Weidmüller

Industrial Ethernet Training

Using Weidmueller managed switches for Ethernet/IP

Abstract:
This application note shows the practical application of Weidmüller switches in Ethernet/IP networks, showing how to optimize network performance through IGMP snooping and how to implement DSCP values for QoS.

Hardware reference

No.	Component name	Article No.	Hardware / Firmware version
1	IE-Training Kit-01	2874670000	1.1.2 (Build 125086)
2			
3			

IE-Training Kit Content

No.	Component name	Article No.	Hardware / Firmware version
1	IE-SR-4TX	2751270000	1.6.4
2	IE-SW-AL08M-8TX	2682280000	1.11
3	IE-SW-AL05M-5TX	2682250000	1.16
4	IE-CS-MBGW-2TX-1COM	2682600000	3.14

Software reference

No.	Software name	Article No.	Software version
1			
2			
3			

File reference

No.	Name	Description	Version
1			
2			

Contact
Weidmüller Interface GmbH & Co. KG
Klingenbergstraße 26
32758 Detmold, Germany
www.weidmueller.com

For any further support please contact your local sales representative:
https://www.weidmueller.com/countries

Content

1 Warning and Disclaimer

Warning
Controls may fail in unsafe operating conditions, causing uncontrolled operation of the controlled devices. Such hazardous events can result in death and / or serious injury and / or property damage. Therefore, there must be safety equipment provided / electrical safety design or other redundant safety features that are independent from the automation system.

Disclaimer
This Application Note / Quick Start Guide / Example Program does not relieve you of the obligation to handle it safely during use, installation, operation and maintenance. Each user is responsible for the correct operation of his control system. By using this Application Note / Quick Start Guide / Example Program prepared by Weidmüller, you accept that Weidmüller cannot be held liable for any damage to property and / or personal injury that may occur because of the use.

Note
The given descriptions and examples do not represent any customer-specific solutions, they are simply intended to help for typical tasks. The user is responsible for the proper operation of the described products. Application notes / Quick Start Guides / Example Programs are not binding and do not claim to be complete in terms of configuration as well as any contingencies. By using this Application Note / Quick Start Guide / Example Program, you acknowledge that we cannot be held liable for any damages beyond the described liability regime. We reserve the right to make changes to this application note / quick start guide / example at any time without notice. In case of discrepancies between the proposals Application Notes / Quick Start Guides / Program Examples and other Weidmüller publications, like manuals, such contents have always more priority to the examples. We assume no liability for the information contained in this document. Our liability, for whatever legal reason, for damages caused using the examples, instructions, programs, project planning and performance data, etc. described in this Application Note / Quick Start Guide / Example is excluded.

Security notes
In order to protect equipment, systems, machines and networks against cyber threats, it is necessary to implement (and maintain) a complete state-of-the-art industrial security concept. The customer is responsible for preventing unauthorized access to his equipment, systems, machines and networks. Systems, machines and components should only be connected to the corporate network or the Internet if necessary and appropriate safeguards (such as firewalls and network segmentation) have been taken.

2 Prerequisites

You need to have the following hardware and documentation

- Via Ethernet connected Industrial Ethernet Training Kit
- Application Note Industrial Ethernet Training 01 "*Setting up default configuration of IE Training Kit*" for applying default IP address configuration

Note: *The mentioned Prerequisites are only mandatory for performing the exact use case we are exemplifying in this Application Note. These are optional, if you only want to understand the functionality of the following Application and implement it by yourself.*

Note: *Additional information and tutorial videos to this Application Note can be found in the Weidmueller support center (*Weidmüller - Support Center (weidmueller.com)). These videos can also be found by searching for "*Industrial Ethernet tutorials"* in the support center.

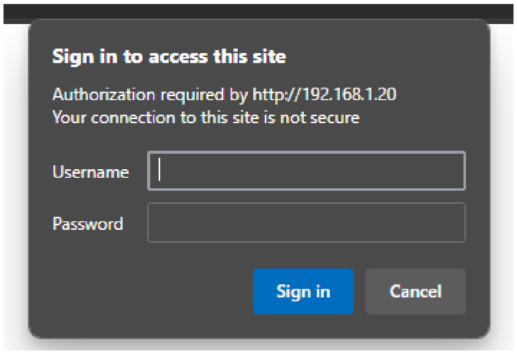
3 Introduction to EtherNet/IP

Ethernet/IP is an industrial protocol based on the application layer of the Open Systems Interconnection model and utilizing the Common Industrial Protocol for that. This means that EtherNet/IP is the way how data is stored and organized in an IP packet. This allows the users to deploy standard Ethernet technology in industrial automation applications using managed switches and different network topologies like a star topology. Moreover, the user has access to different functionalities to improve network performance, like QoS using DSCP values which prioritizes important traffic in the network, and also IGMP snooping, which helps to mitigate and group multicast traffic for the addressed devices to avoid general congestions in the network traffic.

4 Configuring IGMP snooping

An important feature for EtherNet/IP is IGMP snooping. With IGMP snooping, one is able to control and limit multicast and broadcast traffic in a network. Instead of flooding the network by sending packets to devices not addressed by them, traffic is grouped and directed automatically via the IGMP snooping protocol to devices, that send a join request to the multicast traffic stream.

1. Login in to the 8-port managed switch with the IP 192.168.1.20 using the corresponding credentials.
   Note that a managed switch is needed for EtherNet/IP functionality.



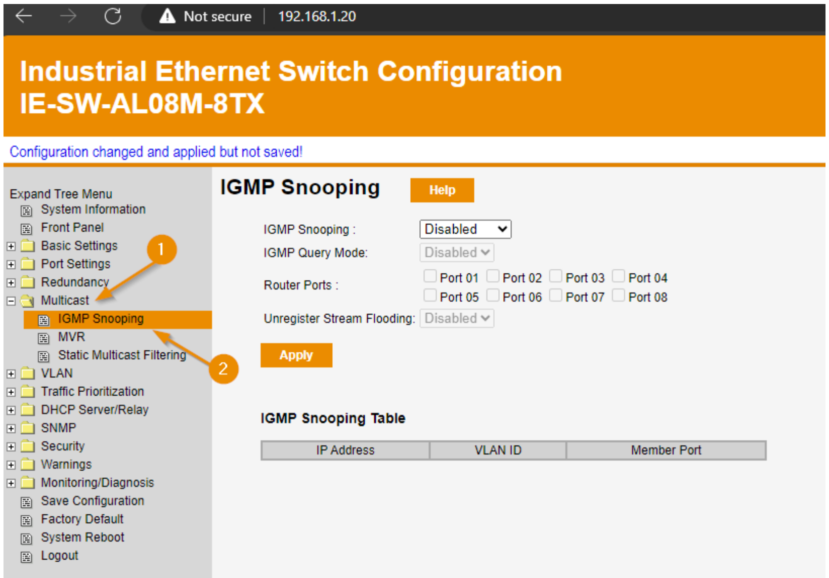
Sign in to access this site

Authorization required by http://192.168.1.20
Your connection to this site is not secure

Username
Password

Figure 1: Login to the switch

2. Navigate the menu tree to "*Multicast*" and select the "*IGMP snooping*" option.



Not secure | 192.168.1.20

Industrial Ethernet Switch Configuration
IE-SW-AL08M-8TX

Configuration changed and applied but not saved!

IGMP Snooping

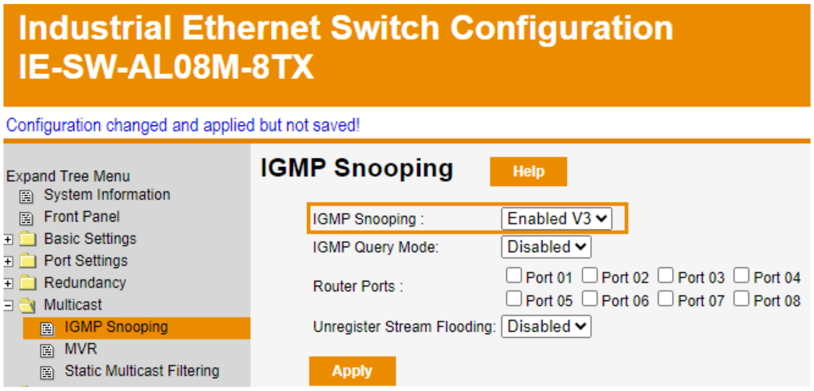
IGMP Snooping : Disabled
IGMP Query Mode: Disabled
Router Ports : □ Port 01 □ Port 02 □ Port 03 □ Port 04 □ Port 05 □ Port 06 □ Port 07 □ Port 08
Unregister Stream Flooding: Disabled

IGMP Snooping Table

IP Address	VLAN ID	Member Port

Figure 2: IGMP snooping menu

3. Enable IGMP snooping and select “*Enabled V3*” in the drop-down menu. IGMP snooping V3 is the newest version with the most functionalities. Moreover, it is backward compatible with IGMP snooping v2.



Industrial Ethernet Switch Configuration
IE-SW-AL08M-8TX

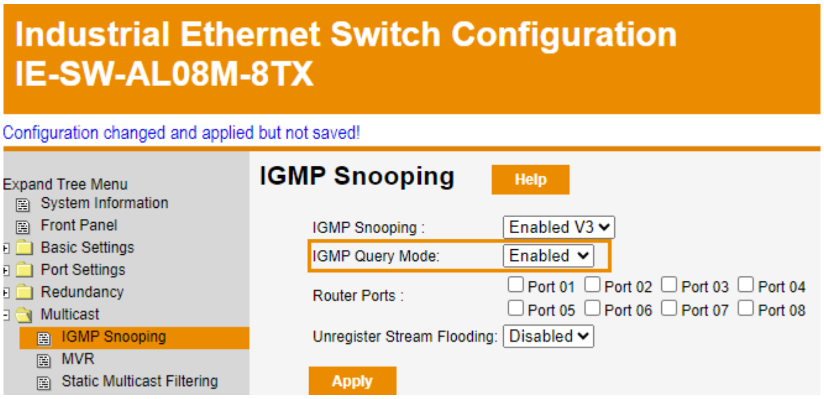
Configuration changed and applied but not saved!

IGMP Snooping

IGMP Snooping : Enabled V3
IGMP Query Mode: Disabled
Router Ports : □ Port 01 □ Port 02 □ Port 03 □ Port 04 □ Port 05 □ Port 06 □ Port 07 □ Port 08
Unregister Stream Flooding: Disabled

Figure 3: Enabling IGMP snooping

4. To use IGMP snooping, an IGMP querier is needed that sends IGMP general queries to all hosts and devices on the local subnet to check for the existence of multicast group members. In this case, the 8-port switch is the querier and needs to be enabled in the option “*IGMP Query Mode*”.



Industrial Ethernet Switch Configuration
IE-SW-AL08M-8TX

Configuration changed and applied but not saved!

IGMP Snooping

IGMP Snooping : Enabled V3
IGMP Query Mode: Enabled
Router Ports : □ Port 01 □ Port 02 □ Port 03 □ Port 04 □ Port 05 □ Port 06 □ Port 07 □ Port 08
Unregister Stream Flooding: Disabled

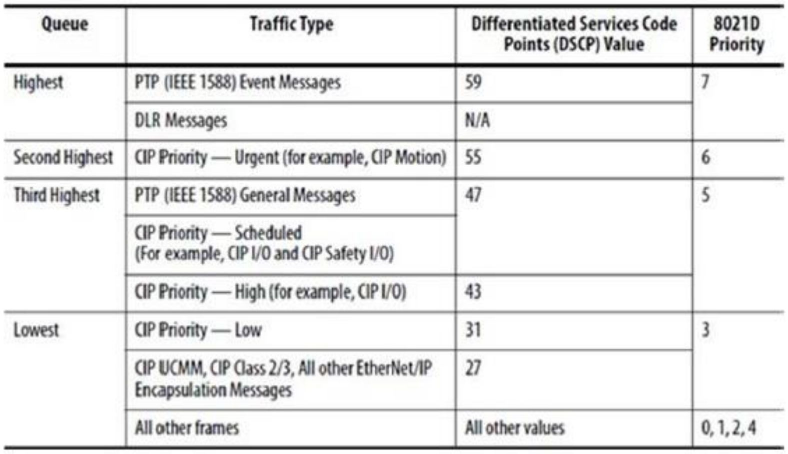
Figure 4: IGMP Query Mode

5. To complete the configuration, select the router ports. These are the ports, where the multicast traffic is sent from. In this case, it is port 5. Moreover, you can select to either enable or disable stream flooding.

5 Configuring DSCP values

Differentiated Service Code Point (DSCP) values are used to classify certain packets to provide quality of service (QoS) on the network. This can be used to reduce latency for important network traffic while maintaining a best-effort service to non-critical traffic like file transfers.

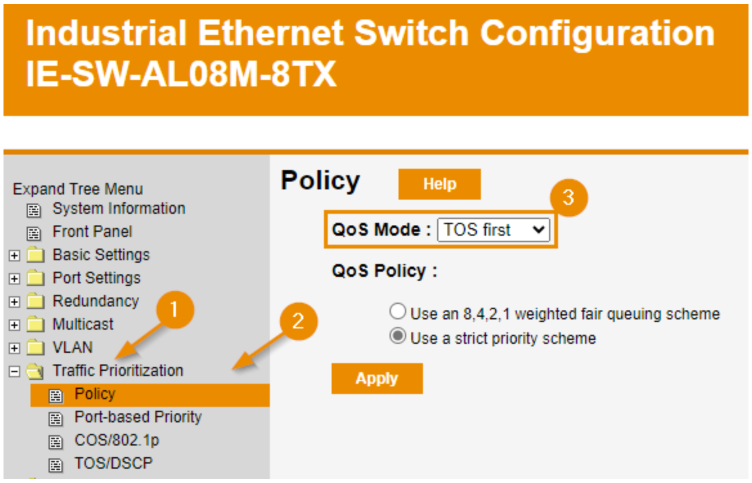
1. The picture below shows the table with four priority queues. The different traffic types are mapped to specific DSCP values which indicate what priority the traffic has.
   For example, PTP Event messages have a DSCP value of 59, meaning that these are considered to have the highest priority in the network whereas PTP general messages are considered as third highest priority.



Queue	Traffic Type	Differentiated Services Code Points (DSCP) Value	8021D Priority
Highest	PTP (IEEE 1588) Event Messages	59	7
	DLR Messages	N/A	
Second Highest	CIP Priority — Urgent (for example, CIP Motion)	55	6
Third Highest	PTP (IEEE 1588) General Messages	47	5
	CIP Priority — Scheduled (For example, CIP I/O and CIP Safety I/O)		
	CIP Priority — High (for example, CIP I/O)	43	
Lowest	CIP Priority — Low	31	3
	CIP UCMM, CIP Class 2/3, All other EtherNet/IP Encapsulation Messages	27	
	All other frames	All other values	0, 1, 2, 4

Figure 5: Assigned DSCP values switch

2. To implement these values, go to "*Traffic Prioritization*", click on "*Policy*" and put the "*QoS Mode*" on "*TOS only*".



Industrial Ethernet Switch Configuration
IE-SW-AL08M-8TX

Policy

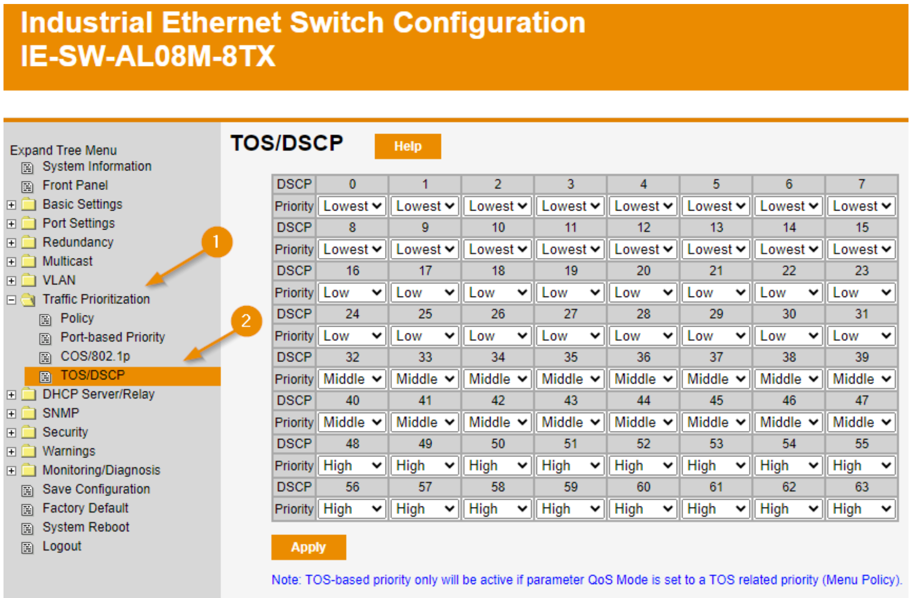
QoS Mode : TOS first

QoS Policy :

○ Use an 8,4,2,1 weighted fair queuing scheme
● Use a strict priority scheme

Figure 6: QoS Policy configuration

3. After activating TOS policy, go to “*Traffic Prioritization*” and select “*TOS/DSCP*”.



Industrial Ethernet Switch Configuration
IE-SW-AL08M-8TX

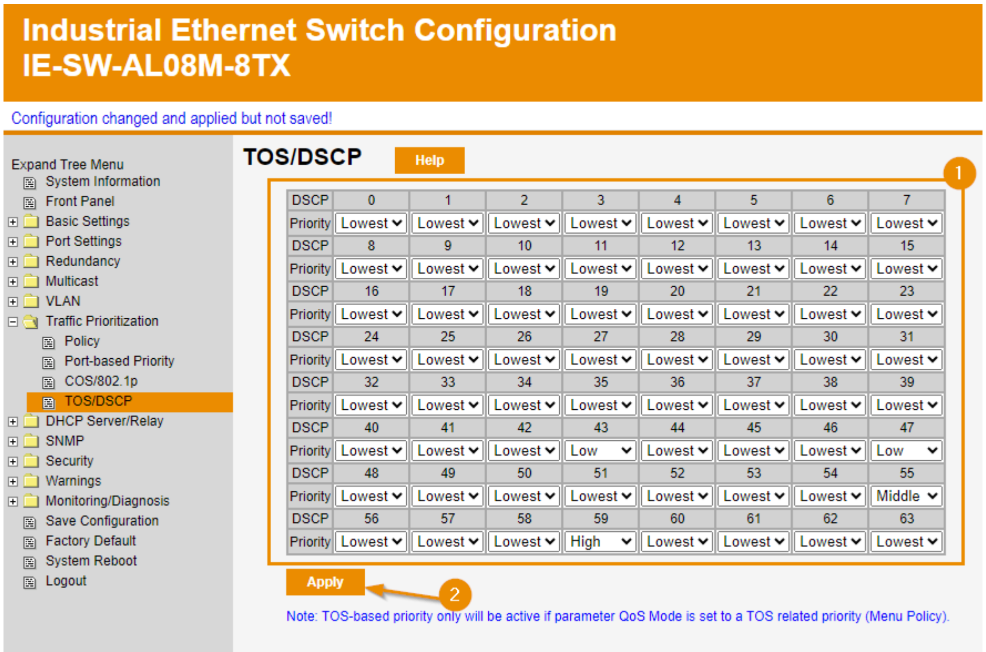
TOS/DSCP

DSCP	0	1	2	3	4	5	6	7
Priority	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest
DSCP	8	9	10	11	12	13	14	15
Priority	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest
DSCP	16	17	18	19	20	21	22	23
Priority	Low	Low	Low	Low	Low	Low	Low	Low
DSCP	24	25	26	27	28	29	30	31
Priority	Low	Low	Low	Low	Low	Low	Low	Low
DSCP	32	33	34	35	36	37	38	39
Priority	Middle	Middle	Middle	Middle	Middle	Middle	Middle	Middle
DSCP	40	41	42	43	44	45	46	47
Priority	Middle	Middle	Middle	Middle	Middle	Middle	Middle	Middle
DSCP	48	49	50	51	52	53	54	55
Priority	High	High	High	High	High	High	High	High
DSCP	56	57	58	59	60	61	62	63
Priority	High	High	High	High	High	High	High	High

Note: TOS-based priority only will be active if parameter QoS Mode is set to a TOS related priority (Menu Policy).

Figure 7: TOS/DSCP menu

4. With the provided table, we can configure the values accordingly, meaning that the corresponding values need to be configured using the drop-down option “*Priority*”. For example, the DSCP value 59 can be left on priority “*High*” whereas DSCP value 47 needs to be changed to priority “*Low*”. Every other unassigned value needs to be set to “*Lowest*” to ensure the functionality.
Repeat these steps for every value from the provided table above and click on “*Apply*”.



Industrial Ethernet Switch Configuration
IE-SW-AL08M-8TX

Configuration changed and applied but not saved!

TOS/DSCP

DSCP	0	1	2	3	4	5	6	7
Priority	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest
DSCP	8	9	10	11	12	13	14	15
Priority	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest
DSCP	16	17	18	19	20	21	22	23
Priority	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest
DSCP	24	25	26	27	28	29	30	31
Priority	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest
DSCP	32	33	34	35	36	37	38	39
Priority	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest
DSCP	40	41	42	43	44	45	46	47
Priority	Lowest	Lowest	Lowest	Low	Lowest	Lowest	Lowest	Low
DSCP	48	49	50	51	52	53	54	55
Priority	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Middle
DSCP	56	57	58	59	60	61	62	63
Priority	Lowest	Lowest	Lowest	High	Lowest	Lowest	Lowest	Lowest

Note: TOS-based priority only will be active if parameter QoS Mode is set to a TOS related priority (Menu Policy).

Figure 8: Configuring DSCP Values

6 Results

The device is ready for EtherNet/IP applications using important features like IGMP snooping and Quality of Service with DSCP Values. Multicast traffic is now addressed only to devices that want to join in this traffic stream meaning that unnecessary multicast traffic throughout the network is avoided, meaning there is more bandwidth available. Lastly, important traffic tagged with the corresponding DSCP values is now queued based on the correct priorities and does not starve when there is a high network load.