Release Notes for Cambium Networks cnMatrix Release 4.1-r3

Contents

Copyright 2021 Cambium Networks. All rights reserved.

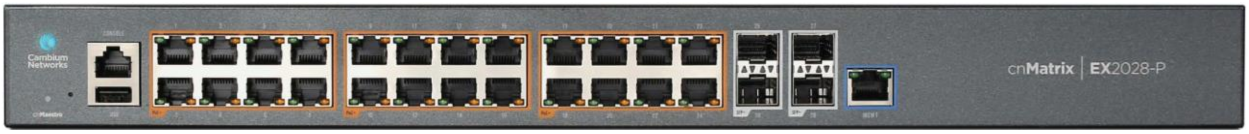
Introduction

This document provides information for the Cambium Networks cnMatrix switch release 4.1-r3. 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 Models

- cnMatrix EX2028

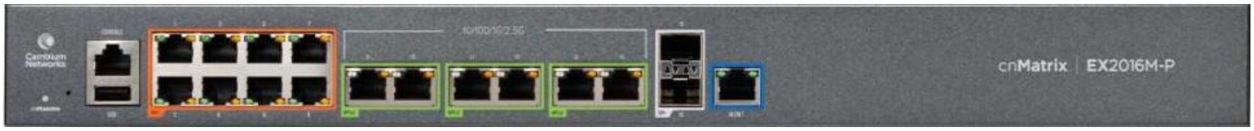
- cnMatrix EX2028-P



- cnMatrix EX2010

- cnMatrix EX2010-P

- cnMatrix EX2016M-P



- cnMatrix EX2052-P and EX2052R-P

- cnMatrix EX2052

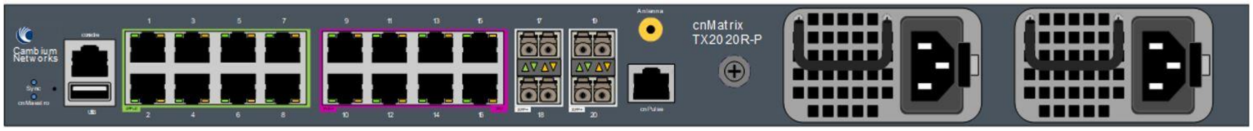
- cnMatrix EX1028

- cnMatrix EX1028-P

- cnMatrix EX1010

- cnMatrix EX1010-P

- cnMatrix TX2020R-P



- cnMatrix TX2012R-P

- cnMatrix TX2028RF-P

Attention: Certain features may not be available on this product line and will be called out explicitly where not applicable. The TX switches do not support running software versions 2.x and 3.x. Downloading unsupported software is prohibited by 4.1-r3 agent.

Cambium Networks products and support

Product information: https://www.cambiumnetworks.com/products/software/

Log in to XMS-Cloud: https://login.xirrus.com

Log in to cnMaestro: https://cloud.cambiumnetworks.com

For more information: salesdev@cambiumnetworks.com

What's New in 4.1-r3

cnMatrix Software Release 4.1 is supported on all cnMatrix hardware platforms: EX2K, EX1K and TX2K.

The cnMatrix 4.1 software archive file can be loaded on both EX and TX models. The archive file name contains EX and TX model names - **cnMatrix-EXTX-4.1-r3.img.tar.gz** .

Support for new TX model

Part Number	Number of Ports	10/100/1000 Mbps RJ45 Ports	SFP Ports	SPF+ Ports	Cambium Sync Ports	Power over Ethernet	Removable Power Supply
cnMatrix TX2028RF-P	**28**	**16**	**8**	**4**	**16**	**Yes**	**Yes**

New Features

cnMatrix Release 4.1 brings new functionality supported on all models or only on specific models. The new features and supported models are listed in the table below.

Copyright 2021 Cambium Networks. All rights reserved.

cnMatrix New Features	EX2K	EX1K	TX2K
IPv6 ND RA Guard	Yes	Yes	Yes
MAC Authentication Bypass - MAB	Yes	Yes	Yes
Port Network Access Control: Authorization	Yes	Yes	Yes
MSTP support in cnMaestro	Yes	Yes	Yes
STP Path Cost method	Yes	Yes	Yes
Port Security: MAC address learn limit	Yes	Yes	Yes
cnMatrix Support For cnMaestro SNMP Agent Configuration	Yes	Yes	Yes
Energy Efficient Ethernet	Yes	Yes	Yes
Counter for link-up/down events	Yes	Yes	Yes
Interface Description History	Yes	Yes	Yes

IPv6 ND RA Guard

This feature prevents malicious and unwitting IPv6 Neighbor Discovery Router Advertisement packets entering the network at the edge. This feature can be enabled on a per-port basis.

```
cnMatrix(config-if)# ipv6 nd raguard attach-policy {host | router}
```

By attaching the “host” policy to a port, the IPv6 ND RA packets received on that port will be dropped at ingress. By attaching the “router” policy, the IPv6 ND RA packets will be allowed on that port.

By default, the “router” policy is attached to all ports.

To view the per-port configuration and statistics, use the command:

Copyright 2021 Cambium Networks. All rights reserved.

```
cnMatrix# show ipv6 nd raguard

 IPv6 Neigbor Discovery RA Guard:

 Port    Policy    Dropped    Forwarded
                     RAs         RAs
------  ------  ---------  ---------
Gi0/1   Router                   189
…
```

MAC Authentication Bypass - MAB

(also known as MAC Based Port Network Access Control)

This is the feature that allows authenticating non-802.1x capable devices based on their MAC address. The switch can use either the local dot1x database or a RADIUS (Remote Authentication Dial In User Service) server to authenticate the MAC address. For the local database, use the MAC address without any separator as the username and password, as shown in this example:

```
dot1x local-database aabbccddeeff password aabbccddeeff permission allow
```

When MAB is enabled, the authentication process will first try to identify any dot1x capable device connected on the port. When that fails, the same amount of time will be spent trying to acquire the MAC address of the device. Once the MAC address has been acquired, the switch will check that it is allowed access to the network, either locally or using a RADIUS server. If the MAC address has not been acquired during this time, the authentication process will start all over again. Despite not sending any identity-request messages during the MAC address acquisition, the switch will still listen for EAP-start messages and will initiate dot1x authentication once such a message is received.

To enable MAB on a port, you need to type the following commands:

Command	**Explanation**
`configure terminal`	Enter global configuration mode
`interface gigabitEthernet 0/1`	Enter interface configuration mode
`dot1x port-control auto`	Enable authentication on the port
`dot1x mac-auth-bypass`	Enable MAB
`dot1x reauth-max 3`	(Optional) Configure the number of times the switch will try to authenticate dot1x devices.
`dot1x timeout tx-period 30`	(Optional) Configure the time to wait for dot1x devices to respond.
`end`	Return to the privileged EXEC mode
`show dot1x interface gigabitEthernet 0/1`	Displays the interface dot1x configuration.

Once a device has been authenticated using MAB, further reauthentication attempts will use the same MAC address. To replace the MAC address, the link admin state or dot1x port-control must be bounced.

When in **single-host** mode, the switch will acquire the first MAC address and only this address will be allowed to access the network.

In **multi-host** mode, the switch will acquire the first MAC address and then allow any MAC address to access the network.

Port Network Access Control: Authorization

This feature adds the ability to change the access VLAN and 802.1p priority based on the attributes received from a RADIUS server. The authorization is disabled by default and can be enabled using the following commands:

Command	**Explanation**
`configure terminal`	Enter global configuration mode
`aaa authorization network default group radius`	Set global dot1x authorization method to RADIUS
`end`	Return to the privileged EXEC mode
`show dot1x`	Displays global dot1x configuration

For authorization to work, the following requirements must be met:

- The authentication method is set to RADIUS.
- The port is in access mode.

For dynamically assigning the VLAN, the switch expects the following attributes from the RADIUS server:

- Tunnel-Type
- Tunnel-Medium-Type
- Tunnel-Private-Group-ID

The Tunnel-Type attribute must be set to VLAN, the Tunnel-Medium-Type attribute must be set to IEEE-802 and the Tunnel-Private-Group-ID attribute must contain the VLAN ID as a string.

For dynamically assigning the 802.1p priority, the switch expects the User-Priority-Table attribute to contain the desired priority repeated 8 times. The reason for this is that cnMatrix 1k and 2k series only support overwriting the priority with a single value.

Here is an example user configuration for FreeRADIUS:

```
bob     Cleartext-Password := "hello"
        Service-Type = Framed-User,
        Auth-Type := Accept,
        Tunnel-Type = VLAN,
        Tunnel-Medium-Type = IEEE-802,
        Tunnel-Private-Group-id = "70",
        User-Priority-Table = "44444444"
```

MSTP support in cnMaestro

Starting with version 4.1-r3, cnMatrix supports MSTP configuration and monitoring from cnMaestro.

Copyright 2021 Cambium Networks. All rights reserved.

New MSTP configuration:

- MSTP enable/disable
- region name
- revision name
- instance-to-VLAN mapping
- instance priority
- priority per port-instance and port-channel group instance.

cnMaestro will also monitor the MSTP state per port-instance.

STP Path Cost method

The switch will allow the user to select between the IEEE 802.1D-1998 (short) and the IEEE802.1T (long) default STP path cost values. This is a per-switch (global) STP configuration and can be set in each STP operating mode (RSTP, PVRST, MSTP). The default method is “long”.

To configure the path cost method via CLI, run the following command :

```
cnMatrix(config)# spanning-tree pathcost method { long | short}
```

The configuration is also available in the Web GUI, for each STP mode.

Path cost values will be immediately modified on the operational ports, and the STP trees will be recalculated accordingly. Ports on which the cost is set manually will not be affected by this global setting.

Port Security: MAC address learn limit

This feature aims to provide a way for the switch to restrict the access to the network to a certain number of devices per port, based on their MAC address. Typically, on access ports there is only one device which accesses the network, and by using this feature, the network administrator ensures that the other devices don’t use the user’s connection to access the network.

The feature allows the network administrator to configure the maximum number of devices that can access the network from a specific port, and the action to be taken in case the configured number is exceeded.

To configure this feature via CLI:

This command enables the feature and set the default maximum to “1” and “protect” as the default action:

```
cnMatrix(config-if)# switchport port-security
```

This command disables the feature:

```
cnMatrix(config-if)# no switchport port-security
```

This command set the maximum number of MAC addresses allowed per port:

```
cnMatrix(config-if)# switchport port-security maximum <1-1000>
```

This command set the action to be taken in case the configured number is exceeded:

```
cnMatrix(config-if)# switchport port-security violation {protect | restrict}
```

"protect"—When the number of port secure MAC addresses reaches the maximum limit allowed on the port, packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses to drop below the maximum value or increase the number of maximum allowable addresses. The violation counter increments. You are not notified that a security violation has occurred.

"restrict" – When the number of secure MAC addresses reaches the limit allowed on the port, packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses or increase the number of maximum allowable addresses. An SNMP trap is sent, a syslog message is logged, and the violation counter increments.

By default, the feature is disabled. When enabled, the maximum number of allowed MAC addresses is set to 1, and the action is set to "protect".

cnMatrix Support For cnMaestro SNMP Agent Configuration

The 4.1-r3 release includes configuration support for the following settings:

- SNMP Agent enable/disable
- SNMPv2c Read-Only Community Name
- SNMPv2c Read-Write Community Name
- Trap Receiver IPv4 Address
- SNMPv3 User Name
- SNMPv3 User Password
- SNMPv3 User Access (read-only, read-write)
- SNMPv3 User Authentication Protocol
- SNMPv3 User Privacy enable/disable

To display the entries that are created via cnMaestro, use the following command:

```
cnMatrix(config)# show running-config snmp
```

Note: entries are read-only but are displayed as comments to provide a complete picture of the current configuration.

Energy Efficient Ethernet

Energy Efficient Ethernet (EEE) is an 802.3az standard that is designed to reduce the power consumption of copper interfaces during idle periods.

EEE can be enabled on devices that support Low Power Idle (LPI) mode. When the device enters LPI mode power consumption is reduced by shutting down certain services that are not needed during idle periods.

For EEE to function, both devices must support LPI mode and they must have EEE enabled.

To enable/disable EEE, via CLI, use the "energy-efficient-ethernet" command from the interface configuration.

Or, from the Web GUI: navigate to System->Energy Efficient Ethernet.

This feature provides a way for the switch to count the number of link transition events per port. And display this count to the user. This information can be displayed via the "show interfaces" command, as well as via the "show interfaces link-transitions" CLI command, and it is also visible in the "Port Basic Settings" page in the Web GUI.

Counter for link-up/down events

The Link-Transitions Count feature provides a way for the switch to count the number of link transition events per port. The feature shows the number of link transition events on a per-port basis, for all ports available and the timestamp of the last transition.

Interface Description History

To assist with tracking the status of connected devices, a short interface description history is now available. cnMatrix maintains both the current interface description (configured manually or based on LLDP/PBA processing) and the previous interface description. Updating the interface description to a new value automatically save the previous interface description value. The previous interface description value is displayed using the CLI "show interface" command and through the Statistics > Interface > Interface Statistics Web page."

Supported Features in cnMatrix 4.1-r3

The list below is a high-level summary of cnMatrix 4.1-r3 supported features. For more detailed information regarding cnMatrix supported features, please access cnMatrix User Guide.

cnMatrix feature availability varies between hardware platforms and cloud managers. Please consult the feature availability table below.

cnMatrix Feature	cnMaestro Configurable (3.0.4)	XMS-Cloud Configurable (10.7)	EX2K	EX1K	TX2K

Industry-standard Command Line Interface (CLI)	Yes	Yes	Yes	Yes	Yes
Web Management	Yes	No	Yes	Yes	Yes
cnMaestro Cloud-based Management	Yes	No	Yes	Yes	Yes
Zero-touch Remote Provisioning	Yes	Yes	Yes	Yes	Yes
SNMPv1/v2c/v3	Yes	No	Yes	Yes	Yes
Telnet Client/Server	Server	No	Yes	Yes	Yes
Out-Of-Band Ethernet Management	No	No	Yes	No	No
SSH/SSH v2	No	No	Yes	Yes	Yes
DHCP Client	Yes	Yes	Yes	Yes	Yes
DHCP Server	No	No	Yes	Yes	Yes
Local/Remote Syslog	No	No	Yes	Yes	Yes
System Resource Monitoring	Yes	No	Yes	Yes	Yes
802.1Q VLAN and Trunking Support	Yes	Yes	Yes	Yes	Yes
802.1d STP, 802.1w RSTP	Yes	Yes	Yes	Yes	Yes
802.1s MSTP	Yes	No	Yes	Yes	Yes
PVRST (Per VLAN RSTP)	Yes	No	Yes	Yes	Yes
802.1p Quality of Service	No	Partially	Yes	Yes	Yes
ACL QoS: Mapping/Marking ToS/DSCP, 802.1p, Priority Queue	Partially	Partially	Yes	Yes	Yes
Inbound Traffic Policing, and Outbound Traffic Shaping	No	No	Yes	Yes	Yes
Storm Control	Yes	No	Yes	Yes	Yes
Flow Control Per Port	No	No	Yes	Yes	Yes
802.1ab Link Layer Discovery Protocol (LLDP)	No	No	Yes	Yes	Yes
802.3ad Link Aggregation	Yes	Yes	Yes	Yes	Yes
Policy-Based Automation with Dynamic Configuration	Yes	Yes	Yes	Yes	Yes
IGMP Snooping v1/v2	Yes	Yes	Yes	Yes	Yes
IGMP Snooping Proxy	No	No	Yes	Yes	Yes
Private VLAN Edge	Yes	No	Yes	Yes	Yes
Port Mirroring: Port-based, ACL-based	Yes (port-based only)	No	Yes	Yes	Yes
SNTP	Yes	Yes	Yes	Yes	Yes

Port Statistics	Yes	No	Yes	Yes	Yes
RMON	No	No	Yes	Yes	Yes
Routing Between Directly Connected Subnets	No	No	Yes	Yes	Yes
Routed Interfaces	No	No	Yes	Yes	Yes
IPv4 static routes	Yes	No	Yes	Yes	Yes
Host routes	No	No	Yes	Yes	Yes
DHCP Relay	No	No	Yes	Yes	Yes
802.1x Authentication	Yes	Yes	Yes	Yes	Yes
Radius/TACACS+	Radius	Yes	Yes	Yes	Yes
DHCP Snooping	Yes	No	Yes	Yes	Yes
Static MAC	No	No	Yes	Yes	Yes
IGMP Filtering	No	No	Yes	Yes	Yes
Locally Managed Username and Password	Yes	Yes	Yes	Yes	Yes
cnMaestro on-premise	Yes	No	Yes	Yes	Yes
RIPv1/v2	No	No	Yes	**No**	Yes
OSPFv2	No	No	Yes	**No**	Yes
USB support	No	No	Yes	Yes	Yes
Reset button	Yes	No	Yes	Yes	Yes
Dynamic ARP Inspection	Yes	No	Yes	Yes	Yes
LLDP-MED	No	No	Yes	Yes	Yes
CLI ‘do’ command	No	No	Yes	Yes	Yes
cnMaestro Configuration	Yes	No	Yes	Yes	Yes
XMS-Cloud Configuration	N/A	Yes	Yes	Yes	Yes
Cambium Sync	Yes	No	No	No	Yes
802.3 af/at/bt	Yes	Yes	Up to 30W (60W on EX2016M-P)	Up to 30W	Up to 90W
PoE autodetect cnMedusa	Yes	No	No	No	Yes (first half of the ports)
PoE autodetect cnWave	Yes	No	No	No	Yes (first half of the ports)
PoE high temperature mode	No	No	No	No	Yes
PoE hybrid mode	Yes	No	Yes	Yes	Yes

PoE Budget	N/A	N/A	Full	Reduced	Full
PoE+ (30W)	N/A	N/A	Yes	Yes	Yes
24V Passive PoE	Yes	No	No	No	Yes (second half of the ports)
54V Passive PoE	Yes	No	No	No	Yes
PoE on 4 Pairs (90W)	N/A	N/A	Only EX2016-M-P, ports 9-14, max 60W	No	Yes (first half of the ports)
Transceiver ports	N/A	N/A	SFP+ (SFP on EX2010)	SFP	SFP+
Cable Diagnostics	cnMaestroX	No	Yes (No on 2.5Gbps ports)	Yes	Yes
Redundant Power Supplies (RPS)	No	No	Yes	No	Yes
Dual Redundant Power Supplies	No	No	No	No	Yes (TX2020R-P only)
PBA	Yes (cnMaestroX on EX1K)	Yes	Yes	Yes	Yes
Auto recovery of connected devices	cnMaestroX	No	Yes	Yes	Yes

Fixed Issues

Tracking	Product	Feature	Description
3404	All	SSH	Exceptions encountered when using monitoring tools which connect to the switch through SSH
3433	All	SSH	Memory leak when multiple SSH sensors are enabled on network monitoring tool such as PRTG
3475	All	DHCP Server	DHCP pool name is not properly generated by ‘show running-config’. This can cause configuration failure when CLI template is pushed from cnMaestro.

Tracking	Product	Feature	Description
3533	All	Spanning-Tree	Root Bridge changes continuously when SNTP is enabled and the clock is synchronized
3562	All	SFP+	Ubiquiti BiTi transceiver not configured by auto-detect. The transceiver type is listed as N/A, the wavelength is displayed incorrectly.
3573	All	LLDP	LLDP-based PBA policy now allows multiple LLDP neighbors on the same port. Device such as IP Phone can use LLDP detection with PBA policy
3574	All	SSH	SSH segmentation fault when running Tenable Nessus software tool

Known Issues (Release 4.1-r3)

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
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.

Tracking	Product	Description	Workaround
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
1555	All	When downloading agent using 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 is not working.	N/A
2103	All CnMaestro	Router Port configuration from CLI Templates will result in faulty port performance tracking	N/A
2122	All	RIPv1/RIPv1 compatible updates are not sent to the RIP neighbors (3.0.1-r4 does not work with RIPv1 RIP router)	Only connect cnMatrix 3.0.1-r4 to RIPv2 neighbors, and set the RIP send update to RIPv2 mode
3669	All	802.1x : Single Host – MAC address of the client is learnt in all the VLANs configured on the switch	N/A
3513	All cnMaestro	MSTP: In some cases, for very long VLAN lists associated to MSTP instances, the configuration may fail	N/A
3514	All cnMaestro	MSTP: When the VLAN-instance mapping is updated, the user may experience a momentary traffic drop	N/A
3646	All	**802.1x:** Vlan Priority Attribute can be configured on Radius server with the standard attribute User-Priority-Table and the value accepted is in the format "xxxxxxxx". (8x)	N/A
3677	All	802.1x : Single Host - Multiple hosts can be authenticated on the same port	N/A
3586	All	Storm-control not working correctly on a SFP+ port with 1G transceiver. Packet are limited on that port at a rate 10 time grater than for a 1G port.	N/A

Copyright 2021 Cambium Networks. All rights reserved.

Tracking	Product	Description	Workaround
3683	All	Port MAC Limiting: Migrated MAC addresses are not deleted from the software FDB table after the limit is reached on the new port.	This is a display issue. Please ignore this output.

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.
    - On EX1028 and EX1028P, VLAN 1 has the default IP address 192.168.1.1
- The Out-of-Band port has the following default IP address: 192.168.0.1.

Limitations

Tracking	Product	Description	Workaround
265		Flow control counters displayed by the command show interface flow control are not incremented on Extreme Ethernet interfaces (10Gbps).	
437	All	SNTP Authentication is not supported for broadcast and multicast modes.	
2103	All	Router Port configuration from CLI Templates will result in faulty port performance tracking	Configuring a router port from a template can lead to unexpected monitoring behavior. The setting is not recommended while using cnMaestro.
2603	All	If a static IP is set on L3 interface from CLI/Web, the out-of-sync condition is not triggered by cnMaestro.	If a static IP is set on L3 interface from CLI/Web, the out-of-sync condition is not triggered by cnMaestro.

Copyright 2021 Cambium Networks. All rights reserved.