Secure Network Device Provision

Contents

Introduction

This document describes the step-by-step approach for a Cisco device to securely onboard the network via DNS lookup.

Prerequisites

Requirements

- Basic knowledge of Cisco DNA Center (DNAC) Management
- Basic knowledge of SSL Certificates

Components Used

This document is based on Cisco DNA Center (DNAC) version 2.1.x.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

DNS lookup is a recommended way to onboard when network device and Cisco DNA Center (DNAC) controller are at remote sites and you want to provision a network device over the public internet.

There are different ways to onboard a network device with the use of Cisco Plug & Play Day0.

- DHCP Vendor-Specific Options
- DNS lookup
- Cisco Cloud Redirection

In order to have secure communication over the public internet, you need to install a Secure Certificate on DNAC. Follow this document to set up a DHCP server, DNS server, generate and install SSL certificate. If you already have the certificate + key and just need to install it on DNAC, then follow the document from Step 11. In this document:

- Cat9K device is the PNP agent.
- pnpserver.cisco.com is the FQDN name of the DNAC controller.
- Cisco switch is configured as DNS Server and DHCP Server.

Generate and Install SSL Certificate on DNAC

By default, DNAC comes with a pre-installed self-signed certificate good to onboard network devices in a private network. However, Cisco recommends that you import a valid X.509 certificate from your internal CA for secure communication to the onboard network device from a remote location over the public internet.

Here is an example to download and install the Open SSL certificate issued by Cisco on DNAC.

In order to download the certificate, first, you have to create a CSR.

Procedure

Step 1. Use an SSH client to log in to the Cisco DNA Center cluster and create a temporary folder under **/home/maglev**, for example, enter the command **mkdir tls-cert;cd tls-cert** while in the home directory.

Step 2. Before you proceed further, ensure that the Cisco DNA Center hostname (FQDN) is set at the time of the Cisco DNA Center configuration with the use of the **maglev cluster network display** command:

```
Input:

$maglev cluster network display

Output:

cluster_network:
 cluster_dns: 169.254.20.10
  cluster_hostname: fqdn.cisco.com
```

> **Note**: You need to have root privileges in order to run this command.

If the output field cluster_hostname is empty or is not what you want, add or change the Cisco DNA Center hostname (FQDN) with the use of the maglev cluster config-update command:

```
Input:

$maglev-config update

Output:

Maglev Config Wizard GUI
```

Note: You need to have root privileges in order to run this command.

Click **Next** until you see the step titled MAGLEV CLUSTER DETAILS that contains the input prompt Cluster hostname. Set the hostname to the desired Cisco DNA Center FQDN. Click **Next** and proceed until Cisco DNA Center is reconfigured with the new FQDN.

Step 3. Use a text editor of your choice, create a file named **openssl.cnf** and upload it to the directory that you created in the previous step. Use this example as your guide, but adjust it to fit your deployment.

- Adjust default_bits and default_md if your certificate authority admin team requires 2048/sha256 instead.
- Specify values for every field in the req_distinguished_name and alt_names sections. The only exception is the OU field, which is optional. Omit the OU field if your certificate authority admin team does not require it.
- The e-mail address field is optional; omit it if your certificate authority admin team does not require it.
- alt_names section: The certificate configuration requirements vary based on the Cisco DNA Center version.

Full support of FQDNs in the Cisco DNA Center certificate is available from Cisco DNA Center 2.1.1 onwards. For Cisco DNA Center versions earlier than 2.1.1, you need a certificate with IP addresses defined in the Subject Alternative Name (SAN) field. The alt_names section configurations for Cisco DNA Center versions 2.1.1 and later and Cisco DNA Center versions earlier than 2.1.1 are as follows:

Cisco DNA Center versions 2.1.1 and later:

1. Pay close attention to the alt_names section, which must contain all DNS names (which includes the Cisco DNA Center FQDN) that are used to access Cisco DNA Center, either by a web browser or by an automated process such as PnP or Cisco ISE. The first DNS entry in the alt_names section must contain Cisco DNA Center FQDN (DNS.1 = FQDN-of-Cisco-DNA-Center). You cannot add a wildcard DNS entry in place of Cisco DNA Center FQDN, but you can use a wildcard in subsequent DNS entries in the alt-names section (for PnP and other DNS entries). For example, *.example.com is a valid entry.

Important: If you use the same certificate for disaster recovery setup, wildcards are not allowed while you add a DNS entry for a disaster recovery system site in the alt_names section. However, we recommend that you use a separate certificate for a disaster recovery setup. For more information, see the "Add Disaster Recovery Certificate" section in the Cisco DNA Center Administrator Guide.

2. The alt_names section must contain FQDN-of-Cisco-DNA-Center as a DNS entry, and must match the Cisco DNA Center hostname (FQDN) set at the time of Cisco DNA Center configuration through the config wizard (in the input field "Cluster hostname"). Cisco DNA Center currently supports only one hostname (FQDN) for all interfaces. If you use both management and enterprise port on Cisco DNA Center for devices connection to Cisco DNA Center in your network, you must configure the GeoDNS policy to resolve to the management IP/virtual IP and enterprise IP/virtual IP for the Cisco DNA Center hostname (FQDN) based on the network from which the DNS query is received. Set up GeoDNS policy is not required if you use only the enterprise port on Cisco DNA Center for devices connection to Cisco DNA Center in your network.

Note: If you have enabled disaster recovery for Cisco DNA Center, you must configure the GeoDNS policy to resolve the disaster recovery management virtual IP and the disaster recovery enterprise virtual IP for the Cisco DNA Center hostname (FQDN) based on the network from which the DNS query is received.

3. Cisco DNA Center versions earlier than 2.1.1:

Pay close attention to the alt_names section, which must contain all IP addresses and DNS names that are used to access Cisco DNA Center, either by a web browser or by an automated process such as PnP or Cisco ISE. (This example assumes a three-node Cisco DNA Center cluster. If you have a standalone device, use SANs for only that node and the VIP. If you cluster the device later, you need to recreate the certificate to include the IP addresses of the new cluster members.)

If a cloud interface is not configured, omit the cloud port fields.

- In the extendedKeyUsage extension, the attributes serverAuth and clientAuth are mandatory. If you omit either attribute, Cisco DNA Center rejects the SSL certificate.
- If you import a self-signed certificate (not recommended), it must contain the X.509 Basic Constraints "CA:TRUE" extension.

Example openssl.cnf (Applicable for Cisco DNA Center versions 2.1.1 and later):

```
req_extensions = v3_req
distinguished_name = req_distinguished_name
default_bits = 4096
default_md = sha512
prompt = no

[req_distinguished_name]

C = <two-letter-country-code>
ST = <state-or-province>
L = <city>
O = <company-name>
OU = MyDivision
CN = FQDN-of-Cisco-DNA-Center
emailAddress = responsible-user@mycompany.tld

[ v3_req ]

basicConstraints = CA:FALSE
keyUsage = digitalSignature, keyEncipherment
extendedKeyUsage=serverAuth,clientAuth
subjectAltName = @alt_names

[alt_names]

DNS.1 = FQDN-of-Cisco-DNA-Center
DNS.2 = pnpserver.DomainAssignedByDHCPDuringPnP.tld
DNS.3 = *.example.com

!--- Example openssl.cnf (Applicable for Cisco DNA Center versions earlier than 2.1.1)

req_extensions = v3_req
distinguished_name = req_distinguished_name
default_bits = 4096
default_md = sha512
```

```
prompt = no

[req_distinguished_name]

C = <two-letter-country-code>
ST = <state-or-province>
L = <city> O = <company-name>
OU = MyDivision
CN = FQDN-of-Cisco-DNA-Center
emailAddress = responsible-user@mycompany.tld

[ v3_req ]

basicConstraints = CA:FALSE
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
extendedKeyUsage=serverAuth,clientAuth
subjectAltName = @alt_names

[alt_names]

DNS.1 = FQDN-of-Cisco-DNA-Center
DNS.2 = pnpserver.DomainAssignedByDHCPDuringPnP.tld
IP.1 = Enterprise port IP node #1
IP.2 = Enterprise port IP node #2
IP.3 = Enterprise port IP node #3
IP.4 = Enterprise port VIP
IP.5 = Cluster port IP node #1
IP.6 = Cluster port IP node #2
IP.7 = Cluster port IP node #3
IP.8 = Cluster port VIP
IP.9 = GUI port IP node #1
IP.10 = GUI port IP node #2
IP.11 = GUI port IP node #3
IP.12 = GUI port VIP
IP.13 = Cloud port IP node #1
IP.14 = Cloud port IP node #2
IP.15 = Cloud port IP node #3
IP.16 = Cloud port VIP
```

> **Note**: If you don’t include the cluster IP addresses in the **openssl.cnf** file, you cannot schedule software image activation. To fix this problem, add the cluster IP addresses as SANs to the certificate.

Use a text editor of your choice, create a file named **openssl.cnf** and upload it to the directory that you created in the previous step. Use this example as your guide, but adjust it to fit your deployment.

- Adjust default_bits and default_md if your certificate authority admin team requires 2048/sha256 instead.
- Specify values for every field in the req_distinguished_name and alt_names sections. The only exception is the OU field, which is optional. Omit the OU field if your certificate authority admin team does not require it.
- The emailAddress field is optional; omit it if your certificate authority admin team does not require it.
- alt_names section: The certificate configuration requirements vary based on the Cisco DNA Center version.
- The FQDNs support is available from Cisco DNA Center 2.1.1 onwards. For Cisco DNA Center versions earlier than 2.1.1, you need a certificate with IP addresses in the Subject

Alternative Name (SAN). The alt_names section configurations for Cisco DNA Center versions 2.1.1 and later, and Cisco DNA Center versions earlier than 2.1.1. are as follows:

- Cisco DNA Center versions 2.1.1 and later:Pay close attention to the alt_names section, which must contain all DNS names (which includes the Cisco DNA Center FQDN) that are used to access Cisco DNA Center, either by a web browser or by an automated process such as PnP or Cisco ISE.The first DNS entry in alt_names section must contain the FQDN of Cisco DNA Center (DNS.1 = FQDN-of-Cisco-DNA-Center). You cannot add a wildcard DNS entry in-place of FQDN of Cisco DNA Center. But you can use a wildcard in subsequent DNS entries in the alt-names section (for PnP and other DNS entries). For example, *.example.com is a valid entry.

Important: If you use the same certificate for disaster recovery setup, wildcards are not allowed while you add a DNS entry for a disaster recovery system site in the alt_names section. However, we recommend that you use a separate certificate for a disaster recovery setup. For more information, see the "Add Disaster Recovery Certificate" section in the Cisco DNA Center Administrator Guide.

- The alt_names section must contain FQDN-of-Cisco-DNA-Center as a DNS entry, and must match the Cisco DNA Center hostname (FQDN) set at the time of Cisco DNA Center configuration through the config wizard (in the input field "Cluster hostname").

Cisco DNA Center currently supports only one hostname (FQDN) for all interfaces. You must configure the GeoDNS policy to resolve to the management IP/virtual IP and enterprise IP/virtual IP for the Cisco DNA Center hostname (FQDN) based on the network from which the DNS query is received.

> **Note**: If you have enabled disaster recovery for Cisco DNA Center, you must configure the GeoDNS policy to resolve the disaster recovery management virtual IP and the disaster recovery enterprise virtual IP for the Cisco DNA Center hostname (FQDN) based on the network from which the DNS query is received.

- Cisco DNA Center versions earlier than 2.1.1:

Pay close attention to the alt_names section, which must contain all IP addresses and DNS names that are used to access Cisco DNA Center, either by a web browser or by an automated process such as PnP or Cisco ISE. (This example assumes a three-node Cisco DNA Center cluster. If you have a standalone device, use SANs for only that node and the VIP. If you cluster the device later, you need to recreate the certificate to include the IP addresses of the new cluster members.)

- If a cloud interface is not configured, omit the cloud port fields.
  - In the extendedKeyUsage extension, the attributes serverAuth and clientAuth are mandatory. If you omit either attribute, Cisco DNA Center rejects the SSL certificate.
  - If you import a self-signed certificate (not recommended), it must contain the X.509 Basic Constraints "CA:TRUE" extension.

Example openssl.cnf (Applicable for Cisco DNA Center versions 2.1.1 and later)

```
req_extensions = v3_reqdistinguished_name = req_distinguished_namedefault_bits = 4096default_md
= sha512prompt = no[req_distinguished_name]C = <two-letter-country-code>ST = <state-or-
province>L
= <city>O = <company-name>OU = MyDivisionCN = FQDN-of-Cisco-DNA-CenteremailAddress =
responsible-user@mycompany.tld [ v3_req ]basicConstraints = CA:FALSEkeyUsage = digitalSignature,
```

```
keyEnciphermentextendedKeyUsage=serverAuth,clientAuthsubjectAltName = @alt_names[alt_names]DNS.1
=
FQDN-of-Cisco-DNA-CenterDNS.2 = pnpserver.DomainAssignedByDHCPDuringPnP.tldDNS.3 = *.example.com
```

Example openssl.cnf (Applicable for Cisco DNA Center versions earlier than 2.1.1)

```
req_extensions = v3_reqdistinguished_name = req_distinguished_namedefault_bits = 4096default_md
= sha512prompt = no[req_distinguished_name]C = <two-letter-country-code>ST = <state-or-
province>L
= <city> O = <company-name>OU = MyDivisionCN = FQDN-of-Cisco-DNA-Centeron-GUI-portemailAddress =
responsible-user@mycompany.tld[ v3_req ]basicConstraints = CA:FALSEkeyUsage = nonRepudiation,
digitalSignature, keyEnciphermentextendedKeyUsage=serverAuth,clientAuthsubjectAltName =
@alt_names[alt_names]DNS.1 = FQDN-of-Cisco-DNA-Center-on-GUI-portDNS.2 =
FQDN-of-Cisco-DNA-Center-on-enterprise-portDNS.3 =
pnpserver.DomainAssignedByDHCPDuringPnP.tldIP.1 =
Enterprise port IP node #1IP.2 = Enterprise port IP node #2IP.3 = Enterprise port IP node #3IP.4
=
Enterprise port VIPIP.5 = Cluster port IP node #1IP.6 = Cluster port IP node #2IP.7 =
Cluster port IP node #3IP.8 = Cluster port VIPIP.9 = GUI port IP node #1IP.10 = GUI port IP node
#2IP.11
= GUI port IP node #3IP.12 = GUI port VIPIP.13 = Cloud port IP node #1IP.14 = Cloud port IP node
#2IP.15
= Cloud port IP node #3IP.16 = Cloud port VIP
```

> **Note**: If you don't include the cluster IP addresses in the **openssl.cnf** file, you cannot schedule software image activation. To fix this problem, add the cluster IP addresses as SANs to the certificate.

In this case, the next output is the config of my **openssl.conf**

```
req_extensions = v3_req
distinguished_name = req_distinguished_name
default_bits = 4096
default_md = sha512
prompt = no

[req_distinguished_name]

C = US
ST = California
L = Milpitas
O = Cisco Systems Inc.
OU = MyDivision
CN = noc-dnac.cisco.com
emailAddress = sit-noc-team@cisco.com

[ v3_req ]

basicConstraints = CA:FALSE
keyUsage = digitalSignature, keyEncipherment
extendedKeyUsage=serverAuth,clientAuth
subjectAltName = @alt_names

[alt_names]

DNS.1 = noc-dnac.cisco.com
DNS.2 = pnpserver.cisco.com
IP.1 = 10.10.0.160
IP.2 = 10.29.51.160
```

Step 4. Enter this command to create a private key. Adjust the key length to 2048 if required by

your certificate authority admin team. **openssl genrsa -out csr.key 4096**

Step 5. After the fields are populated in the **openssl.cnf** file, use the private key that you created in the previous step to generate the Certificate Signing Request.

```
openssl req -config openssl.cnf -new -key csr.key -out DNAC.csr
```

Step 6. Verify the Certificate Signing Request content and ensure that the DNS names (and IP addresses for the Cisco DNA Center version earlier than 2.1.1) are populated correctly in the Subject Alternative Name field.

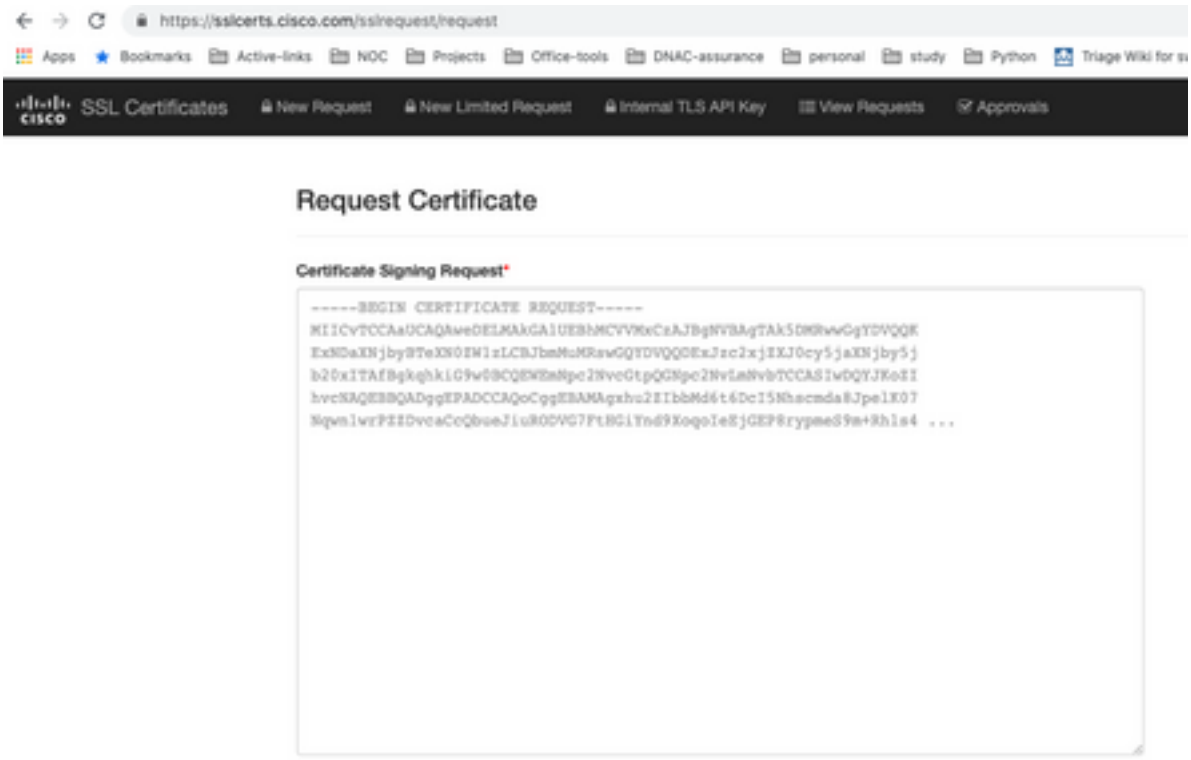
```
openssl req -text -noout -verify -in DNAC.csr
```

Step 7. Copy the Certificate Signing Request and paste it to a CA (example Cisco Open SSL).

Go to the link to download certificate. [Cisco SSL Certificates]

Click “Request Certificate” to download permanent certificate.

Or Click “Request Limited Test certificate” for limited purpose.



The user receives an email with the certificate info. Right-click and download all the three PEM files on your laptop. In this case, I have received 3 separate files, so skip step 8 and continue to Step 9.

Step 8. If the certificate issuer provides the certificate full chain (server and CA) in p7b:

Download the p7b bundle in DER format and save it as **dnac-chain.p7b**.

Copy the dnac-chain.p7b certificate to the Cisco DNA Center cluster through SSH.

Enter this command:

```
openssl pkcs7 -in dnac-chain.p7b -inform DER -out dnac-chain.pem -print_certs
```

Step 9. If the certificate issuer provides the certificate and its issuer CA chain in loose files:

Download the PEM (base64) files or use openssl to convert DER to PEM.

Concatenate the certificate and its issuer CA, start with the certificate, followed by subordinate CA, all the way to the root CA, and output it to dnac-chain.pem file.

```
cat certificate.cer subCA.cer rootCA.cer > dnac-chain.pem
```

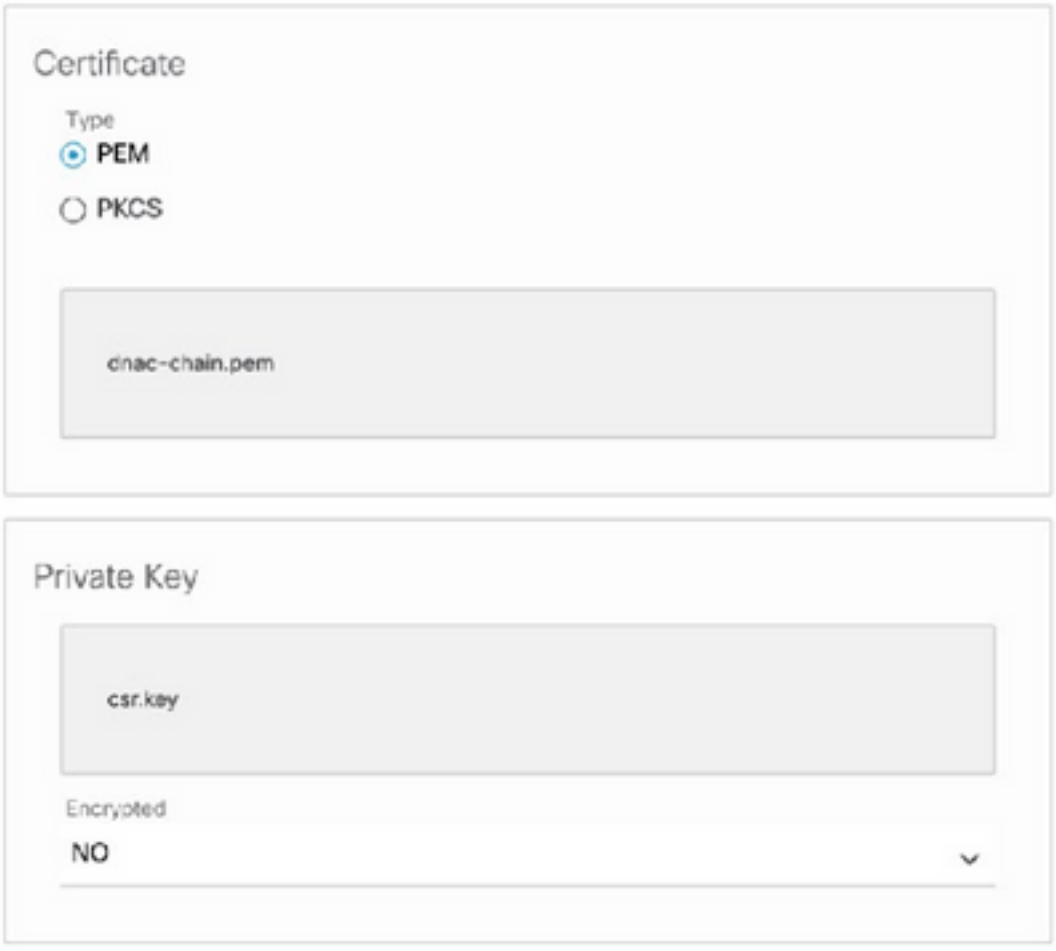
Step 10. Copy the file dnac-chain.pem from your laptop to Cisco DNA Center in tls-cert dir created above.

Step 11. In the Cisco DNA Center GUI, click the Menu icon () and choose System > Settings > Certificates.

Step 12. Click Replace Certificate.

Step 13. In the Certificate field, click the PEM radio button and perform the next tasks.

- For the Certificate field, import the **dnac-chain.pem** file, just drag and drop this file into the Drag n' Drop a File Here field.
- For the Private Key field, import the private key (csr.key), just drag and drop this file into the Drag n' Drop a File Here field.
- Choose No from the Encrypted drop-down list for the private key.



Step 14. Click Upload/Activate. Log out and log in on DNAC again.

DHCP Server Configuration

Configure a DHCP Server pool to assign IP address to the DUT. Also configures DHCP server

to send domain name and DNS server IP address.

```
ip dhcp pool PNP-A4
 network 192.0.2.0 255.255.255.252
 default-router 192.0.2.2
 domain-name cisco.com
 dns-server 203.0.113.23
```

DNS server configuration. Configure a DNS server in your network to resolve FQDN name of the DNAC.

```
 ip dns server
 ip host pnpserver.cisco.com <dnac-controller-ip>
```

Step 1. The new device to be onboarded is cabled and powered on. Since the startup configuration in NVRAM is empty, PnP agent is triggered and sends “Cisco PnP” in DHCP Option 60 in DHCP DISCOVER message.

Step 2. The DHCP server is not configured to recognize “Cisco PnP” in Option 60, it ignores Option 60. DHCP server assigns an IP address and sends DHCP offer along with configured domain name and DNS server IP address.

Step 3. PnP agent reads domain name and formulates fully qualified PnP server hostname and append the domain name to the string “pnpserver”. If the domain name is “example.com”, fully qualified hostname of PnP server would be “pnpserver.example.com”. PnP agent resolves “pnpserver.example.com” for its IP address with the DNS server received in the DHCP options.

Example when pnp agent is triggered for onboarding:

Power on a new switch or “write erase” followed by reload in case of brown field deployment

Verify the next workflow on the switch console.

```
Would you like to enter the initial configuration dialog? [yes/no]:

*Jan 19 22:23:21.981: %IOSXE-0-PLATFORM: R0/0: udev: disk0: has been inserted

Autoinstall trying DHCPv6 on Vlan1

Autoinstall trying DHCPv4 on Vlan1

Autoinstall trying DHCPv6 on Vlan1

Redundant RPs -

Autoinstall trying DHCPv6 on Vlan119

Autoinstall trying DHCPv6 on Vlan119

Acquired IPv4 address 192.0.2.3 on Interface Vlan119

Received following DHCPv4 options:
```

```
        domain-name     : cisco.com
        dns-server-ip   : 203.0.113.23
        si-addr         : 203.0.113.21

stop Autoip process

OK to enter CLI now...

pnp-discovery can be monitored without entering enable mode

Entering enable mode will stop pnp-discovery

Autoinstall trying DHCPv6 on Vlan119

Guestshell destroyed successfully

Autoinstall trying DHCPv6 on Vlan119

Press RETURN to get started!
```

Related Information

- PnP server discovery
- Cisco DNA Center Security Best Practices Guide
- **Technical Support & Documentation - Cisco Systems**