



# KS8695P Application Note

## Using Tag-Based VLAN to support DMZ port

AN119

### Introduction

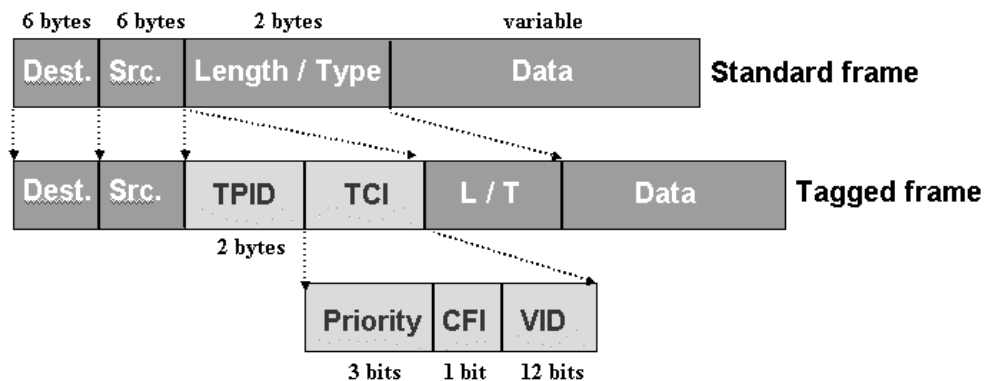
The KS8695P has a built-in 5-port switch that supports both 802.1Q Tag-based VLAN and port-based VLAN. This application note will illustrate how to configure the KS8695P tag-based VLAN feature to support a dedicated DMZ port.

VLAN (Virtual Local Area Network) is commonly used to split up groups of network users into manageable broadcast domains, to create logical segmentation of workgroups, and to enforce security policies among each logical segment.

Regarding IEEE 802.1Q standard, Tag-based VLAN uses an extra tag in the MAC header to identify the VLAN membership of a frame. This tag is used for VLAN and QoS (Quality of Service) priority identification. The VLAN ID associates a frame with a specific VLAN and provides the information that switches need to forward 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) and two bytes of TCI (Tag Control Information)

**Figure 1 Tagged Ethernet Packet**



#### Priority value

Three-bit binary number that specifies a packet's priority. This number can represent eight priority levels, 0 through 7.

#### CFI

A single-bit flag value. If this bit is reset (that is, equal to 0), all MAC address information present in the packet is in canonical format (that is, the simplest form). If this bit is set (that is, equal to 1), E-RIF is present in the 802.3 Ethernet header. Currently, the only packets that are supported are those with CFI equal to 0; therefore, E-RIF is not present.

#### VID (VLAN ID)

An unsigned twelve-bit binary number that identifies the VLAN to which a packet belongs. If the VLAN ID is 0, the tag header contains only priority information.

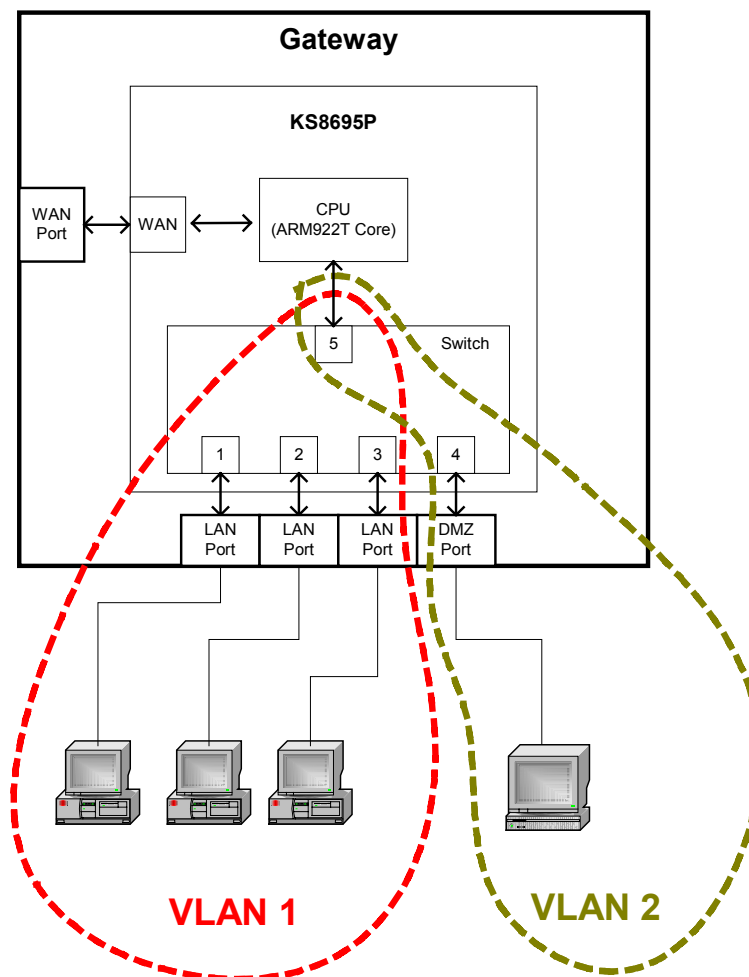
DMZ stands for Demilitarized Zone. A DMZ is a separate ethernet port on a firewall that is used to connect publicly accessed servers to the internet. A publicly accessed server would be an email, web or FTP server.

The main advantage of using a DMZ port is to keep your private network protected from internet users. If a publicly accessed server becomes compromised by a malicious user then that user may be able to access resources on that network LAN segment. By keeping your private LAN on a separate network segment you do not run the risk of the malicious user accessing your private network.

## Scenario

A gateway implemented with the KS8695P is shown in Figure-2.

**Figure-2 KS8695P Gateway Configuration**



Port 1, 2 and 3 are LAN ports. Port 4 serves as the DMZ port. Port 5 is connected to the ARM microprocessor. To achieve the LAN/DMZ separation, we configure two different VLANs. VLAN 1 includes the LAN port 1, 2, 3 and the microprocessor port. VLAN 2 includes the microprocessor port and the DMZ port. This VLAN configuration also solves security integrity issues. With port-based VLAN, broadcast and multicast packets from the microprocessor port (Port 5) are forwarded to both LAN and DMZ ports. This violates our LAN/DMZ separation requirements. With the tag-based VLAN feature, multicast and broadcast packets received in a VLAN are only forwarded to the ports that are members.

The following are the steps for configuring the KS8695P registers to support this tag-based VLAN scenario.

1. Enable the 802.1Q VLAN support.

**Switch Engine Control 1 Register** (SEC1 Offset 0xE804) Bit 4 <= 1

2. Assign port 1, 2, 3, and 5 to VLAN 1

VLAN Table Write (with the 1<sup>st</sup> entry) through

**Indirect Access Control Register** (SEIAC Offset 0xE850) and

**Indirect Access Data Register Low** (SEIAC Offset 0xE85C)

**SEIADL** <= 0x00371001

**SEIAC** <= 0x00000400

3. Assign port 4 and 5 to VLAN 2

VLAN Table Write (with the 2<sup>nd</sup> entry)

**Indirect Access Control Register** (SEIAC Offset 0xE850) and

**Indirect Access Data Register Low** (SEIAC Offset 0xE85C)

**SEIADL** <= 0x00382002

**SEIAC** <= 0x00000400

4. Configure Port 1, 2, and 3 with a default VLAN ID of 1.

The KS8695P Switch will insert the default VLAN ID on untagged packets or packets with a null VLAN ID of the ingress port.

**Port 1 Configuration Register 1** (SEP1C1 Offset 0xE80C) Bit [27:16] <= 1

**Port 2 Configuration Register 1** (SEP2C1 Offset 0xE80C) Bit [27:16] <= 1

**Port 3 Configuration Register 1** (SEP3C1 Offset 0xE80C) Bit [27:16] <= 1

5. Configure Ingress VLAN filtering on port 1, 2 and 3.

This will enable the KS8695P Switch to discard packets with an invalid VLAN ID.

**Port 1 Configuration Register 2** (SEP1C2 Offset 0xE80C) Bit 28 <= 1

**Port 2 Configuration Register 2** (SEP2C2 Offset 0xE80C) Bit 28 <= 1

**Port 3 Configuration Register 2** (SEP3C2 Offset 0xE80C) Bit 28 <= 1

6. Configure Port 4, the DMZ port, with a default VLAN ID of 2.  
This will ensure that the untagged packets coming into the KS8695P switch on the DMZ port will be tagged with a VLAN ID of 2.

**Port 4 Configuration Register 1** (SEP4C1 Offset 0xE80C) Bit [27:16] <= 2

7. Configure ingress VLAN filtering on port 4. This will enable the KS8695P switch to discard packets with an invalid VLAN ID.

**Port 4 Configuration Register 2** (SEP4C2 Offset 0xE80C) Bit 28 <= 1

8. Enable tag insertion on port 5, the microprocessor port. This setting enables the KS8695P switch to insert the default VLAN ID of each untagged ingress packets before it is sent to the microprocessor port. These tags ,along with the source address, tell the microprocessor which port was received from.
9. The microprocessor must tag all packets that are sent to port 5 of the switch. The tag and destination address that the microprocessor inserts in each packet will tell the switch whether to forward the packet to LAN ports or DMZ port.

---

This information is believed to be accurate and reliable, however no responsibility is assumed by Micrel for its use nor for any infringement of patents or other rights of third parties resulting from its use. No license is granted by implication or otherwise under any patent or patent right of Micrel Inc.

© 2003 Micrel Incorporated

---