

# ةي لحملا ةكبشلا ةتمتأ تاحيملت وحنائصن (DNA) ةيمقرلا ةكبشلا ةينب زكرم (LAN)

## تايوتحملا

[ةمدقملا](#)

[درسم](#)

[ةيساسأل تابلطتملا](#)

[تابلطتملا](#)

[ةيساسأتامولعم](#)

[ءدبلالبق](#)

[هلغشت ءانثأ LAN ةكبشل ئئاقلتلا ليغشتلا اهبرمي يتلا تاوطخلا ام](#)

[اهحالص او ءاطخأل فاشكتسال يطيطخت مسر](#)

[DNA 1.1 LAN زكرم ةتمتأ ةلصل تاذ تالچسلا](#)

[DNA 1.2 LAN زكرم ةتمتأ ةلصل تاذ تالچسلا](#)

[DNA 1.x زكرم \(PKI\) ماعلا حاتفملا ةيساسأل ةينبال ةلصل تاذ تالچسلا](#)

[؟يبايسنالاططخمل يف رهظي يذلا tcpdump غيغشت متي فيك](#)

[؟هخسن لواجت يذلا Bridge.png فلم وه ام](#)

[عقوتم وه امك \(SSL\) ةنمأل ليصوتلا ذخأم ةقبط لاصتا لمعي ال ام دنع جذومن طقتلي](#)

[\(ةلاقملا هذبه ةقفرم ةلماك .pcap تافل م\)](#)

[ةححص ريغ ةداهش](#)

[:لمتحملا ببسلا](#)

[ضرعتسم مادختساب ةداهشلا نم ققحتلا](#)

[ةنيعل طاقنتلا](#)

[رارقلا](#)

[لاصتالاطبض ديعي ةيمقرلا ةكبشلا ةينب زكرم](#)

[:لمتحملا ببسلا](#)

[ةنيعل طاقنتلا](#)

[ةداهشلاب ةقلمتحملا لكاشملا PnP ليكوي ليع ةديفملا ءاطخأل احيحصت رماوا](#)

[اقباس هيلع قديملا لمعلا ةسلج حاتفم ةباجتسال دقت في](#)

[اهجمدو \(LAN\) ةي لحملا ةكبشلا ليغشتلا ليغشتلا في مكحتلا](#)

[س دكم يلع LAN ةتمتأ ءارجا ةيفي ك](#)

[ةتمتأ ةمهم يلا هداريتسال يننكمي يذلا فيضملا مسا ةطيرخ فلم قييسنت ديرت له](#)

[؟يب ةصاخلا LAN ةكبش](#)

[1.2؟ في /mypnp بهذ نيأ](#)

[نوزخمل يف أطخ](#)

[PnP ماع يلا حاجنب PKI تاداهش عفدمتي ال نكلو دوجوم لاصتلا](#)

## ةمدقملا

(LAN) ةي لحملا ةقطنملا ةكبشلا ليغشتلا ليغشتلا يلع ةماع ةرطن دننتسملا اذه مدقي  
وه امك LAN ةكبشلا ليغشتلا لمعي ال ام دنع لكاشملا صيغشت في ك تدعاسم  
(DNA) ةيمقرلا ةكبشلا ةينب زكرم في عقوتم

Cisco نم TAC سندنهم، وديكس اراك وردناسك ليل لب ق نم م هاسم ل ت مت

## درس م

تاداهش نودبو نيوكت نودب هليغش ت ب تم ق ديدج زا هج (PnP) ليلغش ت ل اولي صوت ل ل ليمع  
ةيمقر ل ةكبش ل ةينب زكرم ةطساوب ايئاق لت اهنيوك ت متي س

يذ ل اولع فل اب هري فوت ب (DNA) ةيمقر ل ةكبش ل ةينب زكرم ماق يذ ل زا هج ل : يذ ل اول زا هج ل  
(DHCP) فيض م ل ل يكي م اني ذ ل نيوك ت ل لوكوت و رب م داخ ك ل م ع ي

## ةيساس ال ا ت ا ب ل ط ت م ل

### ت ا ب ل ط ت م ل

ل ح و (LAN) ةيل ح م ل ةكبش ل ة ت م ت ا ل و ح ة م ا ع ة ف ر ع م ك ي ذ ل ن و ك ت ن ا ب ة د ش ب Cisco ي ص و ت  
ن م م غ ر ل ا ي ل ع (LAN) ةيل ح م ل ةكبش ل ة ت م ت ا ي ل ع ة م ا ع ة ر ظ ن م د ق ت . ل ي غ ش ت ل ا و ل ي ص و ت ل ا  
م و DNA Center 1.1 ز ك ر م ي ل ع م و ه ف م ل س ف ن ق ب ط ن ي و ، DNA Center 1.0 ز ك ر م ي ل ع ة م ا ق ا ه ن ا  
ه د ع .

## ةيساس ا تام و ل ع م

اهري فوت و ةكبش ل ةزهج ا نيوكت نم كنكمي ابيرقت سمل نود نم رشن ل ح يه LAN ة ت م ت ا ن ا  
ي س ا س ا ه ي ج و ت ل و ك و ت و ر ب ك ISIS م ا د خ ت س ا ب

## ء د ب ل ل ب ق

م ت تاداهش يا هيدل سيل ك ب صاخال PnP ليمع ن ا نم دك ا ت ، LAN ةكبش ة ت م ت ا ل ي غ ش ت ل ب ق  
NVRAM ةرك ا ذ ي ف ا ه ل ي م ح ت .

```
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
```

ةزهج ال ا درج > ةزهج ال ا > دادع ا ةحفص ي ف ةبولطم ريغ ةزهج ا ي ا دوجو م د ع نم دك ا ت

Devices

Fabric

## Device Inventory

Inventory (6)

Unclaimed Devices (0)

الاسر يقلتت دقو، ةبلاطملا مدع ةلاح تاسدكملا ضع ب كرتت ال دق ، [CSCvh68847](#) ب ب سب ةكبش ةتمتأ لواحي ام دنع ةلاسرلا هذه ثدحت . ERROR\_STACK\_UNSUPPORTED أطيخ Catalyst لوحم سدكم وه زاهجلا نأل ، كلذ عمو . ادحاو الوحم ناك ول امك طبضل زاهجالب ةبلاطملا زاهجال رهظي و ، زاهجال LAN ةكبش ل يئاقلتلا ليغشتلا بللطي نأ نكمي الف ، زاهجال ريفوت متي ال كلذل ، سدكم هنأل زاهجالب PnP بللطي ال ، لثملابو . بولطم ريغك

## LAN ةكبش ل يئاقلتلا ليغشتلا اه ب رمي يتلا تاوطخلا ام هل يغشت اناثا

يتلا IP نيوانع قاطن . DHCP نيوكت عم يلوألا زاهجال ةيمقرلا ةكبشلا ةينب زكرم رفوي عمجت زجح دنع هفيعرعتب تمق يذلا يلوألا عمجتلا نم عزج وه يلوألا زاهجال اهيلع لصحي لقالا يلع 25/ نوكي نأ بجي عمجتلا اذه نأ ظحال . كعقومل IP نيوانع

ءازجا ةثالث يلى عمجتلا اذه مسقي : ةظحالم

1. كيديل PnP ءالمع يلع 1 مقرر VLAN ةكبش يلى اه عفدم تي يتلا IP نيوانع .

2. كيديل PnP ءالمع يلع Loopbac0 يلى اه عفدم تي يتلا IP نيوانع .

3. لصتي يذلا طابترالا يلع كيديل PnP ءالمع يلى اه عفدم تي يتلا IP 30/ نيوانع . ك ب ةصاخلا يخالل ةينبال ةزهجا وأ رودبالب

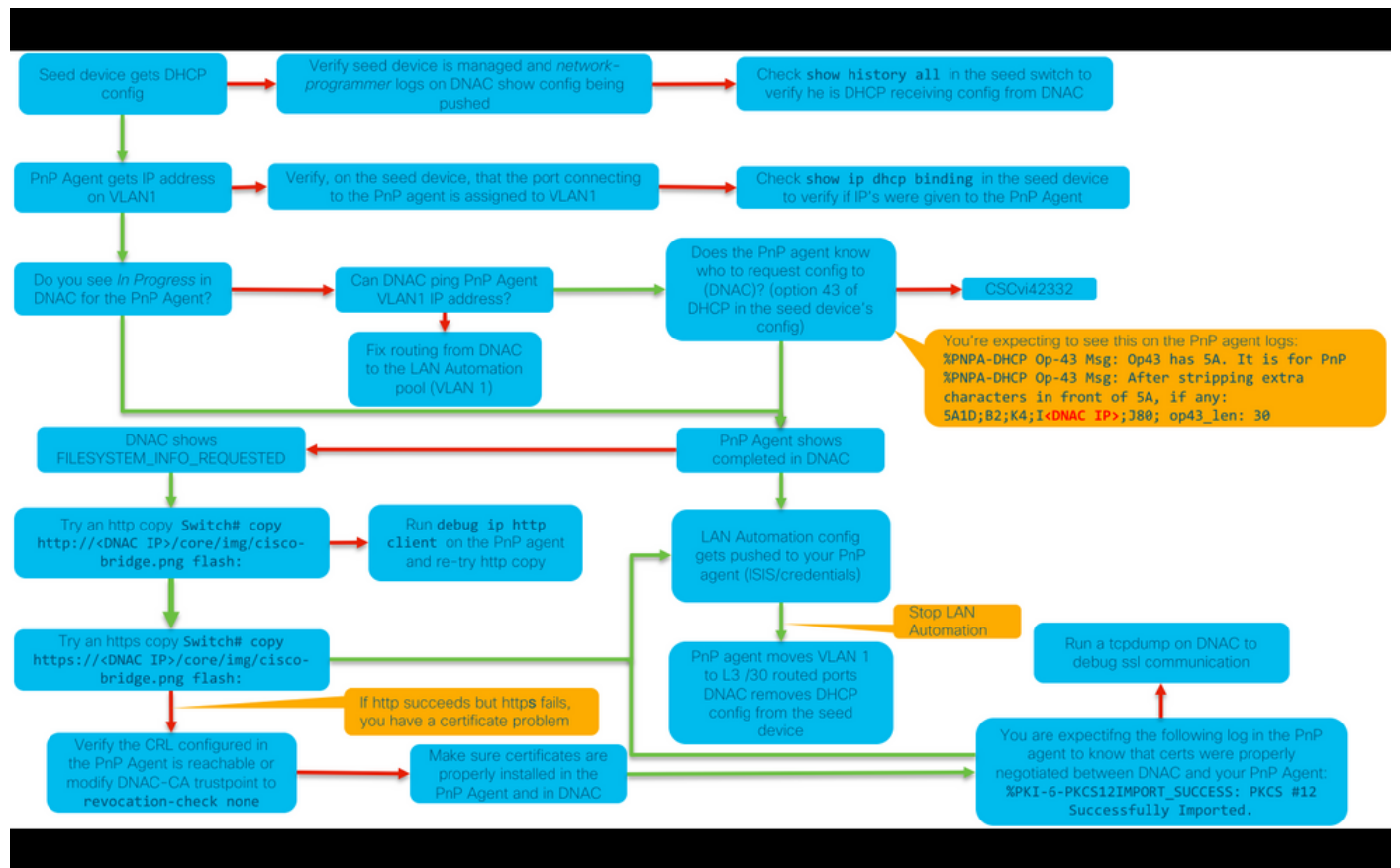
نيوكتل نوكي نأ بجي ، كيديل PnP ءالمع ريفوتل (DNA) ةيمقرلا ةكبشلا ةينب زكرم لصاخلا IP ناوانع مادختساب ددجملا 43 راخالل يلوألا زاهجال هملتسي يذلا DHCP لوكتورب ناك اذا ، (VIP) يرهاطلال IP ناوانع وأ (DNA) ةكبشلا ةينب زكرم (NIC) ةكبشلا ةهجاو ةقاطبب n. ةدقع ةعومجم كيذل

يللاتلابو . VLAN 1 نم عزج مهءانيم لك ، كلذل . نيوكت مهيدل نوكي ال ، PnP ءالمع ديمت دنع ضرع عم يلوألا زاهجال بيجتسي . يلوألا زاهجال يلى DHCP فاشتك لئاسر زهجالا لسرت ةيحلحمل ةكبشلا ةتمتأ عمجت لخاد IP نيوانع

ةيلمعلا ءاطخا فاشكتسأ كنكمي ، LAN ةتمتأ نم يلوألا لسلسلتلا تمهف نأ دعب نألا

عقوتم وه امك لمعت نكت مل اذا احوال صاو

## اهحال صاو ءاطخ ال فاش ك تسال يطي طخت مسر



### DNA 1.1 LAN زكرم ةتمت أب ةلصل اذ اتال ج سالا

- ةكبش ل قيسنت ةمدخ
- ةمدخ pnp

### DNA 1.2 LAN زكرم ةتمت أب ةلصل اذ اتال ج سالا

تامدخلال نع شحب ل اىل جاتحت يلات ل اب و PNP-Service ةمدخ كانه دعتم ل 1.2 رادصلال يف احوال صاو LAN ةكبش ل يئاق ل لتال ليغش لتال ءاطخ ا فاش ك تسال دن ع ةي لتال

- يكبش نمازت
- ةكبش ل ميمصت
- ري دمل ةمدخ ل اصتال
- (1. 1 نم Pnp ةمدخل مي دقل ائفا كمل وه اذه) قاح ل ال ةمدخ

### DNA 1.x زكرم ل (PKI) ماعل جات فم ل ل ةي ساس ال ةي نبل ل اذ اتال ج سالا

- APIC-em-PKI-broker-service
- APIC-em-jboss-ejbca

في باي س نال طاطخ م ل يف رهظي يذل tcpdump غي رفت ليغش متي فيك

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

\*مادختسالا اذه فاقيل Ctrl+C

زكرم نم فلم لا خسن ي نأ جاتحت نأ /data/tmp/ ي ف pnp\_capture.pcap فلم نيزختب اذه موق ي  
يالاتل رمألا مادختساب DNA زكرم نم فلم لا أرت نأ وأ (SCP) ةنم أ خسن رمأ مادختساب DNA

```
$ 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
```

## هخسن لواحت ي ذلا Bridge.png فلم وه ام

(DNA) ةيمقرلا ةكبشلا ةينب زكرم ي ف هعقوم ديدحت مت تي اب 191 مچحب ةروص فلم هن  
(تاداهشلا مادختساب) HTTPS وأ (تاداهشلا مادختساب) نودب) HTTP مادختساب هخسن ديرت ي ذلا  
كب صاخلا PnP ليك وو (DNA) ةيمقرلا ةكبشلا ةينب زكرم ني ب لاصتالا رابتخال

## ليصوتلا ذخأم ةقبط لاصتا لمعي ال ام دنع جذومن طقت لي هذهب ةقفرم ةلماك .pcap تافلم) عقوقتم وه امك (SSL) ةنم آلا (ةلاقملا)

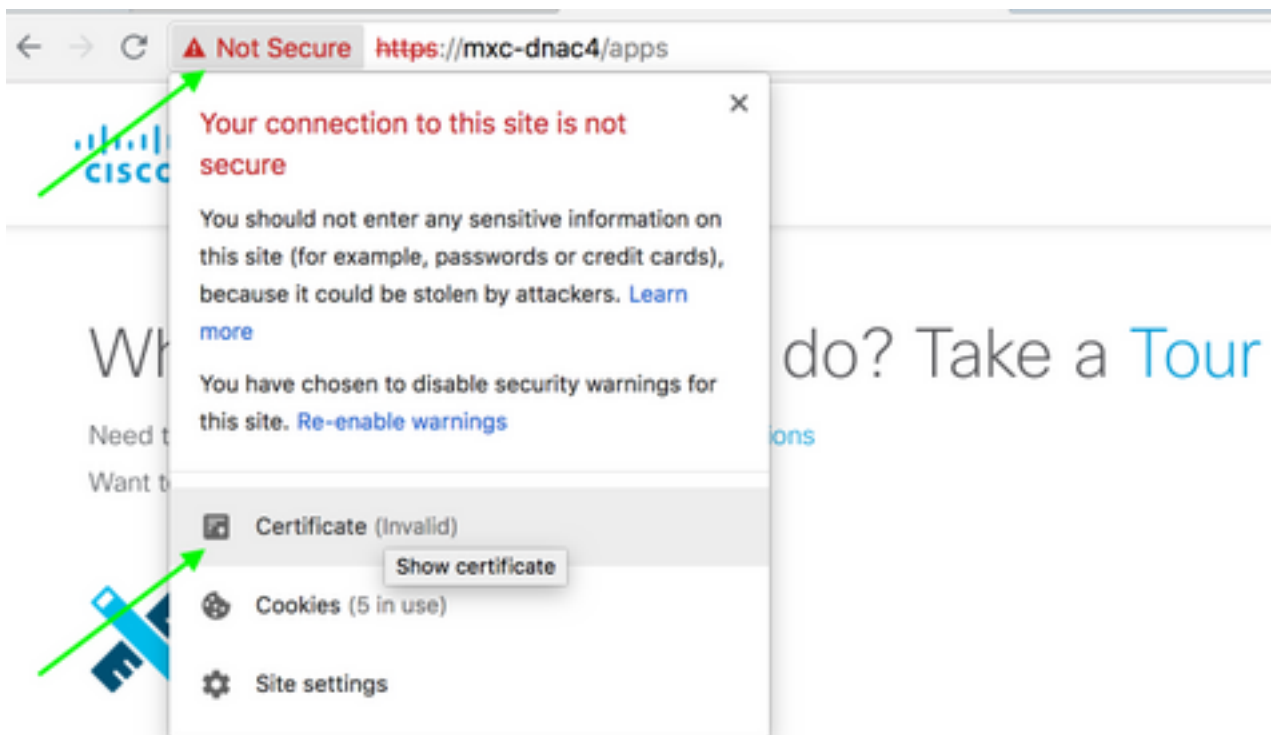
### ةححص ريغ ةداهش

#### لمتحملا ببسلا

- مسالا" لوق ي ف حيحصلا IP ناو نع لىع ةيمقرلا ةكبشلا ةينب زكرم ةداهش يوتحت ال  
"عوضوملل لي دبلا (SAN).

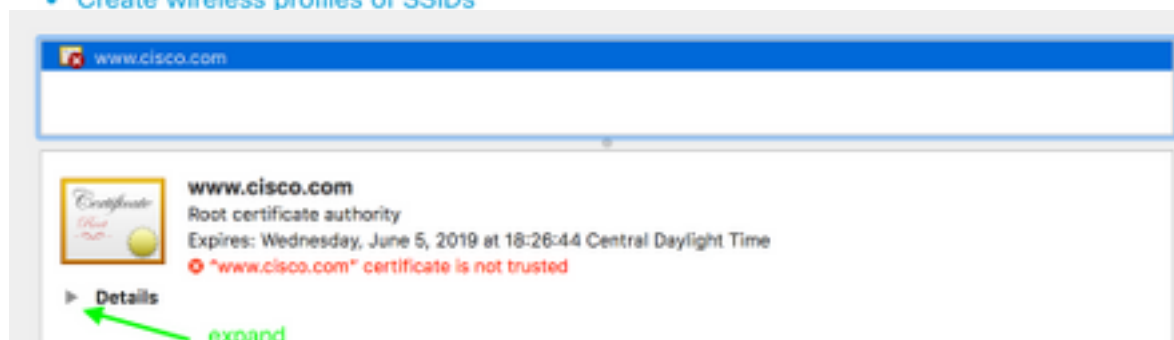
ي: لي امب مايقلا كنكمي، كصيخرت ي ف (SAN) نيزختلا ةقطنم ةكبش لوق نم ققحتلل

#### ضرتسم مادختساب ةداهشلا نم ققحتلا



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



**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**

| No. | Time                       | Source        | Destination   | Protocol | Length | Info                                                              |
|-----|----------------------------|---------------|---------------|----------|--------|-------------------------------------------------------------------|
| 1   | 2018-03-08 14:10:11.073236 | 192.168.31.1  | 192.168.31.10 | TLSv1.2  | 201    | Client Hello                                                      |
| 2   | 2018-03-08 14:10:11.079597 | 192.168.31.10 | 192.168.31.1  | TLSv1.2  | 2095   | Server Hello, Certificate, Server Key Exchange, Server Hello Done |
| 3   | 2018-03-08 14:10:11.092431 | 192.168.31.1  | 192.168.31.10 | TLSv1.2  | 65     | Alert (Level: Fatal, Description: Bad Certificate)                |

▼ Frame 3: 65 bytes on wire (520 bits), 65 bytes captured (520 bits)

▶ Ethernet II, Src: 2c:31:24:cf:d0:62 (2c:31:24:cf:d0:62), Dst: 00:5d:73:c0:c7:90 (00:5d:73:c0:c7:90)

▶ 802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 0

▶ Internet Protocol Version 4, Src: 192.168.31.1, Dst: 192.168.31.10

▶ Transmission Control Protocol, Src Port: 31441, Dst Port: 443, Seq: 144, Ack: 2042, Len: 7

▼ Secure Sockets Layer

▼ TLSv1.2 Record Layer: Alert (Level: Fatal, Description: Bad Certificate)

Content Type: Alert (21)

Version: TLS 1.2 (0x0303)

Length: 2

▼ Alert Message

Level: Fatal (2)

Description: Bad Certificate (42)

## بارقلا

يوتحت ةداهش كئاطعإ نم دكأتف (قدصم عجرم) ةيجراخ ةهج نم (CA) قدصم عجرم كيدل ناك اذإ قدصم عجرم كيدل نك ي مل اذإ. هيف ةمهمل ةيصخشلالو DNA زكرمب ةصاخلال IP نيوانع ىلع كداشراال Cisco TAC ب لاصتالال ىجري. كل ةداهش ءاشنإ DNA زكرم نك ميف، ةيجراخ ةهج نم ةيملعلا هذه لالخ.

## لاصتالال طبض دي عي ةيمقرلا ةكبشلال ةينب زكرم

### لمتحملا بسلا

يضا رتفا لكشب طقف TLS نم 1.2 رادصإلا (DNA) ةيمقرلا ةكبشلال ةينب زكرم معدي.

اذه عابتاب TLS v1 مادختسإ نم ةيمقرلا ةكبشلال ةينب زكرم ني كمتب مق، ةلكشملا هذه لجل [لجل](#)

### ةنيعل طاقلا

| No. | Time                       | Source       | Destination  | Protocol | Length | Info                                               |
|-----|----------------------------|--------------|--------------|----------|--------|----------------------------------------------------|
| 4   | 2018-03-14 08:20:21.563736 | 10.213.1.20  | 10.213.1.223 | SSL      | 120    | Client Hello                                       |
| 5   | 2018-03-14 08:20:21.563773 | 10.213.1.223 | 10.213.1.20  | TCP      | 54     | 443->49365 [ACK] Seq=1 Ack=67 Win=29200 Len=0      |
| 6   | 2018-03-14 08:20:21.563926 | 10.213.1.223 | 10.213.1.20  | TCP      | 54     | 443->49365 [RST, ACK] Seq=1 Ack=67 Win=29200 Len=0 |

▶ Frame 4: 120 bytes on wire (960 bits), 120 bytes captured (960 bits)

▶ Ethernet II, Src: CiscoInc\_cf:90:41 (dc:ce:c1:cf:90:41), Dst: 38:0e:4d:9c:3b:b8 (38:0e:4d:9c:3b:b8)

▶ Internet Protocol Version 4, Src: 10.213.1.20, Dst: 10.213.1.223

▶ Transmission Control Protocol, Src Port: 49365, Dst Port: 443, Seq: 1, Ack: 1, Len: 66

▼ Secure Sockets Layer

▼ SSL Record Layer: Handshake Protocol: Client Hello

Content Type: Handshake (22)

Version: TLS 1.0 (0x0301)

Length: 61

▼ Handshake Protocol: Client Hello

Handshake Type: Client Hello (1)

Length: 57

Version: TLS 1.0 (0x0301)

▶ Random

Session ID Length: 0

Cipher Suites Length: 18

▶ Cipher Suites (9 suites)

Compression Methods Length: 1

▶ Compression Methods (1 method)

## لكاشملا PnP ليك وىلع ةديفملا ءاطخالال حىحصت رماوا ةداهشلاب ةقلعتملا

- debug crypto pki transactions





س دكم ل تالبك ل صفا أ.

وضع لوحم لكل مكحتلا ةدحو ىلإ لوخدلا ليجستب مق ب.

ج. nvram:\* .cer فذح # .تاداهشل فذح ج.

د. flash:vlan.dat فذح # .تاي طعم ةدعاق flas vlan ل تاحم د.

هـ. س دكم ل تالبك ل لصوت دعأ ..

7. ليغشتلا ةداعإ .

8. راوح ءدب لواحو ،ءاضألأ عيمج بلج مث ،س دكمك ليجستلاب لوحملا موقوي ىتح رظتنا .  
ي لوال نيوكتل

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

```
--- System Configuration Dialog ---
```

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

9. ليغشتلا فاقيا متي مل # .روزبالا (ةزهجأ) زاوجل تالصولا نيكم تب مق .

## يننكم يي ذلا فيضملا مسا ةطيخ فلم قي سننت ديرت له بي ةصاخلا LAN ةكبش ةتمتأ ةمهم ىلإ هداريتسا

مقرلاو فيضملا مسا ب CSV فلم دوجو (DNA) ةيمقرلا ةكبشلا ةينب زكرم عقوتي  
:يلاتلا لاثملا يف حضوم وه امك (ي لس لس لتلا مقرلاو فيضملا مسا) ي لس لس لتلا

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

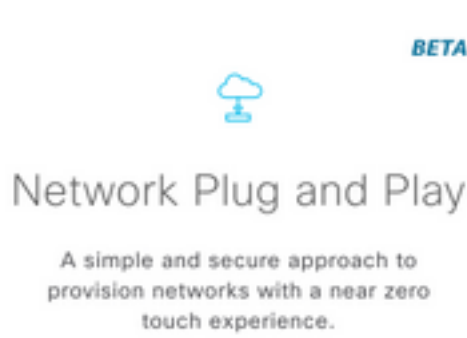
فيضم مسا لاخذاب CSV فلم كل حمسي ،س دكم لاب ةصاخلا LAN ةكبش ةتمتأل ةبسنلاب  
عجار .لصاوب ةي لس لس لتلا ماقرالا لصف بجي .فص لكل ةددعتم ةي لس لس لت ماقراو دحاو  
عجرم لل قفرملا CSV فلم

## 1.2 في mypnp /بهذ نيأ

ةيلاتلا قرطلا يدحإ ب PnP ىلإ لوصول:

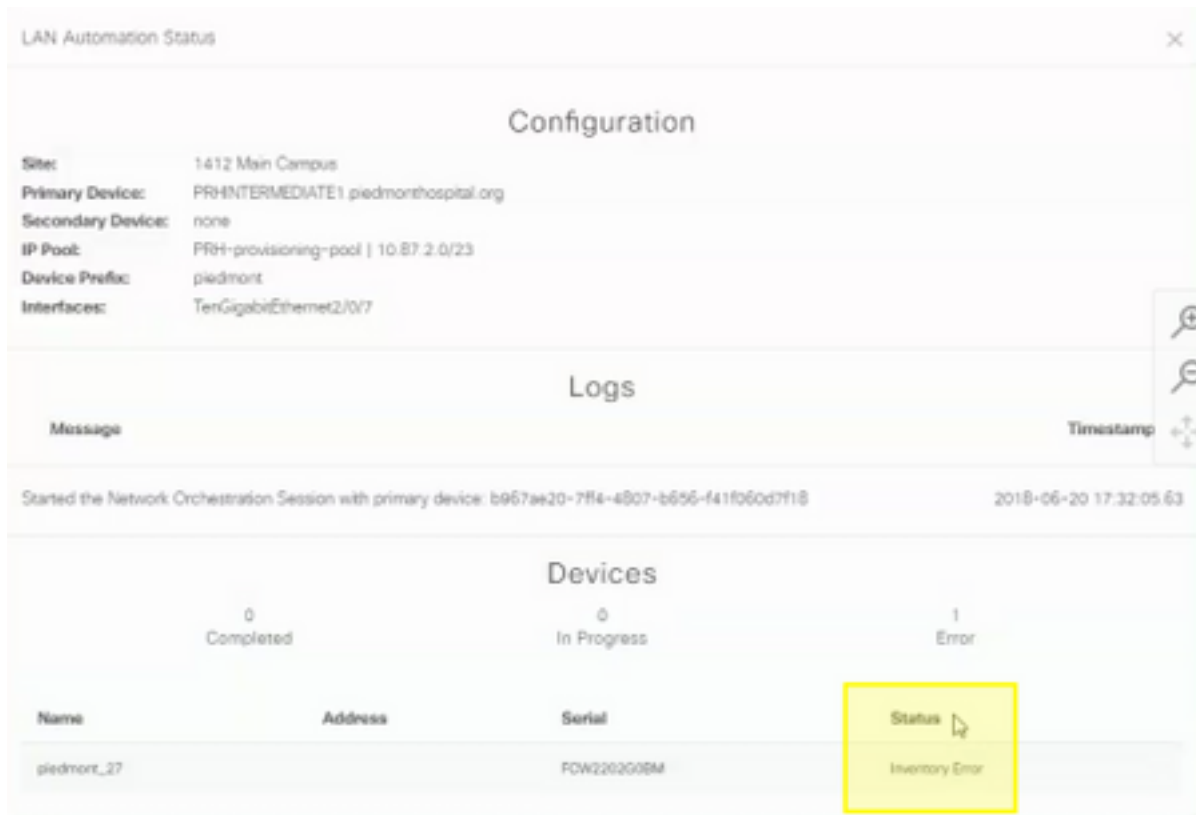
- ب صاخلا بيولا ضرعتسم نم
- ليغشتلاو ليصوتلا ةادأ دح ،ةيمقرلا ةكبشلا ةينب زكرم ةيسيئرلا ةحفصل نم

ةيالاتلا ةكبشلل:



أىل باهذلا قيرط نع وأ <https://<DNA Center IP>/NetworkPNP>

## نوزخمل ايف أطخ



مالاتساو LAN ةكبش ةتمتأة طساوب هب ةبلاطملا دعب، زاهجلا نأ نوزخملا أطخ ينعى ببسب أطخلا اذه ثدحي ام ةداع. نوزخملا اىل هتفاضل متت، لشف دق هب صاخلا نيوكتللا دامتعا تانايب لكاشم وأ هيچوتلا ضعب وأ نيوكتللا

LAN، ةكبشل يئاقللتلا ليغشتلا لالخال نم حيجصللا زاهجلا ضرع لواحت كنأ نم ققحتلل مادختساب زاهجلا اىل 0 عاجرتساللا ةهجاوب صاخلا IP ناونع اىل دعب نع لوصولا كنكمي (SSH وأ Telnet). لصفملا لاصتالا لوكوتورب

## ءالمع اىل حاجنب PKI تاداهش عفدم تيال نكلو دوجوم لاصتالا PnP

ليغشتب فرصت نملا ايف ةدوجوملا ةزهجالا ايف موقت نأ نكمي يتلا تارملا ضعب كانه

مزحل لاهات في كلذ ببستتي دق. PnP لم اووو DNAC نيب مزحل (DF) ةئزجت مدع تب تادحو  
لمتكي ال دق يلاتلابو، ةداهشل ال ع دواع يوتحت ياتلابو، تياب 1500 ن ع اهمج دي زي ياتلابو  
ي وونل لاضمحل زكرم ةقحلم تالجس في رهظت ياتلابو ةئاشل تالجسل لاضع ب LAN. ةتمت أ  
ه:

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

ةيمقرلة ةكبشل لة نيب زكرم نيب راسم ل ن أ ن م دك أتل وه ةلحل هذه في حرتقم لاءارجل  
MTU رم اووال ماظن مادختس لال خ ن م رورم لابل مچحل ةري ب ك تاراط لابل حمسي PnP لم اووو (DNA)  
9100.

```
switch(config)# system mtu 9100
```

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذه Cisco تچرت  
ملاعلاء انءمچ يف نيمدختسمل معدى وتحم مي دقتل ةيرشبلاو  
امك ةقيد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچرئى. ةصاغل مهتغب  
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحل وه  
ىلإ أمئاد عوچرلاب يصوت وتامچرتل هذه ةقد نع اهتيلوئسم Cisco  
Systems (رفوتم طبارلا) يلصلأل يزيلچنلإ دن تسمل