Lenovo ThinkSystem NE1032/NE1032T/NE1072T RackSwitch

Release Notes

For Lenovo Cloud Network Operating System 10.10

Lenovo™

Note: Before using this information and the product it supports, read the general information in the *Safety information and Environmental Notices* and *User Guide* documents on the Lenovo *Documentation* CD and the *Warranty Information* document that comes with the product.

First Edition (April 2019)

Release Notes

This release supplement provides the latest information regarding Lenovo Cloud Network Operating System 10.10 for the Lenovo ThinkSystem NE1032/NE1032T/NE1072T (referred to as NE1032/NE1032T/NE1072T throughout this document).

This supplement modifies and extends the following Cloud NOS documentation for use with *CNOS* 10.10:

- *Lenovo Network Application Guide for Lenovo Cloud Network Operating System 10.10*
- *Lenovo Network Command Reference for Lenovo Cloud Network Operating System 10.10*
- *Lenovo Network Python Programming Guide for Lenovo Cloud Network Operating System 10.10*
- *Lenovo Network REST API Programming Guide for Lenovo Cloud Network Operating System 10.10*
- *Lenovo ThinkSystem NE1032/NE1032T/NE1072T Installation Guide for Lenovo Cloud Network Operating System*

These publications are available from the following website:

http://systemx.lenovofiles.com/help/topic/com.lenovo.systemx.common.nav.doc/overview_rack_switches.html

Please keep these release notes with your product manuals.

Note: The Lenovo Cloud Network OS is based on the Embedded Linux Integration Environment (ELIE). To obtain open source code licenses, go to https://github.com/lenovo/ELIE/tree/master/elie-1.7.1/licenses/. For details on how to obtain open source code, please contact Lenovo Support.

Hardware Support

CNOS 10.10 software is supported on the NE1032/NE1032T/NE1072T high performance Layer 2-3 network switches.

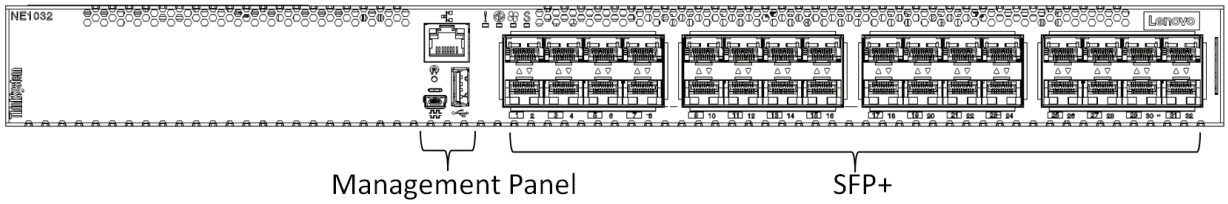
The NE1032/NE1032T/NE1072T is a 1U GbE switch and it can be mounted horizontally or vertically, depending on your application. Mounting options are available for a variety of rack systems.

For superior reliability, the NE1032/NE1032T/NE1072T uses redundant, hot-swap power supply modules and three (NE1032 and NE1032T) or five (NE1072T) hot-swap fan modules. Module options are available for either front-to-rear airflow, or rear-to-front airflow.

The NE1032 contains the following ethernet ports:

- Thirty-two 10 Gigabit Ethernet (GbE) Small Form Pluggable Plus (SFP+) ports which also support legacy 1 GbE connections

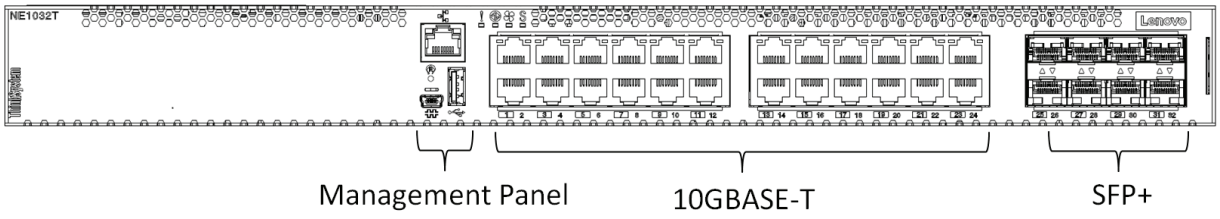
Figure 1. NE1032 front panel



The NE1032T contains the following ethernet ports:

- Twenty-four 1G/10G BASE-T RJ45 ports
- Eight 10G SFP+ Uplinks
- Ten Gigabit Ethernet (GbE) Small Form Pluggable Plus (SFP+) ports which also support legacy 1 GbE connections

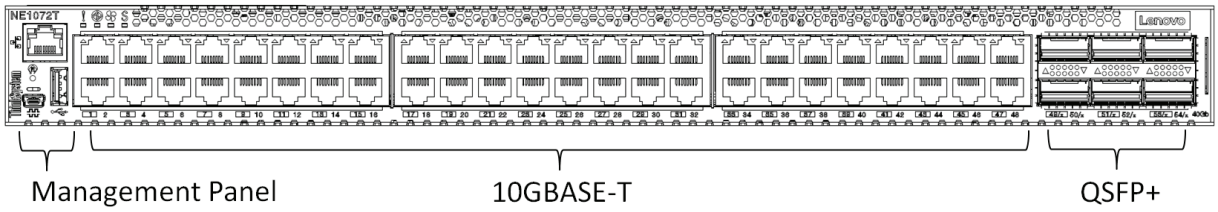
Figure 2. NE1032T front panel



The NE1072T contains the following ethernet ports:

- Forty-eight 1G/10G BASE-T RJ45 ports
- Six 40 GbE Quad Small Form Pluggable Plus (QSFP+) ports, all of which ports can optionally be used as four 10 GbE ports

Figure 3. NE1072T front panel



Updating vLAG Switches

Following are the steps for updating the software and boot images for switches configured with vLAG:

1. Having an earlier than CNOS 10.10 version on both vLAG switches, load the CNOS 10.10 image on both of them.

   Note: Do not reboot the switch.

2. On the Primary switch, shutdown all the port-channels associated with the vLAG instances. All traffic goes through the Secondary switch.

   Note: Do not save the configuration with the disabled port-channels.

3. Reload the Primary switch so that the current Secondary switch becomes the new Primary.

   Note: The operational VLAG roles are swapped after this step.

4. After reboot, ISL automatically enters in the `Active` state.

5. A syslog notification appears alerting the user that the vLAG OS version is mismatched, but vLAG becomes operational with all its instances in the `Formed` state, after startup-delay expires.

6. On the current Primary switch, shutdown all the port-channels associated with the vLAG instances. All traffic goes through the Secondary switch.

   Note: Do not save the configuration with the disabled port-channels.

7. Reload the current Primary switch so that the current Secondary switch becomes the new Primary.

   Note: The operational VLAG roles are swapped after this step (the initial roles from the beginning of this procedure are restored).

8. After reboot, ISL automatically enters in the `Active` state, and vLAG becomes operational with all its instances in the `Formed` state, after startup-delay expires.

Supplemental Information

This section provides additional information about configuring and operating the NE1032/NE1032T/NE1072T and CNOS.

The Boot Management Menu

The Boot Management menu allows you to switch the software image or to recover from a failed software download.

You can interrupt the boot process and enter the Boot Management menu from the serial console port. When the system displays Memory Test, press **Shift + B**. The Boot Management menu appears.

```
The system is going down for reboot NOW!
INIT: reboot: Restarting system
...

Press shift-B for startup menu or shift-R for recovery mode: ..
Running Startup Menu
...

Boot Management Menu
        I - Change booting image
        C - Change configuration to factory default
        R - Boot in recovery mode (tftp and xmodem download of images to
recover switch)
        P - Reset the Network Administrator (admin) password
        B - Reset the password required to enter privileged exec mode
        Q - Reboot
        E - Exit
Please choose your menu option:
```

The Boot Management menu allows you to perform the following actions:

- To change the booting image, press **I** and follow the screen prompts.
- To reset the switch configuration to factory defaults, press **C** and follow the screen prompts.
- To boot in recovery mode, press **R**.
- To reset the Network Administrator account (admin) password, press **P** and follow the screen prompts.
- To reset the password required to enter Privileged EXEC configuration mode, press **B** and follow the screen prompts.
- To reload the switch, press **Q**. The reloading process will start again.
- To exit the Boot Management menu, press **E**. The reloading process continues.

Recovering from a Failed Software Upgrade

Use the following procedure to recover from a failed software upgrade.

1. Connect a PC to the serial port of the switch.
2. Open a terminal emulator program that supports TFTP (preferred) or Xmodem download (for example, HyperTerminal, SecureCRT, PuTTY). If using Xmodem, make sure the following settings are in effect:
   - Speed: 9,600 bps
   - Data Bits: 8
   - Stop Bits: 1
   - Parity: None
   - Flow Control: None
3. To access the Rescue Mode menu, you must interrupt the boot process from the Console port. Boot the NE1032/NE1032T/NE1072T, and when the system begins displaying Memory Test progress (a series of dots), press **Shift + R**. The Rescue Mode menu will be displayed:

```
Entering Rescue Mode.
Please select one of the following options:
        T) Configure networking and tftp download an image
        U) Install image from USB stick
        P) Physical presence test (low security mode)
        F) Run filesystem check
        I) Select which image to boot
        C) Reset configuration to factory default
        R) Reboot
        E) Exit

Option?:
```

   - If you choose option **T** (TFTP download), go to step 4.

4. **TFTP download**: The switch prompts you to enter the following information:

```
Performing TFTP rescue. Please answer the following questions (enter 'q'
to quit):
IP addr    :
Server addr:
Netmask    :
Gateway    :
Image Filename:
```

   a. Enter the required information and press **Enter**.

   b. You will see a display similar to the following:

```
Host IP    : 10.10.98.110
Server IP  : 10.10.98.100
Netmask    : 255.255.255.0
Broadcast  : 10.10.98.255
Gateway    : 10.10.98.254
Installing image NE1032/NE1032T/NE1072T-CNOS-10.10.2.0_OS.imgs from
TFTP server 10.10.98.100
```

   c. When you see the following prompt, enter the image number where you want to install the new software and press **Enter**.

```
Install image as image 1 or 2 (hit return to just boot image): 1
```

   d. The following message is displayed when the image download is complete. Continue to step 7.

```
Entering Rescue Mode.
Please select one of the following options:
        T) Configure networking and tftp download an image
        U) Install image from USB stick
        P) Physical presence test (low security mode)
        F) Run filesystem check
        I) Select which image to boot
        C) Reset configuration to factory default
        R) Reboot
        E) Exit

Option?:
```

5. Image recovery is complete. Perform one of the following steps:

   - Press **R** to reboot the switch
   - Press **E** to exit the Boot Management menu
   - Press **Esc** to re-display the Boot Management menu

New Features in This Release

This release of Lenovo Cloud Network OS contains the following significant enhancements.

VXLAN Routing

This feature enables VXLAN routing, which is the process in which a VTEP receives a VXLAN packet destined to itself, removes the VXLAN header and then performs a Layer 3 route lookup on the inner decapsulated packet.

Controller-less VXLAN (TNO + VXLAN) on VMWare and Nutanix

This feature integrates controller-less VXLAN (VXLAN bridging without requiring an SDN controller) for VMware and Nutanix applications with the automated Layer 2 port provisioning provided by ThinkAgile Network Orchestrator.

ARP Suppression

This feature reduces traffic across controller-less VXLAN DC by keeping learning packets local to the VTEP. This is done by avoiding ARP packet flooding, which occupies core network bandwidth.

Standalone Unified Fabric Port (UFP)

This feature uses vPorts to create isolation between vNICs within the compute node and maintain that isolation within the switch. Unified Fabric Port (UFP) defines an architecture that allows the logical subdivision of a single high speed physical networking link connecting a server Network Interface Controller (NIC) or Network Adapter port to an edge switch port such that each subdivision appears to the server operating system or hypervisor as an independent physical NIC, and each subdivision can be uniquely identified at the edge switch port, which can then be configured to provide the same isolation and functionality as if each logical subdivision were a separate physical connection.

Port Mode Change Without Reboot

This feature provides flexibility of configuration by allowing port speeds to be changed without resetting the switch.

802.1X Port Authentication

802.1X is a standardized framework that provides port-based access control. This protocol authenticates the network clients by using a unique information like personal credentials (username/password) or digital certificates. In 802.1X architecture, the switch is a Network Access Server (NAS), and relies on a central identity/attributes repository to authenticate and authorize the client. The 802.1X standard specifies the Extensible Authentication Protocol (EAP) as a method to provide authentication and authorization using a centrally administered Authentication Server and defines the EAP over LAN (EAPoL) message format.

Boot Profiles

Traditional switches provide a fixed number of forwarding table entries, which are referred to as the size of that respective table. The forwarding tables refer to the Layer 3 Route table, ARP cache table, and MAC address table. The numbers are fixed according to capability of underlying ASIC. The latest ASICs from Broadcom allow these forwarding tables to share a common pool of resources, which in turn allows customizing the share for each of those tables. The Boot Profiles feature leverages capabilities in the Broadcom ASIC to allow forwarding tables to share a common pool of resources. A new profile was added, allowing you to choose between two predefined table sizes.

Telemetry Data Set Extension

New features allow CNOS telemetry to store data using an embedded Redis database. When used, the database can help streamline the REST/Python API processing for pull requests by allowing direct access from the Python API layer to the database.

Static NAT Support

Static Network Address Translation (NAT) provides the capability to configure one-to-one, many-to-few, and many-to-one mappings of the inside local addresses to the inside global addresses. This feature can provide either only IP addresses translations or both IP addresses and UDP/TCP L4 port number translations from inside to outside traffic, and outside to inside traffic.

Static NAT is useful when a host from private network must be accessible by a fixed address from external network.

BGP EVPN Layer 3

This feature provides support for VXLAN routing, which enables inter-subnet connectivity among tenant systems. It allows end hosts, such as virtual machines on a bare-metal server that are connected to a top of rack switch, to send MAC and IP information to remote Virtual Tunnel End-Points. The information is collected using ARP Suppression protocol and transformed into BGP EVPN routes. It also permits the redistribution of connected, static, OSPF, and BGP IPv4 unicast routes present in the tenant system into EVPN. Based on this information, on the remote VTEP, host (/32) or subnet (such as /24) routes are installed in the corresponding Tenant System routing table, thus achieving the possibility of routing.

Anycast Gateway

The feature introduces the capability of having a preferred MAC address associated with a desired SVI. This in turn offers the possibility for any device acting as a VTEP inside a VN to become the distributed Anycast Gateway for the end hosts that reside in its subnetwork.

Fibre Channel over Ethernet

Fibre Channel over Ethernet (FCoE) is an effort to converge two of the different physical networks in today's data centers. It allows Fibre Channel traffic (such as that commonly used in Storage Area Networks, or SANs) to be transported without loss over 10Gb Ethernet links (typically used for high-speed Local Area Networks, or LANs). This provides an evolutionary approach toward network consolidation, allowing Fibre Channel equipment and tools to be retained, while leveraging cheap, ubiquitous Ethernet networks for growth.

FCoE Initialization Protocol (FIP) Snooping

FCoE Initialization Protocol (FIP) snooping is a feature of FCoE. In order to enforce point-to-point links for FCoE traffic outside the regular Fibre Channel topology, Ethernet ports used in FCoE can be automatically and dynamically configured with access control lists (ACLs).

Using FIP snooping, the switch examines the FIP frames normally exchanged between the FCF and ENodes to determine information about connected FCoE devices. This information is used to create narrowly tailored ACLs that permit expected FCoE traffic to and from confirmed Fibre Channel nodes, and deny all other undesirable FCoE or FIP traffic.

MAC-move Notification

This feature enables MAC-move notification, which generates syslog messages when the switch detects that a MAC address has moved between switch ports.

MAC-move Loop Detection

This feature enables MAC-move loop detection, which detects MAC-move loops and error-disable ports that appear in the loops.

OSPFv2 with VRF

Using VRF together with OSPF enables multiple OSPF instances to be run on the switch.

NTP Server Support

The switch can be configured to act as an NTP server.

Link Flap Dampening

Link-Flap Dampening (LFD) allows the switch to separately monitor each interface for flapping events. If flapping events on an interface exceed the maximum allowed number of flaps within a time interval, then the switch automatically shuts down that interface.

PKI CRL, CDP Check and Credential Expiry

Added support for Public Key Infrastructure (PKI) CRL, CDP check, and credential expiry alert.

vLAG Orphan Ports and SVI Shutdown

Added the vLAG Orphan port option to set a port that is not part of a vLAG aggregation to also go to suspend state on secondary vLAG switch when the ISL fails with the peer vLAG switch alive.

Similarly, added the option to shutdown on a secondary vLAG switch the Layer 3 SVIs that the ISL LAG belongs to in order to disable Layer 3 forwarding while being in dual-active state.

Known Issues

This section describes known issues for CNOS 10.10 on the Lenovo ThinkSystem NE1032/NE1032T/NE1072T RackSwitch.

Note: Please check the Change History documentation posted with the Switch Firmware to check if any of these issues have been fixed in the latest release.

BGP

When the switch detects that it cannot reach the next-hop in a route, the BGP instance does not deactivate the route from its routing table. The route is deactivated only when the BGP session with the next-hop times out. (ID: 135910)

Copying Configuration Files

When copying a new configuration file over the switch's current running configuration, CNOS does not overwrite the old configuration. Instead, it appends the new configuration over the old one, leaving settings that are not present in the new configuration intact. It only overwrites settings present in both configurations. (ID: 133055)

LACP

The default behavior of Link Aggregation Control Protocol (LACP) Individual has been changed. Now, by default, LACP enabled ports transition to suspend.

When upgrading the firmware to CNOS 10.10 from 10.7 or an earlier version, the following LACP behavior occurs:

- For Link Aggregation Groups (LAGs) with default configuration, before the upgrade, LACP enabled ports transition to individual state when not receiving Link Aggregation Control Protocol Data Units (LACPDUs). After the firmware upgrade, the LACP configuration remains the same, but LACP enabled ports now transition to suspended state when no LACPDUs are received.

  To configure the LACP enabled ports as individual, use the following command on a LAG:

  ```
  NE1032(config)# interface port-channel <LAG number (1-4096)>
  NE1032(config-if)# no lacp suspend-individual
  ```

- For LAGs with non-default configuration, if before the upgrade LACP enabled ports transition to suspended state when not receiving LACPDUs, then after the firmware upgrade this behavior remains the same. However, the LACP configuration is changed to reflect the new default behavior: the LACP individual setting for LAGs is removed from the switch's running configuration. (ID: 132111)

Network Virtualization Gateway

The following limitations exist:

- For optimal performance, we recommend that the number of VLAN-VXLAN Network Identifier (VNI) mappings does not exceed 1,000 entries. Going above this limit leads to longer convergence times when attaching or detaching the Lenovo hardware Layer 2 gateway to or from NSX logical switches. (ID: 99467)
- For optimal Equal Cost Multiple Paths (ECMP) load balancing, we recommend that only Layer 3 routed ports are used for connecting to spine switches. (ID: 123627)
- When broadcast, unknown unicast, and multicast (BUM) traffic is received on the switch, it is replicated on all member ports of the same VXLAN Network, except the port that is the source port of the BUM traffic. This is displayed in the source port statistics as dropped packets. (ID: 95658)
- Throughput statistics of the southbound interface of the VXLAN gateway do not display on the NSX GUI. (ID: 113832)
- After Bidirectional Forwarding Detection (BFD) failover, when using the default value for the probe interval of 300 ms, the active service node election takes approximately three seconds to occur. (ID: 116882)
- The VLAN used in VLAN-VXLAN Network Identifier (VNI) mapping must be used exclusively for switching within the associated VNI domain. Different access vPorts belonging to the same VLAN must be mapped to the same VNI. Hence, only one-to-one VLAN-VNI bindings are supported. (ID: 100606, 123143)
- In case all network ports go down on one of the vLAG switches, all ingress traffic received on the local access ports is flooded to all other local access ports from the same VXLAN Network Identifier (VNI). Flooding stops when the network ports are back up. (ID: 110732)
- In High Availability (HA) mode, the recommended maximum number of local unicast MAC addresses is 32,000. If this limit is exceeded, MAC address synchronization between the vLAG switches might not work properly. More than 32,000 unicast MAC addresses can be used, but the synchronization process fails to function normally. (ID: 113145)
- When using NSX manager 6.4.1, the remote FDB (forwarding database) table is not correctly updated on the remote gateways, when changing the PVID or the access VLAN on the local access port. This issue has been fixed starting with NSX Manager 6.4.2. (ID: 159591)

REST API

VMware vSphere Distributed Switch (vDS) information retrieval is not supported using REST API. (ID: 138329)

SolarWinds

After setting up a SFTP/SCP server using SolarWinds, the switch fails most times to establish a connection to the server. We recommend using other SFTP/SCP servers. (ID: 135539)

Telemetry

Sometimes, when the egress CPU queue is full, Buffer Statistics Tracking (BST) gets disabled and telemetry messages are no longer sent to remote monitoring servers. Use REST to re-enable BST. (ID: 139654)

VLAG

- When upgrading the firmware of vLAG peer switches one by one to CNOS 10.10 from 10.7 or an earlier version, vLAG configuration consistency checks fail on both vLAG peer switches until the upgrade process is complete for both. (ID: 131917)
- When upgrading the firmware to CNOS 10.10 from 10.9.3, an incorrect syslog appears, alerting the user that the VLAG peer is using an older image than 10.9.x.

```
%VLAG-5-ECP_VERSION_MISMATCH: vLAG peer is running an image older than
10.9.x. Use the upgrade procedure described in the Release Notes to
ensure there is no traffic loss!
```

  This message does not affect the upgrade process and should be ignored. (ID: 141257)

vNIC Statistics

When rebooting the switch, vNIC statistics can be quickly retrieved by toggling vnic-stats state. (ID: 131081)

QLogic Firmware

QLogic QL41262 does not establish 25G link with passive SFP28 DAC cable when QL41262 is set to auto negotiation. (ID: 148199)

Lenovo HCI Solution with Nutanix

ThinkAgile Network Orchestrator is broken on Nutanix Prism v5.9.1 release. You must have Nutanix AOS version 5.0.2 – 5.8 or 5.9.2 – 5.10 installed for the ThinkAgile Network Orchestrator to work properly.

IGMP

- The number of IGMPv3 source entries (for a multicast group) is limited to 64 when VLAG is enabled. (ID: 171858)

Logging

- When establishing a second SSH or Telnet session with the switch, terminal logging may not properly initialize for the session. (ID: 158589) The following message appears:

```
%IMI-6-TTY_LOGGING_INIT_IGNORE: Terminal logging initialization
ignored due to log service busy (cannot obtain mutex lock), no log
messages will forward to the corresponding terminal (/dev/pts/0)
```

- If the logging service is busy, syslog messages are cached and logged once the service is free. In this situation, the log message timestamp is not sequenced in the log file or on the terminal. (ID: 158487)

DCI MP-BGP L2VPN

- BGP-EVPN is not backwards compatible with earlier CNOS releases. (ID: 157557)
- Tunnels to other vendors will remain in the up state if BGP protocol/neighbors are shut down manually. (ID: 158106) Each time BGP/BGP neighbor is shut down the following message appears:

```
Losing BGP evpn connectivity while DCI BGP evpn is enabled will result
in traffic loss.
```

Note: In these situations, disabling/enabling DCI mode BGP EVPN deletes the inactive tunnels.

- HW clean-up messages are not displayed when the NWV mode is disabled on the newly elected vLAG primary. (ID: 156759)
- Some internal messages are duplicated in certain scenarios. This is not causing any functional issues. (ID: 157434)

Firmware Update Error

- When upgrading the firmware to CNOS 10.10 from 10.7.1, 10.8.1 or 10.9.1, an incorrect error message appears:

```
WARNING: Downgrade from 10.7.x or later to 10.6.x or earlier version
detected.Prior to proceeding with the downgrade, please save/backup
the 10.6.x or earlier version startup-config file by using the 'copy
file config-10-6' command.
After the downgrade, once the switch comes up on 10.6.x or earlier
version, the saved 10.6.x or earlier version startup-config file needs
to be copied over to the running and startup configuration manually.
```

This message does not affect the upgrade process and should be ignored. (ID: 157431)

- When upgrading from an earlier version to 10.10, make sure both the software image and the boot image are updated. (ID: 161315)

Port Breakout on NE1072T

On NE1072T, port breakout CLIs are allowed only when CEE is disabled. (ID: 172041) The following error will be displayed on breakout when CEE is enabled:

```
NE1072T(config)# cee enable
Port breakout is not supported when CEE is enabled. Please disable CEE
and retry.
```