Finally, the switches are physically connected by means of cables.

VLANs can span multiple switches if connected via one or more switch-to-switch connections, or trunk. In a port-based VLAN, each VLAN requires a separate pair of trunk ports. Using tags, multiple VLANs can be connected through two switches by means of a single trunk.

Such an assignment of a port to multiple VLANs is another advantage of tagged VLANs. This is particularly useful for devices such as servers, which must belong to multiple VLANs. These devices, however, must have both network adapters and a driver that support tagging.

It is possible to assign a server to multiple VLANs and connect it to a switch by using a network adapter that supports tagged VLANs. Through a separate IP interface, all VLANs are bound to the same network adapter on the server, which - with the help of the tags delivered - uses its driver to determine the destination address of the packets. The switch receives the tagged packets and passes them on, tagged or untagged, as required by the port configuration.

In the reverse direction, the adapter receives the tagged packets from the switch. The driver strips off the tags before it passes the packets on to the higher protocol layers. These will only “see” Standard Ethernet packets.

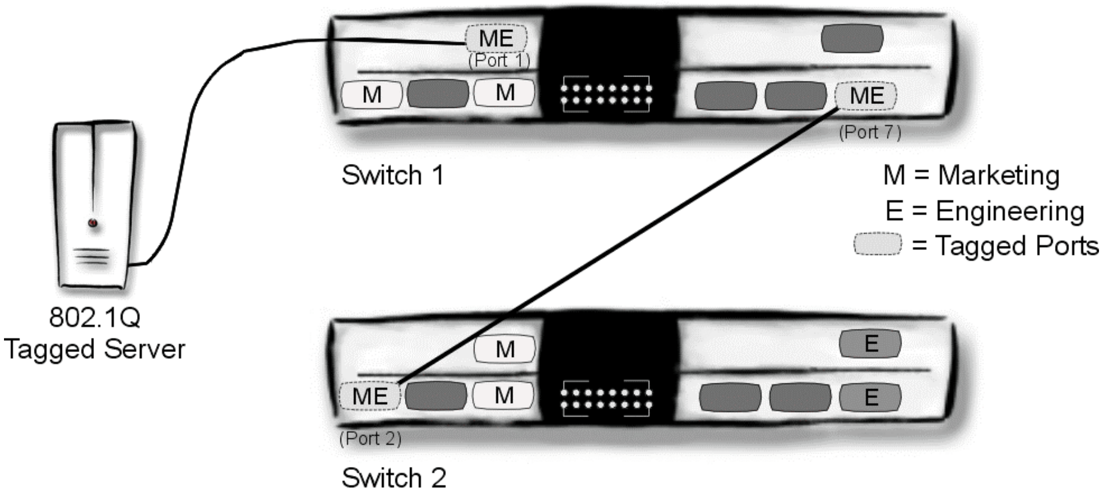

Figure 5. Physical setup for tagged and untagged traffic

Logical Connection

A single port can only be a member of one port-based VLAN. If the port should be assigned to multiple VLANs it must be configured accordingly for any additional VLAN (as permitted by the vendor), e.g. by providing each VLAN with a separate VLAN tag.

During the assignment of ports to VLANs, the network administrator can define whether a port should use tagging or not. Not all ports in a VLAN must be tagged. Tagged ports are only useful for trunks between two switches or a server and a switch, as network adapters that do not support VLANs would reject tagged packets. During data transfer the switch checks its configuration to decide if the packet for a particular destination port must be equipped with a VLAN tag. Accordingly, it deletes or adds a suitable tag.

In our example (figures 5 and 6), the packets sent between port 7 of switch No. 1 and port 2 of switch No. 2 are tagged. The remaining data exchange is carried through untagged. Depending on the workstation a packet is intended for, the switch forwards packets as tagged or untagged. Packets coming from and going to ports 1 and 7 of switch No. 1 are tagged. Data destined for other ports is switched untagged.

The server connected to port 1 of switch No. 1 is both part of the VLAN “Marketing“ and part of VLAN “Engineering“. Packets coming from and going to the server are always tagged.

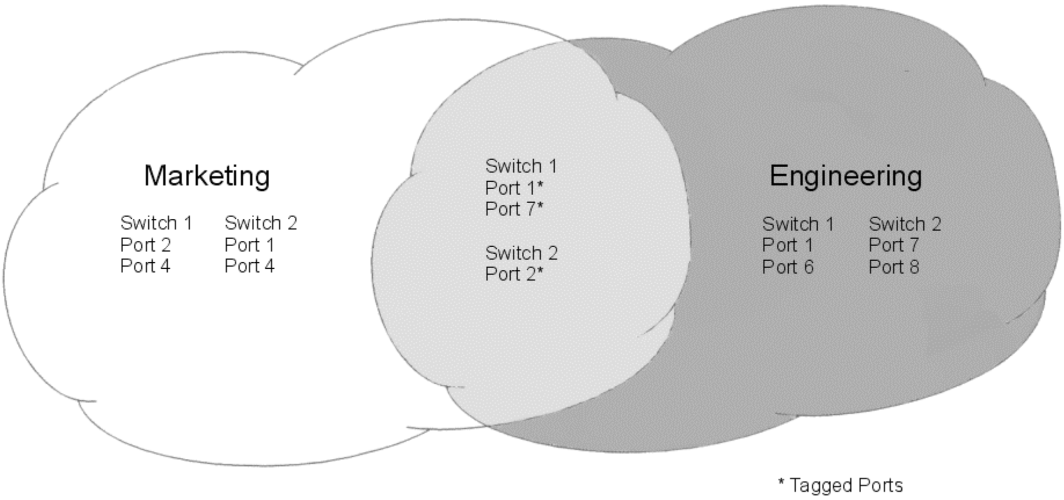

Figure 6. Logical setup for tagged and untagged traffic

Packet identification with Frame Tagging

Many vendors have already developed their own proprietary VLAN solutions and products. Thus, an industry standard was required to ease confusion and make the benefits of VLANs publicly available. Therefore, working group IEEE 802.1Q has ratified a standard to improve the interoperability of VLAN between switches and network adapters from different vendors.

The standard defines the following:

- Support of existing IEEE standards 802.X
- Extension of quality-of-service (802.1p*)
- One spanning tree per VLAN
- Support of Token Ring-based structures

*This IEEE standard defines the use of priority bits that are part of the VLAN tag as defined in the standard 802.1Q.

…

Destination Address	6 Byte
Source Address	6 Byte
Length/Type	2 Byte
Data	46-1500 Byte
Frame Check Sequence	4 Byte

Standard Ethernet Frame
(1518 Byte)

…

Destination Address	6 Byte
Source Address	6 Byte
VLAN tag	4 Byte
Length/Type	2 Byte
Data	46-1500 Byte
Frame Check Sequence	4 Byte

Tagged VLAN Frame
(1522 Byte)

Structure of a VLAN tag

A VLAN tag has the following structure:

TPID (Tag Protocol Identifier)	**TCI (Tag Control Information)**		
Identification for the VLAN header: 0x8100 (16 Bit)	User Priority: 0-7 (3 Bit)	CFI (1 Bit)	VLAN ID: 0-4095 (12 Bit)

VLAN IDs 0 and 4095 have a special meaning. For further information, see the IEEE standard 802.1Q. Therefore, VLANs can be identified with any values from 1 to 4094.

Receive and Transmit

When a packet arrives at a switch, the latter checks by means of the destination address, whether or not the desired workstation is a member of the connected subnetwork. If so, the packet is forwarded accordingly.

In tagged VLANs, the data transfer was initially performed on a switch-to-switch basis. Here, both transmitting and receiving switches must be able to send and receive tagged packets. SysKonnect additionally offers drivers that permit data traffic on switch-to-station basis (for further information, see next section).

In the examples from figure 5 and figure 6, the switch checks the incoming and outgoing packets. In the transmitting direction a Standard packet is sent from the transmitting workstation to the switch. If the packet is destined for a workstation belonging to the same VLAN, it is forwarded unchanged. If the packet is destined for a different VLAN, the switch adds a tag if required by the configuration of the destination VLAN. If, for example, a packet is sent from VLAN “Marketing“ to VLAN “Engineering“, the switch adds the VLAN tag required for

VLAN “Engineering“ before passing it on. If a packet is destined for another workstation belonging to a LAN or a VLAN that does not use tagging, the switch strips the VLAN tag from the sender (here: VLAN “Marketing“) before passing the packet along.

The receiving switch uses the VLAN tag to determine the VLAN for which the packet is destined. In our example, switch No. 2 would determine by means of the VLAN tag, that it received a packet for VLAN “Engineering.“ Then it would strip off the tag to obtain a Standard Ethernet packet and forward the packet to the destination address. Tagged packets containing a VLAN ID not configured in the switch will be discarded.

SysKonnect VLAN drivers

For several operating systems, SysKonnect offers drivers that support VLAN tagging and thus can be applied for VLAN servers and terminal units.

For example, a server can be assigned to several VLANs and be connected to an appropriately configured switch through a network adapter. In this case, each VLAN on the server is assigned a separate IP interface with a unique IP address.

Example A server running on Solaris 7 should be integrated into three different VLANs:

VLAN Sales	IP address: 192.9.130.59	VLAN-ID: 2
VLAN Marketing	IP address: 192.9.140.59	VLAN-ID: 3
VLAN Engineering	IP address: 192.9.150.59	VLAN-ID: 4

The VLAN-IDs are selected randomly within the valid scope. After driver and IP interface have been configured (the method varies according to the operating system applied; in case of Solaris, entries are made in a driver configuration file, manually or by means of a configuration script), the three VLANs are displayed as ordinary IP interfaces assigned to the same SysKonnect network adapter if, e.g., `ifconfig -a` is executed:

```
lo0: flags=849<UP,LOOPBACK,RUNNING,MULTICAST> mtu 8232
       inet 127.0.0.1 netmask ff000000
hme0: flags=863<UP,BROADCAST,NOTRAILERS,RUNNING,MULTICAST> mtu 1500
       inet 192.54.37.59 netmask ffffff00 broadcast 192.54.37.255
       ether 8:0:20:89:15:e4
skge0: flags=863<UP,BROADCAST,NOTRAILERS,RUNNING,MULTICAST> mtu 1500
       inet 192.9.130.59 netmask ffffff00 broadcast 192.9.130.255
       ether 0:0:5a:98:21:24
skge100: flags=863<UP,BROADCAST,NOTRAILERS,RUNNING,MULTICAST> mtu 1500
       inet 192.9.140.59 netmask ffffff00 broadcast 192.9.140.255
       ether 0:0:5a:98:21:24
skge200: flags=863<UP,BROADCAST,NOTRAILERS,RUNNING,MULTICAST> mtu 1500
       inet 192.9.150.59 netmask ffffff00 broadcast 192.9.150.255
       ether 0:0:5a:98:21:24
```

The driver adds or removes VLAN tags to or from the packets transparently. Thus, the programs on the server (including the operating system) only “see” the usual Ethernet packets without tags.

The number of VLANS as well as the VLAN assignment (via the VLAN ID) can be changed and adapted to the respective requirements anytime by re-configuring the driver.

In the example above, the server behaves as a system with four network adapters although only two physical adapters are installed in the system (`lo0` is the so-called „loopback Interface“). The communication between two IP interfaces is always performed by means of routing, notwithstanding if the interfaces are VLAN interfaces or not. The same applies for a VLAN switch: Two or more VLANs are treated as two completely independent networks. If data is to be transferred between two VLANs on a switch either the switch must be able to perform routing tasks or routing has to be carried out by a router.

VLANs and SysKonnect Dual Link operation

SysKonnect offers use of its Gigabit Ethernet dual link adapter with an additional function called RLMT (Redundant Link Management Technology). RLMT serves to assure a continuation of traffic by switching the link of the active port to the failover port in case of failures. This functionality can, however, only be applied if it is assured that both ports of the adapter belong to the same VLAN. Otherwise correct RLMT functionality cannot be guaranteed.

Example

A VLAN is bound to port A of a Gigabit Ethernet dual link adapter. If this connection fails for whatever reason, RLMT switches the link automatically to the port that is configured as the failover port (port B of the Gigabit Ethernet dual link adapter). Thus, the connection remains, even if the initial port fails. If multiple VLANs are bound to the active port (port A) but only some of them are bound to the failover port (port B), all VLAN connections that are not configured for the failover port will fail.

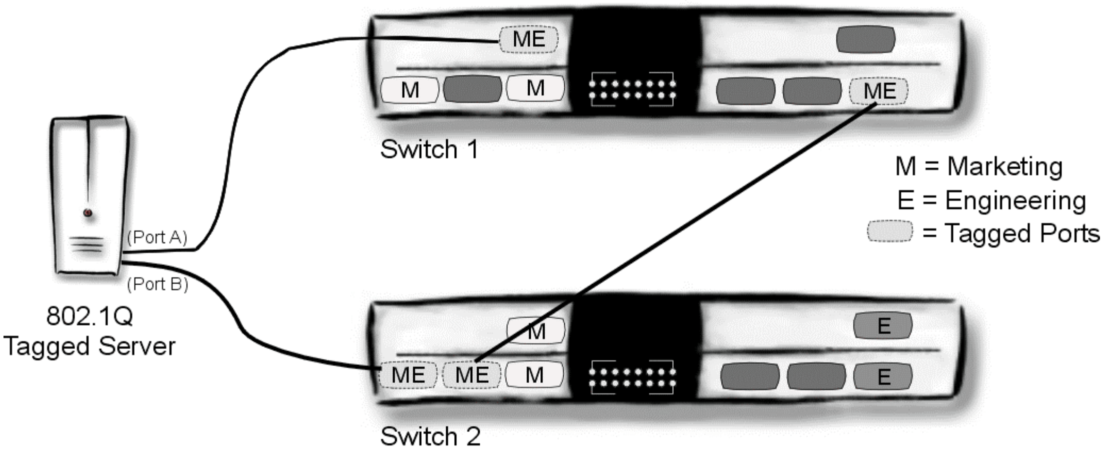

Figure 7. Active port (A) and failover port (B)

4 Glossary

Broadcast Network traffic that is disseminated to all the nodes on a shared-media segment.

Explicit VLAN model VLAN membership is indicated through a tag added to the packet.

Implicit VLAN model VLAN membership is determined by examining information already existing within the packet (the MAC address).

Independent VLAN model One of two explicit VLAN models that are defined in the IEEE standard 802.1Q.

Layer 3 (or: protocol)-based VLANs VLAN membership is determined by examining each packet’s protocol or Layer 3 addressing (IP address).

MAC address-based VLANs VLAN membership is determined through the MAC address of each individual node.

Multicast Network traffic that is disseminated to selected nodes.

Node Each individual computer or other device in a network.

Packet A fixed number of data bits and associated information, including source and destination address formatted for the transfer between nodes.

Port-based VLANs Each port of a switch is assigned to separate VLANs.

Router A device connecting two networks at the Network Layer (Layer 3) of the OSI model that operates as a bridge but can also choose routes through a network.

Segmentation The division of a network into subnetworks.

Shared VLAN Model One of two explicit VLAN models that are defined in the IEEE standard 802.1Q.

Switch A device connecting several network segments at the Data Link Layer (Layer 2) of the OSI model that operates more simply, and at a higher speed, than a router.

Unicast Network traffic between two nodes.

VLAN A logical grouping of network nodes that act as if they were connected in a single network.

Headquarters

SysKonnect GmbH
Siemensstrasse 23
D-76275 Ettlingen

Germany

Phone:	+ 49 7243 502 100
Support:	+ 49 7243 502 330
Fax:	+ 49 7243 502 989

E-mail: sales@syskonnect.de

Americas, Canada,
and Pacific Rim

SysKonnect, Inc.
1922 Zanker Road
San Jose, CA 95112

USA

Phone:	+ 1 408 437 3800
Sales:	+ 1 800 752 3334
Support:	(866) 782 2507
	+ 1 408 437 3857
Fax:	+ 1 408 437 3866

E-mail: info@syskonnect.com

Europe, Middle East,
and Africa

SysKonnect Ltd.
55 Henley Drive
Frimley Green, Camberley
Surrey, Gu16 6NF

United Kingdom

Phone:	+ 44 1 276 453 999
Fax:	+ 44 1 276 453 990

E-mail: sales-uk@syskonnect.de

Visit our web site
www.syskonnect.com