Firmware for TN-4500A Series Release Notes

Version: v3.13	Build: FWR_TN4500A_V3.
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