



Possibilities

#CiscoLive

3 Steps to Design Cisco SD-WAN On-Prem - Addendum

Andraz Piletic, Technical Solutions Architect / Instructor
Prashant Tripathi, Global Technical Solutions Architect
DGTL-BRKRST-2559



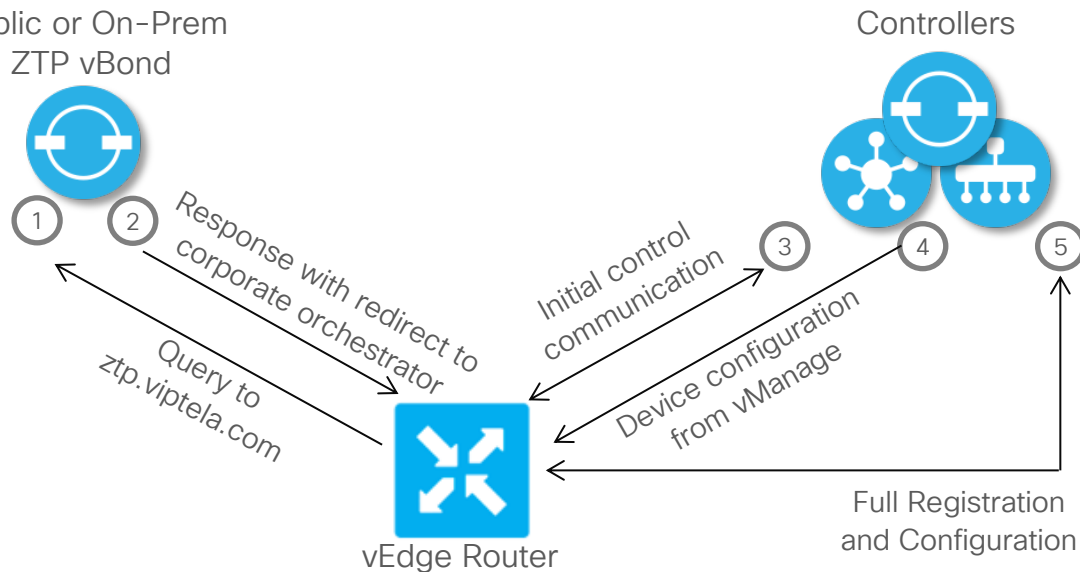
#CiscoLive



Agenda

- Introduction
- On-Prem Zero Touch Provisioning
 - Viptela OS Specifics
 - IOS-XE Specifics
- On-Prem ZTP vBond Deployment

Zero Touch Provisioning – Viptela OS



- Public or On-Prem ZTP vBond can redirect to cloud hosted or On-Prem controllers.
- New devices are linked to organization using the Smart Account when placing order.
- Additional devices can be associated with the customer using the PnP Connect portal on <https://software.cisco.com>.

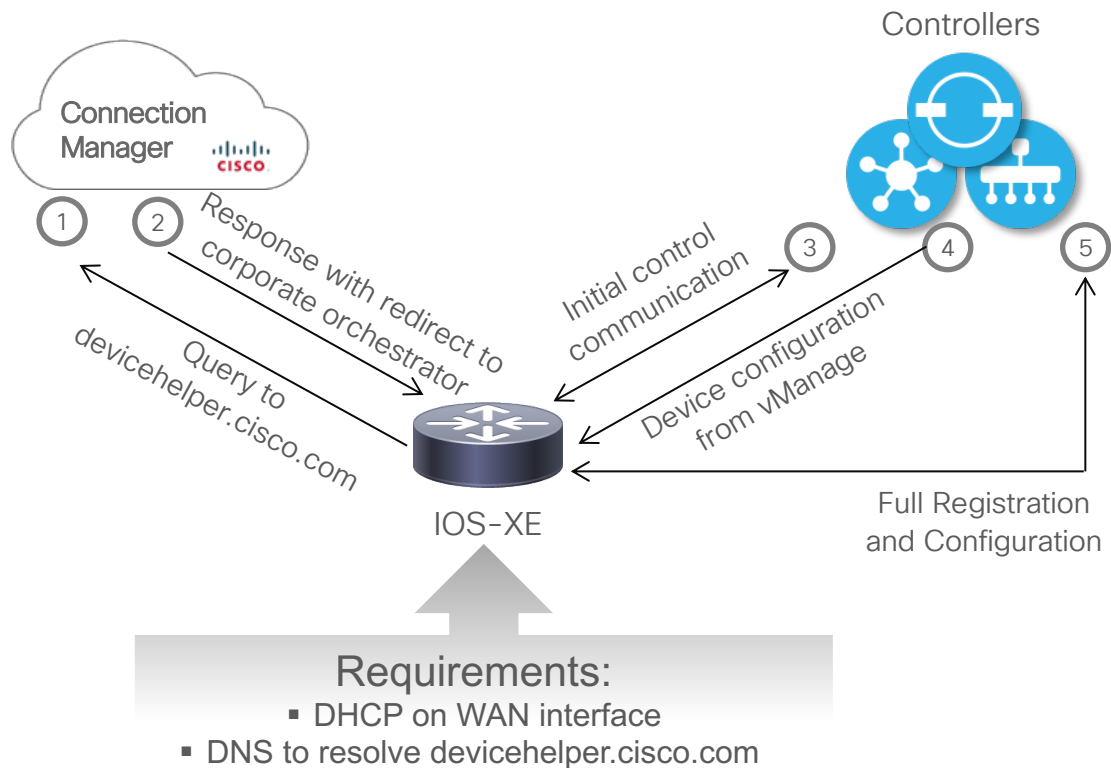
Option1:

- DHCP on WAN interface
- DNS to resolve ztp.viptela.com

Option2:

- Discover local addressing via ARP
- Google DNS: resolve ztp.viptela.com

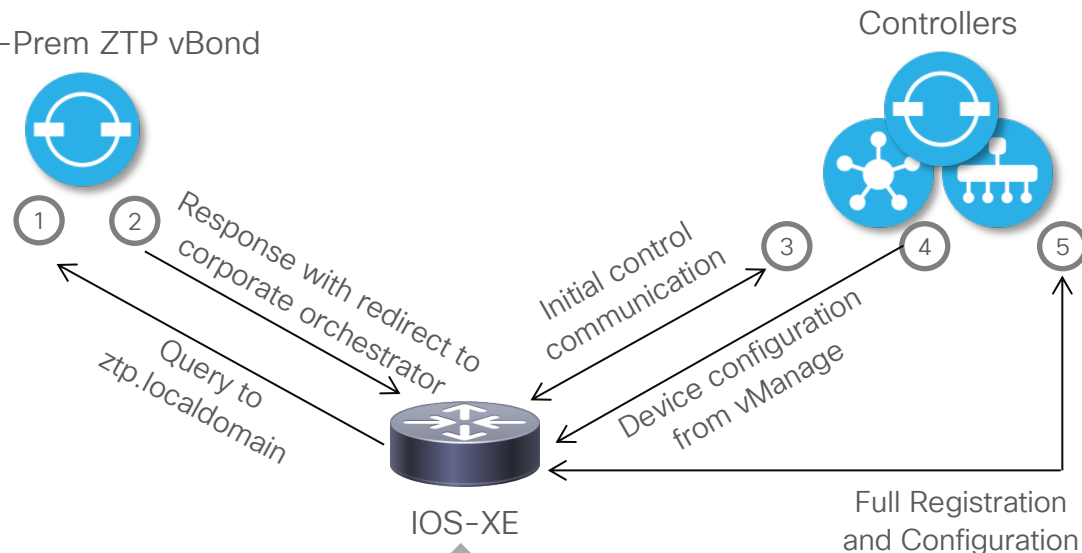
Zero Touch Provisioning - IOS-XE (Cloud Hosted)



- The PnP Connection Manager can redirect to cloud-hosted or On-Prem controllers.
- New devices are linked to organization using the Smart Account when placing order.
- Additional devices can be associated with the customer using the PnP Connect portal on <https://software.cisco.com>.

Zero Touch Provisioning - IOS-XE (On-Prem)

On-Prem ZTP vBond



Requirements:

- DHCP on WAN interface
- DNS to resolve ztp.localdomain, where local domain is learned via DHCP

- On-Prem ZTP vBond can redirect to cloud hosted or On-Prem controllers.
- New devices are linked to organization using the Smart Account when placing order.
- Additional devices can be associated with the customer using the PnP Connect portal on <https://software.cisco.com>.
- Available since IOS-XE 17.3

ZTP – WAN Edge – Static IP Support

```
#cloud-boothook
system
  personality          vedge
  device-model         vedge-ISR-4321
  host-name            WanEdge
  system-ip            10.255.255.121
  site-id              21
  organization-name     "CiscoLive 2020 BRKRST-2559"
  console-baud-rate     9600
  vbond 10.0.0.23 port 12346
  !
  !
  !
interface GigabitEthernet0/0/0
  no shutdown
  ip address 192.168.10.10 255.255.255.0
exit
!
ip route 0.0.0.0 0.0.0.0 192.168.10.1
```



- Upon bootup, the router searches bootflash: or usbflash: for filename ciscosdwan.cfg.
- The config file with basic interface configuration, Root CA, Organization Name, vBond information, is fed into the PnP process.
- Supported only on SD-WAN IOS-XE (since 16.10).



Setting Up On-Prem ZTP vBond Server

Configuring On-Prem ZTP vBond Server

Dedicated vBond server can act as a ZTP server. Required steps:

1. Activate the ZTP role.

```
vBondZTP(config)# system vbond ip-address local ztp-server
```

2. Obtain a signed certificate by a trusted CA (Symantec / Digicert).
3. Define and upload the whitelist file.
4. Configure a local DNS server to resolve ztp.viptela.com and ztp.localdomain with ZTP vBond IP.
5. Define device templates.

Obtaining Signed Certificate by Trusted CA

```
vBondZTP# request csr upload /home/admin/ztp.csr
Uploading CSR via VPN 0
Enter organization-unit name           : ZTPvBond
Re-enter organization-unit name        : ZTPvBond
Generating private/public pair and CSR for this vbond device
Generating CSR for this vbond device   .....[DONE]
Copying ... /home/admin/ztp.csr via VPN 0
CSR upload successful
```

- Generate and submit CSR to [Symantec Certificate Enrollment portal](#)

Obtaining Signed Certificate by Trusted CA (Cont.)

```
vBondZTP# request certificate install /home/admin/ztp.pem
```

```
Installing certificate via VPN 0
```

```
Copying ... /home/admin/ztp.pem via VPN 0
```

```
Successfully installed the certificate
```

```
vBondZTP# show certificate installed
```

```
Data:
```

```
Version: 3 (0x2) Serial Number: 6f:3a:61:cd:a8:de:3e:d5:e7:b1:b9
```

```
Signature Algorithm: sha256WithRSAEncryption
```

```
Issuer: C=US, O=Symantec Corporation, OU=Symantec Trust Network,  
CN=Symantec Class 3 Secure Server CA - G4
```

```
Validity
```

```
Not Before: Jul 30 00:00:00 2020 GMT
```

```
Not After : Jul 31 23:59:59 2021 GMT
```

```
Subject: C=US, ST=California, L=San Jose, O=vIPTela Inc,  
OU=ZTPvBond, CN=vbond-088b7cc2-a905-2f4ee1729bf9-0.viptela.com
```

Uploading The ZTP Whitelist Chassis File

```
vBondZTP# vshell
vBondZTP:~$ cat ztp-chassis-file
1920C,6123,valid,10.0.0.22,12346,CiscoLive BRKRST-2559,/home/admin/ca.crt
```

Define and verify chassis file

```
vBondZTP# request device-upload chassis-file /home/admin/ztp-chassis-file
```

```
Uploading chassis numbers via VPN 0
Copying ... /home/admin/ztp-chassis-file via VPN 0
Successfully loaded the chassis numbers file to the database.
Uploading the serial numbers to the vedge-list ...
Uploading serial numbers via VPN 0
Copying ... /home/admin/ztp-chassis-file via VPN 0
Successfully loaded the vEdge serial numbers
```

Apply chassis file

```
vBondZTP# show ztp entries
```

INDEX	NUMBER	CHASSIS SERIAL	VALIDITY	VBOND IP	PORT	ORGANIZATION	NAME	ROOT CERT	PATH
1	1920C	6123	valid	10.0.0.22	12346	CiscoLive	BRKRST-2559	/home/admin/ca.crt	

Validate ZTP entries

Thank you



Possibilities

#CiscoLive