User Manual

MG205X

Draft 1.0

Wohlenbergstraße 3, 30179 Hannover,
Germany
www.dzsi.com / DZS @ email / (+DZS) contact number

Copyright

Disclaimer

DZS, Inc. makes no representation or warranties with respect to the contents hereof, and specifically disclaims any implied warranties of merchantability or fitness for a particular purpose. Further, DZS, Inc. reserves the right to revise this publication and to make changes from time to time in the contents hereof without obligation of DZS, Inc. to notify any person of such revision or changes.
Changes and enhancements to the product and to the information herein will be documented and issued as a new release to this manual.

Release for Update

Summary: Issue 1

Draft release

Details:

Chapter/Section	Reasons for update
All	Draft release

Version history

Status	Date of release	Reasons for change
Draft 1.0	2021/05/03	Draft release

◈ Contents ◈

Overview

This user manual describes overall MG205X introduction and setting procedures. Detailed explanations and examples are included for easier understanding of MG205X.

This user manual is for setup of MG205X and provided for network manager. So, the network manager needs to have professional knowledges of network equipments and experiences of LAN installation and operation.

This chapter is composed of following contents.

- Document structure
- Symbols
- Notation

1.1 Document structure

▣ **Product introduction:** MG205X functions and features are introduced.

▣ **Using CLI:** It introduces structure of DSH commands and basic usage briefly.

▣ **System interface and IP address setting:** It explains system interface related information and IP address setting method for network communication.

▣ **Port Default Settings:** This introduces basic parameter setting method of Ethernet ports and G.fast port of MG205X, and setting methods of port mirroring.

▣ **System environment:** This introduces basic environment setup, setting management, system check.

▣ **Network management function setting:** This introduces network management function settings including SNMP, Syslog, and packet filtering etc.

▣ **System main functions setting:** This introduces setting methods of VLAN, STP(Spanning Tree Protocol), IP multicasting etc.

▣ **Multicast setting:** This describes multicasting setting methods.

▣ **G.fast CPE setting:** This describes remote setting method of G.fast CPE.

▣ **Appendix A. System Image Installation:** It explains how to install new system image to existing equipment.

1.2 Symbols

Warning

This indicates the matters that must not be performed. Failing to comply with this warning may result in death or injury to the user. In addition, it indicates that significant physical damage may occur.

Attention

This mark prohibits actions indicated. Or, attentions to be advised.

Reference

This shows the references for setting commands.

1.3 Notation

◈ Commands notation of console terminal

Commands notation of MG205X console terminal are shown in Table 1-1. Use recognize the meaning of commands correctly, and use it for the right purpose.

【Table 1-1】Console Terminal Commands Notation

Notation	Meaning
a	Command that must be keyed-in as prescribed is indicated by a lowercase (small letter) alphabetic characters.
A	Variables to be keyed-in by user are written in capital letter.
[ ]	Selectable commands, depending on the user's judgment or variables are indicated in square brackets [ ].
< >	Range of numbers that can be entered will be shown in angle brackets < >.
( )	Among the many variables, that must be selected to be entered will be shown in parentheses ( ).
|	Selectable variables are shown with vertical |

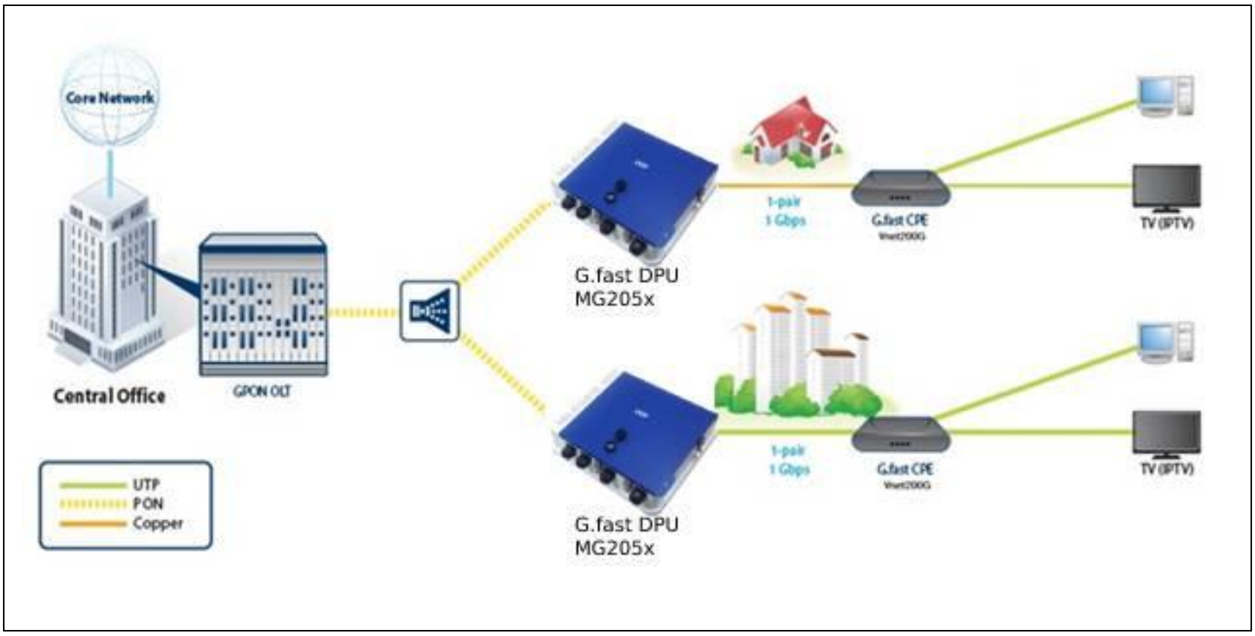
2. Product Introduction

MG205X is a device that provides Gigabit level G.fast service in copper standard lines. MG205X is a product developed to provide an image of the Ultra-HDTV grade, which was not possible from conventional xDSL. In addition, service is well prepared with flexibility for the distance, and is capable of high-speed data communications in 300m range. Layer2 Gigabit Ethernet supporting MG205X can provide high-quality multimedia services and high-speed and high-capacity services.

MG205X can implement G.fast service interface based on TDD scheme using the same frequency for uplink and downlink, and the transmission rate of the uplink and downlink service can be varied.
In addition, 10/100/1000BASE-T (2 ports) and 1000BASE-X SFP/10G SFP+ (2 ports) are used as selective uplink options.

On the other hand, MG205X ensures stable communication network with a Layer 2 MG205X, and provides the intelligent services such as QoS, security ACL (Access Control List), multicast management for establishing a high-performance network. In addition, RADIUS, TACACS +, and 802.1x are supported to limit user access, and higher security level is provided by supporting SSH to encrypt the data sent and received via SSH.

Here is an example of network configuration using MG205X.



【Picture 2-1】An example of MG205X Network Configuration

2.1 Key Features

MG205X equipped with a Layer 2 MG205X offers a variety of features of QoS, IP multicasting, STP, VLAN and more. Without rebooting, the setting contents of user are applied, and monitoring the status of equipment is done by syslog and SNMP. Also, automatic detection and alerting for duplicate IP addresses and MAC addresses are possible.

The following are the key features of MG205X.

- **CLI based DSH**

Users can set up and monitor a MG205X or full MG205X group using DSH consisting of statements by the command format. User can use DSH by PC with console terminal program and MG205X Console or by Telnet service.

- **QoS (Quality of Service)**

In a typical network environment, if the traffic is over-loaded, user's data can be lost (dropped) automatically. But QoS-supported MG205X divides the traffic into several grades by IEEE 802.1p CoS standards, and re-establish a procedure for each grade (reprioritize). QoS prevent the loss of data by placing the priority on sensitive data, and provides differentiated bandwidth for each packet to avoid transmission delays.

- **Multicast communication**

MG205X supports multicast communication with IGMP Snooping and IGMP Querier functionality. Multicast communication can prevent the overload phenomenon from unnecessary packet because the packets are sent only to the hosts that need it.

- **SNMP (Simple Network Management Protocol) / RMON (Remote Monitoring)**

The MG205X equipped with SNMP functionality can be checked and monitored remotely. MG205X supports SNMP version 1 and 2 and four groups of RMON, and administrator can check statistics at any time.

- **DHCP Server and Relay functionality**

MG205X supports DHCP function to give an IP address automatically to the client, and enables user to utilize the limited network resources more efficiently. In particular, the DHCP server manages IP addresses from a center and reduces network management costs.

- **VLAN (Virtual Local Area Network)**

VLAN is virtual LANs which is divided from a network logically by network administrator. VLAN is physically on the same network. and depending on the settings, it has high security effect as well as economic advantages of the bandwidth because it can send and receive packets only in the same network area. MG205X can configure the VLAN Up to 256 per system.

- **Stacking**

In MG205X group, master MG205X has 1 IP address, and slave MG205X can be set-up, managed and monitored. This function is useful to save IP resources because several MG205X systems can be managed by 1 IP address.

- **Link aggregation**

MG205X supports port trunking functionality that multiple physical interfaces are integrated into 1 logical port (aggregate port). Port Trunking integrates interfaces based on the same speed, same duplex mode and the same VLAN ID. MG205X can set 6 integrated port which covers up to eight ports based on IEEE 802.3ad standard to reduce traffic and improve disaster recovery capabilities.

- **Bandwidth setting (Rate-limit)**

MG205X provides each port with differentiated bandwidth. By providing a differential bandwidth according to the user's requirements, ISP operators can have efficient and economical line management as well as differentiated rate costs.

- **Flood Guard Set**

Other than Rate Limit which limits the number of packets by bandwidth setting, flood guard function of MG205X provides packet adjustment by limit of packets which can accommodate in one second.

- **STP(Spanning Tree Protocol)**

STP is a network management protocol to prevent a loop continues to occur on the network. It helps you keep the traffic speed because it prevents useless loop. MG205X STP has this feature.

- **PVST(Per VLAN Spanning Tree)**

MG205X supports PVST (Per VLAN Spanning Tree) that STP is operated independently for each VLAN. Using PVST (Per VLAN Spanning Tree), you can prevent whole network failure (down) by a loop because each STP is working on each VLAN.

- **RSTP(Rapid Spanning Tree Protocol) (802.1w)**

MG205X also supports RSTP (Rapid Spanning Tree Protocol) in accordance with IEEE 802.1W standard, and it enables reliable and flexible network configuration from the Metro Ethernet environment or existing RING P-to-P environment. RSTP is developed to reduce STP Reconvergency time in small-scale MG205X network, and it reduces fail over time dramatically in a Layer 2 MG205X with redundant link.

- **802.1x-based user authentication**

MG205X can set the user authentication policy based on the IEEE 802.1x on a port-by-port basis. 802.1x based user authentication port can be used only by user who are authorized by RADIUS server, it increases the security of network management and mobility.

- **SSH Server**

MG205X can increase security for TELNET, FTP services by activating the (Secure Shell) SSH server.

- **RADIUS and TACACS+**

MG205X support user authentication protocol as RADIUS (Remote Authentication Dial-In User Service) and Tacacs + (Terminal Access Controller Access Control System +). In addition to the registered user ID and Password to MG205X, MG205X has enhanced security of the system management and network administration because the server requires authentication through RADIUS and TACACS + server.

- **Storm Control**

Storm is a phenomenon of network time-out which happens from a large amount of a particular packet occupying the most of the transmission capacity. MG205X support the Storm Control that Drops broadcast packets, multicast packets, and DLF packets in excess of the limit during the time set by the user.

2.2 Product Specifications

Items	MG205X
CPU	ARMCPU
Flash memory	256MB
System memory	512MB SDRAM
Service ports	G.Fast 4/8/16ports, Terminal block (MG2051 : 4port, MG2052 : 8port, MG2053 : 16Port)
Uplink ports	Fixed SFP uplink for 1G/10G AON or xGPON
Console port	1 console port (RS232 - RJ-45 connector)
MGMT port	1 port 100/1000BASE-TX (RJ-45 connector)
Power input	AC97-264V, 50~60Hz
Power output	DC 15.4V, 3A (Max 46.2W)
Power consumption	Max. 40W
Operating temperature.	-5~45°C (23~113°F)
Storage Temperature	-20~70°C (-4~158°F)
Humidity	0~90%(non condensing)
Dimension(W * H * D)	380mm x 340mm x 112mm

【 Table 2-2 】 MG205x Specification

2.3 Safety information

This manual describes information and instructions for safe usage of products to prevent any damage or injury to the property or body of users or others. This system should be installed and managed only by experienced technicians who fully understand how to use this product after completely understanding the contents of this manual. This manual describes overall cautions for installation and operation of the product.

(1) Warning in handling

Do not disassemble, remodel and repair.
Disassembling this product may result in personal or material damages due to electric shock or failure.

Do not drop or give strong impact on the product.
Damaging inside may result in fire or electric shock during use.

Do not insert foreign materials inside.
If foreign materials are inserted inside, turn off the power immediately, remove the power cable, and contact the designated customer center. If you keep using the product while foreign substance is inserted inside, it may result in fire or electric shock.

Do not touch the product with wet hands.
It may result in fire or electric shock. If water comes inside, immediately remove power cable and contact the designated customer center. It may result in fire or electric shock if you keep using.

Do not block the vent of product.
It will raise the temperature inside and result in fire or electric shock.

Remove all power plugs and TNV connections prior to open the unit.

(2) Power Supply

Do not use power voltage other than designated.
It may result in fire or failure.

Connect the power cable firmly to the power outlet.
If you keep using the product while the power cable is improperly connected to the power outlet, it may

result in a fire or electric shock.

Do not use power wiring with too many equipment connected when you connect the power cable of this product.
It may result in fire or a problem in the product performance.

Do not cut or damage power cord or cable.
It may result in fire or electric shock if you keep using the product while cable or cord is damaged.

(3) Smoke, Thunderstorm

If you notice a smoke comes out from the product, immediately remove the power cable connected to this product.
It may result in fire or electric shock if you keep using. Contact the designated customer center.

Do not expose the product or cables connected to the product to lightning.
It may result in severe personal or physical damages such as electric shock or failure of product. Be careful not to expose product to dangerous environment which may result in lightning damage. Install surge protection system.

(4) Electromagnetic Wave

Make sure to install and operate the product in the way that electromagnetic wave does not affect the product and cable.
Electromagnetic wave may cause abnormal operation or deteriorate the system performance.

(5) Power

Take out the power cord if you do not use it for a long period of time.
It may result in electric shock or electric leakage by insulation deterioration.

Do not pull out the power cord with excessive force.
If you pull out power cord strongly, some part of power cord may be broken and result in generating heat or fire.

(6) Installation place

Do not install the product where IP43 grade can’t protect the device.

This product is designed for indoor use only and not for outdoor applications. For outdoor application, please simulate it first as there are various factors affecting the performance of the system.

Do not install the products at the place with high temperature or exposed to direct sunlight, or near the heat generating devices.

It may result in fire due to high temperature or in the problem in product operation.

Do not use it at the place near cooler or heater where temperature changes abruptly.

If abrupt temperature change occurs, dew may form inside the product, resulting in fire or electric shock.

Do not use it at too dry or humid place.

Too high humidity may result in fire or electric shock. If it is dry too much, it may result in electric shock or fire.

Use it at the well-ventilated place.

If you use it at the place where ventilation is improper, it may raise the heat inside and result in fire or failure.

Do not install at unstable and high place.

It may fall down and suffer impact, resulting in failure of the product.

(7) Cautions in moving and installing MG205X

Do not move or transport this product carelessly.

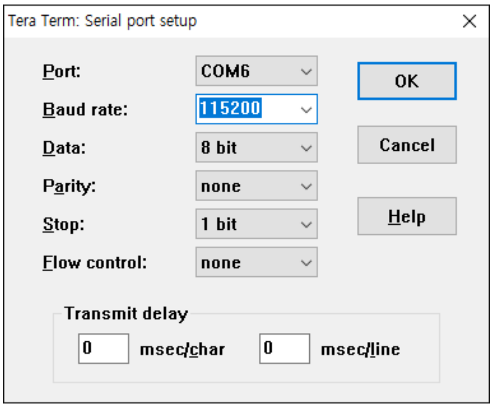
Since this product is not designed for easy transportation, special caution is required when transporting or installing the product. Special care is required not to give excessive power when transporting product. Be careful not to fall down the product. If the product falls down, it may cause problem in operation of product.

2.4 Installation

2.4.1 Tools and Device required

Following components and tools are needed to install MG205X Components and Tools which are not provided at the time of system purchase shall be prepared by the installer:

- MG205X system
- MILEGATE-205x installation manual
- Cross(+) type screw driver
- Interface cables to be connected to service ports
  - G.fast port: Twisted Cable(above CAT3 class)
- Uplink port and interface cable
  - 1000BASE-X or 1/10G PON SFP module and SC fiber cable
- RJ-45-to-DB-9 cable to be connected to console port
- RJ-45-to-RJ-45 cable to be connected to MGMT port
- Power cable (Terminal Block Type)
- Protective earth cable
- Ethernet MILEGATE-205x or PC to be connected to Ethernet port
- Console terminal with settings of 115200baud, 8 data bits, no parity, 1 stop bits, flow-control-none (Please refer to following 【 **Picture 2-6** 】)



Tera Term: Serial port setup

Port: COM6
Baud rate: 115200
Data: 8 bit
Parity: none
Stop: 1 bit
Flow control: none

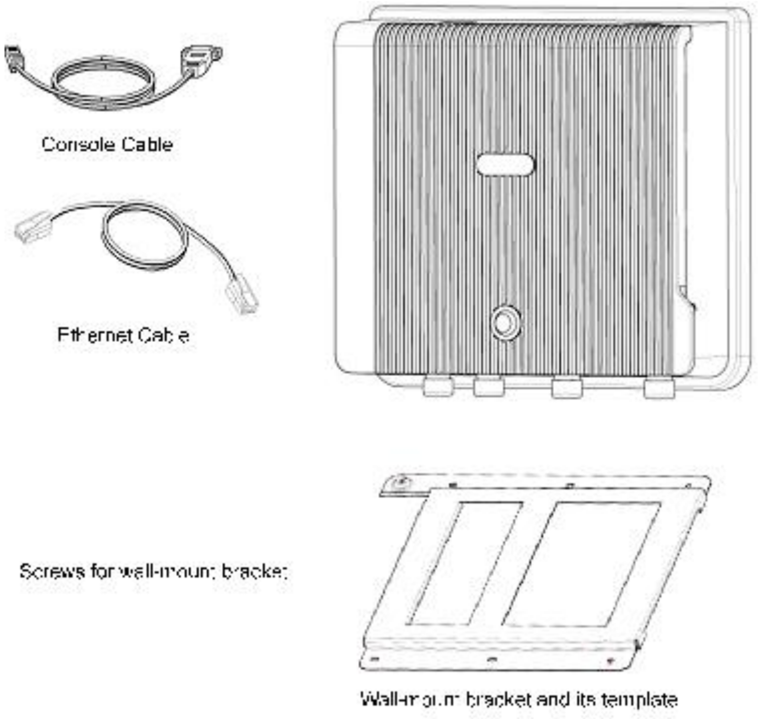
Transmit delay
0 msec/char 0 msec/line

【 **Picture 2-6** 】 **Serial port setting of console terminal**

2.4.2 Product Components

Check the components of the system you purchased before installing MG205X G.Fast System. Following components should be included:

- MG205X
- 1 x Metal bracket for wall mounting
- 7 x Screw for wall mounting bracket
- 1 x Paer template for wall mount bracket
- 1 x CATV Conveter cable


Console Cable
Ethernet Cable
Screws for wall-mount bracket
Wall-mount bracket and its template

【Picture 2-2】Product Components of MG205X

2.4.3 Installation Place

MG205X is designed to mount on the wall and the wall-mount bracket provided in the product package shall be fixed on the wall using the screws provided in the package prior to mounting the MG205X on the bracket.

Pay specially attention on following matters regarding installation place.

Install the product at the place where easy power connection and cable wiring are possible. Avoid to install the product at the place where water flow or moisture possibly affects the equipment.

Install the product at the indoor environment only (not outdoor) where temperature does not go below 5 degree C or above 45 degree C.

Do not place the separate device or object that may block the flow of air around the equipment.

2.4.4 Installation to wall-mount

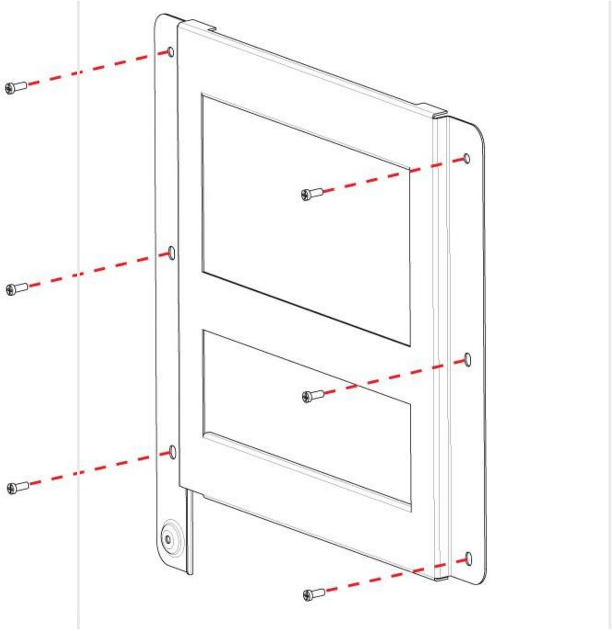
Be careful of the following with regard to the power.

- Make sure that the power supply is properly grounded with protective earthing.
- System power should be connected to the grounded power source.
- Power outlet should be near the system and easily accessed.
- System operator can disconnect power source of the MG205X by pulling out power cord from an outlet.
- System performance may differ depending on power status. If there is too much noise or sparks, it is recommended to install separate power control equipment.
- Make sure to turn off the power MG205X Before pull out the power cord from the system.

MG205X shall be installed on the wall. Follow steps below for installation.

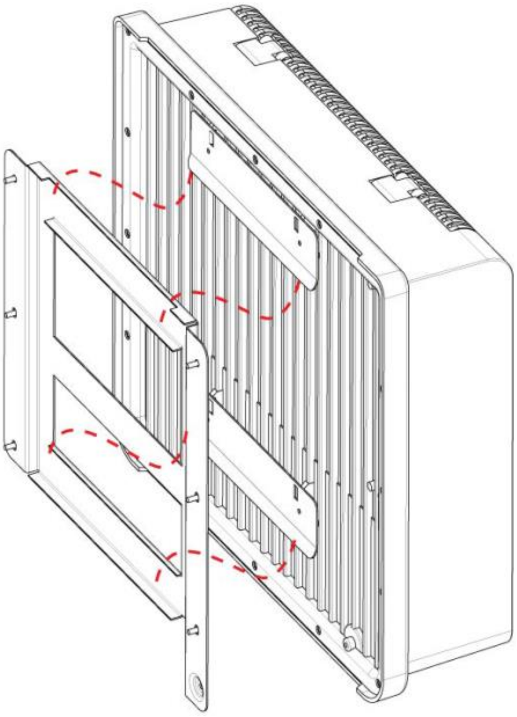
(1) Check the components provided.

(2) Once proper installation place is decided, start the installation of MG205X. To mount MG205X on the wall, the wall-mount bracket provided with product package shall be fixed on the wall first. Use the paper template to mark position of mounting holes on the wall.



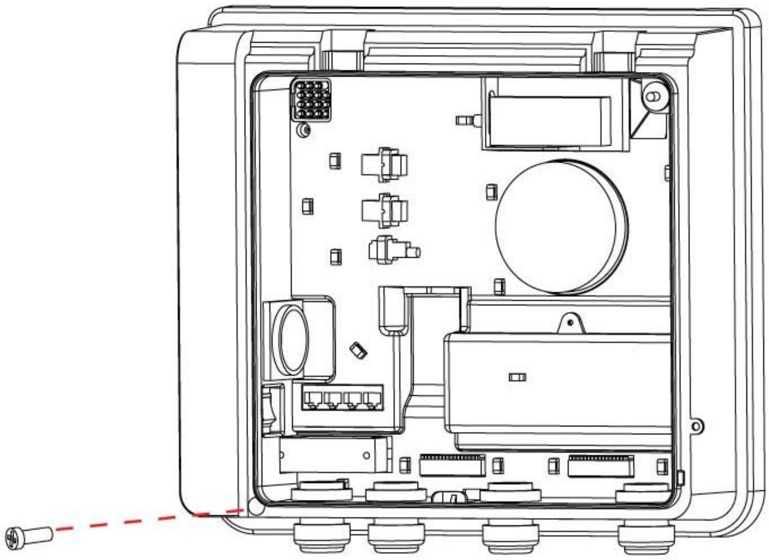
【Picture 2-3】Wall-mount Bracket of MG205X

(3) Mount MG205X on the wall-mount bracket as shown below.



【Picture 2-4】Wall-mount Bracket of MG205X (2)

(4) Fasten MG205X to the wall-mount bracket using the screw provided in the product package as shown below.



【Picture 2-5】Wall-mount Bracket of MG205X (3)

(5) For safety reasons, connect the earth wire to the ground terminal block located in the lower left part of MG205X. When installing the unit, the ground connection must always be made first and disconnected last.

(6) Connect power cord and turn the power MG205X on and check the indication of power LED is normal.

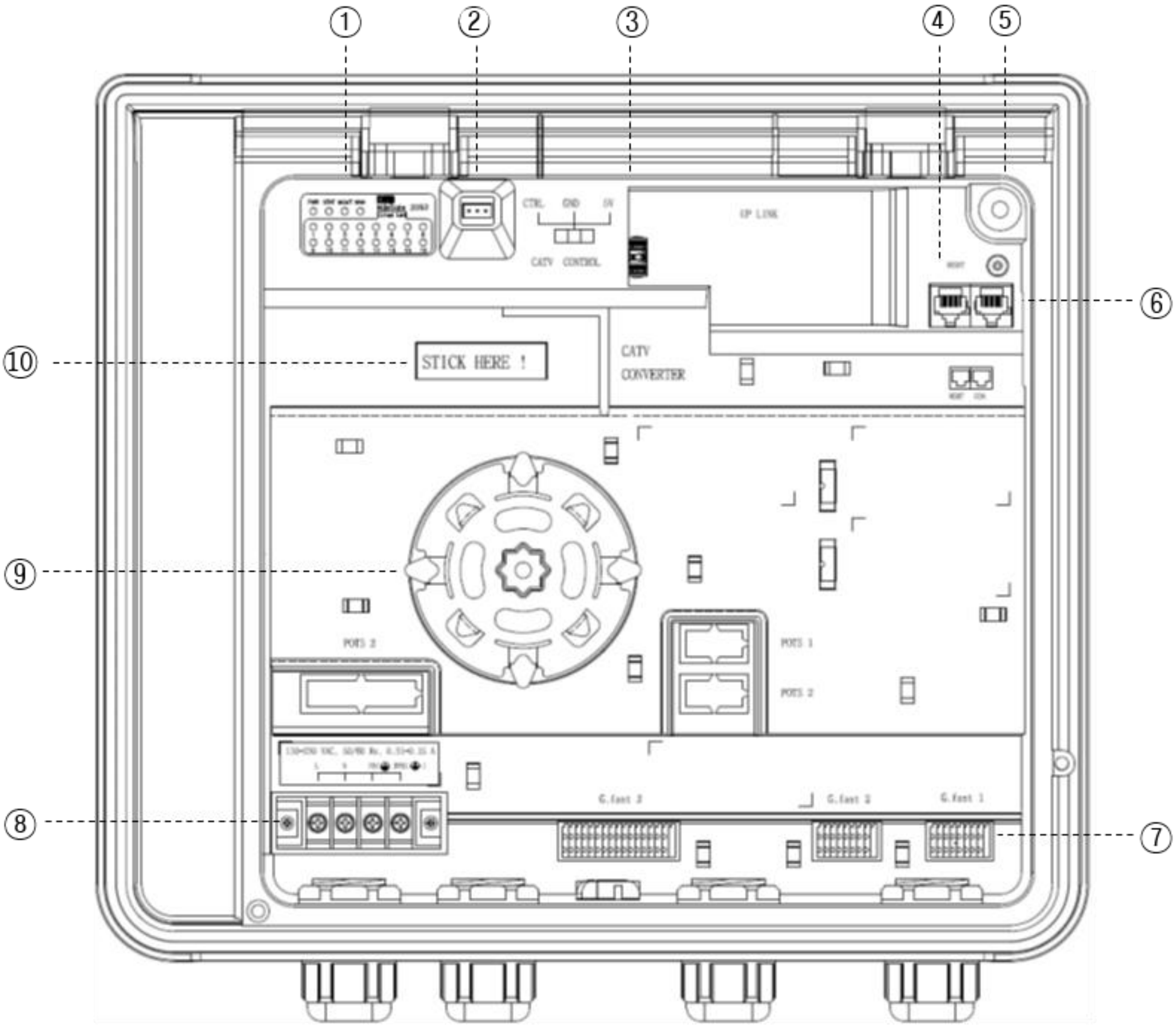
(7) It is recommended to turn the power MG205X off before optional uplink board installation for the first time for the safety.

(8) In case that it is required to set and check the system, connect console port of MileGate2011 to operation terminal.

(9) Turn the power MG205X on and check if the power LED is on and other LEDs of various I/O interface modules are properly operated.

2.4.5 System Front View

Following shows the components of the front panel of MG205X after opening the front cover.



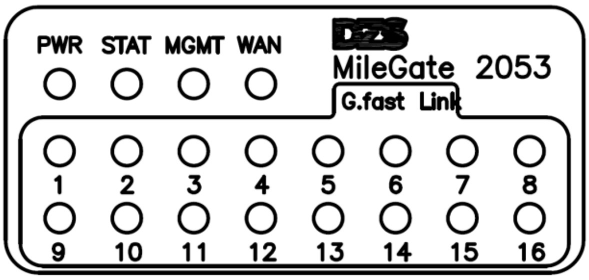
【Picture 2-7】Front View of MG205X

① **System LED**	LEDs show ⑩status of system/G.fast operation.
② **CATV connector**	CATV connector to be connected to CATV converter

③ **Uplink port**	Uplink module can be inserted into the port
④ **MGMT port**	Equipment management port without effect to system performance.
⑤ **Door button**	The button monitor door open or instrusion.
⑥ **Console port**	Console terminal can be connected to equipment through this port.
⑦ **G.fast(RJ21)**	The ports to be connected to subscriber CPE.
⑧ **Terminal Block**	AC power input terminal
⑨ **Fiber handling**	Mechanical handling of optical fibre
⑩ **CATV Converter fixation**	CATV converter fixation location.

【 Table 2-2 】 MILEGATE-205x front configurations

MG205X supports LED indicators for such status of Power, System, MGMT port link, Uplink port link and VDSL line. The following table shows the description of each LED indicator in MG205X.



【Table 2-1】LED Indicators of MG205X

LED	Color	Status	Function description
PWR	Green	On	Power supply of system is on.
		Off	Power supply of system is off.
STAT	Green	ON	System is booting.
		Blinking	System operates in normal mode after booting.
		Off	Power is off or System is overloaded with high CPU load more than 70%.
MGMT	Green	On	Link is normally established.
		Blinking	Link is established and data is being transmitted.
		Off	Power is off or link is not established.

WAN	Green	On	Link is normally established or Data is being transmitted.
		Off	Link is not established.

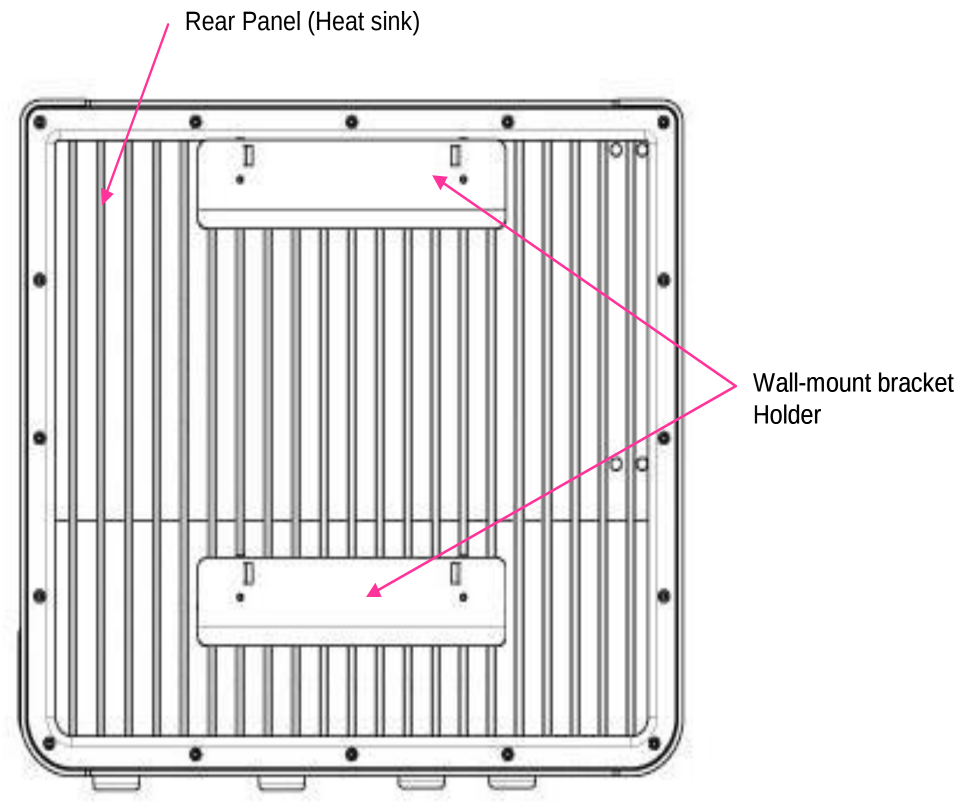
【 Table 2-3 】System LED configuration

LED	Color	Status	Function description
G.fast LINK	Green	On	G.fast service port is linked in normal mode.
		Blinking	G.fast service is in starting / handshaking / training / showtime.
		Off	G.fast service is not supported.

【 Table 2-4 】G.fast service port LED configuration

2.4.6 System Rear View

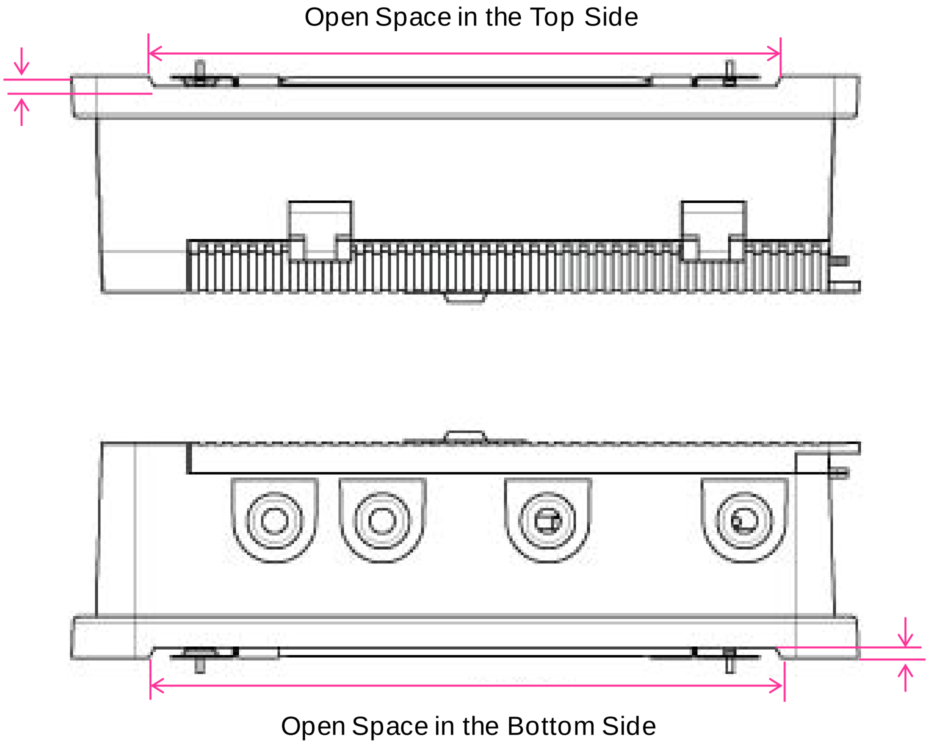
MG205X housing is basically composed of the front cover and the rear cover which is made of aluminum and plays a role of heat sink for heat management of the system as shown below.



【Picture 2-8】Rear View of MG205X

2.4.7 System Top View

MileGate2011 housing is basically composed of the front cover and the rear cover which is made of aluminum and plays a role of heat sink for heat management of the system as shown below. The front housing has open space on the top side and the bottom side as shown below to have proper airflow for heat dissipation of heatsink (the rear part of the housing).



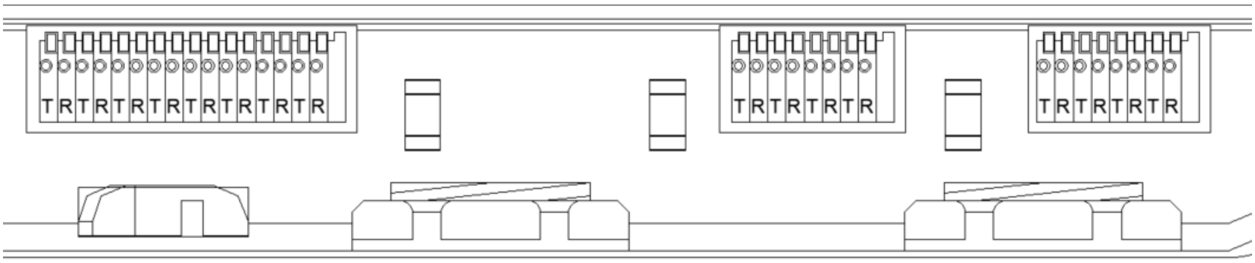
【Picture 2-9】Top / Bottom View of MG205X

Attention

Do not block the open space of the top side and the bottom side of MG205X housing for proper airflow. Blocking the open space may cause the system down and damage.

2.4.8 Port Connection

G.fast service port connection

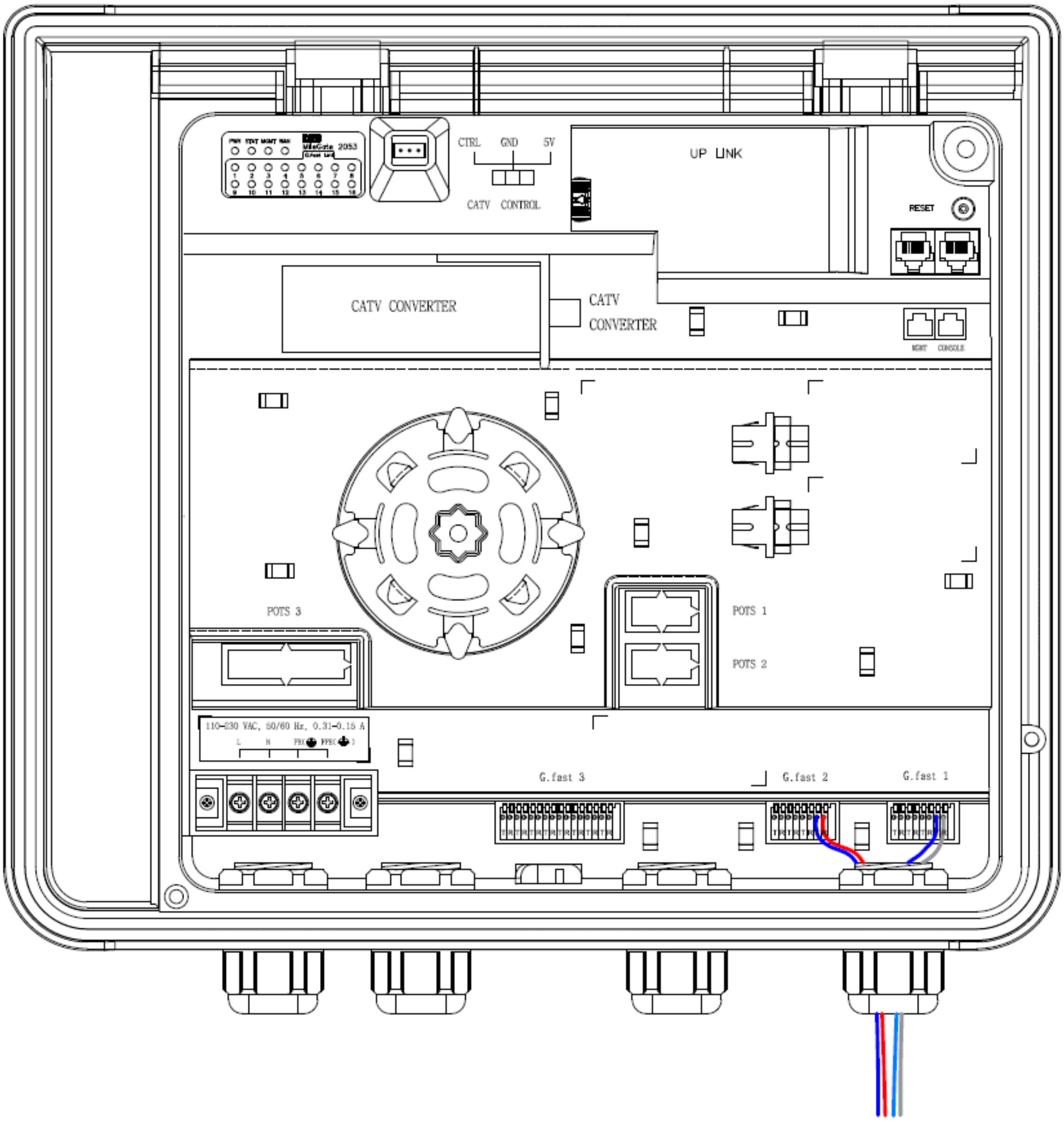


MILEGATE-205x has 4/8/16 x G.fast server port. This is to be used for connection between MILEGATE-205x and subscrier G.fast CPE

【 Picture 2-9 】 is Terminal for connection to MILEGATE-205x G.fast port.

Group	PIN	Signal(TIP)	Group	PIN	Signal(PING)
G.fast 1	1	RING_1	G.fast 3	1	RING_9
	2	TIP_1		2	TIP_9
	3	RING_2		3	RING_10
	4	TIP_2		4	TIP_10
	5	RING_3		5	RING_11
	6	TIP_3		6	TIP_11
	7	RING_4		7	RING_12
	8	TIP_4		8	TIP_12
G.fast 2	1	RING_5		9	RING_13
	2	TIP_5		10	TIP_13
	3	RING_6		11	RING_14
	4	TIP_6		12	TIP_14
	5	RING_7		13	RING_15
	6	TIP_7		14	TIP_15
	7	RING_8		15	RING_16
	8	TIP_8		16	TIP_16

【 Table 2-12 】 MILEGATE-205x G.fast Terminal port pin arrangement



【 Picture 2-10 】 Service port cable connection

Followings are the procedures to connect service port cable to MILEGATE-205x.

Step 1

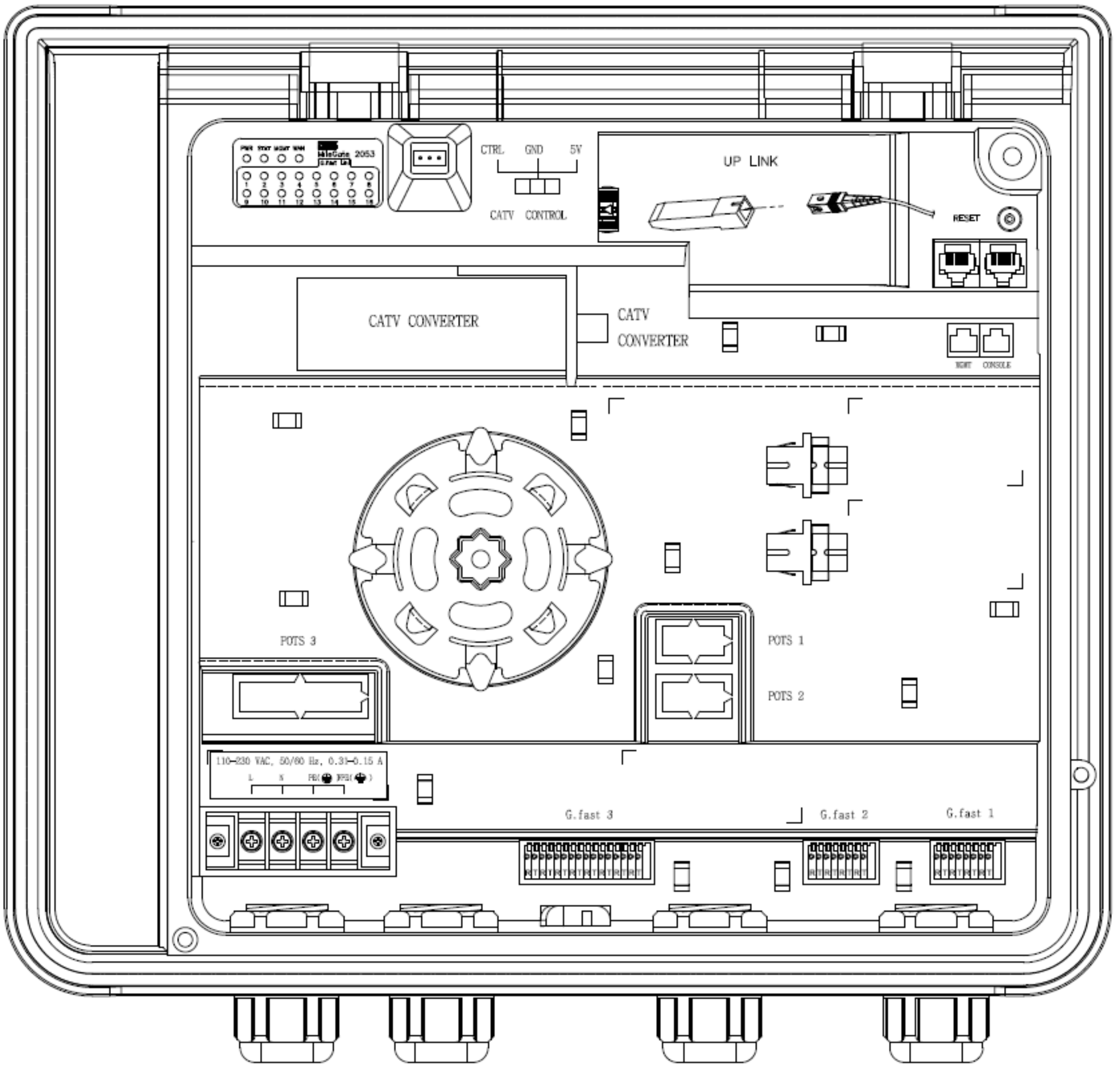
Press Terminal block push button and connect twisted pair cable.

Step 2

Release Terminal block push button and make sure the cable is secure.

Uplink moduel installation

MILEGATE-205x can connect a uplink modules by the demand. Followings are the procedures of 1/10G Base-X SFP or xPON uplink module installation.



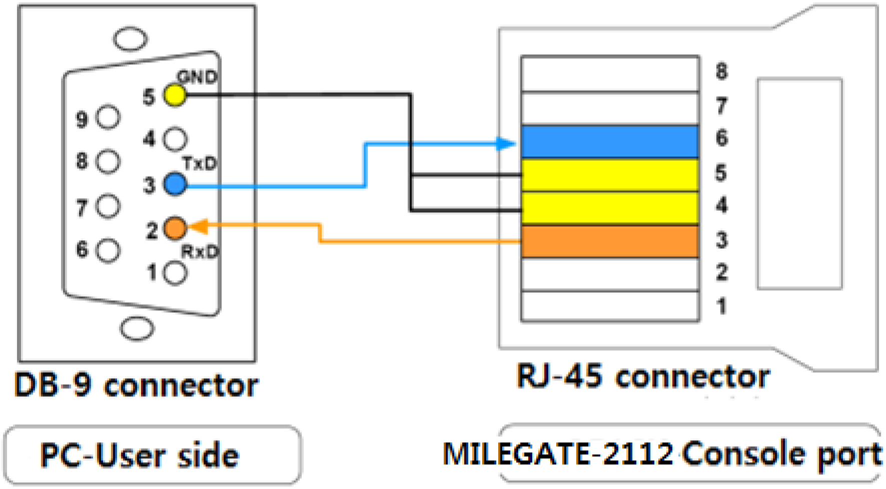
【 Picture 2-1 】 1/10G Base-X or xPON SFP+ uplink module installation

Caution

During operation of MILEGATE-205x, port setting as ‘inactive(disabled)’ is necessary to replace uplink module. Otherwise, system error may happen.

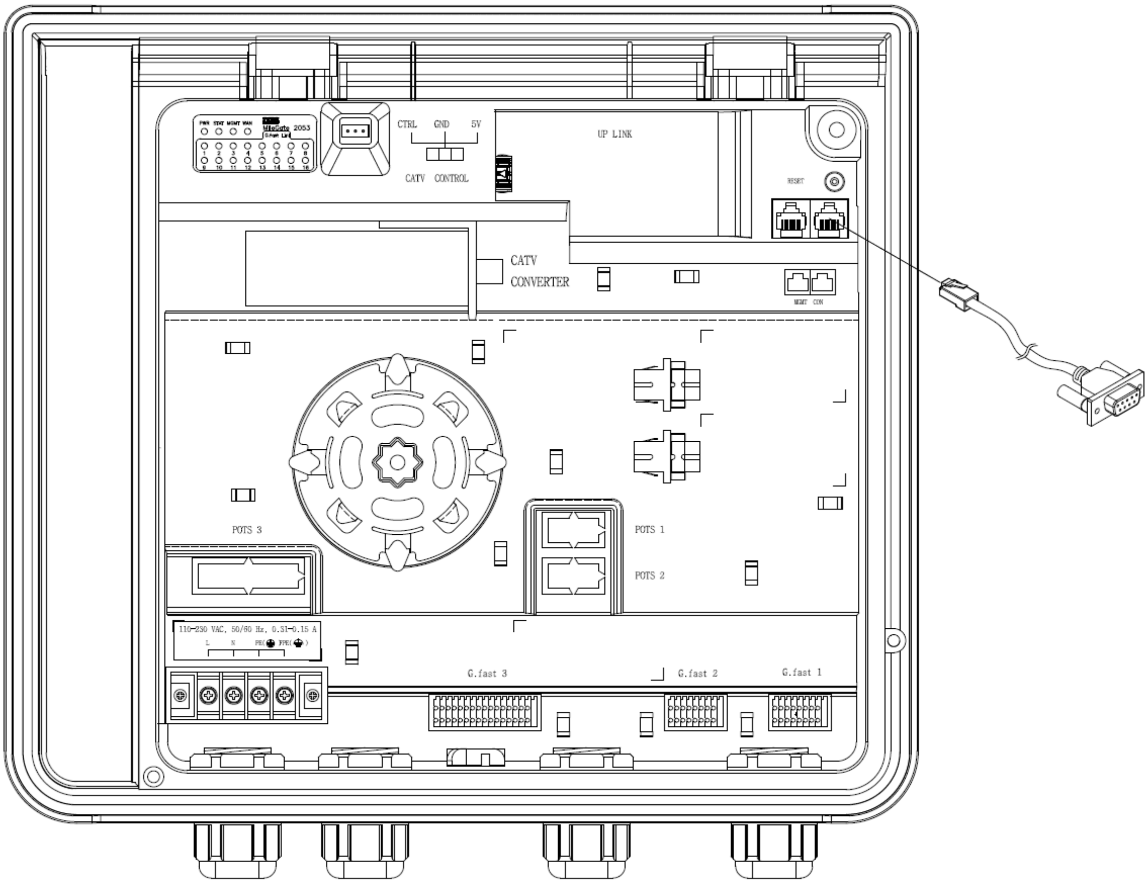
Console port connection

User can manage the equipment by using console terminal. Following pin assignment is for the console cable of MILEGATE-205x.



【 Picture 2-14 】 Console cable pin assignment

Followings are the steps to connect the console port to PC which has terminal program installed.



【 Picture 2-15 】Console port connection

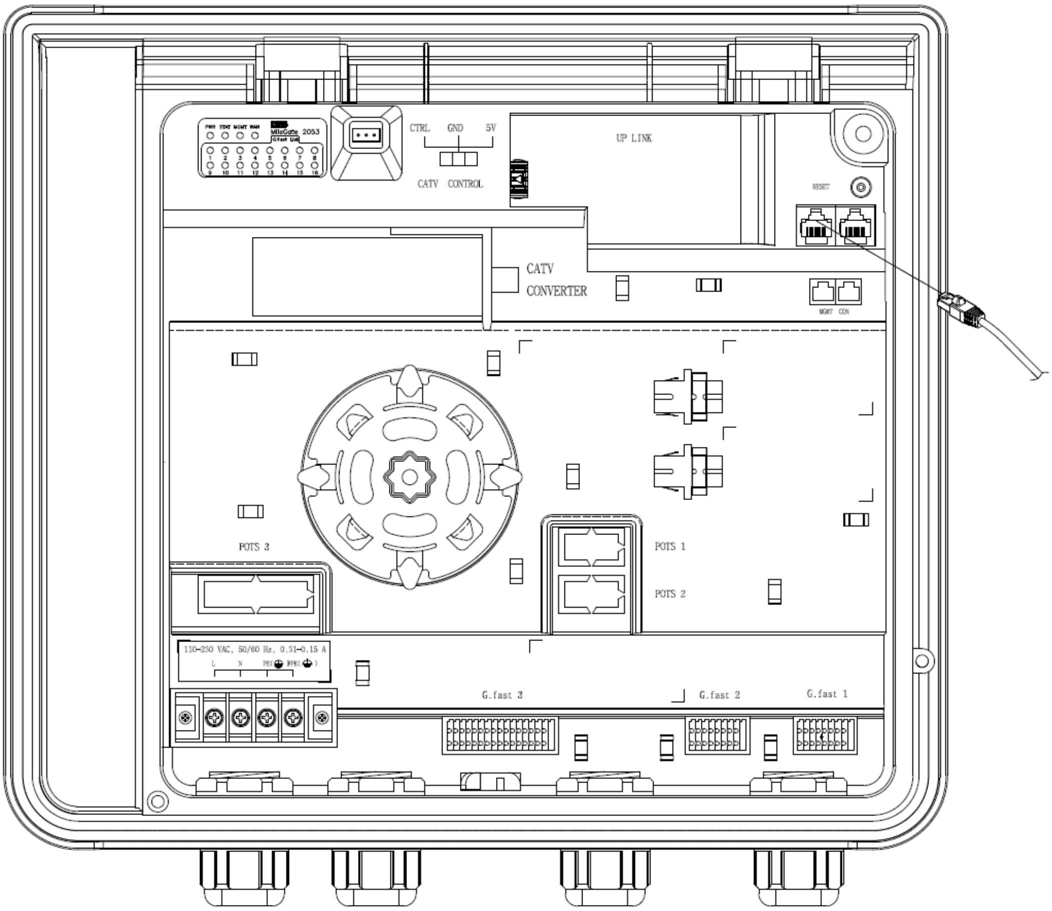
Step 1 Please connect RJ-45 plug connector of the console cable to MILEGATE-205x console port.

Step 2 Please connect DB-9 connector of the console cable to terminal or PC which terminal emulation software is installed.

Step 3 Please set the terminal program to ; 115200 baud, 8 data bits, no parity, control flow-none, 1 stop bit.

MGMT port connection

User can download the running images and manage the equipment by using MGMT port.



【 **Picture 2-16** 】 **MGMT cable connection**

Followings are the steps to connect the MGMT port with PC which terminal program is installed.

Step 1 Please connect one side of RJ-45-to-RJ-45 cable to MGMT port of MILEGATE-205x.

Step 2 Please connect the other end of the cable to MILEGATE-205x, hub or PC.

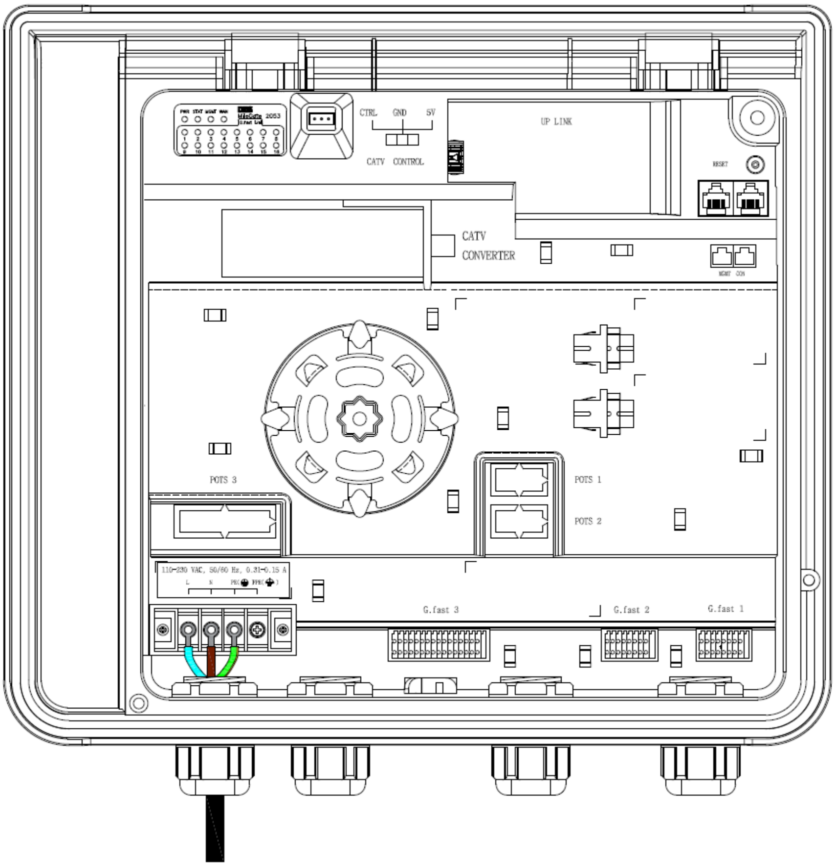
Step 3 Please check MGMT LNK LED. If MGMT port is connected in network normally, green LED will be turned on.

Reference

MGMT port of MILEGATE-205x recognize MDI/MDIX connector automatically, crossover cable is not needed to connect with any other equipment.

2.4.9 Power cable connection

After connection of Ethernet port and console port of MILEGATE-205x, electric power should be supplied. Followings are the procedures for power cable connection.



【 Picture 2-17 】 Power cable connection

Caution

User should do protective earthing of MILEGATE-205x for electric safety. Prior to power cable connection, please connect earth wire to the screw with ⏚d mark. The other end of earthwire should be grounded as well.

Followings are the steps of power cable connection of MILEGATE-205x.

Step 1 Please insert the power cable socket to the power inlet port of MILEGATE-205x.

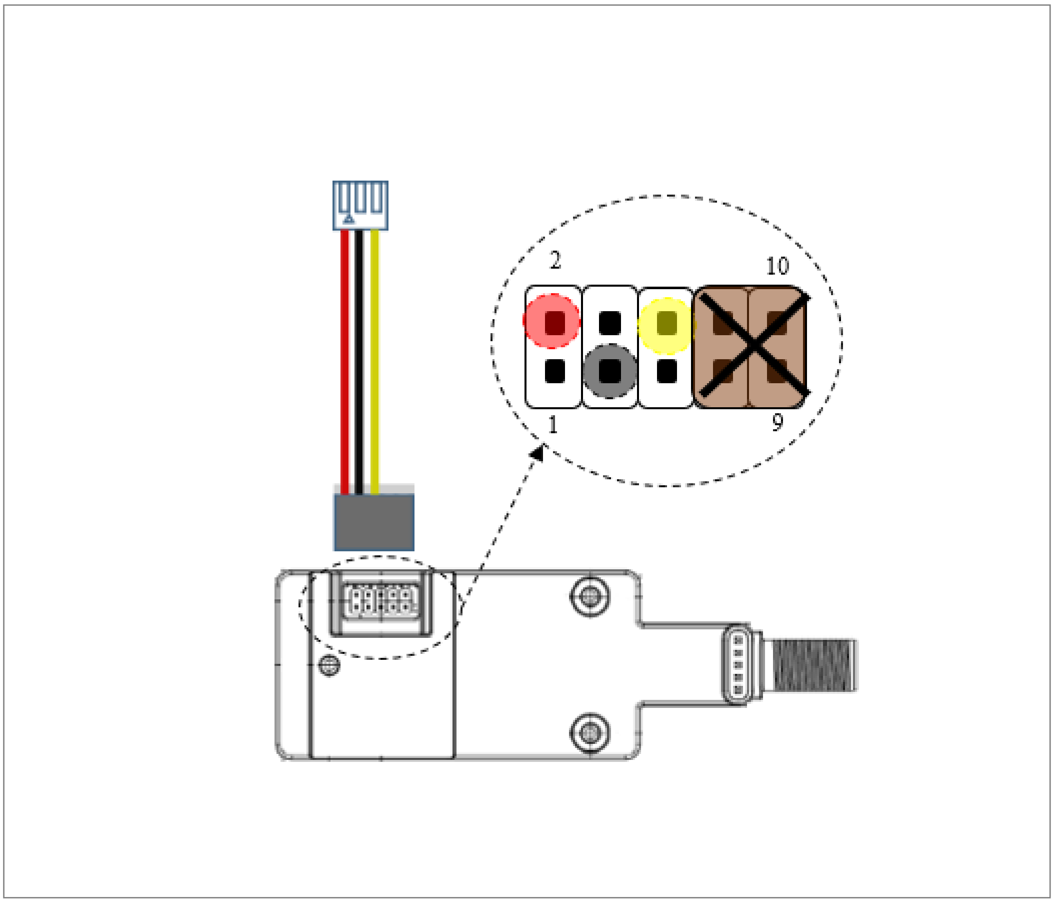
Step 2 Please insert the AC power plug of the cable to AC power socket.

Step 3 Please check the LED to make sure that the power is on.

2.4.10 Additional connection info.

CATV cable connection

Followings are the procedures for CATV converter cable connection.



【 Picture 2-17 】 CATV Converter cable connection

Caution

CATV Converter is not provide and user should be use

Followings are the steps of CATV converter cable connection of MILEGATE-205x.

Step 1 Please turn-off MILEGATE-205x.

Step 2 Please confirm CATV cable pin mapping then connect CATV converter with MILEGATE-205x

Step 3 Please make sure the CATV converter operation.

2.4.11 Trouble check

If MILEGATE-205x has any problem, it is very helpful if we know the right cause of the problem. Generally, we can find the reasons after comparison between normal operation and problematic operation.

Possible situations of MILEGATE-205x and solutions are following.

System power check

Following problems are related with power supply, and the reason can be found by several steps.

(1) Power is on, but power LED is off.

▫ Please check power cord/switch or RPF power source.

(2) After power ‘on’, the system turned off after a while.

▫ Please check if electric leakage is in power connection points.
▫ Please check AC power concentric socket if it has leakage or instable current when AC mode
▫ Please check RPF PSE concetirc socket when RPF mode.
▫ It is possible that internal power supply unit has operational problem.
▫ Please check air ventilation of the MILEGATE-205x, and make sure it is clean.

System check

It is often to have network related problems from cable, cable connection and connected hub or terminal. To find out the reasons, please check following points.

(1) System doesn’t recognize network interface.
▫ Please check interface cable itself and cable connection.
▫ Please check status LEDs of network interface.

(2) Network interface is recognized, but the interface is not initiated.
▫ Please check processor or hardware/software.

(3) System booting failed.
▫ Please check processor or hardware/software.
(4) Console stopped during system booting.
▫ Please check outside console connection.

▫ Please check the settings of terminal.

- 115200bps
- 8data bits
- No parity
- Flow control : none
- 1 stop bit

2.4.12 Network connection check

If MILEGATE-205x has operational problem, please check if it is possible to communicate with other connected equipment in the same network. If a server is connected in the same network, please try to transmit traffic data first, and if it is failed, please check if MILEGATE-205x can transfer/receive packets with the other equipments.

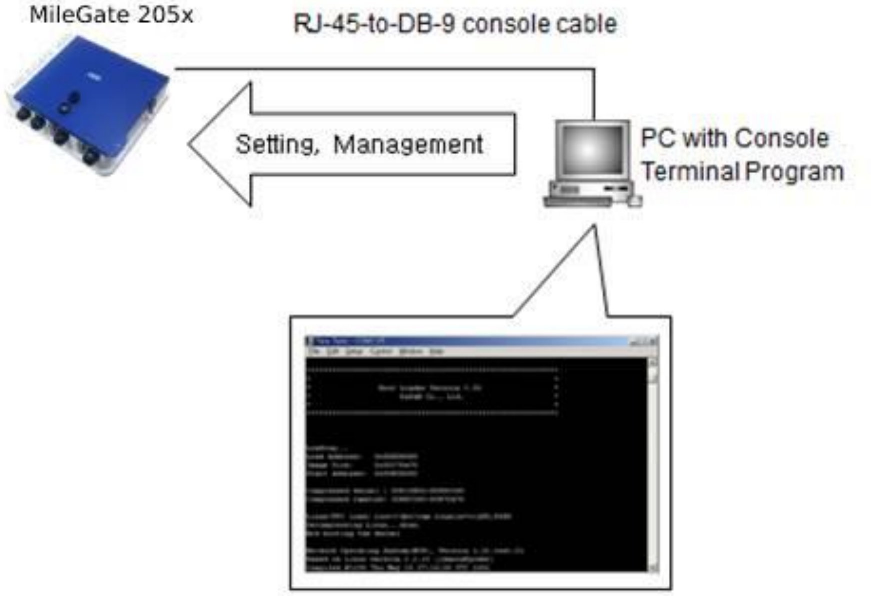
Please try ‘ping’ test to the system in the network if TCP/IP is possible. If it is failed, please check the interface cable and cable connection etc. If cable connection has no problem, please make sure that there is no problem in network environment of the user, and if you are sure that the network environment has no problem, please contact DZS email.

3. Using CLI

- Commands Structure
- Basic Command Usage

3.1 Commands Structure

MG205X can set up and manage the system through a console terminal or PC with terminal program. The user will use the CLI (Command Line Interface) based DSH.



【Picture 3-1】System Setup and Management Using Console Terminal

The following modes are for DSH configuration of commands that are used in MG205X.

- Privilege Exec View mode
- Privilege Exec Enable mode
- Global Settings mode
- Bridge mode settings
- Interface Mode Settings
- Rule Set mode
- DHCP Pool Setting Mode
- DHCP Option-82 Setup mode
- RMON setup mode

3.1.1 Privilege Exec View Mode

When a user does login successfully to the MG205X, it starts Privilege Exec View mode of DSH commands. Privilege Exec View mode is a read-only access mode provided to all users who have access to the equipment. In Privilege Exec View mode, most of commands are for check-out of the settings.

Following table shows the main commands used in the Privilege Exec View mode of MG205X.

【Table 3-1】Privilege Exec View Mode Key Commands

Command	Function
enable	Privilege Exec Enable starts.
exit	Log out the system.
show	Settings of the equipment are checked.

3.1.2 Privilege Exec Enable Mode

To have not only read access but also set-up authority, user need to enter into Privilege Exec Enable mode. Using the "enable" command in the Privilege Exec View mode, user can enter into the Privilege Exec Enable mode.

If user is in the Privilege Exec Enable mode, command prompt is changed from MG205X > is replaced by MG205X #.

Command	Mode	Function
enable	View	Privilege Exec Enable mode starts from User Exec. Mode.

In addition, to have higher security level, user can specify a password. In the Privilege Exec View mode, if user do login successfully into the MG205X, it enters into the Privilege Exec Enable mode of DSH command. Privilege Exec Enable mode commands are used in changing terminal settings, network status check, and system information check.

Following table shows the Privilege Exec Enable mode key commands of MG205X.

【Table 3-2】Privilege Exec Enable Mode Key Commands

Command	Function
clock	Enter the time and date on the system clock.
configure terminal	Enter into the Global Configuration Mode.
reload	Reboot the system
telnet	Telnet to connect to the other equipment
terminal length	Sets the number of lines to be output to the terminal screen.
traceroute	Track the packet transmission path.
where	Check the remote user who have access to the system.

3.1.3 Global Setting Mode

Global Setting mode can be entered if you type the following command in the Privilege Exec Enable mode. If user enters into the Global Setting mode, system prompt changed from MG205X# to MG205X(config)#.

Command	Mode	Function
config terminal	Enable	Global Setting mode starts from Privilege Exec Enable.

In Global Setting Mode is used to set the overall function and SNMP, RMON functionality of the entire system before setting a specific protocol or a specific function. In addition, user can enter into DHCP, Interface, Bridge setting mode from Global Setting mode.

Following table shows key commands of the Global Setting mode of MG205X.

【Table 3-3】Global Setup Mode Key Commands

Command	Function
Arp	Register IP address and MAC address in ARP table.
exec-timeout	Automatic log-out function starts.
hostname	Change the host name of system prompt.
interface	Enter into interface setting mode.
ip	Set up various functions to interface of DHCP server etc.
passwd	Change password.
qos	Set up QOS.
snmp	Set up SNMP.
syslog	Set up Syslog.
time-zone	Set up time-zone.

3.1.4 Bridge Setting Mode

From Global Setting mode, command “**bridge**” changes system prompt from MG205X(config)# into MG205X(bridge)#. It starts Bridge mode.

Command	Mode	Function
bridge	Global	Bridge Setting mode starts from Global Setting mode.

In Bridge Setting mode, the MAC address are managed, and users set the functions such as VLAN, port trunking, stacking, and mirroring of Layer 2 MG205X.

【Table 3-4】Bridge Setup Mode Key Commands

Command	Function	Command	Function
lacp	Set up LACP function.	**rate-limit**	Set up Rate-limit function.
mac-flood-guard	Set up Mac-flood-guard function.	**trunk**	Set up Trunking function.
mirror	Set up Mirroring function.	**vlan**	Set up VLAN function.

3.1.5 Interface Setting Mode

In interface configuration mode of MG205X, user can set the IP address for each Interface and check the transmission speed, duplex mode, communication bandwidth and related statistics. To enter into the specific Interface Setting mode, use '**interface** *interface-name'* command in Global Setting mode or other interface setting mode. System prompt of Interface Setting mode is MG205X(config-if) #.

Command	Mode	Function
interface *interface-name*	Global	Interface Setting mode starts from Global setting mode.

【Table 3-5】Interface Setup Mode Key Commands

Command	Function
description	Record descriptions of interface.
interface *interface-name*	Move to the other interface setting mode.
ip	Set up IP address.
shutdown	Disable the interface.

3.1.6 Rule Setting Mode

In Global Settings mode, the "flow flow-name create", "policer policer-name create", "policy policy-name create" commands are used to enter into Rule Setting mode of corresponding Flow, Policer and Policy. In Rule Setting mode, the command prompt will be changed from MG205X(config)# into MG205X(config-flow [name])#, MG205X(config-policer [name])# and MG205X(config- policy [name]) respectively.

To enter into the setting mode with new rule, use the following command:

Command	Mode	Function
flow *flow-name* **create**	Global	Enter into Flow setting mode form Global setting mode.
policer *policer-name* **create**		Enter into Policer setting mode form Global setting mode.
policy *policy-name* **create**		Enter into Policy setting mode form Global setting mode.

In Rule Settings mode, you can set the packet conditions to apply Rule function and operating behavior of the packet.

【Table 3-6】Flow Setup Mode Key Commands

Command	Function
apply	Save the rule settings and apply it to the equipment.
cos	Set up CoS to corresponding rule.
dscp	Set up policy with DSCP values in the range of TOS of packet.
ethtype	Set up packet condition by Ethernet type.
ip-precedence	Set up policy with IP TOS precedence.
mac	Set up packet condition by MAC address.
tos	Set up policy with ToS value.

【Table 3-7】Policer Setup Mode Key Commands

Command	Function
apply	Save the rule settings and apply it to the equipment.
color	Set up metering.
counter	Set up packet counter.
rate-limit	Set up rate limit.

【Table 3-8】Policy Setup Mode Key Commands

Command	Function
action	Set up packet action.
apply	Save the rule settings and apply it to the equipment.
include-class	Include Class in policy.
include-flow	Include Flow in policy.
include-policer	Include Policer in policy.
interface-binding	Fix interface for Rule application.
priority	Set up priority.

3.1.7 DHCP Pool Setting Mode

In Global Setting mode, by entering the "ip dhcp pool pool-name" command to set the subnet, the system prompt is changed from MG205X (config)# to MG205X (config-dhcp[pool-name]) in DHCP Setting mode.

Command	Mode	Function
ip dhcp pool *pool-name*	Global	Enter into DHCP Setting mode.

In DHCP Pool Setting Mode, user can set the IP address range used by the DHCP server, specify the group in subnet, and set the default gateway on the subnet.

【Table 3-9】DHCP Pool Setup Mode Key Commands

Command	Function
default-router	Set up default gateway in subnet.
dns-server	Set up DNS server.
fixed-address	Assign IP address to the host with specific MAC address.
lease-time	Set up IP release time.
range	Set up the range of IP address to be used by DHCP server.

3.1.8 DHCP Option-82 Setting Mode

In Global Setting mode, entering "ip dhcp option82" command to set the subnet, the system prompt is changed from MG205X(config)# to MG205X(config-dhcpoption)# in DHCP Setting mode.

Command	Mode	Function
ip dhcp option82	Global	Enter into DHCP Setting mode.

In DHCP Setting mode, user can set the IP address range used by the DHCP server, specify the group in the subnet, and set the default gateway of the subnet.

【Table 3-10】DHCP Option-82 Setup Mode Key Commands

Command	Function
lease	Set up conditions of IP lease.
policy	Set up policy of Option-82 packet.
system-circuit-id	Set up circuit-id of system.
system-remote-id	Set up remote-id of system.

3.1.9 RMON Setting Mode

In global mode, "Rmon-alarm <1-65,535>", "rmon-event <1-65,535>" and "rmon-history <1-65,535>" commands are used to enter into Rmon-alarm setting mode, Rmon-event setting mode and Rmon-history setting mode respectively. In each Rmon setting mode, system prompt is changed from MG205X(config)# to MG205X(config-rmonalarm[n])#, MG205X(config-rmonevent[n])# and MG205X(config-rmonhistory[n]).

【Table 3-11】RMON Setup Mode Command Commands

Command	Function
active	Activate each Rmon.
end	Stop present mode and start Privilege Exec Enable mode.
exit	Stop present mode and go back to previous mode.
owner	Define the owner who set up each RMON and use related information.

3.2 Commands Basics

There are several convenient features to know for using DSH command. Its features include:

- Available Commands
- Previous Commands Recalling
- Abbreviated Commands Usage
- Executed Commands List Save
- Using Privilege Exec Enable Mode Commands
- Using 'no' Command
- Using 'show' Command

- Move To Other Mode

3.2.1 Available Commands

Question mark (?) command shows available commands. Entering a question mark (?) in each command mode user can see all commands available in that mode. Also, user can see the variables followed by the commands.

Followings are the commands available in Privilege Exec Enable mode of MG205X.

```
MG205X # ?
Exec commands:
  clear              Clear DHCP Relay status
  clock              Manually set the system clock
  command-history-log  log the history of commands
  configure           Enter configuration mode
  copy               Copy from one file to another
  debug              Debugging functions
  default-os          Select default OS
  disconnect          Disconnect user connection
  enable             Turn on privileged mode command
  erase              Erase saved configuration
  execute             Execute
  exit               End current mode and down to previous mode
  halt               Halt process
  help               Description of the interactive help system
  no                 Negate a command or set its defaults
  ping               Send echo messages
  quote              Execute external command
  rcommand            Management stacking node
  release             Release the acquired address of the interface
  reload             Reload the system
  renew              Re-acquire an address for the interface
  restore             Restore configurations
  show              Show running system information
  ssh               Configure secure shell
  tech-support      Technical Supporting Function for Diagnosis System
  telnet            Open a telnet connection
  terminal          Set terminal line parameters
  traceroute         Trace route to destination
  where              List active user connections
  write              Write running configuration to memory, network, or
                     terminal

MG205X #
```

Attention

The question mark (?) is not seen on the screen after keyboard input, and a list of available commands will be shown directly without pressing enter key. This manual is based on version 1.42 of the NOS. Be aware that the output list from the NOS installed on the product maybe different by the version.

User of MG205X with DSH can recognize the commands started by a specific letter. After typing the first character of a word you want to know, enter a question mark without space!

Here is how to find out the commands starting with ‘s’ at the Privilege Exec Enable mode of MG205X.

```
MG205X # s?
  show        Show running system information
  ssh         Configure secure shell

MG205X #
```

User can also learn the variables that must be entered after the command. After entering the appropriate command, then type a question mark after a space. Here is how to find out the parameters followed by the traceroute commands in Privilege Exec Enable mode. After entering the appropriate commands, please remember that always we need to have a space.

```
 MG205X # traceroute?
  WORD  Trace route to destination address or hostname
  icmp  Use ICMP ECHO instead of UDP datagrams
  ip    IP Trace
  ipv6  IPv6 trace
  <cr>
MG205X # traceroute
```

If you want to know more detailed commands and to see a list of variables to be entered in each mode, use the following command.

Command	Mode	Function
show list	All	Show the list of available commands in present mode.
show cli		Show the list of available commands with tree structure in present mode.

The following is output list of commands from the command ‘show list’ that can be used in the Privilege Exec Enable mode.

```
MG205X # show list
  clear area (os1|os2)
  clear arp
  clear arp IFNAME
  clear auto-reset history
  clear gfast port PORTS
  clear ip arp inspection log
  clear ip arp inspection statistics (vlan VLAN_NAME|)
  clear ip dhcp authorized-arp invalid
  clear ip dhcp leasedb A.B.C.D/M
```

```
   clear ip dhcp leasedb all
   clear ip dhcp leasedb pool POOL
   clear ip dhcp relay statistics
   clear ip dhcp statistics
   clear ip igmp snooping stats port (PORTS|cpu|)
   clear ip mcfdb (*|vlan VLAN)
   clear ip mcfdb vlan VLAN group A.B.C.D source A.B.C.D
   clear ip prefix-list
   clear ip prefix-list WORD
   clear ip prefix-list WORD A.B.C.D/M
   clear ip route kernel
   clear ipv6 dhcp binding
   clear ipv6 dhcp client (IFNAME| )
   clear ipv6 mcfdb (*|vlan VLAN)
 --More--
```

Reference

To check the following list after 'More' from the output, please enter any key except for the ENTER key. If the enter key is pressed, it will show only one command.

Reference

In order to stop the list check of commands after 'More' from the output, please enter the q key or Ctrl+C.

Attention

This manual is based on version 1.42 of the NOS. Be aware that the output list from the NOS installed on the product maybe different by the version.

3.2.2 Previous Commands Recalling

It is not necessary to enter whole command which is repeated in DSH. Recalling previously-used commands is done by up-arrow (↑) key. If you enter the up-arrow key, it shows the commands one after another from the recently-used one.

The following example shows previous commands recalling after using the various commands.

Entered commands: show clock → configure terminal → interface default → exit

Recalled commands by up-arrow key: exit → interface default → configure terminal → show clock

```
MG205X # show clock
Fri, 30 Sep 2017 07:10:07 +0000
MG205X # configure terminal
MG205X (config)# interface default
MG205X (config-if)# exit
MG205X (config)# exit
MG205X # (↑ key entered)                           ⎫
         ↓                                          ⎪
MG205X # exit(↑ key entered)                        ⎪
        ↓                                           ⎪
MG205X # interface default(↑ key entered)           ⎬  This is output on
         ↓                                          ⎪  the same line
MG205X # configure terminal(↑ key entered)          ⎪
         ↓                                          ⎪
MG205X # show clock(↑ key entered)                  ⎭
```

3.2.3 Using Abbreviated Commands

Abbreviated commands with minimum characters which are distinguished from other commands are used.

The following table shows some examples of the abbreviated commands.

Command	Abbreviated Command
clock	**cl**
configure terminal	**con te**
show	**sh**
syslog	**sys**

3.2.4 Executed Commands List Save

In MG205X, user can see the executed commands in ascending order. Early executed command has low number, and recently executed command has high number in the executed commands list.

To see the executed commands list, use following command.

Command	Mode	Function
show history	View / Enable / Global / Bridge	Show executed commands list.

But the above execution commands are recorded temporarily, and it will be lost if the equipment is turned off. If you want to store the executed commands in the equipment, use the following command.

Command	Mode	Function
history non-volatile	Global	Save executed commands in non-volatile memory.
no history non-volatile		Release the saved commands in non-volatile memory.

Following commands show the saved executed commands in non-volatile memory.

Command	Mode	Function
show history non-volatile	Enable/ Global	Show saved executed commands in non-volatile memory.
show history non-volatile <1-2000>		Show saved executed commands in non-volatile memory. Numbered commands will be shown.
show history non-volatile tail <1-2000>		Show saved executed commands in non-volatile memory. Numbered commands will be shown from recent one.

To erase the saved executed commands list, use following command.

Command	Mode	Function
clear history non-volatile	Global	Erase saved executed commands list.

3.2.5 Using Privilege Exec Enable Mode Commands

Privilege Exec Enable mode commands can be used in other modes by following command in MG205X.

command	Mode	Function
do *command*	Global/RMON/DHCP/Option-82/Bridge Interface/Rule	Commands of Privilege Exec Enable mode can be used in other modes.

Following example shows the ping test in Bridge Setting mode.

```
MG205X (bridge)# do ping do ping 192.168.101.1
PING 192.168.101.1 (192.168.101.1) 56(84) bytes of data.
64 bytes from 192.168.101.1: icmp_seq=1 ttl=64 time=9.05 ms
64 bytes from 192.168.101.1: icmp_seq=2 ttl=64 time=0.372 ms
64 bytes from 192.168.101.1: icmp_seq=3 ttl=64 time=0.381 ms
64 bytes from 192.168.101.1: icmp_seq=4 ttl=64 time=0.375 ms
64 bytes from 192.168.101.1: icmp_seq=5 ttl=64 time=0.374 ms
64 bytes from 192.168.101.1: icmp_seq=6 ttl=64 time=0.378 ms
64 bytes from 192.168.101.1: icmp_seq=7 ttl=64 time=0.377 ms
64 bytes from 192.168.101.1: icmp_seq=8 ttl=64 time=0.377 ms
^C
--- 192.168.101.1 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7004ms
rtt min/avg/max/mdev = 0.372/1.461/9.056/2.870 ms

MG205X (bridge)#
```

3.2.6 Using ‘no’ Command

The ‘no’ command in MG205X turns off the settings or returns the user settings to the default value specified by the system.

3.2.7 Using ‘show’ Command

MG205X function settings or setting contents can be checked by ‘show’ command.

All ‘show’ commands in MG205X can identify only corresponding information to the keyword with the following options at the end.

|begin Show settings starting with this keyword.
|include Show settings including this keyword.
|exclude Show settings excluding this keyword.

Command	Mode	Function
show {**command** | *command*} [**| begin**]	All	Show settings of equipment.
show {**command** | *command*} [**| include**]		
show {**command** | *command*} [**| exclude**]		

3.2.8 Move to Other Mode

Using the CLI in MG205X, the mode will be returned to the previous setting mode, or it can return to Enable mode. On the other hand, in Enable mode, there is no command to return to the previous mode, and the command to log out of the system can be used alternatively.

To return to the previous mode or return to the Enable mode, use the following command:

Command	Mode	Function
exit	Global / RMON / DHCP / Option-82 / Bridge Interface / Rule	Return to the previous mode.
end	Global / RMON / DHCP / Option-82 / Bridge Interface / Rule	Return to the Enable mode.

Following command is used to log-out from the system.

Command	Mode	Function
exit	View / Enable	Log out from the system.

4. System Interface and IP Address Setting

- System interface
- IP address settings
- SSH (Secure Shell)
- User authentication port settings (802.1x)
- user authentication system

4.1 System Interface

After MG205X installation is finished, it goes final check that each port is connected to network and management PC. After all the checks, user will have interface to the system in order to set up and manage MG205X

In this chapter, next procedures are described, such as changing the password required for interface to the system, remote interface by Telnet etc.

- System Login
- System Login Password Change
- Privilege Exec Enable Mode Interface Password Setting
- Auto Logout Function Setting
- User Account Management
- Setting Limited Number of Interfaced User
- Remote Access
- Remote Interface User Check and Forced Interface Disconnection
- System Rebooting
- Auto Reset
- Auto Reset Option
- System Logout

4.1.1 System Login

After the installation of MG205X, please do the final check that each port is connected to network and management PC. After all checks, turn on the power MG205X to boot as follows:

Step 1. When you turn on the power MG205X, automatic booting will start with a login prompt.

```
************************************************************
*                                                          *
*            Boot Loader Version 02.01.0001                *
*                        Dzs GmbH                       *
*                                                          *
************************************************************
Press 's' key to go to Boot Mode:  0
[Loading OS1 image ...]
[Image OK : os1]

Starting kernel at 0x80761a10 ...

Primary instruction cache 32kB, VIPT, 4-way, linesize 32 bytes.
Primary data cache 32kB, 4-way, VIPT, cache aliases, linesize 32 bytes
CPU: BCM5300 rev 1 at 400 MHz
brcmboard: brcm_board_init entry
INIT: version 2.85 booting
Start on MG205X Initialization
Extracting configuration
Mon, 02 May 2016 20:51:00 +0000
Starting INET services
INIT: Entering runlevel: 3

INIT: Start UP (Cold start)

MG205X login:
```

Reference

Above output can be vary depending on the version of the equipment.

Step 2. If user enters login name in the login prompt, password prompt will be shown. Then, the user can enter the password and move to the Privilege Exec View mode. Log-in default name from factory is 'admin' and the password is not set. After entering 'admin', then press 'enter' key.

```
MG205X login: admin
Password:
MG205X>
```

Step 3. User will have only the right to check the settings of the equipment in Privilege Exec View mode. To have the authority to set and manage the equipment, user have to enter into Privilege Exec Enable mode. The following is a case to enter into the Privilege Exec Enable mode.

```
MG205X> enable
MG205X#
```

4.1.2 System Login Password Change

User with permission to set up and manage the MG205X, can change the password. To ensure security, it is recommended that users change their passwords often. To change the password, use the following command in Global Configuration Mode.

Command	Mode	Function
passwd	Global	Change the password of user.

Reference

The password can be more than 16 characters including letters and numbers. Please avoid password similar to the login ID name.

On the other hand, user can also change the read-only password by using 'user add' command. To change the read-only password, use the following command:

Command	Mode	Function
passwd *user-name*	Global	Change the read-only password of user.

[Setting example 1]

The following are example of password change to 'networks'.

```
MG205X (config)# passwd
Changing password for admin
Enter the new password (maximum of 16 characters)
Please use a combination of upper and lower case letters and numbers.
Enter new password: networks
Re-enter new password: networks
Password changed.
MG205X (config)#
```

Reference

The password is to be entered twice to avoid a mistake because there is no output on the screen.

4.1.3 Privilege Exec Enable Mode Interface Password Setting

When user moves from Privilege Exec View mode to Privilege Exec Enable mode, user can set a password to increase security further. To set an interface password to Privilege Exec Enable mode, use the following command.

Command	Mode	Function
passwd enable *password*	Global	Set the password to enter into Privilege Exec Enable mode.

Privilege Exec Enable mode password set by the user can be checked by using the 'show running-config' command.

However, other users cannot see the password by using the ‘show running-config’ command for the security of the password.

Other ordinary users cannot see the password by using ‘show running config’ because the password is encrypted by the following command. They will see only encrypted view.

Command	Mode	Function
service password-encryption	Global	Encrypt password for security.

To show original password from encryption, use the following command.

Command	Mode	Function
no service password-encryption	Global	Encrypted password is set to original password.

On the other hand, to have increased security, you can set to show only encrypted password without using ‘service password-encryption’ command. However, this method requires user to enter password in an encrypted character string.

To set an encrypted password string not to be public by any means, use the following command.

Command	Mode	Function
passwd enable 8 *encrypted-password*	Global	Set an encrypted password string

Reference

If user wants to know the encrypted string of the intended password, use ‘passwd enable password’ command to set a password, then, please activate the ‘service password-encryption’ to check the password by ‘show running-config’ command.

Reference

If you set a password using the commands above, the password is shown by encrypted string though ‘service password-encryption’ is not activated.

To delete the password setting, use the following command.

Command	Mode	Function
no passwd enable	Global	Delete password to enter into Privilege Exec Enable mode.

[Setting Example 1]

The following case shows how to set a password as ‘networks’ to access Privilege Exec Enable mode.

```
MG205X # configure terminal
MG205X (config)# passwd enable networks
MG205X (config)# show running-config
!
hostname MG205X
!
passwd enable networks
!
exec-timeout 0 0
(Omitted)
MG205X (config)#
```

The following shows interface after password setup.

```
MG205X login: admin
Password:
MG205X > enable
Password: networks
MG205X #
```

The following is password check after activation ‘**service password-encryption’**.

```
MG205X (config)# show running-config
!
hostname MG205X
!
passwd enable 8 bJ6fclPZlAIRk
!
service password-encryption
exec-timeout 0 0
!
(Omitted)
MG205X (config)#
```

[Setting Example 2]

The following shows how to set encrypted password (networks), and login afterwards.

Reference

The encrypted string can be shown in the same way as the [Setting Example 1].

Password setting is done by ‘passwd enable password’ command, and then, activating ‘service password-encryption’, and user can check the password by using ‘show running-config’ command.

```
MG205X # configure terminal
MG205X (config)# passwd enable 8 bJ6fclPZlAIRk
```

```
MG205X (config)# exit
MG205X # exit

MG205X login: admin
Password:
MG205X > enable
Password: networks
MG205X #
```

4.1.4 Auto Logout Function Setting

If the administrator leaves the MG205X with turned on console terminal, the system will be kept in log-in status. Then, the other user can change the settings of the administrator. Therefore, if there is no keyboard input during the setup time of the administrator, system will be logged out automatically. The setup time can be set by the administrator.

Here is the command to set the automatic logout function.

Command	Mode	Function
exec-timeout *exec-minute* [*exec-seconds*]	Global	Set the auto logout function
exec-timeout 0		Disable the auto logout function.

Reference

The automatic logout time can be set by minutes (exec-minute) and seconds (exec-seconds). Minutes setting is in between <1-35791> and seconds setting is in between <0-59>. The default time is set as 10 minutes.

To check the automatic logout time set on your device, use the following command.

Command	Mode	Function
show exec-timeout	Enable / Global	Show automatic logout time setting.

Here is an example of the auto logout time set to 60 minutes.

```
MG205X (config)# exec-timeout 60
MG205X (config)# show exec-timeout
Log-out time : 60 seconds
MG205X (config)#
```

4.1.5 User Account Management

In MG205X, system administrator can add user accounts. In addition, the administrator can specify the level of users from Level 0 to Level 15 for having increased security levels of the equipment.

The following shows account management method, such as adding users, setting user levels, etc.

- Adding User Account
- Setting User's Right
- Setting Example

(1) Adding User Account

MG205X can add user accounts other than administrator. When administrator adds user accounts, user level can be set at the same time. If user level is not specified, user permission level is given as Level 0.

To add a user account, use the following command.

Command	Mode	Function
user add *name description*	Global	Add user account with Level 0.
user add *name* **level** <0-15> *description*		Add user account with specified level.

Reference

Users with Level 0 up to Level 14 can only use 'exit' and 'help' commands at Privilege Exec View Mode. and they cannot interface to the Privilege Exec Enable Mode. Only the highest Level 15(admin) has the authority to write and read all.

To delete the added user account, use the following command.

Command	Mode	Function
user del *name*	Global	Delete user account.

To check the user accounts which are added by the administrator, use the following command.

Command	Mode	Function
show user	Enable / Global	Show the added user accounts.

(2) Setting User's Right

MG205X can set user privileges, separated by 16 steps from 0 to Level 15 to access the equipment. Level 15 is the highest level (administrator) with all 'read' and 'write' permissions. Level 0 to Level 14 can have specified rights from the administrator. Administrator can set the available commands for each level in each mode. They can use only 'exit' and ‘help’ commands only in the Privilege Exec View mode. They are not allowed to interface to the Privilege Exec Enable mode.

Followings are the commands to set up user’s right in each level.

Command	Mode	Function
privilege bridge level <0-15> {*command* ｜ **all**}	Global	User in this level can use this command in Bridge setting mode.
privilege configure level <0-15> {*command* ｜ **all**}		User in this level can use this command in Global setting mode.
privilege dhcp-option82 level <0-15> {*command* ｜ **all**}		User in this level can use this command in DHCP Option82 setting mode.
privilege dhcp-pool level <0-15> {*command* ｜ **all**}		User in this level can use this command in DHCP setting mode.
privilege dhcp-pool-class level <0-15> {*command* ｜ **all**}		User in this level can use this command in Pool Class setting mode.
privilege dhcp- class level <0-15> {*command* ｜ **all**}		User in this level can use this command in DHCP Class setting mode.
privilege enable level <0-15> {*command* ｜ **all**}		User in this level can use this command in Privilege Exec Enable mode.
privilege interface level <0-15> {*command* ｜ **all**}		User in this level can use this command in Interface setting mode.
privilege route-map level <0-15> {*command* ｜ **all**}		User in this level can use this command in Route-map setting mode.
privilege flow level <0-15> {*command* ｜ **all**}		User in this level can use this command in Flow setting mode.
privilege policer level <0-15> {*command* ｜ **all**}		User in this level can use this command in Policer setting mode.
privilege policy level <0-15> {*command* ｜ **all**}		User in this level can use this command in Policy setting mode.
privilege rmon-alarm level <0-15> {*command* ｜ **all**}		User in this level can use this command in RMON setting mode.
privilege rmon-event level <0-15> {*command* ｜ **all**}		
privilege rmon-history level <0-15> {*command* ｜ **all**}		
privilege view level <0-15> {*command* ｜ **all**}		User in this level can use this command in Privilege Exec View mode.

Attention

Commands available in low level will be available in all higher level. For example, the command set to be used in Level 0 will be available on all levels from Level 0 up to Level 14.

Reference

Representing word of all series commands are available together in the level. For example, if administrator enters 'show', all commands that start with 'show' will be available in the level of the mode.

Here is the command used to delete the information of user's right. This is to be done by administrator.

Command	Mode	Function
no privilege	Global	Delete all command settings of the user.
no privilege bridge level <0-15> {*command* ｜ **all**}		Delete all command settings of user in each mode.
no privilege configure level <0-15> {*command* ｜ **all**}		
no privilege dhcp-option82 level <0-15> {*command* ｜ **all**}		
no privilege dhcp-pool level <0-15> {*command* ｜ **all**}		
no privilege dhcp-pool-class level <0-15> {*command* ｜ **all**}		
no privilege dhcp- class level <0-15> {*command* ｜ **all**}		
no privilege enable level <0-15> {*command* ｜ **all**}		
no privilege interface level <0-15> {*command* ｜ **all**}		
no privilege rmon-alarm level <0-15> {*command* ｜ **all**}		
no privilege rmon-event level <0-15> {*command* ｜ **all**}		
no privilege rmon-history level <0-15> {*command* ｜ **all**}		
no privilege route-map level <0-15> {*command* ｜ **all**}		
no privilege flow level <0-15> {*command* ｜ **all**}		
no privilege policer level <0-15> {*command* ｜ **all**}		
no privilege policy level <0-15> {*command* ｜ **all**}		
no privilege view level <0-15> {*command* ｜ **all**}		

To check user's right in each level set by the administrator, use the following command.

Command	Mode	Function
show privilege	Global	Show user's right of the level set by administrator.
show privilege now		Show the level of present user.

(3) Setting Examples

[Setting Example 1]

The following shows the case which administrator adds 2 users without password. The one user (test 0) is with level 0 and the other user (test 15) is with level 15.

```
MG205X (config)# user add test0 test
Changing password for test0
Enter the new password (minimum of 5, maximum of 8 characters)
Please use a combination of upper and lower case letters and numbers.
Enter new password

Warning: weak password (continuing).
Re-enter new password:
Password changed.
MG205X (config)# user add test15 level 15 test
Changing password for test15
Enter the new password (minimum of 5, maximum of 8 characters)
Please use a combination of upper and lower case letters and numbers.
Enter new password:
Bad password: too short.

Warning: weak password (continuing).
Re-enter new password:
Password changed.
MG205X (config)# show user
====================================================
 User name            Description       Level
====================================================
test0                test                 0
test15               test                 15

MG205X (config)#
```

[Setting Example 2]

The following shows the case which administrator adds 2 users without password. The one user (test 0) is with level 0 and the other user (test 1) is with level 1.

```
MG205X # configure terminal
MG205X (config)# user add test0 test
Changing password for test0
Enter the new password (minimum of 5, maximum of 8 characters)
Please use a combination of upper and lower case letters and numbers.
Enter new password:
Bad password: too short.

Warning: weak password (continuing).
Re-enter new password:
Password changed.
```

```
MG205X (config)# user add test1 level 1 test
Changing password for test1
Enter the new password (minimum of 5, maximum of 8 characters)
Please use a combination of upper and lower case letters and numbers.
Enter new password:
Bad password: too short.

Warning: weak password (continuing).
Re-enter new password:
Password changed.
MG205X (config)# show user
====================================================
 User name           Description        Level
====================================================
test0                test                 0
test1                test                 1

MG205X (config)#
```

[Setting Example 3]

The following is to set the user's right for Level 0 and Level 1.

```
MG205X # configure terminal
MG205X (config)# privilege view level 0 enable
MG205X (config)# privilege enable level 0 show
MG205X (config)# privilege enable level 1 clock
MG205X (config)# privilege enable level 1 configure terminal
MG205X (config)# show privilege

 Command Privilege Level Configuration
 -----------------------------------------------
 Node         All   Level   Command

 EXEC(ENABLE)         1     clock
 EXEC(ENABLE)         1     configure terminal
 EXEC(VIEW)           0     enable
 EXEC(ENABLE)         0     show

 4 entry(s) found.

MG205X (config)#
```

When it is set as above, user with Level 0 can use only 'show' command in Privilege Exec Enable mode, and user with Level 1 can have not only Level 0 right but also the right to use 'clock' and 'configure terminal' commands in Privilege Exec Enable mode.

4.1.6 Setting Limited Number of Interfaced User

MG205X administrator can limit the number of users who can be interfaced to the equipment. At this time, limited users are including both the users through console ports and the remote users. And, if the equipment is set as a RADIUS server or a TACACS + server, the limited users include users interfaced to the server.

To limit the number of users that can connect to the equipment, use the following command.

Command	Mode	Function
login connect <1-10>	Global	Set the limit of the users to be interfaced.

Reference

MG205X has basic limit of the users as 10.

Release settings that limit the number of users as following.

Command	Mode	Function
no login connect	Global	Release the limit of accessible users to the equipment.

4.1.7 Remote Access

MG205X can be interfaced remotely by using the following command:

Command	Mode	Function
telnet *destination*	Enable	Interface to the other equipment (IP address or hostname).
telnet *destination port-number*		Interface to the other equipment (Port).

Attention

When you use the ‘write memory’ to save the settings, the message [OK] will appear after the successful saving. When you save settings after making changes on Telnet, if you cut Telnet session without confirming [OK], all changed settings will be disappeared. Please make sure to disconnect after checking the [OK] message.

```
MG205X # write memory
[OK]
MG205X #
```

4.1.8 Remote Check of Interfaced User and Forced Interface Disconnection

Administrator of MG205X can check the remote user and disconnect the interface of the user who is not intended to be in the network. To disconnect the interface with remote user, use the following command to verify 'tty' of the remote user.

Command	Mode	Function
where	Enable /Global	Check the remote user.

After checking of remote user, administrator can disconnect the interface of remote user by following command.

Command	Mode	Function
disconnect *tty*	Enable	Disconnect the interface of remote user.

The following is an example. After check the remote user, the interface of remote user with 'ttyP1' is disconnected.

```
MG205X (config)# where
admin at ttyS0 from console for 23 hours 50 minutes 17.27 seconds
admin at ttyp0 from 172.16.30.2:3246 for 4 hours 31 minutes 46.65 seconds
hyun at ttyp1 from 172.16.119.201:2633 for 2 hours 31 minutes 51.61 seconds
MG205X (config)# disconnect ttyp1          ID of
MG205X (config)#                            remote
```

4.1.9 System Rebooting

Since the TFTP / FTP server has downloaded new system images, the system should be rebooted. and while the MG205X is in setup and management through a terminal program, the system may need to be rebooted.

To reboot the system, use the following command in the Privilege Exec Enable mode.

Command	Mode	Function
reload	Enable	Reboot the system.
reload { **os1** | **os2** }		Select NOS and reboot the system.

Attention

If the system is rebooted, the settings will be erased if it is not saved earlier. Therefore, please make sure to save your settings prior to rebooting.

MG205X has a protection not to reboot the system without saving settings. If the system setting is not saved by 'write memory' command, it gives a question about saving issue prior to rebooting. If administrator wants to save the settings, 'y' is to be entered. If the settings are to be removed, 'n' will be entered by the administrator.

The following message is shown if you save and reboot the system after new setting.

```
MG205X # reload
Do you want to save the system configuration? [y/n] y
Do you want to reload the system? [y/n] y
```

When users reboot the system by using the 'reload' command in Enable mode, it will reboot the system immediately. If the system rebooting reservation is made in Global mode, the system will be rebooted periodically or at any time when the user want.

To make rebooting reservation on a certain period of time or scheduled time, use the following command.

Command	Mode	Function
reload at *HH:MM DAY MONTH YEAR*	Global	Reboot the system at scheduled or appointed time.
reload at *HH:MM* **in daily**		Reboot the system at a designated time every day.
reload in *HH:MM*		Reboot the system after designated period.

To delete the rebooting reservation setting, use the following command.

Command	Mode	Function
no reload all	Global	Delete all rebooting reservation.
no reload at [*HH:MM DAY MONTH YEAR*]		Delete rebooting reservation at the scheduled time.
no reload at *HH:MM* **in daily**		Delete daily rebooting reservation.
no reload in		Delete periodic rebooting reservation.

To check the rebooting reservation details, use the following command.

Command	Mode	Function
show reload	Global	Show all information about rebooting reservation.

4.1.10 System Logout

System logout is done from Privilege Exec View mode or Privilege Exec Enable mode. If the process is in another mode, the user has to go back to Privilege Exec Enable.

System logout command is as following.

Command	Mode	Function
exit	View / Enable	Log out from the system.

4.2 IP Address Setting

MG205X decides transmission route by MAC address of the data. This IP address was not needed originally for packet transmission, but remote interface by SNMP or Telnet requires IP address.

Reference

MG205X has virtual default interface (interface 1), and all ports are set as member port as default.

To set IP address in MG205X, please go through following procedures.

- Interface Activation
- Shutdown of Activated Interface
- IP Address Setting To Network Interface
- Setting of Static Route and Default Gateway
- Interface Description

4.2.1 Interface Activation

Prior to IP address allocation to an interface, that interface should be activated for the communication. If the interface is not activated, it is not possible to do communication though the IP address is allocated. To check whether the interface is activated or not, use ‘show running-config | interface’ command.

Following is a case of interface check if it is activated.

```
MG205X # show running-config interface
!
interface lo
 no shutdown
!
interface default
 no shutdown
MG205X #
```

Reference

VLAN name of Interface 1 is「default」.

To activate an interface, user should be in interface setting mode by following command.

Command	Mode	Function
interface *interface-name*	Global	Enter into the interface setting mode.

User can activate the interface in interface setting mode by following command.

Command	Mode	Function
no shutdown	Interface	Activate the interface.

4.2.2 Shutdown of Activated Interface

To shutdown activated interface in interface setting mode, use following command.

Command	Mode	Function
shutdown	Interface	Deactivate the interface.

4.2.3 IP Address Setting to Network Interface

IP address can be allocated to the activated interface by manual way and automatic way as follows.

(1) Manual Setting

Manual IP address allocation to interface is by following command.

Command	Mode	Function
ip address *ip-address/M*	Interface	Allocate IP address to the interface.
ip address *ip-address/M* **primary**		Change the primary IP address to new one.
ip address *ip-address/M* **secondary**		Change the secondary IP address to new one.

To check the allocated IP address, use following command.

Command	Mode	Function
show ip	Interface	Show IP address which was set to the interface.

To remove allocated IP address, use following command.

Command	Mode	Function
no ip address [*ip-address/M*]	Interface	Remove IP address of the interface.
no ip address *ip-address/M* **secondary**		Remove secondary IP address of the interface.

(2) Automatic Allocation Setting

MG205X can have IP address allocation to the interface automatically through DHCP server. As a client of DHCP server, use following command to have automatic IP address allocation.

Command	Mode	Function
renew dhcp *interface-name*	View/Enable	Request automatic IP address allocation to the interface.

To return the IP address to DHCP server, use following command.

Command	Mode	Function
release dhcp *interface-name*	View/Enable	Return the automatically allocated IP address back to DHCP.

4.2.4 Setting of Static Route and Default Gateway

MG205X can set Static route. Packet goes to the destination though this static route which user set. Static route includes destination address, neighbor router which is to receive packets, and the number of routes to the destination.

To set static route, use following command in Global Setting mode.

Command	Mode	Function
ip route *ip-address prefix-mask* {*ip-gateway-address* ∣ **null**} [1-255]	Global	Set static route.
ip route *ip-address/m* {*ip-gateway-address* ∣ **null**} [<1-255>]		
ip route *ip-address/m* {*ip-gateway-address* ∣ **null**} **src** *ip-address*		

To set default gateway, use following command.

Command	Mode	Function
ip route default {*default-gateway-address* ∣ **null**} [<1-255>]	Global	Set Default Gateway.

To check static route, use following command.

Command	Mode	Function
show ip route [*ip-address* ∣ *ip-address/m*]	Enable / Global /Bridge	Show Static Route.
show ip route [**database**]		

To remove static route setting, use following command.

Command	Mode	Function
no ip route *ip-address prefix-mask* {*ip-gateway-address* ∣ **null**} [1-255]	Global	Remove Static Route setting.
no ip route *ip-address/m* {*ip-gateway-address* ∣ **null**} [<1-255>]		

To remove Default gateway setting, use following command.

Command	Mode	Function
no ip route default { *ip-address* | **null**} [<1-255>]	Global	Remove Default gateway setting.

4.2.5 Interface Description

MG205X can have registration of specific interface description for easy management. To register description of each interface, use following command.

Command	Mode	Function
description *description*	Interface	Register description of the interface.

Following shows a case of registering interface descriptions.

```
MG205X (config-if)# description sample_description
MG205X (config-if)# show interface 1
Interface mgmt
  Hardware is Ethernet, address is 00d0.cb00.0d83
  Description: sample_description
  index 43 metric 1 mtu 1500  <UP,BROADCAST,RUNNING,MULTICAST>
  VRF Binding: Not bound
  Bandwidth 100m
  inet 10.27.41.91/24 broadcast 10.27.41.255
    input packets 3208070, bytes 198412141, dropped 203750, multicast packets 0
    input errors 12, length 0, overrun 0, CRC 0, frame 0, fifo 12, missed 0
    output packets 11444, bytes 4192789, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
    collisions 0
MG205X (config-if)#
```

On the other hand, registered interface description can be removed by following command.

Command	Mode	Function
no description	Interface	Remove the interface description.

4.2.6 Interface Check

Interface setting and status can be checked by following command.

Command	Mode	Function
show interface [*interface-name*]	Enable/Global/ Bridge/Interface	Show the setting and status of the interface.

4.2.7 Setting Example

[Setting Example 1]

This is to activate the interface 1.

```
MG205X # configure terminal
MG205X (config)# interface 1
MG205X (config-if)# no shutdown
MG205X (config-if)#
```

[Setting Example 2]

This shows IP address allocation to the interface 1. IP address is 192.168.1.10.

```
MG205X (config-if)# ip address 192.168.1.10/16
MG205X (config-if)# show ip
IP-Address         Scope   Status
-------------------------------------
192.168.1.10/16     global

MG205X (config-if)#
```

[Setting Example 3]

Following shows the Default gateway setting case.

```
MG205X # configure terminal
MG205X (config)# ip route default 192.168.1.254
MG205X (config)#
```

4.3 IPv6 Interface Setting

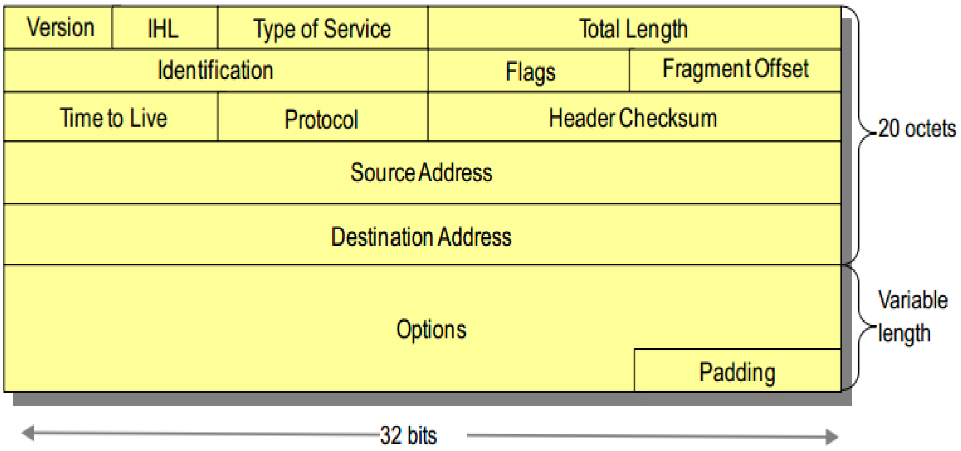
IPv6 is to solve the problems from lack of IP addresses and to have next generation protocol with increased performances.

Unlike 32-bit IPv4, IPv6 is composed of 128-bit, and it can have endless numbers of IP addresses. In addition, due to its simpler packet header than IPv4, it is expected that the speed of packet processing will be faster than IPv4. Also, it will have stronger security and automatic address setting of stateless method which will provide improved and easier IP address setting.

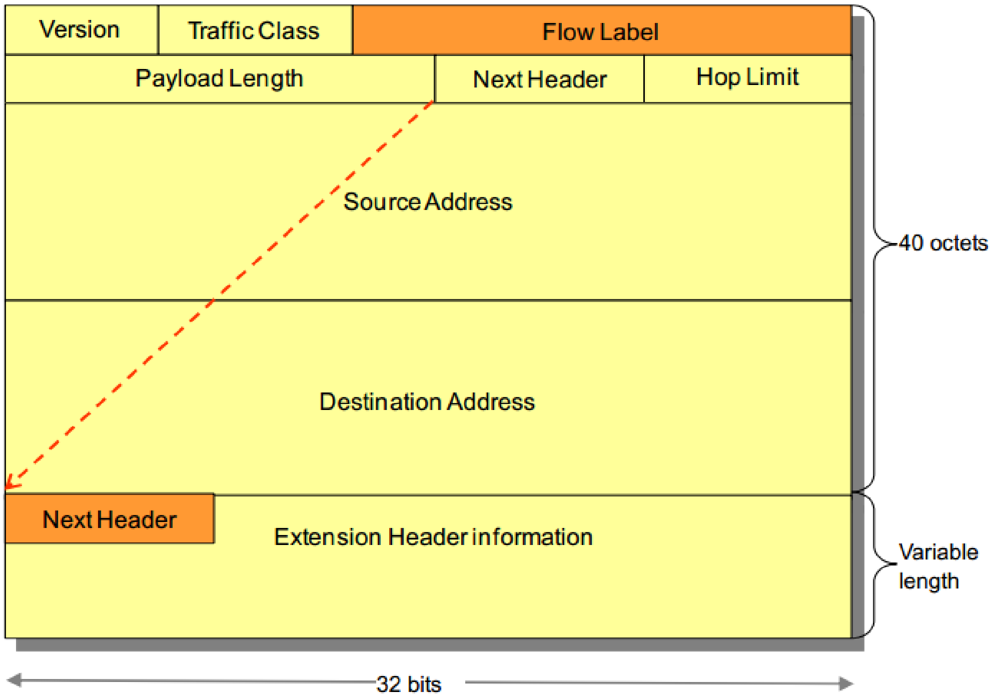
IPv6 is developed to provide unique IP addresses to all interfaced devices. If all devices have its own IP addresses, NAT (Network Address Translation) will be used less than IPv4. Then, each node will not need to do special processing for packet transactions, and new application protocols will be able to be used, too.

IPv6 packet header is simpler than IPv4, and it makes the speed of packet processing faster than IPv4. Also, as IPv6 doesn’t need packet check functions like IP header checksum, packet transmission performance will be increased.

Following shows packet headers of IPv4 and IPv6.



【Picture 4-1】Structure of IPv4 packet header



【Picture 4-2】Structure of IPv6 packet header

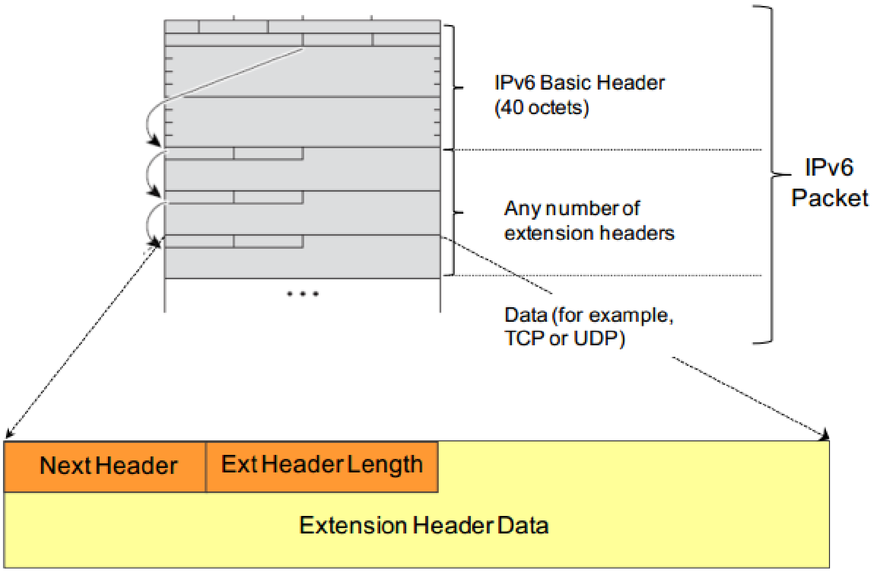
【Table 4-1】IPv6 Packet Header Field

Command	Function
Version	Version of IP. Length is 4-bit, and set as ‘6’.
Traffic Class	Length is 8-bit, and this field is corresponding to ToS (Type of Service) of IPv4. It is the class of packet or its priority.

Flow Label	New field in IPv6 packet header. Length is 20-bit. Flow Label is used to have high quality of real-time services like voice or image data.
Payload Length	Total length of packet materials. This is similar to total length field of IPv4 packet header. It has 16-bit which can express maximum 65,535 bytes, and it contains extended header and upper layer PDU. If the length is 65,535 bytes or more than that, the setting is '0', and Jumbo Payload option is used for option extension header per Hop.
Next Header	This is similar to the protocol field of IPv4 packet header. Next Header shows the type of information located next to IPv6 header. It is the protocol of upper layer PDU, and the length is 8-bit.
Hop Limit	Maximum number of router which IPv6 packet can pass. When it passes through each router, it deducts '1' from the limit number, and it can pass though until the limit number becomes '1'. As IPv6 header has no 'Checksum', router doesn't need the procedure of 'Checksum' processing. Length is 8-bit. This is similar to 'Time To Live' of IPv4 packet header if there is no Hop limit and packet queue time of router in IPv4. If Hop Limit is '0', packet will not be regarded and ICMP time termination message will be transferred to the source address.
Source Address	IPv6 address of host, and the length is 128-bit.
Destination Address	IPv6 address of host, and the length is 128-bit.

Located to IPv6 packet header, 8 fields are extension header and packet materials. If the fields are existing, each extension header will be aligned in 64-bit. Number of extension header in IPv6 packet is not fixed. At the same time, extension headers create header chains. Each extension header is differentiated by Next Header of previous header. In general, last extension header has next header field of transmission layer protocol like TCP or UDP.

Following picture shows the structure of IPv6 extension header.



【Picture 4-3】Structure of IPv6 extension header

Next table shows of extension header types and values of next header field.

【Table 4-2】Type of IPv6 extension header

Header	Next Header	Function
Hop-by-hop options header	0	This header is processed by all hops though the packet routes. This header is located next to the IPv6 packet header if this is exists as extension.
Destination options header	60	Destination options header is located next to Hop-by-hop options header, and it is processed in last destination or visiting address assigned by routing header. If this destination options header is located next to Authentication header and ESP(Encapsulating Security Payload), it is processed only in the last destination.
Routing header	43	Routing header is used for source routing.
Fragment header	44	Fragment header is used for packet fragmentation of bigger packets than MTU(Maximum Transmission Unit) in the routes between Source and Destination.

Authentication header	51	Authentication header and ESP header are used to authenticate the node which packet is sent, and it makes sure whether transmitted data needs to be corrected or not. This is the same in IPv4 and IPv6.
ESP header	50	
Upper-layer header	6 (TCP)/17 (UDP)	Upper-layer header is used internally in packet to send data, and it is based on TCP and UDP protocols.
Mobility header	IANA	It is used by mobile node, communication node and home agent in message transmission related with interface and management.

4.3.1. IPv6 address setting

Interface address can be set up by following command.

Command	Mode	Function
ipv6 address *ipv6-address/m* **[anycast]**	Interface	It sets up the address of interface.
ipv6 address *prefix_name ipv6-address/m*		

To delete the existing address, use the following command.

Command	Mode	Function
no ipv6 address [*ipv6-address/m*]	Interface	It deletes the existing address of the interface.
no ipv6 address *prefix_name ipv6-address/m*		

4.3.2. Link local address setting

Link local address can be set up by following command.

Command	Mode	Function
ipv6 address link-local *ipv6-address*	Interface	It sets up link local address.

To delete the existing link local address, use the following command.

Command	Mode	Function
no ipv6 address link-local *ipv6-address*	Interface	It deletes the existing link local address of the interface.

Neighbor Discovery related information can be shown by following command.

Command	Mode	Function
show ipv6 neighbors	Enable / Global	It shows Neighbor Discovery related information.

Neighbor Discovery related information can be deleted by following command.

Command	Mode	Function
clear ipv6 neighbors	Enable / Global	It deletes Neighbor Discovery related information.

4.3.3. Static Route and Default Gateway setting

MG205X can have static route setting. The static route is assigned by user, and packets go through static route up to destination. Static route setting includes destination address, neighbor router which will receive packets, and number of routes to go through up to the destination.

Static route setting can be done by following command in global setting mode.

Command	Mode	Function
ipv6 route *ipv6-address/m* {*ipv6-gateway-address* ∣ *interface-name*} [1-255]	Global	It sets up static route.
ipv6 route *ipv6-address/m ipv6-gateway-address interface-name* [<1-255>]		

To check the static route setting, use the following command.

Command	Mode	Function
show ipv6 route [*ipv6-address* | *ipv6-address/m*]	Enable / Global	It shows static route.
show ipv6 route [database]		

To delete the static route setting, use the following command.

Command	Mode	Function
no ipv6 route *ipv6-address/m* {*ipv6-gateway-address* ∣ *interface-name*}	Global	It deletes the static route setting.
no ipv6 route *ipv6-address/m ipv6-gateway-address interface-name*		

4.3.4. IPv6 interface check

To check the setting and status of IPv6 interface, use the following command.

Command	Mode	Function
show ipv6 interface [*interface-name*]	Enable/Global/ Bridge	It shows the setting and status of IPv6 interface .
show ipv6 interface brief		

4.4 IPv6 ND setting

4.4.1. RA message setting

Router transmits RA (Router Advertisement) message to hosts in the same links periodically and shows its location, and it provides necessary information. But under IPv6 environments, hosts in initialization transmits RS (Router Solicitation) message to get necessary information for setup.

RA message includes router lifetime, and this lifetime value informs nodes of duration which the corresponding router can keep the status of default router. The lifetime value is shown as seconds with maximum 18.2 hours. If the value is ‘0’, the router is not default candidate, and it means that the router is not in the router list of any host.

In addition, RA message includes reachable time and retransmission timer. Reachable time which IPv6 node can reach to adjacent router is checked, and it senses rapidly which router can’t reach and it shows how long the router is presumed to be alive. Retransmission timer is transmission timer of NS (Neighbor Solicitation) message, and the unit is millisecond. This is used to check whether ARP and remote node can be reached or not.

User can set 2-bits flag in RA packets, and appoints whether to use stateful automatic setting of host by “managed address configuration” flag and “Other stateful configuration” flag.

If “managed address configuration” flag is set, host receives address allocation by stateful automatic setting like DHCP. Otherwise, stateless automatic setting will assign address.

If “other stateful configuration” flag is set, host use stateful automatic setting to get other information than address.

Options in RA message are link layer address of the source, MTU, prefix information etc. If link layer address of the source is included, hosts don’t need to execute ARP to the other default routers. MTU option creates optimum size of datagram to be used between source host and specific destination node, and it helps quick transmission of it.

Prefix information option includes data used for on-link decision and stateless automatic setting.

(1) Stateful automatic setting and deletion

If “managed address configuration” flag is set in RA message, host can be set to receive address allocation by stateful automatic setting. The setting can be done or released by following command.

Command	Mode	Function
ipv6 nd managed-config-flag	Interface	Host is set to receive address allocation by stateful automatic setting.
no ipv6 nd managed-config-flag		Corresponding flag is released, and host is set not to use stateful automatic setting.

If “other stateful configuration” flag is set in RA message, host can be set to receive other information, such as DNS server, domain name etc. by stateful automatic setting. The setting can be done or released by following command.

Command	Mode	Function
ipv6 nd other-config-flag	Interface	“Other stateful configuration” flag is set to receive other information by using stateful automatic setting.
no ipv6 nd other-config-flag		“other stateful configuration” flag is released not to receive other information by using stateful automatic setting.

(2) IPv6 Prefix setting

Prefix of IPv6 RA message can be set or released by following command.

Command	Mode	Function
ipv6 nd prefix *ipv6-address/M* [<0-4294967295>]	Interface	This sets IPv6 Prefix information of RA messages which receive and send RS messages for IPv6 automatic address setting.
ipv6 nd prefix *ipv6-address/M* <0-4294967295> [0-4294967295]		
no ipv6 nd prefix *ipv6-address/M*		This deletes IPv6 Prefix information for specific IPv6 automatic address setting.

To change the IPv6 address setting in corresponding interface into ND Prefix setting, use the following command.

Command	Mode	Function
ipv6 nd prefix default [<0-4294967295>] [<0-4294967295>]	Interface	This changes the IPv6 address setting in corresponding interface into ND Prefix setting.
no ipv6 nd prefix default		This deletes the ND Prefix setting in corresponding interface.

(3) Message transmission period setting

To set up RA message transmission period, use the following command.

Command	Mode	Function
ipv6 nd ra-interval <3-1800> [<3-1350>]	Interface	It sets RA message transmission period.

Reference

Default setting of RA message transmission period is 600 seconds.

To change previous RA message transmission period setting into default value, use the following command.

Command	Mode	Function
no ipv6 nd ra-interval	Interface	It deletes previous RA message transmission period setting.

(4) Router Lifetime setting

To set router lifetime which makes user's MG205X to be used as default router during the time, use the following command.

Command	Mode	Function
ipv6 nd ra-lifetime<0-9000>	Interface	This sets lifetime to be operated as default router.

To delete router lifetime of the default router and change it into default setting value, use the following command.

Command	Mode	Function
no ipv6 nd ra-lifetime	Interface	It deletes router lifetime of the default router and change it into default setting value.

Reference

If user did router lifetime setting of the default router, the RA message transmission period value should be the same or smaller than router lifetime.

(5) Reachable-time setting

Reachable-time setting specify the time that remote IPv6 nodes take to reach corresponding router. With this setting, router detects which neighbor can't reach to the router. This reachable time setting is involved to all transmitted RA messages to the outside of the interface, all nodes in the same link are using the same reachable time.

Reference

The shorter Reachable-time is set, the faster unreachable neighbors are detected. But this needs considerations as it may cause losses of network bandwidth and resources.

Reachable time for remote IPv6 nodes can be set or released by following command.

Command	Mode	Function
ipv6 nd reachable-time <0-3600000>	Interface	It sets reachable time.
no ipv6 nd reachable-time		It deletes reachable time setting.

(6) RA Suppression setting

If an interface has activated unicast routing, basically, IPv6 RA message is transmitted to Ethernet and FDDI interface automatically.

To stop IPv6 RA message transmission of LAN interface, use following command.

Command	Mode	Function
ipv6 nd suppress-ra	Interface	It stops IPv6 RA message transmission of LAN interface.

To re-activate IPv6 RA message transmission of LAN interface, use following command.

Command	Mode	Function
no ipv6 nd suppress-ra	Interface	It activates IPv6 RA message transmission of LAN interface.

(7) Maximum Hop limit

Maximum hop limit of RA messages and all IPv6 packets transmitted by router can be set up by following command.

Command	Mode	Function
ipv6 nd ra-hoplimit <0-255>	Interface	It sets maximum hop limit.

To delete maximum hop limit and return to default value, use the following command.

Command	Mode	Function
no ipv6 nd ra-hoplimit	Interface	It deletes maximum hop limit setting.

(8) Message Re-transmission Period setting

To set up re-transmission period of NS (Neighbor Solicitation) message, use the following command.

Command	Mode	Function
ipv6 nd retrans-time *<0-4294967295>*	Interface	It sets re-transmission period of NS message.

To delete re-transmission period of NS message and return to default, use the following command.

Command	Mode	Function
no ipv6 nd retrans-time	Interface	It deletes re-transmission period of NS message.

Reference

This re-transmission period is set and transmitted with RA message.

4.5 SSH(Secure Shell)

The more developments of network, the more importance of security is recognized by the users. But, the security is very weak in conventional service of FTP and Telnet. SSH is secured log-in shell for security. Using SSH, all data is encrypted for security, and compressed data traffic enables faster transmission efficiency. In addition, it provides tunnel to unsafe services, such as FTP and POP. MG205X provides SSH server and client modes as follows.

- SSH Server
- SSH Client
- Authentication key setting

4.5.1 SSH Server

(1) SSH Server 'Enable'

To activate SSH server in MG205X, use following command.

Command	Mode	Function
ssh server enable	Global	Activate SSH server.

Not to use SSH server function in MG205X, use following command.

Command	Mode	Function
ssh server disable	Global	Deactivate SSH server.

(2) Client Check

To check the client which is interfaced to SSH server of MG205X, use following command.

Command	Mode	Function
show ssh	Enable / Global	Check the client interfaced to SSH server.

(3) Disconnection of Client Interface

To disconnect the client from the interfaced SSH server, use following command in Global Setting mode.

Command	Mode	Function

ssh disconnect *pid*	Global	Disconnect the client from the interfaced SSH server.

Reference

The *'pid'* is the number of SSH client, and 'show ssh' command will show the number.

(4) Client Interface History Check

To check the history of client which has been interfaced to SSH server of MG205X, use following command.

Command	Mode	Function
show ssh history	Enable / Global / Bridge	Show the history of clients which has been interfaced to SSH server.

Reference

The 'show ssh history' command will show the recorded history of clients after disconnection, so present client is not included in the history. 'show ssh' command will show the present interfaced client information.

4.5.2 SSH Client

(1) SSH Server Login

MG205X can be used as a client of SSH server. In this case, to log-in the SSH server, use following command.

Command	Mode	Function
ssh login *destination* [*public-key*]	Enable	Interface to SSH server.

Reference

The *'Destination'* is IP address of server, 「account@IP address」 or 「Host domain name(ex : abc@100.1.1.1)」.

4.5.3 Authentication Key Setting

SSH creates authentication key, and this will strengthen security by sharing the authentication key from server and client.

Authentication key is safer than direct entering password in log-in process, and 1 key can have multiple interfaces to SSH server.

(1) Authentication Key Generation

To create authentication key in MG205X, use following command. This key will be saved in the system until it is removed.

Command	Mode	Function
ssh keygen {**rsa1** | **rsa** | **dsa** }	Global	Generate authentication key.

Reference

'rsa1' is 'ssh1' supporting authentication type. **'rsa' and 'dsa'** are 'ssh2' supporting authentication type.

(2) Authentication Key Verification

To verify the authentication key which was generated in MG205X, use following command.

Command	Mode	Function
ssh key verify *public-key-file-name*	Global	Verify authentication key by entering the file name.

(3) Authentication Key List Check

To check the authentication key list which is saved in MG205X, use following command.

Command	Mode	Function
show key-list	Enable/Global	Check the authentication key list

4.5.4 Setting Example

[Setting Example 1] SSH Server Activation

Following shows the server activation.

```
MG205X (config)#ssh server enable
Generating SSH public/private RSA1 key ...
Generating SSH public/private RSA key ...
Generating SSH public/private DSA key ...
SSH Server start!
MG205X (config)#show ssh
 connected clients :  000
num  pid  ppid  srv_usr   remote_ip   Start_Time  Stop_Time

MG205X (config)#
```

[Setting Example 2] Client interface disconnection

Following shows forced disconnection of client interface after checking of client number.

```
MG205X # show ssh
 connected clients :  001
num     pid     ppid    srv_usr       remote_ip       Start_Time             Stop_Time

001     150      96      root   203.236.124.89   Wed Mar  5 15:40:55 1980  ---------
MG205X # config terminal
MG205X (config)# ssh disconnect 150
MG205X (config)# show ssh
 connected clients :  000
num     pid     ppid    srv_usr       remote_ip       Start_Time             Stop_Time

MG205X (config)#
```

[Setting Example 3] Client interface to server

Following shows client interface to server addressed as 172.16.209.10. After being client to interface to SSH server, question message about interface permission comes out.

```
MG205X (config)# ssh login 172.16.209.10
The authenticity of host '172.16.209.10 (172.16.209.10)' can't be established.
RSA key fingerprint is ea:af:c8:e9:3f:4f:22:1c:61:2e:2b:9d:0a:f6:2b:7e.
Are you sure you want to continue connecting (yes/no)?
```

If it is to interface to server continuously, enter ‘yes’. Then, question about password will come out. The password of SSH server account should be entered to be interfaced successfully.

```
MG205X (config)# ssh login 172.16.209.10
The authenticity of host '172.16.209.10 (172.16.209.10)' can't be established.
RSA key fingerprint is ea:af:c8:e9:3f:4f:22:1c:61:2e:2b:9d:0a:f6:2b:7e.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '172.16.209.10' (RSA) to the list of known hosts.
admin@172.16.209.10's password:
MG205X (config)#
```

Above case happens only when client interfaced to server for the first time. Once interfaced server creates known-host, simple question about password will come out next time. Following case shows the example of known-host interface.

```
MG205X (config)# ssh login 172.16.209.10
admin@172.16.209.10's password:
MG205X (config)#
```

[Setting Example 4] Server interface by authentication key

Following method is server interface by authentication key after key setting.

Step 1. Authentication key should be set for the equipment. Following shows authentication key setting as ‘networks’ to the MG205X A by DSA authentication method.

```
MG205X A(config)# ssh keygen dsa
Generating public/private dsa key pair.
Enter file in which to save the key (/etc./.ssh/id_dsa):
```

```
Enter passphrase (empty for no passphrase):networks
Enter same passphrase again:networks
Your identification has been saved in /etc./.ssh/id dsa.
Your public key has been saved in /etc./.config/id_dsa.pub.
The key fingerprint is:
d9:26:8e:3d:fa:06:31:95:f8:fe:f6:59:24:42:47:7e admin@MG205X
MG205X A(config)#
```

Saved directory
And filename

Step 2 Authentication key file should be saved to the MG205X B which is server. To copy the file, interface to the MG205X B is needed with password of the account. The IP address of the MG205X B is 172.16.20910.

```
MG205X A(config)# ssh copy /etc./.ssh/id_dsa.pub
root@172.16.209.10:/etc./.ssh/authorized_keys
The authenticity of host '172.16.209.10 (172.16.209.10)' can't be established.
RSA key fingerprint is ea:af:c8:e9:3f:4f:22:1c:61:2e:2b:9d:0a:f6:2b:7e.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '172.16.209.10' (RSA) to the list of known hosts.
root@172.16.209.10's password:
id_dsa.pub   100% |*****************************************|   600     00:00
MG205X _A(config)#
```

Step 3 Interface to SSH server by authentication key is made.

```
MG205X A(config)# ssh login 172.16.209.10
Enter passphrase for key '/etc./.ssh/id_dsa': networks
MG205X _B#
```

5. Port Default Setting

User can set basic system environments of MG205X ports, such as Auto-negotiate, transmission speed, flow control etc. For port settings change from default, Global setting mode should be changed to Bridge Setting mode using ‘bridge’ command. If we change the mode to Bridge Setting mode’, system prompt is changed from ‘MG205X (config)#’ to ‘MG205X (bridge)#’ as follows.

```
MG205X (config)# bridge
MG205X (bridge)#
```

Followings are the port default settings in MG205X Ethernet port.

【Table 5-1】Default Settings of Ethernet Port

Items	Default Setting
Port status	Activated
Auto-negotiation	ON(100BASE-FX excluded)

Duplex mode	Full Duplex Mode
Flow control	On
VLAN	Default VLAN
STP	Used for default VLAN

To check port default settings in MG205X Ethernet port, use following command.

Command	Mode	Function
show port	Enable / Global / Bridge	Show status of all ports.
show port *port-number*		Show status of the numbered port.

Reference

The *'port-number'* can be multiple at one time. Multiple port numbers can be enumerated with comma (**,**) without blank, or starting port number and last port number with dash bar (**-**) without blank.

'*port-number*' : Wrong input of port number will result in following output messages.

```
MG205X (bridge)# show port port
%Port port is invalid
MG205X (bridge)# show port 100
%Invalid input parameter: 100
MG205X (bridge)#
```

In this chapter, port default settings include following details.

- Logical Port 'Enable'
- Auto Nego Setting
- Port Speed Setting
- Duplex Mode Setting
- Flow Control Setting
- Port Description
- Check and Initialization of Port Statistics
- Check of Port Status
- G.FAST Operation Method
- G.FAST Port Settings
- Line Counter Check of G.FAST Port
- Config-Profile Setting
- Port Mirroring Setting

5.1 Logical Port ‘Enable’

All ports of MG205X are activated basically, but user can change physically-activated port into disabled port logically. Changing port status logically can be done by following command in Bridge Setting mode.

Command	Mode	Function
port enable *port-number*	Bridge	Activate the numbered port.
port disable *port-number*		Deactivate the numbered port.

Attention

G.fast ports of MG205X have different method to change the port status.

Please refer to ‘**5.11 G.FAST Port Setting’.**

Attention

If user replaces uplink modules during the operation of MG205X, at first, port status should be deactivated. If the port is activated physically, it should be deactivated logically. If the uplink modules are replaced by other one without port deactivation, it will may cause system failure.

Following is a case showing deactivation of port 27

```
MG205X (bridge)# show port 27
--------------------------------------------------------------------------------
NO       TYPE     PVID  COS    STATUS       MODE       FLOWCTRL     INSTALLED
                        (ADMIN/OPER)             (ADMIN/OPER)
--------------------------------------------------------------------------------
 27:        None      1    0    Up/Down  Force/Half/0      N/A/ Off       N
ILEGATE-2042 (bridge)# port disable 27
MG205X (bridge)# show port 27
--------------------------------------------------------------------------------
NO       TYPE     PVID  COS    STATUS       MODE       FLOWCTRL     INSTALLED
                        (ADMIN/OPER)             (ADMIN/OPER)
--------------------------------------------------------------------------------
 27:        None      1    0  Down/Down  Force/Half/0      N/A/ Off       N
MG205X (bridge)#
```

5.2 Auto Nego Setting

Auto Negotiation of MG205X is to set the transmission speed and duplex mode to interfaced equipment. Auto negotiation setting can be done by following command.

1000BASE-X gigabit port requires fiber optic module in the system to be activated.

Command	Mode	Function
port nego *port-number* **on**	Bridge	Set auto negotiation on the port.
port nego *port-number* **off**		Deactivate auto negotiation on the port.

Attention

G.fast ports of MG205X have different method to set auto negotiation.

Please refer to '**5.11 G.FAST Port Setting'**

Reference

MG205X has activated auto negotiation function on all ports as default.

Attention

After auto nego setting in MG205X, transmission speed or duplex mode can be changed later.

For example, if user changes transmission speed to 100Mbps after auto nego setting, new auto nego setting will be 100Mbps/Full Duplex.

Attention

1000BASE-FX port can't have auto nego setting.

Attention

Any port without activated auto nego function will not support Auto MDIX.

5.3 Port Speed Setting

MG205X can have speed setting on each port by using following command.

Command	Mode	Function
port speed *port-number* {**10** ∣ **100** ∣ **1000**}	Bridge	Set the speed of the port.

Attention

G.fast ports of MG205X have different method to set the speed of each port.

Please refer to ‘**5.11 G.FAST Port Setting’.**

Attention

1000BASE-X Gigabit port can’t have speed setting.

5.4 Duplex Mode Setting

MG205X has half duplex mode for single directional communication and full duplex mode for bi-directional communication. The bidirectional packet transmission expands 2 times bigger Ethernet bandwidth than single mode. So, in full duplex mode, 10Mbps can be 20Mbps, and 100Mbps can be 200Mbps. Before being linked, MG205X is set up by default to half duplex mode.

To set up the port to duplex mode, use following command.

Command	Mode	Function
port duplex *port-number* {**full** | **half**}	Bridge	Set up the port to duplex mode.

Following example shows setting up the port 27 from duplex mode to half duplex mode.

```
MG205X (bridge)# show port 27
-------------------------------------------------------------------------------
NO       TYPE     PVID  COS    STATUS       MODE       FLOWCTRL    INSTALLED
                            (ADMIN/OPER)           (ADMIN/OPER)
-------------------------------------------------------------------------------
 27:     Ethernet      1    0    Up/Up    Auto/Full/100     Off/ Off       Y
MG205X (bridge)# port duplex 27 half
MG205X (bridge)# show port 27
-------------------------------------------------------------------------------
NO       TYPE     PVID  COS    STATUS       MODE       FLOWCTRL    INSTALLED
                            (ADMIN/OPER)           (ADMIN/OPER)
-------------------------------------------------------------------------------
 27:     Ethernet      1    0    Up/Down  Auto/Half/0      Off/ Off       Y
MG205X (bridge)#
```

Attention

G.fast ports of MG205X have different method to set up duplex mode.

Please refer to ‘**5.11 G.FAST Port Setting’.**

Attention

100BASE-FX Ethernet and 1000BASE-X Ethernet can have only full duplex mode. User can’t change the mode of 2 ports.

5.5 Flow Control Setting

MG205X Ethernet port sends a signal of transmission stop to limit packet transmission for specific time.

In general, if there is no free space in the receive buffer, port sends a "transmission stop" message to stop the transmission of packets over a period of time. It is the same to Ethernet port. If Ethernet port receives a "stop" message from another system, it also stops the packet transmission for a period of time.

To set the transmission stop signal to the Ethernet port, use the following command.

Command	Mode	Function
port flow-control *port-number* {**on** ∣ **off**}	Bridge	Set the transmission stop signal to the Ethernet port.

Reference

Subscriber ports of MG205X are set up as default to Flow Control-Off.

Following case shows Flow Control-off (transmission stop signal – off) on port 4.

```
MG205X (bridge)# port flow-control 4 off
MG205X (bridge)# show port 4
--------------------------------------------------------------------------------
NO       TYPE     PVID  COS    STATUS       MODE       FLOWCTRL    INSTALLED
                           (ADMIN/OPER)            (ADMIN/OPER)
--------------------------------------------------------------------------------
4:        Gfast      1   0     Up/Down  Auto/Full/0      Off/ Off       Y
MG205X (bridge)#
```

5.6 Port Description

In MG205X, each port description can be registered for user’s conveniences. To register the description of each port, use following command.

Command	Mode	Function
port description *port-number description*	Bridge	Register the description of the port.

To delete the description of each port, use following command.

Command	Mode	Function
no port description *port-number*	Bridge	Delete the description of each port.

To check the description of each port, use following command.

Command	Mode	Function
show port description [*port-number*]	Enable / Global / Bridge	Show the description of each port.

Following is the case of registering the descriptions of port 1 and 2.

```
MG205X (bridge)# port description 1 test1
MG205X (bridge)# port description 2 test2
MG205X (bridge)# show port description 1-2
-------------------------------------------------------------------
NO TYPE         STATE      LINK     DESCRIPTION
              (ADM/OPR)
-------------------------------------------------------------------
1 Gfast       Up/Down     0/FDX    test1
2 Gfast       Up/Down     0/FDX    test2
MG205X (bridge)#
```

5.7 Check and Initialization of Port Statistics

In MG205X, user can check average traffic of each port or interface MIB and RMON MIB data which are defined in SNMP MIB.

Following commands are used to check average traffic of each port or interface MIB and RMON MIB data which are defined in SNMP MIB.

Command	Mode	Function
show port statistics avg [*port-number*]	Enable / Global / Bridge	Show average traffic of the port.
show port statistics avg type [*port-number*]		Show average traffic of the port classified by traffic types.
show port statistics avg-pkt [*port-number*]		Show average traffic of the port classified by traffic packet
show port statistics avg-pps [*port-number*]		Show average traffic of the port classified by Unicast/ Multicast/ Broadcast traffic.
show port statistics interface [*port-number*]		Show interface statistics data of the port.
show port statistics interface all-stats [*port-number*]		Show all interface information of the port.
show port statistics packet-buffer [*port-number*]		Show packet information per queue of the port.
show port statistics rmon [*port-number]*		Show RMON MIB data of the port.

To remove the recorded statistics of the port to initialize, use following command.

Command	Mode	Function
clear port statistics {*port-number* | **all**}	Enable	Remove the recorded statistics of the port to initialize.

Following is the case to check average traffic of the port 27.

```
MG205X (bridge)# show port statistics avg-pkt 27
================================================================
   Port   |           Tx           |          Rx
----------------------------------------------------------------
   Time   |  pkts/s  |    bits/s    |  pkts/s  |    bits/s
================================================================
port    27 ---------------------------------------------------
    5 sec:         0            0         0            0
    1 min:         0            0         0          128
   10 min:         0            0         0           64

MG205X (bridge)#
```

Following is the case to check the interface MIB information of the port 1.

```
MG205X (bridge)# show port statistics interface 1
--------------------------------------------------------------------------------
Port No.1                        Interfaces Statistics
--------------------------------------------------------------------------------
IfInOctets        :          150,290 IfOutOctets      :              128
IfInUcastPkts     :                2 IfOutUcastPkts   :                1
IfInMcastPkts     :              470 IfOutMcastPkts   :                0
IfInBcastPkts     :               90 IfOutBcastPkts   :                1
IfInNUcastPkts    :              560 IfOutNUcastPkts  :                1
IfInDiscards      :              465 IfOutDiscards    :                0
IfInErrors        :                0 IfOutErrors      :                0
IfInPauseFrame    :                0 IfOutPauseFrame  :                0
IpFwDatagrams     :                0 IpInReceives     :                0
IfType            :                6 IfSpeed          :         1000Mbps
IfMtu             :             1500 IfLastChange(msec):           7,302
IfAdminStatus     :               UP IfOperStatus     :               UP
IfPhysAddress     :  00:d0:cb:ff:ed:13 IfSpecific      :                0
IfInUnknownProtos :                0 IfDescr          :      port8-Gfast
IfOutQLen         : 0

MG205X (bridge)#
```

Following is the case to check the RMON MIB information of the port 1.

```
MG205X (bridge)# show port statistics rmon 1
--------------------------------------------------------------------------------
Port No.1                        RMON Statistics
--------------------------------------------------------------------------------
The Index of statsv :          1  (Port 18)
DropEvents          :               0 Jabbers              :               0
```

```
Octets              :          163,216 Collisions        :              0
Pkts                :              588  Pkts64Octets      :             8
BroadcastPkts       :               91  Pkts65to127Octets  :           202
MulticastPkts       :              494  Pkts128to255Octets  :          178
CRCAlignErrors      :                0  Pkts256to511Octets  :           36
UndersizePkts       :                0  Pkts512to1023Octets :          164
OversizePkts        :                0  Pkts1024to1518Octets:            0
Fragments           :                0

MG205X (bridge)#
```

5.8 Check of Port Status

To check the port status, use following command.

Command	Mode	Function
show port status [*port-number*]	Enable / Global / Bridge	Show the port status.

5.9 G.FAST Operation Method

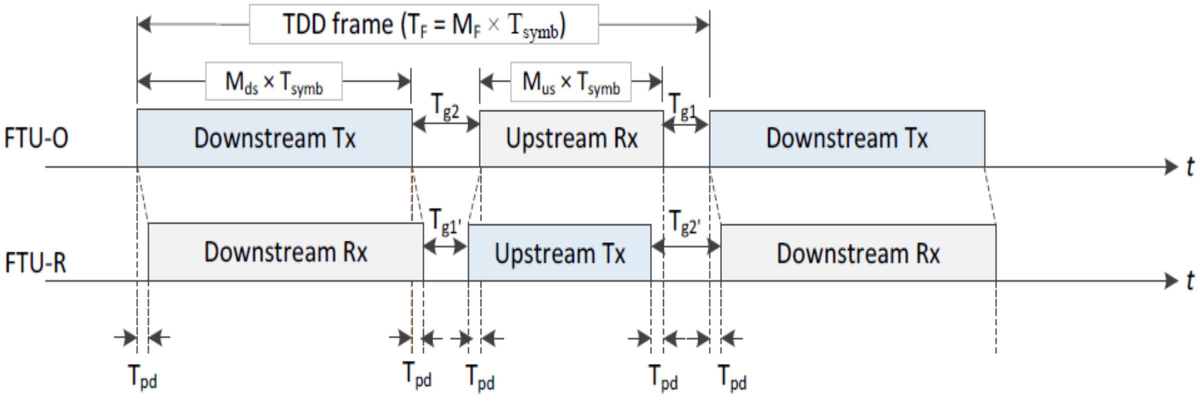
MG205X is using DSL technology, and providing internet communication and telephone communication services via existing telephone lines with up to 2Gbps aggregated data transmission speed using 2.2 ~ 212MHz.

(1) TDD (Time-Division Duplexing)

MG205X has a frame structure of the TDD scheme.

TDD method is doing Tx and Rx with time division using the same frequency in downstream and upstream.

Following figure shows the communication procedures based on TDD between FTU-O and FTU-R.



【Picture 5-1】TDD Frame Operation

(2) G.INP Retransmission

MG205X is using G.INP Retransmission to prevent data loss in the event of impulse noise.

Impulse noise is divided into SHINE and REIN, and each noise has the following characteristics.

SHINE (Single High Impulse Noise Event) - User cannot predict the frequency band of this noise event, and it has various amplitude and length.

REIN (Repetitive Electrical Impulse Noise) – This impulse noise occurs in a predictable frequency range, and it creates cross talks and interferences on external power cables.

Following is retransmission procedures.

step 1. Save the DTU in ReTx queue and send it to the Receiver.

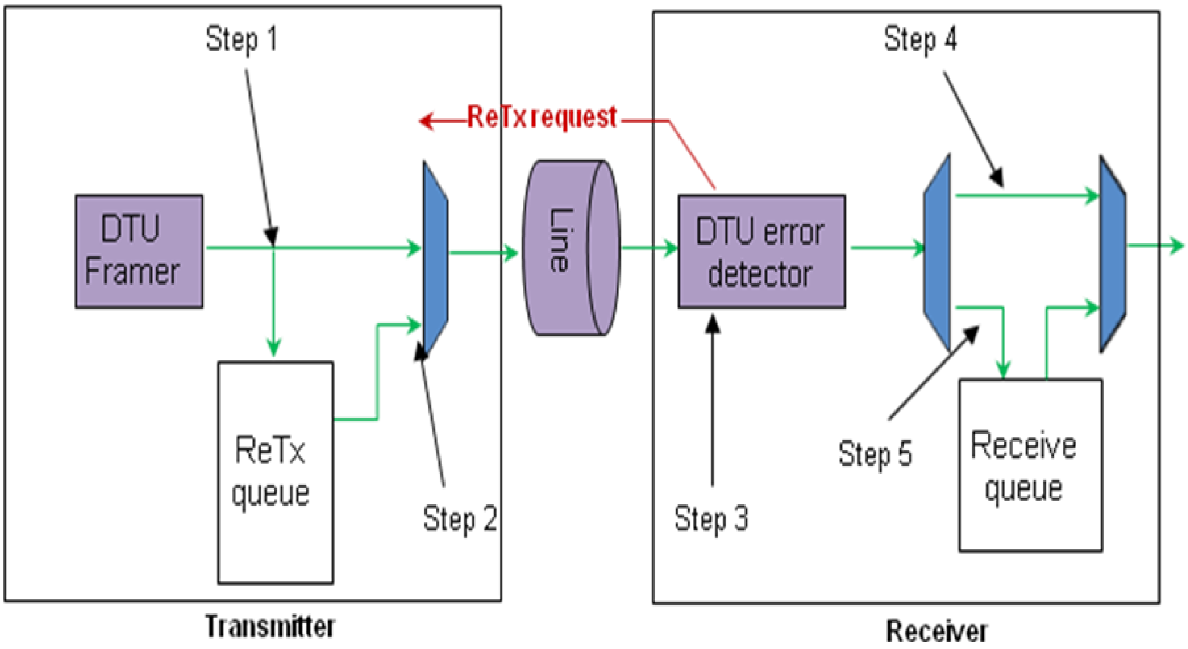
step 2. If there is a Retransmission Request, DTU stored in ReTx queue is resent to Receiver.

step 3. If DUT is received with error, Retransmission is to be requested to Transmitter.

step 4. If retransmission is not occurred, received DTU is passed to the upper layer.

step 5. If retransmission is occurred, received DPU is to be saved in Receive queue.

If failed DUT is repaired afterwards, queued DUT is to be passed to the upper layer in order.



【Picture 5-2】Retransmission Operation

5.10 G.FAST Symbol Position Settings

MILEGATE-204x is using TDD method, and downstream and upstream speeds ratio are decided by the ratio of M_{ds} (Number of Downstream symbol position in TDD frame) and M_{us} (Number Upstream symbol position in TDD frame).

MG204X is using 36 as fixed value of M_f (Number of symbol period in TDD frame).

$M_f = M_{ds} + M_{us} + 1$ (‘1’ is the gap-time between upstreamTx and downstreamRx)

Use the following command to set the Mds of G.FAST DSP.

Command	Mode	Function
dsp mds *<10-32>*	GFAST	Set the Mds value of all DSP.

Attention

After changing Mds value, DSP needs to be restarted to use changed setting. Reloading of system is recommended for this.

Reference

Mds value settings change the speed ratio of DS(downstream) and US(upstream) as followings;

DS = Mds / (Mf - 1), US = (Mf - Mds -1) / (Mf - 1)

DS : US ratio in relation to Mds value

8 : 2 = Mds is 28

7 : 3 = Mds is 25

6 : 4 = Mds is 21

5 : 5 = Mds is 18

4 : 6 = Mds is 14

Mds settings can be checked by following command.

Command	Mode	Function
show gfast dsp info	Enable /Global/ GFAST	Show the detailed status information of the MDS.

5.11 G.FAST Port Settings

MG205X user can apply and activate Config files to G.FAST port.

(1) G.FAST Port Status Check

In MG205X, user can verify the G.FAST port status or can check the setting details of G.Fast port. Check the port status of G.FAST by using the following commands.

Command	Mode	Function
show gfast line status *port-number*	Enable/ Global/ GFAST	Show the basic status information of the numbered G.FAST port.
show gfast line status detail *port-number*		Show the detailed status information of the numbered G.FAST port.

The above commands will provide the following information respectively. Therefore, please select the appropriate command based on the required information.

【Provided information from command 'line status'】

구분	내용
State	It shows connection status between CO and related network and shows the status of port to be configured.
Line Rate	It shows max. throughput of Ethernet frame on G.FAST line.
Data Rate	It shows Ethernet frame transmission rate excluding G.FAST RMC (Robust Management Channel) transmission rate.
SNRM	It shoes SNR margin of current line.
Output Power	It shows signal power in dMm between CO and CPE
port Profile	It shows the ID of config profile applied to the G.FAST.
Aggregate Data Rate	It shows total transmission rate of upstream and downstream data-rate of the G.FAST line.
Attainable Data Rate	It shows attainable max rate of upstream and downstream data-rate of the G.FAST line under restricted conditions of delay and coding.
Actual Inp	It shows guaranteed actual INP(symbol) in latency path.
Actual Inp Rein	It shows guaranteed actual INP(symbol) to REIN noise in latency path.
LPR Status	It shows the LNR occurrence status on the current line.
Uptime	It shows the amount of time(seconds) after the showtime status on the line.

```
MG205X # show gfast line status detail 3

Port 3
---------------------------------------------------------
Port Profile........................  Default
Line Status.........................  SHOWTIME
Line Protocol.......................  G.9701
Line Profile........................  212 MHz
US/DS Line Rate[Kbps]...............   292028 :   1368349
US/DS Data Rate[Kbps]...............   291687 :   1368008
Aggregate Data Rate[Kbps]...........   1360377
US/DS Attainable Data Rate[Kbps].....  292044 :   1368081
US/DS Snrm[dB]......................     8.5 :      7.6
US/DS Output Power[dBm].............     4.0 :      4.0
US/DS Actual Inp[symbol]............    319.0 :    319.0
US/DS Actual Inp Rein[symbol].......    24.0 :     24.0
Estimated Loop Length[m]............     0.0
LPR Status..........................    False
Uptime[sec].........................       5
```

----

(2) G.FAST Port ‘Enable’

G.FAST port activation is different from previously described port settings. G.FAST port activation requires synchronization setting to interfaced equipment. Therefore, even if the cable is connected between equipments, ‘disable’ setting of G.FAST port will not synchronize the connection status.

Use the following command to set the sync status of G.FAST port.

Command	Mode	Function
line admin enable *port-number*	GFAST	Set the port synchronized to the connected equipment.
line admin disable *port-number*		Set the port not-synchronized(disable) to the connected equipment. The disabled port will be changed to CONFIG status.
line reset *port-number*		Reset the port synchronized to the connected equipment. The G.fast line will be reset, but disabled port will not be reset.

Attention

G.FAST ports of MG205X are set to be synchronized to the connected equipment by default.

Following case is a setting of not-synchronized(disabled) line between G.FAST port 1 and connected equipment.

```
MG205X (config-gfast)# show gfast line status 1
--------------------------------------------------------------------------------
 Port |     State     |   LineRate    |   DataRate    |    SNR    | TX Power
      |    ADM/OPR    |  US/DS[Mbps]  |  US/DS[Mbps]  | US/DS[dB]| US/DS[dBm]
--------------------------------------------------------------------------------
   1  |  ON / SHOWTIME |   293 /   1396|   292 /   1395|  6.1/ 4.3|  3.9/ 4.0
--------------------------------------------------------------------------------
MG205X (config-gfast)# line admin disable 1
MG205X (config-gfast)# show gfast line status 1
--------------------------------------------------------------------------------
 Port |     State     |   LineRate    |   DataRate    |    SNR    | TX Power
      |    ADM/OPR    |  US/DS[Mbps]  |  US/DS[Mbps]  | US/DS[dB]| US/DS[dBm]
--------------------------------------------------------------------------------
   1  | OFF / CONFIG   |     0 /     0 |     0 /     0 |  0.0/ 0.0 |  0.0/ 0.0
--------------------------------------------------------------------------------
```

(3) Active Line Noise PSD per subcarrier group Check

To check the line noise PSD value per sub-carrier group of specific port, use the following command.

Command	Mode	Function

show gfast line aln *port-numbr*	Enable/Global/GFAST	Show ALN value of the port.(DownStream only)

(4) Bit Allocation Check

The 'BitAlloc' is the number of bit that can be carried per tone and the maximum of G.FAST specification is 12bit per tone. MG205X administrators need to change the settings of Ham-band or Option-band, or need to check the Bitalloc value if the G.Fast line has cross talks. To check the BitAlloc per sub-carrier, use following command.

Command	Mode	Function
show gfast line bitalloc {ds | us} *port-numbr*	Enable/Global/ GFAST	Show the value of Bit allocation on the port.

(5) HLOG Check

HLOG indicates the size of log scale channel transfer function of 4 sub-carriers by group. To check the HLOG value per sub-carrier group of specific port, use the following command.

Command	Mode	Function
show gfast line hlog {ds | us}*port-numbr*	Enable/Global/GFAST	Show HLOG value of the port.

(6) QLN Check

QLN is the value of quiet line noise PSD of the 4 subcarriers by group. To check the QLN per sub-carrier group of ports, use the following command.

Command	Mode	Function
show gfast line qln {ds | us} *port-numbr*	Enable/ Global/ GFAST	Show the QLN per sub-carrier group of the port.

(7) SNR Check

SNR indicates 'signal-to-noise ratio' of the subcarrier. To check the SNR per sub-carrier of ports, use the following command.

Command	Mode	Function
show gfast line snr {ds | us} *port-numbr*	Enable/Global/ GFAST	Show the SNR per sub-carrier of the port.

(8) SELT (Single Ended Loop Test)

To setup single ended loop test, use the following command.

Command	Mode	Function
line selt config <loc_ROW|loc_US> <awg22 | awg24 | awg26 | pe0_32mm | pe0_4mm | pe0_5mm | pe0_63mm | pe0_9mm | tp100 | tp150>	GFAST	Loop test-settings of test area and cable type
line selt start port-number	GFAST	Loop test-start

Reference

SELT-start can be done only when the port is disabled.

"line admin disable <port>" command will disable the port prior to SELT-start.

Reference

SELT-start takes about 15 seconds for the test. If "**line selt analyse** <port> command is executed before the test is finished, error message will be shown. In this case, SELT analysis can be done after some time.

To check the result of SELT (Single ended loop test), use the following command.

Command	Mode	Function
show gfast line selt config	Enable/Global/GFAST	Loop test-Setting of test area and cable type will be shown.
show gfast line selt result	Enable/Global/GFAST	Result of 'SELT analyse' will be shown.

Following is an example of SELT on port 1 of G.Fast.

```
MG205X (config-gfast)# line selt config loc_ROW pe0_5mm
MG205X (config-gfast)# line selt start 1
MG205X (config-gfast)# line selt analyse 1
 Looking for line 8 SELT results...
 Done! SELT analyse for line 1
MG205X (config-gfast)# show gfast line selt result
```

```
PORT : 1
-----------------------------------------------------------------------------------------------------------------------------------------------------------------
 Refl.|Valid|Delay |Error     |Atn@180kHz|Atn@300kHz|Atn@1MHz  |FitError  |Termination|Loop Type|Loop length|Match Error
 0     | Yes |2.7        |0.0         |-1.9        |-2.4        |-4.4        |0.0         |1.00          | PE 0.5mm|        224 m|       0%
 1     | No   |2.7        |0.6         |-5.6        |-3.1        |5.0         |1.1         |1.00          | PE 0.5mm|            0 m|       0%
 2     | Yes |58.7       |19.7        |-41.8       |-39.4       |-30.6       |5.3         |1.00          | PE 0.5mm|       3685 m|      24%
 3     | No   |65.4       |12.0        |-34.4       |-36.4       |-43.6       |7.6         |0.00          | PE 0.5mm|       3405 m|      37%
Loop type PE 0.5mm, Loop length 224 m, fitError 0 %
Downstream capacity =   28800 kbps (AWGN (-140dBm/Hz), 6.0 dB margin, 480 tones)
Upstream capacity     =     1560 kbps (AWGN (-140dBm/Hz), 6.0 dB margin, 26 tones)
-----------------------------------------------------------------------------------------------------------------------------------------------------------------
```

5.12 Line Counter Check of G.Fast Port

MG205X can check the occurred errors and the information from the G.FAST port.

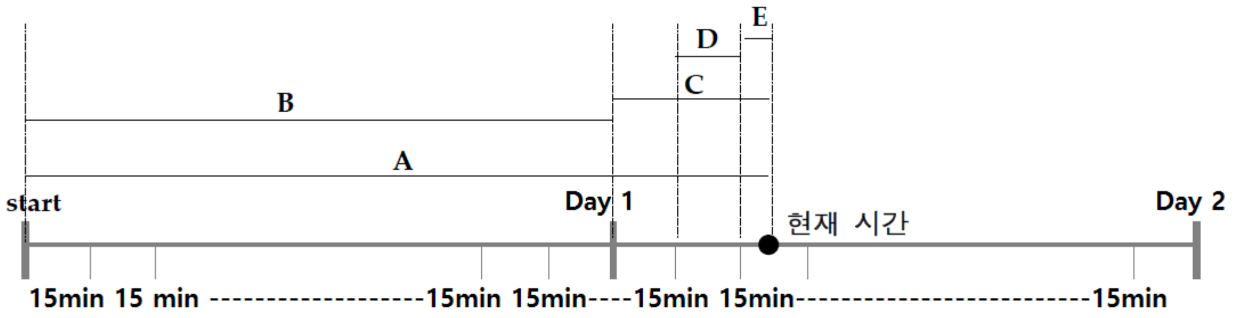
(1) Check of Error Counts and Retransmission Counts

MG205X can check the number of errors that occurred in G.Fast line.

These error occurrences will be counted at every 15 minutes from the turn-on time of the equipment, and the error counts will be reset to '0' after 15 minutes. In addition, this error counts are checked by day, and this will be reset to 0 after a day. Therefore, if you check the error count of the current time, from the moment you turn the MG205X on the equipment, it will show error counts of current 15 minutes period and previous 15 minutes period.

In addition, error counts of current day (current 24 hours) and earlier day (previous 24 hours) can be checked with total running error counts from turn-on time of the equipment.

It will be easier to understand the basis of the error counts provided by the MG205X as shown below.


E
D
C
B
A
start
Day 1
Day 2
현재 시간
15min 15 min -------------------15min 15min----15min 15min-------------------------15min

A period : Total

B period : Previous 24 Hours

C period : Current 24 Hours

D period : Previous 15 Min

E period : Current 15 Min

【Picture 5-3】Error Count Principle

To check the line counter of G.Fast port in MG205X, use following command.

Command	Mode	Function
show gfast line statistics *period port-number*	Enable/Global/ GFAST	Check the line counter of the G.Fast port during the period.

Following is the line counter of current 15 minutes on port 1.

```
MG205X (config-gfast)# show gfast line statistics 0 1
------------------------------------------------------------------
Port 1:(current 15min)
------------------------------------------------------------------
US Min Eftr       :          0  DS Min Eftr       :          0
US Fecs           :          0  DS Fecs           :          0
US Loss           :          0  DS Loss           :          0
US Es             :          0  DS Es             :          0
US Ses            :          0  DS Ses            :          0
US Uas            :        373  DS Uas            :        373
US Cv             :          0  DS Cv             :          0
US Lols           :          0  DS Lprs           :        373
US Uncorr. Cw     :          0
US RtxCw          :          0  DS Rtx Cw         :          0
US Rtx Corr. Cw   :          0
US Rtx Uncorr. Cw  :          0  DS Rtx Uncorr. Cw  :          0
Full Init Count   :          0
Fast Init Count   :          0
MG205X (config-gfast)#
```

Items	Information
Min Eftr	Minimum value of **Error Free Throughput** is shown in kbps.
Fecs	Count of **Forward error correction in 1 second**, which is more than 1.
Loss	Count of **LOS error in 1 second**, which is more than 1.
Es	Count of errors, such as **CRC, LOS, LOR etc. in 1 second**, which is more than 1.
Ses	Count of errors, such as **CRC, LOS, LOR etc. in 1 second**, which is more than 18.
Uas	Count of line error **in 1 second** which user can't use the G.FAST line.

Cv	Count of Superframe a CRC-8 error.
Lol	Count of error which is **Loss of Link**.
Lpr	Count of error which interfaced CPE has **Loss of Power**.
Uncorrect Cw	Count of **Uncorrected(unmodified) code words.**
Rtx Cw	Count of **retransmitted code words**.
Rrx Correct Cw	Count of **Corrected(modified) code words after retransmission**.
Rtx Uncorrect Cw	Count of **Uncorrected(unmodified) code words** which is left in buffer.

To initialize Line Statistics Counter and Event Counter of G.FAST ports in MG205X, use following command.

Command	Mode	Function
clear gfast port *port-number*	Enable/Global/ GFAST	Initialize the count of Line Counter of the G.FAST port.

(2) Event Counter Check

Event Counter shows the number of events in G.Fast Line.

To check the event counter of G.AST ports in MG205X, use following command.

Command	Mode	Function
show gfast line event *period* *port-number*	Enable/Global/ GFAST	Check to show the number of event of the G.AST port.

Following shows the number of event on the G.FAST port 1 during the current 15minutes.

```
MG205X (config-gfast)# show gfast line event 0 1

Port 1 (current 15min)
---------------------------------------------------------
US/DS LOS.................         0 :         0
US/DS LOM.................         0 :         0
US/DS LOR.................         0 :         0
LPR.......................         0
LOL.......................         0
US/DS BS..................         0 :         0
US/DS RAU.................         0 :         0
US/DS RAD.................         0 :         0
US/DS FRA.................         0 :         0
US/DS RPA.................         0 :         0
TIGA......................         0
---------------------------------------------------------
```

Items	Information
LOS	Count of LOS(Loss of Signal) event from US/DS(upstream/downstream).
LOM	Count of LOM(Loss of Margin) event from US/DS(upstream/downstream).

LOR	Count of LOR(Loss of RMC) event from US/DS(upstream/downstream).
LPR	Count of LPR(Loss of Power) event which supplied power voltage to MODEM is lower than specified level.
LOL	Count of LOL(Loss of Link) event.
BS	Count of BitSwap event from US/DS(upstream/downstream).
RAU	Count of SRA Upshift event from US/DS(upstream/downstream).
RAD	Count of SRA Downshift event from US/DS(upstream/downstream).
FRA	Count of FRA event from US/DS(upstream/downstream).
RPA	Count of RPA event from US/DS(upstream/downstream).
TIGA	Count of TIGA event from US/DS(upstream/downstream).

5.13 CPE Inventory Check

User can check the vendor, Serial Number and software version of the CPE using the following command.

Command	Mode	Function
show gfast cpe-inventory PORTS’	Enable / Global / gfast	Show the CPE inventory information.

The following case is an example.

```
MG205X (config-gfast)# show gfast cpe-inventory 1
Port 01:
  Vendor ID     :
  Serial Number :
  Version   : AfH042o_rc91
```

5.14Config-Profile Setting

A specified profile can be applied to G.FAST port as a setting policy in MG205X. Line Config Profile is a set policy of the Band Plan, SNR margin G.FAST line, PSD mask, Retransmission and more. This feature is useful when an ISP apply rated services to customers. User can specify various grades of profiles to apply it by the policies of each port.

(1) Gfast line config profile Setting

Here's how to set the Gfast Line Config Profile. 4 steps.

Step 1. To set the Gfast Line Config Profile, please enter into Gfast-profile configuration mode.

To enter the Gfast Line Config Profile Settings mode, use the following command in Gfast setting mode.

Command	Mode	Function
profile *profile-name*	GFAST	Enter into Gfast-profile setting mode.

Following is an example.

Gfast Line Config Profile is to be set under the name of ‘TEST’ in Config Profile Setting mode.

```
MG205X # configure terminal
MG205X (config)# gfast
MG205X (config-gfast)# profile TEST
MG205X (gfast-profile[TEST])#
```

To get out of G.Fast Config Profile Setting mode, use following command.

Command	Mode	Function
exit	Gfast-profile	Get out of Config Profile Setting mode(Gfast-profile).

Step 2. Profile contents setting. Use following commands to do profile contents setting.

Command	Mode	Function
Active	Gfast-Profile	This applies profile and profile-vdsl settings to the designated port.
bandplan *<ds | us><lower | upper> <43-4090>*		This sets the Sub-Carrier range to be used. The unit is 51.75kHz.
lor-persistency *<ds | us> <1-20>*		This sets the LOR Persistency of G.FAST line. The unit is 100ms.
lom-persistency <ds | us> <2-20>		This sets the time-limit of LOR persistency under fast retrain occurance. Time-limit is in seconds.
los-persistency <ds | us> <1-20>		Set the LOS Persistency of G.FAST line. The unit is 100ms
target-margin *<ds | us> <0-310>*		Set the SNR margin of G.FAST line. The unit is 0.1dB.
max-margin *<ds | us> <0-310>*		Set the maximum SNR margin. The unit is 0.1dB.
min-margin *<ds | us> <0-310>*		Set the minimum SNR margin. The unit is 0.1dB.
max-tx-power *ds <-50 - 200>* **max-tx-power** *us <-130 - 200>*		Set the maximum Tx Power. The unit is 0.1dBm.
sra-mode *<ds | us> <disable | enable>*		Set the operation of SRA(enable or disable)
sra-downshift-margin *<ds | us> <0-310>*		Based on the SNR Margin, it sets the down-shift value which SRA is operating. The unit is 0.1dB.
sra-upshift-margin *<ds | us> <0-310>*		Based on the SNR Margin, it sets the up-shift value which SRA is operating. The unit is 0.1dB.

sra-downshift-delay *<ds | us> <0-16383>*	Gfast-Profile	Set the SNR Monitoring Time until when SNR down-shift value operates. The unit is 1sec.
sra-upshift-delay *<ds | us> <0-16383>*		Set the SNR Monitoring Time until when SNR up-shift value operates. The unit is 1sec.
rpa-mode *<ds | us> <disable | enable>*		Set the operation of RPA(disable, enable)
target-margin-rmc *<ds | us> <0-310>*		Set the SNR margin of RMC channel. The unit is 0.1dB.
min-margin-rmc *<ds | us> <0-310>*		Set the minimum SNR margin of RMC channel. The unit is 0.1dB.
profile-map <106a | 106b | 212a>		Set the G.fast profile protocol to be activated.
profile-map *<106a | 106b | 212a>*		Set the G.fast profile protocol to disable.
(no) retrain-allowed		Enable the PSD optimization feature. When the function is activated, the output power changes according to the line status.
max-bitloading-rmc *<ds | us> <2-6>*		It sets the maximum bit load size of the RMC channel.
fra-mode *<ds | us> <disable | enable>*		Set the operation of FRA(disable, enable)
fra-time *<ds | us> <0-8>*		Specify the time window size that monitors FRA. Time window size range is 1 ~ 8, and the unit is logical frame length.
fra-ntones *<ds | us> <0-100>*		Set the minimum percentage of sub-carrier deteriorated by FRA generating condition. The unit is %.
fra-rtxuc *<ds | us> <0-1023>*		Set the number of rtx-uc error by FRA generating condition.
max bitloading per tone[bit] <12/14>		Set the Max Bitloading per tone. The unit is 12 or 14 bit.
fra-vendisc *<ds | us> <enable | disable>*		Set the usage(enable, disable) of FRA generating conditions specified by provider.
max-ndr <ds | us> <16000-2000000>	Gfast-profile	Set the maximum transmission speed of G.FAST line. The unit is 1kbps.
rtx-etr-min *<ds | us> <1-"max-ndr">*		Set the minimum transmission speed expected (expected throughput rate). The unit is kbps.
rtx-max-delay <ds | us> <1000-16000>		Set the maximum retransmission delay. The unit is µsec, and can be entered by 250µsec unit.
rtx-inp-min-shine *<ds | us> <0-1040>*		Set the minimum impulse noise protection value. The unit is 0.5symbol.
rtx-inp-min-rein *<ds | us> <0-126>*		Set the minimum impulse noise protection values against

	REIN. The unit is 0.5 symbol.
rtx-shine-ratio *<ds | us> <0-100>*	Set the rate of NDR loss which is needed to compensate for SHINE noise. The unit is 0.001unit.
rtx-rein-flag *<ds | us> <0-3>*	Set REIN inter-arrival time. Setting value is 0:100Hz, 1:120Hz, 2: 300Hz and 3:360Hz.
rtx-rn-ratio *<ds | us> <0-8>*	Set the ratio of minimum requirement in R_{FEC} / N_{FEC}. The unit is 1/32.
tx-method *<gfast-only | vdsl-fallback | vdsl-only>*	Set the protocols to be supported in G.fast line.
upbo *<enable|disable> <A> <B> <kl0>*	Set the upstream power back-off function.

Reference

Sub-carrier (Tone) has steps of 51.75kHz. For example, if band plan setting is 43 – 2043, user can use 2.2 ~ 212MHz.

Reference

Some parameters can't be set by the relations to the other parameters.

Minimum value of DS Band-Plan should be smaller than the minimum value of US Band-Plan, and maximum value case is the contrary case. Target margin should be bigger than SRA down-shift- margin, and should be smaller than up-shift-margin.

To check the settings, use following command.

Command	Mode	Function
show gfast profile *profile-name*	Enable/Global/GFAST/ Gfast-profile	Show the settings of Line Config Profile.

Step 3. Profile setting details should be applied to the ports by following command.

Command	Mode	Function
profile *profile-name* **add** *port-number*	GFAST	Apply the profile settings to the port.

To check the availability of profile settings, use following command.

Command	Mode	Function
show gfast profile associate	Enable/Global/GFAST/	Show available G.Fast profile settings.

	Gfast-profile	

Following is a case that the profile settings are applied to the corresponding port.

```
MG205X (config-gfast)# profile TEST add 1-8
MG205X (config-gfast)# show gfast profile associate
----------------------------------------------------------------
 Line Number...................       Profile Name | Status
 Line 1........................             TEST | Active
 Line 2........................             TEST | Active
 Line 3........................             TEST | Active
 Line 4........................             TEST | Active
 Line 5........................             TEST | Active
 Line 6........................             TEST | Active
 Line 7........................             TEST | Active
 Line 8........................             TEST | Active
----------------------------------------------------------------
```

To make changes of profile details, use following command.

Command	Mode	Function
active	Gfast-profile	Activate the profile.

Following is a case that changed profile settings are applied to the ports again.

```
MG205X (gfast-profile[TEST])# max-ndr ds 500000
MG205X (gfast-profile[TEST])# show gfast profile associate
----------------------------------------------------------------
 Line Number...................       Profile Name | Status
 Line 1........................             TEST | Deactivate
 Line 2........................             TEST | Deactivate
 Line 3........................             TEST | Deactivate
 Line 4........................             TEST | Deactivate
 Line 5........................             TEST | Deactivate
 Line 6........................             TEST | Deactivate
 Line 7........................             TEST | Deactivate
 Line 8........................             TEST | Deactivate
----------------------------------------------------------------
MG205X (gfast-profile[TEST])#

MG205X (gfast-profile[TEST])# active
MG205X (gfast-profile[TEST])# show gfast profile associate
----------------------------------------------------------------
 Line Number...................       Profile Name | Status
 Line 1........................             TEST | Active
 Line 2........................             TEST | Active
 Line 3........................             TEST | Active
 Line 4........................             TEST | Active
 Line 5........................             TEST | Active
 Line 6........................             TEST | Active
 Line 7........................             TEST | Active
```

```
    Line 8........................              TEST | Active
    ----------------------------------------------------------------
   MG205X (gfast-profile[TEST])#
```

To release the profile settings applied to specific port, use following command.

Command	Mode	Function
profile *profile-name* **del** *port-number*	GFAST	Release the profile settings applied to the port.

Step 4. Profile settings are to be saved.

```
MG205X # write memory
[OK]
MG205X #
```

On the other hand, profile settings can be deleted by following command.

Command	Mode	Function
no profile *profile-name*	GFAST	Erase the profile.

Reference

After **using ‘profile** *profile-name* **del** *port-number*‘ and ‘**no profile** *profile-name*‘ commands, the ports will have default profile after removal of the profiles.

(2) Vdsl line config profile Setting

Here's how to set the Vdsl Line Config Profile.

Step 1. Set the Vdsl Line Config Profile. As the Vdsl profile index is included in the Gfast profile index, creating a G.fast profile(1 or more) should be advanced to Vdsl-profile Setting mode.

To enter the Vdsl Line Config Profile Settings mode, use the following command in Gfast setting mode.

Command	Mode	Function
profile-vdsl *profile-name*	GFAST	Enter into Vdsl-profile Setting mode.

Following is the case which user enter into Config Profile Setting mode to set Vdsl Line Config Profile under the name of ‘TEST’.

```
MG205X # configure terminal
MG205X (config)# gfast
MG205X (config-gfast)# profile TEST
MG205X (gfast-profile[TEST])# exit
```

```
                MG205X (config-gfast)# profile-vdsl TEST
                MG205X (vdsl-profile[TEST])#
```

To get out of Config Profile Setting mode, use following command.

Command	Mode	Function
exit	Vdsl-profile	Get out of Vdsl-profile Setting mode.

Step 2. Profile Setting. Following commands are used for profile setting.

Command	Mode	Function
Active	Vdsl-profile	Applies Profile and profile-vdsl settings to the specified port.
shape < 997-M1c-A-7 | 997-M1x-M | 997-M1x-M-8 | 997-M2x-A | 997-M2x-M | 997-M2x-M-8 | 997E17-M2x-A | 997E30-M2x-NUS0 | 998-M1-NUS0 | 998-M1x-A | 998-M1x-B | 998-M2x-A | 998-M2x-B | 998-M2x-M | 998-M2x-NUS0 | 998ADE17-M2x-A | 998ADE17-M2x-B | 998ADE17-M2x-M | 998ADE17-M2x-NUS0-M | 998ADE30-M2x-NUS0-A | 998ADE30-M2x-NUS0-M | 998ADE35-M2x-A | 998ADE35-M2x-B | 998ADE35-M2x-M | 998E17-M2x-A | 998E17-M2x-NUS0 | 998E17-M2x-NUS0-M | 998E30-M2x-M | 998E30-M2x-NUS0 | 998E35-M2x-A | adlu-128 |		Set the shape to use

adlu-32 | adlu-36 | adlu-40 | adlu-44 | adlu-48 | adlu-52 | adlu-56 | adlu-60 | adlu-64 | eu-128 | eu-32 | eu-36 | eu-40 | eu-44 | eu-48 | eu-52 | eu-56 | eu-60 | eu-64 | hpE17-M1-NUS0 | hpE30-M1-NUS0 | nus0 >	Vdsl-profile	
profile-map <8a | 8b | 8c | 8d | 12a | 12b | 17a | 30a>		Set the VDSL profile protocol to be activated
no profile-map *<8a | 8b | 8c | 8d | 12a | 12b | 17a | 30a>*		Set the VDSL profile protocol to be deactivated
Channel <fast | slow>		Set the operation mode of channel
ghs {a43 | b43 | a43c-b43c | v43} | none)		Set the G.handshake tone carrier set of each port
target-margin *<ds | us> <0-310>*		Set the SNR margin of the VDSL line. The unit is 0.1dB.
max-margin *<ds | us> <0-310>*		Set the maximum SNR margin. The unit is 0.1dB. -1 is used when no margin is applied.
target-margin *<ds | us> <0-310>*		Set the SNR margin of the VDSL line. The unit is 0.1dB.
max-margin *<ds | us> <-1-310>*		Set the maximum SNR margin. The unit is 0.1dB.
min-margin *<ds | us> <0-310>*		Set the minimum SNR margin. The unit is 0.1dB.
max-tx-power <-256 - 40>		Set the maximum Tx Power. The unit is 0.1dBm.
max-rx-power <-256 - 256>		Set the maximum Rx Power. The unit is 0.1dBm.
max-delay <ds | us> <1-100>		Set the maximum Delay. The unit is 1ms
sra-mode *<ds | us> <disable | enable>*		Set the operation of SRA(enable or disable).
sra-downshift-margin *<ds | us> <0-310>*		Based on the SNR Margin, it sets the down-shift value which SRA is operating. The unit is 0.1dB.
sra-upshift-margin *<ds | us><0-310>*		Based on the SNR Margin, it sets the up-shift value which SRA is operating. The unit is 0.1dB.
sra-downshift-delay *<ds | us><0-16383>*		Set the SNR Monitoring Time until when SNR down-shift value operates. The unit is 1sec.
sra-upshift-delay *<ds | us> <0-16383>*		Set the SNR Monitoring Time until when SNR up-shift value operates. The unit is 1sec.
sos-mode *<ds | us> <disable | enable>*		Set the operation of SOS.
sos-min-rate *<ds | us> <0-100000>*		Set the minimum transmission speed of SOS. The unit is 1Kbps.

sos-time *<ds | us> <64-16320>*	Set the time window to check the SOS event. The unit is 1ms.
sos-crc *<ds | us> <0-65535>*	Set the CRC trigger condition of SOS. The unit is 0.02unit.
sos-ntone *<ds | us> <0-100>*	Set the SOS tone as degraded condition. The unit is%.
sos-max *<ds | us> <0-15>*	Set the maximum number of SOS operations for 120 seconds
rtx-max-ndr *<ds | us> <64-512000>*	Set the maximum transmission speed of VDSL line. The unit is 1kbps.
rtx-etr-max *<ds | us> <64-"max-ndr">*	Set the maximum transmission rate (expected throughput rate). The unit is 1kbps.
rtx-etr-min *<ds | us> <64-"max-ndr">*	Set the minimum transmission rate (expected throughput rate). The unit is 1kbps.
rtx-max-delay *<ds | us> <0-63>*	Set the maximum retransmission delay. The unit is msec.
rtx-min-delay *<ds | us> <0-63>*	Set the minimum retransmission delay. The unit is msec.
rtx-inp-min *<ds | us> <0-63>*	Set the minimum impulse noise protection values. The unit is 1symbol.
rtx-min-rein *<ds | us> <0-7>*	Set the minimum impulse noise protection values against REIN. The unit is 1symbol.
rtx-shine-ratio *<ds | us> <0-255>*	Set the rate of NDR loss which is needed to compensate for SHINE noise. The unit is 0.001unit.
rtx-rein-frequency *<ds | us> <100 | 120>*	Set the REIN frequency. The settings are 100Hz, 120Hz.
rtx-rn-ratio *<ds | us> <0-64>*	Set the ratio of minimum requirement in R_{FEC} / N_{FEC}. The unit is 1/2563
rtx-ginp *<ds | us> <disable | enable>*	Sets the G.Inp mode.
ptm-mode *<ikanos | standard>*	Sets whether or not non-standard ptm mode of Ikanos cpe is compatible.
vector-mode <disable | enable>	Set the operation of VDSL Vectoring config

Reference

Some settings can be unchanged by the relation to the other settings.

Target margin is bigger than SRA down-shift- margin, and it is smaller than the up-shift-margin.

To check the setting details, use following commands.

Command	Mode	Function
show vdsl profile *profile-name*	Enable/Global/ GFAST/Vdsl-profile	Show the settings of Vdsl Line Config Profile.

Reference

Vdsl profile index is included in Gfast profile index. Same method can be applied as above 'Step 3' of '5.14.1 Gfast line config profile Setting'.

(3) Tx-method Setting

Tx-method is set to divide the frequency band when G.Fast and VDSL are mixed. VDSL is using 2.2MHz ~ 30MHz, and G.Fast is using 2.2MHz ~ 212MHz. Mode has Gfast only mode, vdsl only and vdsl fallback mode.

Here's how to set the tx-method.

Command	Mode	Function
Tx-method *<gfast-only |vdsl-fallback | vdsl only>*	GFAST-Profile	Set the tx-method.

Reference

What would be changed depending on mode is setting value of Bandplan lower of Gfast.

The setting of bandplan lower in Gfast-only mode is 43

The setting of bandplan lower in Vdsl-fallback mode is 580

The settings of bandplan lower of default and all created profiles are applied according to tx-method settings.

Reference

VDSL MODEM can't be linked in gfast-only mode.

To check the settings, use following commands.

Command	Mode	Function
show gfast profile **PROFILE_NAME**	Enable/Global/ GFAST	Show the setting details of tx-method.

Following shows tx-method settings and check.

```
MG205X (config-gfast)# profile fall
MG205X (gfast-profile[fall])# tx-method ?
  gfast-only    G.Fast Only
  vdsl-fallback VDSL Fallback
  vdsl-only     VDSL Only

MG205X (gfast-profile[fall])# tx-method vdsl-only
MG205X (gfast-profile[fall])# show gfast profile fall

------------------------------------------------------------
Profile Name............................. fall
Transmission Method...................... VDSL Only
MG205X (config-gfast)# **show running-config**
!
profile Default
  bandplan ds lower 43
  bandplan ds upper 2042
  bandplan us lower 43
  bandplan us upper 2042
  target-margin ds 80
  target-margin us 80
 !
 profile Default add 1-16
 profile fall
  bandplan ds lower 43
  bandplan ds upper 2042
  bandplan us lower 43
  bandplan us upper 2042
  target-margin ds 80
  target-margin us 80
  tx-method vdsl-only
 !
 profile-vdsl fall
 !
MG205X (config-gfast)#
```

6. System Environment

This chapter describes system environment setting, settings management, system check etc.

6.1 Environment Setting

MG205X has following environment settings.

- □ Hostname Setting
- □ Date and Time Setting
- □ Time-zone Setting
- □ NTP Setting
- □ NTP Message Address Setting
- □ SNTP Setting
- □ Terminal Screen Output Setting
- □ DNS Server Setting
- □ Login Banner Setting
- □ Fan Operation Setting
- □ Daemon ‘Disable’
- □ MAC Learning Mode Setting
- □ Software Watchdog Setting
- □ FTP Server ‘Enable’

6.1.1 Host Name Setting

Host name is shown in prompt status, and it is required to differentiate each equipment in the network.

To have new MG205X name or change the existing name, use following command.

Command	Mode	Function
hostname *name*	Global	Name the host as written name.
show running-config | include hostname		Show the host name.

Reference

The *‘name’* is new host name of the MG205X, and it is in the distinguished form of capital letter and small letter.

```
MG205X (config)# hostname DZS
DZS(config)#
```

6.1.2 Date and Time Setting

In MG205X, user can set or change the current time and date by following command. The format of date and time can be entered freely. For example, "17:25 Mar 15 2019" or "15 Mar 2019 5:25 pm".

Command	Mode	Function
clock *datetime*	Enable	Set or change the current time and date.
show clock		Show the current time and date.

This example sets the time of ‘March 23, 2019 1:50 pm.

```
MG205X # clock 23 Mar 2019 1:50 pm
MG205X # show clock
Thu, 23 Mar 2019 13:50:02 +0000
MG205X #
```

6.1.3 Time-zone Setting

Users can set the Time-zone. Please check the type of Time-zone prior to settings by following command.

Command	Mode	Function
show time-zone	Enable/Global	Show the type of time-zone..

Reference

The ‘show time-zone’ command shows only the types of Time-zone. To check the setting of Time-zone, use the ‘show clock’ command.

The following table shows the time-zone of major countries and regions belonging to the GMT time that can be set.

【Table 6-1】GMT Time

Time-zone	Country	Time-zone	Country	Time-zone	Country
GMT-12	Enigma witok	**GMT-3**	Rio de Janeiro	**GMT+6**	Rangoon
GMT-11	Samoa	**GMT-2**	Maryland	**GMT+7**	Bangkok, Singapore
GMT-10	Hawaii. Honolulu	**GMT-1**	Azores	**GMT+8**	Hong Kong, Beijing
GMT-9	Alaska	**GMT+0**	London, Lisbon	**GMT+9**	Seoul, Tokyo

GMT-8	LA, Seattle	**GMT+1**	Berlin, Rome	**GMT+10**	Sydney, Melbourne
GMT-7	Denver	**GMT+2**	Cairo, Athens	**GMT+11**	Okhotsk
GMT-6	Chicago, Dallas	**GMT+3**	Moscow	**GMT+12**	Linton Wells
GMT-5	New York, Miami	**GMT+4**	Tehran		
GMT-4	Georgetown	**GMT+5**	Delhi		

To set the Time-zone in MG205X, use the following commands.

Command	Mode	Function
time-zone *time-zone*	Global	Set the Time-zone in MG205X.
show clock		Show the Time-zone.

Reference

MG205X is set to UTC (Universal Coordinated Time) by default.

Attention

Changing the Time-zone will also change the date and time according to the time-zone that corresponds.

If user wants to delete the time-zone setting and revert to the default settings, use the following command.

Command	Mode	Function
clear time-zone	Global	Delete the time-zone setting and revert to the default settings.

The following is a case of setting to January 23, 2016, 1:50 pm, time-zone of Seoul.

```
MG205X (config)# time-zone GMT+9
MG205X (config)# exit
MG205X # clock 23 Mar 2019 1:50 pm
MG205X # show clock
Thu, 23 Mar 2019 13:50:02 GMT+0900
MG205X #
```

6.1.4 NTP Setting

NTP (Network Time Protocols) are used in matching a fine time of the MG205X to 1/1000 second to ensure the correct time on the network. NTP communicate with the NTP server constantly to match the current time and the time in MG205X.

Correct current time in MG205X is very important even to operate properly. For more information about the NTP, it can be found in STD and RFC 1119. NTP server can be officially-used one or self-built one, and can be used by entering IP address or domain name of it. NTP server that is officially used in South Korea is "time.nuri.net" with IP address "203.255.112.96".

Here is the command used to register NTP server and to set up for operation.

Command	Mode	Function
ntp *server 1* [*server 2*] [*server 3*]	Global	Register NTP server.

Reference

3 NTP servers can be registered.

To disable the NTP function, use the following command in Global Configuration Mode.

Command	Mode	Function
no ntp *server 1* [*server 2*] [*server 3*]	Global	Disable the NTP functions from your MG205X.

To check the settings for NTP, use the following command:

Command	Mode	Function
show ntp	Enable / Global	Show the NTP settings

[Setting example 1]

The following is an example of NTP server setting by 203.255.112.96. After setting, NTP function is checked.

```
MG205X (config)# ntp 203.255.112.96
MG205X (config)# ntp start
MG205X (config)# show ntp
ntp started
ntp server 203.255.112.96
MG205X (config)#
```

[Setting example 2]

Following shows the case which NTP server is disabled.

```
MG205X (config)# no ntp
MG205X (config)# show ntp
ntp stopped
MG205X (config)#
```

6.1.5 NTP Message Address Setting

If user registered an NTP server to match exact time of MG205X, the MG205X and NTP server send messages each other constantly to converge the current time of the equipment. In this case, the messages sent and received can have IP address by setting. This IP address helps NTP server identifying user equipment.

To set the IP address of messages which are sent and received from NTP server, use following command.

Command	Mode	Function
ntp bind-address *{ip-address* | *ipv6-address}*	Global	Set the IP address of messages which are sent and received from NTP server

To delete the IP address of messages, use the following command.

Command	Mode	Function
no ntp bind-address	Global	Delete the IP address of messages which are sent and received from NTP server.

6.1.6 Terminal Screen Output Setting

MG205X shows 24 rows consisting of 80 characters per row on the console terminal by default. User can change the number of rows.

To set the number of rows on the terminal screen, use the following command.

Command	Mode	Function
terminal length <0 - 512>	Enable	Set the number of lines on the terminal screen.

Reference

The console terminal screen has 24 lines.

Reference

When user sets the output rows to 0, all the information desired by the user is shown at a time.

Here is an example of 20 lines setting to the terminal screen.

```
MG205X # terminal length 20
MG205X #
```

To turn off the setting number of rows on the terminal screen, use the following command.

Command	Mode	Function
no terminal length <0 - 512>	Enable	Turn off the setting number of rows on the terminal screen

6.1.7 Login Banner Setting

MG205X can have banner message which is shown on system log-in screen before log-in. This is for the users of console terminal program or ftp, telnet. The banner can be shown before/after log-in or when log-in is failed. Using this function, system administrator can register cautions or messages to the other users.

To register the banner message to the system login screen, use the following command.

Command	Mode	Function
banner	Global	Register the banner messages to be shown before log-in.
banner login		Register the banner messages to be shown after successful log-in.
banner login-fail		Register the banner messages to be shown after log-in failure.

To delete registered banner message in the system login screen, use the following command.

Command	Mode	Function
no banner	Global	Delete the banner messages to be shown before log-in.
no banner login		Delete the banner messages to be shown after successful log-in.
no banner login-fail		Delete the banner messages to be shown after log-in failure.

To check the registered banner message, use the following command.

Command	Mode	Function
show banner	Enable/Global/Bridge	Show the registered banner message.

[Setting Example 1]

Following shows the way to register the banner message using above commands.

Reference

The following example is with "banner" command, but the three commands have the same method.

```
MG205X (config)# banner
Save & Exit : CTRL-D
```

Ctrl-D. With this key, the banner will be saved, and user will be out to system prompt.

After entering messages, enter ‘Ctrl + D’ key twice.

```
MG205X (config)# banner
Save & Exit : CTRL-D
MG205X MG205X.
Dzs GmbH.
MG205X (config)#
```

After entering ‘Ctrl-D’, user is out to system prompt.

After banner setting as above, the following message will be shown when user do log-in.

```
MG205X MG205X.
Dzs GmbH.
MG205X login:
```

Following is the banner setting cases of successful log-in and log-in failure.

```
MG205X (config)# banner login
Save & Exit : CTRL-D
Success Login
MG205X (config)# banner login-fail
Save & Exit : CTRL-D
Login Fail!!
MG205X (config)#
```

All above three cases are confirmed by following.

```
MG205X (config)# show banner
 < Login banner >
MG205X MG205X
Dzs GmbH.

 < Login success banner >
Complete!!

 < Login fail banner >
Fail!!

MG205X (config)#
```

After above settings are saved, if we try log-in to the system again, following messages will be shown.

```
************************************************************
*                                                          *
*             Boot Loader Version 02.01.0001               *
*                      Dzs GmbH.                       *
*                                                          *
************************************************************
Press 's' key to go to Boot Mode:  0
```

```
[Loading OS1 image ...]
[Image OK : os1]
Saving Environment to Flash...

Starting kernel at 0x80761870 ...



Primary instruction cache 32kB, VIPT, 4-way, linesize 32 bytes.
Primary data cache 32kB, 4-way, VIPT, cache aliases, linesize 32 bytes
CPU: BCM5300 rev 1 at 400 MHz
(syncopation)

MG205X login: root
Password:
Login incorrect

MG205X login: admin
Password:


MG205X >
```

6.2 Settings Management

User can check the detailed setting information and save the settings in the system. This setting management describes following information:

- Check of Settings
- Save(Write) Settings
- Auto Save(Write) Settings
- Settings Initialization
- Data Backup(Copy) Setting

6.2.1 Check of Settings

In MG205X, user can find the settings of MG205X for each mode. Following commands are to be used to check the setting information.

Command	Mode	Function
show running-config	All	Show the setting information.
show running-config {**admin-flow** | **arp** | **bridge** | **dns** | **full** | **hostname** | **login** | **qos** | **rmon-alarm** | **rmon-event** | **rmon-history** | **flow** | **policer** | **policy** |**snmp** | **syslog** | **time-out** | **time-zone**}		Show the selected setting information.

Attention

Only ‘show running-config’ command can be used in View mode.

Here is the case of showing the settings for Syslog.

```
MG205X # show running-config syslog
syslog start
syslog output info local volatile
syslog output info local non-volatile
!
MG205X #
```

6.2.2 Save(Write) Settings

After user downloaded new system image via TFTP / FTP server, if the user set up the MG205X or changed the contents of the settings, the user must save the new settings or changed contents to flash memory. Otherwise, previous setting or changed contents will be lost after restart or rebooting the system.

When you save the settings or changed contents to the flash memory, use the following command.

Command	Mode	Function
write memory	All	Save the settings or changed contents to the flash memory.

Attention

In View mode, this command is not supported.

The following is an example of saving the settings or changed contents.

```
MG205X # write memory
Building configuration...
[OK]
MG205X #
```

Attention

When user save the settings or changed contents to the flash memory using above command, any key shouldn’t be entered until the [OK] message is shown.

6.2.3 Settings Initialization

User can delete or change the settings for each one respectively, but initialization to the factory default is also possible. To initialize the settings to factory default, use the following command in Global Configuration Mode.

Command	Mode	Function
restore factory-defaults	Enable	Initialize the settings to factory default.
restore layer2-defaults		Initialize the settings of L2 to factory default.

Attention

After initialization by using the ‘restore factory-defaults’ command, it is necessary to reboot the MG205X. Otherwise, settings will not be initialized to factory default.

The following is the case of settings initialization of the MG205X.

```
MG205X # restore factory-defaults
Do you want to restore factory defaults? [y/n]y
MG205X # reload
```

6.2.4 Data Backup(Copy) Setting

In MG205X, user can save the settings to help restoring the broken data afterwards and maintaining system operation. User can also use the following commands described later to install the system image.

On the other hand, in MG205X, user can do the data backup by using SSH (Secure Shell) for security. By using SSH, all the data is encrypted, and traffic can be compressed to increase the efficiency of the operation.

(1) Global Mode Backup Setting

To back up the setting contents set by the user, use the following commands in Global Configuration Mode. The variable "name" can be a kind of backup file name which user names it.

Command	Mode	Function
copy running-config {*file-name* | **startup-config**}	Enable	Back up the current settings as a file name which user specified or as the settings of the startup.
copy startup-config *file-name*		Back up the settings of the Startup.
copy *file-name1 file- name2*		Back up again the file-name1 with file-name2.

To back up the settings by using FTP server or TFTP server, use the following command.

Command	Mode	Function
copy {**ftp**|**tftp**} **config upload** {*file-name* ㅣ **startup-config**}	Enable	Upload the backed-up 'file-name' to remote FTP or TFTP server or upload it to the settings of the Startup.
copy {**ftp**|**tftp**} **config download** {*file-name* ㅣ **startup-config**}		Download the backed-up 'file-name' from remote FTP or TFTP server or download it to the settings of the Startup.
copy {**ftp**|**tftp**} **os upload** {**os1**| **os2**}		Upload os to remote FTP or TFTP server.
copy {**ftp**|**tftp**} **os download** {**os1**| **os2**}		Download os from remote FTP or TFTP server.

Attention

For backup and download the settings via FTP, User should know the ID and password for interface to FTP.

Reference

While user does backup and download the settings via FTP, 'hash-on' function is activated automatically to see the file transfer rate.

To call out the backup files, use the following command in Global Configuration Mode.

Command	Mode	Function
copy *file-name* **startup-config**	Enable	Call out the backup setting file named as 'file name' to use it in the startup-config.

Attention

In order to apply the downloaded backup files to the MG205X, user must reboot the system.

(2) SSH-used Backup Setting

The client MG205X can copy a file to server or download it from the server using SSH. In addition, FTP service is very weak in security, but user can have more secured FTP service by using SSH.

To copy files or to use FTP service by using SSH, use the following commands:

Command	Mode	Function
copy {**scp** ㅣ **sftp**} **config** {**download** ㅣ **upload**} *config-file*	Enable	Upload or download data by using SSH.
copy {**scp** ㅣ **sftp**} **config download running-config**		Download the settings by using SSH.

copy {**scp** ∣ **sftp**} **key upload** *key-file*	Upload the data with authentication key by using SSH.
copy scp os {**download** ∣ **upload**} {**os1** ∣ **os2**}	Upload or download OS by using SSH.

(3) Backup File Check

To check the Startup config, use the following command.

Command	Mode	Function
show startup-config	Enable / Global / Bridge	Show Startup config file.

To check the Backed up file, use the following command:

Command	Mode	Function
show config-list	Enable / Global / Bridge	Show the backed up file list.

The following is an example in MG205X. The current settings are backed up with a file named " MG205X ", and backup file list is shown.

```
MG205X # copy running-config MG205X
[OK]
MG205X # show config-list
=========================
      CONFIG-LIST
=========================
  MG205X
MG205X #
```

(4) Backup File 'Erase'

To erase backed up file, use the following command:

Command	Mode	Function
erase config *config-file-name*	Enable/ Global	Erase(Delete) backed up setting file.
erase key *key-file-name*		Erase(Delete) backed up SSH Key file.

6.3 System Check

When there is a failure in the MG205X, the user must find the cause and check the system at any time though there is no failure. Therefore, when there is a failure in the MG205X, the user should be able to check the system's status, and should check whether the correction is made correctly after making changes in settings.

In MG205X, user can check the following items by using DSH command.

- Network Interface Check
- IP ICMP Source Routing
- Packet Routing ‘Trace’
- IP Address Check of Remote User
- MAC table Check and Deletion
- Aging Time Setting
- Equipment Operation Time Check
- New-mac Interval Setting and Check
- System Information Check
- CPU Load Check
- CPU Process Check
- Limitation number of CPU Packet in Processing
- CPU Statistics Check
- Memory Information Check
- System Image Check
- System Image Version Check
- Check of System Image File-size
- Default OS Setting
- System Temperature Check
- Tech-support Check
- Protocol Statistics Check
- Booting information Check
- Cable Length Check Per Port

6.3.1 Network Interface Check

To find out whether the MG205X is properly connected to the relevant network, the ‘ping’ command is used.

In the IP network, the ping command sends ICMP (Internet Control Message Protocol) echo messages. ICMP is an Internet protocol that informs user of the error conditions and IP packet destination information. If destination receives ICMP echo messages, destination gives response message to ICMP echo message back to sender.

To do ping test to check the network connection with the destination, use the following command in the Privilege Exec Enable mode.

Command	Mode	Function

ping ipv6 {ip-address｜host—name} [interface-name]	Enable	Run the Ping test to check the network connection with the destination.

Here is the basic setting information to do Ping tests. Before doing the Ping test in Enable mode, please enter the following basic setting information.

【Table 6-3】Basic Setting for Ping Test

Items	Default settings
Protocol [ip]	IP is default protocol which is supported to do the Ping test.
Target IP address	If user enters the IP address or hostname of destination to check the network connection, the switch sends an ICMP echo message to the destination.
Repeat count [5]	The default is 5 times. If user enter the number, the switch sends an ICMP echo message by the numbered times.
Datagram size [100]	The Default is 100 bytes. The size of Ping packet can be entered.
Timeout in seconds [2]	The default is 2 seconds. The reply to the Ping test of the packet should be received within the specified time. Otherwise, the ping test is regarded as 'failed'.
Extended commands [n]	The default is 'no'. Extended commands can be determined.

[Setting Example 1]

To check the network connection to the IP address 192.168.1.10, 3 times of the Ping test is executed as follows.

```
MG205X # ping
Protocol [ip]: ip
Target IP address: 172.16.1.254
Repeat count [3]: 3
Datagram size [100]: 100
Timeout in seconds [2]: 2
Extended commands [n]: n
PING 172.16.1.254 (172.16.1.254) 100(128) bytes of data.
Warning: time of day goes back (-394us), taking countermeasures.
108 bytes from 172.16.1.254: icmp_seq=1 ttl=255 time=0.058 ms
108 bytes from 172.16.1.254: icmp_seq=2 ttl=255 time=0.400 ms
108 bytes from 172.16.1.254: icmp_seq=3 ttl=255 time=0.403 ms
--- 172.16.1.254 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 8008ms
rtt min/avg/max/mdev = 0.058/0.581/1.632/0.542 ms
MG205X #
```

6.3.2 IP Address Check of Remote User

To check the user who is interfaced to the system, use the following command in Privilege Exec Enable mode or Global setting mode.

Command	Mode	Function
Where	Enable	Check the remote user who is interfaced to the system.

The following shows that the user with IP address 172.16.119.251 is interfaced to the system.

```
MG205X # where
 admin at ttyS0 from console for 44 minutes 18.96 seconds
 admin at ttyp0 from 172.16.119.251:1847 for 31 minutes 28.73 seconds
```

6.3.3 MAC table Check and Deletion

To check the recorded MAC table in a particular port, use the following command:

Command	Mode	Function
show mac	Enable/ Global/ Bridge	Show the MAC addresses registered in the equipment.
show mac *bridge-name*		Show the MAC addresses registered in particular interface.
show mac *bridge-name port-number*		Show the MAC addresses registered in certain ports.
show usermac [*port-number*]		Show the user's MAC address information in certain port.
show mac count [*port-number*]		Show the MAC entry statistics in certain port.

Following case shows a MAC table recorded in the default interface.

```
MG205X # show mac default
==================================================================
port          mac addr             permission     in use
==================================================================
Eth17          00:0c:f1:da:9c:09      OK             170.66
Eth18          00:0c:f1:c0:ea:d8      -               12.53
```

Reference

The above output information can be various depending on the equipment.

Reference

If the number of accessible MAC is limited, output information of exceeded MAC over limit is not shown.

Reference

MAC table can register more than one thousand MAC addresses. Therefore, if all registered information is shown at a time, it is difficult to find needed information. So, after a certain amount of information is shown with「**-more-**」at the end, it will be ready status. However, after obtaining the needed information, press the "q" key to return to the system prompt immediately without showing the rest output of the MAC table.

6.3.4 Equipment Operation Time Check

User can check the operating time of the system since it is booted. To check the operating time of the MG205X, use the following command:

Command	Mode	Function
show uptime	View / Enable / Global	Show the operating time of the system.

Following is a case of checking operation time of the MG205X.

```
MG205X # show uptime
0 days 0 hours 17 minutes 50 seconds
MG205X #
```

6.3.5 System Information Check

System information including system model name, memory capacity, type of hardware, NOS version etc. can be checked by the following command:

Command	Mode	Function
show system	View / Enable / Global	Show the system configuration information.

The following is an example which system configuration information of the equipment is checked.

```
MG205X (config)# show system

SysInfo(System Information)
    Model Name          : MG205X
    Main Memory Size     : 512 MB
    Flash Memory Size    : 64 MB
    H/W Revision        : R2A
    H/W Address         : 00:d0:cb:ff:dd:a1
    RTC Information      : M41T11
    Serial Number        : MEORRWG189A0000
    S/W Compatibility    : 2, 3
    NOS Version         : 1.00
    B/L Version         : 01.13.0010
    PLD Version         : 0x00
      MG205X (config)#
```

Reference

The output information above can be various depending on the equipment.

6.3.6 CPU Load Check

In MG205X, user can check the average usage and usage statistics of the CPU. CPU usage statistics is a record of the average CPU utilization for five seconds, 1 minute and 10 minutes.

To check the average CPU usage of MG205X, use the following commands.

Command	Mode	Function
show cpuload	View / Enable / Global	Check the average CPU usage of MG205X.

On the other hand, to check the average CPU usage every 5 seconds, use the following commands.

Command	Mode	Function
show cpu-trueload	View / Enable / Global	Check the average CPU usage every 5 seconds for the recent 10 minutes.

6.3.7 CPU Process Check

In MG205X, user can check the CPU load, separated by each process. User can see the daemon which occupy the CPU mostly, the existence of unnecessary daemons, and the operation process of daemons which have problems, via this feature. Such information may also be an important clue to solve the problem when the problem occurs in the equipment.

To check the CPU process of MG205X, use the following commands.

Command	Mode	Function
show process	Enable / Global	Check the CPU process of MG205X.

6.3.8 Memory Information Check

To check the memory information of the MG205X, use the following command in Enable mode or Global mode settings.

Command	Mode	Function
show memory	Enable / Global/ Bridge	Check the memory usage information of the MG205X.
show memory { **dhcp** | **imi** | **lib**| **nsm** }		Check the memory usage information of a particular function.

6.3.9 System Image Check

The flash memory of the MG205X shows information of installed images. To see the information of the flash memory, use the following command.

Command	Mode	Function
show flash	View / Enable / Global	Show the system image installed in the equipment.

MG205X can support dual-OS, depending on the flash memory. If it is more than 32MB flash memory, MG205X supports dual-OS. Flash memory capacity can be checked by 'show system' command.

```
MG205X # show system

SysInfo(System Information)
    Model Name          : MG205X
    Main Memory Size     : 512 MB
    Flash Memory Size    : 64 MB
    H/W Revision        : R2A
    H/W Address         : 00:d0:cb:ff:dd:a1
    RTC Information      : M41T11
    Serial Number       : MEORRWG189A0000
    S/W Compatibility    : 2, 3
    NOS Version         : 1.00
    B/L Version         : 01.13.0010
    PLD Version         : 0x00
```

The following is to check installed NOS on equipment that supports dual-OS.

```
Flash Information(Bytes)

 Area                          total        used        free
 ------------------------------------------------------------------
 OS1                            29360128     17597459     11762669    1.00 #0001
 OS2(default)(running)          29360128     17717632     11642496    1.00 #0001
 CONFIG                          4194304       425984      3768320
 ------------------------------------------------------------------
 Total                        62914560     35741075     27173485
```

To delete the OS which is saved in flash memory, use the following command:

Command	Mode	Function
clear area {**os1** | **os2**}	Enable/Global	Delete the OS which is saved in flash memory.

6.3.10 System Image Version Check

In MG205X, user can check the version of the system image that is running currently. To see the system image version that is running currently, use the following command.

Command	Mode	Function
show version	View / Enable / Global	Show the version of the system image.

6.3.11 Check of System Image Filesize

In MG205X, user can check the size of the system image file. To check the file size of the system image, use the following command:

Command	Mode	Function
show os-size	Enable / Global	Show the size of the system image file.

6.3.12 Default OS Setting

MG205X can support dual-OS, depending on the flash memory in it. If the Flash Memory is 8MB + 16MB, single-OS is supported, and if flash memory is 8MB + 32MB, dual-OS is supported.

Flash memory information is checked by ‘show system’ command. In MG205X, user can select to set the default OS by when two systems of images are installed.

Reference

In MG205X, system image installed in OS1 is assigned to be the Default OS.

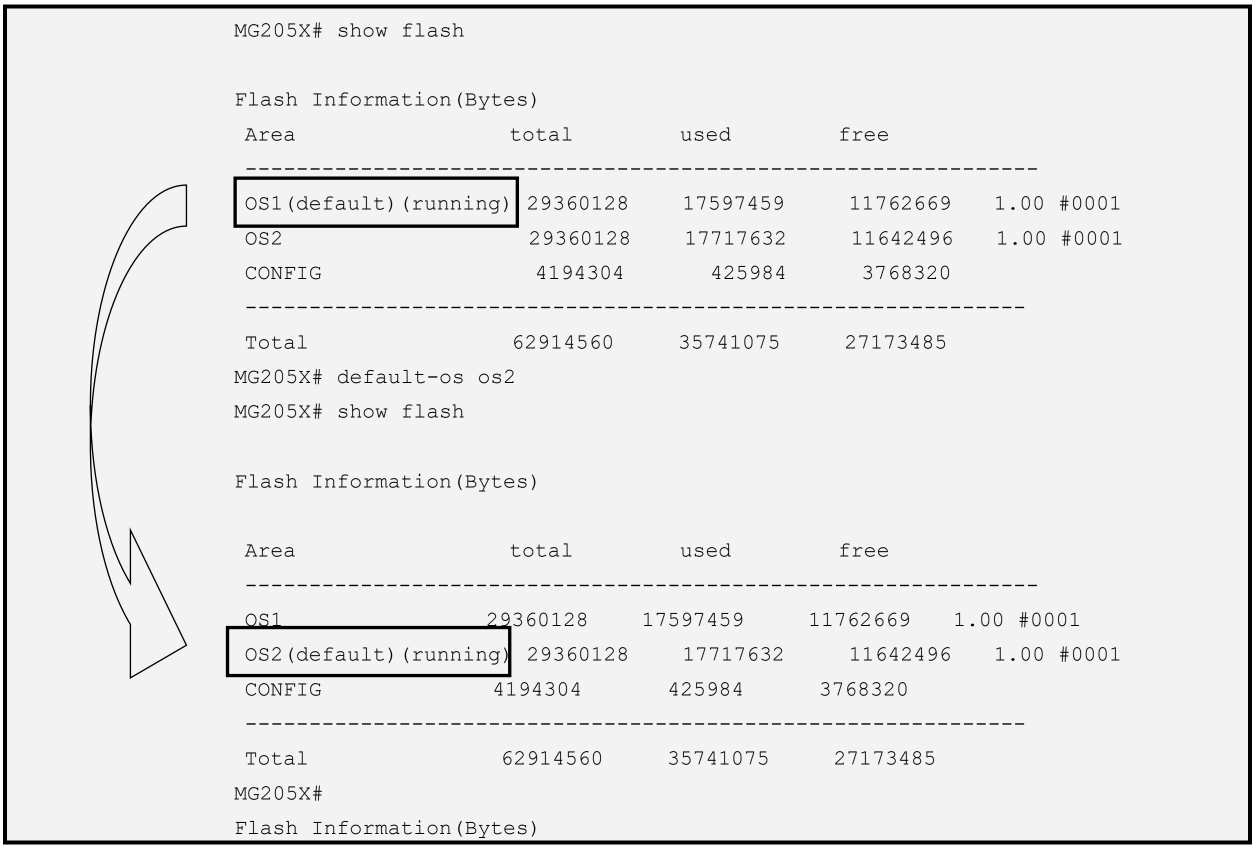
Use the following command in Enable mode for setting the Default OS.

Command	Mode	Function
default-os {**os1** | **os2**}	Enable	Set Default OS.

The following is a case for setting OS2 as Default OS.

```
MG205X # default-os os2
MG205X #
```

To check the default OS settings, user can see the system image installed in flash memory by ‘show flash’ command. The following case shows the changed settings of default OS from OS1 to OS2 in MG205X.



```
MG205X# show flash

Flash Information(Bytes)
 Area                 total        used        free
 --------------------------------------------------------------
 OS1(default)(running) 29360128    17597459     11762669   1.00 #0001
 OS2                   29360128    17717632     11642496   1.00 #0001
 CONFIG                 4194304      425984      3768320
 -------------------------------------------------------------
 Total                 62914560     35741075     27173485
MG205X# default-os os2
MG205X# show flash

Flash Information(Bytes)

 Area                 total        used        free
 --------------------------------------------------------------
 OS1                 29360128    17597459     11762669   1.00 #0001
 OS2(default)(running) 29360128    17717632     11642496   1.00 #0001
 CONFIG              4194304      425984      3768320
 -------------------------------------------------------------
 Total               62914560     35741075     27173485
MG205X#
Flash Information(Bytes)
```

6.3.13 System Temperature Check

In MG205X, to check the temperature information of the equipment, use the following command:

Command	Mode	Function
show status temp	Enable /Global / Bridge	Show the current temperature and the temperature threshold of MG205X.
show environment		Show the current temperature of MG205X.

6.3.14 Booting information Check

To check the information of booting/rebooting and power on/off of the system, use following command.

Command	Mode	Function
show boot-info	Enable/ Global/ Bridge	Check the recent information of system booting.

7. Network Management Function setting

It describes how to set the network management functions in MG205X network. This chapter contains the following topics:

- SNMP
- LLDP
- RMON Setting
- Syslog Setting
- DDM (Digital Diagnostic Monitoring)
- QoS (Quality of Service)
- NetBIOS Filtering
- MAC Filtering
- Martian Filter Statistics Check
- Limit of Accessible Users Number
- MAC Table management
- ARP
- ICMP Message Control
- TCP Flag Control
- Dump Packet
- Port Security
- PPS-Control
- LLCF (Link Layer Carrier Forward)
- Traffic Monitoring Setting Per Port

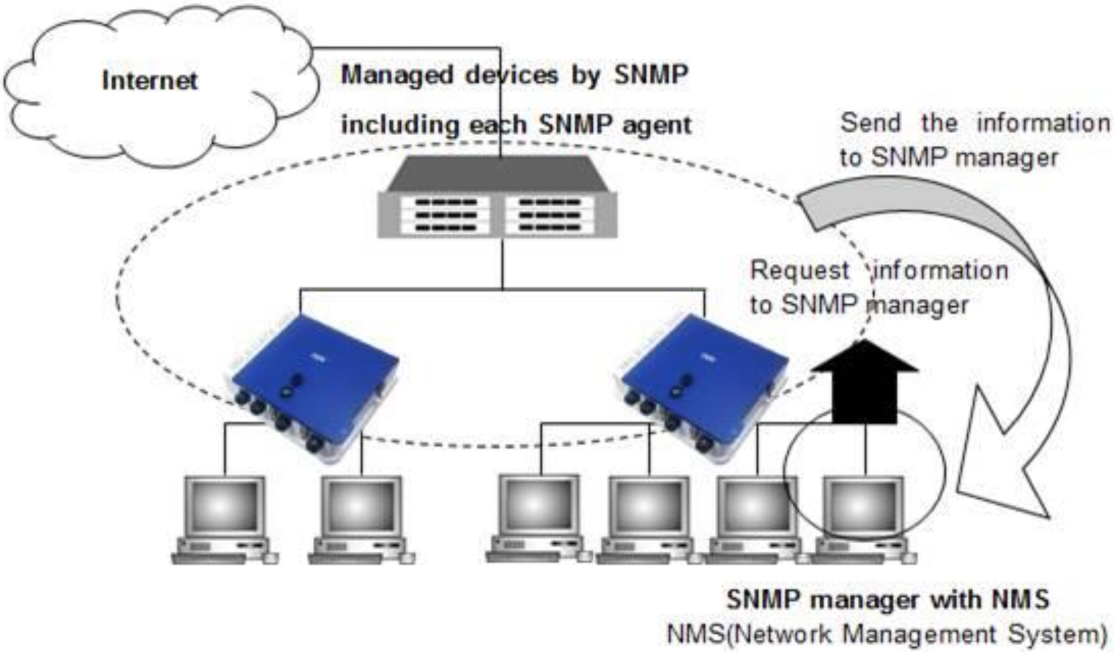
7.1 SNMP

SNMP (Simple Network Management Protocol) is consisted of SNMP manager, managed devices configured in the network, and SNMP agent that is installed in the managed devices. SNMP is a protocol that defines communicated information style between the SNMP manager and SNMP agent.

When you set up SNMP on the MG205X, the user can grant read-only authority or read and write authorities for specifying the relationship between the SNMP manager and the agent by the community.

The SNMP agent has MIB variables that can respond to the requests from SNMP manager, and the SNMP manager can obtain the data from the agent or store the data in the agent. Agent obtains the data from the MIB which stores information about the system and network.

Meanwhile, SNMP agent can send a trap to administrator when it occurs by incident. Trap is a warning message indicating the status of the network to the SNMP manager. Trap shows the incorrect user authentication information, rebooting information, connection status (active or inactive) information, TCP connection termination information, and communication problem with the MG205X in the network.



【Picture 7-1】An Example of SNMP Configuration

MG205X offers enhanced functionality to support SNMP v2c and v3 in addition to V1. These SNMP enhancements strengthen the network management with the SNMP agents, and user can limit the opened range of OID to the agent.

The following is a list of SNMP setting method in MG205X.

- SNMP v1 – Community setting
- SNMP v2c - com2sec setting
- SNMP v2c and v3 – Group setting
- SNMP v2c and v3 - OID Open Range Limitation (View Setting)
- SNMP v2c and v3 – Granting Access to Limited OID (Access Setting)
- SNMP v3 – User Setting
- SNMP v3 Notification Setting
- SNMP Trap Setting
- SNMP Agent – IP Address Setting
- SNMP Log Message
- SNMP Setting Check
- SNMP Function Releasing

Attention

SNMP has several versions by enhancements, such as v1, v2c and v3. Our MG205X has different support levels by the products, but MG205X supports all 3 versions.

7.1.1 SNMP v1 – Community setting

An SNMP agent of MG205X can have multiple ‘community’ relationships with a group of several SNMP managers. 1 SNMP and its each community can have unique ‘community name’, and the same community name should be set in SNMP manager and SNMP agent to share information with each other.

Here is the command to set the community name.

Command	Mode	Function
snmp community {**rw** ∣ **ro**} *community-name* [*ip-address*] [*oid*]	Global	Set the SNMP Community that grant access rights with written name.

Reference

MG205X can have read-only authorized community and read/write authorized community up to 3 in total.

Community name is generally implying the meaning of the password as we know it. The user can enter the password to a variable called "community-name". User can authorize the read-only or read/write permission by the password (or community). ‘ro’ and ‘rw’ followed by the snmp community command are the abbreviations of read-only and read/write that distinguishes a read-only access and read/write access.

On the other hand, to delete the community settings, use the following command:

Command	Mode	Function
no snmp community {**rw** | **ro**} *community-name*	Global	Remove the named community.

To check the community settings, use following command.

Command	Mode	Function
show snmp community	Enable/Global	Show the community settings.

7.1.2 SNMP Agent Manager – Contact Information, Installation

If the system administrator information and the device location which the agent is installed are specified, the information will be saved in the setting file of SNMP.

Here is the command to enter system administrator information and the equipment location of SNMP agent.

Command	Mode	Function
snmp contact *name*	Global	Enter the system administrator information of SNMP agent.
snmp location *name*		Enter the equipment location of SNMP agent.

On the other hand, to delete the system administrator information and equipment location of the SNMP agent, use the following command.

Command	Mode	Function
no snmp contact	Global	Delete the system administrator information of SNMP agent.
no snmp location		Delete the equipment location of SNMP agent.

To check the system administrator information and equipment location of the SNMP agent, use the following command.

Command	Mode	Function
show snmp contact	Enable / Global	Show the system administrator information of SNMP agent.
show snmp location		Show the equipment location of SNMP agent.

7.1.3 SNMP v2c - com2sec setting

In SNMP v2, access to agent is permitted by management of host origin and community name. The com2sec command defines the range of host to be accessed and community name as security name.

To register com2sec, use the following command.

Command	Mode	Function
snmp com2sec*security-name* {*ip-address* ∣ *ip-address/m*} *community*	Global	Register the Manager to be allowed for agent access and its community Name.

To delete the registered com2sec, use the following command.

Command	Mode	Function
no snmp com2sec *security-name*	Global	Delete the com2sec registration.

To check the registered com2sec, use the following command.

Command	Mode	Function
show snmp com2sec	Enable / Global	Show the registered com2sec.

7.1.4 SNMP v2c and v3 – Group setting

In MG205X, administrator can do group setting of SNMP manager to be accessed to agent and its community as following.

Command	Mode	Function
snmp group *group-name* {**v1** ǀ **v2c** ǀ **v3**} *security-name*	Global	Do SNMP group setting.

In {v1 v2c v3} section of above command, administrator can select the security model to be given to planned group setting. The 'security-name' of above command can be the same security name of com2sec setting. However, SNMP v3 model has security name as a part of SNMP basic protocol, so, it can be specified in this command directly without the same setting like com2sec of V2.

On the other hand, this group setting can be released by using following command.

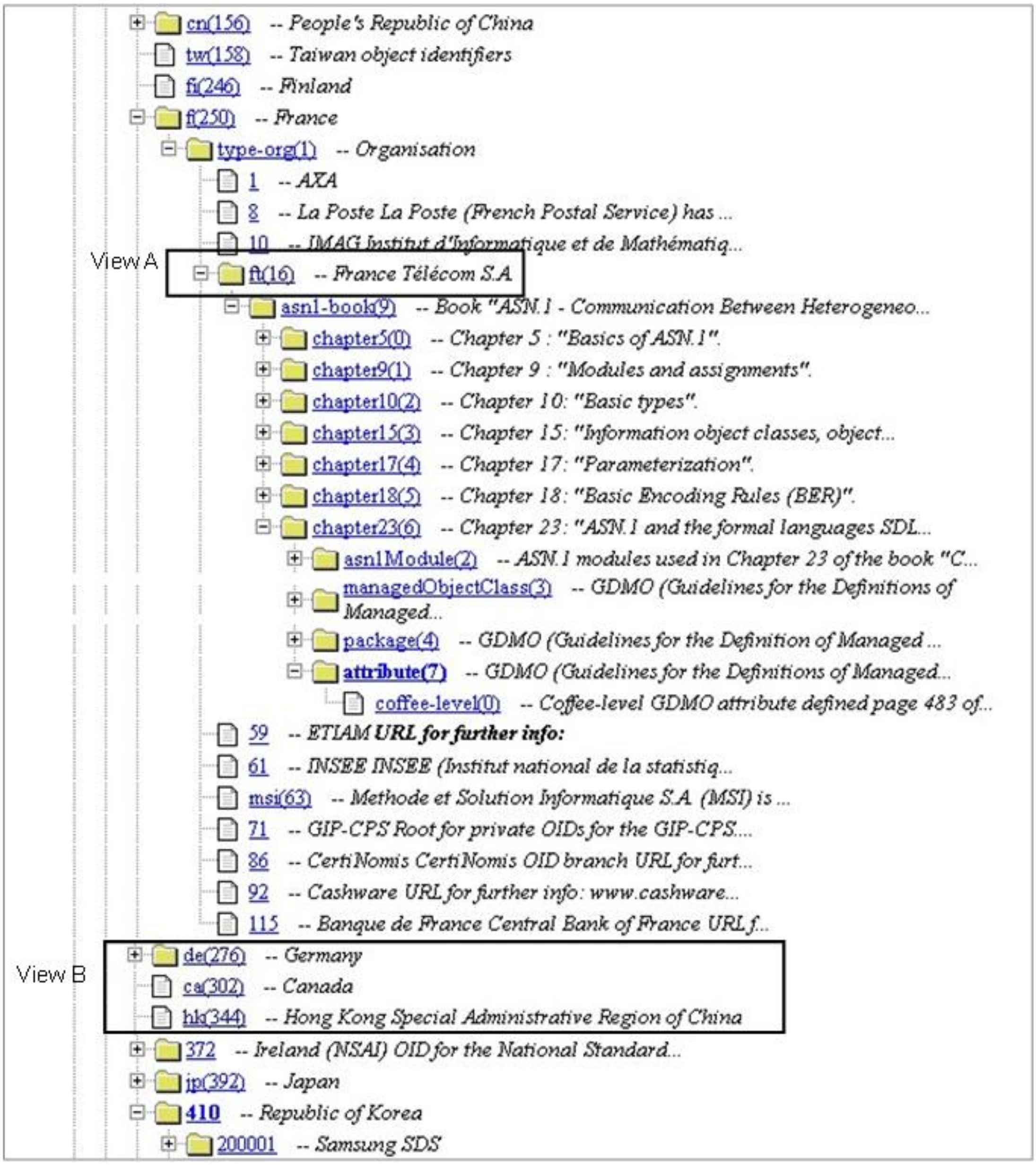
Command	Mode	Function
no snmp group *group-name* [[**v1** ǀ **v2c** ǀ **v3**] | [*security-name*]]	Global	Disable the named group setting.

To check the registered group, use the following command.

Command	Mode	Function
show snmp group	Enable / Global	Show the registered Group.

7.1.5 SNMP v2c and v3 - OID Open Range Limitation (View Setting)

In SNMP v2c and v3, administrator can set up separate groups with a range which has right to open the MIB. This is called "View".



```
cn(156) -- People's Republic of China
tw(158) -- Taiwan object identifiers
fi(246) -- Finland
fr(250) -- France
  type-org(1) -- Organisation
    1 -- AXA
    8 -- La Poste La Poste (French Postal Service) has ...
    10 -- IMAG Institut d'Informatique et de Mathématiq...
    ft(16) -- France Télécom S.A
      asn1-book(9) -- Book "ASN.1 - Communication Between Heterogeneo...
        chapter5(0) -- Chapter 5 : "Basics of ASN.1".
        chapter9(1) -- Chapter 9 : "Modules and assignments".
        chapter10(2) -- Chapter 10: "Basic types".
        chapter15(3) -- Chapter 15: "Information object classes, object...
        chapter17(4) -- Chapter 17: "Parameterization".
        chapter18(5) -- Chapter 18: "Basic Encoding Rules (BER)".
        chapter23(6) -- Chapter 23: "ASN.1 and the formal languages SDL...
          asn1Module(2) -- ASN.1 modules used in Chapter 23 of the book "C...
          managedObjectClass(3) -- GDMO (Guidelines for the Definitions of
          Managed...
          package(4) -- GDMO (Guidelines for the Definition of Managed ...
          attribute(7) -- GDMO (Guidelines for the Definitions of Managed...
            coffee-level(0) -- Coffee-level GDMO attribute defined page 483 of...
    59 -- ETIAM URL for further info:
    61 -- INSEE INSEE (Institut national de la statistiq...
    msi(63) -- Methode et Solution Informatique S.A. (MSI) is ...
    71 -- GIP-CPS Root for private OIDs for the GIP-CPS....
    86 -- CertiNomis CertiNomis OID branch URL for furt...
    92 -- Cashware URL for further info: www.cashware...
    115 -- Banque de France Central Bank of France URL f...
de(276) -- Germany
ca(302) -- Canada
hk(344) -- Hong Kong Special Administrative Region of China
372 -- Ireland (NSAI) OID for the National Standard...
jp(392) -- Japan
410 -- Republic of Korea
  200001 -- Samsung SDS
```

By using this command, administrator can set the View Name to set or limit MIB hierarchy ranges that can access each View.

To do view setting, use the following command:

Command	Mode	Function
snmp view *view-name* **included** *oid* [*mask*]	Global	Do view setting as 'view name' for OID including sub-trees.
snmp view *view-name* **excluded** *oid* [*mask*]		Do view setting as 'view name' for OID excluding sub-trees.

Reference

[Mask] is used to determine whether an OID is included in which view, and to control whether the components of an OID sub-tree is appropriate. When the full OID is included in the view, this can be omitted.

To delete the View Setting, use the following command:

Command	Mode	Function
no snmp view *view-name* [*oid*]	Global	Delete the View named "view-name".

To see the View Settings, use the following command:

Command	Mode	Function
show snmp view	Enable / Global	Show the registered view.

7.1.6 SNMP v2c and v3 – Granting Access to Restricted OID (Access Setting)

System administrator of MG205X can see the OID(View) which limits the opening range to specific group. To permit access to OID which has restricted opening to specific group, use the following command.

Command	Mode	Function
snmp access *group-name* {**v1** │ **v2c**} *read-name write-name notify-name*	Global	Set the View to be granted to the named group in SNMP v1 and SNMP v2c.
snmp access *group-name* **v3** {**noauth** │ **auth** │ **priv**} *read-name write-name notify-name*		Set the View to be granted to the named group in SNMP v3.

In above command, ‘read-name, write-name, notify-name’ is the view-name which was specified in the view settings. If this grant is without restriction to all, please enter "none". ‘v1’, ‘v2c’ or ‘v3’ can be selected as a security model given to the group from the group setting.

Reference

In above command, {**noauth** │ **auth** │ **priv**} are security level to be specified. ‘noauth’ is an authentication method using username, and ‘auth’ and ‘priv’ are the authentication methods based on MD5 or SHA algorithm. However, ‘priv-level’ is using DES encryption for higher security.

To disable the granting access to restricted OID, use the following command.

Command	Mode	Function
no snmp access *group-name*	Global	Disable the granting access to the named group which had restricted OID.

To check the granted group to access to restricted OID, use the following command:

Command	Mode	Function
show snmp access	Enable / Global	Show the granted group to access to restricted OID

7.1.7 SNMP v3 – User Setting

In SNMP v3, user should be registered with authentication key to make access to USM which is the security model of agent. To do user setting in SNMP v3, use following command.

Command	Mode	Function
snmp user *user-name* {**md5** ｜ **sha**} *auth-passphrase* [**des** *private-passphrase*]	Global	Set the User of SNMP v3.

Reference

Each passphrase should be at least 8 characters which is using the alphabet or numbers. Capital letters, small letters and special characters are differentiated.

To delete a registered user, use the following command:

Command	Mode	Function
no snmp user *user-name*	Global	Delete the user name.

To check the registered user, use the following command.

Command	Mode	Function
show snmp user	Enable / Global	Show the registered User.

7.1.8 SNMP Engine ID Setting

Engine ID is the unique ID to identify the SNMP agent in SNMPv3. To set the SNMP Engine ID, use the following command.

Command	Mode	Function
snmp engine-id {**hex** *hexstring* **| text** *string* }	Global	Set the SNMP Engine ID.
no snmp engine-id		Return the SNMP Engine ID as the default.

To check the SNMP Engine ID settings, use the following command.

Command	Mode	Function
show snmp engine-id	Enable/Global/Bridge	Show the information of the SNMP Engine ID

7.1.9 SNMP v3 Notification Setting

(1) SNMP Target Setting

To set the destination address for the SNMP notifications, use the following command.

Command	Mode	Function
snmp targetaddr {*A.B.C.D* | *X:X::X:X*} [*port-number timeout retries tag*]	Global	Set the destination address for the SNMP notifications.
no snmp targetaddr		Delete the destination address for the SNMP notifications.

Reference

In above command, 'targetaddr' is the name of the destination address. 'A.B.C.D' is the IPv4 address, and 'X: X :: X: X' is the IPv6 address. 'port-number' is UDP port number which can be set with the range of <1~65535>. The 'timeout' is the waiting time for approval before unauthorized PDU is returned, and the time is in seconds. The 'retries' is the number of return retries of the known PDU, and 'tag' is the name of the Tag list.

To set the SNMP security model and parameters, use the following command.

Command	Mode	Function
snmp targetparams *targetparm* { **v1**| **v2c**} *security*	Global	Set the SNMP parameters used to generate the destination message, and specify a security model.
snmp targetparams *targetparm* **v3** *security* { **noauth**| **auth** | **priv**}		Set the SNMP parameters, and specify the v3 security model and level for the user.
no snmp targetparams *targetparm*		Delete the notification of destination parameter.

Reference

In above command, ‘security’ is com2sec name. {**noauth** | **auth** | **priv**} are security level to be specified. ‘noauth’ is an authentication method using username, and ‘auth’ and ‘priv’ are the authentication methods based on MD5 or SHA algorithm. However, ‘priv-level’ is using DES encryption for higher security.

To check the destination address and the notification setting of parameters, use the following command.

Command	Mode	Function
show snmp targetaddr	Enable/ Global/ Bridge	Check the notification for the destination address.
show snmp targetparams		Check the notification for the destination parameter.

(2) SNMP Notification Type Setting

To specify the definition and type of SNMP notifications (Trap / Inform), use the following command.

Command	Mode	Function
snmp notify *NOTIFY TAG* [**trap** | **inform**]	Global	Set for the definition and type of SNMP notifications.
no snmp notify *NOTIFY*		Delete the definition and type of SNMP notifications.

To check the information for the notification type, use the following command.

Command	Mode	Function
show snmp notify	Enable/Global /Bridge	Check the information on the type of SNMP notifications.

7.1.10 SNMP Trap Setting

The SNMP trap is a warning message (alert message) which SNMP agent report to SNMP manager about the incident that occurred by accident. With this setting of SNMP trap function, MG205X transmit the information related with the network management program when specific event occurs.

SNMP traps of MG205X are largely divided into Event Mode and Alarm-report mode. In Event mode, the basic SNMP traps are set in the equipment for notification. In Alarm-report mode, not only basic SNMP traps operation, but also more detailed and separated SNMP traps with each level are passed to the trap host.

Reference

MG205X has SNMP trap setting in Alarm-report mode as default.

(1) SNMP Trap Host Setting

‘SNMP trap host’ receives trap message from SNMP agent. In MG205X, specified trap host will receive the SNMP traps. SNMP trap host can be set by using IP address of SNMP manager.

In MG205X, these settings can be done by trap host setting of SNMP v1, trap host setting of SNMP v2c and informing trap host setting of SNMP v3 respectively.

To set the SNMP Trap-host, use the following command.

Command	Mode	Function
snmp trap-host *ip-address* [*community*]	Global	Set the recipient of SNMP v1 trap messages.
snmp trap2-host *ip-address* [*community*]		Set the recipient of SNMP v2c trap messages.
snmp inform-trap-host *ip-address* [*community*]		Set the recipient of SNMP v3 informing trap messages.

At this time, ‘ip-address’ is the IP address of the destination that will receive the trap messages, for example, if SNMP Manager is going to be set as trap-host, IP address of the SNMP manager should be typed.

[Setting example 8]

The following is an example of setting to send trap message to the trap manager with an IP address of 10.1.1.3.

```
MG205X (config)# snmp trap-host 10.1.1.3
MG205X (config)#
```

Reference

MG205X of SNMP Tap-host can be set up to 16. If multiple trap-host is going to be set, IP addresses can be entered one by one or multiple at one time.

[Setting example 9]

The following explains two types of commands which the IP addresses (: 10.1.1.3, 20.1.1.5, 30.1.1.2) are set as multiple trap-hosts.

```
MG205X (config)# snmp trap-host 10.1.1.3
MG205X (config)# snmp trap-host 20.1.1.5
MG205X (config)# snmp trap-host 30.1.1.2
```

```
MG205X (config)#

MG205X (config)# snmp trap-host 10.1.1.3 20.1.1.5 30.1.1.2
MG205X (config)#
```

Here is an example of checking the trap-host setting above.

```
MG205X # show running-config
 (syncopation)
snmp trap-host 10.1.1.3 20.1.1.5 30.1.1.2
!
MG205X #
```

On the other hand, deletion of SNMP trap host setting can be done by following command:

Command	Mode	Function
no snmp trap-host *ip-address*	Global	Delete the SNMP trap host setting to send the SNMP v1 trap message to the appropriate IP address.
no snmp trap2-host *ip-address*		Delete the SNMP trap host setting to send the SNMP v2c trap message to the appropriate IP address.
no snmp inform-trap-host *ip-address*		Delete the SNMP trap host setting to send the SNMP v3 informing trap message to the appropriate IP address.

(2) SNMP Trap Mode Setting

In MG205X, SNMP traps have Event mode and Alarm-report mode. The default is set to the Event mode, but it can be changed to Alarm-report mode if needed.

To set the SNMP trap mode, use the following command:

Command	Mode	Function
snmp trap-mode {**event** ǀ **alarm-report**}	Global	Set the SNMP trap mode to either Event mode or Alarm-report mode.

(3) SNMP Trap Log and Threshold Setting

To record SNMP trap messages, use the following command.

Command	Mode	Function
snmp trap-log non-volatile	Global	Record SNMP trap messages.
no snmp trap-log non-volatile		Don't record SNMP trap messages.

To set the thresholds for SNMP track log, use the following command.

Command	Mode	Function
snmp trap-log threshold *VALUE*	Global	Set the SNMP trap log threshold.
no snmp trap-log threshold		Don’t set extra SNMP trap log threshold, and return to the default value(90%).

Reference

The threshold ‘VALUE’ is set as % in the range of 1-99%. The default value is set to 90%.

To delete all the logs of SNMP trap in non-volatile memory, use the following command.

Command	Mode	Function
clear snmp trap-log non-volatile	Global	Delete all the SNMP trap logs recorded in non-volatile memory.

To check the SNMP trap logs, use the following command.

Command	Mode	Function
show snmp trap-log	Enable Global Bridge	Show all the SNMP trap logs.
show snmp trap-log non-volatile [<1-200>]		Show the SNMP trap logs recorded in non-volatile memory.

Reference

<1-200> is the order of the SNMP trap log lines.

(4) SNMP Trap Setting in Event Mode

In MG205X, as described above, SNMP traps are divided largely into Event mode and Alarm-report mode. When it is set to Event mode as default, only trap messages set by trap manager will be transferred among the following main types of traps.

【Table 7-1】Basic SNMP Trap of MG205X

SNMP Trap	Functional description
active-link-down/ **active-link-up**	This message will be sent when the connection to the Active-link is failed, or when the network connection is made again with physical changes.
admin-access-login	This message will be sent when the user logged in or logged out.

atgd-storm-end/start	This message will be sent when Broadcast Storm is started or ended at the MG205X fabric.
auth-fail	This message will be sent when the user typed wrong community name.
cold-start	This message will be sent when the SNMP agent is turned off and rebooted again.
config-load-fail	This message will be sent when loading of configuration file is failed or the loaded file has errors.
cpu-threshold	This message will be sent when CPU usage is exceeded the threshold set in the "CPU usage threshold settings" of Syslog in this manual. Additionally, it will be sent when the CPU usage is dropped back below the threshold.
dhcp-lease	This message will be sent when there is no more IP address to be assigned in subnet of DHCP server. If there are multiple subnets, this trap message will be sent even when 1 subnet has no more IP address to be assigned in it.
dying-gasp	This message will be sent when electric power is not supplied or when connected sub-equipment has problems.
falling-alarm	This message will be sent when the lower threshold is crossing in alarms table.
input-error-threshold	This message will be sent when the Input error value is higher than threshold.
ip-conflict	This message will be sent when IP addresses have collision.
link-up/down	This message will be sent when the network connection to the specified port is failed, or when the network connection is made again.
mem-threshold	This message will be sent when the remained memory is smaller than the "available memory threshold setting" of Syslog in this manual. In addition, this message will be sent when the remained memory became more than the "available memory threshold setting".
mfgd-block	This message will be sent when a port is blocked by Mac flood guard setting.
module	This message will be sent when uplink module has problems.
new-mac	This message will be sent when snmp trap is activated to new mac address.
new-root	This message will be sent when new root is selected by the STP algorithm.
nos-load-fail	This message will be sent when system image operation is failed.
port-threshold	This message will be sent when the port traffic exceeded the threshold setting of "port traffic threshold settings" of Syslog in this manual. In addition, this message will be sent when the port traffic is fell down to the threshold again.
power	This message will be sent when the power supply has problems.
redundant-link-down/up	This message will be sent when the connection of redundant-link is failed or when the network connection is made again with physical changes.
rising alarm	This message will be sent when the upper threshold is crossing in alarms table.
script-load-fail	This message will be sent when execution of script file is failed.

system-restart	This message will be sent when the system is rebooted.
temp-threshold	This message will be sent when the equipment temperature exceeds the threshold set in the "temperature threshold setting" of Syslog in this manual.
topology-change	This message will be sent when the network topology is changed.
trap-log	This message will be sent when the trap logs are more than 90%.

Reference

In MG205X, all trap messages described above are set to be transferred by default. Default SNMP traps in MG205X is to send trap messages in each situation. However, among the all trap messages, unnecessary frequent messages can be inefficient. To make it efficient, administrator of MG205X can select the type of trap messages to be passed to the trap host.

Reference

SNMP of MG205X is set to transmit all kinds of trap messages by default.

To release the default behavior of the SNMP trap messages from the Event mode, use the following command.

Command	Mode	Function
no snmp trap active-link-down	Global	Stop the relevant trap message operation.
no snmp trap active-link-up		
no snmp trap auth-fail		
no snmp trap cold-start		
no snmp trap cpu-threshold		
no snmp trap dying-gasp		
no snmp trap link-down *port-number*		
no snmp trap link-up *port-number*		
no snmp trap mem-thrshold		
no snmp trap port-thrshold		
no snmp trap admin-access-login		
no snmp trap atgd-storm-end		
no snmp trap atgd-storm-start		
no snmp trap config-load-fail		
no snmp trap falling-alarm		
no snmp trap input-error-threshold		

Command	Mode	Function
no snmp trap ip-conflict		
no snmp trap login-failed		
no snmp trap mfgd-block		
no snmp trap new-root		
no snmp trap nos-load-fail		
no snmp trap redundant-link-down		
no snmp trap redundant-link-up		
no snmp trap rising-alarm		
no snmp trap script-load-fail		
no snmp trap self-test-completed		
no snmp trap system-restart		
no snmp trap topology-change		
no snmp trap trap-log		

To start or activate the default behavior of the SNMP trap messages again, use the following command:

Command	Mode	Function
snmp trap active-link-down	Global	Enable trap message - active-link-down.
snmp trap active-link-up		Enable trap message - active-link-up.
snmp trap auth-fail		Enable trap message - auth-fail.
snmp trap cold-start		Enable trap message - cold-start.
snmp trap cpu-threshold		Enable trap message - cpu-threshold.
snmp trap dying-gasp		Enable trap message - dying-gasp.
snmp trap link-down *port-number*		Enable trap message - link-down.
snmp trap link-up *port-number*		Enable trap message - link-up.
snmp trap mem-thrshold		Enable trap message - mem-thrshold.
snmp trap port-thrshold		Enable trap message - port-threshold.
snmp trap admin-access-login		Enable trap message - admin-access-login.
snmp trap atgd-storm-end		Enable trap message - atgd-storm-end.
snmp trap atgd-storm-start		Enable trap message - atgd-storm-start.
snmp trap config-load-fail		Enable trap message - config-load-fail.
snmp trap falling-alarm		Enable trap message - falling-alarm.

snmp trap input-error-threshold	Enable trap message - input-error-threshold.
snmp trap ip-conflict	Enable trap message - ip-conflict.
snmp trap login-failed	Enable trap message - login-failed.
snmp trap mfgd-block	Enable trap message - mfgd-block.
snmp trap new-root	Enable trap message - new-root.
snmp trap nos-load-fail	Enable trap message - nos-load-fail.
snmp trap redundant-link-down	Enable trap message - redundant-link-down.
snmp trap redundant-link-up	Enable trap message - redundant-link-up.
snmp trap rising-alarm	Enable trap message - rising-alarm.
snmp trap script-load-fail	Enable trap message - script-load-fail.
snmp trap self-test-completed	Enable trap message - self-test-completed.
snmp trap system-restart	Enable trap message - system-restart.
snmp trap topology-change	Enable trap message - topology-change.

(5) SNMP Trap Setting in Alarm Mode

In Alarm-report mode, more detailed SNMP traps will show the status of the equipment. Detailed SNMP traps sent from Alarm-report mode can have each severity level (priority level) setting. The severity level from the higher order is; critical> major> minor> warning> intermediate. If the administrator has not set the severity level, the basic default settings will be applied, and it is 'minor' level. The default setting can be changed by the user.

To set the default severity level separately to the detailed SNMP traps, use the following command.

Command	Mode	Function
snmp alarm-severity default {**critical**|**major**|**minor** |**warning**|**intermediate**}	Global	Set the selected level as default severity level of the trap.

Reference

The default severity level is set to 'minor' level.

Detailed SNMP traps used in Alarm-report mode can have optional transmission settings depending on its importance. At this time, 'criteria' is the importance level to judge whether the transmission is needed or not. If the severity level of a SNMP trap is the same or lower to the criteria level, this SNMP trap will not be transferred. To set the criteria of each SNMP trap, use the following command.

Command	Mode	Function
snmp alarm-severity criteria {critical|major|minor |warning|intermediate}	Global	Set the criteria as selected level for the judgment of SNMP trap transmission.

To set the severity level of each SNMP trap in alarm-report mode, use the following command.

Command	Mode	Function
snmp alarm-severity active-link-down {critical|major|minor |warning|intermediate}	Global	Set the severity level of active-link-down Alarm.
snmp alarm-severity active-link-up {critical|major|minor |warning|intermediate}		Set the severity level of active-link-up Alarm.
snmp alarm-severity admin-access-login {critical|major|minor |warning|intermediate}		Set the severity level of admin-access-login Alarm.
snmp alarm-severity atgd-storm-end {critical|major|minor |warning|intermediate}		Set the severity level of atgd-storm-end Alarm.
snmp alarm-severity atgd-storm-start {critical|major|minor |warning|intermediate}		Set the severity level of atgd-storm-start Alarm.
snmp alarm-severity auth-fail {critical|major|minor |warning|intermediate}		Set the severity level of auth-fail Alarm.
snmp alarm-severity cold-start {critical|major|minor |warning|intermediate}		Set the severity level of Cold-start Alarm.
snmp alarm-severity config-load-fail {critical|major|minor |warning|intermediate}		Set the severity level of config-load-fail Alarm.
snmp alarm-severity broadcast-over {critical|major|minor |warning|intermediate}		Set the severity level of Broadcast-over Alarm.
snmp alarm-severity cpu-load-over {critical|major|minor |warning|intermediate}		Set the severity level of Cpu-load-over Alarm.
snmp alarm-severity dhcp-lease {critical|major|minor |warning|intermediate}		Set the severity level of DHCP-Lease Alarm.
snmp alarm-severity dhcp-illegal {critical|major|minor |warning|intermediate}		Set the severity level of DHCP-illegal Alarm.
snmp alarm-severity dying-gasp {critical|major|minor |warning|intermediate}		Set the severity level of dying-gasp Alarm.
snmp alarm-severity ip-conflict {critical|major|minor |warning|intermediate}	Global	Set the severity level of Ip-conflict Alarm.

snmp alarm-severity memory-over {**critical**|**major**|**minor** |**warning**|**intermediate**}	Set the severity level of Memory-over Alarm.
snmp alarm-severity mfgd-block {**critical**|**major**|**minor** |**warning**|**intermediate**}	Set the severity level of Mfgd-block Alarm.
snmp alarm-severity port-link-down {**critical**|**major**|**minor** |**warning**|**intermediate**}	Set the severity level of Port-link-down Alarm.
snmp alarm-severity port-remove {**critical**|**major**|**minor** |**warning**|**intermediate**}	Set the severity level of Port-remove Alarm.
snmp alarm-severity port-thread-over {**critical**|**major**|**minor** |**warning**|**intermediate**}	Set the severity level of Port-thread-over Alarm.
snmp alarm-severity power-fail {**critical**|**major**|**minor** |**warning**|**intermediate**}	Set the severity level of Power-fail Alarm.
snmp alarm-severity power-remove {**critical**|**major**|**minor** |**warning**|**intermediate**}	Set the severity level of Power-remove Alarm.
snmp alarm-severity rmon-alarm-rising {**critical**|**major**|**minor** |**warning**|**intermediate**}	Set the severity level of Rmon-alarm-rising Alarm.
snmp alarm-severity rmon-alarm-falling {**critical**|**major**|**minor** |**warning**|**intermediate**}	Set the severity level of Rmon-alarm-falling Alarm.
snmp alarm-severity stp-bpdu-guard {**critical**|**major**|**minor** |**warning**|**intermediate**}	Set the severity level of STP BPDU Guard Alarm.
snmp alarm-severity stp-root-guard {**critical**|**major**|**minor** |**warning**|**intermediate**}	Set the severity level of STP Root Guard Alarm.
snmp alarm-severity system-restart {**critical**|**major**|**minor** |**warning**|**intermediate**}	Set the severity level of System-restart Alarm.
snmp alarm-severity module-remove {**critical**|**major**|**minor** |**warning**|**intermediate**}	Set the severity level of Module-remove Alarm.
snmp alarm-severity temperature-high {**critical**|**major**|**minor** |**warning**|**intermediate**}	Set the severity level of Temperature-high Alarm.
snmp alarm-severity input-error-threshold {**critical**|**major**|**minor** |**warning**|**intermediate**}	Set the severity level of input-error-threshold Alarm.
snmp alarm-severity login-failed {**critical**|**major**|**minor** |**warning**|**intermediate**}	Set the severity level of login-failed Alarm.
snmp alarm-severity new-root {**critical**|**major**|**minor** |**warning**|**intermediate**}	Set the severity level of new-root Alarm.

snmp alarm-severity nos-load-fail {critical|major|minor |warning|intermediate}		Set the severity level of nos-load-fail Alarm.
snmp alarm-severity port-link-up {critical|major|minor |warning|intermediate}		Set the severity level of port-link-up Alarm.
snmp alarm-severity self-test-completed {critical|major|minor |warning|intermediate}		Set the severity level of self-test-completed Alarm.
snmp alarm-severity trap-log {critical|major|minor |warning|intermediate}		Set the severity level of trap-log Alarm.
snmp alarm-severity topology-change {critical|major|minor |warning|intermediate}		Set the severity level of topology-change Alarm.

To cancel the severity level settings of each trap, use the following command.

Command	Mode	Function
no snmp alarm-severity cold-start	Global	Set the severity level of each trap to default(minor).
no snmp alarm-severity broadcast-over		
no snmp alarm-severity cpu-load-over		
no snmp alarm-severity dhcp-lease		
no snmp alarm-severity dhcp-illegal		
no snmp alarm-severity ipconflict		
no snmp alarm-severity memory-over		
no snmp alarm-severity mfgd-block		
no snmp alarm-severity port-link-down		
no snmp alarm-severity port-remove		
no snmp alarm-severity port-thread-over		
no snmp alarm-severity power-fail		
no snmp alarm-severity power-remove		
no snmp alarm-severity rmon-alarm-rising		
no snmp alarm-severity rmon-alarm-falling		
no snmp alarm-severity stp-bpdu-guard		
no snmp alarm-severity stp-root-guard		
no snmp alarm-severity system-restart		
no snmp alarm-severity module-remove		
no snmp alarm-severity temperature-high		

To set the severity level of ADVA Alarm, use the following command:

Command	Mode	Function
snmp alarm-severity adva-if-misconfig {critical|major|minor|warning|intermediate}		Set the severity level of adva-if-misconfig Alarm.
snmp alarm-severity adva-if-opt-thres { critical|major|minor |warning|intermediate}		Set the severity level of adva-if-opt-thres Alarm.
snmp alarm-severity adva-if-rcv-fail { critical|major|minor |warning|intermediate}		Set the severity level of adva-if-rcv-fail Alarm.
snmp alarm-severity adva-if-sfp-mismatch { critical|major|minor |warning|intermediate}		Set the severity level of adva-if-sfp-mismatch Alarm.
snmp alarm-severity adva-if-trans-fault { critical|major|minor |warning|intermediate}		Set the severity level of adva-if-trans-fault Alarm.
snmp alarm-severity adva-psu-fail { critical|major|minor |warning|intermediate}		Set the severity level of adva-psu-fail Alarm.
snmp alarm-severity adva-temperature { critical|major|minor |warning|intermediate}		Set the severity level of adva-temperature Alarm.
snmp alarm-severity adva-voltage-high { critical|major|minor |warning|intermediate}		Set the severity level of adva-voltage-high Alarm.
snmp alarm-severity adva-voltage-low { critical|major|minor |warning|intermediate}		Set the severity level of adva-voltage-low Alarm.

To release(cancel) the setting information using above command, use the following command:

Command	Mode	Function
no snmp alarm-severity adva-if-misconfig		
no snmp alarm-severity adva-if-opt-thres		
no snmp alarm-severity adva-if-rcv-fail		
no snmp alarm-severity adva-if-sfp-mismatch		
no snmp alarm-severity adva-if-trans-fault		
no snmp alarm-severity adva-psu-fail		
no snmp alarm-severity adva-temperature		
no snmp alarm-severity adva-voltage-high		
no snmp alarm-severity adva-voltage-low		

(6) ERP Alarm Priority Setting and Releasing

To set the severity level of Alarm on ERP, use the following command:

Command	Mode	Function
snmp alarm-severity erp-domain-lotp {critical|major|minor|warning|intermediate}	Global	If there is no response after sending test packets three times, set the severity level of transmitted trap in SNMP alarm mode on ERP.
snmp alarm-severity erp-domain-multi-rm {critical|major|minor|warning|intermediate}		Set the severity level in SNMP alarm mode on ERP when Multiple RM node is created.
snmp alarm-severity erp-domain-reach-fail {critical|major|minor|warning|intermediate}		Set the severity level in SNMP alarm mode on ERP when the ERP Link Failure is detected.
snmp alarm-severity erp-domain-ulotp {critical|major|minor|warning|intermediate}		Set the severity level in SNMP alarm mode on ERP when only specific port has response to the test packets.

To release(cancel) the severity level settings above, use the following command:

Command	Mode	Function
no snmp alarm-severity erp-domain-lotp	Global	Cancel the severity level setting on ERP.
no snmp alarm-severity erp-domain-multi-rm		
snmp alarm-severity erp-domain-reach-fail		
no snmp alarm-severity erp-domain-ulotp		

(7) Notify-Activity ‘Enable’

In MG205X, if the SNMP trap is in alarm-report mode, notification is to be made when the administrator does setting on specific function of the system. This notification feature is called ‘Notify-Activity’, and this notification is set for each function internally. To activate this ‘Notify-Activity’ to inform that the specific function setting is made on the device, use the following command.

Command	Mode	Function
snmp notify-activity enable	Global	Activate ‘Notify-Activity’ to inform that the specific function setting is made on the device.

Reference

Notify-Activity feature is disabled by default.

To disable(cancel) ‘Notify-Activity’ function again, use the following command.

Command	Mode	Function
snmp notify-activity disable	Global	Cancel the ‘Notify-Activity’ setting.

(8) SNMP Trap Setting Check

To check the basic settings of SNMP traps in Event mode, use the following command:

Command	Mode	Function
show snmp trap	Global	Check the basic settings of SNMP traps.

[Setting Example 10]

The following case is cancellation of auth-fail trap message and its check.

```
MG205X (config)# no snmp trap auth-fail
MG205X (config)# show snmp trap
Trap-Host List
            Host         Community
------------------------------------------
inform-trap-host 30.1.1.1
trap2-host       20.1.1.1
trap-host        10.1.1.1
Trap List
Trap-type      Status
--------------------------
auth-fail      disable
cold-start     enable
cpu-threshold   enable
port-threshold  enable
dhcp-lease     enable
power          enable
module         enable
fan            enable
temp-threshold  enable
mem-threshold   enable
MG205X (config)#
```

To check the importance of detailed SNMP traps setting of the user, use the following command.

Command	Mode	Function
show snmp alarm-severity	Enable/Global	Show the importance of detailed SNMP traps setting of the user.

[Setting Example 11]

The following example shows the settings for the alarm-severity level.

```
MG205X (config)# snmp notify-activity enable
MG205X (config)# snmp alarm-severity criteria critical
```

```
MG205X (config)# snmp alarm-severity cpu-load-over warning
MG205X (config)# show snmp alarm-severity
notify activity   : enable
default severity  : minor
severity criteria : critical
cpu-load-over       : warning
MG205X (config)#
```

On the other hand, to check SNMP alarm message which is sent to the system, use the following command.

Command	Mode	Function
show snmp alarm-report	Global	Show the report of SNMP alarm which was sent to the system.
show snmp alarm-history		Show the history record of SNMP alarm which was sent to the system.

To delete all the record of SNMP alarm which was sent to the system, use the following command.

Command	Mode	Function
snmp clear alarm-report	Global	Delete alarm-report sent to the system.
snmp clear alarm-history		Delete alarm-history record sent to the system.

Reference

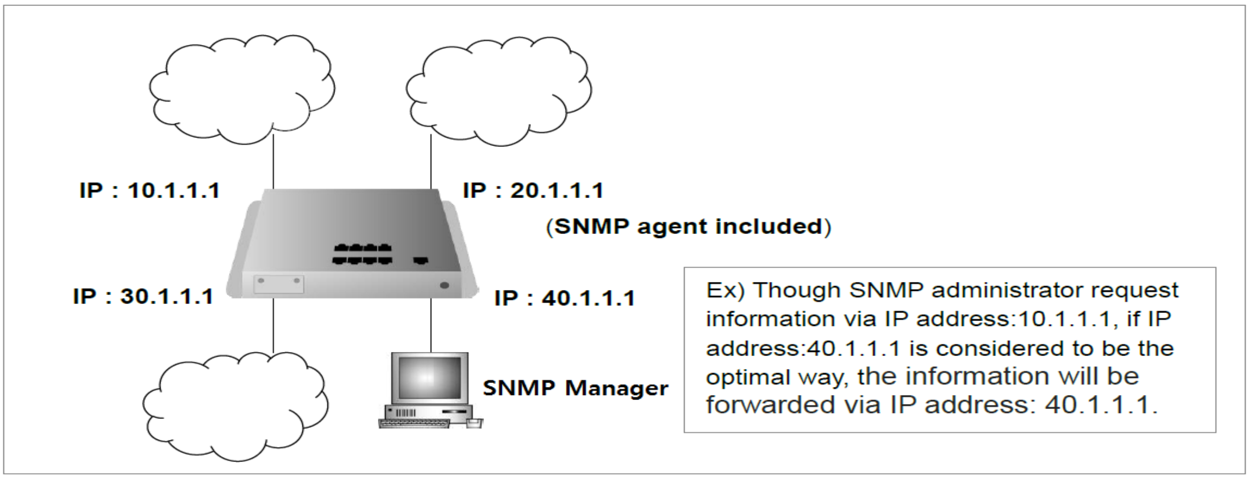
The ‘snmp clear alarm-report’ command is available only when the trap is in ‘alarm-report mode.

The following case is check of alarm record and deletion of it.

```
MG205X (config)# show snmp alarm-history
cold-start        minor       Fri Mar 25 15:30:56 2019 System booted.
MG205X (config)# snmp clear alarm-history
MG205X (config)# show snmp alarm-history
MG205X (config)#
```

7.1.11 SNMP Agent – IP Address Setting

If SNMP agent has multiple IP addresses, SNMP is to transmit the information through the optimal path when SNMP manager requests information. Therefore, transmitted information may have different IP address from the specified IP address of SNMP manager. Please refer to the following illustration.



Ex) Though SNMP administrator request information via IP address:10.1.1.1, if IP address:40.1.1.1 is considered to be the optimal way, the information will be forwarded via IP address: 40.1.1.1.

【Picture 7-2】IP Address of SNMP Agent

However, in MG205X, SNMP manager can specify the IP address of the SNMP agent to receive information again through the specified IP address when requests the information. To explain it in above illustration, if the SNMP manager specifies the IP address of agent as 10.1.1.1, the SNMP information should always be received through the IP address of 10.1.1.1.

To specify the IP address of the SNMP agent, use the following command:

Command	Mode	Function
snmp agent-address *ip-address*	Global	Specify the IP address of the SNMP agent.
no snmp agent-address *ip-address*		Delete the IP address of the SNMP agent.

Attention

If IP address is deleted from system which is the SNMP agent with the specified IP address, SNMP agent may not reply.

If it is tried to delete the IP from the SNMP agent with specified IP address, the warning will show that SNMP agent may not reply.

```
MG205X (config)# snmp agent-address 10.1.1.1
MG205X (config)#interface br1
MG205X (config-if)# no ip address 10.1.1.1/8
Warning : 172.16.209.100/16 is specified to the SNMP agent address.
SNMP agent may not reply.
MG205X (config-if)#
```

To check the IP address of the SNMP agent, use the following command:

Command	Mode	Function
show snmp agent-address	Enable/Global	Show the IP address of the SNMP agent.

7.1.12 SNMP Log Message

SNMP log messages are useful for troubleshooting network problems. To set the SNMP log messages to be saved in non-volatile memory, use the following command.

Command	Mode	Function
snmp log non-volatile	Global	Set the SNMP log messages to be saved in non-volatile memory.
no snmp log non-volatile		Disable the SNMP settings to save the log messages.

To delete all the SNMP log messages saved in non-volatile memory, use the following command.

Command	Mode	Function
clear snmp log non-volatile	Global	Delete all the SNMP log messages saved in non-volatile memory.

To check the contents of the SNMP log messages in non-volatile memory, use the following command.

Command	Mode	Function
show snmp log	Enable Global	Show the saved SNMP log messages.
show snmp log non-volatile [<1-2000>]		Show the saved SNMP log messages in non-volatile memory.
show snmp log non-volatile tail <1-2000>		Show the saved current SNMP log messages in non-volatile memory.

7.1.13 SNMP Setting Check

To check the information of SNMP settings by the user, use the following command:

Command	Mode	Function
show snmp	Enable/Global	Show the SNMP settings.

7.1.14 SNMP Function Releasing

To stop the SNMP function, use the following command in Global Setting Mode.

Command	Mode	Function
no snmp	Global	Disable and delete the SNMP function.

Attention

Using the above command, all settings related to the SNMP will be deleted.

7.1.15 Setting Example

[Setting Example 1]

This example sets the community name as ‘public’ which is granted to read / write and the other community name as ‘private’ which is grated to read only.

```
MG205X (config)# snmp community rw public
MG205X (config)# snmp community ro private
MG205X (config)# show snmp community

Community List
Type Community       Source           OID
-----------------------------------------------
rw   public
ro   private

MG205X (config)#
```

[Setting Example 2]

The following example is that the information of system administrator of SNMP agent is opentelecom<02.838.5033> and the equipment location of SNMP agent is Seoul, Korea.

```
MG205X (config)# snmp contact opentelecom
MG205X (config)# snmp location Seoul,Korea
MG205X (config)#
```

[Setting Example 3]

The following is an example of setting the com2sec.

```
MG205X (config)# snmp com2sec opentelecom 100.1.1.1 public
MG205X (config)# show snmp com2sec

Com2Sec List
SecName        Source           Community
------------------------------------------------
opentelecom          100.1.1.1        public
MG205X (config)#
```

[Setting Example 4]

The following is an example of setting group.

```
MG205X (config)# snmp group rogroup v1 opentelecom
MG205X (config)# show snmp group

Group List
GroupName       SecModel SecName
------------------------------------
rogroup        v1      opentelecom
MG205X (config)#
```

[Setting Example 5]

The following case is registering 1 view.

```
MG205X (config)# snmp view TEST included 1.3.6
MG205X (config)# show snmp view

View List
ViewName        Type    SubTree / Mask
-------------------------------------------
TEST           included 1.3.6

MG205X (config)#
```

[Setting Example 6]

The following example is granting access.

```
MG205X (config)# snmp access rogroup v1 none
MG205X (config)# show snmp access

Access List
GroupName       SecModel SecLevel ReadView        WriteView       NotifyView
--------------------------------------------------------------------------------
rogroup        v1      noauth   none


MG205X (config)#
```

[Setting Example 7]

The following example is user setting.

```
MG205X (config)# snmp user root md5 vertex25 des vertex25
MG205X (config)# show snmp user

User List
Name           AuthMode AuthPassphrase   PrivMode PrivPassphrase
---------------------------------------------------------------------
root           md5     vertex25       des     vertex25

MG205X (config)#
```

[Setting Example 8]

The following example is that trap setting to trap manager with IP address of 10.1.1.3, and that ‘auth-fail’ trap message is disabled.

```
MG205X (config)# snmp trap-host 10.1.1.3
MG205X (config)# no snmp trap auth-fail
MG205X (config)# show snmp trap

Trap-Host List
            Host        Community
------------------------------------------
trap-host       10.1.1.3
```

```
Trap List
Trap-type      Status
--------------------------
auth-fail      disable
cold-start     enable
cpu-threshold   enable
port-threshold  enable
dhcp-lease     enable
power          enable
module         enable
fan            enable
temp-threshold  enable
MG205X (config)#
```

[Setting Example 9]

The following example shows the settings of alarm-severity.

```
MG205X (config)# snmp notify-activity enable
MG205X (config)# snmp alarm-severity criteria critical
MG205X (config)# snmp alarm-severity cpu-load-over warning
MG205X (config)# show snmp alarm-severity
notify activity   : enable
default severity  : minor
severity criteria : critical
cpu-load-over     : warning
MG205X (config)#
```

The following case is that informed alarm-history is checked and deleted.

```
MG205X (config)# show snmp alarm-history
cold-start         minor      Fri Mar 25 15:30:56 2005 System booted.
MG205X (config)# snmp clear alarm-history
MG205X (config)# show snmp alarm-history
MG205X (config)#
```

7.2 Syslog Setting

Syslog (system logger) is messages which inform administrator of the information such as errors occurring in the use of MG205X by default.

In relation to the Syslog, following topics are described:

- Syslog Message Level Setting
- System Facility Setting
- Syslog Message Priority setting
- Syslog Setting Check
- Syslog Message IP Address Setting
- Remote Monitoring of Debug Message

- Executable Command Syslog Setting
- CPU Usage Threshold Setting
- CPU Statistics (Processing Packet Number) Threshold Setting
- Port Traffic Threshold Setting
- Temperature Threshold Setting
- Memory Capacity Threshold Setting

7.2.1 Syslog Message Level Setting

Syslog messages in MG205X are shown with its level and priority. Regardless of priority, all the Syslog messages can have its level by following command. At this time, administrator can set the destination location of the Syslog message.

To set the level and destination location of the Syslog messages, use the following command.

Command	Mode	Function
syslog output {**emerg**|**alert**|**crit**|**err**| **warning**|**notice**|**info**|**debug**} **console**	Global	Forward syslog messages of specified level to the console.
syslog output {**emerg**|**alert**|**crit**|**err**|**warning**| **notice**|**info**|**debug**} **local** {**volatile** | **non-volatile**}		Forward syslog messages of specified level to the selected local memory.
syslog output {**emerg**|**alert**|**crit**|**err**|**warning**| **notice**|**info**|**debug**} **remote** *ip-address*		Forward syslog messages of specified level to the host in the network with the IP address.

Syslog message has 8 levels by the importance and priority as emergency(0) | alert(1) | cirtical(2) | error(3) | warning(4) | notice(5) | info(6) | debug(7). The smaller numbered, the more important. Emergency has the highest importance, and debug has the lowest priority.

The user can set the level of syslog messages, and can't receive the lower level syslog messages than the setting level. If user selects debug level which is the lowest, all level syslog messages can be received. On the other hand, the user can set the destination location to receive syslog messages. To receive syslog messages from the console of users PC, user can set the location to 'console'. To receive it from the inside memory of the system, user can set the location to 'local'. To receive it from the host in the network, user can set the location to 'remote ip-address'.

To disable the syslog message settings of level and destination location, use the following command.

Command	Mode	Function
no syslog output {**emerg**|**alert**|**crit**|**err**|**warning**| **notice**|**info** |**debug**} **console**	Global	Disable the syslog message settings of level and destination location.

no syslog output {**emerg**|**alert**|**crit**|**err**|**warning**| **notice**|**info** |**debug**} **local** {**volatile** | **non-volatile**}		
no syslog output {**emerg**|**alert**|**crit**|**err**|**warning**| **notice**|**info** |**debug**} **remote** *ip-address*		

7.2.2 System Facility Setting

Providing facility of syslog message with local-code can be done in MG205X by the following command. Depend on facility local-code which is set by the user, syslog message management can be done by each system or by each system group.

Command	Mode	Function
syslog local-code <0-7>	Global	Set the local-code to the system facility.
no syslog local-code		Disable the local-code setting of the system Facility.
show syslog		Show the system facility setting.

Here is an example of System Facility setting as 3.

```
MG205X (config)# syslog local-code 3
MG205X (config)# show syslog
System logger on running!
info                local volatile
info                local non-volatile
local_code           3
MG205X (config)#
```

7.2.3 Syslog Message Priority setting

In MG205X, user can select the Priority of Syslog Message. User can send only the syslog messages with selected priority by using following command. At this time, level and destination location of the syslog message can be set at the same time.

Command	Mode	Function
syslog output priority {**auth** | **authpriv** | **kern** | **syslog** | **user**} {**emerg** | **alert** | **crit** | **err** | **warning** | **notice** | **info**} **console**	Global	Forward syslog messages of specified priority and level to the console.
syslog output priority {**auth** | **authpriv** | **kern** | **syslog** | **user**} {**emerg** | **alert** | **crit** | **err** | **warning** | **notice** | **info**} **local** {**volatile** | **non-volatile**}		Forward syslog messages of specified priority and level to the selected local memory.

syslog output priority {{**auth** ǀ **authpriv** | **kern** ǀ **syslog** ǀ **user**} {**emerg** ǀ **alert** ǀ **crit** ǀ **err** ǀ **warning** ǀ **notice** ǀ **info**} **remote** *ip-address*	Forward syslog messages of specified priority and level to the host in the network with the IP address.

In MG205X, there are 5 selectible priority levels as auth, authpriv, kern, syslog and user.

On the other hand, MG205X has a priority local code from 0 to 7 which can be defined by the user. This priority can be used for the syslog server with messages from multiple devices when user separates syslog messages from each equipment.

Setting the user-defined priority and forwarding the syslog messages can be done by the following command.

Command	Mode	Function
syslog output priority {**local0** ǀ **local1** ǀ **local2** ǀ **local3** ǀ **local4** ǀ **local5** ǀ **local6** ǀ **local7** | **syslog** | **user**} {**emerg** ǀ **alert** ǀ **crit** ǀ **err** ǀ **warning** ǀ **notice** ǀ **info** } **console**	Global	Set the user-defined priority and forward the syslog messages to the selected destination. ● Console : console of PC ● Local : Local memory of the system ● Remote IP address : Host in the network
syslog output priority {**local0** ǀ **local1** ǀ **local2** ǀ **local3** ǀ **local4** ǀ **local5** ǀ **local6** ǀ **local7** | **syslog** | **user**} {**emerg** ǀ **alert** ǀ **crit** ǀ **err** ǀ **warning** ǀ **notice** ǀ **info** } **local** {**volatile** ǀ **non-volatile**}		
syslog output priority {**local0** ǀ **local1** ǀ **local2** ǀ **local3** ǀ **local4** ǀ **local5** ǀ **local6** ǀ **local7** | **syslog** | **user**} {**emerg** ǀ **alert** ǀ **crit** ǀ **err** ǀ **warning** ǀ **notice** ǀ **info** } **remote** *ip-address*		

To disable the syslog message priority setting, use the following command.

Command	Mode	Function
no syslog output priority {**auth** | **authpriv** | **kern** | **local** <0-7> | **syslog** | **user**} {**emerg** ǀ **alert** ǀ **crit** ǀ **err** ǀ **warning** ǀ **notice** ǀ **info**} **console**	Global	Disable the syslog message priority setting and its destination location setting.
no syslog output priority {**auth** | **authpriv** | **kern** | **local** <0-7> | **syslog** | **user**} {**emerg** ǀ **alert** ǀ **crit** ǀ **err** ǀ **warning** ǀ **notice** ǀ **info**} **local** {**volatile** ǀ **non-volatile**}		

no syslog output priority
{**auth** | **authpriv** | **kern** | **local** <0-7> | **syslog** | **user**}
{**emerg** | **alert** | **crit** | **err** | **warning** | **notice** | **info**}
remote *ip-address*		

[Setting Example 1]

The following setting is to forward a syslog message named ‘local1.info’ to console.

```
MG205X (config)# syslog output notice remote 10.1.1.1
MG205X (config)# syslog output priority local1 info console
MG205X (config)# show syslog
System logger on running!

info              local volatile
info              local non-volatile
notice            remote 10.1.1.1
local1.info       console
MG205X (config)#
```

[Setting Example 2]

The following setting is to change the priority of all remote syslog messages to local0.

```
MG205X (config)# syslog output err remote 10.1.1.1
MG205X (config)# syslog local-code 0
MG205X (config)# show syslog
System logger on running!

info              local volatile
info              local non-volatile
err               remote 10.1.1.1
local_code         0
MG205X (config)#
```

7.2.4 Syslog Setting Check

To check the setting details of syslog or syslog messages, use the following command.

Command	Mode	Function
show syslog	Enable/ Global	Show the current setting of syslog.
show syslog local {**volatile** | **non-volatile**}		Show the syslog message.
show syslog local {**volatile** | **non-volatile**} *number*		Show the latest messages to the corresponding number entered by the user. For example, if the entered number is "2", it will show the latest two-line messages.

show syslog local {**volatile** ︱ **non-volatile**} **reverse**	Show the messages from the latest one.
show syslog {**volatile** ︱ **non-volatile**} **information**	Show the status information of syslog.

Attention

Syslog settings cannot be checked by "show running-config" command.

Following setting is saving syslog messages over info level to the volatile file and saving syslog messages in or over emergency level to the console.

```
MG205X (config)# show syslog
System logger on running!

info              local volatile
emerg             console
MG205X (config)#
```

To delete log messages saved in syslog file, use the following command:

Command	Mode	Function
clear syslog local {**volatile** ︱ **non-volatile**}	Enable/Global/Bridge	Delete the log messages saved in the Syslog file.

On the other hand, to check the syslog status information, use the following command.

Command	Mode	Function
show syslog status	Enable/Global/Bridge	Check the syslog status information.

7.2.5 Syslog Message IP Address Setting

In MG205X, user can specify the IP address of the syslog messages to be sent to a remote location.

To specify the IP address of the syslog message, use the following command.

Command	Mode	Function
syslog bind-address *ip-address*	Global	Specify the IP address of the syslog messages to be sent to remote location.
no syslog bind-address		Release the IP address of the syslog messages to be sent to remote location.

Following example is setting the IP address 192.168.253.0 to syslog messages.

```
MG205X (config)# syslog bind-address 192.168.253.0
MG205X (config)# show syslog
System logger on running!
info              local volatile
info              local non-volatile
kern.=err          console
alert             console
==========================================
agent address       192.168.253.0
MG205X (config)#
```

7.2.6 Remote Monitoring of Debug Message

Remotely interfaced users can check the syslog messages through server when they send syslog messages to remote server. But, it is possible to do setting which remote user check syslog messages on the console window directly. However, it is not for all syslog messages, but only for the syslog messages with lower priority than certain level. Each level of available syslog messages can be different by the equipments, and this level of syslog message can be checked by 'show syslog' command.

```
MG205X # terminal monitor
MG205X # show syslog
System logger on running!

info              local volatile
info              local non-volatile
info              console
info              /dev/pts/0
MG205X #
```

Message level to be checked by remote terminal monitor is '**info'**

To check the syslog message from the console window of remote visitor, use the following command.

Command	Mode	Function
terminal monitor	Enable	Check the syslog message from the console window of remote visitor.

The following case is setting which remote visitor checks the debug messages from their console windows.

```
MG205X # terminal monitor
MG205X # show syslog
System logger on running!

info              local volatile
info              local non-volatile
user.debug         /dev/ttyP1
MG205X #
```

To disable the remote monitoring of debug messages from console window, use the following command.

Command	Mode	Function

no terminal monitor	Enable	Disable the remote monitoring of debug messages from remote console window

7.2.7 Executable Command Syslog Setting

Executable Commands issued to run on the device can be informed or recorded by syslog message. 'Show' command which is used to check the equipment status is not recorded in command syslog. User can leave the commands entered to the equipment as syslog messages by following command.

Command	Mode	Function
command-history-log enable [**default**]	Global	Record the commands entered to the equipment as syslog messages. Default setting is 'enable'.
command-history-log disable [**default**]		Disable the command syslog settings. Default setting is 'disable'.

Reference

'Show' command which is used to check the equipment status is not recorded in command syslog.

To check the command syslog message settings, use following command.

Command	Mode	Function
show command-history-logging status	Enable/ Global	Show the command syslog message settings.

7.2.8 CPU Usage Threshold Setting

In MG205X, If user set the threshold of CPU usage, CPU usage information will be informed by syslog messages when it is over the threshold or returned back to under the threshold. To set a CPU usage threshold in MG205X, use the following command in Global setting mode.

Command	Mode	Function
threshold cpu <21-100> {**5** ∣ **60** ∣ **600**}	Global	Set the upper limit threshold of CPU usage.
threshold cpu <21-100> {**5** ∣ **60** ∣ **600**} <20-100> {**5** ∣ **60** ∣ **600**}		Set the upper and lower limit thresholds of CPU usage.

Reference

The unit of the threshold value is "%". The upper limit can be set from 21% to 100%, and the lower limit can be set from 20% to 100%.

Reference

MG205X has default CPU usage thresholds as upper limit of 70% and lower limit of 30%.

Reference

Timer interval can be set to 5 seconds, 60 seconds, and 600 seconds. By default, it is set to 60 seconds.

If the user wants to revert to the default CPU usage threshold settings, use the following command.

Command	Mode	Function
no threshold cpu	Global	Return to the default settings of CPU usage threshold.

To check the CPU usage threshold settings by the user, use the following command:

Command	Mode	Function
show cpuload	Enable/ Global	Show the CPU usage threshold values and average CPU usage of user equipment.

Following example is a setting which the upper limit value of the CPU usage threshold is 80%.

```
MG205X (config)# threshold cpu 80 60 40 600
MG205X (config)# show cpuload
----------------
Average CPU load
----------------
 5 sec:   3.04( 0.42) %
 1 min:   3.04( 0.41) %
10 min:   4.44( 0.41) %

cpuload threshold (high) :   80
timer   interval (high) :   60
cpuload threshold (low)  :   40
timer   interval (low)  :   600
MG205X (config)#
```

7.2.9 CPU Statistics (Processing Packet Number) Threshold Setting

In MG205X, if user set processed packet number of CPU, syslog message will be sent when the packet number of the CPU exceeds the set value. This feature allows system administrators to manage the MG205X and network status more effectively.

This can be set by following command.

Command	Mode	Function
cpu statistics-limit {**unicast** | **multicast** | **broadcast**} *port-number* <10-100>	Global	Set the number of packets to be processed by the CPU. If CPU packets exceed the specified value, syslog messages will be sent.

Reference

Unit number of packets in setting is 1000. Therefore, if the set value is 10, actual packet number is 10,000 in setting.

To disable the CPU statistics (processing packet number) setting, use the following command.

Command	Mode	Function
no cpu statistics-limit {**unicast** | **multicast** | **broadcast** ｜ **all**} {*port-number* ｜ **all**}	Global	Disable the CPU statistics(processing packet number) setting to send syslog messages when the CPU packets exceed a specified value.

To check the CPU statistics (processing packet number) setting to send syslog messages when the CPU packets exceeds a specified value, use the following command.

Command	Mode	Function
show cpu statistics-limit	Enable/ Global/ Bridge	Show the CPU statistics(processing packet number) setting to send syslog messages when the CPU packets exceed a specified value.

7.2.10 Port Traffic Threshold Setting

In MG205X, if the user specifies the threshold for the traffic amount of each port, syslog message will be sent when the traffic amount is over the threshold or returned back to under the threshold. To set the traffic thresholds for each port of MG205X, use the following command in Global Setting Mode.

Command	Mode	Function
threshold port *port-number range* {**5** ｜ **60** ｜ **600**} { **rx** ｜ **tx** }	Global	Set the traffic threshold of the port. The unit of the threshold is "kbps".
threshold port *port-number* **block timer** <10-3600>		Set block time to block the port for the time when the traffic amount exceeds threshold value of the setting.

Reference

Traffic threshold of the port is set to the maximum speed of the port. The default setting is 1000000kbps for the Giga port, and 100000kbps for 100M port.

Reference

Time interval can be set to 5 seconds, 60 seconds, and 600 seconds.

If the user wants to revert to the default port traffic threshold settings, use the following command.

Command	Mode	Function
no threshold port *port-number* { **rx** ∣ **tx** }	Global	Disable the port traffic thresholds.
no threshold port *port-number* **block**		Disable the block time setting of port traffic.

To check the port traffic threshold setting, use the following command.

Command	Mode	Function
show port threshold	Enable/Global/Bridge	Show the port traffic threshold settings of the user.

The following is a port traffic threshold setting with threshold of 500Mbps to port 1.

```
MG205X (config)# threshold port 1 500 5 rx
MG205X (config)# show port threshold
-----------------------------------------------------------------
 port |  current(Kbps) | threshold(Kbps) | interval(sec) | mode
-----------------------------------------------------------------
   1            0            500              5        rx
```

7.2.11 Temperature Threshold Setting

In MG205X, if user set the temperature threshold value of the equipment, syslog messages will be sent when the temperature is over the threshold or returned back to under the threshold.

To set the temperature threshold value of the equipment, use the following command in Global Setting Mode.

Command	Mode	Function
threshold temp <-40-100> <-40-100>	Global	Set the temperature threshold value of the equipment.

Reference

By default, the temperature thresholds of the MG205X is 80℃ as upper limit and -20℃ as lower limit.

If the user wants to revert to the default equipment temperature threshold settings, use the following command.

Command	Mode	Function
no threshold temp	Global	Return to the default equipment temperature threshold settings

To check the temperature of the equipment and equipment temperature threshold, use the following command.

Command	Mode	Function
show status temp	Enable/Global	Show the temperature of the equipment and equipment temperature threshold.

Following is an equipment temperature settings of 65℃ as high-temperature threshold and -10℃ as lower thresholds.

```
MG205X (config)# threshold temp 65 -10
MG205X (config)# show status temp

Temperature 1 current :  36 C
Temperature Threshold : High (80 C) Low (-20 C)

MG205X (config)#
```

7.2.12 Memory Capacity Threshold Setting

In MG205X, if user set the unused memory threshold value, syslog messages will be sent when unused memory capacity is less than the threshold value or returned back to more than threshold.

Unused memory capacity threshold can be set by following command.

Command	Mode	Function
threshold memory <20-100>	Global	Set the unused memory capacity threshold value.

To return the unused memory capacity threshold setting back to default value, use the following command.

Command	Mode	Function
no threshold memory	Global	Return the unused memory capacity threshold setting back to default value.

7.3 DDM (Digital Diagnostic Monitoring)

SFP uplink module port of MG205X is DDMI (Digital Diagnostic Monitoring Interface) which supports DDM (Digital Diagnostic Monitoring) function. DDM function is monitoring of the information about the temperature or electric power of the system.

MG205X is using DDM function. It monitors SFP uplink module, and gives alarm signal when the temperature level or electric power level is over or under the threshold settings. With this monitoring and alarm function, administrator can respond quickly to an environment that the SFP uplink module does not operate normally.

7.3.1 DDM Setting

When user wants to see collected information through DDM function together with SFP module information, DDM function should be activated. In addition, SFP-related threshold settings will inform the information of module temperature or electric power consumption when they are over the threshold value while the DDM function is activated.

To activate the DDM function, use the following command.

Command	Mode	Function
module ddm enable	Global	Activate the DDM function to monitor the module related information.

Reference

In MG205X, DDM function is activated by default.

To release the DDM function, use the following command.

Command	Mode	Function
module ddm disable	Global	Deactivate the DDM functionality.

Reference

Activated DDM can affect the CPU Load by its data collection. In this case, user can deactivate the DDM function.

Attention

If user use the ‘show port module-info’ command to show the information about the module, DDM information of the port will not be shown while the DDM function is not activated.

To check the settings of the DDM function, use the following command.

Command	Mode	Function
show module ddm	Enable/Global/Bridge	Show the settings of the DDM function.

The following is the case after deactivation of DDM on MG205X.

```
MG205X (config)# module ddm disable
MG205X (config)# show module ddm
----------------------------------------
    Module Diagnostics Monitoring
----------------------------------------
module diagnostics monitor(ddm) : disable
```

7.3.2 SFP Module-related Threshold Setting

As described above, SFP module port of MG205X is DDMI, and module related information can be monitored though

DDM function. If user set the threshold temperature and the power consumption of the SFP module while DDM function is activated, alarm will be sent when the monitored information is higher or lower than the threshold value.
At this time, if the threshold value is saved in SFP module and operation is by the internal settings, it is called 'SFP mode'. But, if the operation is by the settings of system inside without SFP internal setting, it is called 'system mode'. By default, it is set to operate as a system mode. If both the system mode and SFP mode are set to work, system mode will work with higher priority, and SFP mode will work when system mode is disabled.

Reference

By default, the system mode will operate with higher priority than SFP mode.

Syslog level of SFP modules thresholds operates as 'info'. In addition, regardless of the Link interface status, if the DDM function is activated, syslog for the threshold will be generated.
Though the link interface is down, if the DDM function is activated, syslog to the threshold will be generated.

To set the threshold regarding voltage, current, temperature, and bias of the SFP module, use the following command.

Command	Mode	Function
threshold module {**rxpower** | **txpower**} {**alarm** | **warning**} *port-number low-threshold high-threshold* [**system** | **sfp**]	Global	Set the threshold regarding power of the SFP port to monitor the SFP module.
threshold module temper {**alarm** | **warning**} *port-number low-threshold high-threshold* [**system** | **sfp**]		Set the threshold regarding temperature of the SFP port to monitor the SFP module.
threshold module txbias {**alarm** | **warning**} *port-number low-threshold high-threshold* [**system** | **sfp**]		Set the threshold regarding TX bias of the SFP port to monitor the SFP module.
threshold module voltage {**alarm** | **warning**} *port-number low-threshold high-threshold* [**system** | **sfp**]		Set the threshold regarding power voltage of the SFP port to monitor the SFP module.

The following is a warning case which the module temperature becomes lower than the threshold of the setting in SFP mode.

```
MG205X (config)# threshold module temper warning 1 53 85 sfp
MG205X (config)# Mar  1 12:37:54  fiber_dmid: port 1 temper(52.0000 C) is
under WarningLow(53.0000 C)
```

To delete the threshold values regarding voltage, power, temperature, bias of the SFP module, use the following command.

Command	Mode	Function

no threshold module {**rxpower** ∣ **txpower**| **txbias**| **voltage** | **temper**} {**alarm** ∣ **warning**} *port-number*	Global	Delete the threshold values regarding voltage, power, temperature, bias of the SFP module.

To check the threshold values for the SFP module status, check the system inside setting if it is in system mode. If it is in SFP mode, please check the SFP module status.

To check the threshold values in the system mode, use the following command.

Command	Mode	Function
show running-config	All	Check the threshold values in the system mode.

Only the corrected threshold values in system mode can be shown. Following check is after correction of only temper alarm, txpower alarm and rxpower warning of port 1.

```
MG205X (config)# show running-config
(syncopation)…
syslog output info console
!
(syncopation)
interface lo
 no shutdown
!
threshold module temper alarm 1 -120.0000 120.0000 system
threshold module txpower alarm 1 -20.0000 1.0000 system
threshold module rxpower warning 1 -10.0000 7.0000 system
(Syncopation)
```

To check the threshold values in the SFP mode, use the following command:

Command	Mode	Function
show port module-info [*port-number*]	Enable/Global/Bridge	Check the threshold values in the SFP mode.

Attention

If DDM function is not activated, the threshold information will not be shown.

Following case is checking of threshold values in the SFP mode while the DDM function is activated.

```
MG205X (config)# show port module-info 1
Port    1
           Transceiver type:  SFP
               Transceiver:  1000Base-LX
                   Length:  10 Km [ Single Mode ]
                    Speed:  1250 Mb/s
```

```
                       Wavelength:  1310 nm
                   Connector Type:  LC
                      Vendor name:  CORETEK
                 Vendor part name:  CT-1250TSP-MB4LD
                  Vendor revision:  0000
             Vendor serial number:  CF0032H1400079
                     Product date:  2008-03-11

DDM SFP Temperature: 40.6562 C  (Warn: -5.0000 / 90.0000)(Alarm:-10.0000 /  100.0000)
DDM SFP Vcc: 3.3120 V      (Warn:   3.1000 /    3.5000)(Alarm:   3.0000 /    3.6000)
DDM SFP TX bias: 0.0000 mA (Warn:   4.0000 /   70.0000)(Alarm:   2.0000 /   80.0000)
DDM SFP TX power: -40.0000 dBm (Warn: -9.5001 /  -2.9999)(Alarm: -10.5012 /   -1.9997)
DDM SFP RX power: -40.0000 dBm  (Warn: -21.0237 / -2.9999)(Alarm:-22.0066 /  -1.9997)

MG205X (config)#
```

Following is the same case while the DDM is disabled.

```
MG205X (config)# show port module-info 1
Port   1
             Transceiver type:  SFP
                  Transceiver:  1000Base-LX
                       Length:  10 Km [ Single Mode ]
                        Speed:  1250 Mb/s
                   Wavelength:  1310 nm
               Connector Type:  LC
                  Vendor name:  CORETEK
             Vendor part name:  CT-1250TSP-MB4LD
              Vendor revision:  0000
         Vendor serial number:  CF0032H1400079
                 Product date:  2008-03-11

MG205X (config)#
```

7.4 QoS (Quality of Service)

Typically, when processing data in a network, first-in data is processed first (First-in, first-out). This way is not useful when there are high priority processing data. Also it is dangerous when many packets are arrived at one time.

However, using QoS, it is possible to provide better service to the selected network traffic by setting priorities etc. by the importance level especially when traffics are overloaded.

◆ Benefits of QoS

- Network Resource Control

Network administrator can limit the bandwidth for FTP transmission, or put high priority on important data.

- Efficient use of resources

It is possible to check the data processing of the network, and can take high priority data firstly.

- Customized services

Network administrator can provide differentiated services to users.

- Important priority data

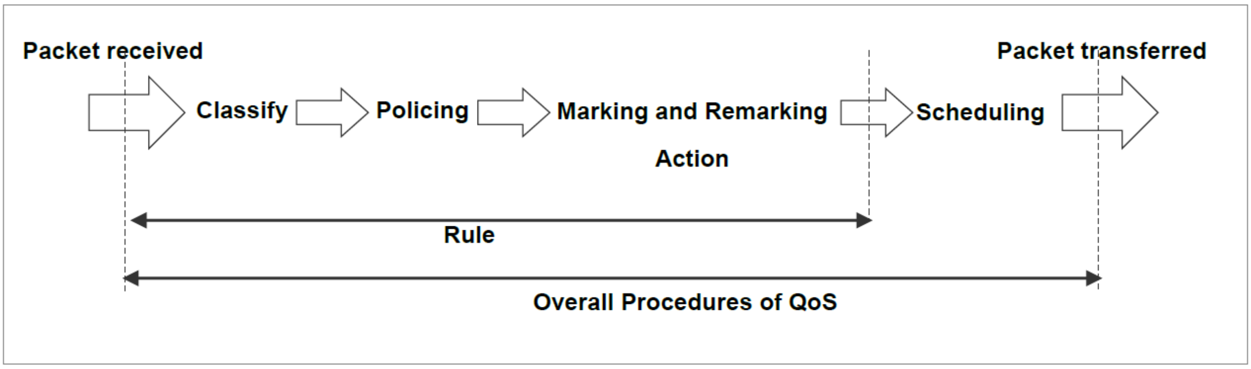
Our QoS guarantee bandwidth to process high priority data and audio data first, and minimize the delay time. The rest general data processing is processed by priority-based FIFO (first-in, first-out) scheduling.

On the other hand, it should be noted in the QoS setting that high priority packet processing shouldn't cause the failure of any other packet transmission.

7.4.1 QoS operation Principle

Briefly explanation of the QoS process in MG205X is as follows: User sets the condition to classify the arrived packets and packet policy(Policing), and then, the packets will be processed by the settings of the user. Then, the processed packet will be sent to the outside according to the scheduling method set by the user.

The following is a brief illustration shows the operating structure of MG205X QoS.



【Picture 7-3】Operation Structure of QoS

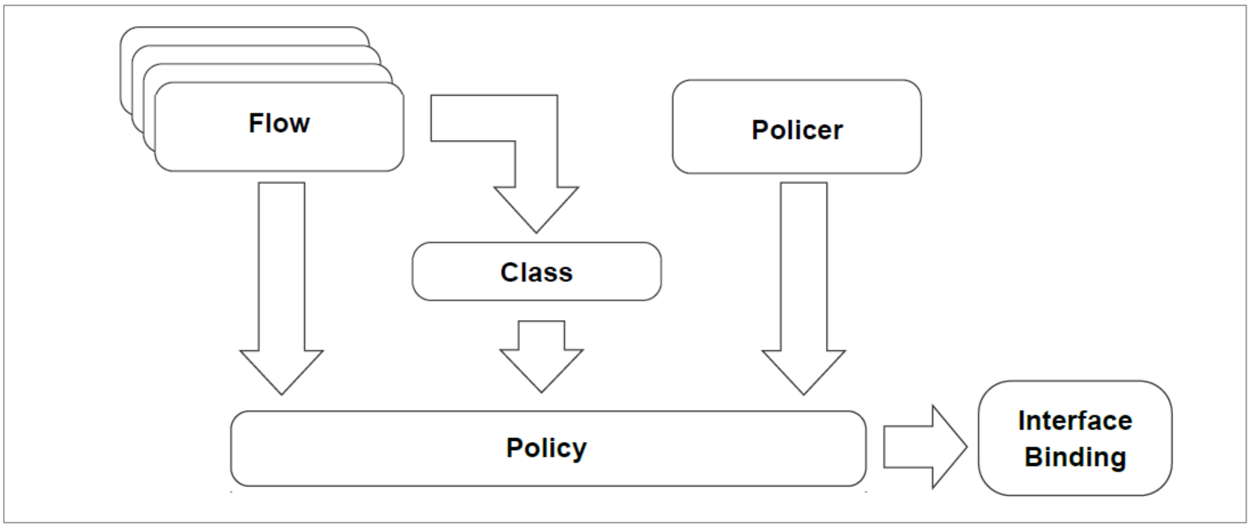
'Rule' is a function used for classification and processing of packets partially, and it is useful because it helps making various settings into a single rule to run at a time.

The basic structure of the Rule is classified into four types - Flow, Class, Policer and Policy.
Each type is responsible for followings.

● Flow: It defines the criteria for classifying packets. The values specified by the classification criteria are MAC address, IP address, DSCP, Ether type, etc.

- Class: It is considered as a collection of flow. It is introduced for more efficient management in policy application to flow.
- Policer: It defines the policy which will be applied to the flow and class. It will set the metering and counting, etc. to the corresponding flow and class.
- Policy: It can select flow, class or policier by the demand, and it makes decision on action of packet, or set or adjust the various values used for priority setting(marking/remarking).

Flow, Class, Policer and Policy are the basic structure of Rule, and their relationship is as follows.



【Picture 7-4】Structure of Rules

Flows more than 2 can be managed as a single class. Flow, class and policer will be executed by becoming a part of single policy. Flow, Class or Policer which are not included in policy are regarded as only data of the equipment that simply can be used to run the rule, and will not be executed at all.

As a single policy cannot have flow and class at the same time, policy including flow cannot include class, policy including class cannot include flow. and the same flow or class can be included in plural policy, but one policer is possible to be included only in one policy.

In MG205X, about 1,000 executable rules are supported to compose policy.

7.4.2 Packet Classification Setting

In MG205X, flow is made with the criteria for classifying packets which rule is to be applied, and class is to be used for managing multiple flows.

(1) Flow Setting

To set flows, user should create flows first, and then, settings of detailed packet classification criteria can be followed in Flow setting mode.

To create flows and do settings of packet classification criteria in Flow setting mode, use the following command.

Command	Mode	Function
flow *flow-name* **create**	Global	Create a flow and enter into Flow setting mode.

On the other hand, use the following command to delete the settings of the flow.

Command	Mode	Function
no flow *flow-name*	Global	Delete the named flow.
no flow all		Delete all Flow.

Packet classification criteria in Flow setting mode are MAC address, IP address, Ethertype, CoS, DSCP, etc.

To classify packets based on the MAC address, use the following command.

Command	Mode	Function
mac {*src-mac-address* | *src-mac-address/mask* | **any**} {*dst-mac-address* | *dst-maca-address/mask* | **any**}	Flow	Classify packets based on source MAC address and destination MAC address.

To classify packets based on IP address and protocol, use the following command.

Command	Mode	Function
ip {*src-ip-address* | *src-ip-address/m* | **any**} {*dst-ip-address* | *dst-ip-address/m* | **any**}	Flow	Classify packets based on source IP address and destination IP address.
ip {*src-ip-address* | *src-ip-address/m* | **any**} {*dst-ip-address* | *dst-ip-address/m* | **any**} <0-255>		
ip {*src-ip-address* | *src-ip-address/m* | **any**} {*dst-ip-address* | *dst-ip-address/m* | **any**} {**icmp** | **tcp** | **udp**}		Classify packets based on source IP address and destination IP address which corresponds to the protocols.
ip {*src-ip-address* | *src-ip-address/m* | **any**} {*dst-ip-address* | *dst-ip-address/m* | **any**} **icmp** {<0-255> | **any**} {<0-255> | **any**}		Classify packets based on source IP address and destination IP address which corresponds to code value of ICMP.
ip {*src-ip-address* | *src-ip-address/m* | **any**} {*dst-ip-address* | *dst-ip-address/m* | **any**} **tcp** {<1-65535> | **any**} {<1-65535> | **any**} [*tcp-flag* | **any**]		Classify packets based on source IP address and destination IP address which corresponds to TCP.

ip {*src-ip-address* | *src-ip-address/m* | **any**} {*dst-ip-address* | *dst-ip-address/m* | **any**} **udp** {<1-65535> | **any**} {<1-65535> | **any**}		Classify packets based on source IP address and destination IP address which corresponds to UDP.

To classify packets based on IP v6 address and protocol, use the following command.

Command	Mode	Function
Ipv6 {*src-ipv6-address* | *src-ipv6-address/m* | **any**} {*dst-ipv6-address* | *dst-ipv6-address/m* | **any**}	Flow	Classify packets based on source IP address and destination IPv6 address.
Ipv6 {*src-ipv6-address* | *src-ipv6-address/m* | **any**} {*dst-ipv6-address* | *dst-ipv6-address/m* | **any**} <0-255>		
Ipv6 {*src-ipv6-address* | *src-ipv6-address/m* | **any**} {*dst-ipv6-address* | *dst-ipv6-address/m* | **any**} {**icmp** | **tcp** | **udp**}		Classify packets based on source IP address and destination IPv6 address which corresponds to the protocols
Ipv6 {*src-ipv6-address* | *src-ipv6-address/m* | **any**} {*dst-ipv6-address* | *dst-ipv6-address/m* | **any**} **icmp** {<0-255> | **any**} {<0-255> | **any**}		Classify packets based on source IP address and destination IPv6 address which corresponds to code value of ICMP
Ipv6 {*src-ipv6-address* | *src-ipv6-address/m* | **any**} {*dst-ipv6-address* | *dst-ipv6-address/m* | **any**} **tcp** {<1-65535> | **any**} {<1-65535> | **any**} [*tcp-flag* | **any**]		Classify packets based on source IP address and destination IPv6 address which corresponds to TCP
Ipv6 {*src-ipv6-address* | *src-ipv6-address/m* | **any**} {*dst-ipv6-address* | *dst-ipv6-address/m* | **any**} **udp** {<1-65535> | **any**} {<1-65535> | **any**}		Classify packets based on source IP address and destination IPv6 address which corresponds to UDP.

To classify packets based on IP ToS precedence, CoS, ToS, DSCP, Ethertype, packet length, IP-Header etc., use the following command.

Command	Mode	Function
ip-precedence {<0-7> | **any**}	Flow	Classify packets based on setting of IP TOS precedence.
cos {<0-7> | **any**}		Classify packets based on setting of CoS value.
tos {<0-255> | **any**}		Classify packets based on setting of ToS value.
dscp {<0-63> | **any**}		Classify packets based on setting of DSCP values.
ethtype {*ethertype* | **arp** | **any**}		Classify packets based on setting of Ethtype.
outer-vlan {<1-4094> | any} **outer-cos** {<0-7> | any} **inner-vlan** {<1-4094> | any} **inner-cos** {<0-7> | any}		Classify packets corresponding to the outer VLAN information and the inner VLAN information that are set.

Reference

User can set multiple criteria of packet classification to a flow.

On the other hand, to delete the settings of packet classification criteria in the flow, use the following command in Flow setting mode.

Command	Mode	Function
no cos	Flow	Delete the settings of packet classification criteria in the flow.
no dscp		
no ethtype		
no ip		
no ipv6		
no ip-precedence		
no length		
no mac		
no tos		

(2) Flow Setting Save and Modification

After flow settings, user should save it in the equipment by using the following command.

Command	Mode	Function
apply	Flow	Save the flow settings in the equipment.

Reference

If user return from Flow setting mode to Global mode without flow settings saving, all flow settings will be deleted.

On the other hand, if user wants to modify the contents of an existing Flow, user should enter the Flow setting mode of the particular intended to be modified. To enter into the Flow setting mode to modify the contents of Flow, use the following command.

Command	Mode	Function
flow *flow-name* **modify**	Global	Enter into the Flow setting mode to modify the contents of Flow.

Reference

After modification of the contents in the flow, please save the contents using ‘apply’ command.

(1) Class Setting

If the packets are classified by several conditions, it may require two or more flows. In this case, if multiple flows are bundled as ‘class’, it is easy to manage and the settings are related settings are easy.

To make class setting by bundling multiple flows, use the following command to set the Class.

Command	Mode	Function
class *class-name* **flow** *flow-name* [*flow-name*] [*flow-name*]···	Global	Make class setting by bundling named multiple flows

Meanwhile, to delete class setting, use the following command.

Command	Mode	Function
no class all	Global	Delete all class setting.
no class *name*		Delete the named class setting.
no class *name* **flow** *flow-name* [*flow-name*] [*flow-name*] ···		Delete the named flows in the class.

7.4.3 Packet Policing Setting

Setting policies(policing) to classified packet is done in Policer. Packet policies that can be applied in policer have Metering, Rate-limit setting, packet counter setting etc.

(1) Policer Creation

To set policies for classified packets, user can enter into the Policer setting mode after creating policer by following command.

Command	Mode	Function
policer *policer-name* **create**	Global	Create a Policer and enter into the Policer setting mode.

On the other hand, to delete the Policer setting, use the following command.

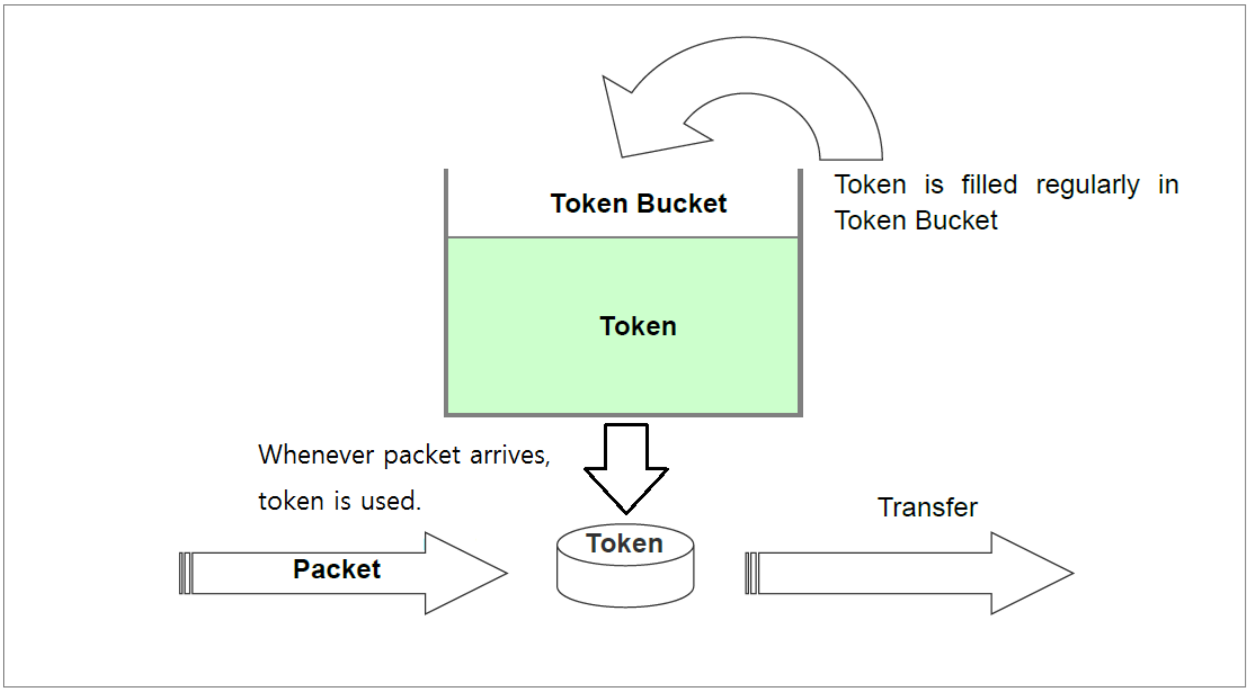
Command	Mode	Function
no policer *policer-name*	Global	Delete the named Policer setting.
no policer all		Delete all Policer settings.

(2) Metering

Metering supported by MG205X has two methods of SRTCM (Single Rate Three Color Marker) and TRTCM (Two Rate Three Color Marker). The two methods are operating by Token Bucket way.

Token Bucket way

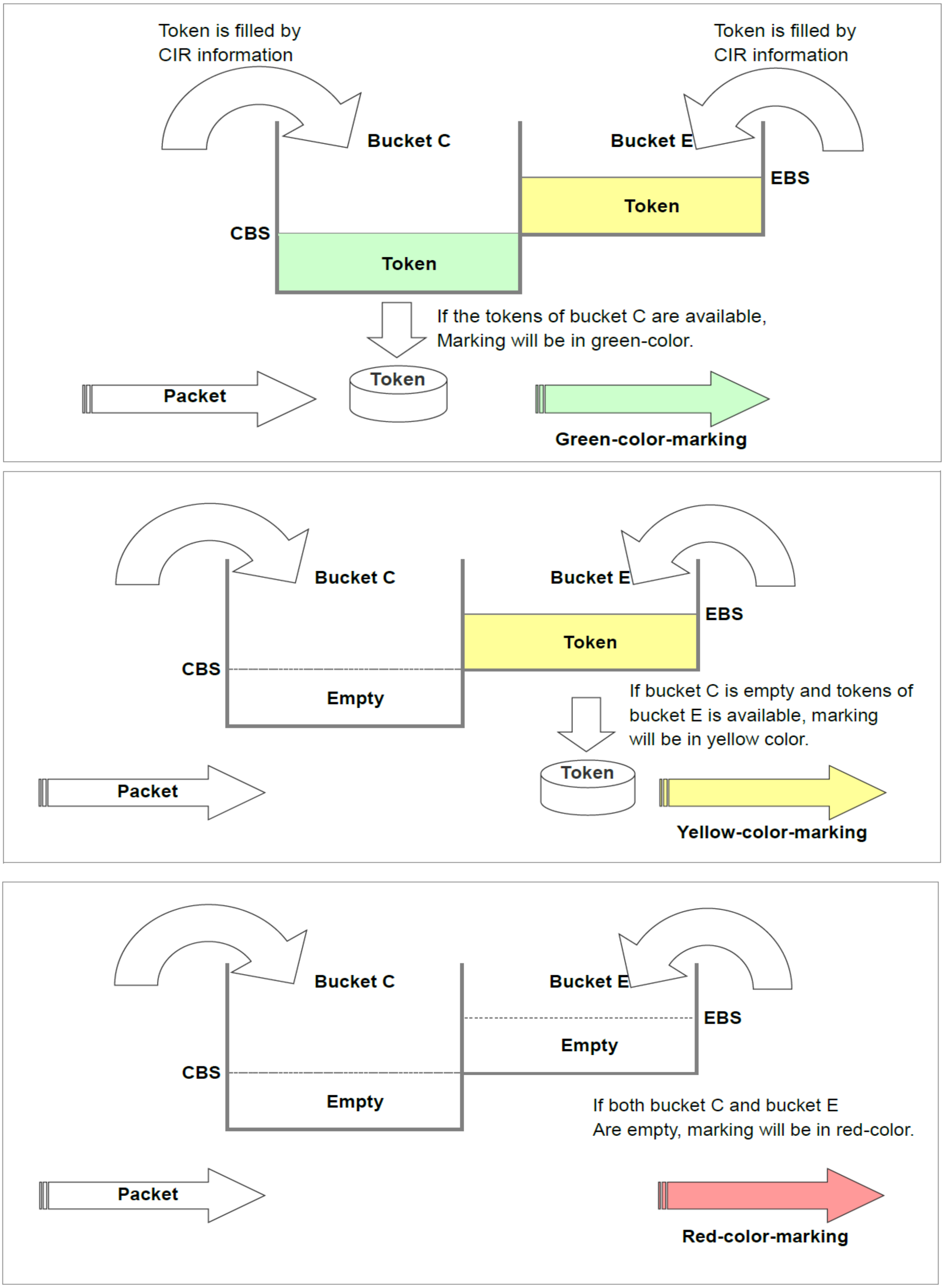
Token Bucket way is using packet transmission by using tokens in the token bucket. Tokens are populated in the token bucket continuously with certain quantity, and after using up the tokens by massive packets, it will not be possible to transmit any packet until the token bucket is filled by token.


Token Bucket
Token
Token is filled regularly in Token Bucket
Whenever packet arrives, token is used.
Packet
Token
Transfer

【Picture 7-5】Token Bucket Method

SRTCM (Single Rate Three Color Marker)

SRTCM is defined in RFC2697. Based on criteria of CIR (Committed Information Rate) and CBS (Committed Burst Size) and EBS (Excess Burst Size), three colors of Green, Yellow and Red will be marked. CIR is the speed rate of filling the token in the bucket, and the bucket size is used as criteria of color marking in two steps of CBS and EBS in different color.



If the tokens of bucket C are available,
Marking will be in green-color.

If bucket C is empty and tokens of
bucket E is available, marking
will be in yellow color.

If both bucket C and bucket E
Are empty, marking will be in red-color.

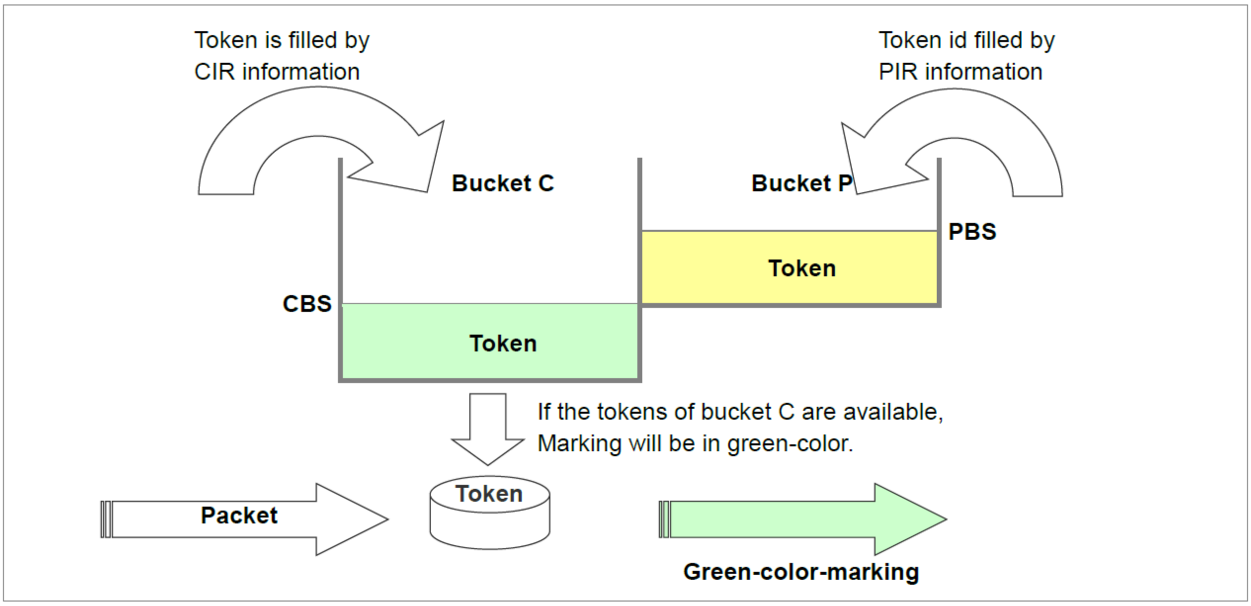
【Picture 7-6】Color Marking of Single Rate Three Color Marker

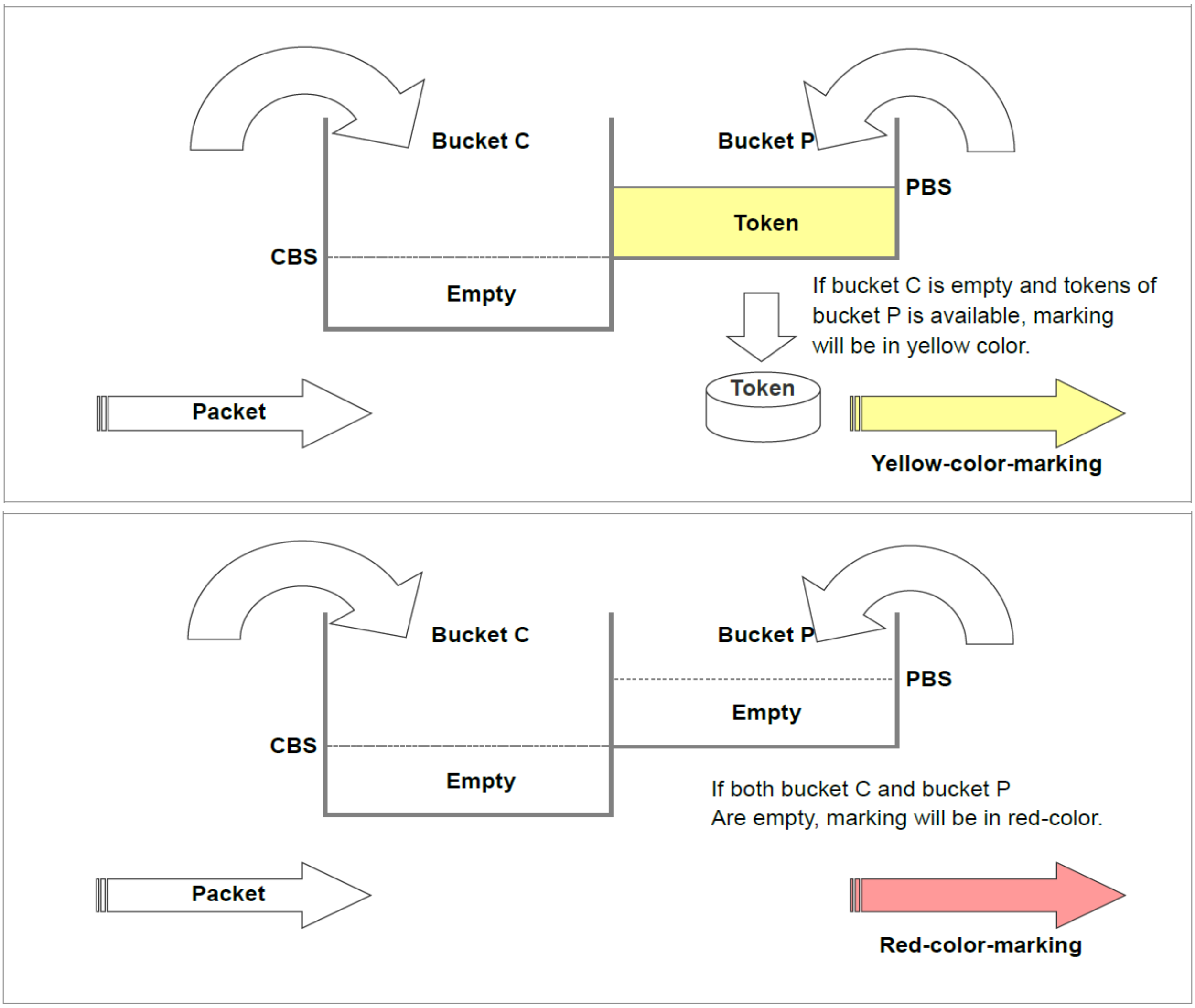
When the packet is sent to equipment, if the token of bucket C based on CBS is available, green color will me market, if bucket C is empty and the token of bucket E based on EBS is available, yellow-color will be market. But, due to high packet transmission rate, if both bucket C and bucket E are empty, red-color will be marked.

In RFC2697, one of the CBS and the EBS must be set to a value greater than zero, and it should have the same or greater value setting then the maximum size of a packet to be received by the equipment. This is to let minimum 1 packet pass.

TRTCM (Two Rate Three Color Marker)

TRTCM is defined in RFC2698. Based on criteria of CIR (Committed Information Rate) and PIR (Peak Information Rate) and PBS (Peak Burst Size), three colors of Green, Yellow and Red will be marked.
SRTCM is using CIR based on speeds of filling tokens of CBS bucket C and EBS bucket E, TRTCM is based on the speed with CBS to fill the token in the Bucket C and PBS to fill the token in the bucket P. These are CIR and PIR, which is applied differently respectively




Bucket C
Bucket P
PBS
Token
CBS
Empty
If bucket C is empty and tokens of bucket P is available, marking will be in yellow color.
Token
Packet
Yellow-color-marking
Bucket C
Bucket P
PBS
Empty
CBS
Empty
If both bucket C and bucket P Are empty, marking will be in red-color.
Packet
Red-color-marking

【Picture 7-7】Color Marking of Two Rate Three Color Marker

When the packet is sent to equipment, if the token of bucket C based on CBS is available, green color will me market, if bucket C is empty and the token of bucket P based on PBS is available, yellow-color will be market. But, due to high packet transmission rate, if both bucket C and bucket P are empty, red-color will be marked.

In RFC2698, one of the CBS and the PBS must be set to a value greater than zero, and it should have the same or greater value setting than the maximum size of a packet to be received by the equipment. This is to let minimum 1 packet pass.

To run metering for the classified packets, please set the metering mode first by following command.

Command	Mode	Function
color mode {srtcm ∣ trtcm} blind	Policer	Set the metering mode to color-blind mode.

Blind mode is metering without consideration of marked color, and 'Aware' is metering with consideration of marked color.

If the metering mode setting is finished, each value of metering should be set. If it is SRTCM, the values of CIR, CBS and EBS should be set, and if it is TRTCM, the values of CIR, PIR, CBS and PBS should be set.

To delete metering mode setting, use the following command.

Command	Mode	Function
no color mode	Policer	Delete the settings in metering mode and return to the default mode.

To set the value of each criteria used in the metering, use the following command.

Command	Mode	Function
color cir *bandwidth* **cbs** *burst*	Policer	Set the CIR and CBS values.
color ebs *burst*		Set EBS value.
color pir *bandwidth* **pbs** *burst*		Set the PIR and PBS values.

Reference

Unit of CIR and PIR settings is Kbps, and it is a multiple of 64 Kbps is. EBS, CBS and PBS settings are by a certain bytes.

Reference

If there is no setting in Metering, all packets will be classified as Green-color.

To have changed setting of the DSCP values of each color-marked packet based on the metering criteria, use the following command.

Command	Mode	Function
color dscp <0-63> {**green** | **yellow** | **red**}	Policer	Set the changed DSCP value for each color-marking packet.

In the Blind mode, red-colored or yellow-colored packets can be set to drop by using following command.

Command	Mode	Function
color red action drop	Policer	Set to drop the packets with red-colored marking.
color yellow action drop		Set to drop the packets with yellow-colored marking.
no color {**red** | **yellow**} **action**		Disable the setting which is to drop the packets with red or yellow-colored marking.

In the Aware mode, to do remarking of packets marked in red-color or yellow-color, use the following command.

Command	Mode	Function
color {**red** | **yellow**} **action marking** [**drop-precedence** {**red** | **yellow** | **green**}]	Policer	Set to do remarking of packets marked in red or yellow-color.

(3) Packet Counter

In MG205X, packet counter can be set to count the packets processed by the rule. This feature is helpful to identify the characteristics of packets that are sent to the equipment according to the rule settings of the administrator.

To check the received number of packets corresponding to the rules of administrator, use the following command in Policer mode.

Command	Mode	Function
counter	Policer	Check the received number of packets corresponding to the rules of user.

⃠ **Attention**

In MG205X, packet counter can't count the packets which are dropped by the rule of administrator.

To disable the packet counter setting to check the received number of packets corresponding to the rules of administrator, use the following command in Policer mode.

Command	Mode	Function
no counter	Policer	Disable the packet counter setting to check the received number of packets corresponding to the rules of administrator

To initialize the MG205X Policy Counter, use the following command.

Command	Mode	Function
clear policy counter {*policer-name* | **all**}	Enable/Global/Bridge	Initializes the Policy Counter.

To check the counted number of Rule, use the following command.

Command	Mode	Function
show flow statistics	Enable/Global	Show the counted number of the flow.
show policer statistics		Show the counted number of the policer.

show policy statistics		Show the counted number of the policy.

(4) Packet Rate-limit

In MG205X, user can adjust the bandwidth for the packet classified. To set the rate-limit for the packets classified, use the following command in Policer mode.

Command	Mode	Function
rate-limit *bandwidth*	Policer	Set the rate-limit for the packets classified

Reference

Rate-limit of the classified packet is set as Kbps.

(5) Policer Setting Save and Modification

After policer setting for the classified packets, user must save the contents of policer by using the following command.

Command	Mode	Function
apply	Policer	Save the policer settings in the equipment.

Reference

If policer setting is not saved and return Global setting mode, the settings will be deleted.

On the other hand, if user wants to modify the contents of the existing policer, user has to enter into the setup mode of the policer. To enter into the setting mode of a certain policer to modify the contents of it, use the following command.

Command	Mode	Function
policer *policer-name* **modify**	Global	Enter into the setting mode of the policer to modify the contents.

Reference

After the modification of the policer contents, the modified contents must be saved by 'apply' command.

7.4.4 Rule Operation Setting

After flow and class settings for packet classification and policer setting to be applied for the classified packet, policy setting by selective composition of needed flow, class or policer and rule operating will be followed.

(1) Policy Setting

To create Policy and enter into Policy setting mode, use following command.

Command	Mode	Function
policy *policy-name* **create**	Global	Create Policy and enter into Policy setting mode

On the other hand, to delete the created Policy and its setting, use the following command.

Command	Mode	Function
no policy *policy-name*	Global	Delete the policy and its setting.
no policy all		Delete all policy.

After creating Policy, please include Flow, Class and Policer in the Policy by using following command.

Command	Mode	Function
include-flow *flow-name*	Policy	Include the specified flow in the policy.
include-class *class-name*		Include the specified class in the policy.
include-policer *policer-name*		Include the specified policer in the policy.

Reference

It's not possible to include flow and class in policy at the same time.

Reference

The same flow and class can be included in multiple policies, but one policer can be included on only one policy.

To delete flow, class or policer that had been included in policy, use the following command.

Command	Mode	Function
no include-flow	Policy	Delete flow.
no include-class		Delete class.
no include-policer		Delete policer.

(2) Policy Priority Setting

User can set the priority to the created Policy by following command.

Command	Mode	Function

priority {**low** | **medium** | **high** | **highest**}	Policy	Set the priority to the policy

Reference

All Policy had default priority as ‘low’.

(3) Action Setting

To set action of the Rule to process the packet, use the following command in the Policy Mode.

Command	Mode	Function
action match copy-to-cpu	Policy	Copy to send the classified packet to CPU.
action match deny		Don’t accept the classified packet.
action match mirror		Copy to send the classified packet to mirroring port.
action match dmac *dst-mac-address*		Set the destination MAC address of the packetcorresponding to the rule.
action match dscp <0-63>		Set the DSCP value to the ToS area of packet corresponding to the rule.
action match egress filter *port-number*		Exclude the corresponding port from egress port of packets corresponding to the rule.
action match egress port *port-number*		Replace the egress port of packet corresponding to rule with specified port.
action match permit		Permit to accept classified packet.
action match redirect *port-number*		Transfer the classified packet to the specified port.

Attention

Command of ‘redirect’ cannot be used together with ‘MAC filtering’.

To disable the settings of Rule action for the classified packet, the following command in the Policy Mode.

Command	Mode	Function
no action match copy-to-cpu	Policy	Disable the corresponding setting of Rule action.
no action match deny		
no action match mirror		
no action match dmac		

no action match dscp		
no action match egress		
no action match permit		
no action match redirect		

(4) Cos Value and ToS Value Setting

To apply scheduling values by using the rule set by the user, rating should be applied to each rule first. CoS values are separated by a total of 8 ratings. Meanwhile, ‘overwrite’ variables are used to decide if packets are processed with CoS rating only in the equipment or if packets go out with the CoS value to outside network too. In other words, CoS value will be applied for internal and external communication if ’overwrite’ is included in commands, and CoS value will be applied only for internal communication if ‘overwrite’ is not included in the commands.

For applying a rating to a packet corresponding to the rule of user, use the following command.:

Command	Mode	Function
action match cos <0-7> [**overwrite**]	Policy	Set CoS value to the packet corresponding to the rule.
action match cos same-as-tos overwrite		Set Cos value as IP ToS precedence value to the packet corresponding to the rule.
action match ip-precedence <0-7>		Set IP ToS precedence value to the packet corresponding to the rule.
action match ip-precedence same-as-cos		Set IP ToS precedence value as Cos value to the packet corresponding to the rule.

To disable above CoS and ToS value settings, use the following command.

Command	Mode	Function
no action match cos [**overwrite**]	Policy	Disable the CoS / ToS value settings.
no action match cos same-as-tos overwrite		
no action match ip-precedence		
no action match ip-precedence same-as-cos		

(5) Rule-applied Interface Setting

If the settings of ‘Classify’, ‘Policing’ and ‘Rule’ operations are finished in MG205X, user must specify an interface to apply the rule. Otherwise, the rule will not work.

To specify an interface to apply the Rule, use the following command.

Command	Mode	Function
interface-binding port ingress {*src-port-number* ǀ **any**}	Policy	Apply the rule to the interface which the packets received through the specified ports.
interface-binding vlan {<1-4094> ǀ **any**}		Apply the rule to the interface which the packets received with the VLAN ID.

To disable the interface setting to apply the rule, use the following command.

Command	Mode	Function
no interface-binding port ingress [*src-port-number*]	Policy	Disable the interface setting to apply the rule.
no interface-binding vlan		

(6) Policy Setting Save and Modification

After setting the Policy to run the operation of rule, user must save the policy setting in the equipment by using the following command.

Command	Mode	Function
apply	Policy	Save the policy setting in the equipment.

Reference

If user returns to Global mode from Policy setting mode without saving the settings, all the settings will be deleted.

On the other hand, if user wants to modify the contents of the existing policy setting, user need to enter into the Policy setting mode by using following command.

Command	Mode	Function
policy *policy-name* **modify**	Global	Enter into the Policy setting mode of the specified policy.

Reference

After modification of the policy contents, user must save the contents using ‘apply’ command.

(7) Policy Setting Check

To check the policy information set per each port by the user, use the following command.

Command	Mode	Function

show port policy *port-number*	Enable/global/bridge	Show the policy information set for the specified port.

7.4.5 Rule Setting Check

To check the Rule Profile set by the user, use the following command.

Command	Mode	Function
show flow-profile	Flow	Show the rule profile of the corresponding profile.
show policer-profile	Policer	Show the rule profile of the corresponding policer.
show policy-profile	Policy	Show the rule profile of the corresponding policy.

To check the contents of the Rule set by the user, use the following command.

Command	Mode	Function
show {**flow** | **class** | **policer** | **policy**} [*name*]	View/Enable/ Global/Bridge	Show the contents of the Rule.
show {**flow** | **class** | **policer** | **policy**} **detail** [*name*]		

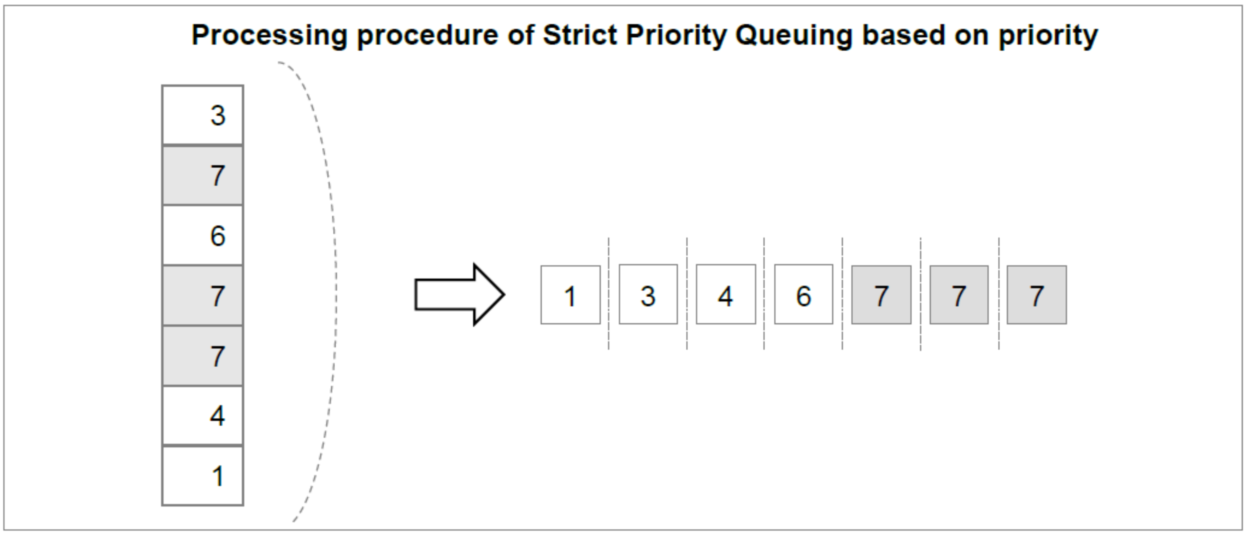
7.4.6 Scheduling Setting

Packets processed by the rule setting of the user will be sent out of the equipment after scheduling finally. In MG205X, supported scheduling methods are Strict Priority Queuing, WRR and DRR.

- **Strict Priority Queuing**

Strict Priority Queuing is a scheduling method which packet with high priority queue is processed first. In other words, packets in low priority queue are processed after all of the packets of the high priority queue are processed. Even though packets in low priority queue are in processing, if any packet in high priority queue is entered, the processing for the packet of the low priority queue is stopped temporarily. This approach is simple method with an advantage of differentiated services based on priority.

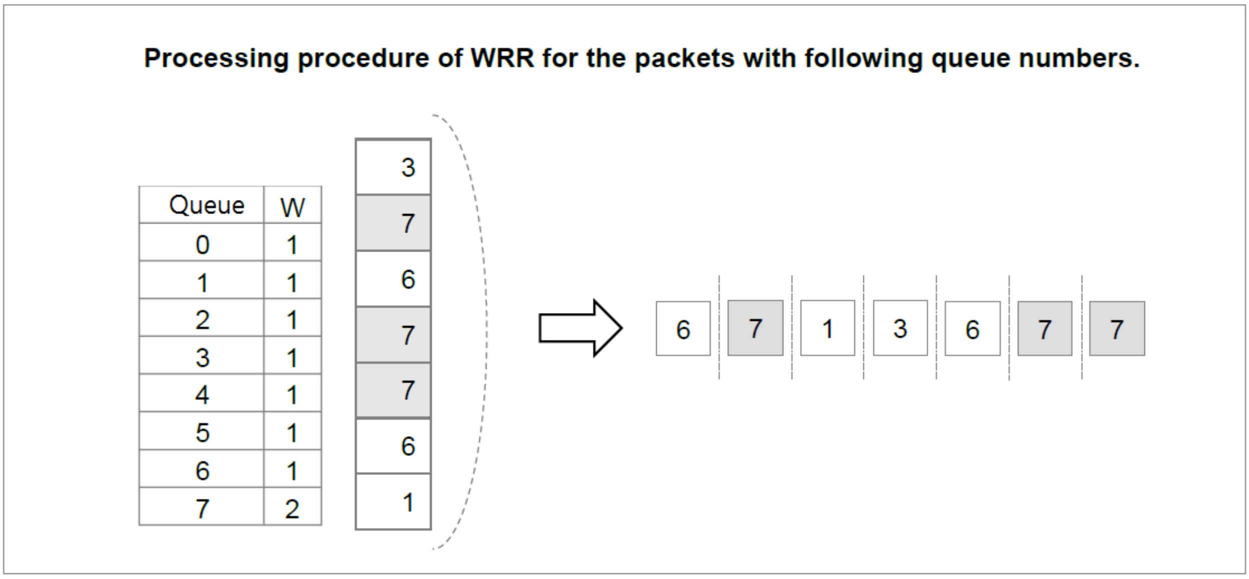
However, if high priority packets are entered continuously, it will cause a problem that the packets of lower priority queue are not processed.


Processing procedure of Strict Priority Queuing based on priority
3
7
6
7
7
4
1
1
3
4
6
7
7
7

【Picture 7-8】Packet Processing in Strict Priority Queuing

- **WRR(Weighted Round Robin)**

WRR is a method for processing packets in turn given by the Weight value. The packet with first priority queue is processed first in the same way of the Strict Priority Queuing, but the difference is that the packet processing is as much as the given weight value and it goes to process the next packet. This method provides unbiased processing to high priority queue, but it has limits to provide enough differentiated services in fair services.


Processing procedure of WRR for the packets with following queue numbers.
3
7
6
7
7
6
1
6
7
1
3
6
7
7

Queue	W
0	1
1	1
2	1
3	1
4	1
5	1
6	1
7	2

【Picture 7-9】Packet Processing in WRR

- **DRR(Deficit Round Robin)**

DRR determines the packet processing sequence by the parameters from percentage value of receiving port bandwidth assigned to queue, total amount of bytes which can be transferred each time by scheduler and bytes to weight ratio. It is an advantage that allocated bandwidth per class is guaranteed precisely regardless of the packet size.

(1) Scheduling Mode Setting

To set scheduling method from the three types, use the following command.

Command	Mode	Function
qos scheduling-mode {**sp** | **wrr** | **drr**} *port-number*	Global	Set the scheduling method as selected.

Reference

MG205X is set to "WRR" as the default method.

(2) Weight Setting

WRR scheduling method is using weight value which can be set by the following command

Command	Mode	Function
qos weight *port-number queue-number weight-value*	Global	Set weight value to the corresponding queue of the specified port.
qos weight *port-number queue-number* **unlimited**		Set the corresponding queue of the specified port as strict priority queuing.

Reference

The queue-number can be set from 0 to 3, and weight-value can be from 1 to 255.

Reference

In MG205X, weight value of all queues are set to "1" as default.

To set up the quantum to use the DRR method, use the following command.

Command	Mode	Function
qos quantum *port-number queue-number quantum- value*	Global	Set quantum value to the corresponding queue of the specified port.
qos quantum *port-number queue-number* **unlimited**		Set the corresponding queue of the specified port as strict priority queuing.

Reference

The queue-number can be from 1 to 3, and the quantum- value can be from 1 up to 255.

Reference

In MG205X, the quantum- value of all queues are set to "1" as default.

To set scheduling method from the three types, use the following command.

Command	Mode	Function
qos scheduling-mode {**sp** ǀ **wrr** ǀ **drr**} *port-number*	Global	Set the scheduling method as selected.

(3) Min-bandwidth Setting

DRR scheduling method limits the throughput of packet in the corresponding queue by bandwidth. Therefore, when using the DRR approach, user must set the guaranteed bandwidth for each queue. This guaranteed bandwidth is called Min-bandwidth.

Reference

In MG205X, the minimum guaranteed bandwidths for all queues are set to "0".

To set the guaranteed bandwidth, use the following command.

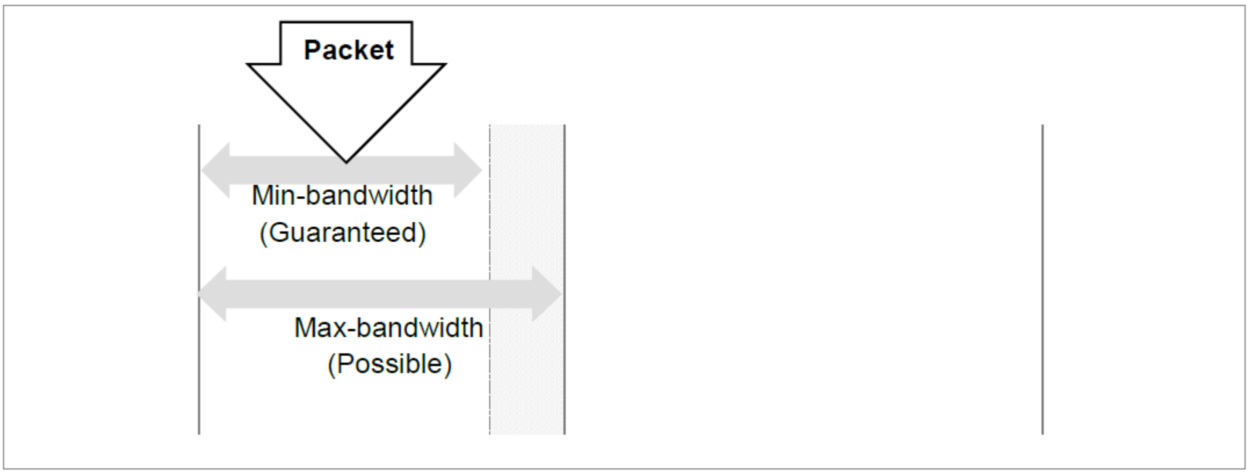
Command	Mode	Function
qos min-bandwidth *port-number* <0-3> <1-100>	Global	Set the min-bandwidth to the port.
qos min-bandwidth *port-number* <0-3> **unlimited**		Set the min-bandwidth as unlimited.

Reference

If the scheduling method is set to SP or WRR, then guaranteed bandwidth can’t be set.

(4) Max-bandwidth Limit Setting

Scheduling by Strict Priority Queuing method can cause concentrated processing of packets in only high priority rating. To prevent these, user can have a maximum limit on bandwidth. Max-bandwidth is the function of this role.



【Picture 7-10】Min-bandwidth and Max-bandwidth in DRR

To set the maximum bandwidth available to the queue, use the following command:

Command	Mode	Function
qos max-bandwidth *port-number* <0-3> <1-100>	Global	Set the maximum bandwidth for the port.
qos max-bandwidth *port-number* **unlimited**		Set the maximum bandwidth for the port as unlimited.

Reference

In MG205X, max-bandwidth is set as unlimited by default.

Reference

If the scheduling method is set to SP or WRR, then maximum bandwidth can’t be set.

(5) Traffic Limit Setting for Specific Port

In MG205X, user can limit the traffic on specific port by using the QoS function. To limit the buffer size of the specific receiving port (Ingress Port), use the following command.

Command	Mode	Function
qos ibp *port-number* <1-576>	Global	Limit the buffer size of specific receiving port. (Default value : 192)

To disable the limit setting of buffer size in the receiving port, use the following command.

Command	Mode	Function
no qos ibp *port-number*	Global	Disable the limit setting of buffer size in the receiving port.

Meanwhile, user can limit the number of packets and buffer size for the transferring port (Egress Port) at the same time. To limit the traffic of the transferring port, use the following command.

Command	Mode	Function
qos pktlimit *port-number queue-number* <4-2047>	Global	Limit the number of packets used in the queue of specific transferring port. (Default value : 256)
qos seglimit *port-number queue-number* <1-8191>		Limit the buffer size used in the queue of specific transferring port. (Default value : 32)

Reference

The queue-number can be from 0 up to 3.

To disable the limit setting of the number of packets and buffer size for the transferring port (Egress Port), use the following command.

Command	Mode	Function
no qos pktlimit *port-number* <0-3>	Global	Disable the limit setting of the number of packets for the specified transferring port.
no qos seglimit *port-number* <0-3>		Disable the limit setting of the buffer size for the specified transferring port.

On the other hand, to check the traffic limit setting on specific port, use the following command.

Command	Mode	Function
show qos buffer *port-number*	Enable/Global/ Bridge	Show the traffic limit setting information for the specific port.

(6) CPU Packet Scheduling Mode Setting

Scheduling method of CPU packet processing can be set to either Priority Queuing or WRR by following command.

Command	Mode	Function
qos cpu scheduling-mode {**sp** ∣ **wrr**}	Global	Set the CPU packet scheduling method.

Reference

In MG205X, "Strict Priority Queuing" is used as default method.

(7) CPU Packet Weight Setting

WRR scheduling method is processed by weight value which can be set by following command.

Command	Mode	Function
qos cpu weight *queue-number weight-value*	Global	Set the weight value to the specified queue.
qos cpu weight *queue-number* **unlimited**		Set the scheduling of specified queue as Strict Priority Queuing.

Reference

The queue-number can be 0 up to 3, and the weight-value can be entered from 1 up to 15.

Reference

In MG205X, the default value of weight is "1" to all queues.

(8) QoS Setting Check

To check the settings of QoS, use the following command.

Command	Mode	Function
show qos	Enable/Global/ Bridge	Show the settings of QoS scheduling.
show qos *port-number*		Show the settings of QoS scheduling per port.
show qos cpu		Show the settings of QOS regarding CPU packets.

(9) Traffic Queue Status Check Per Port

In MG205X, the amount of traffic on each port queue can be checked by following command.

Command	Mode	Function
show queue status *port-number* <0-3>	Enable/Global/ Bridge	Show the traffic amount of queue per specified port.

7.4.7 Admin Rule Setting

To block the interface of telnet, ftp, icmp, snmp etc., many rules should be applied, and it is complicated. In order to improve this inconvenience, the MG205X supports a function to do filtering the packets before forwarding to the connected equipment. To block the service interface of Telnet, FTP, ICMP, SNMP, etc. coming into the MG205X itself, 'Admin Rule' function is used.

7.4.8 Admin Rule Packet Classification Setting

In MG205X, user makes a flow setting of packet classification condition to apply admin rule, and class is used for managing multiple admin flow.

(1) Admin Flow Setting

In MG205X, to set Admin Rule, Admin Flow should be created and enter into the Flow Setting mode. To enter into Flow setting mode for setting detailed conditions of packet, use the following command.

Command	Mode	Function
flow admin *name* **create**	Global	Enter into Flow setting mode for setting detailed conditions of packet after creating new Admin Flow.

If user enters into the admin flow setting mode, the command prompt will be changed from 'MG205X (config) #' to 'MG205X (config-admin-flow [name])#, MG205X (config-admin-policy [name])#.

Reference

User can set various Policy to an Admin Flow or a Policy.

On the other hand, to delete the Admin Flow setting, use the following command.

Command	Mode	Function
no flow admin *flow-name*	Global	Delete the created admin flow.
no flow admin all		Delete all flows

User can set the Admin Flow/Policy properly in Admin Flow/Policy setting mode. In Admin Flow/Policy, packet condition to be applied to Admin Flow/Policy and packet processing method to handle the packets that meet the conditions are to be set.

Packet classification conditions will be set in admin flow, and user can do the setting by the various conditions of IP address, ICMP, TCP, UDP etc.

To classify packets by the basis of IP addresses, use the following command.

Command	Mode	Function
ip {*src-ip-address* ｜ *src-ip-address/m* ｜ **any**} {*dst-ip-address* ｜ *dst-ip-address/m* ｜ **any**}	Admin Flow	Set policy by Source IP address, Destination IP address.

ip {*src-ip-address* ｜ *src-ip-address/m* ｜ **any**} {*dst-ip-address* ｜ *dst-ip-address/m* ｜ **any**} <0-255>		Set policy by Source IP address, Destination IP address.
ip {*src-ip-address* ｜ *src-ip-address/m* ｜ **any**} {*dst-ip-address* ｜ *dst-ip-address/m* ｜ **any**} {**icmp** ｜ **tcp** ｜ **udp**}		Set policy by Source IP address, Destination IP address and protocol.
ip {*src-ip-address* ｜ *src-ip-address/m* ｜ **any**} {*dst-ip-address* ｜ *dst-ip-address/m* ｜ **any**} **icmp** {<0-255> ｜ **any**} {<0-255> ｜ **any**}		Set policy by Source IP address, Destination IP address and ICMP code value..
ip {*src-ip-address* ｜ *src-ip-address/m* ｜ **any**} {*dst-ip-address* ｜ *dst-ip-address/m* ｜ **any**} **tcp** {<1-65535> ｜ **any**} {<1-65535> ｜ **any**} [*tcp-flag* ｜ **any**]		Set policy by Source IP address, Destination IP address and TCP source and destination port.
ip {*src-ip-address* ｜ *src-ip-address/m* ｜ **any**} {*dst-ip-address* ｜ *dst-ip-address/m* ｜ **any**} **udp** {<1-65535> ｜ **any**} {<1-65535> ｜ **any**}		Set policy by Source IP address, Destination IP address and UDP source and destination port.
ip header-length <1-15>		Classify packets with specified length of IP header..

To classify packets by the basis of IPv6 addresses, use the following command.

Command	Mode	Function
ipv6 {*src-ip-address* ｜ *src-ip-address/m* ｜ **any**} {*dst-ip-address* ｜ *dst-ip-address/m* ｜ **any**}	Admin Flow	Set policy by Source IP address, Destination IP address..
ipv6 {*src-ip-address* ｜ *src-ip-address/m* ｜ **any**} {*dst-ip-address* ｜ *dst-ip-address/m* ｜ **any**} <0-255>		
ipv6 {*src-ip-address* ｜ *src-ip-address/m* ｜ **any**} {*dst-ip-address* ｜ *dst-ip-address/m* ｜ **any**} {**icmp** ｜ **tcp** ｜ **udp**}		Set policy by Source IP address, Destination IP address and protocol.
ipv6 {*src-ip-address* ｜ *src-ip-address/m* ｜ **any**} {*dst-ip-address* ｜ *dst-ip-address/m* ｜ **any**} **icmp** {<0-255> ｜ **any**} {<0-255> ｜ **any**}		Set policy by Source IP address, Destination IP address and ICMP code value..
ipv6 {*src-ip-address* ｜ *src-ip-address/m* ｜ **any**} {*dst-ip-address* ｜ *dst-ip-address/m* ｜ **any**} **tcp** {<1-65535> ｜ **any**} {<1-65535> ｜ **any**} [*tcp-flag* ｜ **any**]		Set policy by Source IP address, Destination IP address and TCP source and destination port.
ipv6 {*src-ip-address* ｜ *src-ip-address/m* ｜ **any**} {*dst-ip-address* ｜ *dst-ip-address/m* ｜ **any**} **udp** {<1-65535> ｜ **any**} {<1-65535> ｜ **any**}		Set policy by Source IP address, Destination IP address and UDP source and destination port..

Reference

User can set various Policies to one Admin Flow.

On the other hand, to delete the packet classification condition which was set in the Admin Flow, use the following command in the Admin Flow setting mode.

Command	Mode	Function
no ip	Admin Flow	Delete the packet classification condition which was set in the Admin Flow.
No ipv6		
no ip header-length		

(2) Admin Flow Setting Save and Modification

Admin Flow setting about the packet classification criteria must be saved in the equipment by using the following command.

Command	Mode	Function
apply	Admin Flow	Save the Admin Flow setting in the equipment.

Reference

If user returns from Admin Flow setting mode to Global mode without saving the admin flow settings, the settings will be deleted.

On the other hand, to modify the contents of an existing Admin Flow, user must enter the Admin Flow setting mode by using the following command.

Command	Mode	Function
flow admin *flow-name* **modify**	Global	Enter into the specified Admin Flow setting mode.

Reference

After modifying the contents of Flow, the contents should be saved by using ‘apply’ command.

(3) Admin Class Setting

If the packets are classified with a number of conditions, it may require two or more Admin Flows. In this case, if several Admin Flows are bundled to an Admin Class, it is easy to manage and the setting is simple. To use several Admin

Flows bundled as an Admin Class, use the following command to set the class.

Command	Mode	Function
class admin *class-name* **flow** *flow-name* [*flow-name*] [*flow-name*]…	Global	Set Admin Class by bundling Admin Flows.

Meanwhile, to delete Admin Class setting, use the following command.

Command	Mode	Function
no class admin all	Global	Delete all Admin Class settings.
no class admin *class-name*		Delete specified Admin Class setting.
no class admin *class-name* **flow** *flow-name* [*flow-name*] [*flow-name*] …		Delete specified Flow from the Admin Class setting.

7.4.9 Admin Rule Operation Setting

After setup of Admin Flow and Admin Class for packet classifications, Admin Policy setting will be followed by selective configuration of Admin Flow, Admin Class or Admin Policer by the demand of user. Then, Admin rule will be operated.

(1) Admin Policy Setting

To set the Admin Policy, Admin Policy should be created and user should enter into the setting mode by using following command.

Command	Mode	Function
policy admin *policy-name* **create**	Global	Create Admin Policy with specified name and enter into the setting mode of it.

On the other hand, to delete the Admin Policy setting, use the following command.

Command	Mode	Function
no policy admin *policy-name*	Global	Delete the created Admin Policy setting.
no policy admin all		Delete all Admin Policy.

After creating the Admin Policy, the Flow or Class in which Admin Rule will be operated can be included in the Policy. The action setting is possible by each Policy.

To include specific Class or Flow in Admin Policy, use the following command:

Command	Mode	Function
include-class *class-name*	Admin Policy	Include specified Admin Class in the Admin Policy.

include-flow *flow-name*		Include specified Admin Flow in the Admin Policy.

Attention

The Admin Flow and Admin Class cannot be included in the Admin Policy at the same time.

To delete the included Flow or Class from the Admin Policy, use the following command.

Command	Mode	Function
no include-class	Admin Policy	Delete the Admin Class.
no include-flow		Delete the Admin Flow.

(2) Admin Policy Priority Setting

Admin Policy with high priority will be processed first. To set priority to the Admin Policy set by the user, use the following command.

Command	Mode	Function
Priority {**low** ∣ **medium** ∣ **high** ∣ **highest**}	Admin Policy	Set priority to the new Admin Policy.

Reference

All Admin Policy has priority setting as 'low' by default.

(3) Processing Action Setting of Admin Policy

If the criteria of packet to be applied to Admin Policy is set, user needs to set up how to process the packets that match with the criteria by using following command.

Command	Mode	Function
action match deny	Admin Policy	Deny the packets corresponding to the Admin Policy.
action match permit		Permit the packets corresponding to the Admin Policy.

To disable the above settings, use the following command.

Command	Mode	Function
no action match deny	Admin Policy	Disable the settings to deny/permit the packets corresponding to the Admin Policy.
no action match permit		

On the other hand, the followings are the commands to process the packets which are not corresponding to the Admin Policy.

Command	Mode	Function
action no-match deny	Admin Policy	Deny the packets not corresponding to the Admin Policy.
action no-match permit		Permit the packets not corresponding to the Admin Policy.

To disable the above settings, use the following command.

Command	Mode	Function
no action no-match deny **no action no-match permit**	Admin Policy	Disable the settings to deny/permit the packets not corresponding to the Admin Policy.

(4) Admin Policy Setting Save and Modification

After all settings of Admin Rules, user must save the Admin Rule to the equipment by using the following command.

Command	Mode	Function
apply	Admin Policy	Save the settings of Admin Policy to apply it to the equipment.

Reference

If user returns from Admin Policy setting mode to Global mode without saving the admin policy settings, the settings will be deleted.

On the other hand, to modify the contents of an existing Admin Policy, user must enter into the Admin Policy setting mode by using the following command.

Command	Mode	Function
policy admin *policy-name* **modify**	Global	Enter into the specified Admin Policy setting mode to modify.

Reference

After modifying the content of the Admin Policy, user must save the contents using ‘apply’ command.

7.4.10 Admin Rule Setting Check

To check the Admin Rule Profile settings, use the following command.

Command	Mode	Function
show flow-profile admin	Admin Flow	Show the Admin Profile of the corresponding flow.
show policy-profile admin	Admin Policy	Show the Admin Profile of the corresponding policy.

To check the contents of the Admin Rule setting, use the following command.

Command	Mode	Function
show {**flow** | **class** | **policy**} **admin** [*name*]	View/Enable/ Global/Bridge	Check the contents of the Admin Rule setting.
show {**flow** | **class** | **policy**} **admin detail** [*name*]		
show running-config {**admin-flow | admin-policy**}	All	Check the detailed settings of Admin Flow or Admin Policy.

7.5 MAC Table management

In MAC table, two types of addresses will be registered. They are dynamic address and static address. Dynamic address is registered in MAC table by the equipment itself and will be deleted if it is not used. Static address is registered in MAC table by the user and will be remained in the table even when the equipment is rebooted. To register a static address in the MAC table, use the following command in Bridge setting mode.

Command	Mode	Function
mac *brdge-name port-number mac-address*	Bridge	Register MAC address, bridge name and port number.
show mac *brdge-name port-number*	Enable /Global/Bridge	Show the MAC addresses which was registered.

The following shows the registration of the MAC address in the MAC table.

```
MG205X (bridge)# mac default 1 00:01:02:9a:61:1a
MG205X (bridge)#
```

The following is an example that shows destination MAC address, port number, VLAN ID and time values registered in the MAC table.

```
MG205X (bridge)# show mac 1 1
==================================================================
port   mac addr           permission    status     in use
==================================================================
1      00:11:22:33:44:55    OK           static       0.00
```

```
1      00:10:5a:84:46:76    OK                          0.01
1      00:e0:4c:1a:37:17    OK                          0.07
 (omitted)
MG205X (bridge)#
```

To delete a static address from the MAC table, use the following command in Bridge setting mode.

Command	Mode	Function
no mac *brdge-name port-number mac-address*	Bridge	Delete the specified static address from the MAC table.

To reset the address registered in the MAC table, use the following command in Bridge setting mode.

Command	Mode	Function
clear mac *brdge-name port-number mac-address*	Enable/ Global/Bridge	Reset the specified MAC table.

7.6 ARP

Equipment connected to the IP network has LAN address and network address. Typically, LAN address is called as data link address because it is used in Layer 2, and also known as MAC address. To send packets when a MG205X is working through Ethernet, user needs to know the MAC address composed of 48 bits first. At this point, Address Resolution means the procedures of finding the MAC address that matches the IP address, and Reverse Address Resolution is procedures of finding the IP address from the MAC address which is contrary process. Then, the protocol used to find the MAC address that matches the IP address is ARP(Address Resolution Protocol).

ARP is using request packets and reply packets. Request packets are sent only to all nodes on the same Ethernet, and it is not transmitted by the Router. Reply packets are sent by nodes that received request packets to inform the MAC address. Whenever MAC address that matches the IP address is found, that information obtained through the ARP is managed by recording it on the ARP table, so that it can prevent repeated broadcasting of ARP request packets. However, the contents recorded on the table will be extinguished after a certain period of time for managing the ARP table effectively.

MG205X has ARP settings as following chapters.

7.6.1 ARP Table Setting

The contents of the ARP table is automatically recorded when the matching MAC address to the IP address is found through ARP. Network administrators can also register the MAC address of a specific IP address directly on the ARP table for use it on the network.

To register matching IP address to a MAC address, use the following command in Global setting mode

Command	Mode	Function
arp *ip-address mac-address* [*interface-name*]	Global	Register a matching IP address to a MAC address on ARP table.

To delete the registered IP address and MAC address, or to remove all the contents of the ARP table, use the following command:

Command	Mode	Function
no arp	Global	Remove all MAC and IP address on the ARP table
no arp *ip-address* [*interface-name*]		Delete the registered IP address of the interface on the ARP table.
clear arp [*interface-name*]	Global/Bridge	Delete all contents of ARP table.

To check the ARP table registered in the device, use the following command:

Command	Mode	Function
show arp [*ip-address* | *interface-name*]	View / Enable / Global/Bridge	Show the registered information on ARP table.

7.6.2 ARP Inspection

ARP packets may trust all hosts on the network as it is used to find the MAC address by using the IP address. In this point, ARP has low security level, and it is easy to be used for the purpose of interfering with the communication network.

For example, consider a case which the host B has a MAC address that is associated with the IP address of the host A, and it transmits broadcast messages to all the hosts belonged to the broadcast domain. If the host C responded to the broadcast message of host B with the IP address of host A and its own MAC address, host B can use the MAC address of host C as the destination of the traffic to be forwarded to the host A.

ARP Inspection may block the ARP packet transmitted for the purpose of interference with the communication network, and it will increase the security level for the ARP packet. To block the ARP packet using the ARP inspection feature, user must activate this function first and set the policy for the ARP packets.

(1) ARP Inspection Activation

To activate ARP inspection to a specific VLAN, use the following command.

Command	Mode	Function

ip arp inspection vlan *vlan-name*	Global	Activate ARP inspection to specified VLAN.

To disable the ARP inspection setting to s specific VLAN, use the following command.

Command	Mode	Function
no ip arp inspection vlan *vlan-name*	Global	Disable the activated ARP inspection to specified VLAN.

Attention

ARP inspection activation cannot block ARP packets properly. Be sure to use the ARP ACL filtering function to block ARP packets. It is described in the next chapter.

Reference

In general, it refers to the static ARP inspection table. However, if DHCP snooping is operating, ARP inspection can refer to DHCP snooping binding table and add the IP address registered in the corresponding table in the ARP entry table.

(2) ARP ACL Setting

In order to block the ARP packet using the ARP inspection function, user must create an ARP ACL (ARP Access List). Through the ARP ACL settings, user can set the policy for blocking specific range of IP address or for permitting the users with static IP. To set an ARP ACL, user must create an ARP ACL first and set a policy for the ARP packet in ARP ACL setting mode.

To enter into the ARP ACL setting mode, use the following command.

Command	Mode	Function
arp access-list *arp-acl-name*	Global	Create ARP ACL, and enter into the ARP ACL setting mode.
no arp access-list *arp-acl-name*		Delete the settings of the named ARP ACL.

Reference

ARP ACL is set to block all IP addresses and MAC addresses by default.

When an ARP ACL is created, system prompt is changed from MG205X (config)# to MG205X (config-arp-acl[arp-acl-name]) which is in ARP ACL setting mode. In the ARP ACL settings mode, user can set a range of IP addresses to apply the ARP inspection.

To block the ARP packets for specific IP address range, use the following command.

Command	Mode	Function
deny ip any mac { **any** | **host** *mac-address* }	Arp-acl	Block ARP packets for all MAC address or specified host MAC address.
deny ip any mac pattern *pattern* **offset** <0-5>		Block ARP packets for all MAC pattern.
deny ip host *ip-address* **mac** { **any** | **host** *mac-address* }		Block ARP packets for specified host IP address or IP and MAC address of specified host.
deny ip host *ip-address* **mac pattern** *pattern* **offset** <0-5>		Block ARP packets for specified host IP address and specified MAC pattern.
deny ip *A.B.C.D/M* **mac** { **any** | **host** *mac-address* }		Block ARP packets for specified subnet IP address / or specified subnet IP and host MAC address.
deny ip *A.B.C.D/M* **mac pattern** *pattern* **offset** <0-5>		Block ARP packets for specified subnet IP address and specified MAC pattern.
deny ip range *start-ip-address* *end-ip-address* **mac any**		Block ARP packets for the specified range of IP address.

To disable the setting to block the ARP packet, use the following command.

Command	Mode	Function
no deny ip any mac { **any** | **host** *mac-address* }	Arp-acl	Disable the ARP packet settings for the specified ranges.
no deny ip host *ip-address* **mac** { **any** | **host** *mac-address* }		
no deny ip *A.B.C.D/M* **mac** { **any** | **host** *mac-address* }		
no deny ip range *start-ip-address* *end-ip-address* **mac any**		
no deny ip any mac pattern *pattern* **offset** <0-5>		
no deny ip host *ip-address* **mac pattern** *pattern* **offset** <0-5>		
no deny ip *A.B.C.D/M* **mac pattern** *pattern* **offset** <0-5>		

In order to enable ARP packets for a specific IP address range, use the following command.

Command	Mode	Function
permit ip any mac { **any** | **host** *mac-address* }	Arp-acl	Allow(permit) ARP packet to all MAC address, or specified host MAC address.
permit ip any mac pattern *pattern* **offset** <0-5>		Allow(permit) ARP packet to all MAC pattern.

permit ip host *ip-address* **mac** { **any** | **host** *mac-address* }		Allow(permit) ARP packet to specified host IP address, or specified host IP address and MAC address.
permit ip host *ip-address* **mac pattern** *pattern* **offset** <0-5>		Allow(permit) ARP packet to specified host IP address and specified MAC pattern.
permit ip *A.B.C.D/M* **mac** { **any** | **host** *mac-address* }		Allow(permit) ARP packet to specified subnet IP address, or specified subnet IP address and host MAC address.
permit ip *A.B.C.D/M* **mac pattern** *pattern* **offset** <0-5>		Allow(permit) ARP packet to specified subnet address and mac pattern.
permit ip range *start-ip-address end-ip-address* **mac any**		Allow(permit) ARP packet to the ranged IP addresses.

Reference

After the setting of the ARP ACL, filtering setting must be followed to save the setting of ARP ACL.

To disable the setting to allow ARP packet, use the following command.

Command	Mode	Function
no permit ip any mac { **any** | **host** *mac-address* }	Arp-acl	Disable the setting to allow ARP packet for the specified IP address.
no permit ip host *ip-address* **mac** { **any** | **host** *mac-address* }		
no permit ip *A.B.C.D/M* **mac** { **any** | **host** *mac-address* }		
no permit ip range *start-ip-address end-ip-address* **mac any**		
no permit ip any mac pattern *pattern* **offset** <0-5>		
no permit ip host *ip-address* **mac pattern** *pattern* **offset** <0-5>		
no permit ip *A.B.C.D/M* **mac pattern** *pattern* **offset** <0-5>		

Attention

If user deletes the ARP ACL with filtering setting, the filtering will be removed at the same time.

On the other hand, DHCP Snooping function is used to set a limit for the fixed IP users to allow ARP packets. To allow ARP packet to the DHCP users, use the following command.

Command	Mode	Function
permit dhcp-snoop-inspection	Arp-acl	Allow(permit) ARP packet to the DHCP users.

no permit dhcp-snoop-inspection	Disable the settings to allow ARP packet to the DHCP users.

Reference

After the setting of the ARP ACL, filtering setting must be followed to save the setting of ARP ACL.

To disable all the settings of ARP ACL, use the following command.

Command	Mode	Function
arp access-list delete all	Global	Delete all ARP ACL settings.

(3) ARP Inspection Filtering Setting

MG205X has default setting to permit all MAC addresses by activated ARP Inspection function. Therefore, after user specifies ARP ACL of the IP address ranges to allow or block, this should be set to apply for the ARP packet blocking by ARP Inspection.

To enable ARP packet blocking function which is set by ARP ACL, use the following command.

Command	Mode	Function
ip arp inspection filter *arp-acl-name* **vlan** *vlan-name*	Global	Enable ARP packet blocking function.
no ip arp inspection filter *arp-acl-name* **vlan** *vlan-name*		Disable the ARP packet blocking function.

Reference

In MG205X, if ARP Inspection function is set, allows all MAC addresses as a default. Therefore, to block ARP packets, use the above command to apply the ARP ACL.

Reference

By disabling ARP ACL by above command, ARP filtering settings will be deleted at the same time.

(4) Port Status Setting

The port in ARP Inspection has trusted status and untrusted status. ARP packets received through the trusted port will pass directly without ARP inspection, but ARP packets received by untrusted port will pass only if it is appropriate from ARP inspection. Thus, generally, ports related with the subscribers are set to untrusted port and the ports connected to the upper level equipment are set to trusted port.

To set the status of a port in ARP Inspection, use the following command.

Command	Mode	Function
ip arp inspection trust port *port-number*	Global	Set the specified port to trusted port.
no ip arp inspection trust port *port-number*		Set the specified port to untrusted port.

To check the status of a port in ARP Inspection, use the following command.

Command	Mode	Function
show ip arp inspection trust	Enable/ Global/Bridge	Show the port status in ARP Inspection.
show ip arp inspection trust port *port-number*		

(5) ARP Address-validation Inspection Setting

ARP Address-validation inspection is a function that checks the validity of IP address and MAC address of the ARP packet to do following packet processing.

• If the MAC address of the ARP packet transmitter is not matching with the source MAC address of Ethernet header, the ARP packet will be dropped.

• If the target MAC address of the ARP reply packet is not matching with the destination MAC address of Ethernet header, the ARP reply packet will be dropped.

• IP address of the ARP packet transmitter or target IP address of ARP reply packet is '0.0.0.0' or '255.255.255.255' or multicast IP address, the ARP packet will be dropped.

To set ARP address-validation inspection, use the following command.

Command	Mode	Function
ip arp inspection validate {**src-mac** | **dst-mac** | **ip**}	Global	Set ARP address-validation inspection.
no ip arp inspection validate {**src-mac** | **dst-mac** | **ip**}		Disable the setting of ARP address-validation inspection.

Reference

The 'src-mac', 'dst-mac' and 'ip' options can be set as duplicated settings.

(6) Illegal Fixed IP User List Check

MG205X can check the list of subscribers using fixed IP illegally using a ‘Log-buffer function’. Log-buffer is the function that stores subscriber information that is blocked or disabled by the ARP inspection and generates syslog messages periodically.

Log-buffer function is automatically executed when the ARP Inspection is enabled, and if the received ARP packets are corresponding to ‘Deny’ or ‘Invalid’ ARP Inspection, the log-buffer function generates subscriber information entry by the dropped order and save it. The entry stored in the log-buffer contains information such as port number, VLAN ID, packet source IP address and the MAC address, packet number, dropped reason, receiving time etc. In addition, the user can specify the maximum number of entries to save.

Then, this stored information is sent as syslog message output periodically in saved order, and will be deleted from the log-buffer. If received ARP packets exceed specified maximum number of entries by the user, the exceeded packets are stored in a single entry, and the syslog message of this will be output as ‘Special Log Entry’ form at last.

On the other hand, if the same ARP packets are received from the subscriber stored in log-buffer earlier, only the packet number and received time will be changed while the stored entry order is not changed. And, if user changes the number of entry to a value smaller than the number of entries that are currently stored, stored entries on log buffer will be deleted by the saved order and syslog message will not be output.

To change the option values for log-buffer function, use the following command.

Command	Mode	Function
ip arp inspection log-buffer { **entries** <0-1024> | **logs** <0-1024>} **interval** <0-86400>	Global	Set the option values for log-buffer function.

Reference

The ‘entries’ is the maximum number of entries that can be stored in the log-buffer. It can be from 0 to 1024, and the default value is set as 32.

Reference

The ‘logs’ indicates the number of syslog messages to be output. It can be from 1 to 1024, and the default value is set as 5. If it is set as ‘0’, any syslog message will not have any output though the stored entries are remained in the log-buffer.

Reference

The ‘interval’ represents the time interval to output the syslog message. It can be from 0 to 86400 seconds, and the default is 1 second. If it is set to ‘0’, all saved entries in log-buffer and received new entries will be output as syslog messages immediately.

Reference

The syslog message output time is calculated as interval time divided by logs. (Syslog rate = interval / logs) However, the first syslog message output time is determined at random within syslog rate.

To disable the option settings of log-buffer function and return to the default, use the following command.

Command	Mode	Function
no ip arp inspection log-buffer {**entries** | **logs**}	Global	Disable the option settings of log-buffer function and return to the default.

To delete all entries stored in log-buffer, use the following command.

Command	Mode	Function
clear ip arp inspection log	Enable/Global/ Bridge	Delete all entries stored in log-buffer.

To check the settings of log buffer and the stored entry information, use the following command.

Command	Mode	Function
show ip arp inspection log	Enable/Global/ Bridge	Show the settings of log buffer and the stored entry information.

(7) Settings and Statistics Check

To check the setting of the ARP Inspection, use the following command:

Command	Mode	Function
show ip arp inspection	Enable/ Global/ Bridge	Show the settings of ARP Inspection.
show ip arp inspection vlan *vlan-name*		
show ip arp inspection statistics		Show the statistics of ARP Inspection.
show ip arp inspection statistics vlan *vlan-name*		

To reset the statistics of ARP Inspection, use the following command:

Command	Mode	Function

clear ip arp inspection statistics	Enable/ Global/Bridge	Reset the statistics of ARP Inspection.
clear ip arp inspection statistics vlan *vlan-name*		

7.6.3 ARP-Alias Setting

MG205X can do ASP reply though the IP address not registered in the equipment. If ARP-Alias is registered to the DSLAM in the access network which the communication between subscribers is set to be impossible to maintain the security of the subscribers, the ARP communication between subscribers is possible by the DSLAM and it looks as if communication is possible between subscribers.

(1) ARP-Alias Registration

To register ARP-Alias, use the following command.

Command	Mode	Function
arp alias *start-ip-address end-ip-address* [*mac-address*]	Global	Register ARP-Alias for ARP reply with specified IP address range and MAC address.
arp alias *start-ip-address end-ip-address* **vlan** *vlan-ID* **gateway** *gateway-ip-address*		Register ARP-Alias for ARP reply with specified IP address range, VLAN ID and gateway IP address.

Reference

If MAC address is not specified, the ARP will reply with the MAC address of the user's equipment.

To delete ARP-Alias setting, use the following command.

Command	Mode	Function
no arp alias *start-ip-address end-ip-address*	Global	Delete the address range setting of ARP-Alias.

To check the registered information of ARP-Alias setting, use the following command:

Command	Mode	Function
show arp alias	View/ Enable/ Global/Bridge	Show all the registered information of ARP-Alias setting.

(2) Aging Time Setting

MG205X using ARP-Alias for Tx and Rx of packets records ARP-Alias to prevent broadcasting whenever a packet is sent. From this record, unnecessary ARP-Alias are deleted if there is no response for the setting time which is called ‘aging time’.

To set the aging time, use the following command.

Command	Mode	Function
arp alias aging-time *time*	Global	Set aging time to delete unnecessary ARP-Alias from the record.

Reference

The ‘time’ can be set from 5 to 2,147,483,647 in seconds.

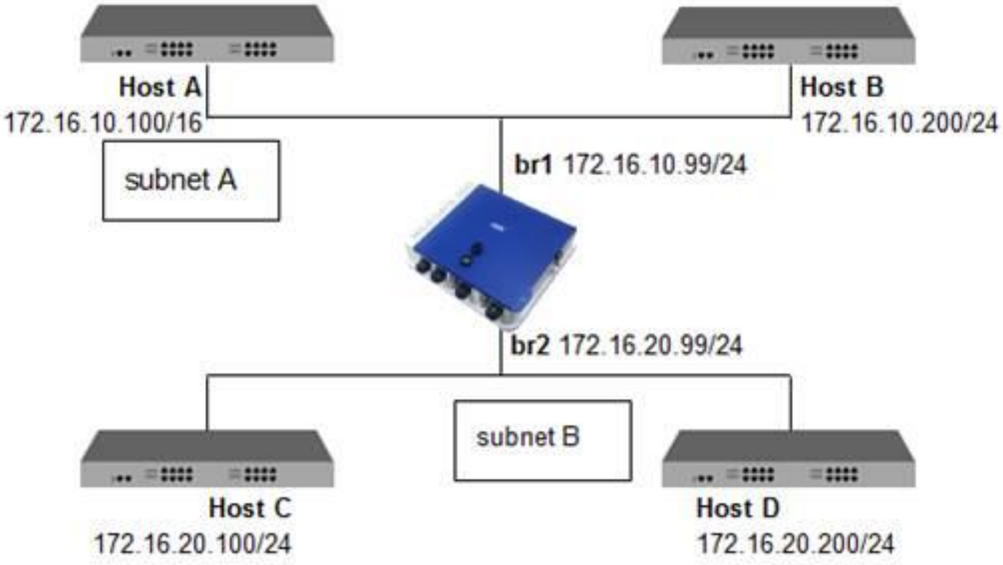
7.6.4 Proxy-ARP Setting

MG205X has the Proxy-ARP feature. Proxy-ARP is, simply, does reply to the ARP request for the other equipment. In the picture below, IP address of host A is set to 172.16.10.100 with subnet mask as /16. Host A think that it is connected to a network of 172.16.0.0.

If host A need to send a packet to host D, host A believes that host D will be on the same network and send ARP request to host D. ARP request is forwarded by broadcast, the ARP request of host A is sent only to the nodes that belong to the interface corresponding to the br1 of MG205X and the subnet A, and it not delivered to host D.

However, MG205X is aware that host D belongs to a different subnet, and it can send a packet to Host D. Therefore, MG205X replies to ARP request with its MAC address on behalf of host D.

In this way, the ARP request of subnet A to subnet B will be replied by MAC address of MG205X, and the packet transfer from host A to host D will be carried out safely through MG205X.



【Picture 7-12】Proxy-ARP

To set the Proxy-ARP, enter into the interface setting mode of the corresponding Interface and use the following command.

Command	Mode	Function
ip proxy-arp	Interface	Set the Proxy-ARP to the interface.

To disable the Proxy-ARP setting, use the following command:

Command	Mode	Function
no ip proxy-arp	Interface	Disable the Proxy-ARP setting.

[Setting Example 1]

The following is an example of setting the Proxy-ARP to br1.

```
MG205X # configure terminal
MG205X (config)# interface default
MG205X (config-if)# ip proxy-arp
MG205X (config-if)# show running-config
(syncopation)
interface default
 no shutdown
 ip proxy-arp
 ip address 172.16.209.50/16
ip route 0.0.0.0/0 172.16.1.254
no snmp
MG205X (config-if)#
```

7.6.5 Gratuitous ARP

MG205X ensures that the Gratuitous ARP including IP address and MAC address of the gateway is broadcasted, so that the communication continues even if IP address of the gateway is assigned as duplicated to a particular host on the network.

Use the following command to set the Gratuitous ARP transmission interval(interval) and transmission count(count) and. If you want to transfer the Gratuitous ARP after the ARP reply, set the transmission start time(delivery-start) as well.
After ARP is transmitted, Gratuitous ARP will be sent after the setup time.

Command	Mode	Function
arp patrol *interval count* {*delivery-start*}	Global	Set the Gratuitous ARP.
no arp patrol		Disable the Gratuitous ARP setting.
show running-config		Show the settings of Gratuitous ARP.

8. System Main Functions Setting

This chapter is about system main functions of MG205X including VLAN, port trunking, STP etc.

Followings are described;

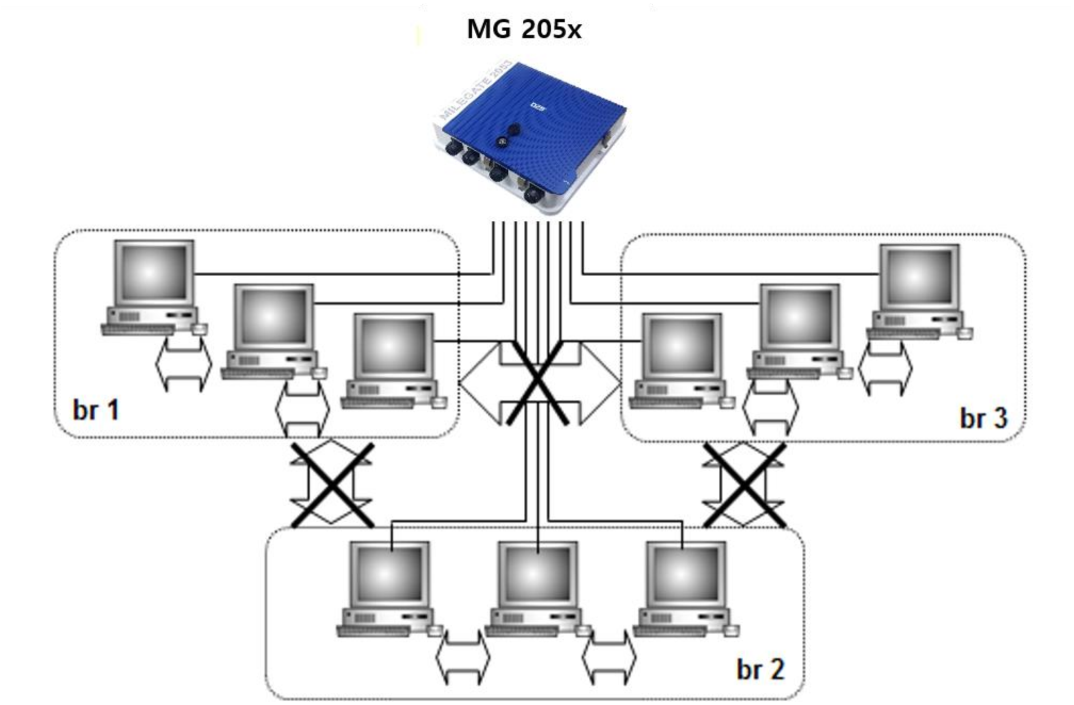
- Access List Setting
- VLAN (Virtual Local Area Network)
- Link Aggregation
- STP
- Loop Detection Function Setting
- Stacking Setting
- Rate Limit and Flood Guard
- DHCP (Dynamic Host Configuration Protocol)
- DHCPv6 (Dynamic Host Configuration Protocol for IPv6)
- Storm Control
- Jumbo-frame Setting
- Maximum Transmission Unit (MTU) Setting
- Bandwidth Value Setting

8.1 VLAN (Virtual Local Area Network)

Nodes belong to the same LAN can receive the same information if it is sent by broadcast function from a node. But, there is no choice in this broadcast function to receive it or not if it is not necessary information. At this time, when this LAN is configured by logical LAN, only the nodes in the same logical LAN will receive the information which was sent by the broadcast function.

This logically separated LAN is called as ‘VLAN’, namely virtual LAN. VLAN is a network logically divided according to the user's needs, and a VLAN contains multiple ports. Network configured with VLAN can send and receive packets each other only between the belonged ports unless routing function is there.

The following example shows a picture of VLAN configuration based on ports under Layer 2 environment.



【Picture 8-2】VLAN Configuration Based On Layer 2 Environment Port

In above picture, br1, br2 and br3 are logically configured VLAN in virtual network. When operating as a Layer 2 MG205X, the communication is possible in the virtual network, inter-communication between different virtual networks is not possible.

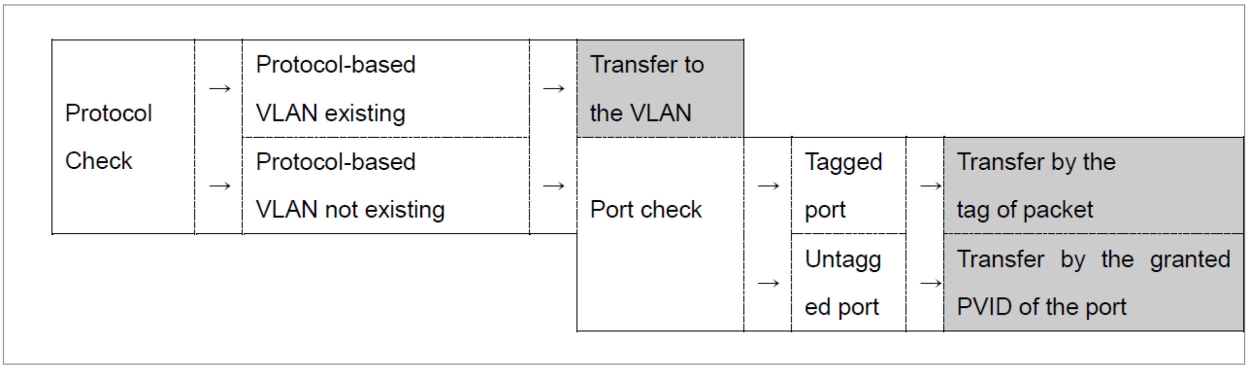
MG205X supports port-based VLAN and protocol-based VLAN. The total number of configurable VLAN in MG205X is 4096 pieces, and protocol-based VLAN can be maximum 8 pieces from them.

To decide the path of packet, protocol-based VLAN will be used first.

When a packet corresponding to the protocol of VLAN setting in MG205X is transferred, MG205X checks it and transfer to the related VLAN. However, when a packet which is not corresponding to the protocol of VLAN is transferred, MG205X will set a route based on the port-based VLAN.

MG205X follows the IEEE 802.1q standard, and it has own VLAN ID(PVID) which is set to all ports in the system. MG205X keeps its own PVID to the Incoming packets to tagged ports, and grants PVID of the system setting to the incoming packets to untagged Ports. For example, if port A of MG205X is set as untagged port, the PVID of port A will be granted to the incoming packet. So, MG205X ports configuring a VLAN network can send packets to the corresponding VALN by PVID.

Following method is to decide the path of packet based on VLAN set in MG205X.


Protocol Check
→
Protocol-based VLAN existing
→
Transfer to the VLAN
Protocol-based VLAN not existing
→
Port check
→
Tagged port
→
Transfer by the tag of packet
→
Untagged port
→
Transfer by the granted PVID of the port

【Picture 8-3】Determination Procedures of Packet Routing Based on VLAN

VLAN has the following characteristics.

◆ **Wide network bandwidth**

By eliminating unnecessary broadcast information to the other VLAN users, users can have wider network bandwidth than the case without VLAN.

◆ **Cost Reduction**

To separate the LAN to prevent the unwanted traffic load from the broadcast, there is no need to install each MG205X for the different network. Thus, VLAN helps cost-effective network configuration.

◆ **Enhanced Security**

In general MG205X equipments, all nodes share the broadcasted information, but some of them may need security. VLAN can enhance security by providing with VLAN configuration by only certified member.

In relation to the setting of the VLAN, it is described by the following order.

- Default VLAN
- Port-based VLAN Setting
- Protocol Based VLAN Setting
- MAC Address Based VLAN Setting
- Subnet Based VLAN Setting
- VLAN Priority(Precedence) Setting
- QinQ Setting
- Shared-VLAN Setting
- Protected Port Assignment
- VLAN Description Registration
- VLAN Translation Setting
- VLAN Settings Check
- Setting Example

8.1.1 Default VLAN

All ports of MG205X are set to Default VLAN. Default VLAN has PVID as ‘1’, and cannot be deleted. To include a new port in the newly created VLAN without overlap, user must delete the port from the Default VLAN. Deleted port from the other VLAN is automatically included in the Default VLAN. In addition, disabled port which was a member port of the trunk port will be automatically included in the Default VLAN.

The following is the case which port 3 is deleted from br2(VLAN2), the port 3 goes back to default VLAN.

```
MG205X (bridge)# vlan create 2
MG205X (bridge)# vlan del 1 3,4
MG205X (bridge)# vlan add 2 3,4 untagged
MG205X (bridge)# show vlan
                       u: untagged port, t: tagged port
      -----------------------------------------------------------------
                          |         1         2         3         4
         Name( VID| FID) |1234567890123456789012345678901234567890
      -----------------------------------------------------------------
       default(   1|   1) |uu..uuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu
          br2(   2|   2)  |..uu....................................
MG205X (bridge)# vlan del 2 3
MG205X (bridge)# show vlan
                       u: untagged port, t: tagged port
      -----------------------------------------------------------------
                          |         1         2         3         4
         Name( VID| FID) |1234567890123456789012345678901234567890
      -----------------------------------------------------------------
       default(   1|   1) |uuu.uuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu
          br2(   2|   2)  |...u....................................
```

8.1.2 Port-based VLAN Setting

To set up a port-based VLAN in MG205X, user needs to create a new VLAN first and specify a member, and user can assign the PVID.

(1) VLAN Creation

In MG205X, the VLAN is named as "brN (N = integer. "N" can be entered) when user creates a VLAN, where VID of each VLAN is automatically set to "N". In other words, VID of br2 is ‘2’, and VID of br100 is ‘100’. VLAN with VID 1 is defined as default VLAN. Thus, user can’t create a VLAN named as br1.

To create a new VLAN to set up a new VLAN in the network, use the following command.

Command	Mode	Function
vlan create *vlan-id*	Bridge	Create a new VLAN with the specified name.

Reference

The vlan-id can be entered is in the form of "brN (N = integer) or ‘N’. If user enters any other character other than this form, following message will be shown.

```
MG205X (bridge)# vlan create A
%invalid input parameter: A
MG205X (bridge)#
```

Reference

The vlan-id ‘N’ can be entered with a range using dash (-) or can be listed with comma (,). If it is "brN", the setting is to be one by one.

(2) PVID Setting

In MG205X, the N of vlan-id is used as VID automatically. For example, if the vlan-id is set to "br2" or "2", the VID is "2". On the other hand, PVID can also be set by the user temporarily.

To set the PVID on the port, use the following command.

Command	Mode	Function
vlan pvid *port-number* <1-4094>	Bridge	Set the PVID on the port. PVID setting range is <1~4094>.

(3) VLAN Port Assignment and Deletion

After user created a new VLAN, user must assign ports that are to be the VLAN members. In MG205X, all ports are integrated into the default interface, user must delete the ports from the "default" to assign them in other VLAN without overlapping.

To add/delete ports in VLAN, use following command.

Command	Mode	Function
vlan add *vlan-id port-number* {**tagged** | **untagged**}	Bridge	Add the port in the VLAN as tagged or untagged.
vlan del *vlan-id port-number*		Delete the port from the VLAN.

Reference

The port-number can be entered as multiple at one time. The multiple numbers can be entered with a range using dash (-) or can be listed with comma (,).

(4) VLAN Assigned Port Deletion

To delete a VLAN that is set in MG205X, user should delete the belonged ports first, and user can inactivate the interface to delete the VLAN.

Here's how to delete a VLAN that is set in MG205X.

Step 1. Delete all the ports belonged to the VLAN by using following command in Bridge setting mode.

Command	Mode	Function
vlan del *vlan-id port-number*	Bridge	Delete all the ports belonged to the VLAN.

Step 2. Enter into the interface mode of VLAN to be deleted from Global setting mode and deactivate the virtual interface.

Command	Mode	Function
interface *vlan-id*	Global	Enter into the interface mode of VLAN to be deleted.
shutdown	Interface	Deactivate the virtual interface.

Step 3. Delete the VLAN in Bridge mode by using following command:

Command	Mode	Function
no vlan *vlan-id*	Bridge	Delete the VLAN.

Attention

When you delete a VLAN, all ports belonged to the VLAN will be deactivated. These ports are maintained as inactive until they are assigned to a new VLAN.

8.1.3 Protocol Based VLAN Setting

When user set a protocol-based VLAN, user should specify port, protocol and PVID. Then, incoming packet to the specified port will be transferred to the VLAN with the specified PVID when the incoming packet is corresponding to the protocol that makes up the VLAN.

To set the protocol-based VLAN, use the following command:

Command	Mode	Function
vlan pvid *port-number* **ethertype** *ethertype* <1-4094>	Bridge	Set the protocol-based VLAN.

On the other hand, to disable the protocol-based VLAN, use the following command:

Command	Mode	Function
no vlan pvid *port-number* **ethertype** [*ethertype*]	Bridge	Disable the protocol-based VLAN.

8.1.4 MAC Address Based VLAN Setting

The MAC address-based VLAN is configured by the basis of MAC address entered by the user. To set the MAC address-based VLAN, use the following command.

Command	Mode	Function
vlan macbase *mac-address* <1-4094>	Bridge	Set MAC address based VLAN.
no vlan macbase [*mac-address*]		Delete MAC address based VLAN.
show vlan macbase	Enable / Global / Bridge	Show MAC address based VLAN.

8.1.5 Subnet Based VLAN Setting

Subnet based VLAN is configured by the basis of subnet entered by the user. To set the subnet-based VLAN, use the following command.

Command	Mode	Function
vlan subnet *ip-address/m* <1-4094>	Bridge	Set subnet based VLAN.
no vlan subnet [*ip-address/m*]		Delete subnet based VLAN.
show vlan subnet	Enable / Global / Bridge	Show subnet based VLAN.

8.1.6 VLAN Priority(Precedence) Setting

In MG205X, if the MAC address-based VLAN and Subnet-based VLAN are set at this same time, the user can specify the VLAN priority to be processed first by the system. To specify the VLAN priority, use the following command:

ommand	Mode	Function
vlan precedence {**mac** | **subnet**}	Bridge	Specify the VLAN priority to be processed first.

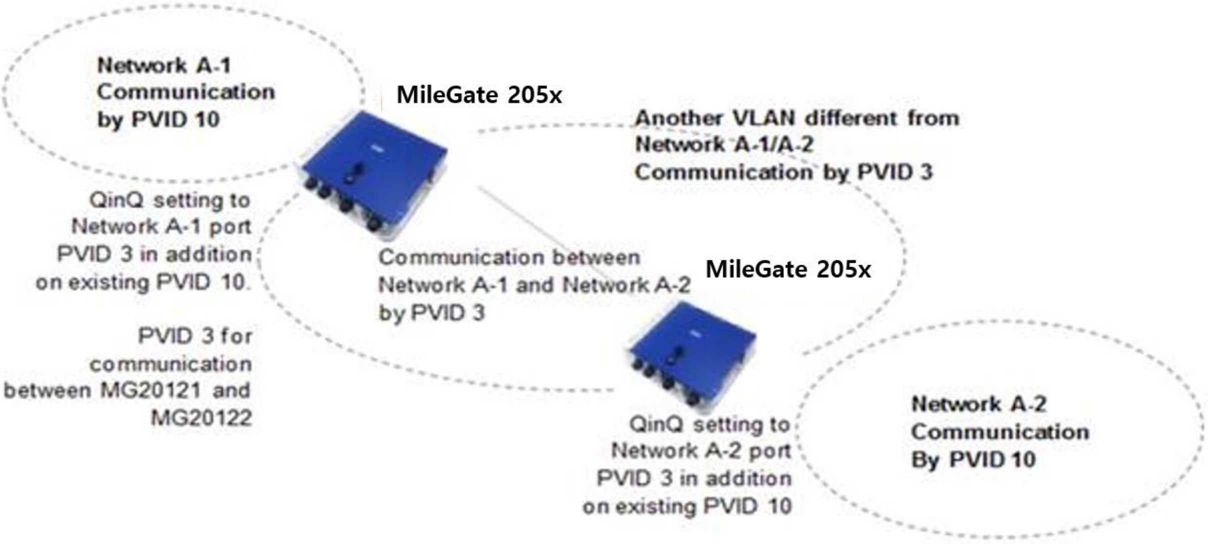
Reference

Default priority is set to MAC address-based VLAN first, and subnet address-based VLAN next to it.

8.1.7 QinQ Setting

QinQ is a function that enables inter-communication between several different VLAN in the network environment as one VLAN. Since tagging another tag to pass packets, it is also known as 'double Q-tag'. In conventional network environment, the equipments in different VLAN needed additional VLAN settings and more things to the media devices.

However, when using the QinQ function in MG205X, multiple VLAN can be set easily to one.



【Picture 8-4】An Example of QinQ Network Configuration

In the above picture, when Network A-1 sends packets to Network A-2, the packets are forwarded to the QinQ port of MG205X 1, then, it will be forwarded to Network A-2 through the QinQ port of MG205X 2.

At this time, if a packet is transferred from Network A-1 to MG205X 1, the outgoing packet through the QinQ port will have additional tag, and the tag will be used for the internal network with multiple VLAN. When this packet is transferred to the final destination Network A-2 through QinQ port, the packet will release the additional tag and arrive at the destination with its original tag.

Attention

Other ports than QinQ port should be set as 'tagged' to transfer the tagged packets.

(1) QinQ Setting On Port

To set the QinQ, set the port connected to a network with the other VLAN as QinQ port, and the port need to have PVID setting which is used to communicate with another VLAN. **【Picture 8-4】An Example of QinQ Network Configuration** has QinQ PVID 3.

Followings are QinQ setting procedures.

Step 1. Specify the port to be set as QinQ.

Command	Mode	Function
vlan dot1q-tunnel enable *port-number*	Bridge	Set QinQ to the specified port.

Reference

QinQ port does not work as a member of VLAN.

Step 2. Set the PVID to the QinQ port. The PVID should be the same one to communicate with the other VLAN.

Command	Mode	Function
vlan pvid *port-number* <1-4094>	Bridge	Set PVID on the QinQ port. PVID range is '1 to 4094'.

(2) TPID Setting

TPID (Tag Protocol Identifier) is a kind of tag protocol, that shows the protocol of tag which is used now. User can also change these TPID.

Reference

TPID is not operating basically to ports set to 802.1q(0x8100) as a member of the VLAN.

To set the TPID to QinQ port, use the following command:

Command	Mode	Function
vlan dot1q-tunnel tpid *tpid*	Bridge	Set the TPID to the QinQ port

(3) Double Tag Setting

To set the additional VLAN tag to tagged packet, use the following command

Command	Mode	Function
vlan tagging inbound *port-number* **vlan** *vlan-id1* **vlan** *vlan-id2*	Bridge	Set the additional VLAN tag(*vlan-id2*) to tagged packet(with *vlan-id1*).
no vlan tagging inbound *port-number* **vlan** *vlan-id*		Delete the added VLAN tag(*vlan-id2*) from tagged packet(with *vlan-id1*).

To delete the VLAN tag from the outgoing packets to a specific port, use the following command.

Command	Mode	Function
vlan tagging outbound *port-number* **vlan** *vlan-id*	Bridge	Delete the corresponding VLAN tag from the outgoing packet if the outer tag is VLAN ID.
no vlan tagging outbound *port-number* **vlan** *vlan-id*		Release the setting of VLAN tag deletion of outgoing packet.

To check the VLAN Double tag settings, use the following command.

Command	Mode	Function
show vlan tagging inbound [*port-number*]	Enable/ Global/ Bridge	Show the additional settings of VLAN tag on the port.
show vlan tagging outbound [*port-number*]		Show the settings of VLAN tag deletion.

(4) Inner Tag Setting

To set up VLAN inner tag to be applied to packets coming into the QinQ port, use the following command.

Command	Mode	Function
vlan dot1q-tunnel inner-tag *port-number* **pri** <0-7> **cfi** <0-1> **vlan-id** <0-4094>	Bridge	Set up VLAN inner tag to be applied to untagged packets coming into the QinQ port.
no vlan dot1q-tunnel inner-tag *port-number*		Delete the settings of inner tag.

To set up to apply the inner tag settings to a port, use the following command.

Command	Mode	Function
vlan dot1q-tunnel push inner-tag ingress-port *port-number*	Bridge	Set up to apply the inner tag settings to the incoming packets on the specified port.
no vlan dot1q-tunnel push inner-tag ingress-port [*port-number*]		Disable the settings to apply inner tag.

To set up to remove the inner tag for outgoing packets to a specified port, use the following command.

Command	Mode	Function
vlan dot1q-tunnel pop inner-tag egress-port *port-number*	Bridge	Set up to remove the inner tag for outgoing packets to a specified port.
no vlan dot1q-tunnel pop inner-tag egress-port [*port-number*]		Disable the settings of inner tag removal.

(5) S-VLAN Priority Setting

To set up the priority to be applied to packets with the S-VLAN tag incoming to a specified port, use the following command.

Command	Mode	Function
port priority *port-number* **cos** <0-7>	Bridge	Set up the COS priority to be applied to packets with the S-VLAN tag incoming to a specified port.
no port priority [*port-number*]		Disable the settings of S-VLAN prioroty.

To check the priority setting of S-VLAN Tag, use the following command.

Command	Mode	Function
show port priority [*port-number*]	Enable/Global/ Bridge	Show the priority setting of S-VLAN Tag.

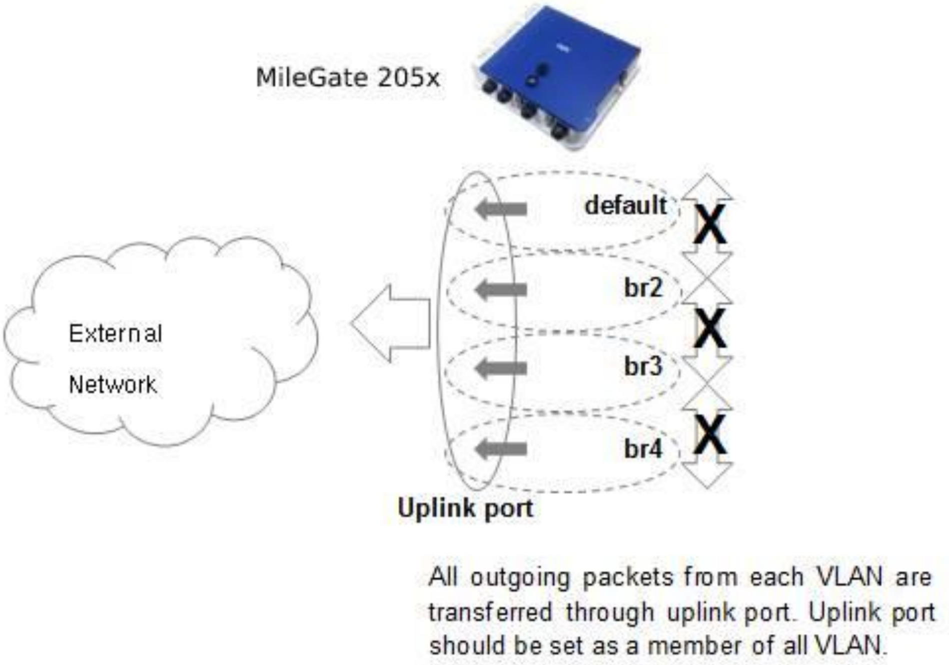
(6) QinQ ‘Disable’

To disable the setting to be a QinQ port on specified port, use the following command.

Command	Mode	Function
vlan dot1q-tunnel disable *port-number*	Bridge	Disable the setting to be a QinQ port on specified port.

8.1.8 Shared-VLAN Setting

```
MG205X (bridge)# show vlan
                                   u: untagged port, t: tagged port
             -----------------------------------------------------
                               |        1        2
                Name( VID| FID) |12345678901234567890123456789
             -----------------------------------------------------
              default(   1|   1) |uuuuuuuuuuuuuuuuuuuuuuuuuuuuuu
MG205X (bridge)#
```


MileGate 205x
default
br2
br3
br4
External Network
Uplink port
All outgoing packets from each VLAN are transferred through uplink port. Uplink port should be set as a member of all VLAN.

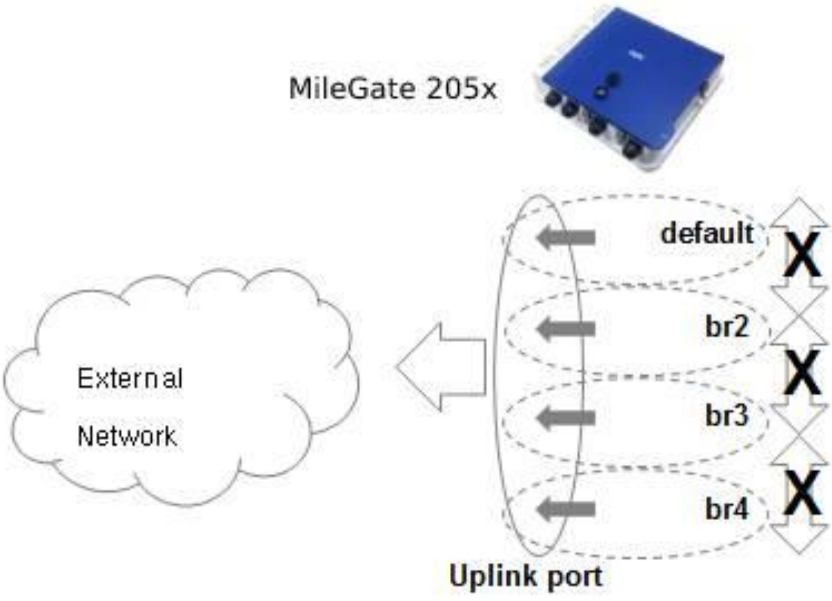
【Picture 8-5】Outgoing Packet Case Based on Layer 2 Environment

MG205X is a layer 2 MG205X without routing function, so inter-communication between VLANs is not possible. In particular, the port specified as Uplink port needs to receive packets from all VLAN, but the uplink port cannot receive packets if it is not set to be belonged to all VLANs. Therefore, when user set the VLAN in layer 2 MG205X equipments, the uplink port must be belonged to all VLANs as follows.

On the other hand, in above example of communication with untagged packet, if untagged packets are coming into port 1, it will be tagged with tag 1 because the PVID is 1, and the uplink port 24 can transfer in port 24 because it is belonged to VLAN 1, too.

But the problem is with the untagged packets entering through the uplink port. Untagged packets coming into the uplink port will not know where to be transferred with which PVID and to which port.

```
MG205X (bridge)# show vlan
                       u: untagged port, t: tagged port
       -----------------------------------------------------------------
                          |         1         2
          Name( VID| FID) |1234567890123456789012345678
       -----------------------------------------------------------------
      default(   1|   1) |u...uuuuuuuuuuuuuuuuuuuuuuuu
         br2(   2|   2)  |.u....................u.....
         br3(   3|   3)  |..u...................u.....
         br4(   4|   4)  |...u..................u.....
MG205X (bridge)#
```

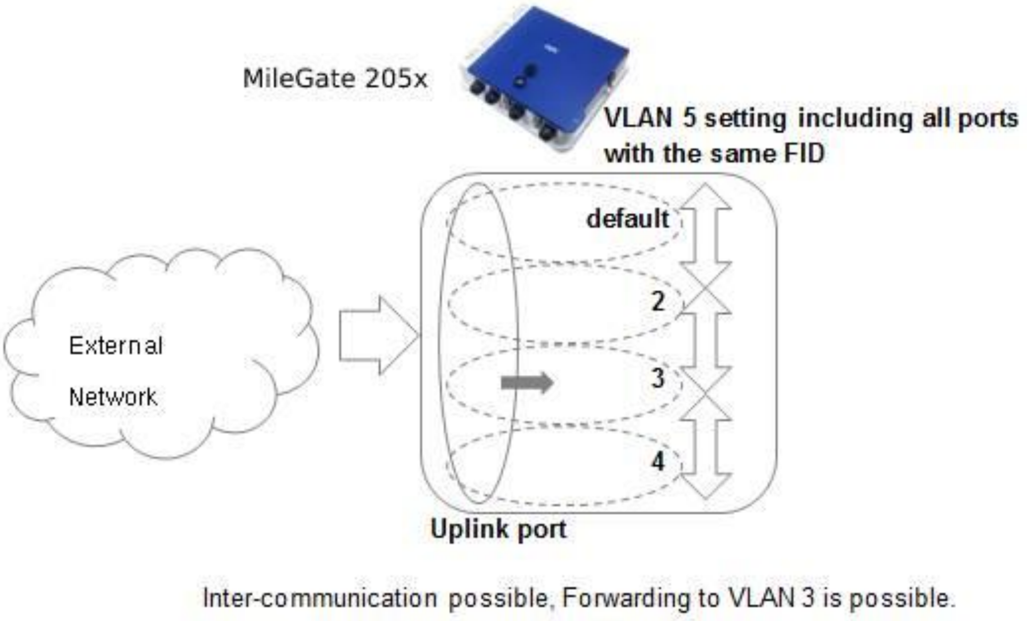


All outgoing packets from each VLAN are transferred through uplink port. Uplink port should be set as a member of all VLAN.

【Picture 8-6】Incoming External Packet Case Based On Layer 2 Environment ①

To be able to transfer the untagged packets came into an uplink port to another port, user has to create another VLAN in which all ports are included as members. Then, the uplink port will know the existence of all ports. At this point, FID packet is used to help packet transmission by using FID which is ID for managing MAC table. Because the same FIDs are managing the same MAC tables each other, it guides how to process the packets. If the FID setting is not the same, packet flooding will happen as the information of MAC table is not known.

```
MG205X (bridge)# show vlan
                       u: untagged port, t: tagged port
       ----------------------------------------------------------------
                          |         1         2
          Name( VID| FID) |1234567890123456789012345678
       ----------------------------------------------------------------
       default(   1|   5) |u...uuuuuuuuuuuuuuuuuuuuuuuu
           br2(   2|   5) |.u.....................u....
           br3(   3|   5) |..u....................u....
           br4(   4|   5) |...u...................u....
           br5(   5|   5) |uuuuuuuuuuuuuuuuuuuuuuuuuuuu
MG205X (bridge)#
```


MileGate 205x
VLAN 5 setting including all ports with the same FID
default
2
3
4
External Network
Uplink port
Inter-communication possible, Forwarding to VLAN 3 is possible.

【Picture 8-7】Incoming External Packet Case Based On Layer 2 Environment ②

Therefore, in layer 2 equipment, the uplink port should be belonged as a member to all VLAN, and the same FID should be set to do inter-communication between VLANs.

To set FID, use the following commands.

Command	Mode	Function
vlan fid *vlan-id FID value*	Bridge	Set specified FID of VLAN.

8.1.9 Protected Port Assignment

To do internet communication with guaranteed security on the same network, there is a way to have communication with only uplink port and to block the communication with the other ports. In MG205X, protected port is used to enable the internet communications with security by blocking packets coming from other ports except for uplink port. The port assigned to be protected port is set to be protected from all traffics, such as unicast, multicast, broadcast, etc. coming from other ports than the uplink port.

To set protected port, use the following command.

Command	Mode	Function
port protected *port-number*	Bridge	Set the specified port as protected port.

To disable the protected port setting, use the following command.

Command	Mode	Function
no port protected *port-number*	Bridge	Disable the setting of protected port.

To check the setting of protected port, use the following command.

Command	Mode	Function
show port protected	Enable/Global	Show the protected port.

8.1.10 VLAN Description Registration

In MG205X, description of each VLAN can be registered to use with ease as following.

Command	Mode	Function
vlan description *vlan-id description*	Bridge	Register the description of the VLAN.

To check the description of each VLAN registered, use the following command:

Command	Mode	Function
show vlan description	Enable /Global/Bridge	Show the description of the VLAN.

8.1.11 VLAN Translation Setting

VLAN Translation is simply an action of Rule. This function is to translate the value of specific VLAN ID which classified by Rule. The MG205X makes Tag adding PVID on Untagged packets, and use Tagged Packet as it is. That is, all packets are tagged in the MG205X, and VLAN Translation is to change the VLAN ID value of Tagged Packet in the MG205X. This function is to adjust traffic flow by changing the VLAN ID of packet.

Step 1 Open Rule Configuration mode using the flow NAME create command.

(※ Refer to 'making rule' of rule and QOS)

Step 2 Classify the packet that VLAN Translation will be applied by Rule.

(※ Refer to 'packet conditions' of rule and QoS')

Step 3 Designate the VLAN ID that will be changed in the first step by the match vlan <1-4094> command.

(※ Refer to 'rule operation setting' of rule and QoS.)

Step 4 Open Bridge Configuration mode using the bridge command.

Step 5 Add the classified packet to VLAN members of the VLAN ID to be changed to.

(※ Refer to 'VLAN setting method'.)

Sample Configuration

Sample Configuration 1: Configuring Port-based VLAN

The following is assigning br50, br3, and br4 to port 2, port 3, and port 4.

```
MG205X (bridge)# vlan create br50

MG205X (bridge)# vlan create br51

MG205X (bridge)# vlan create br200

MG205X (bridge)# vlan create br250

MG205X (bridge)# vlan create br500

MG205X (bridge)# vlan add br50 1-3 untagged

MG205X (bridge)# vlan add br51 4-6 untagged

MG205X (bridge)# vlan add br200 1-8 tagged

MG205X (bridge)# vlan add br250 1-8 tagged

MG205X (bridge)# vlan add br500 1-8 tagged

MG205X (bridge)# vlan pvid 1-3 50

MG205X (bridge)# vlan pvid 7-8 51

MG205X (bridge)# vlan pvid 1-1

MG205X (bridge)# show vlan

u:      untagged port,   t:      tagged   port

-----------------------------------

|       1

Name(   VID|    FID)    |12345678901234

-----------------------------------

default(1|      1)      |........uuuuuu

br50(   50|     50)     |uuuuuu........

br51(   51|     51)     |......uu......

br200(  200|    200)    |tttttttt......

br250(  250|    250)    |tttttttt......

br500(  500|    500)    |tttttttt......

MG205X (bridge)#
```

Sample Configuration 2: Deleting Port-based VLAN

The following is deleting br3 among configured VLAN.

```
MG205X (bridge)# vlan del br3 3

MG205X (bridge)# exit

MG205X (config)# interface br3

MG205X (interface)# shutdown

MG205X (interface)# exit

MG205X (config)# bridge
```

```
MG205X (bridge)# no vlan br3
MG205X (bridge)# show vlan
u: untagged port, t: tagged port
                    ------------------------------------
                     |         1
   Name( VID| FID)  |12345678901234
                    ------------------------------------
default( 1| 1)      |u...uuuuuuuu
    br2( 2| 2)      |.u.........
    br4( 4| 4)      |...u.......
MG205X (bridge)#
```

Sample Configuration 3: Configuring QinQ

Port 10 of MG205X 1 and port 11 of MG205X 2 are connected to the network where different VLANs are configured. To communicate without changing VLAN configuration of MG205X 1 and MG205X 2 which communicate with PVID 10, configure it as follows.

You should configure the ports connected to network communicating with PVID 11 as Tagged VLAN port.

```
< MG205X 1 >
MG205X (bridge)# vlan dot1q-tunnel enable 10
MG205X (bridge)# vlan pvid 10 11
MG205X (bridge)# show vlan dot1q-tunnel
Tag Protocol Id : 0x8100 (d: double-tagging port)
----------------------------------------------------
     |         1
Port |12345678901234
----------------------------------------------------
dtag  .........d..
MG205X (bridge)#

< MG205X 2 >
MG205X (bridge)# vlan dot1q-tunnel enable 11
MG205X (bridge)# vlan pvid 11 11
MG205X (bridge)# show vlan dot1q-tunnel
Tag Protocol Id : 0x8100 (d: double-tagging port)
----------------------------------------------------
     |         1
Port |12345678901234
```

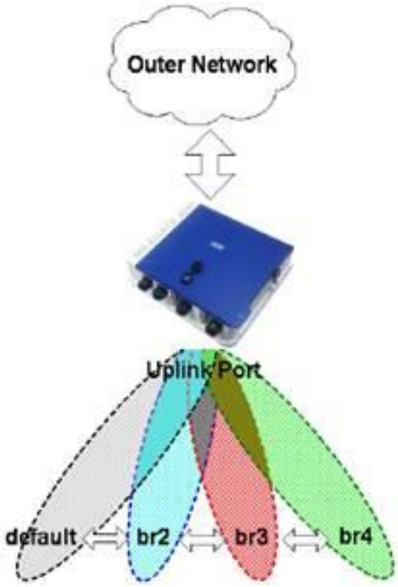
```
---------------------------------------------------

dtag ..........d.

MG205X (bridge)#
```

Sample Configuration 4: Configuring Shared VLAN with FID

Configure br2, br3, br4 in the MG205X configured Layer 2 environment and port 12 as Uplink port is configured. To transmit untagged packet through Uplink port rightly, follow below configuration.



```
MG205X (bridge)# vlan create br2

MG205X (bridge)# vlan create br3

MG205X (bridge)# vlan create br4

MG205X (bridge)# vlan del default 3-8

MG205X (bridge)# vlan add br2 3,4 untagged

MG205X (bridge)# vlan add br3 5,6 untagged

MG205X (bridge)# vlan add br4 7,8 untagged

MG205X (bridge)# vlan add br2 12 untagged

MG205X (bridge)# vlan add br3 12 untagged

MG205X (bridge)# vlan add br4 12 untagged

MG205X (bridge)# vlan create br5

MG205X (bridge)# vlan add br5 1-12 untagged

MG205X (bridge)# vlan fid 1-5 5

MG205X (bridge)# show vlan

u: untagged port, t: tagged port

----------------------------------------------------------------

                |         1

Name( VID| FID) |12345678901234
```

```
-----------------------------------------------------------------
default( 1| 5)  |uu......uuuu
    br2( 2| 5)  |..uu..u.....
    br3( 3| 5)  |....uu..u....
    br4( 4| 5)  |......uu..u..
    br5( 5| 5)  |uuuuuuuuuuuu
MG205X (bridge)#
```

Attention

In case of setting VLAN Translation of untagged port, set the same VLAN FID to be changed as the VLAN FID by using '**vlan fid** *vlan-id port-number*' command. Packet I'll be flooding and inter-communication between VLANs will be possible.

8.1.12 VLAN Settings Check

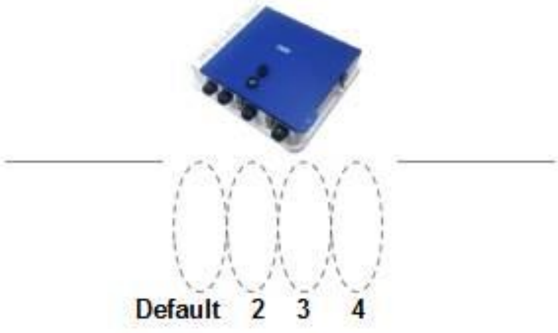
In MG205X, user can check each of the settings, such as port-based VLAN, protocol-based VLAN, MAC address based VLAN, Subnet address-based VLAN, QinQ, etc. by following commands.

Command	Mode	Function
show vlan	Enable / Global / Bridge	Check all the VLAN settings.
show vlan *vlan-id*		Check the settings of specified VLAN.
show vlan description		Check all the VLAN descriptions.
show vlan dot1q-tunnel		Check the QinQ setting.
show vlan protocol		Check the protocol based VLAN.
show port protected		Check the protected Port setting.

8.1.13 Setting Example

[Setting Example 1] Port-based VLAN settings

The following shows VLAN 2, 3, 4 created to assign as port 2, port 3 and port 4 respectively.



```
MG205X (bridge)# vlan create 2
MG205X (bridge)# vlan create 3
MG205X (bridge)# vlan create 4
MG205X (bridge)# vlan del 1 2,3,4
MG205X (bridge)# vlan add 2 2 untagged
MG205X (bridge)# vlan add 3 3 untagged
MG205X (bridge)# vlan add 4 4 untagged
MG205X (bridge)# vlan pvid 2 2
MG205X (bridge)# vlan pvid 3 3
MG205X (bridge)# vlan pvid 4 4


MG205X (bridge)# show vlan
                       u: untagged port, t: tagged port
       ----------------------------------------------------------------
                          |         1         2
          Name( VID| FID) |1234567890123456789012345678
       ----------------------------------------------------------------
        default(   1|   1) |u...uuuuuuuuuuuuuuuuuuuuuuuu
           br2(   2|   2)  |.u..........................
           br3(   3|   3)  |..u.........................
           br4(   4|   4)  |...u........................
MG205X (bridge)#
```

[Setting Example 2] Deletion of port-based VLAN

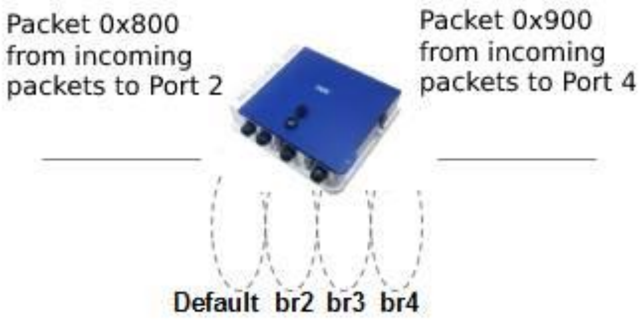
Among the above settings, VLAN 3 is deleted.

```
MG205X (bridge)# vlan del 3 3
MG205X (bridge)# exit
MG205X (config)# interface 3
MG205X (config-if)# shutdown
MG205X (config-if)# exit
MG205X (config)# bridge
MG205X (bridge)# no vlan 3
MG205X (bridge)# show vlan
                       u: untagged port, t: tagged port
       ----------------------------------------------------------------
                          |         1         2
          Name( VID| FID) |1234567890123456789012345678
```

```
              ------------------------------------------------------------------
               default(   1|   1) |u.u.uuuuuuuuuuuuuuuuuuuuuuuuu
                   br2(   2|   2) |.u..........................
                   br4(   4|   4) |...u.........................
       MG205X (bridge)#
```

[Setting Example 3] Protocol-based VLAN settings

The following is a case for setting the protocol-based VLAN on the port 2 and port 4 on above **[Setting Example 1]**.



```
       MG205X (bridge)# vlan pvid 2 ethertype 0x800 5
       MG205X (bridge)# vlan pvid 4 ethertype 0x900 6
       MG205X (bridge)# show vlan
                                u: untagged port, t: tagged port
              ------------------------------------------------------------
                                 |          1          2
                  Name( VID| FID) |1234567890123456789012345678
              ------------------------------------------------------------
                default(   1|   1) |u...uuuuuuuuuuuuuuuuuuuuuuuuu
                    br2(   2|   2) |.u..........................
                    br3(   3|   3) |..u..........................
                    br4(   4|   4) |...u.........................
       MG205X (bridge)# show vlan protocol
                ----------------------------------------------------------
                                |          1         2
                 Ethertype | VID |1234567890123456789012345678
                ----------------------------------------------------------
                      0x0800    5  .p..........................
                      0x0900    6  ...p.........................
       MG205X (bridge)#
```

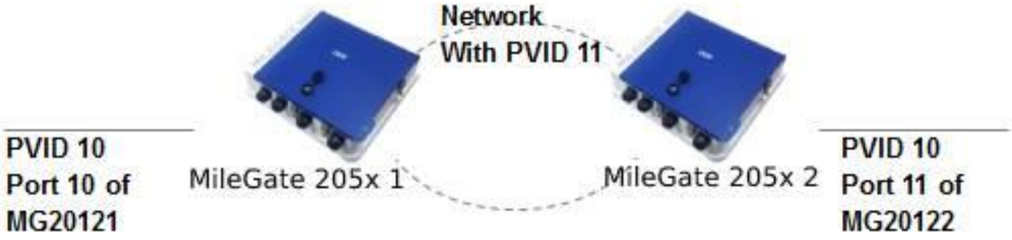
When it is set as above, the incoming packets through port 2 and port 4 will have its path by the type of protocol, and if the protocol is not matched, the path will be determined by the port-based VLAN.

[Setting Example 4] QinQ settings

Port 10 of MG205X 1 and port 11 of MG205X 2are connected to each network with different VLANs. Without changing VLAN settings, MG205X 1 and MG205X 2can communicate through PVID 10 by using QinQ as following.

Attention

Any ports communicating through PVID 11 of MG205X 1 and MG205X 2should be set as tagged VLAN port.



< MG205X 1 >

```
MG205X (bridge)# vlan dot1q-tunnel enable 10
MG205X (bridge)# vlan pvid 10 11
MG205X (bridge)# show vlan dot1q-tunnel
          Tag Protocol Id : 0x8100 (d: double-tagging port)
        -----------------------------------------------
               |         1         2
          Port |1234567890123456789012345678
        -----------------------------------------------
          dtag  .........d..................
MG205X (bridge)#
```

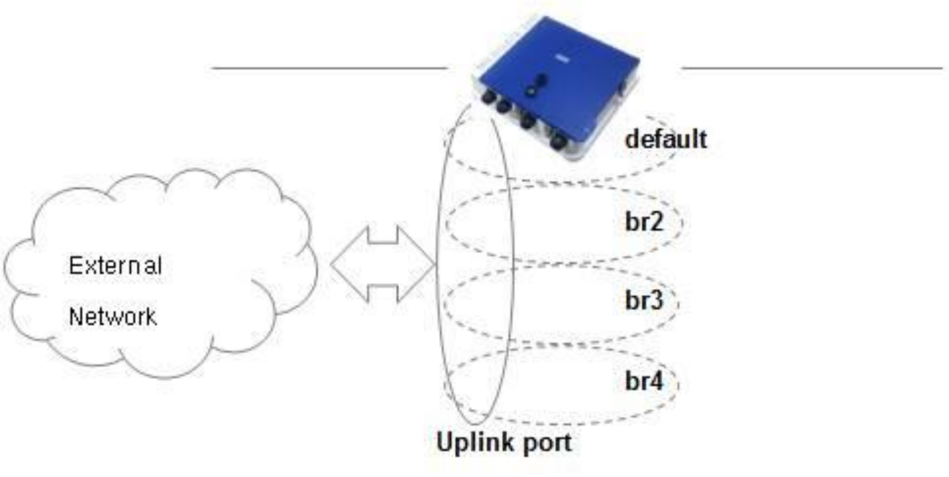
< MG205X 2>

```
MG205X (bridge)# vlan dot1q-tunnel enable 11
MG205X (bridge)# vlan pvid 11 11
MG205X (bridge)# show vlan dot1q-tunnel
          Tag Protocol Id : 0x8100 (d: double-tagging port)
        -----------------------------------------------
               |         1         2
          Port |1234567890123456789012345678
        -----------------------------------------------
          dtag  ..........d.................
MG205X (bridge)#
```

[Setting Example 5] Shared-VLAN settings using FID

After setting VLAN 2, 3 and 4 in MG205X, Uplink port 20 is set to be belonged to all VLAN.

To transfer untagged packets incoming through the uplink port properly, following setting should be done.



```
MG205X (bridge)# vlan create 2
MG205X (bridge)# vlan create 3
MG205X (bridge)# vlan create 4
MG205X (bridge)# vlan del 1 3-8
MG205X (bridge)# vlan add 2 3,4 untagged
MG205X (bridge)# vlan add 3 5,6 untagged
MG205X (bridge)# vlan add 4 7,8 untagged
MG205X (bridge)# vlan add 2 20 untagged
MG205X (bridge)# vlan add 3 20 untagged
MG205X (bridge)# vlan add 4 20 untagged
MG205X (bridge)# vlan create 5
MG205X (bridge)# vlan add 5 1-34 untagged
MG205X (bridge)# vlan fid 1-5 5
MG205X (bridge)# show vlan
                       u: untagged port, t: tagged port
       ------------------------------------------------------------
                         |         1         2
          Name( VID| FID) |1234567890123456789012345678
       ------------------------------------------------------------
        default(   1|   5)  |uu......uuuuuuuuuuuuuuuuuuuu
            br2(   2|   5)  |..uu...............u........
            br3(   3|   5)  |....uu.............u........
            br4(   4|   5)  |......uu...........u........
            br5(   5|   5)  |uuuuuuuuuuuuuuuuuuuuuuuuuuuuu
MG205X (bridge)#
```

8.2 Loop Detection Function Setting

8.2.1 Loop Detection Setting

MG205X can be set to transfer loop detection packet periodically to check if there is a loop from network status or cable connection though there is no dual path.

If the loop status is detected, it can prevent network problems by blocking the affected ports in accordance with the policies set by the user or by other ways. The port received loop detection packet will be recorded in the loop detection list and controlled.

(1) Loop Detection ‘Enable’

To activate the loop detection function in the MG205X, use following command.

Command	Mode	Function
loop-detect enable	Bridge	Activate loop detection function.
loop-detect disable		Disable loop detection function.

Reference

To activate the loop detection function, STP setting should be disabled first.

On the other hand, loop detection function can be activated on a specified port only. To activate the loop detection function to the selected port of MG205X, use the following command.

Command	Mode	Function
loop-detect *port-number*	Bridge	Activate the loop detection function to the port
no loop-detect *port-number*		Disable the loop detection function to the port

(2) Port Blocking Setting

To block the port where a loop is occurred, use following command.

Command	Mode	Function
loop-detect *port-number* **block**	Bridge	Block the port when a loop is occurred
no loop-detect *port-number* **block**		Disable the port blocking setting against loop.

Reference

When a loop is occurred, by default, MG205X is not blocking the port, but it leaves logs about the loop status.

(3) Loop Detection Packet Transmission Timeout Setting

Loop detection packets are transmitted with regular interval. User can set the transmission interval of loop detection packet.

To set the transmission timeout of loop detection packet, use following command.

Command	Mode	Function
loop-detect *port-number* **period** <1-60>	Bridge	Set the transmission timeout of loop detection packet.

Reference

By default, the interval of MG205X is set to 30 seconds by default.

(4) Loop Detection List Timer Setting

If a loop is generated, the corresponding port is registered in the loop detection list, and then, the port can be blocked by the policy of the user. After some time, the port will be out of the list for normal operation.

If the port is registered in the Loop Detection list, the timer is operating until the setting time to enable the blocked port by the loop. After the port is enabled again, it becomes an object to be detected by the loop detection function again. To set timer for loop detection, use following command.

Command	Mode	Function
loop-detect *port-number* **timer** <1-86400>	Bridge	Set the time of timer to exclude specified port from loop detection list and to unblock the port.
loop-detect *port-number* **timer** 0		Disable the timer setting on the port.

Reference

The timer is set to 600 seconds (10 minutes) by default.

On the other hand, if the loop is gone away, user can change the blocked port into unblocked port any time prior to the timer setting. Blocked port by loop detection can be unblocked by following command.

Command	Mode	Function
loop-detect *port-number* **unblock**	Bridge	Delete the port from the loop detection list and unblock the port.

(5) Loop Detection Packet Transmission Source- MAC Address Setting

In loop detection function of MG205X, user can set the source MAC address of periodic loop detection packet as system MAC address or LAA (Locally Administered Address).

LAA is a MAC address starting with 02 by setting the second bit of the first Byte as 1. For example, if a MAC address is 00:D0:cb:00:00:01, LAA is 02:D0:cb:00:00:01.

To set MAC address of loop detection packet, use following command.

Command	Mode	Function
loop-detect srcmac laa	Bridge	Set LAA MAC address as the source MAC address.
loop-detect srcmac system		Set system MAC address as the source MAC address.

Reference

By default in MG205X, system MAC address is set as the source MAC address of loop detection packet.

Reference

To change the source MAC address of loop detection packet, disable the loop detection function first by **'loop-detect disable' command.**

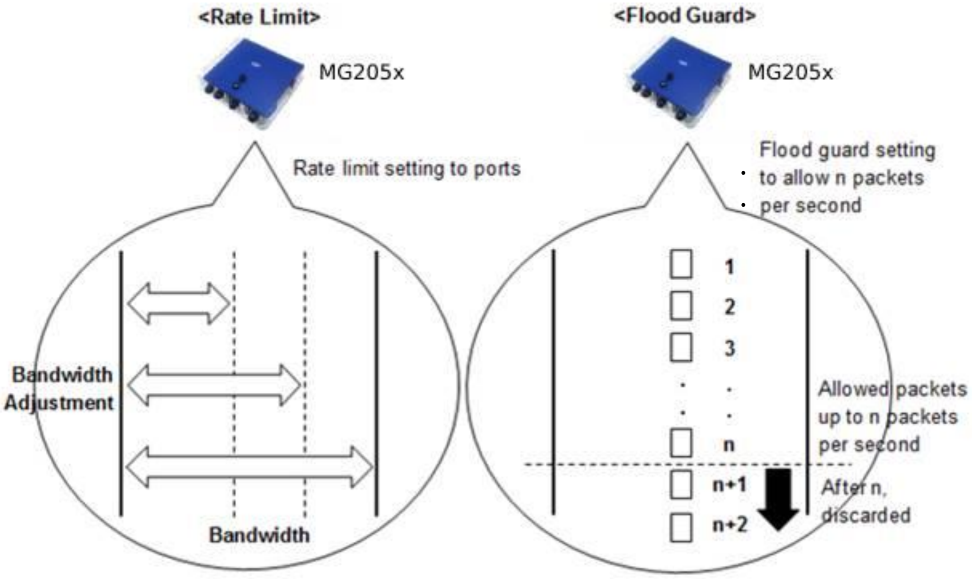
(6) Settings Check of Loop Detection

To check the loop detection settings, use following command.

Command	Mode	Function
show loop-detect	Enable/ Global/ Bridge	Show the settings of loop detection 'enable/disable'.
show loop-detect {*port-number* | **all**}		Show the settings of loop detection to the specified port or all ports.

8.3 Rate Limit and Flood Guard

Rate limit can set up the bandwidth of each port for efficient use, and it can be same or different for the Tx and Rx. Flood guard is to limit the number of packets to be forwarded within the bandwidth.


<Rate Limit>
MG205x
Rate limit setting to ports
Bandwidth Adjustment
Bandwidth
<Flood Guard>
MG205x
Flood guard setting to allow n packets per second
1
2
3
n
n+1
n+2
Allowed packets up to n packets per second
After n, discarded

【Picture 8-32】Rate Limit and Flood Guard

8.3.1 Rate Limit Setting

To set up the bandwidth of each port, use following command in Bridge mode. When user set up the rate limit to the bandwidth if ingress, user can set up the rate limit with flow-control function by the 802.3x descriptions. Ingress is a kind of received point, so it is a kind of upload from the point of connected PC.

Command	Mode	Function
rate-limit port *port-number* **rate** *rate* **egress**	Bridge	Set egress rate limit on the port.
rate-limit port *port-number* **rate** *rate* **ingress dot3x**		Set ingress rate limit on the port.

Reference

The '*rate'* can be entered by multiple of 64Kbps.

To cancel the rate limit setting, use following command.

Command	Mode	Function
no rate-limit port *port-number* **egress**	Bridge	Disable egress rate limit on the port.

no rate-limit port *port-number* **ingress dot3x**		Disable ingress rate limit on the port.

The rate limit can be operated with the bucket size setting. If the bucket size is small, it can affect the speed of uplink port. The bucket size of MG205X can be set up by user.

Command	Mode	Function
rate-limit port *port-number* **burst** <1-4> {**egress**|**ingress**}	Bridge	Set the bucket size of rate limit.

Command	Mode	Function
show rate-limit	Enable / Global / Bridge	Show the rate limit setting.

Reference

The bucket size can be 1(1 x 4Kbps), 2(2 x 4Kbps), 3(3 x 4Kbps) or 4(4 x 4Kbps).

The default is set to 2(2 x 4Kbps). If the bucket size is smaller than 2, it will affect the speed of 10G interface.

8.3.2 Settings Example

[Setting Example 1] Rate limit setting

Following is settings of port 1 with 64Mbps and port 2 with 128Mbps in MG205X.

```
MG205X (bridge)# rate-limit port 1 rate 64 egress
MG205X (bridge)# rate-limit port 2 rate 128 ingress dot3x
MG205X (bridge)# show rate-limit
 unit : kbps E : Enhanced
-------------------------------------------------------------------------------
-
 Port |   Ingress    |    Egress    | Port |   Ingress    |    Egress
-------------------------------------------+-----------------------------------
--
   1  |      N/A     |      64      |   2  |     128      |      N/A
   3  |      N/A     |     N/A      |   4  |     N/A      |      N/A
 (Syncopation)

MG205X (bridge)#
```

[Setting example 2] MAC Flood Guard setting

Following is to set port 1 with receiving packet limit of 600.

```
MG205X (bridge)# mac-flood-guard 1 600
MG205X (bridge)# show mac-flood-guard
---------------------------------
 Port Rate(fps) | Port Rate(fps)
----------------+----------------
```

```
  1    600     |   2  Unlimited
  3  Unlimited  |   4  Unlimited
  5  Unlimited  |   6  Unlimited
  7  Unlimited  |   8  Unlimited
  9  Unlimited  |  10  Unlimited
 11  Unlimited  |  12  Unlimited
 13  Unlimited  |  14  Unlimited
 (Syncopation)
MG205X (bridge)#
```

[Setting example 3] CPU Flood-guard setting

Following is the setting of port 1 with packet limit of 100, and set the timer with 100 seconds.

```
MG205X (bridge)# cpu-flood-guard enable
MG205X (bridge)# cpu-flood-guard 1 timer 100
MG205X (bridge)# show cpu-flood-guard
-----------------------------------------------------------------
 Port Rate(fps)   timer blocked | Port Rate(fps)   timer blocked
-----------------------------------------------------------------
   1  Unlimited    100    no   |   2  Unlimited     60    no
   3  Unlimited     60    no   |   4  Unlimited     60    no
   5  Unlimited     60    no   |   6  Unlimited     60    no
   7  Unlimited     60    no   |   8  Unlimited     60    no
   9  Unlimited     60    no   |  10  Unlimited     60    no
  11  Unlimited     60    no   |  12  Unlimited     60    no
  13  Unlimited     60    no   |  14  Unlimited     60    no
  15  Unlimited     60    no   |  16  Unlimited     60    no
  17  Unlimited     60    no   |  18  Unlimited     60    no
  19  Unlimited     60    no   |  20  Unlimited     60    no
  21  Unlimited     60    no   |  22  Unlimited     60    no
  (Syncopation)
MG205X (bridge)#
```

8.4 Storm Control

MG205X supports broadcast storm control to the broadcast packet. Broadcast storm refers to the phenomenon which massive broadcast packet is forwarded to the network and occupy the most of transmission capacity with network time-out. This may happen by the different versions of protocols.

For example, TCP/IP with mixed versions of 4.3 BSD and 4.2 BSD or mixture of Apple talk Phase I and Phase II can cause broadcast storm. Also, if the information of routing protocol which transfer packets periodically is acknowledged in wrong way by a system which is not supporting the protocol, broadcast storm may happen.

In MG205X, broadcast storm control sets the transmission rate of broadcast packet per second, and it throws away the exceeded packets of the limit which is set by the user. User can change the transmission rate of broadcast, and control the multicast storm and DLF (Destination Lookup Fail) storm in MG205X in addition.

Reference

MG205X is set not to operate storm control by default.

To set Storm Control by the packet types, use the following command.

Command	Mode	Function
storm-control {**broadcast** | **multicast** | **dlf**} *rate* [*port-number*]	Bridge	Set storm control by the specified packet type.
no storm-control {**broadcast** | **multicast** | **dlf**} *rate* [*port-number*]		Release the storm control setting.
show storm-control	Enable / Global / Bridge	Show the storm control setting.

Reference

The *'rate'* can be entered as <1 - 262,142> for FE ports and <1 - 2,097,150> for GE ports.

The port number can be multiple. Use comma (,) or dash (-).

8.5 Jumbo-frame Setting

Acceptable range of packet in Ethernet environment is from 64Byte up to 1,518Byte. Packets out of this range can't be accepted. But, MG205X can be set to accept Jumbo-frame which is bigger than 1,518Byte.

Command	Mode	Function
jumbo-frame *port-number* <1518-9216>	Bridge	Set to accept Jumbo-frame with the specified range on the specified port.

Reference

MG205X can accept the Jumbo-frame up to 9,216Byte.

Command	Mode	Function
no jumbo-frame *port-number*	Bridge	Release the Jumbo-frame setting on the port.

Command	Mode	Function

show jumbo-frame	Enable / Global / Bridge	Show the Jumbo-frame settings.

[Setting Example 1]

Following shows Jumbo-frame of 2500Byte on the ports from 5 up to 8.

```
MG205X # configure terminal
MG205X (config)# bridge
MG205X (bridge)# jumbo-frame 5-8 2500
MG205X (bridge)# show jumbo-frame
port  05 :   2500 / 1518 (current/default)
port  06 :   2500 / 1518 (current/default)
port  07 :   2500 / 1518 (current/default)
port  08 :   2500 / 1518 (current/default)
 (Omitted)
MG205X (bridge)#
```

8.6 Maximum Transmission Unit (MTU) Setting

In data link layer, there are several MTU (Maximum Transmission Unit), such as 1500 octet for Ethernet, 4353 octet for FDDI and 9180 octet for ATM. MTU can be set by following command.

Command	Mode	Function
mtu <68-1500>	Interface	Set MTU of the interface.
no mtu		Release the MTU setting.

8.7 Bandwidth Value Setting

Routing protocol is using bandwidth information to measure the routing distance efficiently. Use the following command to set the bandwidth of the interface.

Command	Mode	Function
bandwidth *bandwidth-value*	Interface	Set the bandwidth of the interface.
no bandwidth		Release the bandwidth setting.

Reference

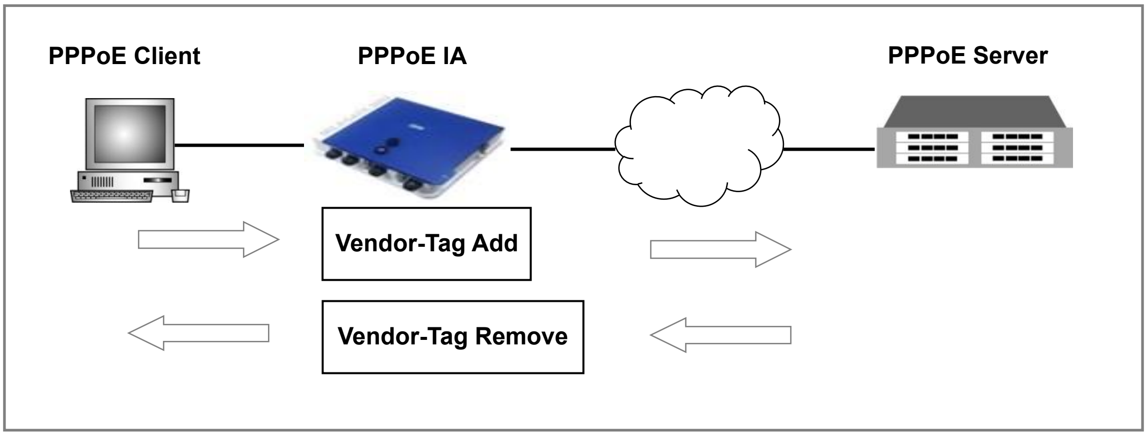
MG205X can set the bandwidth from 1 up to 10,000,000 Kbits on the interface.

Default setting is 1,000,000 Kbits.

8.8 PPPoE-IA Setting

The Point-to-Point Protocol over Ethernet (PPPoE) is a network protocol for encapsulating Point-to-Point Protocol (PPP) frames inside Ethernet frames to send PPP frame to PPP server. The PPPoE has two distinct stages. One is PPPoE discovery stage and the other is PPP session stage. PPPoE discovery stage is the process of connecting the client to the server and PPP session is the process of exchanging information necessary for PPP connection between the client and server and of determining authentication protocol. Point to Point Protocol over Ethernet Intermediate Agent (PPPoEIA) enables subscriber line identification over Ethernet during the PPPoE discovery phase.

The PPPoE IA tags PPPoE packet (PADI and PADR), received from the client during the PPPoE discovery process, with PPPoE tag (0x0105). PPPoE IA tag has information about circuit ID and remote ID. The circuit ID is composed of such fields as strings or IP, vlan ID, slot number and port number and the remote ID has a string field which can NULL



【Picture 8-36】 Examples configuration PPPoE

This chapter describes the following topics related to PPPoE IA configuration.

- PPPoE-IA enable Functionality
- PPPoE-IA Vendor-Tag Policy Settings
- PPPoE-IA Vendor-Tag Strip Settings
- PPPoE-IA Trust-port configuration
- PPPoE-IA enable packet dump feature
- PPPoE-IA view configuration information
- PPPoE-IA Circuit-ID Configuration
- PPPoE-IA Remote-ID Configuration
- PPPoE-IA View / initialize packet statistics

8.8.1 PPPoE-IA Enabling

To activate PPPoE-IA function, please use following command. After PPPoE-IA activation, snooping of PPPoE Discovery packet will be started.

Command	Mode	Function
pppoe-ia enable	Global	Enable PPPoE-IA function.
pppoe-ia disable		Disable PPPoE-IA function.

Reference

After activating PPPoE-IA function, PPPoE discovery packets incoming into all ports will be transferred to CPU. At this time, PPPoE-IA trust-port should be setup as all PPPoE discovery packets incoming into CPU will be thrown away if trust-port is not setup earlier.

8.8.2 PPPoE-IA Vendor Tag Policy Setting

PPPoE-IA provides vendor-tag to PPPoE discovery packets sent by client. At this time, several setup is possible to the packets which has vendor-tag.
Optional packet policy is as followings.

- **drop** : Throw away the packets which has vendor-tag.
- **keep** : Transmit the packet to the destination without vendor-tag change.
- **replace** : Replace existing vendor-tag with new one which is using user’s setting information, and transmit it to the destination.

Command	Mode	Function
pppoe-ia vendor-tag policy (drop | keep | replace)	Global	PPPoE-IA vendor-tag 정책을 설정합니다. (default: keep)

8.8.3 PPPoE-IA Vendor Tag Strip Setting

It is possible to remove the vendor-tag of PPPoE discovery packet which PPPoE Sever responded.

Following command is used to remove the subnet.

Command	Mode	Function

pppoe-ia vendor-tag strip (enable | disable)	Global	Setup PPPoE-IA vendor-tag strip setting as 'enable' or 'disable'. 'Enable' removes the vendor-tag of PPPoE discovery packet which PPPoE Sever responded. (default: disable).

8.8.4 PPPoE-IA Trust-port Setting

After activation of PPPoE-IA function, all ports are working as untrust-port. These ports interfaced to PPPoE server can be set to trust-port. If trust-port is not set under activated PPPoE-IA function, PPPoE packets incoming into CPU will be thrown away. So, after activation of PPPoE-IA function, trust-port setup is necessary.

Command	Mode	Function
pppoe-ia trust-port *PORTS*	Global	Designate the port interfaced to PPPoE Server as trust-port. (default: untrust-port)

8.8.5 PPPoE-IA Packet Dump Enabling

To do 'packet-dump' setting of incoming PPPoE discovery packets after PPPoE-IA activation, use following command.

Command	Mode	Function
pppoe-ia debug packet	Global	Activate PPPoE-IA packet-dump function.
no pppoe-ia debug packet		

8.8.6 PPPoE-IA Setting Information Check

To check out PPPoE-IA function setting, please use following command.

Command	Mode	Function
show pppoe-ia	Global	Show PPPoE-IA function settings.

```
MG205X (config)# show pppoe-ia
 ====================================
       PPPoE IA Configuration
 ====================================
  PPPoE-IA          : Enabled
  Vendor-tag Policy   : Keep
  Vendor-tag Strip    : Enabled
  Debug Packet       : Disabled

           u: untrust, t: trust
  -----------------------
            |         1
   Port     |123456789012
  -----------------------
   PPPoE IA |uuuuuuuutttt
```

8.8.7 PPPoE-IA Circuit-ID Setting

Circuit-ID, to be used as sub-option of PPPoE-IA Vendor-tag, can be designated per each port. If it is not designated, it works as ‘auto’. and remote-ID format under ‘auto’ mode is as following.

- ***%Hostname %Slot/%Port.%Vid***

Command	Mode	Function
pppoe-ia circuit-id *PORTS* **(auto | string** *LINE***)**	Global	Setup Circuit-ID of each port.
show pppoe-ia circuit-id		Show Circuit-ID.

```
MG205X (config)# pppoe-ia circuit-id 1 string HAN035Z208/E1
Slot:301,Port:1,VPI:1,VCI:32
MG205X (config)# pppoe-ia circuit-id 2 string HAN035Z208/E1
Slot:301,Port:2,VPI:1,VCI:32
MG205X (config)# show pppoe-ia circuit-id
 ------------------------------------
 Port      Circuit ID
 ------------------------------------
   1       HAN035Z208/E1 Slot:301,Port:1,VPI:1,VCI:32
   2       HAN035Z208/E1 Slot:301,Port:2,VPI:1,VCI:32
   3       [auto]MG205X 0/03:%VID
   4       [auto]MG205X 0/04:%VID
   5       [auto]MG205X 0/05:%VID
   6       [auto]MG205X 0/06:%VID
   7       [auto]MG205X 0/07:%VID
   8       [auto]MG205X 0/08:%VID
   9       [auto]MG205X 0/09:%VID
  10       [auto]MG205X 0/10:%VID
  11       [auto]MG205X 0/11:%VID
  12       [auto]MG205X 0/12:%VID
 ------------------------------------
```

8.8.8 PPPoE-IA Remote-ID Setting

Remote-ID, to be used as sub-option of PPPoE-IA Vendor-tag, can be designated per each port. If it is not designated, it works as 'auto'. and remote-ID format under 'auto' mode is as following.

- ***%SystemMAC***

Command	Mode	Function
pppoe-ia remote-id *PORTS* **(auto | string** *LINE***)**	Global	Set up remote-ID of each port.
show pppoe-ia remote-id		Show remote-ID.

```
MG205X (config)# pppoe-ia remote-id 1-8 string HAN035Z208/E1
MG205X (config)# show pppoe-ia remote-id
 ------------------------------------
 Port      Remote ID
 ------------------------------------
   1       HAN035Z208/E1
   2       HAN035Z208/E1
   3       HAN035Z208/E1
   4       HAN035Z208/E1
   5       HAN035Z208/E1
   6       HAN035Z208/E1
   7       HAN035Z208/E1
   8       HAN035Z208/E1
   9       [auto]00:d0:cb:00:00:00
  10       [auto]00:d0:cb:00:00:00
  11       [auto]00:d0:cb:00:00:00
  12       [auto]00:d0:cb:00:00:00
 ------------------------------------
```

8.8.9 PPPoE-IA Packet Statistics Check / Initialization

Use following command to check out PPPoE discovery packet statistics from PPPoE-IA function or to initialize the PPPoE-IA packet counter.

Command	Mode	Function
show pppoe-ia stats (*PORTS* |)	Global	Show PPPoE-IA packet statistics.
Clear pppoe-ia stats (*PORTS* |)		Initialize PPPoE-IA packet counter.

```
MG205X (config)# show pppoe-ia stats
 -------------------------------------------------------------------------
                Receive                                      Drop
      ------------------------------------------------  ----------------
 Port    All   PADI   PADO   PADR   PADS   PADT   Unkn    DR_REQ  DR_RES
 ----  ------------------------------------------------  ----------------
   1      0      0      0      0      0      0      0        0       0
   2      0      0      0      0      0      0      0        0       0
   3      0      0      0      0      0      0      0        0       0
   4      0      0      0      0      0      0      0        0       0
   5      0      0      0      0      0      0      0        0       0
   6      0      0      0      0      0      0      0        0       0
   7      0      0      0      0      0      0      0        0       0
   8      0      0      0      0      0      0      0        0       0
   9      0      0      0      0      0      0      0        0       0
  10      0      0      0      0      0      0      0        0       0
  11      0      0      0      0      0      0      0        0       0
  12      0      0      0      0      0      0      0        0       0
```

8.8.10 PPPoE-IA Client Information Check

To check out the PPPoE client information in the current interface, use following command.

Command	Mode	Function
show pppoe-ia client	Global	Show PPPoE Client information.

```
MG205X (config)# show pppoe-ia client
 ----------------------------------------------
 Port  vlan       MAC             IP
 ----------------------------------------------
 1    10     24:65:11:d0:49:74  77.76.230.209
 ----------------------------------------------
```

9. Multicast Setting

Multicast is a packet transmission scheme which transmit corresponding data to one or more specific receivers that requires a specific data. Multicast is similar to unicast in a viewpoint that the data is sent to specific receivers only, but the data is sent to multiple receivers by one time transmission in multicast while unicast is one-to-one transmission.

Because of these features, multicast minimizes the waste of network resources from repeated transmission work, and makes transmission to destination efficiently without wasting network bandwidth.

Multicast transmission scheme has two transmission methods : One is sending one source to multiple recipients, the other is sending multiple sources to multiple recipients.

The method of sending one source to multiple recipients is using PIM-SM or PIM-SSM, etc. is used. This transmission method provides services such as audio and video lectures, TV programs, radio, news headlines, weather updates etc.

The method of sending multiple sources to multiple recipients is using PIM-DM/SM, PIM-Bidir, CBT, etc. This transmission method is used for applications such as distance education, Internet video conferencing, internet computer games, etc. which senders and receivers exchange (give and take) data each other in real-time mode.

MG205X supports advanced IP multicast functions such as PIM-SM, PIM-SSM, IGMP v3, IGMP Snooping, MVR etc. for fast and efficient traffic transmission.

This chapter is consisted of the following contents:

- IGMP (Internet Group Management Protocol)
- Multicast Additional Function Setting

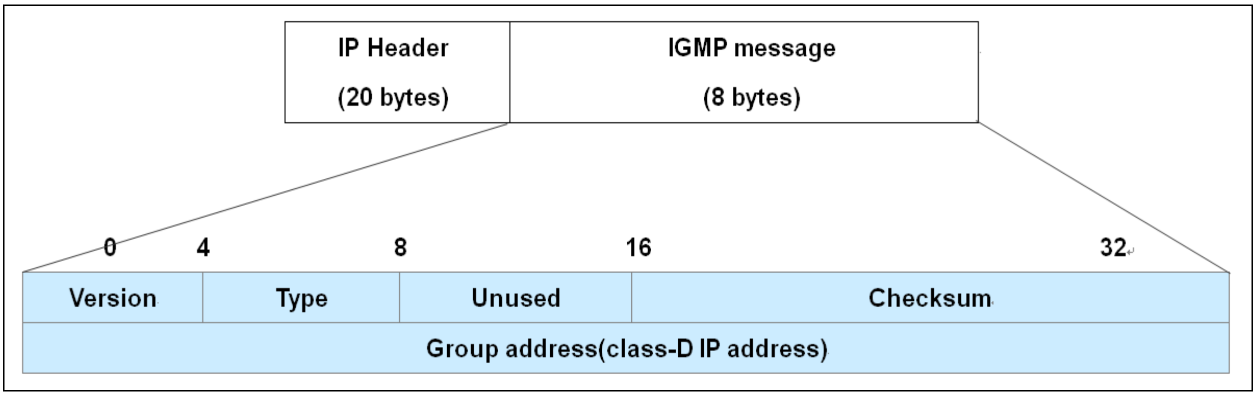
9.1 IGMP (Internet Group Management Protocol)

The important point of the multicast transmission method is multicast group management. Through this group membership, MG205X determines which host requests multicast packet to send traffic to the corresponding group only.

IGMP (Internet Group Management Protocol) is a multicast communication protocol, and when a host is joined in the multicast group, adjacent MG205X manages the group membership based on the information of the joined host.
Currently, IGMP is defined as version 1, version 2 and version 3, and IGMP messages of each version have two types as ‘query’ and ‘report’.

◆ IGMP version 1

The following figure shows IGMP version 1 message format with IGMP massage in the data sector of IP packet.



Version	Type	Unused	Checksum
Group address(class-D IP address)			

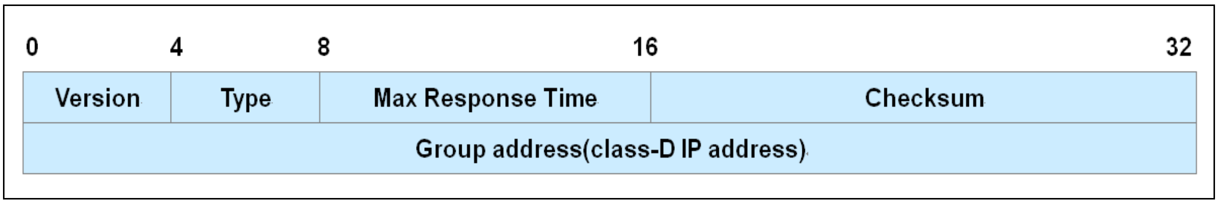
【Picture 9-1】Message Format of IGMP Version 1

In above figure, 'Version' indicates the version of IGMP. 'Type' indicates the type of messages which is either query type (membership query, 0x11) or report type (Membership Report, 0x12). Membership query is sent by multicast router, and membership report is by host joined to group. Group address is the multicast address to join, and it is '0' for query message transmission, and it is ignored for query reception. For the report message sent by host, multicast group address of responding host will be used.

◆ IGMP version 2

The difference between IGMP version 1 and IGMP version 2 is that the host transmit 'leave' message to router in IGMP version 2 when it goes out from multicast group. As an additional process, the multicast router which received a 'leave' message checks if there are other multicast group member on subnet before deleting the group membership. This function in IGMP version 2 makes it possible to reduce the waste of bandwidth by immediate recognition of time when a host leaves the group.

The following figure shows IGMP version 2 message format.



Version	Type	Max Response Time	Checksum
Group address(class-D IP address)			

【Picture 9-2】Message Format of IGMP Version 2

'Type' in the above figure can be either query message (sent by multicast router) or report message (sent by host). Query message has general query message and group-specific query message. General query message is the same as IGMP version 1. Group specific query message is sent by router to check whether other member is left in the specific group after receiving 'leave' message.

Max Response Time (MRT) means the maximum waiting time for a response to each query message, and the host receiving this message must respond within this time with IGMP version 2 Membership report message.

◆ **IGMP version 3**

IGMP version 3 is using the ‘Join’ to the multicast group member and ‘Leave’ from the group member in the same way as IGMP version 2, but it has different feature of Source filtering support.

Source filtering can be set to receive or exclude only the packets from a specific address. This source filtering setting prevents traffic flooding problem from known multicast source to enhance security. In IGMP version 3, group membership can be managed quickly and accurately as all the relevant information on ‘Join’ and ‘Leave’ of host is included in a single message.

In this chapter, following contents with respect to IP IGMP settings are described.

- IGMP Default Setting
- IGMP Version 2 Setting
- IGMP Version 3 Setting
- IGMP Settings Check

9.1.1 IGMP Default Setting

IGMP (Internet Group Management Protocol) manage and maintain the IGMP group membership table for managing the host registered in the multicast group. Host or MG205X will send a membership Join/Report message to an adjacent multicast router and request multicast traffic. Router which received this message sends multicast traffic to the corresponding port or group of hosts.

The ‘IGMP Querier’ is multicast router which sends a query message to the multicast group. Querier manage the host by sending a query message periodically to the host belonged to the multicast group and taking report message about the response where the host is belonged to. If there is no response to the query message for a period of time, the router will block the traffic transmission to the host.

The purpose is IGMP is that IGMP let the multicast router know the changed information of group members, The changed information means the information in multicast group that the ‘join’ and ‘leave’ of host are happened. Multicast router is using this information to manage the multicast membership table, and provides multicast communication services.
MG205X supports IGMP version 1, version 2 and version 3.

(1) IGMP Version Setting

MG205X is operating with IGMP version 3 by default, and the user can change it to other IGMP version if needed.

To change the ICMP interface version, use the following command:

Command	Mode	Function
ip igmp version <1 - 3>	Interface	Change the ICMP interface version.

After IGMP version setting, if user wants to change it back to default IGMP version 3, use the following command.

Command	Mode	Function
no ip igmp version	Interface	Disable the IGMP version setting, and change it back to IGMP version 4(default).

(2) QRV Setting

QRV (Querier's Robustness Variable) is supported in IGMP version 2 and version 3, and used to prevent a situation which response to query message is not received from instable network environment which packet loss is expected. This value is to be set to the query message, and the host should send response by the numbers of QRV value setting to the Query message. If even 1 response is arrived to the router, it is recognized as response of the host. If there is a considerable amount of packet loss in the network, user can set the QRV with high value to send response many times, and this will increase the possibility of packet reception.

Reference

The worse the network condition is, please set the greater QRV value. However, if the response to query message is repeated many times by high value of QRV, ‘leave latency’ will be increased.

To set the value of the QRV in MG205X use the following command.

Command	Mode	Function
ip igmp robustness-variable <2 - 7>	Interface	Set the value of the QRV.

Reference

QRV value in MG205X is set 2 times by default. QRV can be set from 2 times to 7 times.

To change the QRV value setting back to the default value, use the following command

Command	Mode	Function
no ip igmp robustness-variable	Interface	Delete the QRV value setting, and return to the default value.

(3) IGMP Entry Initialization ('Clear')

In MG205X, IGMP database can be initialized by following command. Initialization can be done by each interface or group IP or all database.

Command	Mode	Function
clear ip igmp	Enable	Initialize all IGMP entry database.
clear ip igmp interface *interface-name*		Initialize IGMP entry database of specified interface.
clear ip igmp group *		Initialize all IGMP group cache entry database.
clear ip igmp group *group-address* [*interface-name*]		Initialize IGMP entry database of specified IGMP group.

To reset the statistics of the IGMP packets transmitted and received on each interface, use the following command.

Command	Mode	Function
ip igmp clear-statistics	Interface	Reset the statistics of all IGMP entries.

9.1.2 IGMP Version 2 setting

The characteristics of IGMP version 2 includes IGMP Querier election and report suppression function etc. In addition, version 2 make it possible to minimize the processing time for the host to leave the group member using 'leave' and 'group-specific query' messages.

◈ IGMP version 2 messages

IGMP version 2 messages between host and router can be divided into three categories.

◊ Membership Query message

Query message is used by ICMP querier multicast router to check if a host is joined to group.

IGMP Version 2 query message has two types. One is 'general query' message which querier send to all of the host group to check if they are joined to group, the other is 'group-specific query' message which querier sends to the group to check if there are any other host which wants multicast traffic transmission after receipt of 'leave' message.

◊ Membership Report message

Membership report message has ‘join’ message and ‘report’ message. Join message is sent by the newly-joined host to request multicast packet. Report message is to be replied by the host within the response time limit (Max Response Time) after the receipt of query message from the IGMP querier.

◊ Leave a message

Leave message is sent by host to the multicast router when it leaves the multicast group.

(1) IGMP Static Join Setting

To set the IGMP Static Join function, use the following command:

Command	Mode	Function
ip igmp static-group *group-address* **vlan** *vlan-id* **port** *port-number* [**reporter** *reporter-ip-address*]	Global	Set the IGMP Static Join function to add a host to the port.

Reference

"group-address" of above command is the IP address of multicast group. "Reporter-ip-address" is the IP address of the virtual host.

To disable IGMP Static Join function, use the following command.

Command	Mode	Function
no ip igmp static-group [**vlan** *vlan-id*]	Global	Disable the IGMP Static Join settings.
no ip igmp static-group *group-address* [**vlan** *vlan-id*]		
no ip igmp static-group *group-address* **vlan** *vlan-id* [**port** *port-number*]		
no ip igmp static-group *group-address* **vlan** *vlan-id* **port** *port-number* [**reporter** *reporter-ip-address* | *]		

To specify the access-list to do the settings for IGMP Static Join function to the corresponding group in it, use the following command.

Command	Mode	Function
ip igmp static-group list {<1-99> | <1300-1999> | *access-list-name* } **vlan** *vlan-id* **port** *port-number* [**reporter** *reporter-ip-address*]	Global	Specify the access-list to do the settings for IGMP Static Join function to the corresponding group in it.

To specify the access-list to disable the IGMP Static Join function of the IGMP groups, use the following command:

Command	Mode	Function
no ip igmp static-group list {<1-99> | <1300-1999> | *access-list-name* } [**vlan** *vlan-id*]	Global	Disable the IGMP Static Join function of the IGMP groups in the access-list.
no ip igmp static-group list {<1-99> | <1300-1999> | *access-list-name* } **vlan** *vlan-id* **port** *port-number*		
no ip igmp static-group list {<1-99> | <1300-1999> | *access-list-name* } **vlan** *vlan-id* **port** *port-number* [**reporter** *reporter-ip-address* | *]		

To see the list of groups which have enabled IGMP Static Join setting, use the following command.

Command	Mode	Function
show ip igmp static-group	Enable / Global / Bridge	Show the list of groups which have enabled IGMP Static Join setting.
show ip igmp static-group list {<1-99> | <1300-1999> | *access-list-name* } [**vlan** *vlan-id*]		Show the list of groups in the access-list which have enabled IGMP Static Join setting.

Reference

The IGMP static join function is supported by only IGMP version 2 host, not by IGMP version 3 host.

(2) IGMP Static Group Setting

User can restrict the interface to the hosts of specified static group only. To manage the interface list of multicast group for each interface, use the following command.

Command	Mode	Function
ip igmp static-group *group-address*	Interface	Set the interface list of multicast group for each interface.
ip igmp static-group range *start-ip-address end-ip-address*		

To disable the access list of a multicast group settings, use the following command.

Command	Mode	Function
no ip igmp static-group *group-address*	Interface	Disable the access list of a multicast group settings of the interfaces.

no ip igmp static-group range *start-ip-address end-ip-address*	

(3) IGMP Querier Setting

IGMP Querier serves to send general query messages periodically to manage multicast group. In IGMP version 2, if there are two or more multicast routers on the same network, the router with the lowest IP address will be the IGMP querier after checking the querier messages.

IGMP Query message transmission interval setting

User can set the transmission interval of IGMP Query messages. To set the transmission cycle of the IGMP Query messages, use the following command.

Command	Mode	Function
ip igmp query-interval <1 - 18000>	Interface	Set the transmission interval of the IGMP Query messages.

Reference

The unit of the IGMP query message transmission interval is seconds, and default setting is 125 seconds.

To delete the IGMP query message transmission interval and return to the default settings, use the following command.

Command	Mode	Function
no ip igmp query-interval	Interface	Delete the IGMP query message transmission interval and return to the default settings.

IGMP Startup Query message transmission interval setting

If the MG205X is elected as IGMP Querier in specific IGMP interface, MG205X will send the general query messages to get the multicast membership information of that interface on a regular basis. User can set the transmission interval of IGMP startup query messages. MG205X sends general query messages as many times as the settings of QRV. To set the transmission interval of IGMP startup query messages, use the following command.

Command	Mode	Function
ip igmp startup-query-interval <1 - 18000>	Interface	Set the transmission interval of IGMP startup query messages.

Reference

The unit of the transmission interval of IGMP query message is seconds, and default setting is 32 seconds for IGMP Startup Query messages.

To delete the settings of IGMP startup query message transmission interval and return to the default setting, use the following command.

Command	Mode	Function
no ip igmp startup-query-interval	Interface	Delete the settings of IGMP startup query message transmission interval and return to the default setting.

IGMP Query response timeout settings

IGMP version 2 and version 3 has a time limit in response to the membership query messages, and this the 'Maximum Response Time (MRT)'. After receiving a query, host must transfer the report message within the maximum response time.

To specify maximum response time to the membership query messages, use the following command:

Command	Mode	Function
ip igmp query-max-response-time < 1 – 240 >	Interface	Set the maximum response time to the membership query messages.

Reference

The unit of the maximum response time is seconds, and user can specify it in a range from 1 to 240 seconds. The default is 10 seconds.

To delete the settings of maximum response time to the membership query message and return to the default setting, use the following command.

Command	Mode	Function
no ip igmp query-max-response-time	Interface	Delete the settings of maximum response time to the membership query message and return to the default setting

Re-election period setting IGMP Querier

If multiple multicast routers are operating as queriers, it can exacerbate the waste of network bandwidth as it is sending repeated query messages to all hosts. Therefore, the IGMP querier which sends query messages to the same network periodically should be existing as one.

As mentioned earlier, in the situation when two or more multicast routers exist, the router with the lowest IP address is elected as querier, and the other remaining routers check the query messages which are received periodically by starting to operate the queier with disabled timer from this time. If there is no more query message which is received from querier with the lowest IP address, following router with the next lowest IP address will be is a querier after expiry of the timer.

To set the time of the timer to operate immediately after receiving a query message with a lower IP address than its own, use the following command.

Command	Mode	Function
ip igmp querier-timeout < 60 – 300 >	Interface	Set the timeout period for querier re-election.

Reference

Timer operating cycle of querier re-election is specified in the range from 60 seconds to 300 seconds, and the default is 255 seconds.

To delete the timer setting for querier re-election and return to the default, use the following command.

Command	Mode	Function
no ip igmp querier-timeout	Interface	Delete the timer setting for querier re-election and return to the default.

Transmission Count and Interval settings of IGMP Last Member Query

If IGMP Querier receives a ‘leave’ message from the host, it sends group-specific query message (IGMP Version 2) or group-source-specific query message (IGMP version 3) up to the setting times to ensure whether other members are remaining in the corresponding group. If there is no response from any member after sending query messages up to the set number of times, querier is considering that there is no member and it does not send multicast traffic any more. However, due to the many variables, IGMP messages can be lost before arriving at the destination. To prevent from this case, user can set the number of cycles or period of sending query messages.

To set the number of transmitting group-specific and group-source-specific query messages, use the following command.

Command	Mode	Function
ip igmp last-member-query-count < 2 -7 >	Interface	Set the number of transmitting group-specific and group-source-specific query messages.

Reference

Number of transmitting group-specific and group-source-specific query messages can be specified in a range from 2 to 7, and the default setting is 2 times.

To delete the transmission count setting of group-specific and group-source-specific query messages and return to default setting, use the following command.

Command	Mode	Function
no ip igmp last-member-query-count	Interface	Delete the transmission count setting of group-specific and group-source-specific query messages and return to default setting.

To set the transmission time interval of group-specific and group-source-specific query messages, use the following command.

Command	Mode	Function
ip igmp last-member-query-interval < 1000 – 25500 >	Interface	Set the transmission time interval of group-specific and group-source-specific query messages.

Reference

The transmission time interval of group-specific and group-source-specific query messages is set by milliseconds, and the default values is 1000 milliseconds.

To delete the transmission time interval setting of group-specific and group-source-specific query messages and return to the default value, use the following command.

Command	Mode	Function
no ip igmp last-member-query- interval	Interface	Delete the transmission time interval setting of group-specific and group-source-specific query messages and return to the default value.

Transmission Interval setting of IGMP Unsolicited Report Message

IGMP version 2 Report messages are divided into two. Unsolicited report message is a join message that a new host request multicast packet when it is joined, and solicited report message is a message to be responded within the response limit time (Max Response Time) after receiving query message from the IGMP Querier.

If the membership information is changed while the IGMP proxy is set on the corresponding interface, the MG205X sends IGMP unsolicited report message to the higher level router or MG205X up to the QRV count setting.

To set the transmission interval of the IGMP unsolicited report message, use the following command.

Command	Mode	Function
ip igmp unsolicited-report-interval < 1 – 18000 >	Interface	It sets the transmission interval of the IGMP unsolicited report message.

Reference

Transmission interval of IGMP unsolicited report message is set by seconds, and default interval setting is 10 seconds.

To delete the transmission interval setting of IGMP unsolicited report message and return to the default setting, use the following command.

Command	Mode	Function
no ip igmp unsolicited-report-interval	Interface	Delete the transmission interval setting of IGMP unsolicited report message and return to the default setting.

(4) Immediate Leave Setting

Generally, if querier receive ‘leave’ message when the host wants to leave the multicast group, in IGMP version 2 and version 3, it is sending group-specific and group-source-specific query message to re-check if the host is left the multicast group or not.

In MG205X, when the ‘leave’ message is received from a specific multicast group, procedure of sending group-specific and group-source-specific query message can be set to skip. This is called ‘intermediate-leave’ setting which reduce the bandwidth waste between the time of ‘leave’ from group on the subnet and re-check time that the member is not in the group, and minimize the delay time.

To set IGMP immediate-leave function on the interface that will skip sending the group-specific and group-source-specific query message to the multicast group addresses of related access-list, use the following command in Interface setting mode.

Command	Mode	Function
ip igmp immediate-leave group-list {<1 - 99> I <1300 – 1999> I *access list number-ip*}	Interface	Set IGMP Immediate-Leave function.

To disable IGMP Immediate-Leave function, use the following command in Interface setting mode.

Command	Mode	Function
no ip igmp immediate-leave	Interface	Disable IGMP Immediate-Leave function.

Attention

Immediate-leave function is to be used in a network environment that one host is connected to the interface supporting IGMP version 2 and IGMP version 3. If two or more hosts are existing on the same interface, enabled immediate-leave function of the router will leave all the hosts in the group without any re-check if it receive leave message from a host.

9.1.3 IGMP Version 3 Setting

IGMP version 3 provides a filtering function which can receive multicast packets from group with a particular source address or exclude that group only.

Source filtering function is implemented through the IGMP version 3 Membership report message. IGMP version 3 membership report message includes various types of information, one is the record of the current status of the multicast group that the host is subscribed, and the other is the record on the membership changes. These two records are created based on the information of filter mode and source list. Also, user can recognize recently updated status efficiently by using a small amount of packets as the record of multiple multicast groups about a report message can be included in it.

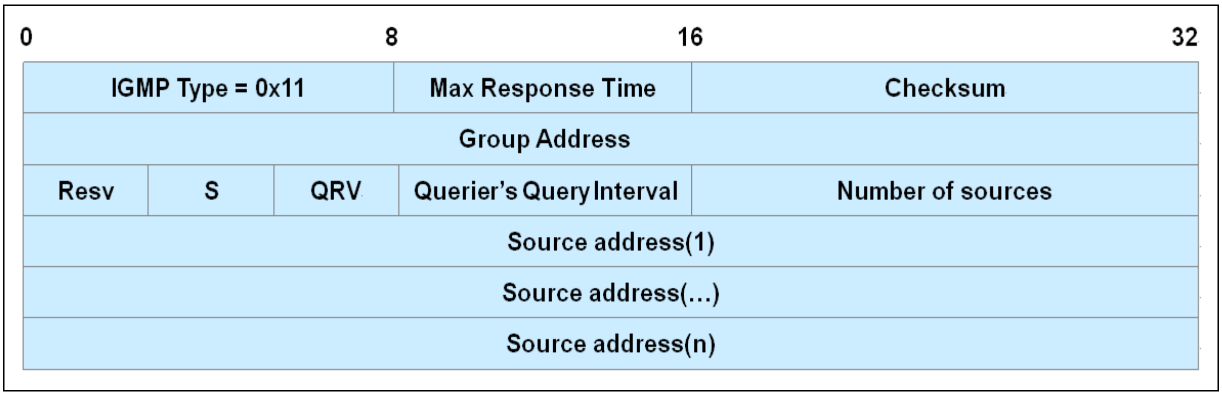
MG205X operates with IGMP version 3 by default and supports IGMP version 3 snooping function.

IGMP version 3 message

IGMP version 3 messages which are sent and received between hosts and multicast router have two types as follows:

- **Membership Query message**

Query message format of IGMP version 3 is shown in the following figure.



0			8	16	32
IGMP Type = 0x11			Max Response Time	Checksum	
Group Address					
Resv	S	QRV	Querier's Query Interval	Number of sources	
Source address(1)					
Source address(…)					
Source address(n)					

【Picture 9-3】Message Format of IGMP Version 3 Query

Multicast Router transfers membership query message to confirm whether host is belonged to the group or not.

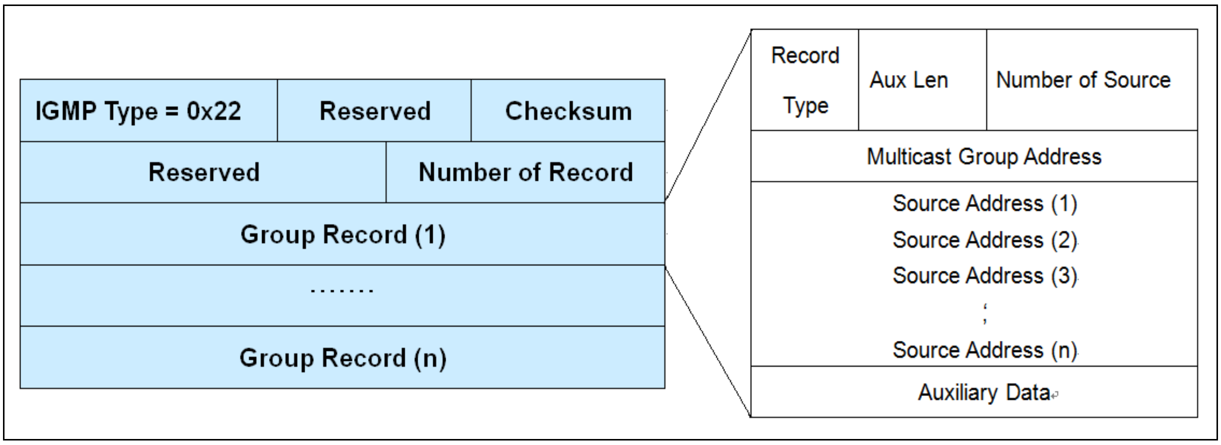
- General Query: Querier send message to the all hosts group periodically to check whether they are belonged to the group or not. This is the same as IGMP version 2 messages.

- Group-specific Query: After querier receives 'leave' message, it sends message to the corresponding group to check again if there is any other host which wants to transmit multicast traffic. This is the same as IGMP version 2 messages.

- Group-source-specific Query: After querier receives report message from the host in the multicast group with a specific source address, it sends message to the same source address to check again if the host is belonged to the group or not.

- **IGMP Version 3 Membership Report message**

Report message format of IGMP version 3 is shown in the following figure.



IGMP Type = 0x22	Reserved	Checksum
Reserved	Number of Record	
Group Record (1)		
…….		
Group Record (n)		

Record Type	Aux Len	Number of Source
Multicast Group Address		
Source Address (1) Source Address (2) Source Address (3) ; Source Address (n)		
Auxiliary Data		

【Picture 9-4】Message Format of IGMP Version 3 Report

IGMP version 3 Report message contains information about the membership status of belonged multicast group, changes, and corresponding interface. In addition, IGMP version 3 Report message contains recorded information such as the source address and the multicast group address of the multiple groups, it is called 'Group Record'. Based on this group record, router will determine if a host wants to join in the multicast group or if a host want to leave the multicast group. A report message may have a multiple group records, and each of the group record contains following information.

- Current-state: Record which the host received/excluded packets from specific multicast address. This includes changed information and checks the 'Join/Leave' status of the host.
- Filter-mode-change: This checks the recent changes in the include/exclude filter mode.
- Source-list-change: This checks the recent list of source multi-cast address with newly-added/removed information.

IGMP version 3 operating modes

IGMP version 3 operating modes manages 'Join/Leave' of multicast group members in a similar way of the IGMP version 2.

Without the procedure of sending leave message, IGMP version 3 report messages can permit or block the packets of specific source address by the information of the message. In other words, report message includes information from responses to query message, such as recent updates and changed information about Join/Leave of specific host to multicast group. Therefore, since a multicast router can recognize detailed information about the membership status of each host, there is no report suppression of IGMP version 2.

9.1.4 IGMP Settings Check

To check the contents of IGMP group-related settings in MG205X, use the following command:

Command	Mode	Function
show ip igmp interface	Enable/ Global/ Bridge	Show the IGMP settings on all the interface or on the named interface.
show ip igmp interface *interface-name*		

9.2 Multicast Additional Function Setting

MG205X supports IGMP Snooping, PIM Snooping and MVR for implementing very efficient and flexible multicast communication.

This chapter is consisted of the following:

- Multicast Forwarding Database Setting
- IGMP Version 2 Snooping IGMP Version 3 Snooping Setting
- IGMP Snooping Setting Information Check
- MVR (Multicast VLAN Registration)
- IGMP Flap Discredit Setting
- Static SSM Mapping Setting

- IGMP State Number Setting
- MRIB Debug

9.2.1 Multicast Forwarding Database Setting

MG205X is using multi-cast forwarding database (McFDB) information internally, to forward multicast traffic, and to maintains and manages multicast forwarding entry information collected by the various multicast protocols, such as IGMP and PIM.

And multicast forwarding database is operating in the same way of the operating principle of L2 FDB (Forwarding Database). If a particular multicast traffic is introduced into the port, the MG205X is comparing the received traffic entry information with the own multicast forwarding database. If the received information is the same as existing one in the database, it will be transferred to the specified port, and if there is no information in the existing database, the database will learn the information first and sent it to all ports. If an information is stored for a long period of time in database without any usage, the database will remove the entry information to allow other traffic forwarding.

(1) Unknown Multicast Traffic Blocking

Unknown multicast traffic is the traffic which was not learned and there is no information of this in McFDB. This is to be flooded to all ports if there is no restriction. User can set to block against flooding of unknown multicast traffic.

To block against flooding of unknown multicast traffic, use the following command.

Command	Mode	Function
ip unknown-multicast [port *port-number*] **block**	Global	Block the port against unknown multicast traffic.
ipv6 unknown-multicast [port port-number] block		

To disable the setting of blocking unknown multicast traffic, use the following command to allow flooding again.

Command	Mode	Function
no ip unknown-multicast [**port** *port-number*] **block**	Global	Allow the port to flood the unknown multicast traffic.

Attention

If a specific port is assigned as multicast router port, be careful not to block the unknown multicast traffic Flooding.

(2) Forwarding Entry Maximum Number Setting

If user does not use the multicast entry information recorded in the multicast forwarding database for a certain period of time, corresponding entry information will be removed to let the other traffic be forwarded. Due to the limited memory capacity of MG205X, this function makes a space to record new address.

To set the aging time or aging-limit of multicast forwarding database of MG205X, use the following command.

Command	Mode	Function
ip mcfdb aging-limit *aging-limit-value*	Global	Set the aging limit which limits the maximum number of McFDB forwarding entry.
ip mcfdb aging-time *aging-time-value*		Set the aging time which limits the maximum storing time of McFDB forwarding entry.

Reference

"Aging-limit-value" is set in the range of '256 to 65535' and the default value is 5000.

"Aging-time-value" is set by 10 seconds steps with the range of '10 to 10 million' seconds. The default value is 300 seconds.

To delete the setting of aging-time or aging-limit and return to the default, use the following command.

Command	Mode	Function
no ip mcfdb aging-limit	Global	Delete the setting of aging-limit.
no ip mcfdb aging-time		Delete the setting of aging-time.

(3) Multicast Forwarding Database 'Show' and 'Clear'

To check the settings of multicast forwarding entry or its recorded information in MG205X, use the following command.

Command	Mode	Function
show ip mcfdb	Enable/ Global/ Bridge	Show the settings for aging-time and aging-limit of multicast entry recorded in the system.
show ip mcfdb aging-entry {**vlan** *vlan-id* | **group** *group-address*} [**mac-based** | **detail**]		Show the information of L2 multicast forwarding entry by the specified options.
show ip mcfdb aging-entry [**mac-based** | **detail**]		

To reset the multicast forwarding entry information, use the following command:

Command	Mode	Function
clear ip mcfdb [***** | **vlan** *vlan-id*]	Enable/ Global	Delete to reset the multicast forwarding entry information of specified VLAN.

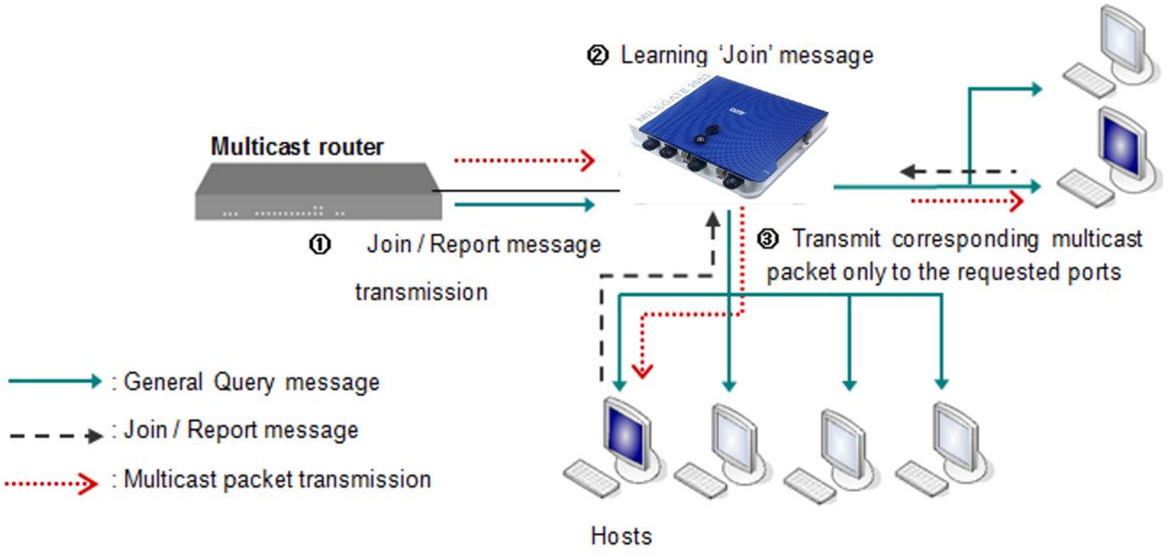
clear ip mcfdb vlan *vlan-id* **group** *group-ip-address* **source** *ip-address*	Delete to reset the specified multicast group information and multicast forwarding entry information of specified VLAN.

9.2.2 IGMP Snooping Default Setting

In general, L2 MG205X systems do packet flooding to all ports of broadcast domain when it receive multicast traffic. Because multicast address is not used for source address, MG205X systems can’t do learning multicast address normally. Therefore, it is not possible to check the entry information of corresponding traffic in MAC table which is L2 forwarding table. This traffic flooding of multicast abuses bandwidth.

IGMP snooping prevents flooding of multicast traffic in L2 network environment. If a MG205X has IGMP snooping activated, it is snooping the transmission route of packet which is sent and received between host and router and save the related information in the table. In addition, if a MG205X receives ‘join’ request message from a host of specific multicast group, the MG205X saves information, related to the ports which the host and corresponding multicast group is connected, in the forwarding table entry. and if a MG205X receives ‘leave’ message from the corresponding host, it deletes corresponding entry from the table.

MG205X is managing multicast forwarding table, and user can send packets efficiently only to the hosts which need multicast traffics. Following shows an example of multicast communication with IGMP snooping.


② Learning ‘Join’ message
Multicast router
① Join / Report message transmission
③ Transmit corresponding multicast packet only to the requested ports
: General Query message
: Join / Report message
: Multicast packet transmission
Hosts

【Picture 9-5】IGMP Snooping Setup Case

(1) IGMP Snooping Activation

ip igmp snooping	Global	Activate IGMP snooping function to the whole system.

ip igmp snooping vlan *vlan-id*		Activate IGMP snooping function to the specified VLAN.

Reference

In MG205X, IGMP Snooping is released by default.

Command	Mode	Function
no ip igmp snooping	Global	Release IGMP snooping function.
no ip igmp snooping vlan *vlan-id*		Release IGMP snooping function in specified VLAN.

Command	Mode	Function
show ip igmp snooping [**vlan** *vlan-id*]	Enable / Global / Bridge	Show the settings of IGMP snooping function.

(2) IGMP Snooping Version Setting

Report messages received by multicast router are transmitted with the IGMP version of each interface. User can set the IGMP snooping version of each interface manually, and then, report messages will be sent only to the corresponding version. MG205X is operating with IGMP snooping version 3.

If a MG205X operating with IGMP snooping version 3 receives IGMP version 1 Query message, it is operating with IGMP version 1 actively and sends IGMP version 1 report message to the corresponding router. If the MG205X is not receiving IGMP version 1 Query message continuously, after some time, the interface will be operating with IGMP snooping version 3 again. Manual setting of IGMP Snooping version can be done by following command.

Command	Mode	Function
ip igmp snooping version <1 – 3>	Global	Set the version of IGMP Snooping for the system.
ip igmp snooping vlan *vlan-id* **version** <1 – 3>		Set the version of IGMP Snooping for the specified VLAN.

Reference

In MG205X, the version of IGMP Snooping can be changed only to static version, and the default is set to IGMP snooping version 3.

Command	Mode	Function

no ip igmp snooping [**vlan** *vlan-id*] **version**	Global	Release the version setting of IGMP Snooping and return to IGMP Snooping version 3.

(3) Robustness Variable Setting

Robustness variable setting is used to prevent transmission failure of response to query under the environment which packet loss is expected from instable network status, such as link failure or abrupt bursty error. The variable is set to query message, and host sends report message numbered times of the robustness variable. If there are many packet losses in the network, user set the robustness variable with high value to send the report message many times, thus the ratio of packet receipt will be increased. But if the responses are increasing from the high value of robustness variable, leave latency will be increased, too.

Command	Mode	Function
ip igmp snooping robustness-variable <1 – 7>	Global	Set the values of robustness variable.
ip igmp snooping vlan *vlan-id* **robustness-variable** <1 – 7>		Set the value of robustness variable to the specified VLAN.

Reference

In MG205X, activated IGMP Snooping has a robustness variable of 2 times by default. This can be set from 2 to 7 times.

Command	Mode	Function
no ip igmp snooping robustness-variable	Global	Delete the setting value of robustness variable and return to the default.
no ip igmp snooping vlan *vlan-id* **robustness-variable**		

9.2.3 IGMP Version 2 Snooping Setting

(1) IGMP Snooping Querier Setting

When there is no IGMP querier on the network, IGMP Snooping Querier is operating for that. In addition, IGMP Snooping Querier supports IGMP Snooping function in specific VLAN without settings of PIM and IGMP.

In MG205X, if IGMP Snooping Querier is activated, likely to ICMP querier, it sends general query periodically to check which host wants to receive multicast traffic.

IGMP Snooping Querier activation

Command	Mode	Function
ip igmp snooping querier [**address** *source-address*]	Global	Activate IGMP Snooping Querier.
ip igmp snooping vlan *vlan-id* **querier** [**address** *source-address*]		Activate IGMP Snooping Querier to the specified VLAN.
no ip igmp snooping [**vlan** *vlan-id*] **querier** [**address** *source-address*]	Global	Release the setting of IGMP Snooping Querier.

Reference

If there is no source address for IGMP Snooping Querier setup, use the IP address of corresponding VLAN interface. Otherwise, set it to 0.0.0.0.

IGMP Snooping Query – Transmission Interval Setting

Command	Mode	Function
ip igmp snooping querier query-interval <1 – 1800>	Global	Set the transmission interval of IGMP Snooping Query message. (Unit : second)
ip igmp snooping vlan *vlan-id* **querier query-interval** <1 – 1800>		Set the transmission interval of IGMP Snooping Query message of the specified VLAN. (Unit : second)

Command	Mode	Function
no ip igmp snooping [**vlan** *vlan-id*] **querier query-interval**	Global	Release the interval setting of IGMP Snooping Query message and return to the default setting.

Reference

Transmission interval of IGMP Snooping Querier message is set to 125 seconds by default.

IGMP Snooping Query – Maximum response time setting

Maximum Response Time (MRT) is added to IGMP version 2 and version 3 membership query, and it is a maximum waiting time of report message from the host since query message is sent periodically from IGMP Snooping Querier. This host should send report message within the maximum response time.

Command	Mode	Function
ip igmp snooping querier max-response-time <1 - 25>	Global	Set maximum response time of IGMP Snooping Query message.
ip igmp snooping vlan *vlan-id* **querier max-response-time** <1 - 25>		Set maximum response time of IGMP Snooping Query message to the specified VLAN.

Command	Mode	Function
no ip igmp snooping querier max-response-time	Global	Release the maximum response time setting of IGMP Snooping Query message to the whole system or specified VLAN, and return to the default setting.
no ip igmp snooping vlan *vlan-id* **querier max-response-time**		

Reference

Maximum response time of IGMP Snooping Query massage can be set from 1 up to 25 seconds, and the default is set to 10 seconds.

IGMP Snooping Querier – Setting information check

Command	Mode	Function
show ip igmp snooping [**vlan** *vlan-id*] **querier** [**detail**]	Enable/ Global/Bridge	Show the setting information of IGMP Snooping Querier.

(2) IGMP Snooping Last Member Query- Transmission Interval Setting

If a MG205X with activated IGMP Snooping receives a 'leave' message, it sends group-specific query(IGMP version 2) or group-source-specific query(IGMP version 3) to the multicast group of corresponding hosts for checking if the host is left the group and rechecks if there is any new host joined.

If there is no response from the host, the MG205X doesn't send the multicast traffic to the group any more. But, if the network is not stable and packet loss is occurred, the ICMP message may be lost. To prevent this problem, user can set the transmission interval of query message temporarily.

Command	Mode	Function

ip igmp snooping last-member-query-interval <100 - 10000>	Global	Set the transmission interval of last member query message to check if the host is left the group.
ip igmp snooping vlan *vlan-id* **last-member-query-interval** <100 - 10000>		Set the transmission interval of last member query message to check if the host is left the specified VLAN.
no ip igmp snooping last-member-query-interval		Delete the transmission interval setting of last member query message.
no ip igmp snooping vlan *vlan-id* **last-member-query-interval**		Delete the transmission interval setting of last member query message to the specified VLAN.

Reference

Transmission interval of Group-specific or Group-source-specific Query message can be set from 100 milliseconds up to 10000 milliseconds. The default is 1000ms.

(3) IGMP Snooping Immediate-Leave Setting

In MG205X, If IGMP Snooping Immediate-leave function is enabled, the process of sending group-specific or group-source-specific query massage will be omitted when host sends ‘leave’ message. and it will delete the multicast group entries of the host from the IGMP Snooping membership table immediately and notify the relevant information to a multicast router.

To set the IGMP Snooping Immediate-leave feature, use the following command.

Command	Mode	Function
ip igmp snooping immediate-leave	Global	Set the IGMP snooping Immediate-leave to the whole system.
ip igmp snooping port *port-number* **immediate-leave**		Set the IGMP snooping Immediate-leave to the specified port.
ip igmp snooping vlan *vlan-id* **immediate-leave**		Set the IGMP snooping Immediate-leave to the specified VLAN.

Attention

Please be sure to use IGMP snooping Immediate-leave function with host tracking function. Please refer to the chapter 9.2.5.7 Host Tracking Setting Note. If the host tracking function is released while IGMP snooping Immediate-leave is enabled, IGMP Snooping querier will drop out all the hosts from the group without check when a host from the group sends ‘leave message. Because of this, the other hosts can’t receive any more traffic even though it is wanted.

To disable IGMP Snooping Immediate-leave feature, use the following command.

Command	Mode	Function
no ip igmp snooping immediate-leave	Global	Disable the settings of IGMP Snooping Immediate-leave function to the specified range.
no ip igmp snooping port *port-number* **immediate-leave**		
no ip igmp snooping vlan *vlan-id* **immediate-leave**		

(4) IGMP Snooping Report Suppression Setting

Even though multicast router receives a report message from a host in the multicast group, it sends multicast traffic to the corresponding group, so every host in the group receive report message and the bandwidth will be abused from unnecessary traffic. The solution to this problem in the IGMP version 2 is report suppression function which prevents from sending repeated messages to the other hosts by sharing the information of the message which was sent first time.

However, if there is an L2 MG205X Between the hosts and router, be sure to support IGMP Report Suppression feature to prevent that each host sends report messages to the multicast router when IGMP Snooping is enabled.
When Report Suppression is activated in the L2 MG205X, it transfers to the multicast router only the first report message from a host in each multicast group or the leave message from the host which is dropped at last.

To enable IGMP Snooping Report Suppression feature, use the following command.

Command	Mode	Function
ip igmp snooping report-suppression	Global	Enable IGMP Snooping Report Suppression function to the whole system.
ip igmp snooping vlan *vlan-id* **report-suppression**		Enable IGMP Snooping Report Suppression function to the specified VLAN.

Attention

The IGMP Snooping Report Suppression function is available only in IGMP version 1 and version 2.

To disable IGMP Snooping Report Suppression feature, use the following command.

Command	Mode	Function
no ip igmp snooping [**vlan** *vlan-id*] **report-suppression**	Global	Disable IGMP Snooping Report Suppression function.

(5) IGMP Snooping S-Query Report Agency Setting

If an equipment receives an IGMP Group Specific Query message from the multicast router while IGMP snooping is enabled, it does flooding on all ports basically. Hosts receiving Group Specific Query message will have increased load because it responds with report messages based on its membership information. If IGMP Snooping Specific-Query Report Agency is activated, the MG205X will not do flooding of the IGMP Group Specific Query messages, and will respond by IGMP Report message on behalf of the host.

To respond with the IGMP Report message on behalf of host when IGMP Group Specific Query message is received from a router, use the following command.

Command	Mode	Function
ip igmp snooping s-query-report agency	Global	Enable IGMP Snooping S-Query Report Agency.

To do flooding in the group when IGMP Group Specific Query message is received from a router, use the following command.

Command	Mode	Function
no ip igmp snooping s-query-report agency	Global	Disable IGMP Snooping S-Query Report Agency.

(6) IGMP Snooping Proxy Setting

IGMP Proxy allows multicast router to send and receive IGMP messages on behalf of hosts connected to the lower network. When IGMP Snooping Proxy feature is enabled on the MG205X, if Query message is received from a multicast router, the MG205X sends report message to all the group MAC addresses registered through MAC Learning without forwarding the report messages to the ports. If it does learning a new group MAC address, the Report message is delivered to all multicast router interface, and if it receives a Leave message from a host, PDU (Protocol Data Unit) is transferred to all multicast router interfaces.

To enable IGMP Snooping Proxy feature, use the following command in Global mode.

Command	Mode	Function
ip igmp snooping proxy	Global	Enable IGMP Snooping Proxy function to whole system.

ip igmp snooping vlan *vlan-id* **proxy**		Enable IGMP Snooping Proxy function to the specified VLAN.

To disable the IGMP Snooping Proxy feature, use the following command.

Command	Mode	Function
no ip igmp snooping [**vlan** *vlan-id*] **proxy**	Global	Disable IGMP Snooping Proxy function.

(7) Host Tracking Setting

Host tracking function is that the membership information of host is collected by report message of host and saved in host tracking database, and the joined hosts can be managed efficiently. This is supported by all IGMP versions, and immediate-blocking of IGMP version 3 or Immediate-leave function of IGMP version 2 prevents the problem that all host can't receive traffics by a leave message of a host in the multicast group.

This feature solves a limitation of Immediate-leave function to be used in a network environment that is connected to only one IGMP host and minimize the required delay time when the host leave the group.

To activate the host tracking feature for managing hosts to be joined, use the following command:

Command	Mode	Function
ip igmp snooping explicit-tracking	Global	Activate the host tracking function to the whole system.
ip igmp snooping vlan *vlan-id* **explicit-tracking**		Activate the host tracking function to the specified VLAN.

To disable the host tracking function setting, use the following command.

Command	Mode	Function
no ip igmp snooping explicit-tracking	Global	Disable the host tracking function setting to the whole system.
no ip igmp snooping vlan *vlan-id* **explicit-tracking**		Disable the host tracking function setting to the specified VLAN.

User can limit the number of hosts to be joined to a particular port. If the hosts are tried to be joined more than the setting limit of the port, they can be joined to the corresponding group, but the information of the host is not saved in the host tracking database, and related message will be provided.

To specify the maximum number of hosts to be joined to a specific port, use the following command.

Command	Mode	Function

ip igmp snooping explicit-tracking max-hosts port *port-number* **count** <1 - 65535>	Global	Set the maximum number of hosts to be joined to the specified port.
no ip igmp snooping explicit-tracking max-hosts port *port-number*		Delete the maximum number setting of hosts to be joined to the specified port, and return to the default.

Reference

The maximum number of hosts to be joined to a specific port can be set within the range from 1 to 65535. The default setting is 1024.

Through the host tracking function, it is possible to check if a host is joined to a group, But, if there is a host which leaves the group without sending 'leave' message abnormally, the information of the host tracking database may not accurate sometimes. Therefore, the equipment is sending the Group specific Query message basically to check it again when it receives a 'leave' message from the host. However, as this may cause a greater load to the equipment and the host, user can release this setting.

To release or enable the Group Specific Query message settings when a 'leave' message is received from a host, use the following command.

Command	Mode	Function
ip igmp snooping explicit-tracking s-query-suppression	Global	Release the Group Specific Query message settings not to send the message when a 'leave' message is received from a host
no ip igmp snooping explicit-tracking s-query-suppression		Enable the Group Specific Query message settings to send the massage when a 'leave' message is received from a host

Reference

MILEGATE-2012 sends the Group Specific Query message after receiving the 'leave' message by default and the settings are applied to all VLAN.

To check the information of IGMP Snooping host tracking, use the following command.

Command	Mode	Function

show ip igmp snooping explicit-tracking	Enable/ Global/ Bridge	Show the information of host tracking to the whole system.
show ip igmp snooping explicit-tracking vlan *vlan-id*		Show the information of host tracking to the specified VLAN.
show ip igmp snooping explicit-tracking port *port-number*		Show the information of host tracking to the specified port.
show ip igmp snooping explicit-tracking group *group-address*		Show the information of host tracking to the specified multicast group address.
show ip igmp snooping explicit-tracking summary vlan *vlan-id*		Show the summary information of host tracking to the specified VLAN.
show ip igmp snooping explicit-tracking summary port *port-number*		Show the summary information of host tracking to the specified port.

(8) Multicast Router Port Setting

The multicast router port is the port connected directly to the multicast router. User can set the port which the multicast router is connected directly, or can the port through a port which PIM hello packet and IGMP Query message is received.

Static Multicast Router Port Settings

User can assign a L2 port as a port that is connected to the multicast router. To specify the multicast router port, use the following command.

Command	Mode	Function
ip igmp snooping mrouter port {*port-number* I **cpu**}	Global	Set the specified port as multicast router port
ip igmp snooping vlan *vlan-id* **mrouter port** {*port-number* I **cpu**}		Set the specified port as multicast router port in specified VLAN.

To disable the specified multicast router port setting, use the following command:

Command	Mode	Function
no ip igmp snooping mrouter port {*port-number* I **cpu**}	Global	Disable the specified multicast router port setting.
no ip igmp snooping vlan *vlan-id* **mrouter port** {*port-number* I **cpu**}		

Learning Setting of multicast router port

Multicast router port is added to the forwarding table for all multicast entries management of L2. MG205X can be set to recognize the ports which PIM hello packets are incoming as the multicast router ports. To set the ports which PIM hello packets are incoming as the multicast router ports, use the following command.

Command	Mode	Function
ip igmp snooping mrouter learn pim	Global	Set the ports of whole system which PIM hello packets are incoming as the multicast router ports.
ip igmp snooping vlan *vlan-id* **mrouter learn pim**		Set the ports of specified VLAN which PIM hello packets are incoming as the multicast router ports.

To disable the multicast router port setting by using PIM hello packets, use the following command.

Command	Mode	Function
no ip igmp snooping mrouter learn pim	Global	Disable the multicast router port setting by using PIM hello packets.
no ip igmp snooping vlan *vlan-id* **mrouter learn pim**		

Forwarding settings of Multicast Router Port

In L2 MG205X, as multicast source information should be sent to the multicast router, multicast traffic should be forwarded to IGMP Snooping membership ports and multicast router ports.

Multicast router port can be set as static port or it can be set to the ports which General Query messages or PIM Hello packets are received.

To forward multicast traffic by multicast router port, use the following command.

Command	Mode	Function
ip multicast mrouter-pass-through	Global	Forward multicast traffic by multicast router port.
no ip multicast mrouter-pass-through		Disable the forwarding setting of multicast traffic by multicast router port.

OK multicast router ports

To check the IGMP Snooping multicast router ports, use the following command.

Command	Mode	Function
show ip igmp snooping mrouter	Enable/ Global/ Bridge	Show multicast router port setting.
show ip igmp snooping vlan *vlan-id* **mrouter**		Show multicast router port setting in specified VLAN.

(9) Multicast TCN Flooding Setting

If a MG205X with enabled IGMP Snooping feature received a TCN, by default, the MG205X does flooding of multicast traffic to all ports until it receives General Query message with 125-seconds transmission cycle twice. User can set the transmission time or cycle of the IGMP Query message to determine the time to stop flooding of multicast traffic.

To set the transmission time of IGMP Query message to stop flooding of multicast traffic, use the following command.

Command	Mode	Function
ip igmp snooping tcn flood query count <1 – 10 >	Global	Set the transmission time of IGMP Query message to stop flooding of multicast traffic.

Reference

The transmission time of IGMP Query message to stop flooding of multicast traffic can be specified from 1 to 10 times, and the default is 2 times.

To disable above setting, use the following command in Global Configuration mode.

Command	Mode	Function
no ip igmp snooping tcn flood query count	Global	Delete the transmission time setting of IGMP Query message, and return to the default value.

Reference

In MG205X, TCN recognition and multicast flooding time can be calculated by multiplying transmission number of Query messages by transmission interval. For example, the number of transmission times is 3 and the transmission interval is set to 100 seconds. Then, flooding of the multicast traffic is continued for 300 seconds only.

To set the transmission cycle of IGMP Query message to limit and stop the multicast flooding, use the following commands.

Command	Mode	Function
ip igmp snooping tcn flood query interval <1 – 1800 >	Global	Set the transmission cycle of IGMP Query message.

Reference

The transmission cycle of IGMP Query message can be set from 1 up to 1800 seconds. The default is set to 125 seconds, and IGMP Query message is to be transferred every 125 seconds.

To disable the transmission cycle setting of IGMP Query message to stop the multicast flooding, use the following commands.

Command	Mode	Function
no ip igmp snooping tcn flood query interval	Global	Delete the transmission cycle setting of IGMP Query message, and return to default value.

Transmission of TCN Flooding Solicitation messages

If the topology of network is changed, Root MG205X sends "General Query Solicitation" message to all ports with the group address setting to 0.0.0.0. If a multicast router receives this Solicitation message, it transmits IGMP General Query message directly.

If MG205X receives a TCN, use following command to transmit Query Solicitation message to the ports.

Command	Mode	Function
ip igmp snooping tcn query solicit	Global	Transmit Query Solicitation message when the system receives a TCN.
ip igmp snooping tcn query solicit address *source-address*		Transmit Query Solicitation message with source address setting.

Reference

In case the Source Address is not set, the IP address of VLAN Interface will be used first. Otherwise, the address will be set to 0.0.0.0.

To disable the setting to send Query Solicitation message, use the following command.

Command	Mode	Function
no ip igmp snooping tcn query solicit	Global	Set not to send Query Solicitation message.
no ip igmp snooping tcn query solicit address		Set not to send Query Solicitation message to the corresponding source address.

TCN Flooding debugging

To debug IGMP Snooping TCN function efficiently, use the following command.

Command	Mode	Function
debug igmp snooping tcn	Enable	Debug the IGMP Snooping TCN function.

no debug igmp snooping tcn	Disable the debugging setting of IGMP Snooping TCN function.

9.2.4 IGMP Version 3 Snooping Setting

Immediate Blocking Settings

The Report message of IGMP version 3 includes filter mode of include/exclude and source multicast list which is allowed/excluded to transfer packet transmission. Immediate blocking function of IGMP version 3 is taking reference of host tracking database and blocks quickly the traffics received from specific multicast address by the host.

For example, if host sends a report message with information that it doesn't want to receive multicast traffic from specific source address, the MG205X Compares the source address of the report messages sent by host with the source list of host tracking information. If the compared information is matched, the MG205X delete the corresponding source entry from the list and blocks multicast traffic which was sent to the host. In other words, if the immediate blocking is enabled, the procedure of sending Group-source-specific Query message is omitted.

To enable IGMP version 3 immediate blocking feature, use the following command.

Command	Mode	Function
ip igmp snooping immediate-block	Global	Enable immediate blocking function to the whole system.
ip igmp snooping vlan *vlan-id* **immediate-block**		Enable immediate blocking function to the specific VLAN.

Attention

Immediate Blocking feature must be activated with host tracking function.
(Refer to the chapter 9.2.5.7 Host Tracking Setting)

To disable IGMP version 3 Immediate Blocking feature set, use the following command:

Command	Mode	Function
no ip igmp snooping immediate-block	Global	Disable immediate blocking function setting to the whole system.
no ip igmp snooping vlan *vlan-id* **immediate-block**		Disable immediate blocking function setting to the specific VLAN.

9.2.5 IGMP Snooping Setting Information Check

To check the latest settings of IGMP Snooping, use the following command.

Command	Mode	Function
show ip igmp snooping info [**vlan** *vlan-id*]	Enable/ Global/Bridge	Check the settings of IGMP Snooping.

To check the information of IGMP Snooping table, use the following command.

Command	Mode	Function
show ip igmp snooping table group [*ip-address*]	Enable/ Global/ Bridge	Check the information of IGMP Snooping table of the whole system.
show ip igmp snooping table port [*port-number*]		Check the information of IGMP Snooping table of the specified port.
show ip igmp snooping table vlan [*vlan-id*]		Check the information of IGMP Snooping table of the specified VLAN.
show ip igmp snooping table reporter [*ip-address*]		Check the information of IGMP Snooping table of the specified report.

To check the summary information of IGMP Snooping group, use the following command:

Command	Mode	Function
show ip igmp snooping groups summary [**vlan** *vlan-id*]	Enable/ Global/ Bridge	Check the summary information of IGMP Snooping group in the specified VLAN.
show ip igmp snooping groups summary [**port** *port-number*]		Check the summary information of IGMP Snooping group related to the specified port.

Use the following command to check the IGMP Snooping statistics.

Command	Mode	Function
show ip igmp snooping stats port {*port-number* | **cpu**}	Enable/ Global/Bridge	Check the IGMP Snooping statistics.

To reset the IGMP Snooping statistics information, use the following command.

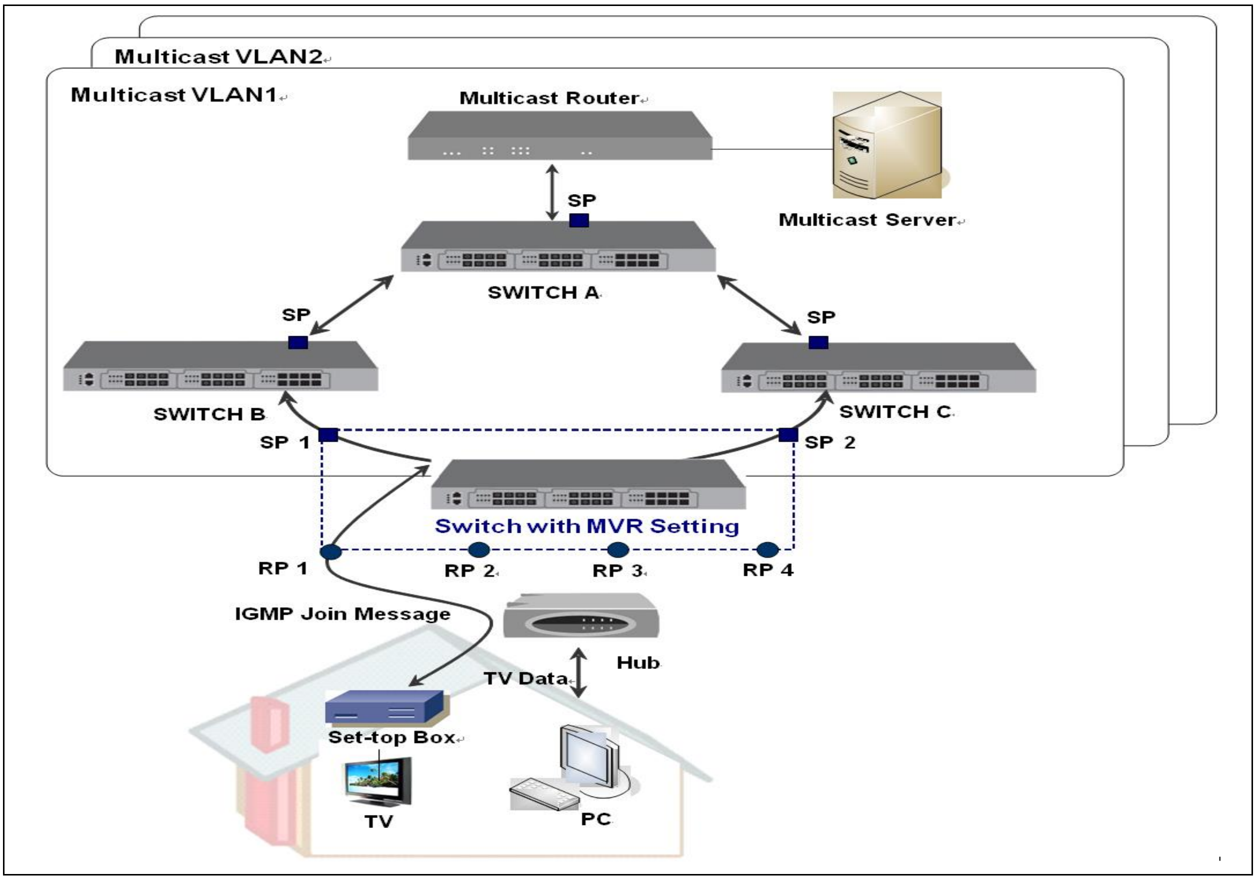
Command	Mode	Function

clear ip igmp snooping stats port {*port-number* | **cpu**}	Enable/ Global/ Bridge	Reset the IGMP Snooping statistics information.

9.2.6 MVR (Multicast VLAN Registration)

MVR (Multicast VLAN Registration) is a function which enables multicast communications in L2 (not L3) by setting the subscribers who receive the same multicast packets in different VLANs to the multicast VLAN. Therefore, it can save the hardware resources and enables continuous transmission of multicast streams without interruption.

Meanwhile, as the multicast VLAN is blocked to the other subscribers VLAN as a separate VLAN, it guarantees bandwidth and security of the multicast communication.



【Picture 9-6】MVR Operation

The above figure is the case which all the equipments, including multicast server, the multicast router, MG205X etc., are belonged to the same VLAN and there is a MG205X with MVR setting. The MG205X with MVR setting transmit IGMP Join message, which is received from PC or set-top box connected to the subscriber port, to the multicast router through SP(Source Port). Then, the multicast traffic will be sent from the multicast router to the requested subscriber through RP (Receiver port).

Attention

When you set the MVR in MG205X, the receiver ports of both MVR VLAN and Subscriber's VLAN should be set to untagged VLAN.

Attention

In order to enable the MVR in MG205X, IGMP Snooping feature must be enabled.

Attention

MVR supports only IGMP version 2.

With regard to MVR settings following topics are described in this chapter.

- MVR Activation
- MVR Group Setting
- MVR Helper Address Setting
- Source/Receiver Port Setting
- MVR Setting Check

(1) MVR Activation

To enable MVR, use the following command.

Command	Mode	Function
mvr	Global	Enable MVR function.
no mvr	Global	Release MVR function setting.

Reference

In MG205X, MVR function is disabled by default.

(2) MVR Group Setting

In order to set the MVR function, user should specify the MVR group and group address. If multiple MVR group is set, IGMP packets are transmitted in accordance with the specified MVR group address from RP (Receiver Port) to SP (Source Port) which MVR group is included.

To specify the MVR group and group address, use the following command.

Command	Mode	Function
mvr vlan *vlan-id* **group** *group-address*	Global	Set MVR group and its address.
no mvr vlan *vlan-id* **group** *group-address*	Global	Delete the MVR group and its address.

Reference

One MVR group address can't be included in two or more MVR group.

(3) Source/Receiver Port Setting

If user set the MVR port, the port will be added to or removed from the corresponding member group. The "source / source +" option here is used to set source port. Source port is uplink port which can send multicast traffic to the multicast router or receive it from the multicast router. Subscribers are not connected to the source port directly, and all source ports are belonged only to the tagged multicast VLAN.

"Receiver" option is used to set the receiver ports. Receiver ports can only receive multicast traffic through the ports connected to the subscriber directly. These ports must be included in both subscriber's VLAN and multicast VLAN as untagged.

"Receiver +" option is used to set the receiver ports like the receiver, and the receiver ports will be changed to tagged or untagged according to the IGMP Report packet. That is, if it receives untagged IGMP Report or leave message, the MVR VLAN receiver port of the group will be changed to untagged. On the other hand, if it receives a tagged IGMP Report or leave message, the MVR VLAN receiver port will be changed to tagged.

To set a specific port with source port or receiver port of MVR, use the following command.

Command	Mode	Function
mvr port *port-number* **type** {**source** | **source+** | **receiver** | **receiver+**}	Global	Set the specified port with source port or receiver port of MVR

Reference

If user set the receiver+, the receiver port of MVR VLAN will be changed to untagged or tagged dynamically. This information is checked by 'show running-config' or 'show VLAN' command.

Reference

After a subscriber port is changed to untagged by the receiver+ operation, if it is changed to ‘tagged’ manually by the administrator, it will cause service disruption. However, if an untagged IGMP message is received, the receiver port will be changed to ‘untagged member’ and the service will be restarted.

(4) MVR Helper Address Setting

If a multicast server is belonged to the other network than user’s equipment, the multicast router will be operated in L3 multicast routing for each MVR group. In this case, when the IGMP packet of a subscriber is to be delivered to a multicast router, the source address of the IGMP packet may not match with the network of MVR group. If it is not matched, the router blocks corresponding IGMP packet. To solve this problem, user can replace the source address of the IGMP packet with a particular MVR helper address. This helper address must be included in MVR group network.

To set MVR helper address to replace IGMP packet source address, use the following command.

Command	Mode	Function
mvr vlan *vlan-id* **helper** {*ip-address* |**br-ip**}	Global	Set specified MVR helper address to replace the IGMP packet source address. ‘**br-ip’** option is to use the IP address set in VLAN interface.

Command	Mode	Function
no mvr vlan *vlan-id* **helper**	Global	Delete MVR helper address setting.

(5) MVR Setting Check

To check the MVR-related settings, use the following command.

Command	Mode	Function
show mvr	Enable/ Global/ Bridge	Check the MVR-related settings.
show mvr vlan *vlan-id*		
show mvr port		

(6) IGMP Filtering Setting

IGMP Profile creation

To use the IGMP filtering feature, use the following command in Global setting mode. After creating an IGMP Profile, user can do detailed settings in IGMP Profile mode.

Command	Mode	Function
ip igmp profile *profile-number*	Global	Create or modify the specified IGMP Profile.
no ip igmp profile *profile-number*		Delete the specified IGMP profile.

Reference

The "*Profile-number*" can be set within the range from 1 to maximum 2,147,483,648, and this number is its profile name simultaneously.

As above, the command "**ip igmp profile** *profile-number*" will change the prompt from 'MG205X (config)#' to MG205X (config-igmp-profile[profile-number])#, and the IGMP profile with the number will be created.

```
MG205X (config)# ip igmp profile 1
MG205X (config-igmp-profile[1])#
```

IGMP group range

To specify the group range to apply IGMP filtering feature, use the following command in IGMP Profile mode.

Command	Mode	Function
range *low- multicast-address* [*high-multicast-address*]	IGMP Profile	Specify the IGMP group range.
no range *low- multicast-address* [*high- multicast-address*]		Release the IGMP group range setting.

Reference

By specifying the "*low-multicast-address*" and "*high-multicast-address*" at the same time, the IGMP group range can be set. In addition, user can specify only one multicast group address without a certain range.

IGMP filtering, policy enforcement

User can set the IGMP filtering policies for the access to corresponding multicast address range. To set IGMP filtering policy, use the following command in the IGMP Profile mode.

Command	Mode	Function
{**permit** I **deny**}	IGMP Profile	Set IGMP group filtering policy in IGMP Profile.

IGMP filtering activation

To activate IGMP filtering function to port, the prepared IGMP profile should be applied to a specific port. To apply

IGMP profile to a specific port and enable IGMP filtering function, use the following command.

Command	Mode	Function
ip igmp filter port *port-number* **profile** *profile-number*	Global	Apply IGMP profile to the specified port.
no ip igmp filter port *port-number*		Disable the IGMP Profile setting applied to the port.

Attention

Multiple IGMP profile cannot be applied to a single port, user can activate the IGMP filtering function while the IGMP Snooping feature is enabled.

Attention

To delete created IGMP Profile, user needs to disable all ports that profile has been applied.

In MG205X, with reference to the DHCP snooping binding table, specified IGMP packet can be filtered. In other words, only the source IP address of host and IGMP packets of the MAC address, which are filtered by the host binding table, are permitted.

To permit only the IGMP packets of authorized host through the entry of DHCP Snooping binding table, use the following command.

Command	Mode	Function
ip igmp filter port *port-number* **permit dhcp-snoop-binding**	Global	With reference to the DHCP snooping binding table, add only corresponding entry to the IGMP Snooping table.
no ip igmp filter port *port-number* **permit dhcp-snoop-binding**		Disable the reference setting of DHCP snooping binding tale.

(7) IGMP Group Maximum Number Setting

User can set the maximum number of IGMP groups that can be joined by the hosts connected to ports. To set the maximum number of IGMP groups that can be joined to all ports or any specific port, use the following command.

Command	Mode	Function
ip igmp max-groups port all count <1-2147483647>	Global	Set the maximum number of IGMP groups that can be joined to all ports.
ip igmp max-groups port *port-number* **count** <1-2147483647>		Set the maximum number of IGMP groups that can be joined to the specified port.

no ip igmp max-groups port {**all** | *port-number*}		Delete the maximum number setting of IGMP groups.

To set the maximum number of IGMP groups that can be joined to the system, use the following command.

Command	Mode	Function
ip igmp max-groups system count <1-2147483647>	Global	Set the maximum number of IGMP groups that can be joined to the system.
no ip igmp max-groups system		Delete the maximum number setting of IGMP groups to the system.

(8) IGMP Filtering Setting by Packet

Depending on the type of ICMP packets, user can set the IGMP filtering function on each port. To block specific multicast packets, use the following command.

Command	Mode	Function
ip igmp filter port *port-number* **packet-type** { **leave** | **query** | **reportv1** | **reportv2** | **reportv3**}	Global	Block the specified type of IGMP packets incoming to the port.
ip igmp filter port *port-number* **packet-type all**		Block all the IGMP packets incoming to the port.
no ip igmp filter port *port-number* **packet-type** { **all** | **leave** | **query** | **reportv1** | **reportv2** | **reportv3**}	Global	Disable the setting of specified IGMP packet filtering.

Reference

IGMP filtering supports only IGMP version 2 by default, but it can block IGMP version 3 report message when the IGMP filtering is set by the type of packet.

(9) IGMP Filtering Setting Check

To check the settings related to IGMP filtering, use the following command.

Command	Mode	Function
show ip igmp filter [**port** *port-number*]	Global	Show the settings related to IGMP filtering.

To check the IGMP Profile, use the following command.

Command	Mode	Function
show ip igmp profile [*profile-number*]	Enable / Global / Bridge	Show the IGMP Profile setting.

9.2.7 IGMP Flap Discredit Setting

When there are multiple upstream interface in IGMP Proxy, the transmission path of multicast packets are determined by priorities. In this case, the priority of interface is determined first, and the most important factor of priority is credit. In MG205X, IGMP Flap Discredit feature is supported to provide more reliable multicast service by imposing a penalty on the instable network interface.

Flap is a phenomenon that a specific interface is repeating the interface-ON and interface-OFF. IGMP Flap Discredit reduces credit on the interface which flap is occurred, so the interface is to be excluded from the multicast path setting. If IGMP Proxy interface is set with first priority mode, the multicast path is to be determined by the high credit level order, and if it is set with load-balance mode, multicast packets are transmitted by the interfaces with high credit level order.

To enable IGMP Flap Discredit feature, use the following command.

Command	Mode	Function
ip igmp if flap discredit	Global	Enable IGMP Flap Discredit function.
no ip igmp if flap discredit		Disable IGMP Flap Discredit function.

Reference

By default, IGMP Flap Discredit feature is enabled.

To set the discredit value which reduces the value of credit every time when a flap occurs on a particular interface, use the following command.

Command	Mode	Function
ip igmp if flap discredit unit <1-50>	Global	Set the discredit value which reduces the value of credit whenever a flap occurs on a particular interface.
no ip igmp if flap discredit unit		Disable the discredit value setting and return to the default.

Reference

The default value of discredit is 5.

On the other hand, credit recovery is possible by checking the VIF credit of all IGMP upstream interface every time which user has set, and the credit value lower then default value (100) can be recovered. However, if the credit value is 0, the credit can't be recovered.

To set the time interval to recover the lowered credit value, use the following command.

Command	Mode	Function
ip igmp if flap recover-interval <0-3600>	Global	Set the time interval to recover the lowered credit value.
no ip igmp if flap recover-interval		Disable the time interval setting and return to the default interval setting.

Reference

Credit recovery time interval can be set in the range of <0-3600>. The default value is 10 seconds.

To set the credit value of one-time-recovery, use the following command.

Command	Mode	Function
ip igmp if flap recover-unit <1-50>	Global	Set the credit value of one-time-recovery
no ip igmp if flap recover-unit		Disable the credit value setting of one-time-recovery, and return to the default.

Reference

Credit value of one-time-recovery is 5 by default.

If user wants to delete current credit value and return it to the default value, use the following command.

Command	Mode	Function
clear ip igmp if flap discredit [*interface-name*]	Enable/Global	Set the credit value of the interface to the default value (100).

Reference

Credit Information of the interface can be shown by the 'show ip igmp interface' command.

9.2.8 Static SSM Mapping Setting

Multicast is available in networks composed of a single source and multiple hosts or multiple sources and multiple hosts. The multicast operating without relations to the number of sources are called as ASM (Any Source Multicast). In ASM, host will Join / Leave the multicast group with (*, G) entry, and '*' represents a certain source, and 'G' represents the multicast group.

On the other hand, in ASM, as user can't know any information that specifies the source, there should be a process to find the source like RP mechanisms which is widely used in PIM-SM. The process to find the source is the core functionality of ASM. In IPv4, multicast groups have addresses in the range from 224.0.0.0 up to 239.255.255.255 (224/4).

Meanwhile, SSM (Source Specific Multicast) is a multicast protocol designed to be particularly suited to multicast networks consisting of multiple hosts with a single source. The multicast receivers in SSM request multicast packets to (S, G) entry. The 'S' represents specific multicast source, and 'G' represents multicast group.

Unlikely to the ASM, it is assumed in SSM that the hosts want to receive multicast packets already know the information about the source. Therefore, there is no specific process to find the source. That is, each multicast receiver in SSM has to find out the information about the multicast source in its own way. By default, the multicast group corresponding to SSM has an address range from 232.0.0.0 up to 232.255.255.255 (232/8).

Static SSM mapping is, to say it easily, the SSM service support to IGMP version 1 and version 2 messages. In other words, the multicast host can receive multicast traffic from the specified group and can be set the source of packet. Users must specify the corresponding source address in order to receive traffic from the particular source.

In MG205X with enabled static SSM mapping, if it received an IGMP version 1 or version 2 report message, that message will be processed as IGMP version 3 report message.

Reference

As IGMP Proxy does not support IGMP version 3, if upstream or downstream interface is set in the interface, static SSM mapping cannot be activated.

To set static SSM Mapping, SSM mapping should be activated in the whole system. To enable SSM mapping, use the following command.

Command	Mode	Function
ip igmp sum-map enable	Global	Enable PIM-SSM to be used in SSM group(232/8) of standard IP range.
no ip igmp sum-map enable	Global	Disable the PIM-SSM setting.

To specify the source IP address of multicast server by the specific access list, use the following command.

Command	Mode	Function

ip igmp ssm-map static {<1 - 99> | <1300-1999> | *access-list-name*} *ip-address*	Global	Set to specify the source IP address of multicast server by the specific access list
no ip igmp ssm-map static {<1 - 99> | <1300-1999> | *access-list-name*} *ip-address*		Delete the specified source IP address of multicast server.

To check the setting information related to SSM mapping, use the following command.

Command	Mode	Function
show ip igmp ssm-map [*ip-address*]	Enable Global Bridge	Show the setting information related to SSM mapping.

9.2.9 IGMP State Number Setting

IGMP state number setting can protect MG205X against DoS (denial of service) attack caused by IGMP packets. IGMP state is an expression of all IGMP, IGMP version 3 lite, URD (URL Rendezvous Directory) membership report message etc. which is joined to multicast router. Membership reports which is over the setting value cannot enter the IGMP cache and can't be forwarded. This function can be set to whole system or specific interface, and user can also exclude specific access list via 'Except' option.

To set the maximum number of IGMP State to be joined to the router in the entire system, use the following command.

Command	Mode	Function
ip igmp limit <1-2097152> [**except** {<1 - 99>| <1300 - 1999> | *access-list-name*}]	Global	Set the maximum number of IGMP State to be joined to the router in the entire system.
no ip igmp limit		Delete the maximum number of IGMP State.

To set the maximum number of IGMP State to be joined to the router in a specific interface, use the following command.

Command	Mode	Function
ip igmp limit <1-2097152> [**except** {<1 - 99>| <1300 - 1999> | *access-list-name*}]	Interface	Set the maximum number of IGMP State to be joined to the router in a specific interface.
no ip igmp limit		Delete the maximum number of IGMP State.

9.2.10 MRIB Debug

To debug the MRIB related information, use the following command.

Command	Mode	Function
debug nsm mcast all	Enable	Debug all the MRIB related information.

debug nsm mcast fib-msg		Debug MFIB (Multicast Forwarding Information Base) information.
debug nsm mcast mrt		Debug multicast routing information.
debug nsm mcast register		Debug multicast PIM register message.
debug nsm mcast stats		Debug multicast related statistics.
debug nsm mcast vif		Debug multicast interface related information.

To disable the MRIB debugging settings, use the following command.

Command	Mode	Function
no debug nsm mcast all	Enable	Disable the debugging of all the MRIB related information.
no debug nsm mcast fib-msg		Disable the debugging of MFIB (Multicast Forwarding Information Base) information.
no debug nsm mcast mrt		Disable the debugging of multicast routing information.
no debug nsm mcast register		Disable the debugging of multicast PIM register message.
no debug nsm mcast stats		Disable the debugging of multicast related statistics.
no debug nsm mcast vif		Disable the debugging of multicast interface related information.

To check the MRIB debugging settings, use the following command.

Command	Mode	Function
show debugging nsm mcast	Enable	Check the MRIB debugging settings

10. Appendix A. System Image Installation

In MG205X, administrator can save and use 2 system images by the environment.

System image file installation is consisted of the following;

- System image installation in enable mode
- System image installation in boot mode
- System image installation by remote way

A.1 System Image Installation in Enable Mode

Administrator can install system image to MG205X by using FTP/TFTP server in Global mode. Please refer to the following procedures.

Step 1 Install the FTP/TFTP server program in your PC.

Step 2 Download a new image file in the Root folder of the FTP/TFTP server in your PC.

Step 3 Connect the MG205X to your PC with a console cable.

Step 4 Set the IP address in the Interface setting mode of the MG205X to interface to the FTP/TFTP server.

Step 5 Install a new image file in the flash memory of the MG205X from FTP/TFTP server.

Following procedures are described for system image installation from PC with FTP/TFTP server.

Step 1 System image download to FTP/TFTP server.

Step 2 System image installation preparation.

Step 3 System image installation

A.1.1 System Image Download To FTP/TFTP Server

To use your PC as FTP/TFTP servers, the FTP/TFTP server program should be installed on your PC. If you installed the FTP/TFTP server program in your PC, then, download the system image file of MG205X in the Root folder of the FTP/TFTP server which you have installed.

A.1.2 System Image Installation Preparation

After downloading system image file to FTP/TFTP server in your PC, prepare the network connection as following.

Step 1. Set the console terminal of your PC as 9600 baud rates, 8 data bits, one stop bit and no parity.

Step 2. Connect your PC to MG205X with a console cable. At this time, the PC and MG205X should be in the same network, respectively.

Step 3. Boot the MG205X

Step 4. If user enter log-in name after the login prompt, password prompt will be shown. After entering password, Privilege Exec View mode will be started.

Factory default log-in name is ‘admin’, and the password is not set.

```
MG205X login: admin
Password:
```

```
MG205X >
```

Step 5. In Privilege Exec View mode, user can only check the setting details of MG205X. To do settings and managing of MG205X, please enter into Privilege Exec Enable mode.

```
MG205X > enable
MG205X #
```

Step 6. Enter into interface setting mode to set IP address.

```
MG205X # configure terminal
MG205X (config)# interface 1
MG205X (config-if)# ip address 192.168.1.10/24
MG205X (config-if)# no shutdown
MG205X (config-if)# show ip
IP-Address         Scope   Status
-------------------------------------
192.168.1.10/16     global

MG205X (config-if)# exit
MG205X (config)#
```

A.1.3 System Image Installation

Download system image file from FTP/TFTP server to install it in MG205X by following steps.

Step 1. Install the system image file from FTP/TFTP server by following command in 'Enable' mode.

Command	Mode	Function
copy {**ftp**|**tftp**} **os download** {**os1**|**os2**}	Enable	Install the system image file in either OS1 or OS2.

Reference

'os1' or 'os2' indicates the location of flash memory where the image files are saved. When storing the system image file in MG205X, the location of flash memory should be specified.

The following is an example which administrator installs the system image file from FTP server. To log-in to the FTP server, account name and password should be entered correctly.

- TFTP server: 50.0.158.1
- TFTP server user name: admin
- TFTP server password: (None)
- System image file: MG205X

```
MG205X (config)# copy ftp os download os1
 To exit : press Ctrl+D
--------------------------------------
IP address or name of remote host (FTP): 50.0.158.1
Download File Name : MG205X
User Name : admin
Password:
Hash mark printing on (1024 bytes/hash mark).
Erasing OS area ..
Downloading NOS ....
#################################################################
#################################################################
9814048 bytes download OK.
MG205X (config)#
```

The following is the case which administrator installs the system image file from TFTP server.

- TFTP Server: 10.47.250.57
- System image file: MG205X

```
MG205X # copy tftp os download os1
 To exit : press Ctrl+D
--------------------------------------
IP address or name of remote host (TFTP): 10.47.250.57
Download File Name : MG205X

Now download NOS from 10.47.250.57 via tftp.
Downloading NOS ....
Received 9635067 bytes.
Erasing Flash.... (1/3)
Programming NOS.. (2/3)
Verifying NOS.... (3/3)
NOS is successfully upgraded.
MG205X #
```

Step 2. If you want to use multiple OS, please install the image file to a different location from the Step 1 by using the instructions above.

Step 3. Reboot the system by ‘reload’ command in Privilege Exec Enable mode, and check the version of system image file to see if the installation is successful.

A.2 System Image Installation In Boot Mode

In Boot mode, you can use only TFTP to install the system image. Followings are the procedures for downloading new system image file to your PC with TFTP server and doing installation of it to MG205X..

Step 1 Install the TFTP server program on your PC.

Step 2 Download new image file in the Root folder of the TFTP server on your PC.

Step 3 Connect the PC to MG205X with a console cable.

Step 4 Set the IP address of the MG205X to interface to the TFTP server in Boot mode or Interface setting mode.

Step 5 Interface to the TFTP server, and install a new image file in the flash memory of MG205X.

Reference

Followings are the procedures of system image installation after downloading it to the PC with TFTP server.

Step 1 System mage installation preparation

Step 2 System image installation

A.2.1 System Image Installation Preparation

Step 1. After connecting your PC to MG205X, turn on the power for booting. If you see the message '**If you want to go to boot mode, press s key..',** enter into Boot mode by using 's' key.

```
************************************************************
*                                                          *
*             Boot Loader Version 02.01.0001               *
*                DZS, Inc.                         *
*                                                          *
************************************************************
Press 's' key to go to Boot Mode:  0
Boot>
```

Step 2 Set the IP address in Boot mode to be able to interface to TFTP server. The command to set the IP from the Boot mode is 'ip ip-address'. The following shows the IP address setting as 192.168.1.10. However, this IP address is only useful in Boot mode.

```
Boot> ip 192.168.1.10
Boot>
```

Step 3 Save the IP address setting by 'save' command, and reboot MG205X by 'reboot' command.

Then, enter into Boot mode by the same way in step 1.

```
Boot> save
Boot> reboot

************************************************************
*                                                          *
*             Boot Loader Version 02.01.0001               *
*                DZS, Inc.                        *
*                                                          *
************************************************************
Press 's' key to go to Boot Mode:  0
Boot>
```

Step 4 Check the IP address setting by ‘show’ command.

```
Boot> show
IP        = 192.168.1.10
EtherAddr 0 = 00:d0:cb:0a:30:23
Boot>
```

Attention

Prior to the interface to TFTP server, please make sure that the PC with TFTP server and MG205X are in the same LAN.

A.2.2 System Image Installation

Step 1 Use the following command to install the system image file.

Command	Mode	Function
load os1 *server-ip-address file-name*	Boot	Install the system image file.

Reference

‘os1’ indicates the location of flash memory where the image files are saved. When storing the system image file in MG205X, the location of flash memory should be specified.

When you see the message ‘Update flash: Are you sure (Y/n)?’, type ‘y’. Then, system image upgrade will be started.

```
Boot> load os1 192.168.1.218 MG205X.1.42.x
Loading MG205X from 192.168.1.218...
Download completed: 5791488 (0x564e88) Bytes.
Update flash: Are you sure (Y/n)? y
```

Step 2. If you want to use multiple OS, please install the image file to a different location from the step 1 by using the instructions above.

Step 3. Reboot the system by ‘reboot’ command, and check the version of system image file to see if the installation is successful.