Deploy Router Using Secure ZTP

With Secure Zero Touch Provisioning (ZTP), you can securely and seamlessly provision thousands of network devices accurately within minutes and without any manual intervention.

Table 1: Feature History Table

Feature	Release Information	Feature Description
Secure Zero Touch Provisioning with Removable Storage Device	Release 7.3.2	This feature allows you to securely sign onboarding data in a removable storage device so that you can use the device for secure ZTP operations. This support gives you the plug-and-play flexibility for ZTP without any additional infrastructure requirements.
Secure Zero Touch Provisioning	Release 7.3.1	This feature allows devices in the network to establish a secure connection with the ZTP server and authenticate information using a three-step validation process involving validation of the network device, the ZTP server, and onboarding information. This eliminates security risks or malicious actions during remote provisioning. The **ztp secure-mode enable** command is introduced.

In a secured network such as datacenter, the zero-touch provisioning mechanism helps you provision hundreds of remote devices without your intervention. But, the access devices are typically in an insecure network. There is a high risk of malicious actions on the device, such as adding an unauthorized or infected device. Security is a critical aspect while remotely provisioning the network devices.

Secure ZTP combines seamless automation with security. Network devices can securely establish a connection with the ZTP server and authenticate the onboarding information that it receives. The process eliminates any security risks or malicious actions during the provisioning of remote devices.

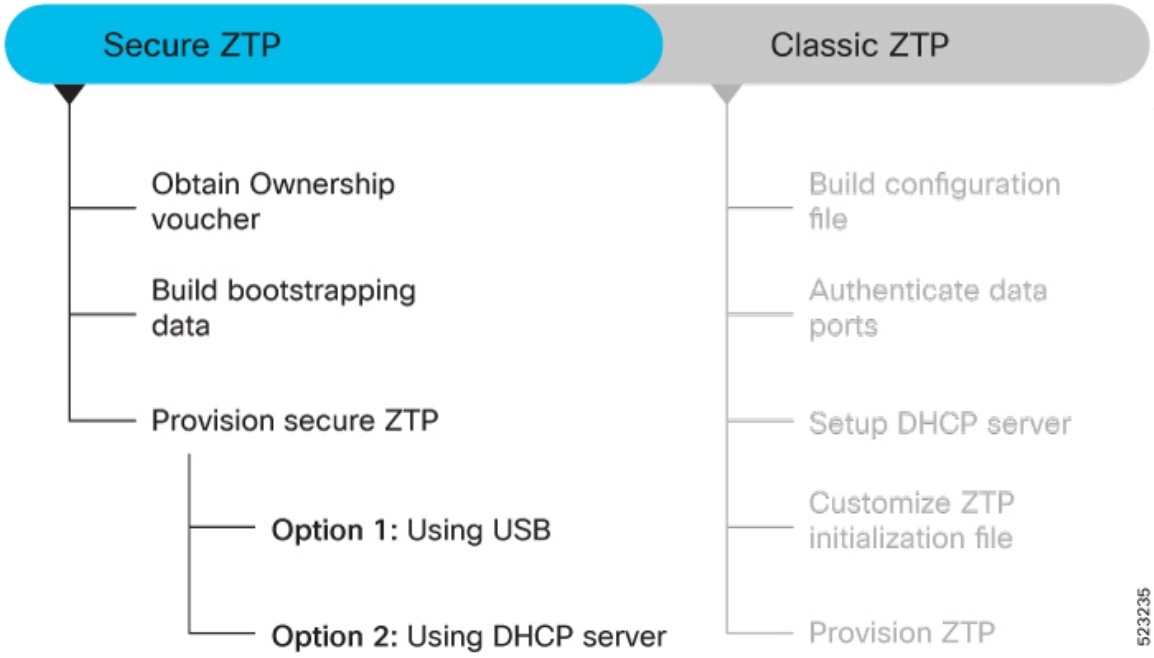
- ZTP helps you remotely provision a router securely anywhere in the network. Thus, eliminate the risk of malicious attacks or unauthorized ownership claims.
- Secure ZTP authenticates not only the onboarding network device but also validates the server authenticity and provisioning information that it is receiving from the ZTP server.

Cisco IOS XR software implements the secure zero touch provisioning capabilities as described in RFC 8572. Secure ZTP uses a three-step validation process to onboard the remote devices securely:

1. Router Validation: The ZTP server authenticates the router before providing bootstrapping data using the Trust Anchor Certificate (also called SUDI certificate).
2. Server Validation: The router device in turn validates the ZTP server to make sure that the onboarding happens to the correct network. Upon completion, the ZTP server sends the bootstrapping data (for example, a YANG data model) or artifact to the router.
3. Artifact Validation: The configuration validates the bootstrapping data or artifact received from the ZTP server.

Follow the workflow to understand the tasks involved in provisioning the router using secure ZTP.

Figure 1: Secure ZTP Workflow



This section contains the following topics:

Obtain Ownership Voucher

Ownership Voucher is used to identify the owner of the device by verifying the owner certificate that is stored in the device. Cisco supplies Ownership Voucher in response to your request. You must submit the Pinned Domain Certificate and device serial numbers with the request. Cisco generates and provides the Ownership Voucher to you.

Contact Cisco Support to obtain a voucher. Provide the following details to request for ownership voucher certificate:

- Pinned Domain certificate (PDC): PDC is an X.509 v3 certificate structure that uses Distinguished Encoding Rules (DER). This certificate is used by the router to trust a public key infrastructure in order to verify a domain certificate supplied to the router separately in the bootstrapping data. This certificate could be an end-entity certificate, including a self signed entity.
- Order details with the Serial numbers of the routers

For example,

```
{
       "expires-on": "2016-10-21T19:31:42Z",
       "assertion": "verified",
       "serial-number": "JADA123456789",
       "idevid-issuer": "base64encodedvalue==",
       "pinned-domain-cert": "base64endvalue==",
       "last-renewal-date": "2017-10-07T19:31:42Z"
   }
```

Based on the details that you provide, Cisco generates the ownership voucher in .vcj format. For example, DCA213140YX.vcj.

Build Bootstrapping Data

The following describe the components of secure ZTP:

- **Onboarding Device (Router):** The router is a Cisco device that you want to provision and connect to your network. Secure ZTP is supported only on platforms that have Hardware TAM support. Routers with HW TAM have the SUDI embedded in TAM.
- **DHCP Server:** The secure ZTP process relies on the DHCP server to provide the URL to access the bootstrapping information.
- **ZTP Server:** A ZTP server is any server used as a source of secure ZTP bootstrapping data and can be a RESTCONF or HTTPs server.

Note ZTP only supports single name-server. When the DHCP server has more than one server address configured, ZTP fails to apply the server configuration.

The ZTP server contains the following artifacts:

- Cisco IOS XR software images: You can download Cisco images, SMU, and patches using the Cisco Support & Downloads page.

- ZTP scripts: Contains the following libraries and you can build a script to initiate the ZTP process.
  - Python library: Includes IOS XR CLI (show commands and configuration commands), YANG-XML (ncclient, native Netconf client), and YANG-JSON (gnmic or gNMI client)).
  - BASH library: Includes IOS XR CLI show commands, configuration commands
- Bootstrapping Data

- **Bootstrapping Data:** It is the collection of data that the router obtains from the ZTP server during the secure ZTP process. You must create and upload the bootstrapping data in the ZTP server. For more information, refer RFC 8572.
  - The bootstrapping data mainly has three artifacts:
    - **Conveyed Information**: Conveyed Information contains the required bootstrapping data for the device. It contains either the redirect information or onboarding information to provision the device.

      For example:

```
module: ietf-sztp-conveyed-info

          yang-data conveyed-information:
            +-- (information-type)
               +--:(redirect-information)
               |  +-- redirect-information
               |     +-- bootstrap-server* [address]
               |        +-- address         inet:host
               |        +-- port?           inet:port-number
               |        +-- trust-anchor?   cms
               +--:(onboarding-information)
                  +-- onboarding-information
                     +-- boot-image
                     |  +-- os-name?              string
                     |  +-- os-version?           string
                     |  +-- download-uri*         inet:uri
                     |  +-- image-verification* [hash-algorithm]
                     |     +-- hash-algorithm    identityref
                     |     +-- hash-value        yang:hex-string
                     +-- configuration-handling?      enumeration
                     +-- pre-configuration-script?    script
                     +-- configuration?               binary
                     +-- post-configuration-script?   script
```

    - **Redirect Information**: Redirect information is used to redirect a device to another bootstrap server. The redirect information contains a list of bootstrap servers along with a hostname, an optional port, and an optional trust anchor certificate that the device uses to authenticate the bootstrap server.

      For Example:

```
{
     "ietf-sztp-conveyed-info:redirect-information" : {
       "bootstrap-server" : [
         {
           "address" : "sztp1.example.com",
           "port" : 8443,
            "trust-anchor" : "base64encodedvalue=="
         },
         {
```

```
            "address" : "sztp2.example.com",
            "port" : 8443,
            "trust-anchor" : "base64encodedvalue=="
          },
          {
            "address" : "sztp3.example.com",
            "port" : 8443,
            "trust-anchor" : "base64encodedvalue=="
          }
        ]
      }
    }
```

- **Onboarding Information:** Onboarding information provides data necessary for a device to bootstrap itself and establish secure connections with other systems. It specifies details about the boot image, an initial configuration the device must commit, and scripts that the device must execute.

  For Example:

```
{
     "ietf-sztp-conveyed-info:onboarding-information" : {
       "boot-image" : {
         "os-name" : "VendorOS",
         "os-version" : "17.2R1.6",
         "download-uri" : [ "https://example.com/path/to/image/file" ],
         "image-verification" : [
           {
             "hash-algorithm" : "ietf-sztp-conveyed-info:sha-256",
             "hash-value" : "ba:ec:cf:a5:67:82:b4:10:77:c6:67:a6:22:ab:\
   7d:50:04:a7:8b:8f:0e:db:02:8b:f4:75:55:fb:c1:13:b2:33"
           }
         ]
       },
       "configuration-handling" : "merge",
       "pre-configuration-script" : "base64encodedvalue==",
       "configuration" : "base64encodedvalue==",
       "post-configuration-script" : "base64encodedvalue=="
     }
   }
```

  - **Owner Certificate**: The owner certificate is installed on the router with the public key of your organization. The router uses the owner certificate to verify the signature in the conveyed information artifact using the public key that is available in the owner certificate.
  - **Ownership Voucher**: Ownership Voucher is used to identify the owner of the device by verifying the owner certificate that is stored in the device. Cisco supplies Ownership Voucher in response to your request. You must submit the Pinned Domain Certificate and device serial numbers with the request. Cisco generates and provides the Ownership Voucher to you.

- **Report Progress:** When the device obtains the onboarding information from a ZTP server, the router reports the bootstrapping progress to the ZTP server using the API calls.

  See RFC 8572 for the detailed report-progress messages that can be sent to the ZTP server.

  The following is the structure of the `report-progress` sent the progress message to a ZTP server.

```
+---x report-progress {onboarding-server}?
         +---w input
```

```
+---w progress-type         enumeration
+---w message?              string
+---w ssh-host-keys
|  +---w ssh-host-key* []
|     +---w algorithm    string
|     +---w key-data     binary
+---w trust-anchor-certs
   +---w trust-anchor-cert*   cms
```

The following example illustrates a device using the Yang module to post a progress report to a ZTP server with a `bootstrap complete` message:

```
{
        'progress-type': 'bootstrap-complete',
        'message': 'example message',
        'trust-anchor-certs': [{
                'trust-anchor-cert': 'base64encodedvalue=='
        'ssh-host-keys': [{
                'key-data': 'base64encodedvalue==',
                'algorithm': 'ssh-rsa'
        }, {
                'key-data': 'base64encodedvalue==',
                'algorithm': 'rsa-sha2-256'
        }]
}
```

```
RESPONSE from the ZTP server

   HTTP/1.1 204 No Content
   Date: Sat, 31 Oct 2015 17:02:40 GMT
   Server: example-server
```

Secure ZTP Options

Provision Secure ZTP Using USB

A Removable storage device such as a USB drive is an untrusted source of bootstrapping data. So, the onboarding information present in the removable storage device must always be signed.

Whenever the data is signed, it's mandatory that the Owner Certificate and Ownership Voucher must also be available. The removable storage device must contain the following three artifacts. For more information on the three artifacts, see Build Bootstrapping Data, on page 3.

- Conveyed Information
- Owner Certificate
- Ownership Voucher

The network administrator performs the following tasks as part of the initial setup for secure ZTP:

Before you begin

The network administrator performs the following tasks as part of the initial setup for secure ZTP:

- Ensure to enable secure ZTP on the router using the **ztp secure-mode enable** command and then reload the router.

- Contact Cisco Support to obtain a voucher. Provide the following details to request for ownership voucher certificate:
  - Pinned Domain certificate (PDC): PDC is an X.509 v3 certificate structure that uses Distinguished Encoding Rules (DER). This certificate is used by the router to trust a public key infrastructure in order to verify a domain certificate supplied to the router separately in the bootstrapping data. This certificate could be an end-entity certificate, including a self signed entity.
  - Order details with the Serial numbers of the routers

  For example,

```
{
        "expires-on": "2016-10-21T19:31:42Z",
        "assertion": "verified",
        "serial-number": "JADA123456789",
        "idevid-issuer": "base64encodedvalue==",
        "pinned-domain-cert": "base64endvalue==",
        "last-renewal-date": "2017-10-07T19:31:42Z"
    }
```

Step 1 Copy the following data to the removable storage device in the **EN9** directory in its root:

- Conveyed information: Conveyed information: Conveyed information must be named as `conveyed-information.cms` and must contain only the onboarding information and not the redirect information. The conveyed information consists of the following onboarding information:
  - Cisco IOS XR software images: You can download Cisco images, SMU, and patches using the Cisco Support & Downloads page.
  - ZTP scripts that include IOS XR configurations, pre, and post configuration scripts. During the secure ZTP process, secure ZTP executes the scripts to provision the router. You can build your script using one of the following methods:
    - Python library: Includes IOS XR CLI (show commands and configuration commands) and YANG-XML (`ncclient`, `native Netconf client`).
    - BASH library: Includes IOS XR CLI show commands, configuration commands.
- Owner certificate: The owner certificate must be named as `owner-certificate.cms`.
- Ownership vouchers: The ownership vouchers must be named as `ownership-voucher.vcj`.

Step 2 Plug in the removable storage device into the router.

Step 3 Power ON the router.

Here is the high-level workflow of the Secure ZTP process using a removable storage device:

a. When you boot the device with an IOS-XR image, the secure ZTP process verifies if the secure ZTP mode (`secure-ztp mode`) is enabled. If not enabled, the device boots normally.

b. The device verifies if the USB is enabled in the `ztp.ini` file. By default, the USB is enabled and assigned the highest priority in the fetcher priority in the `ztp.ini` file.

Fetcher priority defines how secure ZTP can get the provisioning details. By default, each port has a fetcher priority defined in the `ztp.ini` file. The fetcher priority range is from 0 to 9. The lower the number higher is the priority. The value 0 has the highest priority and 9 has the lowest priority.

The following example shows the sample of the `ztp.ini` file:

```
[Startup]
start: True
retry_forever: True

[Fetcher Priority]
USB: 0

Mgmt4:  1
Mgmt6:  2
DPort4: 3
DPort6: 4
```

c. Secure ZTP checks for a removable storage device on the router. If the removable storage device isn't available, the secure ZTP process moves to the next fetcher as defined in the fetcher priority of the `ztp.ini`file.

d. If a removable storage device is available, the router scans for the `EN9` directory in the root of the removable storage device.

If the `EN9` directory isn't available, the secure ZTP process moves to the next fetcher as defined in the fetcher priority of the `ztp.ini`file.

e. **Artifact Validation**:

The router validates the artifacts received from the removable storage device.

1. The router validates the ownership voucher and extracts the `pinned-domain-cert` node, an X.509 certificate from the ownership voucher to verify the owner certificate.
2. The router authenticates the owner certificate by performing the X.509 certificate path verification process on the trusted certificate.
3. Finally, the router verifies whether the conveyed information artifact is signed by the validated owner certificate.

f. **Provision the router**:

1. The device first processes the boot image information.
2. Executes the preconfiguration script and then commits the initial configuration.
3. Execute the post configuration script.

g. After the onboarding process is completed, router is operational.

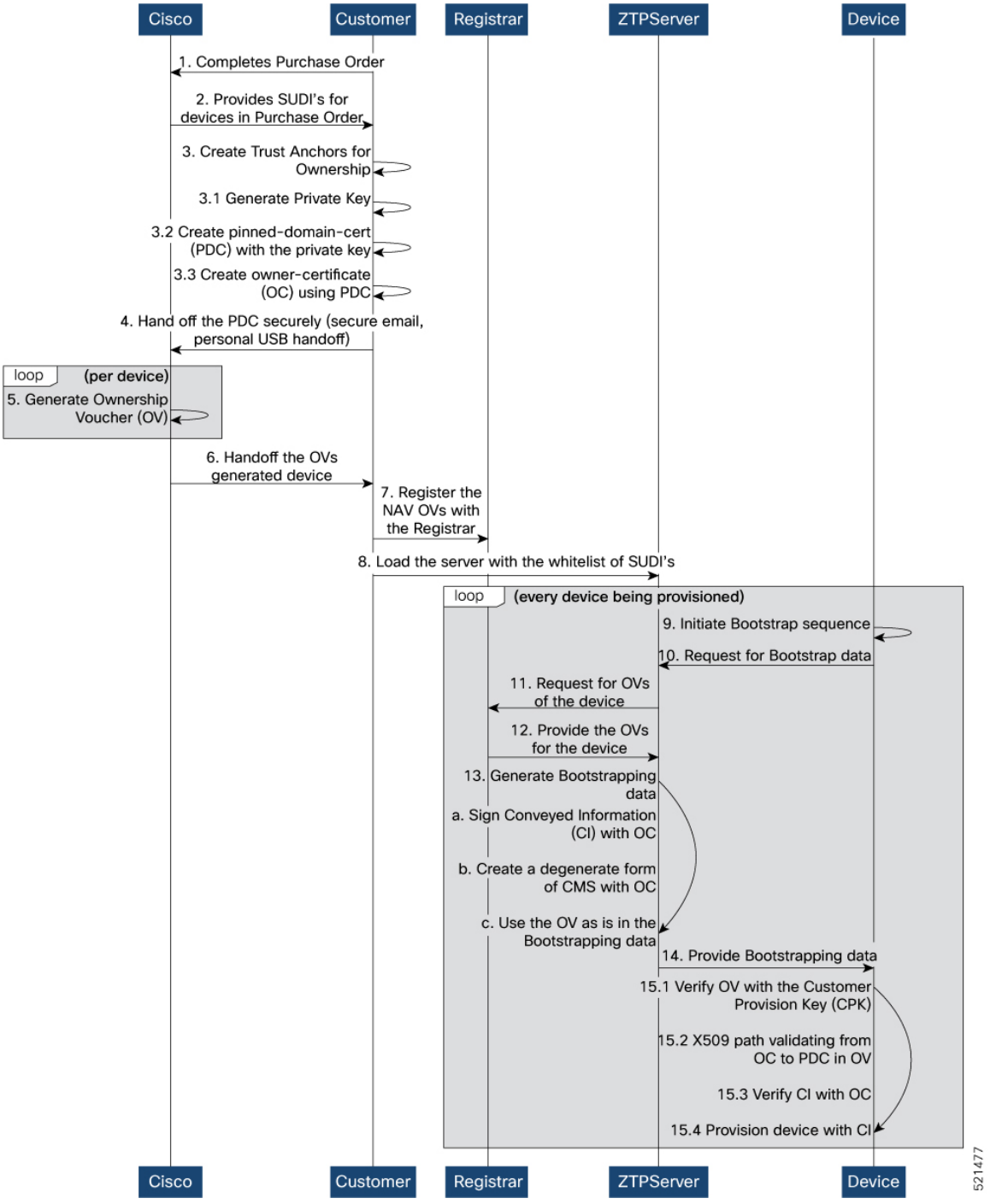
Note If there is a failure in any of the steps, the secure ZTP process moves to the next fetcher as defined in the fetcher priority of the `ztp.ini` file.

Provision Secure ZTP Using DHCP Server

When you boot the device, the ZTP process initiates automatically if the device does not have a prior configuration. During the process, the router receives the details of the configuration file from the DHCP server.

The following figure illustrates the end-to-end sequence of the Secure ZTP process:

Figure 2: End-to-end sequence of the Secure ZTP process



Before you begin

The network administrator performs the following tasks as part of the initial setup for secure ZTP:

- Ensure to enable secure ZTP on the router using the **ztp secure-mode enable** command and then reload the router.
- Contact Cisco Support to obtain a voucher. Provide the following details to request for ownership voucher certificate:
  - Pinned Domain certificate (PDC): PDC is an X.509 v3 certificate structure that uses Distinguished Encoding Rules (DER). This certificate is used by the router to trust a public key infrastructure in order to verify a domain certificate supplied to the router separately in the bootstrapping data. This certificate could be an end-entity certificate, including a self signed entity.
  - Order details with the Serial numbers of the routers

  For example,

```
{
        "expires-on": "2016-10-21T19:31:42Z",
        "assertion": "verified",
        "serial-number": "JADA123456789",
        "idevid-issuer": "base64encodedvalue==",
        "pinned-domain-cert": "base64endvalue==",
        "last-renewal-date": "2017-10-07T19:31:42Z"
    }
```

Step 1 Upload the following bootstrapping data to the ZTP server. Steps to upload may vary depending on the server that you're using, refer to the documentation provided by your vendor.

- Cisco IOS XR software images: You can download Cisco images, SMU, and patches using the Cisco Support & Downloads page.
- ZTP scripts that include IOS XR configurations, pre, and post configuration scripts. Build a script to initiate the ZTP process. See Build Configuration File.
  - Python library: Includes IOS XR CLI (show commands and configuration commands) and YANG-XML (`ncclient`, `native Netconf client`).
  - BASH library: Includes IOS XR CLI show commands, configuration commands
- Serial numbers of the routers you plan to onboard using ZTP
- Owner certificates
- Pinned Domain Certificate (PDC)
- Ownership vouchers

Step 2 Set up the DHCP server to provide the redirect URL to the router:

Before triggering the secure ZTP process, configure the DHCP server to provide the location of the IOS-XR image to the router. For information on how to configure the DHCP server, see your DHCP server documentation.

Configure the following parameters in the DHCP server:

- `option-code`: The DHCP SZTP redirect Option has the following parameters:
  - OPTION_V4_SZTP_REDIRECT (143): Use this DHCP v4 code for IPV4.
  - OPTION_V6_SZTP_REDIRECT (136): Use this DHCP v4 code for IPV6.

For example, `option dhcp6.bootstrap-servers code 136 = text;`

- `option-length`: The option length in octets
- `bootstrap-servers`: A list of servers for the onboarding device to contact the servers for the bootstrapping data.
- `bootfile-url` : The URI of the SZTP bootstrap server should use the HTTPS URI scheme and it should be in the following format:

  `"https://<ip-address-or-hostname>[:<port>]".`

Step 3 Power on the router.

Here is the high-level workflow of the Secure ZTP process using a removable storage device:

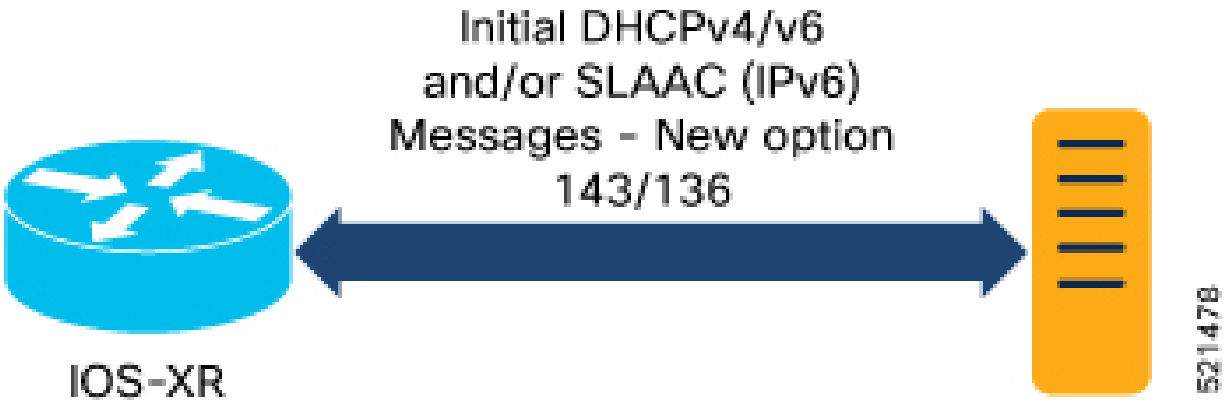
a. When you boot the device with an IOS-XR image, the secure ZTP process verifies if the secure ZTP mode (`secure-ztp mode`) is enabled. If not enabled, the device boots normally.

Note When `secure-ztp mode` is enabled, the ZTP process accepts only the `secure-redirect-URL` and ignores the presence of boot file name option from the DHCP response.

b. **DHCP discovery**:

1. The router initiates a DHCP request to the DHCP server.
2. The DHCP server responds with a DHCPv4 143 address option (for IPv4 addressing) or a DHCPv6 136 option (for IPv6 addressing). In addition, URLs to access bootstrap servers for further configuration is also listed.

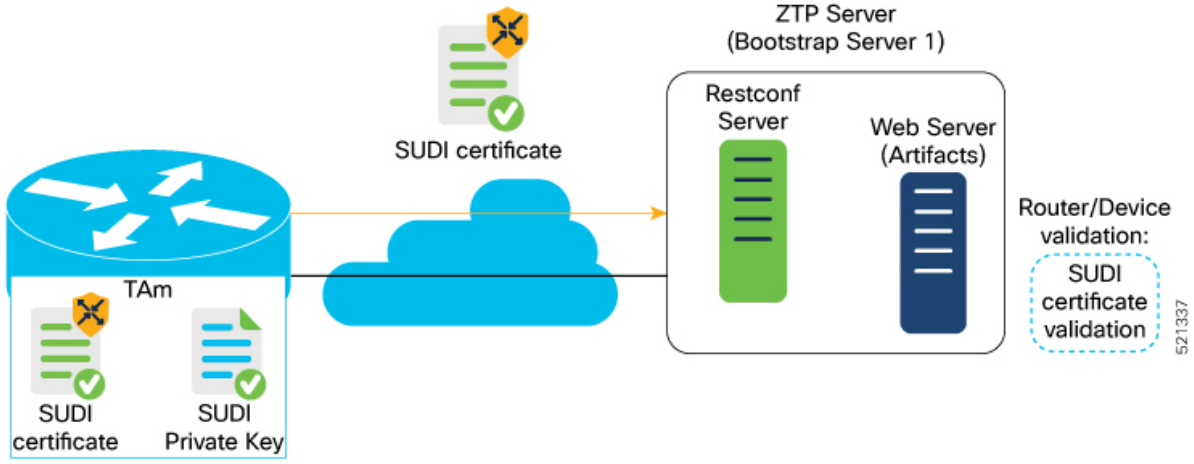
Figure 3: DHCP discovery



c. **Router validation**:

1. After receiving the URL from the DHCP server, the router sends an HTTPs request to the RESTCONF or HTTPs server using the specified URL. Along with the HTTPs request, the device sends the client certificate that is provided by the manufacturer (also called SUDI certificate). This certificate identifies and authenticates itself to the ZTP server.

Figure 4: Router Validation for Secure ZTP Provisioning

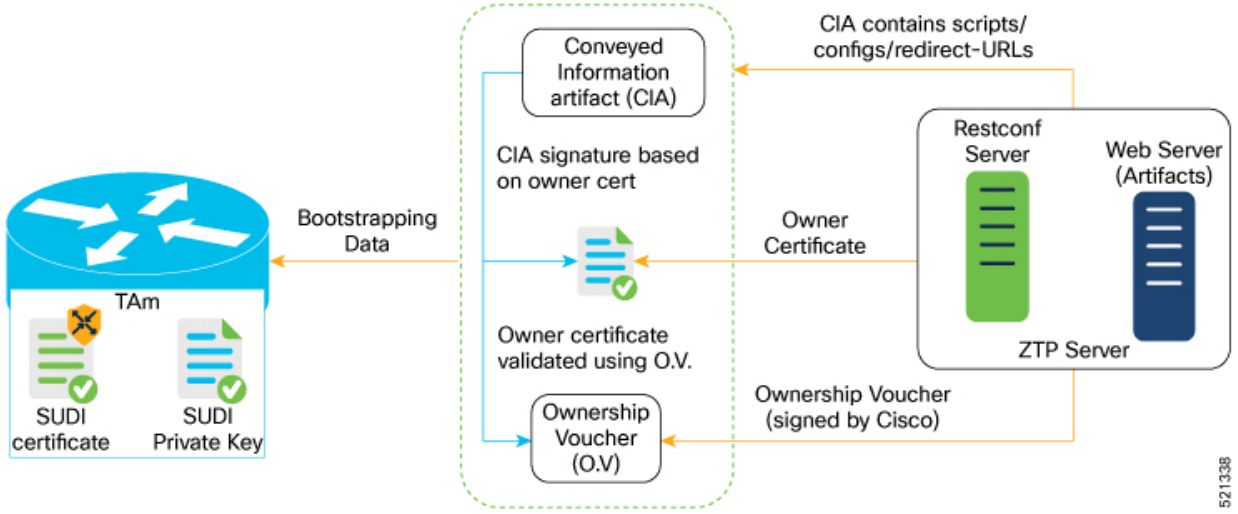


2. The RESTCONF or HTTPs server verifies the received SUDI certificate with the public certificate that it contains. Cisco issues the public certificate to ensure that the onboarding device is an authorized Cisco device.
3. After the onboarding device is authenticated, the web server sends the required artifacts along with the secure ZTP yang model to the onboarding device.

d. Server validation :

The router receives the yang model that contains Owner Certificate, Ownership Voucher, and Conveyed Information artifact. The router verifies the ownership voucher by validating its signature to one of its preconfigured trusts anchors and downloads the image. When the router obtains the onboarding information, it reports the bootstrapping progress to the ZTP server. See RFC 8572 for the progress information.

Figure 5: Server Validation for Secure ZTP Provisioning



e. Artifact Validation:

The router validates the artifact received from the ZTP server.

1. The device extracts the `pinned-domain-cert` node, an X.509 certificate from the ownership voucher to verify the owner certificate.
2. The device authenticates the owner certificate by performing the X.509 certificate path verification process on the trusted certificate.
3. Finally, the device verifies whether the conveyed information artifact is signed by the validated owner certificate.

f. **Provision the device**:

1. The device first processes the boot image information.
2. Executes the pre-configuration script and then commits the initial configuration
3. Execute the post configuration script.

g. After the onboarding process is completed, the network device is operational.