Firmware for TN-4500A Series Release Notes

Version: v4.2	Build: 26040215
Release Date: Apr 10, 2026	

Applicable Products

TN-4500A Series

Supported Operating Systems

N/A

New Features

Not applicable.

Enhancements

• Updated DHCP Client MAC verification for LLDP Chassis ID (Subtype 7) compatibility.

Bugs Fixed

• In an RSTP ring architecture, some switches do not receive discovery packets, preventing MXconfig from discovering all devices.
• The DHCP Client sometimes fails to obtain an IP address from the DHCP server via the switch's DHCP Relay Agent.
• [Vulnerability] CVE-2024-12297: Frontend Authorization Logic Disclosure.
• [Vulnerability] CVE-2024-9404: denial-of-service or service crashes.
• [Vulnerability] CVE-2002-20001: Resource Exhaustion Vulnerability in Diffie-Hellman Key Exchange Protocol.

Changes

Not applicable.

Notes

Not applicable.

Version: v4.1	Build: 25121815
Release Date: Dec 31, 2025	

Applicable Products

TN-4500A Series

Supported Operating Systems

N/A

New Features

N/A

Enhancements

N/A

Bugs Fixed

• After upgrading the device to firmware v4.0, the Fault LED remains constantly on.
• The system unintentionally resolves the DNS IP information and redirect clients to this host IP address to establish the connection.

Changes

• The "Set Device IP" function now operates even when ACCU (Auto Config Change Update) is enabled and the SCP server has not yet connected.

Notes

N/A

Version: v4.0	Build: 25091717
Release Date: Oct 15, 2025	

Applicable Products

TN-4500A Series

Supported Operating Systems

N/A

New Features

• Added support for the Duplicate IP Detection function.
• Added support for the Custom Default function.
• Added support for the Conditional Auto IP Assignment and Train Information functions.
• Added support for the Auto Configuration function.
• Added support for the User Privilege function.
• Added support for the Process and Status Report function.
• Added support for the Auto Config Change Update function.
• Added support for the DHCP Server Option 66/67 function.
• Added support for the ITxPT function.
• Added support for the RSPAN function.

Enhancements

• The switch will now reply to DNS query packets with Additional Records of the OPT type.
• Increased the maximum number of MAC address table entries to 2048.
• Users can now enable or disable IGMP functionality on individual ports.
• Added an action progress indicator icon to the web interface.
• Added a delay option to the Syslog settings to delay sending logs to the Syslog server during startup.
• Added the Custom Encryption Key option to Configuration Backup/Restore.
• Added a Configuration Name option to Configuration Backup/Restore.
• Added an Extended mode option to Fault LED.
• Added a Warning notification option for the Traffic Overload T(X) event.
• Added support for the SNMP Get lldpRemManAddrTable(.1.0.8802.1.1.2.1.4.2) object to retrieve the remote management IP address.
• Added a Log Server field (DHCP Option 7) to Automatic Set Device IP by DHCP/BootP/RARP for sharing log server information.

Bugs Fixed

• The Dynamic Ring Coupling function cannot operate correctly when using Turbo Ring v2 with LACP Trunk ring ports.
• Unplugging a single cable from an LACP Trunk port on a Turbo Ring V2 ring switch will briefly cause both the Dynamic Ring Coupling primary and backup coupling ports to enter a forwarding state simultaneously.
• Clicking "ABC import" in the web user interface will cause the device to reboot.
• The PoE behavior does not align with the corresponding configuration on the device.
• When any redundant protocol (RSTP, Turbo Ring V2, Dynamic Ring Coupling, MSTP) is enabled, importing a configuration file via CLI will temporarily cause a network loop.
• The DSCP value shown on the ToS/DiffServ Mapping page is incorrect.
• When the SNTP Client is enabled, the switch will incorrectly record a "The time server query timed out" log entry every time the device reboots.
• Importing a large number of ACL rules may cause the device to malfunction.
• If a trunk group is configured on the device, when importing a configuration file that contains static multicast entries for the trunk group, the import process will fail.

• Disabling the HTTP interface via the CLI will also disable the HTTPS interface.
• The DHCP filtering object is missing from the MIB file for TN-4528A models.
• The DHCP Server does not work properly on Trunk group interfaces.
• If the configuration file imported via CLI disables the HTTP interface, any subsequent reboot command issued through the CLI will fail.
• The device may reboot after receiving a large volume of DHCP client requests.
• A specific sequence of operations causes the event log to display an out-of-range port number (65536) when logging DHCP client information received by the switch.
• After importing a configuration file via the web interface, the Power Allocation value is set incorrectly.
• After upgrading the TN-4516A-2GTX-2GFC-WV (AFC) to firmware version v3.13, the LED indicator status displays incorrectly, although network communication remains normal.
• After importing a configuration file, the assigned IP address is configured incorrectly, causing the switch to become inaccessible.
• Enabling or disabling the coupling port for Turbo Ring V2 may result in the loss of packets on Ring 2.
• Enabling or disabling the Accessible IP feature by importing a configuration file will fail.
• An excessively large DNS server packet that exceeds the device's defined array size can lead to system instability.
• The SNMP MIB file cannot be successfully imported into the MIB Explorer Pro tool.
• After importing the configuration file via web UI or CLI, the PoE port power allocation value displayed on the web page is incorrect.
• After configuring RSTP and enabling any port, the event log will record abnormal information.
• SNMP bulk polling on TN-4528A models only retrieves data for 20 ports.
• When the device has 512 static multicast entries configured, importing a configuration file may cause the device to reboot unexpectedly.
• Importing a configuration file via the web interface to change the VLAN membership for all 512 static multicast entries fails to update the MAC address table correctly, although no error is reported during the import process.
• Importing a configuration file via the CLI to change the VLAN membership for all 512 static multicast entries prompts an error.
• If Daylight Saving Time (DST) is enabled in the system time settings, after rebooting the switch the system time will be moved up by an extra hour unless it syncs with an NTP server again.
• When a user imports a configuration file via the web interface that contains more than 512 static multicast entries, the web interface fails to display an error message or halt the import process.
• The switch still responds to NTP symmetric mode packets when the NTP Server function is disabled.

• When a device has already dynamically learned multicast addresses via IGMP, importing a configuration file that sets static multicast addresses may fail to apply the new static entries.
• The system time year value changes to 2045 after performing a cold start.
• [CVE-2025-1679] Stored Cross-site Scripting.
• [CVE-2025-1680] Host Header Injection.
• [CVE-2024-7695] Out-of-bounds Write.
• [CVE-2024-9137] ICMP Timestamp Request Remote Date Disclosure.

Changes

• System will disregard IGMPv3 joins for multicast groups within the ranges 224.0.0.x - 239.0.0.x and 224.128.0.x - 239.128.0.x.
• Adjust the way the switch (acting as an NTP Client) handles received Kiss-o'-Death (KoD) packets.
• The measurement unit for the NTP/SNTP DNS server timeout event log has been changed from milliseconds to seconds.
• Spec change for Set Device IP function.
• MAC table implementation changes from SVL (Shared VLAN Learning) to IVL (Independent VLAN Learning).
• DHCP Option 61 MIB OID changes from 84 to 90.
• Packets with a destination IP address in the 224.0.0.X range which are not IGMP will be forwarded on all ports.
• The System Name is now displayed on the WEB UI.
• The ineffective CLI command mcast-filter forward-all has been removed.
• The IGMPv2 Join mechanism has been adjusted.
• The IGMPv2 Leave mechanism has been adjusted.
• Firmware version 4.0 now supports the import of configuration files that include a config header.

Notes

• Firmware v4.0 is incompatible with configuration files from older firmware versions. When restoring the configuration using an ABC-01 Series device, make sure the configuration saved on the ABC-01 was created using firmware v4.0. Importing an older firmware configuration file may cause instability.
• To forward multicast streams for IGMPv2 Join requests to member ports in the 225?239.0.0.x or 225?239.128.0.x address ranges, you must manually configure the corresponding MAC address as a static multicast entry.
• While the device allows you to configure and display a unique querier port for each VLAN, the device cannot forward the multicast stream to the corresponding querier port for that specific VLAN due to a MAC chip limitation.
• When a VLAN and a corresponding Static Multicast rule are configured, deleting the VLAN first before deleting the multicast rule will fail to clear the associated entry from the MAC address table

due to a MAC chip limitation. After restarting the device, the MAC address table entries will be displayed correctly.
• If you encounter issues where you cannot receive packets on the RSPAN Destination Port (DP) in complex setups involving IGMP, RSPAN, and Static Multicast, please consult the following recommendations to prevent errors. When using RSPAN to monitor multicast streams on a device with Static Multicast configured and IGMP enabled, make sure you configure the RSPAN DP and the Designated Trunk Ports (DTP) correctly:
  - For unknown multicast streams: Configure the RSPAN DP and DTP as the Static Multicast Querier to receive the traffic.
  - For known static multicast streams: Configure the RSPAN DP and DTP as a Static Multicast Join member port to receive the traffic.
• To ensure all features work correctly, firmware v4.0 must be used with the latest versions of MXconfig (v3.4) and MXview One (v1.6). Using older versions may cause some functionality to be unstable or unavailable.

Version: v3.13	Build: FWR_TN4500A_V3.13_Build_24041711
Release Date: Apr 17, 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

TN-4500A Series

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.
• Added support for QoS for ACL rules.

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.
• Enhance DNS functionality including:
  - Added support for DNS reverse lookup.
  - DNS now supports multiple domain name mapping to the same IP address.
• 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 switch will now assign port priority for untagged packets based on 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.
• High volumes of DNS queries may cause the device to reboot.
• Configuring the syslog server domain name using SNMP or MXconfig would fail.
• Configuring the 1st DNS server IP address via SNMP 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.
13 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: v3.9	Build: 21070111
Release Date: Jun 30, 2022	

Applicable Products

TN-4524A-16PoE-WV-CT-T, TN-4524A-16PoE-WV-T, TN-4528A-16PoE-2GPoE-2GODC-WV-CT-T, TN-4528A-16PoE-2GPoE-2GODC-WV-T, TN-4528A-16PoE-2GPoE-2GTXBP-WV-CT-T, TN-4528A-16PoE-2GPoE-2GTXBP-WV-T, TN-4528A-16PoE-4GPoE-WV-CT-T, TN-4528A-16PoE-4GPoE-WV-T

Supported Operating Systems

N/A

New Features

N/A

Enhancements

N/A

Bugs Fixed

• If a configuration conflict occurs during firmware upgrading, the device password is unexpectedly changed.
• Some locked fields on the VLAN page in the web UI are editable when loading the page for the first time.
• If an event log is produced during a firmware upgrade, the firmware upgrade process will fail.

Changes

N/A

Notes

N/A

Version: v3.8	Build: 21011813
Release Date: Jan 27, 2021	

Applicable Products

TN-4524A-16PoE-WV-CT-T, TN-4524A-16PoE-WV-T, TN-4528A-16PoE-2GPoE-2GODC-WV-CT-T, TN-4528A-16PoE-2GPoE-2GODC-WV-T, TN-4528A-16PoE-2GPoE-2GTXBP-WV-CT-T, TN-4528A-16PoE-2GPoE-2GTXBP-WV-T, TN-4528A-16PoE-4GPoE-WV-CT-T, TN-4528A-16PoE-4GPoE-WV-T

Supported Operating Systems

N/A

New Features

N/A

Enhancements

N/A

Bugs Fixed

• When loop protection is enabled, end devices cannot be accessed after the link status has changed (e.g., port connected/unplugged).
• When exporting the configuration through the console, the device will reboot.

Changes

N/A

Notes

N/A

Version: v3.7	Build: 20113013
Release Date: Nov 30, 2020	

Applicable Products

TN-4524A-16PoE-WV-CT-T, TN-4524A-16PoE-WV-T, TN-4528A-16PoE-2GPoE-2GODC-WV-CT-T, TN-4528A-16PoE-2GPoE-2GODC-WV-T, TN-4528A-16PoE-2GPoE-2GTXBP-WV-CT-T, TN-4528A-16PoE-2GPoE-2GTXBP-WV-T, TN-4528A-16PoE-4GPoE-WV-CT-T, TN-4528A-16PoE-4GPoE-WV-T

Supported Operating Systems

N/A

New Features

• Added support for TN-4500A Series devices with hardware revision v2.x.

Enhancements

• Added support for TLS v1.2.

Bugs Fixed

• 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 logging in using an account name longer than 8 characters, the device will reboot.
• When using the MSTP protocol in ring topologies, a random device in the topology will reboot several times.
• When exporting the configuration through the console, the device will reboot.
• MDI/MDIX settings are not applied properly.
• The DHCP filter behaves abnormally when importing ACL configurations.
• DHCP clients still receive an IP address from ports which have the “Drop Server” filter function enabled.
• Exported log files are incomplete or show incorrect information.
• Accounts with the "User" privilege level are able to obtain the password information of administrator-level accounts through the CLI.
• CPU may overload which can cause the device to reboot.
• CPU may overload when the link status changes on multiple ports.

Changes

1. Removed the Menu mode from the CLI console.
?

Notes

N/A

Version: v3.6	Build: 19011009
Release Date: Jun 06, 2019	

Applicable Products

TN-4524A, TN-4528A

Supported Operating Systems

N/A

New Features

• Includes Security Guideline level 2, DNS Server, ACL, and DHCP Filter functions.

Enhancements

• Router Alert option on all IGMP packets.

Bugs Fixed

• Y2K 2038 issue.
• Web UI does not accept valid device IP addresses with 255 values in the Set Device IP field..
• DHCP discovery issue for duplicate unicast in Option 82 relay mode.
• Cannot access device using HTTP/HTTPS after IP is changed.
• NTP query interval issue.

Changes

• Changed the DHCP option-82 Relay and Set Device IP settings for all ports.

Notes

N/A

Version: v3.5	Build: 17072820
Release Date: Jan 17, 2019	

Applicable Products

N/A

Supported Operating Systems

N/A

New Features

• Add Router Alert option

Enhancements

N/A

Bugs Fixed

• ABC-01 operation issue
• Static Port Lock issue
• Non-querier port forward Multicast stream

Changes

N/A

Notes

N/A