Firmware for TN-5500A Series (TN-5516A, TN-5518A) Release Notes

Version: v3.13	Build: FWR_TN5516A_18A_V3.
Release Date: May 23, 2024	

Applicable Products

N/A

Supported Operating Systems

N/A

New Features

N/A

Enhancements

• Turbo Ring V2 can now pass through LACP trunk ports when Dynamic Ring Coupling (DRC) is enabled.

Bugs Fixed

• Vulnerability issue: MPSA-230203 including CVE-2005-4900
• Vulnerability issue: CVE-2015-9251
• Vulnerability issue: CVE-2019-11358
• Vulnerability issue: CVE-2020-11022
• Vulnerability issue: CVE-2020-11023

Changes

N/A

Notes

N/A

Version: v3.12	Build: N/A
Release Date: Mar 01, 2024	

Applicable Products

N/A

Supported Operating Systems

N/A

New Features

• Added support for DHCP Option 61 - Option 61 in DHCP is a client identifier that is sent by all DHCP clients in the DHCP packet 1. It is used to identify a DHCP client uniquely and to configure manual bindings, For now, the value of 2. DHCP Option 61 is user-defined.
• Trunk ports can support two redundant protocols - RSTP and Turbo Ring v2.
• Added support for Secure Copy Protocol (SCP) for firmware upgrade, event log, and configuration backup transmissions.

Enhancements

• Enhanced the RADIUS login functionality:
  - Added support for additional authentication types: CHAP, MSCHAPv2.
  - Added support for a 2nd RADIUS authentication server for redundancy purposes.
  - Added a new event log for successful logins.
• Users can set DeviceIP for the trunk port.
• SNMP v3 now supports AES encryption.
• Static multicast and IGMP now share one MAC table to give users more flexibility and higher capacity for their applications.
  - TN-4500A has a total of 512 MAC entries shared between static multicast and IGMP.
  - TN-5500A has a total of 256 MAC entries shared between static multicast and IGMP.
• The web interface can now be accessed through mirror ports.
• The TN-5508A and TN-5510A will now assign the new PCP based on the port priority as configured in the QoS settings.

Bugs Fixed

• Importing a configuration file via TFTP when using DHCP Option 66 & 67 would fail.
• Even if a device and gateway are in the same subnet, users can not assign an IP address (*.*.*.255) to the device using the SetDeviceIP function.
• From the WEB GUI, users can't set an IP address(0.0.0.0) to the DNS and NTP server when using the SetDeviceIP function.
• ACL rules may sometimes make STP unstable and cause network looping.
• Configuring the syslog server domain name using SNMP or MXconfig would fail.
• When IGMP is enabled, the device is unable to forward unknown IP multicast packets.
• CVE-2022-0778: OpenSSL vulnerability.
• UDP/TCP ports remain open even when the relevant network functions that use these ports are disabled.
• The device fails to synchronize with the NTP server periodically if the device has been running for a certain period or after restarting.
• The IGMP Static querier port does not work as intended.
• When IGMP is disabled but a filter for unknown multicast packets is enabled for the Multicast Forwarding Behavior (MFB) function, the device will still forward some IGMP packets.
• The displayed trunk port TX and RX packet counters are inaccurate.
• When using the “show MAC table” CLI command, trunk port entries are missing from the table.
• When users configure the Dual Homing primary and backup ports via SNMP, there is no message to inform users when the settings have reverted to their default values again.

• When acting as a DHCP server, the device will drop DHCP requests from clients using Option 61.
• When consecutively enabling or disabling the Turbo Ring Coupling function, the device will occasionally lose packets on the ring port.
• Turbo Ring slave devices do not correctly adjust their status after recovering from a power failure.
• Cybersecurity vulnerability: MPSA-230307

Changes

• For security reasons, multicast packets will be blocked if the ingress port is not authenticated by 802.1x.
• To improve interoperability with Moxa devices, the “EAP-MD5 Extra Data' field will no longer be used for 802.1x authentication.

Notes

• Secure Copy Protocol (SCP) encrypts file transfers between the switch and the remote host and required considerably more computing power. Therefore, we do not recommend using SCP to transfer event logs as the high volume of logs may cause the web interface to become unresponsive.
• If users want to import a configuration file through DHCP Option 66 & 67, the switch will only support the configuration file format (.ini file) exported via the switch web interface.
• When importing a configuration file through DHCP Option 66 & 67, the following information can not be updated: AUTOIP, IPAddress, Netmask, Gateway, DNSIP, DNSIP1, PV6AddressPrefix, DHCP_FILTER_ENABLE_(port index), HCPRetryPeriod, DHCPRetryTimes, OPTION61_ENABLE, OPTION61_TYPE, OPTION61_USER_DEFINED_CLIENT_ID.
• Static multicast and IGMP static querier port cannot operate at the same time. After configuring a static multicast group, the IGMP static querier port will not forward to that multicast group anymore.
• If users enable Multiple Spanning Tree Protocol (MSTP) and GARP VLAN Registration Protocol (GVRP) at the same time, MSTP convergence would be affected. Therefore, we do not recommend enabling both these functions at any given time.
• From now on, upon receiving a DHCPDISCOVER message with a unicast flag from a DHCP client, the switch will respond to the DHCP client with a DHCPOFFER message via Layer 2 unicast.
• With firmware v3.12, the following functions and protocols are no longer supported:
  - Industrial protocols: Modbus, EtherNet/IP
  - IEEE 1588 PTP
  - Turbo Chain v1
  - TLS v1.0, v1.1

Version: v3.10	Build: N/A
Release Date: Nov 16, 2021	

Applicable Products

TN-5516A, TN-5518A

Supported Operating Systems

N/A

New Features

N/A

Enhancements

• Added support for TLS v1.2.

Bugs Fixed

• If a configuration conflict occurs during firmware upgrading, the device password is unexpectedly changed.
• If loop protection and redundancy protocols are working simultaneously, the set port stp state recorded by the software is different from the actual driver setting.
• When exporting the configuration through the console, the device will reboot.
• When logging in using an account name longer than 8 characters, the device will reboot
• Accounts with the "User" privilege level are able to obtain the password information of administrator-level accounts through the CLI.
• Exported log files are incomplete or show incorrect information.
• If an event log is produced during a firmware upgrade, the firmware upgrade process will fail.

Changes

• Removed the Menu mode from the CLI console.

Notes

N/A

Version: v3.9	Build: 20021315
Release Date: May 06, 2020	

Applicable Products

TN-5516A, TN-5518A

Supported Operating Systems

N/A

New Features

N/A

Enhancements

N/A

Bugs Fixed

• The timestamp (hour) is different from the original setting after the device is rebooted.
• If the RTC battery is fully discharged, the firmware doesn't correctly conduct the RTC battery recharge process.

Changes

N/A

Notes

N/A

Version: v3.8	Build: 20101414
Release Date: Oct 01, 2019	

Applicable Products

TN-5518A, TN-5516A

Supported Operating Systems

N/A

New Features

• Added support for Security Guideline level 2.
• Added DNS Server functionality.

Enhancements

• Added compatibility drivers for new hardware components (Flash/RTC/CPU).

Bugs Fixed

• A Router Alert Option is added to all IGMP packets.
• The event log is unable to display dates after February 2038 (Y2K 2038).
• The “Set Device IP” function in the Web UI rejects valid IP addresses that contain the value "255".
• Under certain conditions, the Option-82 Relay function sends duplicate unicast DHCP Discover packets.
• The device cannot be accessed through HTTP/HTTPS after changing the device IP.
• The NTP query interval does not function properly.
• Incorrect language and information in the UI.

Changes

• The UI can now display both original (5 digits) and extended device serial numbers (12 digits).
• DHCP Option-82 Relay & Set Device IP now function per port.

Notes

N/A

Version: v3.7	Build: N/A
Release Date: May 17, 2016	

Applicable Products

N/A

Supported Operating Systems

N/A

New Features

NA

Enhancements

NA

Bugs Fixed

Fixed PoE user interface settings issue.

Changes

NA

Notes

N/A