Display network connectivity with neighbor discovery protocols

ONTAP System Manager

Barb Einarsen
December 09, 2020

NetApp®

Table of Contents

Display network connectivity with neighbor discovery protocols

In a data center, you can use neighbor discovery protocols to view network connectivity between a pair of physical or virtual systems and their network interfaces. ONTAP supports two neighbor discovery protocols: Cisco Discovery Protocol (CDP) and Link Layer Discovery Protocol (LLDP).

About this task

Neighbor discovery protocols enable you to automatically discover and view information about directly connected protocol-enabled devices in a network. Each device advertises identification, capabilities, and connectivity information. This information is transmitted in Ethernet frames to a multicast MAC address and is received by all neighboring protocol-enabled devices.

For two devices to become neighbors, each must have a protocol enabled and correctly configured. Discovery protocol functionality is limited to directly connected networks. Neighbors can include protocol-enabled devices such as switches, routers, bridges, and so on. ONTAP supports two neighbor discovery protocols, which can be used individually or together.

Cisco Discovery Protocol (CDP)

CDP is a proprietary link layer protocol developed by Cisco Systems. It is enabled by default in ONTAP for cluster ports, but must be enabled explicitly for data ports.

Link Layer Discovery Protocol (LLDP)

LLDP is a vendor-neutral protocol specified in the standards document IEEE 802.1AB. It must be enabled explicitly for all ports.

Use CDP to detect network connectivity

Using CDP to detect network connectivity consists of reviewing deployment considerations, enabling it on data ports, viewing neighbor devices, and adjusting CDP configuration values as needed. CDP is enabled by default on cluster ports.

CDP must also be enabled on any switches and routers before information about neighbor devices can be displayed.

CDP is also used by the cluster switch health monitor to automatically discover your cluster and management network switches.

Related information

System administration

Considerations for using CDP

By default, CDP-compliant devices send CDPv2 advertisements. CDP-compliant devices send CDPv1 advertisements only when they receive CDPv1 advertisements. ONTAP supports only CDPv1. Therefore, when an ONTAP node sends CDPv1 advertisements, CDP-compliant neighboring devices send back CDPv1 advertisements.

You should consider the following information before enabling CDP on a node:

- CDP is always enabled on cluster ports.

- CDP is disabled, by default, on all non-cluster ports.

- CDP is supported for all ports.

- CDP advertisements are sent and received by ports that are in the up state.

- CDP must be enabled on both the transmitting and receiving devices for sending and receiving CDP advertisements.

- CDP advertisements are sent at regular intervals, and you can configure the time interval.

- When IP addresses are changed for a LIF, the node sends the updated information in the next CDP advertisement.

  > **ℹ** Sometimes when LIFs are changed on the node, the CDP information is not updated at the receiving device side (for example, a switch). If you encounter such a problem, you should configure the network interface of the node to the down status and then to the up status.

- Only IPv4 addresses are advertised in CDP advertisements.

- For physical network ports with VLANs, all of the LIFs configured on the VLANs on that port are advertised.

- For physical ports that are part of an interface group, all of the IP addresses configured on that interface group are advertised on each physical port.

- For an interface group that hosts VLANs, all of the LIFs configured on the interface group and the VLANs are advertised on each of the network ports.

- For packets with MTU size equal to or greater than 1,500 bytes, only the number of LIFs that can fit into a 1500 MTU-sized packet is advertised.

Enable or disable CDP

To discover and send advertisements to CDP-compliant neighboring devices, CDP must be enabled on each node of the cluster. By default, CDP is enabled on all cluster ports of a node and disabled on all non-cluster ports of a node.

About this task

The `cdpd.enable` option controls whether CDP is enabled or disabled on the ports of a node:

- on enables CDP on non-cluster ports.

- off disables CDP on non-cluster ports; you cannot disable CDP on cluster ports.When CDP is disabled on a port that is connected to a CDP-compliant device, network traffic might not be optimized.

Steps

1. Display the current CDP setting for a node, or for all nodes in a cluster:

To view the CDP setting of...	Enter
A node	run - node <node_name> options cdpd.enabled
All nodes in a cluster	options cdpd.enabled

2. Enable or disable CDP on all ports of a node, or on all ports of all nodes in a cluster:

To enable or disable CDP on...	Enter...
A node	run -node node_name options cdpd.enable {on or off}
All nodes in a cluster	options cdpd.enable {on or off}

View CDP neighbor information

You can view information about the neighboring devices that are connected to each port of the nodes of your cluster, provided that the port is connected to a CDP-compliant device. You can use the `network device-discovery show -protocol cdp` command to view neighbor information.

About this task

Because CDP is always enabled for cluster ports, CDP neighbor information is always displayed for those ports. CDP must be enabled on non-cluster ports for neighbor information to appear for those ports.

Step

Display information about all CDP-compliant devices that are connected to the ports on a node in the cluster:

```
network device-discovery show -node node -protocol cdp
```

The following command shows the neighbors that are connected to the ports on node cluster-1_01:

```
network device-discovery show -node sti2650-212 -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface        Platform
----------- ------ ------------------------- ---------------  ----------------
sti2650-212/cdp
            e0M    RTP-LF810-510K37.gdl.eng.netapp.com(SAL1942R8JS)
                                             Ethernet1/14     N9K-C93120TX
            e0a    CS:RTP-CS01-510K35        0/8              CN1610
            e0b    CS:RTP-CS01-510K36        0/8              CN1610
            e0c    RTP-LF350-510K34.gdl.eng.netapp.com(FDO21521S76)
                                             Ethernet1/21     N9K-C93180YC-FX
            e0d    RTP-LF349-510K33.gdl.eng.netapp.com(FDO21521S4T)
                                             Ethernet1/22     N9K-C93180YC-FX
            e0e    RTP-LF349-510K33.gdl.eng.netapp.com(FDO21521S4T)
                                             Ethernet1/23     N9K-C93180YC-FX
            e0f    RTP-LF349-510K33.gdl.eng.netapp.com(FDO21521S4T)
                                             Ethernet1/24     N9K-C93180YC-FX
```

The output lists the Cisco devices that are connected to each port of the specified node. The `Remote Capability` column specifies the capabilities of each remote device. The following capabilities are available:

- R—Router
- T—Transparent bridge
- B—Source-route bridge
- S—Switch
- H—Host
- I—IGMP
- r—Repeater
- P—Phone

Configure the hold time for CDP messages

Hold time is the period of time for which CDP advertisements are stored in cache in neighboring CDP-compliant devices. Hold time is advertised in each CDPv1 packet and is updated whenever a CDPv1 packet is received by a node.

- The value of the cdpd.holdtime option should be set to the same value on both nodes of an HA pair.
- The default hold time value is 180 seconds, but you can enter values ranging from 10 seconds to 255 seconds.
- If an IP address is removed before the hold time expires, the CDP information is cached until the hold time expires.

Steps

1. Display the current CDP hold time for a node, or for all nodes in a cluster:

To view the hold time of…	Enter…
A node	run -node node_name options cdpd.holdtime
All nodes in a cluster	options cdpd.holdtime

2. Configure the CDP hold time on all ports of a node, or on all ports of all nodes in a cluster:

To set the hold time on…	Enter…
A node	run -node node_name options cdpd.holdtime holdtime
All nodes in a cluster	options cdpd.holdtime holdtime

Set the interval for sending CDP advertisements

CDP advertisements are sent to CDP neighbors at periodic intervals. You can increase or decrease the interval for sending CDP advertisements depending on network traffic and changes in the network topology.

- The value of the cdpd.interval option should be set to the same value on both nodes of an HA pair.
- The default interval is 60 seconds, but you can enter a value from 5 seconds to 900 seconds.

Steps

1. Display the current CDP advertisement time interval for a node, or for all nodes in a cluster:

To view the interval for…	Enter…
A node	run -node node_name options cdpd.interval
All nodes in a cluster	options cdpd.interval

2. Configure the interval for sending CDP advertisements for all ports of a node, or for all ports of all nodes in a cluster:

To set the interval for…	Enter…
A node	run -node node_name options cdpd.interval interval
All nodes in a cluster	options cdpd.interval interval

View or clear CDP statistics

You can view the CDP statistics for the cluster and non-cluster ports on each node to detect potential network connectivity issues. CDP statistics are cumulative from the time they were last cleared.

About this task

Because CDP is always enabled for cluster ports, CDP statistics are always displayed for traffic on those ports. CDP must be enabled on non-cluster ports for statistics to appear for those ports.

Step

Display or clear the current CDP statistics for all ports on a node:

If you want to...	Enter...
View the CDP statistics	run -node node_name cdpd show-stats
Clear the CDP statistics	run -node node_name cdpd zero-stats

Example of showing and clearing statistics

The following command shows the CDP statistics before they are cleared. The output displays the total number of packets that have been sent and received since the last time the statistics were cleared.

```
run -node node1 cdpd show-stats

RECEIVE
 Packets:         9116  | Csum Errors:        0  | Unsupported Vers:  4561
 Invalid length:     0  | Malformed:          0  | Mem alloc fails:      0
 Missing TLVs:       0  | Cache overflow:     0  | Other errors:        0

TRANSMIT
 Packets:         4557  | Xmit fails:         0  | No hostname:          0
 Packet truncated:   0  | Mem alloc fails:    0  | Other errors:        0

OTHER
 Init failures:      0
```

The following command clears the CDP statistics:

```
run -node node1 cdpd zero-stats
```

```
run -node node1 cdpd show-stats

RECEIVE
 Packets:            0 | Csum Errors:       0 | Unsupported Vers:    0
 Invalid length:     0 | Malformed:         0 | Mem alloc fails:     0
 Missing TLVs:       0 | Cache overflow:    0 | Other errors:        0

TRANSMIT
 Packets:            0 | Xmit fails:        0 | No hostname:         0
 Packet truncated:   0 | Mem alloc fails:   0 | Other errors:        0

OTHER
 Init failures:      0
```

After the statistics are cleared, they begin to accumulate after the next CDP advertisement is sent or received.

Use LLDP to detect network connectivity

Using LLDP to detect network connectivity consists of reviewing deployment considerations, enabling it on all ports, viewing neighbor devices, and adjusting LLDP configuration values as needed.

LLDP must also be enabled on any switches and routers before information about neighbor devices can be displayed.

ONTAP currently reports the following type-length-value structures (TLVs):

- Chassis ID

- Port ID

- Time-To-Live (TTL)

- System name

  The system name TLV is not sent on CNA devices.

Certain converged network adapters (CNAs), such as the X1143 adapter and the UTA2 onboard ports, contain offload support for LLDP:

- LLDP offload is used for Data Center Bridging (DCB).

- Displayed information might differ between the cluster and the switch.

  For example, the Chassis ID and Port ID data displayed by the switch might be different for CNA and non-CNA ports, but the data displayed by the cluster is consistent for these port types.

The LLDP specification defines access to the collected information through an SNMP MIB. However, ONTAP does not currently support the LLDP MIB.

Enable or disable LLDP

To discover and send advertisements to LLDP-compliant neighboring devices, LLDP must be enabled on each node of the cluster. By default, LLDP is disabled on all ports of a node.

About this task

The lldp.enable option controls whether LLDP is enabled or disabled on the ports of a node:

- `on` enables LLDP on all ports.
- `off` disables LLDP on all ports.

Steps

1. Display the current LLDP setting for a node, or for all nodes in a cluster:
   - Single node: `run -node node_name options lldp.enable`
   - All nodes: options `lldp.enable`

2. Enable or disable LLDP on all ports of a node, or on all ports of all nodes in a cluster:

To enable or disable LLDP on...	Enter...
A node	run -node node_name options lldp.enable {on
off}	All nodes in a cluster
options lldp.enable {on	off}

   - Single node:

     ```
     run -node node_name options lldp.enable {on|off}
     ```

   - All nodes:

     ```
     options lldp.enable {on|off}
     ```

View LLDP neighbor information

You can view information about the neighboring devices that are connected to each port of the nodes of your cluster, provided that the port is connected to an LLDP-compliant device. You use the network device-discovery show command to view neighbor information.

Step

Display information about all LLDP-compliant devices that are connected to the ports on a node in the cluster:

```
network device-discovery show -node node -protocol lldp
```

The following command shows the neighbors that are connected to the ports on node cluster-1_01. The output lists the LLDP-enabled devices that are connected to each port of the specified node. If the -protocol option is omitted, the output also lists CDP-enabled devices.

```
network device-discovery show -node cluster-1_01 -protocol lldp
Node/       Local  Discovered
Protocol    Port   Device                    Interface        Platform
----------- ------ ------------------------- ---------------  ----------------
cluster-1_01/lldp
            e2a    0013.c31e.5c60            GigabitEthernet1/36
            e2b    0013.c31e.5c60            GigabitEthernet1/35
            e2c    0013.c31e.5c60            GigabitEthernet1/34
            e2d    0013.c31e.5c60            GigabitEthernet1/33
```

Adjust the interval for transmitting LLDP advertisements

LLDP advertisements are sent to LLDP neighbors at periodic intervals. You can increase or decrease the interval for sending LLDP advertisements depending on network traffic and changes in the network topology.

About this task

The default interval recommended by IEEE is 30 seconds, but you can enter a value from 5 seconds to 300 seconds.

Steps

1. Display the current LLDP advertisement time interval for a node, or for all nodes in a cluster:
    ◦ Single node:

    ```
    run -node node_name options lldp.xmit.interval
    ```

    ◦ All nodes:

    ```
    options lldp.xmit.interval
    ```

2. Adjust the interval for sending LLDP advertisements for all ports of a node, or for all ports of all nodes in a cluster:

   ◦ Single node:

   ```
   run -node node_name options lldp.xmit.interval interval
   ```

   ◦ All nodes:

   ```
   options lldp.xmit.interval interval
   ```

Adjust the time-to-live value for LLDP advertisements

Time-To-Live (TTL) is the period of time for which LLDP advertisements are stored in cache in neighboring LLDP-compliant devices. TTL is advertised in each LLDP packet and is updated whenever an LLDP packet is received by a node. TTL can be modified in outgoing LLDP frames.

About this task

- TTL is a calculated value, the product of the transmit interval (lldp.xmit.interval) and the hold multiplier (lldp.xmit.hold) plus one.

- The default hold multiplier value is 4, but you can enter values ranging from 1 to 100.

- The default TTL is therefore 121 seconds, as recommended by IEEE, but by adjusting the transmit interval and hold multiplier values, you can specify a value for outgoing frames from 6 seconds to 30001 seconds.

- If an IP address is removed before the TTL expires, the LLDP information is cached until the TTL expires.

Steps

1. Display the current hold multiplier value for a node, or for all nodes in a cluster:

   ◦ Single node:

   ```
   run -node node_name options lldp.xmit.hold
   ```

   ◦ All nodes:

   ```
   options lldp.xmit.hold
   ```

2. Adjust the hold multiplier value on all ports of a node, or on all ports of all nodes in a cluster:

- Single node:

```
run -node node_name options lldp.xmit.hold hold_value
```

- All nodes:

```
options lldp.xmit.hold hold_value
```