数字网络架构(DNA)中心的局域网自动化提示和诀窍

目录

简介

本文档概述了局域网(LAN)自动化，以帮助您诊断LAN自动化在数字网络架构(DNA)中心中无法按预期工作时的问题。

作者：Alexandro Carrasquedo，Cisco TAC工程师。

词汇

即插即用(PnP)代理：您刚打开的新设备，无配置，无证书，将由DNA中心自动配置。

种子设备：DNA中心已调配并充当动态主机配置协议(DHCP)服务器的设备。

先决条件

要求

思科强烈建议您对LAN自动化和即插即用解决方案有一定的了解。概述了LAN自动化，尽管它基于DNA中心1.0，但DNA中心1.1及更高版本也采用相同的概念。

背景信息

LAN自动化是一种接近零接触的部署解决方案，使您能够使用ISIS作为底层路由协议来配置和调配网络设备。

开始使用前

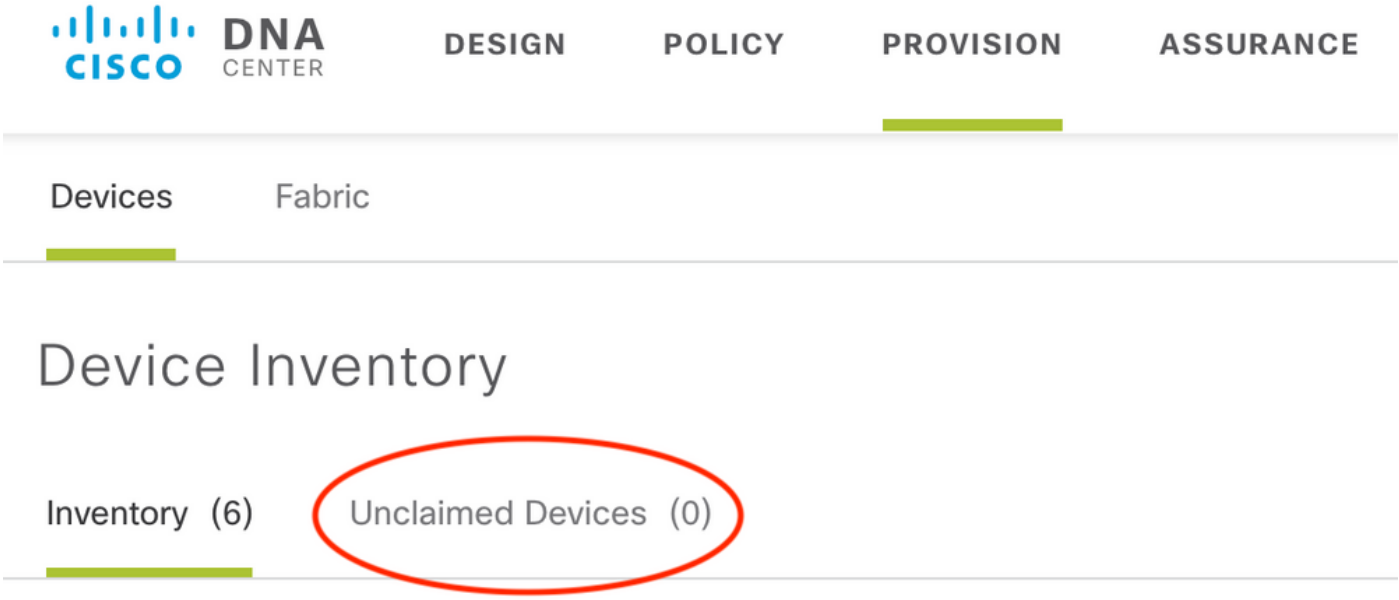
在运行LAN自动化之前，请确保PnP代理在NVRAM中未加载任何证书。

```
Edge1#dir nvram:*.cer
Directory of nvram:/*.cer

Directory of nvram:/

    4  -rw-         820                    <no date>  IOS-Self-Sig#1.cer
    6  -rw-         763                    <no date>  kube-ca#468ACA.cer
    7  -rw-         882                    <no date>  sdn-network-#616F.cer
    8  -rw-         807                    <no date>  sdn-network-#4E13CA.cer
2097152 bytes total (2033494 bytes free)
Edge1#delete nvram:*.cer
```

确保在Provisioning > Devices > Device Inventory页面中没有任何未申请的设备：



因为CSCvh68847，某些堆栈可能不会离开未声明的状态，您可能会收到ERROR_STACK_UNSUPPORTED错误消息。当LAN自动化尝试声明设备是一台交换机时，会出现此消息。但是，由于设备是Catalyst 9300交换机堆叠，LAN自动化无法声明该设备，设备显示为未声明。同样，PnP不会声明设备是堆栈，因此设备未调配。

LAN自动化在运行时要执行哪些步骤？

DNA中心使用DHCP配置调配种子设备。种子设备获取的IP地址范围是您为站点保留IP地址池时定义的初始池的段。请注意，此池必须至少为/25。

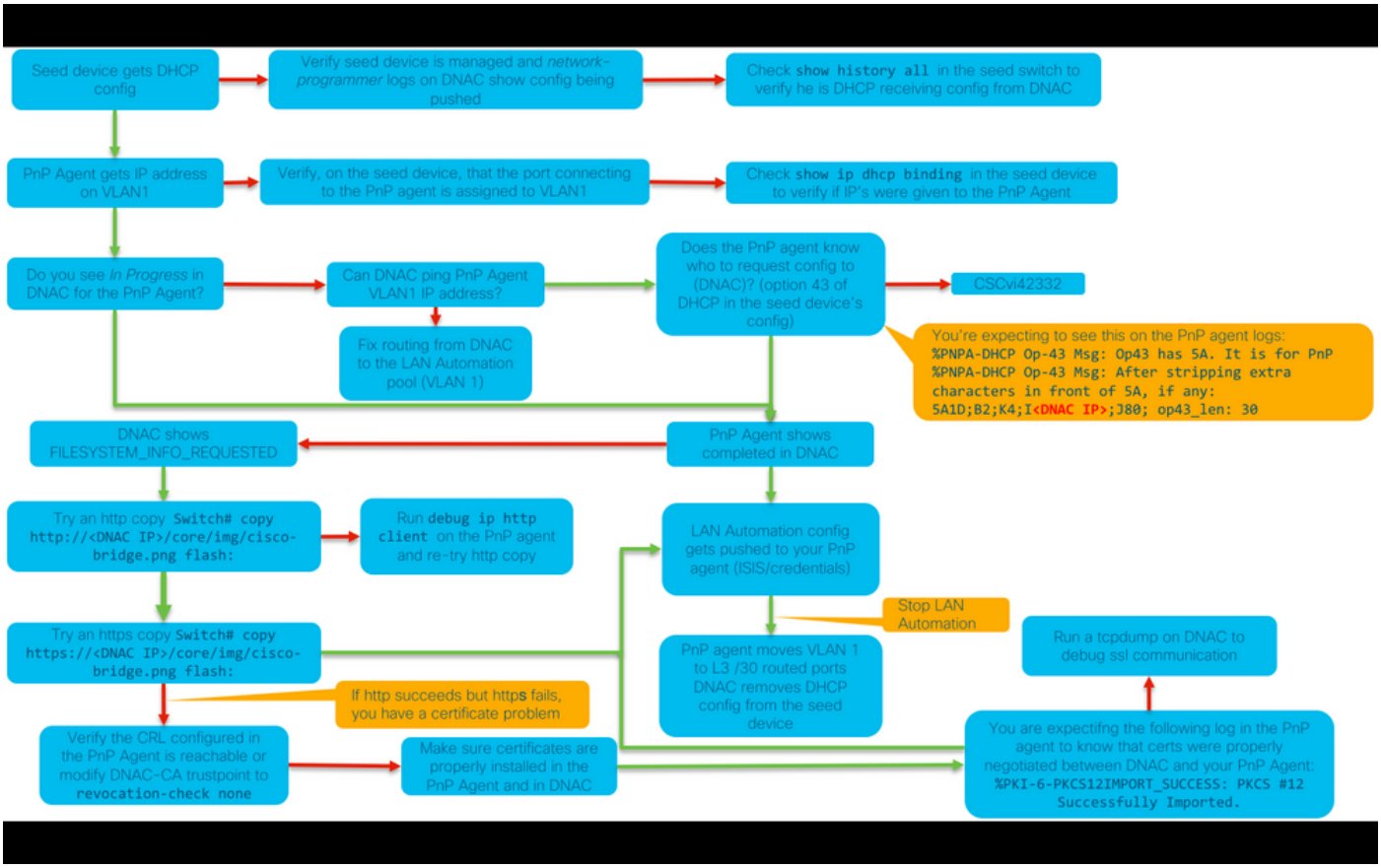
> **注意**：此池分为3个网段：
> 1.在PnP代理上推送到VLAN 1的IP地址。
> 2.在PnP代理上推送到Loopbac0的IP地址。
> 3.在连接到种子或其他交换矩阵设备的链路上推送到PnP代理的/30 IP地址。

如果您有n节点群集，DNA中心要调配PnP代理，种子设备接收的DHCP配置必须具有选项43，其中定义了面向DNA中心企业的网络接口卡(NIC)或虚拟IP(VIP)地址的IP地址。

当PnP代理启动时，它们没有配置。因此，其所有端口都属于VLAN 1。因此，设备会向种子设备发送DHCP发现消息。种子设备通过提供LAN自动化池中的IP地址进行应答。

现在，您了解了LAN自动化的初始顺序，因此，如果LAN自动化不能按预期运行，您就可以排除故障。

故障排除图



DNA中心1.1 LAN自动化相关日志

- network-orchestration-service
- PNP服务

DNA中心1.2 LAN自动化相关日志

在版本1.2中，不再有pnp-service，因此在排除LAN自动化故障时，您需要查找以下服务：

- 网络协调
- 网络设计
- connection-manager-service
- 自注册服务（*这是1.1版旧的pnp服务等价物*）

DNA中心1.x公钥基础设施(PKI)相关日志

- apic-em-pki-broker-service
- apic-em-jboss-ejbca

如何运行流程图中显示的tcpdump?

```
sudo tcpdump -i <DNA Center fabric's interface> host <PnP Agent ip address> -w
/data/tmp/pnp_capture.pcap
```

*要停止此操作，请使用CTRL+C

这会将pnp_capture.pcap文件存储在/data/tmp/中。您需要使用secure copy(SCP)命令从DNA中心复制文件，或使用以下命令从DNA中心读取文件：

```
$ sudo tcpdump -ttttnnr /data/tmp/pnp_capture.pcap
[sudo] password for maglev:
reading from file capture.pcap, link-type EN10MB (Ethernet)
2018-03-08 20:09:27.369544 IP 192.168.31.1 > 192.168.31.10: ICMP host 192.168.1.2 unreachable,
length 36
2018-03-08 20:09:39.369175 IP 192.168.31.1 > 192.168.31.10: ICMP host 192.168.1.2 unreachable,
length 36
2018-03-08 20:09:44.373056 ARP, Request who-has 192.168.31.1 tell 192.168.31.10, length 28
2018-03-08 20:09:44.374834 ARP, Reply 192.168.31.1 is-at 2c:31:24:cf:d0:62, length 46
2018-03-08 20:09:50.628539 IP 192.168.31.10.57234 > 192.168.31.1.22: Flags [S], seq 1113323684,
win 29200, options [mss 1460,sackOK,TS val 274921400 ecr 0,nop,wscale 7], length 0
2018-03-08 20:09:50.630523 IP 192.168.31.1.22 > 192.168.31.10.57234: Flags [S.], seq 2270495802,
ack 1113323685, win 4128, options [mss 1460], length 0
2018-03-08 20:09:50.630604 IP 192.168.31.10.57234 > 192.168.31.1.22: Flags [.], ack 1, win
29200, length 0
2018-03-08 20:09:50.631712 IP 192.168.31.10.57234 > 192.168.31.1.22: Flags [P.], seq 1:25, ack
1, win 29200, length 24
```

您尝试复制的bridge.png文件是什么？

它是DNA中心中的191字节映像文件，您希望使用HTTP（不使用证书）或HTTPS（使用证书）复制该文件，以测试DNA中心与PnP代理之间的通信。

当安全套接字层(SSL)通信未按预期工作时捕获示例（将完整的.pcap文件附加到本文）

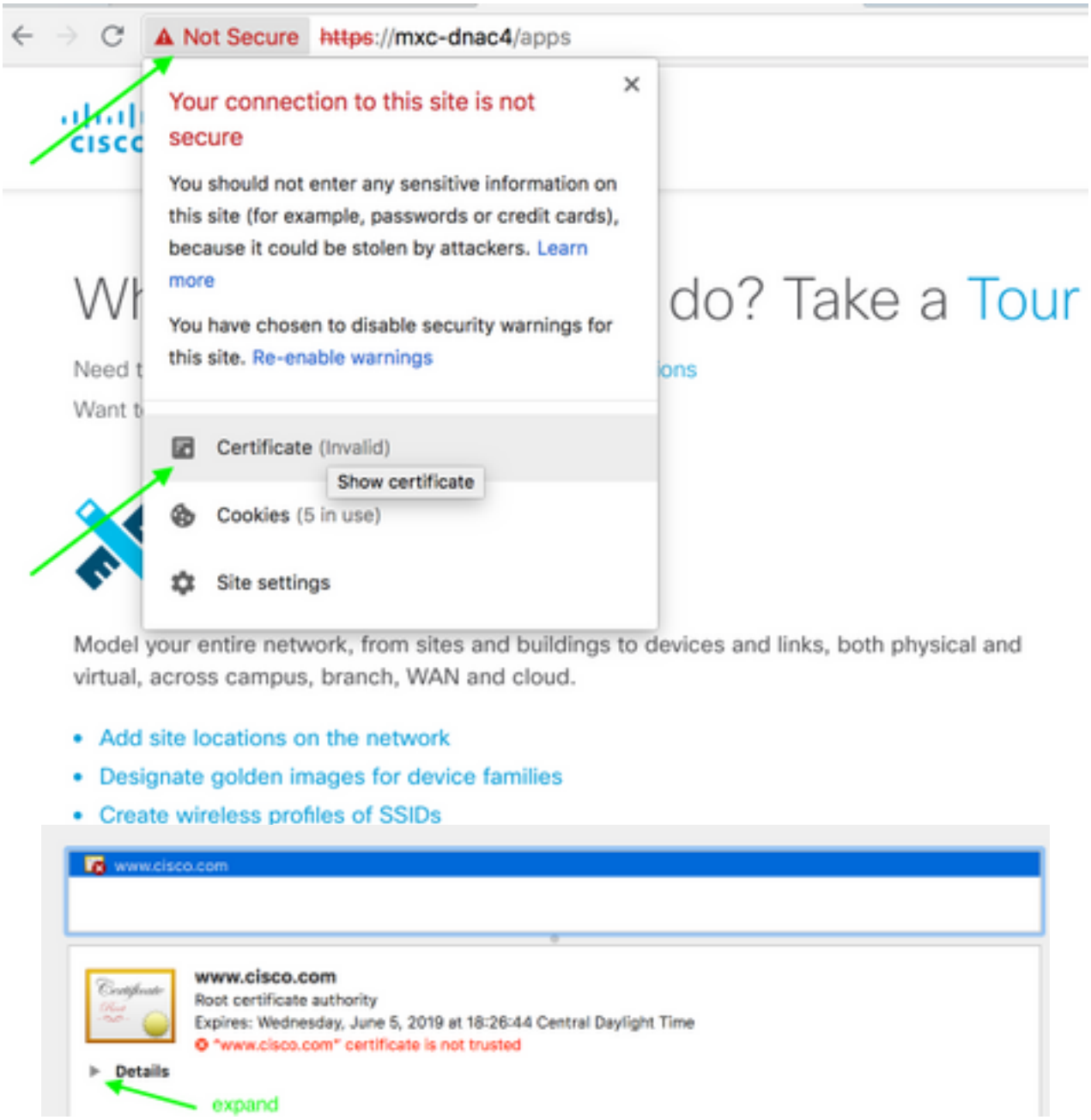
证书错误

可能的原因：

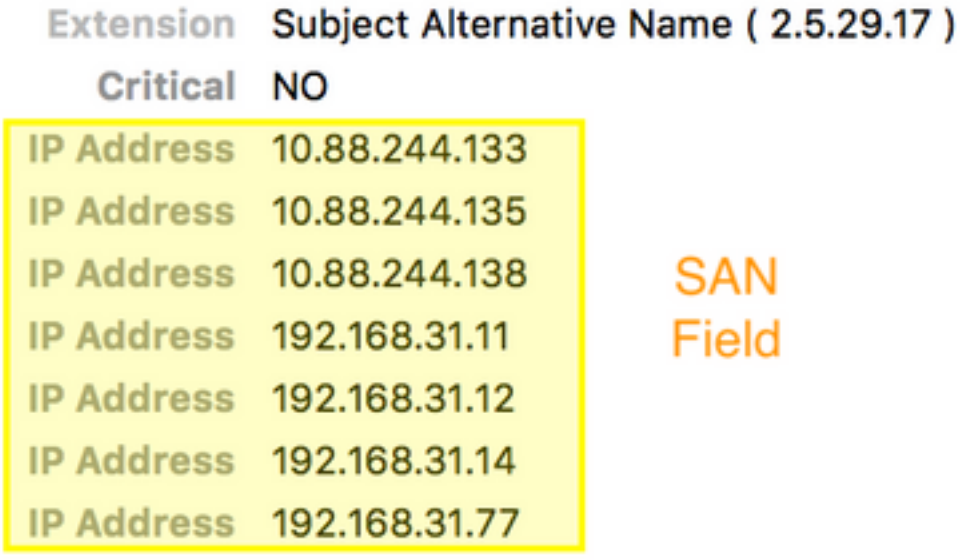
- DNA中心的证书在Subject Alternative Name(SAN)(主题备用名称(SAN))字段中没有正确的IP地址。

要检查证书中的SAN字段，可以执行以下操作：

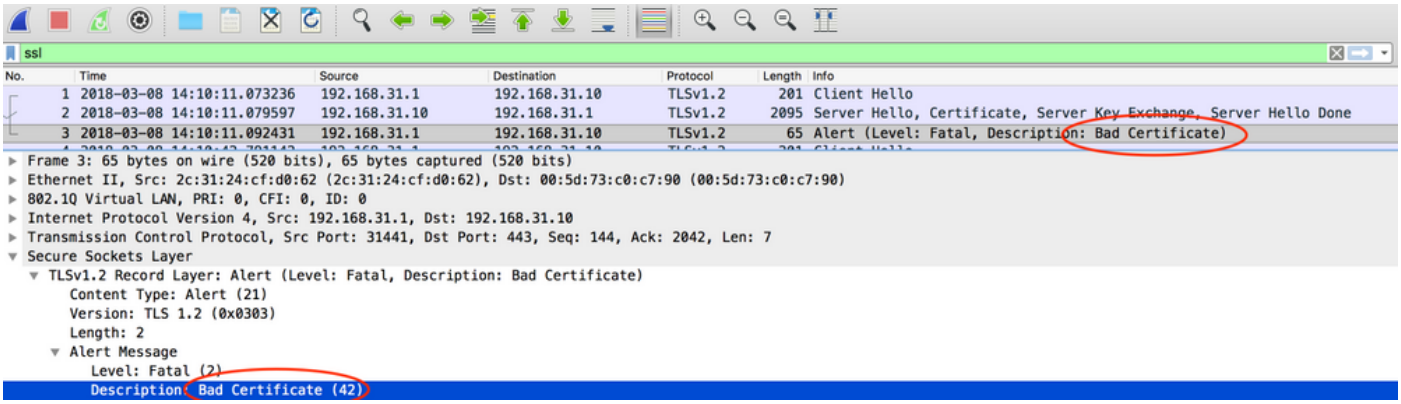
使用浏览器验证证书


Not Secure
https://mxc-dnac4/apps
Your connection to this site is not secure
You should not enter any sensitive information on this site (for example, passwords or credit cards), because it could be stolen by attackers. Learn more
You have chosen to disable security warnings for this site. Re-enable warnings
Certificate (Invalid)
Show certificate
Cookies (5 in use)
Site settings
do? Take a Tour
Model your entire network, from sites and buildings to devices and links, both physical and virtual, across campus, branch, WAN and cloud.
Add site locations on the network
Designate golden images for device families
Create wireless profiles of SSIDs

www.cisco.com
www.cisco.com
Root certificate authority
Expires: Wednesday, June 5, 2019 at 18:26:44 Central Daylight Time
"www.cisco.com" certificate is not trusted
Details
expand


Extension Subject Alternative Name (2.5.29.17)
Critical NO
IP Address 10.88.244.133
IP Address 10.88.244.135
IP Address 10.88.244.138
IP Address 192.168.31.11
IP Address 192.168.31.12
IP Address 192.168.31.14
IP Address 192.168.31.77
SAN Field

捕获示例



解决。

如果您有第三方CA（证书颁发机构），请确保他们向您提供包含DNA中心IP地址和VIP地址的证书。如果您没有第三方CA，DNA中心可以为您生成证书。请联系思科TAC，指导您完成此流程。

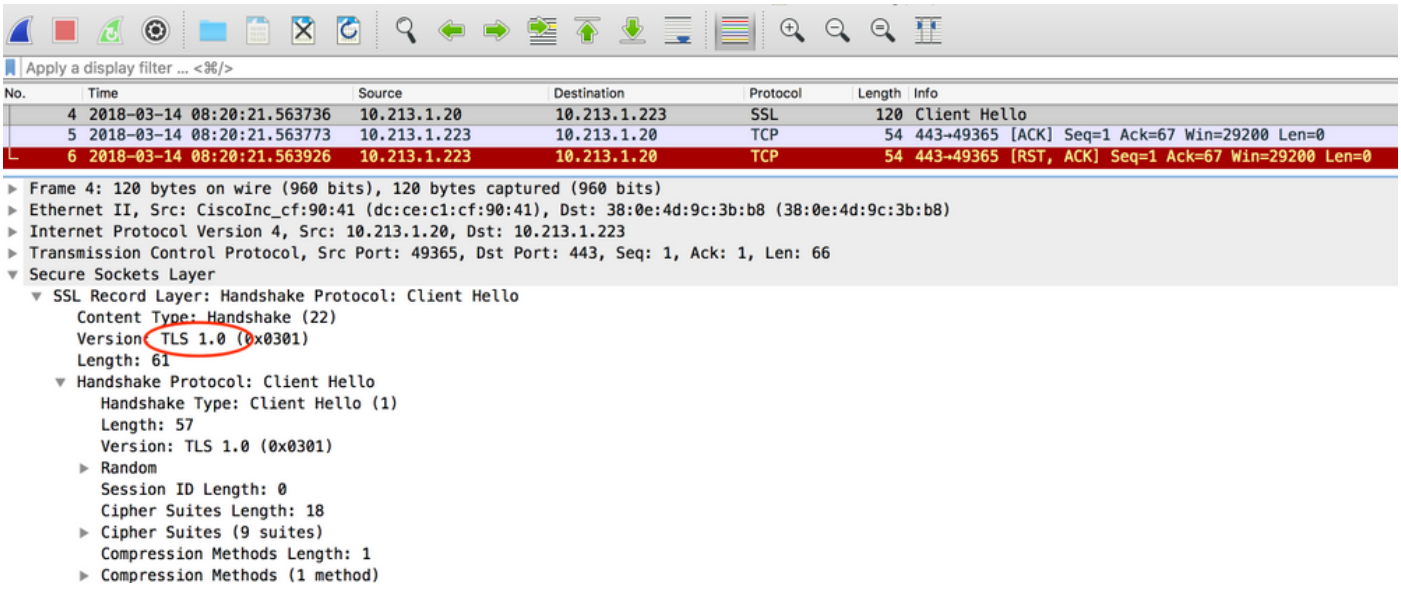
DNA中心重置连接

可能的原因：

默认情况下，DNA中心仅支持TLS v1.2。

要解决此问题，请启用DNA中心以按照本指南使用TLS v1

捕获示例



PnP代理上有用的debug命令，用于证书相关问题

- debug crypto pki transactions
- debug ssl openssl
- debug ssl openssl errores
- debug ssl openssl errors
- debug crypto pki api

- debug crypto pki transactions
- debug ssl openssl msg

响应缺少之前建立的已验证会话密钥

理论上，您不应在Provisioning > Devices > Device Inventory页面中有未申请的设备，但存在以下问题：从此页面删除未申请的设备后，设备仍显示在https://<DNA Center ip>/mypnp中。如果遇到此场景，并且您在PnP日志中看到类似于以下内容的日志，或在GUI中看到相同的指示，请确保设备不显示为PnP中未声明的设备：

```
ERROR | qtp604107971-170 | | c.c.e.z.impl.ZtdHistoryServiceImpl | Device authentication status
has changed to Error(PNP response com.cisco.enc.pnp.messages.PnpBackoffResponse is missing
previously established authenticated session key) | address=192.168.31.10, sn=FCW212XXXXX
```

LAN自动化和堆叠解决方案

- 在DNA中心1.2中，堆栈需要为全环（一个2成员堆栈的堆栈电缆可能无法工作）。
- LAN自动化需要立即声明堆栈设备，大约不到10分钟。
- 连接到DNA中心后，在PnP中显示为未申请。 PnP使用10分钟的时间窗口来确定堆栈，一旦到期，它将保留在LAN自动化的未申请部分。

如果您有RCA或PnP日志，则可以查找未申请的设备消息：

```
more pnp.log | egrep "(Received unclaimed notification|ZtdDeviceUnclaimedMessage)"
```

如果没有消息，则未声明的设备通知不会到达DNA中心，PnP无法声明。

如何在堆栈上实现LAN自动化

1. 关闭到种子设备的上行链路。
2. 在DNA中心上启动LAN自动化。
3. 从堆栈中删除启动配置。**# write erase**
4. 从NVRAM中删除所有证书。**# delete nvram:*.cer**
5. 删除vlan.dat文件。**# delete flash:vlan.dat**
6. 从主交换机删除备用交换机上的证书。**# delete stby-nvram:*.cer**

a.断开堆栈电缆。

b.登录到每台成员交换机的控制台。

c.删除证书。**# delete nvram:*.cer**

d.删除flas vlan数据库。**# delete flash:vlan.dat**

e.重新连接堆栈电缆。

7.重新启动。

8.等待交换机注册为堆栈，启动所有成员，然后尝试启动初始配置对话框。

```
%INIT: waited 0 seconds for NVRAM to be available


         --- System Configuration Dialog ---

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

9.启用到种子设备的上行链路。# no shutdown

我可以导入到LAN Automation任务的主机名映射文件的格式？

DNA Center需要一个主机名和序列号（主机名、序列号）的CSV文件，如下例所示：

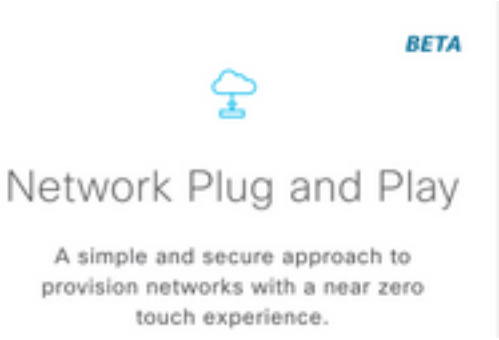
A	B
Edge1	FCW2048Cxxx
Edge2	FCW2131Lxxx, FCW2131Gxxx, FCW2131Gxxx, FCW2131Gxxx
Edge3	FOC2052Xxxx, FCW2052Cxxx, FCW2052Fxxx
Edge4	FXS2131Qxxx

对于堆栈LAN自动化，CSV文件允许您每行输入一个主机名和多个序列号。序列号需要用逗号隔开。请参阅附加的CSV文件以供参考。

/mypnp在1.2中到哪里了？

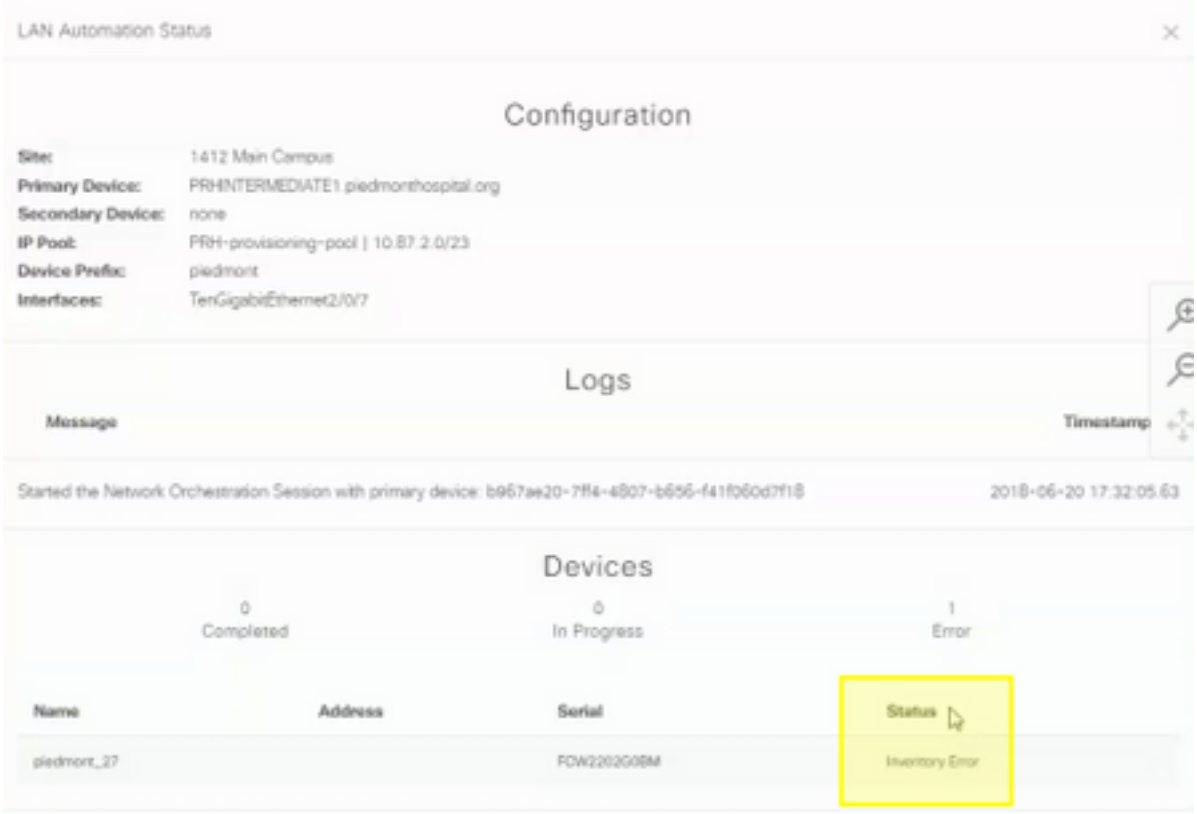
通过以下方式之一访问PnP:

- 在Web浏览器中输入https://<DNA Center IP>/networkpnp
- 从DNA中心主页，选择以下网络即插即用工具：



或者，访问https://<DNA Center IP>/networkpnp

库存错误



资产错误意味着设备在被LAN自动化声明并收到其配置失败后，将被添加到资产中。此错误通常由于配置、某些路由或CLI凭证问题而发生。

要验证您是否尝试通过LAN自动化启动正确的设备，请使用首选连接协议（SSH或Telnet）远程访问设备上loopback 0接口的IP地址。

存在连接，但PKI证书未成功推送到PnP代理

有时，中间的设备会打开DNAC和PnP代*理*之间数据包的“不分段(DF)”位。这可能导致大于1500字节的数据包（通常包含证书的数据包）被丢弃，因此LAN自动化可能无法完成。在DNA中心的自注册日志中看到的一些常*见日*志包括：

```
errorMessage=Failed to format the url for trustpoint
```

本例中建议的操作是确保DNA中心和PnP代理之间的路径允许使用命令system mtu 9100通**过巨型帧**。

Switch(config)#system mtu **9100**