

Firmware Release Note

Product Name:	MGS3530-28
Firmware Version:	V4.10(ACEM.3)C0
Release Date:	2025/9/15

THIS DOCUMENT CONTAINS PROPRIETARY TECHNICAL INFORMATION THAT IS THE PROPERTY OF THE ZYXEL AND SHOULD NOT BE DISCLOSED TO OTHERS IN WHOLE OR IN PART, REPRODUCED, COPIED, OR USED AS BASIS FOR DESIGN, MANUFACTURING OR SALE OF APPARATUS WITHOUT WRITTEN PERMISSION OF ZYXEL.

Table of Content

REVISION HISTORY.....	3
SUPPORTED PLATFORM.....	4
VERSION INFORMATION	4
MAIN FEATURES	5
KNOWN ISSUES	8
TABLE SIZE & LIMITATIONS	8
FIRMWARE UPGRADE	9
CONFIGURATION UPGRADE.....	10
MODIFICATIONS IN V4.10(ACEM.3)C0	11
MODIFICATIONS IN V4.10(ACEM.2)C0	14
MODIFICATIONS IN V4.10(ACEM.1)C0	16
MODIFICATIONS IN V4.10(ACEM.0)C0	17

Revision History

Date	Release	Author	Description
2025/09/15	V4.10(ACEM.3)C0	Frank Chang	FW release
2022/12/27	V4.10(ACEM.2)C0	Frank Chang	Bug fixes and vulnerability patches
2022/07/22	V4.10(ACEM.1)C0	Jacky Liang	FW release
2022/05/31	V4.10(ACEM.0)C0	Jacky Liang	FW release

Supported Platform

V4.10(ACEM.3)C0 supports model: MGS3530-28

Version Information

V4.10(ACEM.3)C0	V4.10(ACEM.3) 09/15/2025 BootBase Version: V1.01 SDK version: V3.6.7.55090
-----------------	--

Main Features

1. 24 Auto MDI/MDI-X 10Base-T/100Base-TX/1000Base-T
2. 4 combo 1G/10 GbE
3. 16K layer 2 MAC addresses table
4. Jumbo frame length 9K
5. IEEE 802.1D transparent bridging
6. IEEE 802.1w, RSTP
7. IEEE 802.1s, MSTP
8. ZYXEL MRSTP
9. Rule-based bandwidth control
10. Port-based egress traffic shaping
11. IEEE 802.3x flow control.
12. DSCP to 802.1p priority mapping
13. Port-based VLAN
14. Protocol-based VLAN
15. IP subnet based VLAN
16. IEEE 802.1Q Static VLANs
17. IEEE 802.1Q dynamic VLANs
18. VLAN trunking
19. GVRP
20. IEEE 802.3ad LACP
21. Port mirroring
22. Support rate limiting, minimum step 64K both ingress and egress
23. Broadcast Storm Control
24. Layer 2 MAC filtering
25. Layer 3 IP filtering
26. Layer 4 TCP/UDP socket filtering
27. DHCP snooping
28. DHCP client
29. DHCP relay/DHCP relay per VLAN
30. DHCP option 82
31. IGMP v1/v2/v3 snooping
32. Static multicast forwarding
33. 802.1x port authentication

34. Port Security
35. Static MAC filtering/forwarding
36. Multiple RADIUS servers
37. Multiple TACACS+ servers
38. AAA by RADIUS / TACACS+
39. SSH v1/SSH v2/SSL
40. Intrusion Lock
41. MAC Freeze
42. ARP Inspection
43. Static IP/MAC/Port binding
44. Policy-based security filtering
45. IEEE 802.1Q VLAN port isolation
46. IP Source Guard
47. Guest VLAN
48. ACL packet filtering
49. PPPoE IA and option 82
50. CPU protection
51. Recovery mechanism for Error disable port/reason
52. Loop guard
53. Dual configuration files
54. Dual images
55. IGMP snooping fast leave
56. IGMP snooping statistics
57. IGMP throttling
58. SNMP v1, v2c, v3
59. SNMP trap group
60. Interface related trap can be enable/disable by port
61. RMON
62. ICMP echo/echo reply
63. Syslog
64. DHCPv6 client and relay
65. NDP: host
66. IPv6 address stateless auto-configuration
67. ZYXEL clustering management
68. Management through console, telnet, SNMP or web management
69. Firmware upgrade by FTP/WEB/TFTP

- 70. Configuration saving and retrieving by WEB/TFTP/FTP
- 71. Support Multiple login
- 72. Configure Clone
- 73. Multilevel CLI
- 74. Daylight Saving
- 75. NTP
- 76. RS232 console port
- 77. Service Access Control Timeout
- 78. IEEE 802.1AB LLDP
- 79. IEEE 802.1AB LLDP-MED
- 80. Authorization on console
- 81. Password encryption
- 82. User access right
- 83. ZYXEL Feature-based private MIB
- 84. Cable diagnostics
- 85. Support Voltage/Temperature Fault Trap
- 86. SNMP trap for error recovery
- 87. MAC aging time
- 88. MAC-based VLAN
- 89. Private VLAN
- 90. MLD snooping proxy
- 91. range-profile
- 92. sFlow

Known Issues

1. Due to chip limitation, ACL Policy Rule does not support the following action.
 - *Replace the 802.1p priority field with the IP TOS value and send the packet to priority queue*
2. Policy rule for ARP/RARP packet, ACL qualify the target MAC address, not the destination MAC address.
3. Due to the Rmirror feature cannot add the RSPAN tag on the frame of CPU port, CPU port can't be mirror by the Rmirror feature.

Table Size & Limitations

1.	802.1Q Static VLANs	4094
2.	Static MAC forwarding entry	256
3.	MAC filtering entry	256
4.	Cluster member	24
5.	Protocol based VLAN entries per port	7
6.	Port-security max address-limit number	16K
7.	Syslog server entry	4
8.	IP source guard entry	512
9.	IP subnet based VLAN entry	16
10.	DHCP snooping binding table	16K
11.	Multicast group	1024
12.	IPv4 ACL entry	128
13.	IPv6 ACL entry	64
14.	DHCP Relay Entry	16
15.	Trunk groups	8
16.	Per trunk group port number	8
17.	MSTP instance	63
18.	MAC-based VLAN	64
19.	VLAN Stacking Selective QinQ entry	128
20.	VLAN Mapping entry	128
21.	Private VLAN entry	8

Firmware Upgrade

The MGS3530-28 series uses FTP to upgrade firmware in run-time through its built-in FTP server. You can use any FTP client (for example, ftp.exe in Windows) to upgrade MGS3530-28 series. The upgrade procedure is as follows:

```
C:\> ftp <MGS3530-28 IP address>  
User : admin  
Password: 1234  
230 Logged in  
ftp> put V4.10(ACEM.0)C0.bin ras-0  
ftp> bye
```

Where

1. User: the management user name, admin by default.
2. Password: the management password, 1234 by default.
3. V4.10(ACEM.X)C0.bin: the name of firmware file you want to upgrade.
4. ras-0: the internal firmware name in MGS3530-28 series(store at 1st ras).
5. ras-1: the internal firmware name in MGS3530-28 series (store at 2nd ras).

Configuration Upgrade

The MGS3530-28 series uses FTP to get/restore configuration through its built-in FTP server. You can use any FTP client (for example, ftp.exe in Windows) to get/restore configuration.

The Get procedure is as follows:

```
C:\> ftp <MGS3530-28 IP address>  
User : admin  
Password: 1234  
230 Logged in  
ftp> get config-0  
ftp> bye
```

The Restore procedure is as follows:

You can restore configuration that previously get from machine.

```
C:\> ftp <MGS3530-28 IP address>  
User : admin  
Password: 1234  
230 Logged in  
ftp> put config_you_named config-0  
ftp> bye
```

Where

1. User: the management user name, admin by default.
2. Password: the management password, 1234 by default.
3. config-0: the internal firmware name in MGS3530-28 series(store at 1st config).
4. config-1: the internal firmware name in MGS3530-28 series (store at 2nd config).

Modifications in V4.10(ACEM.3)C0

[New]

1. Support IGMP Snooping leave proxy
2. [eITS#240501536] Interface bandwidth utilization in "show interface"
3. [eITS#240501534] "show interface vlan" to display vlan membership
4. [eITS#240900749] Customized DHCP option profile

DHCP option profile default4 format example:

Circuit-ID: 0006000100000018

00: binary data follows (1 byte)

06: there will be 6 bytes of binary data (1 byte)

0001 - vlan 1 (2 bytes)

0000 - slot 0 (2 bytes)

0018 - port 24 (2 bytes)

Remote-ID: 082697f6aac2

082697f6aac2 - Switch MAC address

5. [eITS#240901940] Running config autosave

New commands:

running-config auto-write ?

<cr> Enable auto write

<time> Set auto write period in hours, 1~72, Default is 24

For example: Automatically saves the running configuration to flash every two hours.

MGS3520# configure

MGS3520(config)# running-config auto-write 2

MGS3520(config)# running-config auto-write

```
MGS3520(config)# exit
MGS3520#
```

6. [eITS#240900752] "show running | grep"
7. [eITS#240601244] Display spanning tree bridge priority in decimal
8. [eITS#240901082] Display spanning tree port role
9. [eITS#250602057] DHCP snooping database limit

[Change]

1. IGMPv3 also support report proxy.
2. IGMP queries carry the configured 802.1p priority.
3. [eITS#230700294] CLI command "show igmp-snooping" added leave proxy and report proxy settings.
4. [eITS#231001111] Remove poe items in alarm status
5. [eITS#231002173] Web login page
6. [eITS#240501535] [eITS#250400685] Remove "auto" for SFP+ ports, and add "1000-full-Neg"

[Fix]

1. When leave-mode is immediate, the system deletes the port from the group after receiving an IGMP leave from that port, affecting other clients at the same port.
2. vlan-mapping did not work on link aggregations.
3. [eITS#230300287] Password exposure in system log and syslog messages.
4. Zyxel-SI-1464, SSL vulnerabilities
5. [eITS#230900530] SNMP getbulk with max repeat > 50 got incorrect response.
6. [eITS#230800885] 12V voltage reading error.
7. [eITS#230900937] Incorrect ifSpeed and ifHighSpeed value for 10G interfaces.
8. [eITS#231100930] sflow did not send flow samples
9. [eITS#231101603] PPPoE IA failed to forward PADI through LAG
10. [eITS#231200825] Multicast stream blocked after LACP member port down
11. [eITS#240101605] Web config backup cache problem chrome

12. [eITS#240300609] DHCP unicast offer could not be forwarded to link aggregation
13. [eITS#231002173] Cannot login GUI after password change
14. [eITS#240800144] Cable diagnostic showed 4 pairs and 0.0m length in 100M
15. [eITS#250600768] MGS3530-28 SNMPset dot1qPortAcceptableFrameTypes.x; Value 0 timeout
16. [eITS#250601487] Wrong traffic limitation in download direction.
17. [eITS#250800400] Exception after receiving TCP RST during TACACS+ authentication.
18. [eITS#230200860] SFP serial info and DDMI failure at port 26.

Modifications in V4.10(ACEM.2)C0

[Change]

1. [eITS#210900105] Static MAC entries persist under ARP inspection.
2. CVE-2020-1971 and CVE-2022-0778, upgrade openssl from 1.0.2e to 1.1.1n for openssl
[CVE-2020-1971]: A null pointer dereference flaw was found in OpenSSL package. An attacker is able to control the arguments of the GENERAL_NAME_cmp function, could cause the application, compiled with OpenSSL to crash resulting in a denial of service
[CVE-2022-0778]: A security flaw in OpenSSL, which could be used to trigger an infinite loop by crafting a certificate that has invalid elliptic curve parameters

[Fix]

1. [eITS#190900885] Mirror Configuration conflicts with current link aggregation settings
2. [eITS#21070105] MAC flapping prevention
(a) Add an extra broadcast loop-guard packet to avoid the multicast loop-guard packet (01:a0:c5:aa:aa:ab) dropped and cause the loop-guard function not work.
(b) Now the loop-guard control protocol will send the multicast and broadcast loop-guard packet to detect if the loop exist after the loop-guard is enabled.
3. [eITS#211100491] erase running-config interface port-channel <port-list>, will not add the port back to the default vlan
4. [eITS#211100495] After typing command "MAC-freeze" on the LACP port, the system doesn't display the warning message and the command was not blocked
5. [eITS#211100497] The behavior of ARP inspection become strange when it working with the link aggregation (LAG/LAP) run on the downlink port.
6. [eITS#220600144] How to set Classifier using SNMP.
[Symptom] can't set Classifier via SNMP MIB
7. [eITS#220501059] Add RADIUS Privilege level 15 and map it to level 14

8. [eITS#220700676] PADO packets bounced back
9. [eITS#220601398] DHCP problem when DHCP snooping table is full.
10. [eITS#220800980] System crashed due to SNMP bulk set to classifier mib.
11. [eITS#220800806] System crashed after receiving abnormal DHCP packets.
12. [eITS#220800152] broken ARP table help page link.
13. [eITS#220600144] System crashed due to long policy command.
14. Zyxel-SI-1286, DOS attach via abnormal LLDP PDUs with TLVs recording length 0.
15. Zyxel-SI-1434, DOS attach via http request carrying manipulated referrer URL.

Modifications in V4.10(ACEM.1)C0

[Change]

1. [eITS#220601398] DHCP snooping table too small with 16K

[Fix]

1. [eITS#220600144] How to set Classifier using SNMP.
2. [eITS#211100491] The command "erase running-config interface port-channel <port-list>" will not add the port back to the default VLAN.
3. [eITS#220501059] Add TACACS+ or RADIUS server return Privilege level 15 and map it to level 14
4. [eITS#211100497] ARP inspection not work with link aggregation client can't ping DHCP server after getting IP and is added in arp inspection filter list with reason: port

MGS3530# show ip source binding

MacAddress	IpAddress	Lease	Type	VLAN	Port
00:16:d3:2f:12:c2	192.168.1.161	1d23h59m55s	dhcp-snooping	1	1

MGS3530# show arp inspection filter

Filtering aging timeout : 300

MacAddress	VLAN	Port	Expiry (sec)	Reason
00:16:d3:2f:12:c2	1	2	252	Port

Modifications in V4.10(ACEM.0)C0

[New]

1. Initial release for MGS3530-28