Cambium Networks

Contents

Contents ... 1

Introduction ... 2

Supported Platforms ... 2

What’s New in 2.1 ... 3

CLI Improvements/Changes ... 4

Web GUI Improvements/Changes ... 4

cnMaestro-Related Improvements/Changes ... 5

Defect Fixes / Enhancements ... 5

Supported Features in cnMatrix 2.1 ... 7

Known Issues (Release 2.1) ... 9

Feature Notes ... 10

Limitations ... 11

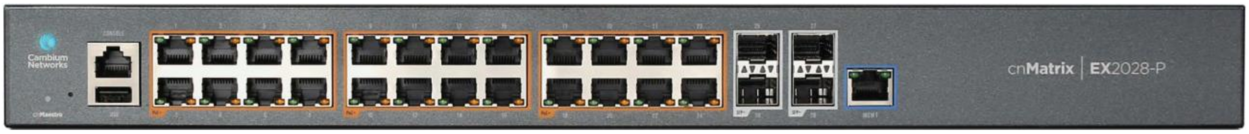
Introduction

This document provides information for the Cambium Networks cnMatrix switch release 2.1. The recommendations, technical data, configurations and statements in this document are believed to be reliable and accurate, but are presented without implied or express warranty. Users must take full responsibility for their applications of any product specified in this document. The information in this document is proprietary to Cambium Networks Ltd.

Supported Platforms

- cnMatrix EX2028

- cnMatrix EX2028-P



- cnMatrix EX2010

- cnMatrix EX2010-P

Attention: Certain features may not be available on this product line and will be called out explicitly where not applicable.

What's New in 2.1

The following features have been added in version 2.1:

- **OSPFv2** (Open Shortest Path First) ➔ dynamic routing support.
- **RIPv1/v2 (Routing Information Protocol)** ➔ dynamic routing support.
- **Dynamic ARP Inspection**➔ security feature that rejects invalid and malicious ARP packets.
- **USB** support ➔ provides access to a flash storage device. An USB stick can now be used for software download as well as a storage medium for configuration saving or restoring.
- **Reload** function can be used to go back to a known good configuration if an error is made while actively configuring the switch that causes a remote user to lose connectivity. The Reload feature loads a timer that causes the switch to automatically reboot which causes the switch to return to the previously saved configuration. Once the new configuration is finished and tested, the reload timer can be cancelled. This feature applies to SSH sessions, the web-GUI, and cnMaestro.
- The **Media Endpoint Discovery** extensions have been added to the **LLDP** protocol, which provides the following facilities:
  - Discovery of network policies – allows the network administrator to set automatically-discoverable policies for phones, video streaming and video conferencing devices. A policy consists of a VLAN ID, a DSCP code point and a dot1p priority for the end device to use.
  - Location discovery – support for Emergency Location Identification Number (ELIN).
  - Extended Power-over–Ethernet (PoE) management.
  - Inventory management – supports tracking of deployed network devices.
- **Do** command➔ allows an administrator to perform any Privileged mode CLI command while in the Configuration and Interface Configuration modes: `do <any command>`
- **Policy Based Automation (Auto Attach) extensions** have been added:
  - Rule capabilities have been extended to include support for MAC-based device detection (MAC OUI, full MAC address, MAC address range) as well as LLDP IPv4 management address matching.
  - Action support has been enhanced to allow policy-based updates to port default user priority, QoS trust mode and PoE priority settings. Dynamic uplink VLAN membership updates are available as well.
  - Enhanced policy capabilities, including support for dynamic tagged and untagged VLAN membership updates and the full range of switch port mode options, are enabled. Automatic and customizable port description updates related to PBA policy status have been added.
  - Push policy support, allowing select Cambium devices to securely push PBA policy criteria to a cnMatrix switch for zero-touch provisioning, is available.
- **TLS 1.2** support has been added for HTTPS Server. Accessing the WEB GUI using HTTPS is now supported for the latest web browsers: Google Chrome, Mozilla Firefox, Internet Explorer and Microsoft Edge.
- **New Software file format**
  - Starting with cnMatrix release 2.1, a new file format is used for cnMatrix software distribution. The new format is a .tar.gz archive and replaces the 2.0.5 .img format.

- The new .tar.gz file contains an .img file and its signature. From 2.1 on, software upgrade/downgrade will check the authenticity of the software image.
- The cnMatrix 2.1 agent will accept only a .tar.gz file for software upgrade or downgrade.
- To upgrade from cnMatrix 2.0.5 to 2.1, use 2.1 .img file posted on the support site. The following files are available on the support site:
  - **cnMatrix-EX2K-2.1-r5.img** - to be used for upgrading from 2.0.5 to 2.1.
  - **cnMatrix-EX2K-2.1-r5.tar.gz** – new file format containing an .img file and its signature.
  - **cnMatrix-EX2K-2.0.5-r2-downgrade.tar.gz** – to be used for downgrading from 2.1 to 2.0.5.
- To upgrade from 2.0.5 to 2.1, please use the following CLI command:
  - `download agent tftp://<TFTP Server Address>/cnMatrix-EX2K-2.1-r5.img`
- To downgrade from 2.1 to 2.0.5, please use the following CLI command:
  - `download agent tftp://<TFTP Server Address>/cnMatrix-EX2K-2.0.5-r2-downgrade.tar.gz`
- To downgrade from 2.1 to 2.0.5 using cnMaestro:
  - Not supported in the current cnMaestro release 2.2.1

CLI Improvements/Changes

The following parameters have been changed in the commands for the HTTPS feature:

- The `secure { crypto key rsa [usage-keys (512|1024)]}` command has been changed to `secure { crypto key rsa [usage-keys (512|1024|2048)]}`.
- The crypto parameter configures the usage key (512, 1024 or 2048).
- The following command has been removed `version {all | ssl3 | tls1}`. For security reasons, only TLS 1.2 is supported.

The `show interfaces transceivers` command has been added to display vendor information regarding inserted transceivers.

The following **Policy Based Automation (Auto Attach)** CLI commands have been added:

- New rule type options exposed `auto-attach rule`.
- New action selections defined `auto-attach action` and `show` output updated.
- Global `update-port-description` option provided.
- Enhanced interface status and statistics display output `show auto-attach interface`, `show auto-attach interface statistics`.

The default host name is generated using the last 6 digits of the base MAC address (e.g: EX2010P-FEB436).

Web GUI Improvements/Changes

- The following menu items have been added in the Web GUI: RIP, OSPF, Reload, ACL&QoS, PoE, Dynamic ARP Inspection, Mirroring, DHCPv6 Client, Route Redistribution.
- The **Last Reload Reason** and the **Manufacture Date** fields have been added to the **System Information** page.

- The **Image Download** menu item has been renamed to **Software Upgrade**.
- The **USB** options have been added in the **Upgrade From** field on the **Software Upgrade** page.
- A port **Description** column, has been added to the Web GUI for all port-related display pages.
- The **Policies Applied**, **Policies Expired** and **Policy Errors** columns have been moved from the **Auto Attach Interface Settings** page to the new **Auto Attach Interface Statistics** page.
- The following columns have been added to the **Auto Attach Interface Settings** page:
    - Message Authentication Key
    - Authentication TLV.
    - Reset Settings
- The **Default Auto Attach Settings** and the **Update Port Description** fields have been added on the **Auto Attach Basic Settings** page.
- The following options have been added to the **Rule Type** drop-down on the **Auto Attach Rule Settings** page: MAC OUI, MAC Full Address, MAC Address Range and LLDP IPv4 Management Address.
- The **Default User Priority**, **QoS Trust Setting**, **Uplink List** and **PoE Priority Setting** fields have been added on the **Auto Attach Action Settings** page.
- The following options have been added to the **Rule Type** drop-down on the Auto Attach Policy Settings page: MAC OUI and MAC Full Address.
- Policy Based Automation pages include inline tool-tip pop-ups as well as page-specific help tips to assist with administrator data configuration.
- The following features have been added to the **Statistics** menu item: RIP, OSPF and Policy Based Automation.

cnMaestro-Related Improvements/Changes

- cnMaestro settings are available through the Web GUI.
- The output of the `show cnmaestro` command has been improved to provide details about the last action performed by the cnMaestro management agent.
- CLI commands can be executed directly via Tools->Debug in cnMaestro.
- Hardware version and manufacturing date information have been added to the cnMaestro interface (requires cnMaestro 2.3.0).
- Display of per-port PoE consumption added (requires cnMaestro 2.3.0).
- Device name can be configured through the Configuration Tab in cnMaestro and is synchronized with the cnMatrix switch (requires cnMaestro 2.3.0).
- **Ping**, **DNS Lookup** and **Traceroute** through cnMaestro Tools->Network Connectivity are supported (requires cnMaestro 2.3.0).

Defect Fixes / Enhancements

- The following changes have been performed for Access mode ports (1089):
    - An Access mode port must be an untagged member in a single VLAN.
    - The PVID of an Access mode port must be equal to the VLAN ID of the VLAN to which it belongs.

    - The Acceptable Frame Type of an Access mode port will be automatically configured to "untaggedAndPriorityTagged".

> Notes: Any attempt to change the PVID to a value different from the VLAN ID of the single VLAN to which the Access mode port currently belongs will fail.

- The following enhancements have been implemented for Policy Based Automation feature**:**
    - Support for the standard Management Address TLV is available.
    - Device detection based on the MAC address data is supported.
    - With the initial cnMatrix release 2.0, administrator operations may supersede PBA-associated (i.e., dynamic) actions. For example, an administrator can manually update dynamic VLAN associations or update a PVID if required. PBA will not block administrator requests. Starting with cnMatrix version 2.1, the administrator can no longer alter most settings that have been updated by PBA. Administrator operations on ports that are associated with an active PBA policy are limited to those not potentially under PBA control. This means that VLAN membership updates are blocked as are PVID and switch port mode modifications. Furthermore, VLANs that are dynamically created though PBA operations are owned by PBA and can't be manipulated (e.g., deleted, associated with other ports) by the user. Administrator modifications to these settings are permitted once PBA settings are cleared from the port.
    - Traffic associated with the PVID egresses the switch as untagged traffic (i.e., the port is made an untagged member of the VLAN).
    - PBA support for all switch port mode options (i.e., Access/Hybrid/Trunk) and dynamic switch port mode updates is available. The PBA support for transitioning to/from Access and Trunk port modes has the following restrictions/behavior:
        - Access
            - Action data with a single VLAN and a matching PVID value must also be specified.
            - All VLANs associated with the applied PBA policy interface are removed (only the single action VLAN is associated with the port) while the policy is active. The removed VLAN memberships are reinstated when the PBA policy is no longer active on the port.
        - Trunk
            - Action data can include a VLAN list. A PVID can't be specified.
    - The QoS Trust mode (i.e., Trust 802.1p/Trust DSCP/Untrusted) for a port can be updated based on device discovery. The QoS Trust mode setting is restored to the previous statically configured value during the device cleanup phase.
    - The default port 802.1p user priority value (0..7) can be updated based on device discovery. The default port 802.1p user priority value setting is restored to the previous statically configured value during the device cleanup phase.
    - The administrator can identify up to four device ports to act as PBA uplinks. VLANs (newly created or existing) that are applied to the port on which the matching device was detected are also associated with the uplink ports. The VLAN membership update remains in effect while the related PBA policy is active. **Uplink ports must be operating in hybrid switch port mode to be valid. Uplinks are identified using the interface type and slot/port naming convention (e.g., 'Gi0/5,Ex0/1'). An action that includes uplink data must also include VLAN data for port membership updates.**

- The PoE priority setting (i.e., Critical/High/Low) for a port can be updated based on device discovery. The PoE priority setting is restored to the previous statically configured value during the device cleanup phase. Requesting this action returns an error on devices that are not PoE-capable.

Note: When using the Policy Based Automation (PBA) feature to support automated device detection and switch configuration, please take advantage of the new MAC address device detection option carefully. Standard MAC address learning can cause addresses to temporarily migrate across a flat network. MAC-based PBA policies can thus match addresses of devices that aren't directly connected to the cnMatrix. If this is not the intended behavior, disabling PBA on device uplinks can prevent any issues from arising. Enhancements allowing the user to customize the PBA MAC address-based device detection behavior will be available in the next release.

Supported Features in cnMatrix 2.1

The below list is a high level summary of cnMatrix 2.1 features. For more detailed information regarding cnMatrix supported features, please access cnMatrix User Guide.

Feature	Release 2.0.5	Release 2.1
Industry-standard Command Line Interface (CLI)	Yes	Yes
Web Management	Yes	Yes
cnMaestro Cloud-based Management	Yes	Yes
Zero-touch Remote Provisioning	Yes	Yes
SNMPv1/v2c/v3	Yes	Yes
Telnet Client/Server	Yes	Yes
Out-Of-Band Ethernet Management	Yes	Yes
SSH/SSH v2	Yes	Yes
DHCP Client, Server	Yes	Yes
Local/Remote Syslog	Yes	Yes
System Resource Monitoring	Yes	Yes
802.1Q VLAN and Trunking Support	Yes	Yes
802.1d STP, 802.1w RSTP, 802.1s MSTP	Yes	Yes

PVRST (Per VLAN RSTP)	Yes	Yes
802.1p Quality of Service	Yes	Yes
ACL QoS: Mapping/Marking ToS/DSCP, 802.1p, Priority Queue	Yes	Yes
Inbound Traffic Policing, and Outbound Traffic Shaping	Yes	Yes
Storm Control	Yes	Yes
Flow Control Per Port	Yes	Yes
802.1ab Link Layer Discovery Protocol (LLDP)	Yes	Yes
802.3ad Link Aggregation	Yes	Yes
Policy-Based Automation with Dynamic Configuration	Yes	Yes
IGMP Snooping v1/v2	Yes	Yes
IGMP Snooping Proxy	Yes	Yes
Private VLAN Edge	Yes	Yes
802.3af/at	Yes	Yes
Port Mirroring: Port-based, ACL-based	Yes	Yes
SNTP	Yes	Yes
Port Statistics	Yes	Yes
RMON	Yes	Yes
Routing Between Directly Connected Subnets	Yes	Yes
Routed Interfaces	Yes	Yes
IPv4 static routes	Yes	Yes
Host routes	Yes	Yes
DHCP Relay	Yes	Yes
802.1x Authentication	Yes	Yes
Radius/TACACS+	Yes	Yes
DHCP Snooping	Yes	Yes

Static MAC	Yes	Yes
IGMP Filtering	Yes	Yes
Locally Managed Username and Password	Yes	Yes
cnMaestro on-premise	Yes	Yes
RIPv1/v2	No	Yes
OSPFv2	No	Yes
USB support	No	Yes
Reset button	Yes	Yes
Dynamic ARP Inspection	No	Yes
LLDP-MED	No	Yes
Reload	No	Yes
CLI ‘do’ command	No	Yes

Known Issues (Release 2.1)

Tracking	Product	Description	Workaround
388	All	DHCP Relay: The switch doesn’t relay all DHCP Release and Renew packets if there are more than 360 DHCP clients connected to the switch.	Use cnMatrix switch to relay DHCP packets for less than 360 DHCP clients.
460	All	LLDP port-id-subtype setting and DHCP server host hardware-type 3 setting are lost after boot.	Reconfigure the settings if they are lost after reboot.
519	All	UP7 traffic not equally serviced if received from 2 different ports - SP scheduler	N/A
554	All	802.1x Single Host : Mac-addresses are not learned in mac-address table after the clients are authenticated in single-host mode while in multi-host are learned properly	N/A
611	All	Agent download via in-band routed port locks the console	Use VLAN interface or Out of Band interface for Agent download. Do not use routed port interface.

Tracking	Product	Description	Workaround
695	All	Ping doesn't work between 1/10 Gb interfaces or 1/10 Gb port-channels when STP mode is PVRST and more than 9 VLANs are created.	N/A
838	All	DHCP Snooping: When disabling DHCP Snooping globally, the DHCP Snooping VLAN configuration is cleared.	Reconfigure DHCP Snooping per VLAN.
848	All	Auto Attach: For phone detection it is advisable not to use rules with LLDP-CAP "phone" as matching criteria.	Phones can be identified using other data LLDP data, such as System Description, System Name or Chassis ID.
946	All	Routing is not working on routed port when static ARP is used	Use static ARPs only for VLAN interfaces.
985	All	Exec-timeout setting is lost after reboot.	Reconfigure this setting after unit reboot.
1056	All	Physical ports that are part of a port-channel are returning to VLAN 1 after remote peer is performing a boot default. 1) When port-channel is deleted, links are not restored to original VLANs 2) When link member is not part of the bundle, it is assigned to VLAN 1	N/A
1193	All	Value of MTU for interfaces from a port-channel is changed only if the interface port-channel is bounced.	MTU can be changed for a physical interface without shutdown. For port-channel, MTU can be changed also without shutdown, but the value is not updated - you need to bounce the port-channel.
1531	All	When using the ACL option as a source for a monitoring session, the monitor session is not functional.	First you have to configure the ACL on the interface and then you have select it as a monitor session for the monitoring session.
1555	All	When downloading agent via SFTP from SSH/telnet session, the download progress is displayed on the console interface, not in the current session.	N/A
1828	All	Establishing a SSH session between two cnMatrix devices running software version 2.1 is not working.	N/A

Feature Notes

- If you remove the default IP address from mgmt0 interface and save the running-config the default IP address is restored after boot.
- DHCP Client is enabled by default on In-Band Ports from VLAN 1.

- The Out-of-Band port has the following default IP address: 192.168.0.1.

Limitations

- 265 - Flow control counters displayed by the command show interface flow control are not incremented on Extreme Ethernet interfaces (10GB).
- 437 – SNTP Authentication is not supported for broadcast and multicast modes.