Controller FAQs

SANtricity 11.8

NetApp
February 12, 2024

Table of Contents

Controller FAQs

What is auto-negotiation?

Auto-negotiation is the ability of a network interface to automatically coordinate its own connection parameters (speed and duplex) with another network interface.

Auto-negotiation is usually the preferred setting for configuring management ports; however, if the negotiation fails, mismatched network interface settings can severely impact network performance. In cases where that condition is unacceptable, you should manually set the network interface settings to a correct configuration. Auto-negotiation is performed by the controller's Ethernet management ports. Auto-negotiation is not performed by iSCSI host bus adapters.

If auto-negotiation fails, the controller attempts to establish a connection at 10BASE-T, half-duplex, which is the lowest common denominator.

What is IPv6 stateless address auto-configuration?

With stateless auto-configuration, hosts do not obtain addresses and other configuration information from a server.

Stateless auto-configuration in IPv6 features link-local addresses, multicasting, and the Neighbor Discovery (ND) protocol. IPv6 can generate the interface ID of an address from the underlying data link layer address.

Stateless auto-configuration and stateful auto-configuration complement each other. For example, the host can use stateless auto-configuration to configure its own addresses, but use stateful auto-configuration to obtain other information. Stateful auto-configuration allows hosts to obtain addresses and other configuration information from a server. Internet Protocol version 6 (IPv6) also defines a method whereby all of the IP addresses on a network can be renumbered at one time. IPv6 defines a method for devices on the network to automatically configure their IP address and other parameters without the need for a server.

Devices perform these steps when using stateless auto-configuration:

1. **Generate a link-local address** — The device generates a link-local address, which has 10 bits, followed by 54 zeros, and followed by the 64-bit interface ID.
2. **Test the uniqueness of a link-local address** — The node tests to make sure that the link-local address that it generates is not already in use on the local network. The node sends a neighbor solicitation message by using the ND protocol. In response, the local network listens for a neighbor advertisement message, which indicates that another device is already using the link-local address. If so, either a new link-local address must be generated or auto-configuration fails, and another method must be used.
3. **Assign a link-local address** — If the device passes the uniqueness test, the device assigns the link-local address to its IP interface. The link-local address can be used for communication on the local network but not over the Internet.
4. **Contact the router** — The node tries to contact a local router for more information about continuing the configuration. This contact is performed either by listening for router advertisement messages sent periodically by the routers or by sending a specific router solicitation message to ask a router for information about what to do next.
5. **Provide direction to the node** — The router provides direction to the node about how to proceed with auto-configuration. Alternatively, the router tells the host how to determine the global Internet address.

6. **Configure the global address** — The host configures itself with its globally unique Internet address. This address is generally formed from a network prefix provided to the host by the router.

Which do I choose — DHCP or manual configuration?

The default method for network configuration is Dynamic Host Configuration Protocol (DHCP). Always use this option unless your network does not have a DHCP server.

What is a DHCP server?

Dynamic Host Configuration Protocol (DHCP) is a protocol that automates the task of assigning an Internet Protocol (IP) address.

Each device that is connected to a TCP/IP network must be assigned a unique IP address. These devices include the controllers in your storage array.

Without DHCP, a network administrator enters these IP addresses manually. With DHCP, when a client needs to start TCP/IP operations, the client broadcasts a request for address information. The DHCP server receives the request, assigns a new address for a specified amount of time called a lease period, and sends the address to the client. With DHCP, a device can have a different IP address each time it connects to the network. In some systems, the IP address for the device can change even while the device is still connected.

How do I configure my DHCP server?

You must configure a Dynamic Host Configuration Protocol (DHCP) server to use static Internet Protocol (IP) addresses for the controllers in your storage array.

The IP addresses that your DHCP server assigns are generally dynamic and can change because they have a lease period that expires. Some devices, for example, servers and routers, need to use static addresses. The controllers in your storage array also need static IP addresses.

For information about how to assign static addresses, see the documentation for your DHCP server.

Why do I need to change the controller network configuration?

You must set the network configuration for each controller—its Internet Protocol (IP) address, subnetwork mask (subnet mask), and gateway—when you use out-of-band management.

You can set the network configuration by using a Dynamic Host Configuration Protocol (DHCP) server. If you are not using a DHCP server, you must enter the network configuration manually.

Where do I get the network configuration?

You can get the Internet Protocol (IP) address, subnetwork mask (subnet mask), and gateway information from your network administrator.

You need this information when you are configuring ports on the controllers.

What are ICMP PING responses?

Internet Control Message Protocol (ICMP) is one of the protocols of the TCP/IP suite.

The `ICMP echo request` and the `ICMP echo reply` messages are commonly known as `ping` messages. `Ping` is a troubleshooting tool used by system administrators to manually test for connectivity between network devices, and also to test for network delay and packet loss. The `ping` command sends an `ICMP echo request` to a device on the network, and the device immediately responds with an `ICMP echo reply`. Sometimes, a company's network security policy requires `ping` (`ICMP echo reply`) to be disabled on all devices to make them more difficult to be discovered by unauthorized persons.

When should I refresh the port configuration or the iSNS server from the DHCP server?

Refresh the DHCP server any time the server is modified or upgraded, and the DHCP information relevant to the current storage array and the storage array that you want to use has changed.

Specifically, refresh the port configuration or the iSNS server from the DHCP server when you know that the DHCP server will be assigning different addresses.

Refreshing a port configuration is destructive to all of the iSCSI connections on that port.

What should I do after configuring the management ports?

If you changed the IP address for the storage array, you might want to update the global array view in Unified Manager.

To update the global array view in Unified Manager, open the interface and go to **Manage › Discover**.

If you are still using the SANtricity Storage Manager, go to the Enterprise Management Window (EMW), where you must remove and re-add the new IP address.

Why is the storage system in non-optimal mode?

A storage system in non-optimal mode is due to an Invalid System Configuration state. Despite this state, normal I/O access to existing volumes is fully supported; however, System Manager will prohibit some operations.

A storage system might transition to Invalid System Configuration for one of these reasons:

- The controller is out of compliance, possibly because it has an incorrect submodel ID (SMID) code or it has exceeded the limit of premium features.
- An internal service operation is in progress, such as a drive firmware download.
- The controller exceeded the parity error threshold and went into lockdown.

- A general lockdown condition occurred.

Copyright information

Trademark information