Lenovo ThinkSystem NE1032/NE1032T/NE1072T

Release Notes

For Lenovo Cloud Network Operating System 10.6

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 (December 2017)

Release Notes

This release supplement provides the latest information regarding Lenovo Cloud Network Operating System 10.6 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* 10.6:

- *Lenovo Network Application Guide for Lenovo Cloud Network Operating System 10.6*
- *Lenovo Network Command Reference for Lenovo Cloud Network Operating System 10.6*
- *Lenovo Network Python Programming Guide for Lenovo Cloud Network Operating System 10.6*
- *Lenovo Network REST API Programming Guide for Lenovo Cloud Network Operating System 10.6*
- *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 10.6 software is supported on the NE1032/NE1032T/NE1072T high performance Layer 2-3 network switches.

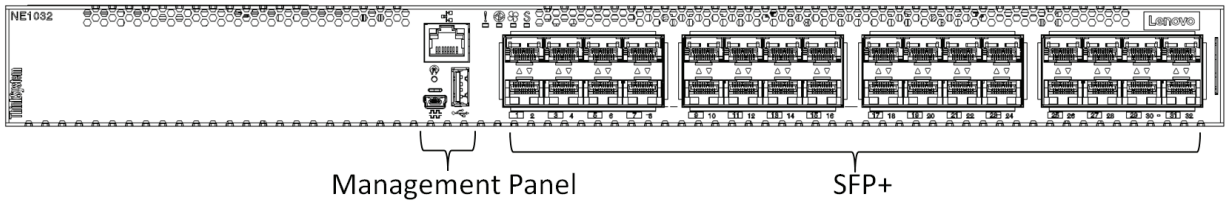
The NE1032/NE1032T/NE1072T is a 1U GbE switch and it can be mounted horizontally or vertically, depending on your application. Mounting options are available for a variety of rack systems.

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

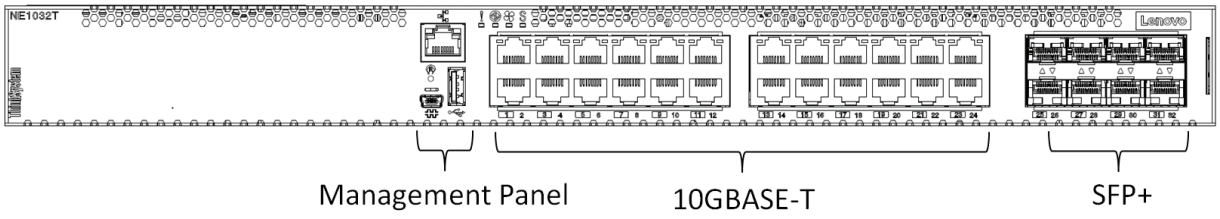
Figure 1. NE1032 front panel



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

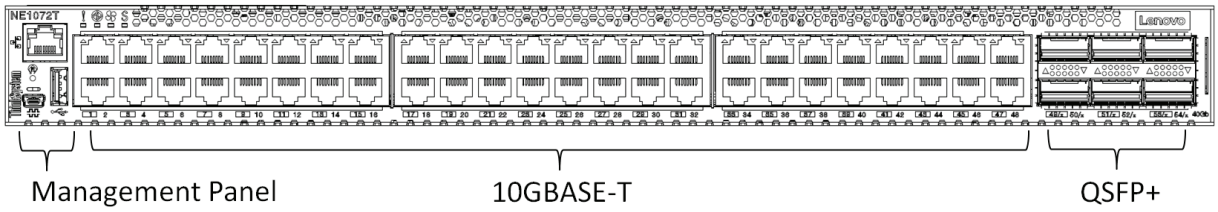
Figure 2. NE1032T front panel



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



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 Boot Management 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 + B**. The Boot Management menu will display:

```
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:
```

4. Select **R** for Boot in recovery mode. You will see the following display:

```
Entering Rescue Mode.
Please select one of the following options:
        T) Configure networking and tftp download an image
        X) Use xmodem 1K to serial download an image
        P) Physical presence (low security mode)
        F) Filesystem check
        R) Reboot
        E) Exit

Option?:
```

- If you choose option **T** (TFTP download), go to step 5.
- If you choose option **X** (Xmodem serial download), go to step 6.

5. **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-10.6.2.0_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
        X) Use xmodem 1K to serial download an image
        P) Physical presence (low security mode)
        F) Filesystem check
        R) Reboot
        E) Exit

Option?:
```

6. **Xmodem download**: When you see the following message, change the Serial Port characteristics to 115,200 bps:

```
Change the baud rate to 115200 bps and hit the <ENTER> key before
initiating the download.
```

   a. Press **Enter** to set the system into download accept mode. When the readiness meter displays (a series of "C" characters), start XModem on your terminal emulator.

   b. When you see the following message, change the Serial Port characteristics to 9,600 bps:

```
Change the baud rate back to 9600 bps, hit the <ESC> key.
```

   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
        X) Use xmodem 1K to serial download an image
        P) Physical presence (low security mode)
        F) Filesystem check
        R) Reboot
        E) Exit

Option?:
```

7. 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 fixes, enhancements, and other changes.

Access Control List Logging

ACL logging provides insight into traffic as it passes the network or is dropped by the switch. ACL logging can be CPU intensive and can slow traffic going through the network device. There are two main factors that contribute to the CPU load increase from ACL logging:

- process switching of packets that match log-enabled access control entries (ACEs)
- generating and transmitting log messages

Access Control Lists Remarks

A remark is comment text that can be added to an Access Control List (ACL) to make the ACL configuration easier to understand.

Address Resolution Protocol Refresh

Each Address Resolution Protocol (ARP) entry is checked periodically to determine its state. Based on the entry's state, ARP undertakes certain actions, like refreshing the entry or removing it from the ARP table.

Border Gateway Protocol and Differentiated Services

Border Gateway Protocol (BGP) works with the Differentiated Services (DS) computer networking architecture. You can use differentiated services with BGP to provide low latency to critical network traffic, such as VoIP, while providing best-effort service to noncritical services.

Border Gateway Protocol Unnumbered

Border Gateway Protocol (BGP) unnumbered is useful for quickly setting up large configurations for CLOS based network design. In a multi-chassis system you have a set of lower layer or line card switches that all interconnect through a different set of upper layer or fabric card switches to the fabric chassis.

Boot Management Menu Password Reset

The Boot Management Menu now includes options to reset the network administrator account password and to reset the password required to enter Privileged EXEC configuration mode. For more details, see "The Boot Management Menu" on page 6.

Dynamic ACL/QoS Provisioning for Lenovo HCI Solution with Nutanix

Guest virtual machines (VMs) can now have Access Control Lists (ACLs) attached to them and these ACLs follow the guest from one host to another within the same Nutanix cluster. IP and MAC security filters, QoS and Queue filters for prioritization can be deployed. Filters must be associated with the VM in the configurations of all switches attached to the Nutanix hosts - this can't be done from PRISM.

Dynamic Peer BFD Support

BFD now provides sub-second failure detection between two dynamic BGP peers.

Hybrid Bridge Port Mode

Hybrid bridge port mode is a trunk bridge port mode that lets you have more than one egress untagged VLAN. Like a trunk port, a hybrid port can carry multiple VLANs to receive and pass traffic for them. The hybrid bridge port mode lets you control which VLANs receive tagged egress traffic and which VLANs receive untagged egress traffic. Unlike trunk bridge port mode, the native VLAN is not considered the only VLAN that can send untagged traffic.

IP Subnet VLAN Assignment

IP subnet VLAN assignment lets you configure the switch to assign a VLAN based on the IP subnet for incoming untagged or priority-tagged packets. This feature can also assign a priority to untagged traffic.

IPv6 Neighbor Table Threshold

The IPv6 Neighbor Table threshold has been increased from 7,040 to 32,000 entries.

Layer 2 Failover

The main purpose of Layer 2 Failover is to support Network Adapter Teaming. With Network Adapter Teaming, all the NICs on each server share the same IP address and are configured into a team. One NIC is the primary link and the other is a standby link.

The Manual Monitor (MMON) enables you to configure a set of ports or LAGs to monitor for link failures (a monitor list), and another set of ports or LAGs to disable when the number of forwarding monitor links is less than the trigger limit (a control list). When the switch detects a link failure on the monitor list, it automatically disables the items in the control list. When server ports are disabled, the corresponding server's network adapter can detect the disabled link and trigger a network adapter failover to another port or LAG on the switch or another switch.

Layer 2 Failover works together with static LAGs, Link Aggregation Control Protocol (LACP), and with Spanning Tree Protocol (STP).

Lenovo Ganglia Plug-in

Lenovo Ganglia plug-in helps the telemetry agent to integrate with Ganglia. It provides pull and push mode support to collect telemetry BST statistics, translates data to Ganglia metrics, and provides a visualization tool.

Lightweight Directory Access Protocol

Lightweight Directory Access Protocol (LDAP) is a protocol for accessing distributed directory information services over a network. LDAP is used for authentication and authorization. With an LDAP client enabled, the switch will authenticate a user and determine the user's privilege level by checking with one or more directory servers instead of a local database of users. This prevents customers from having to configure local user accounts on multiple switches; they can maintain a centralized directory instead.

Proxy Address Resolution Protocol

Proxy Address Resolution Protocol (ARP) is a technique in which a device on a given network answers ARP requests intended for another device. The proxy ARP is aware of the location of the traffic's destination and offers its own MAC address as the destination. The received traffic is then routed by the proxy device to the intended destination via another interface or a tunnel. Proxy ARP is primarily used when hosts in the connected subnet are separated by features such as a private VLAN.

Reserved VLANs

Some features, such as OpenFlow and Layer 3 ports (routed ports), require internal VLANs for their operations. You can expand the range of internal VLANs by reserving a contiguous block of VLANs to guarantee the delivery and operation of features with such requirements. These reserved VLANs cannot be created, deleted, modified, or manipulated, unless the reserved VLAN range is reset to the default range (4000-4094).

Sampled Flow

Sampled Flow (sFlow) a technology for monitoring traffic in networks containing switches and routers. The sFlow monitoring system consists of an sFlow Agent and a central sFlow Collector. The sFlow architecture and sampling techniques were designed for providing continuous site-wide and enterprise-wide traffic monitoring of high speed switched and routed networks.

Scheduled Switch Reloads

This feature lets you schedule a switch reload for a later time, enabling you to perform switch upgrades during off-peak hours.

Secure Mode

Secure mode allows you to determine which protocols can be enabled. In secure mode, only secured traffic and secured authentication management are allowed.

Syslog User Action Logging

You can configure whether user actions are logged to the console or to terminals.

VLAN Access Control Lists over Switch Virtual Interfaces

A VLAN ACL is an Access Control List (ACL) that can be assigned to a VLAN rather than to a switch port as with IPv4 ACLs. This is particularly useful in a virtualized environment where traffic filtering and metering policies must follow virtual machines (VMs) as they migrate between hypervisors.

ACLs can now be also configured over Layer 3 Switch Virtual Interfaces (SVIs).

vNIC Statistics for Lenovo HCI Solution with Nutanix

Statistical data is now generated for traffic in and out of a vNIC as defined in PRISM. These statistics are retrieved from the switch(es) attached to the Nutanix hosts.

Warning Message Displayed when Changing the Default Network Administrator Password

The following warning message is displayed reminding the users to change the default Network Administrator password as soon as possible:

```
Warning: Please change the default Network Administrator password as soon
as possible. Note that in the next CNOS release (10.7.x or later), user
will be forced to change the default password upon first successful
login.
```

Weighted ECMP Routes

In traditional ECMP with next hops, each hop is added to the ECMP multipath once so traffic is distributed equally among the next hops. However, in some scenarios, traffic may use one path more than others, causing congestion. A lack of balance can occur because the ECMP hashing algorithm only considers the source, destination, or both when selecting the path, but not the use of the link.

Weighted ECMP lets you configure the multipath based on the use of each link, thus avoiding congestion and obtaining a better balance of traffic. This is achieved by adding the next hops in the multipath from one to four times.

Known Issues

This section describes known issues for CNOS 10.6 on the Lenovo ThinkSystem NE1032/NE1032T/NE1072T RackSwitch.

Privileged EXEC Mode Password Persistence

When upgrading the switch firmware image from CNOS version 10.3 or 10.4 to CNOS version 10.6, if there exists a previously configured encrypted password used to enter Privileged EXEC mode, it persists across the upgrade process. It is overwritten only when configuring a new clear text password and the switch running configuration is saved.

If a previously configured encrypted password is still used for entering Privileged EXEC configuration mode after the upgrade process, then only the first eight characters are checked when entering the password.

When downgrading the switch firmware image from CNOS version 10.6 to a previous version, if a previously configured Privileged EXEC encrypted password is present in the switch startup configuration file, then the password persist across the downgrade process. The password is required to enter Privileged EXEC configuration mode after the downgrade process is done. (ID: 119771)