

ي ف اه حال ص او APIPA ناو ن ع عاطخأ فاش ك تسأ ة ك ب ش ل ا

تاي و ت ح م ل ا

[ة م د ق م ل ا](#)

[ة م د خ ت س م ل ا ت ا ن و ك م ل ا](#)

[ب ا ب س أ ل ا](#)

[ا ه ج ا ل ص ا و عاطخأ ل ا فاش ك تسأ و ت ا ه و ي ر ا ن ي س ل ا](#)

[ة ي ا م ح ل ا ر ا د ج ل ي و ن ي و ك ت - 1 و ي ر ا ن ي س ل ا](#)

[ة ل ك ش م ل ا ف ص و](#)

[ة ل ك ش م ل ا ض ا ر ع أ](#)

[ا ه ج ا ل ص ا و عاطخأ ل ا فاش ك تسأ ت ا و ط خ](#)

[ا ل ا ن ع ن ا](#)

[ل م ع ل ا ة ط خ](#)

[ق ق ح ت ل ا / ر ا ر ق ل ا](#)

[DHCP م د ا خ ق ا ط ن - 2 و ي ر ا ن ي س ل ا](#)

[ة ل ك ش م ل ا ف ص و](#)

[ض ا ر ع أ ل ا](#)

[ا ه ج ا ل ص ا و عاطخأ ل ا فاش ك تسأ ا ر ج ا م ت](#)

[ا ل ا ن ع ن ا](#)

[ل م ع ل ا ة ط خ](#)

[ق ق ح ت ل ا / ر ا ر ق ل ا](#)

[C9300 - 3 و ي ر ا ن ي س ل ل SDA ن ي و ك ت](#)

[ة ل ك ش م ل ا ف ص و](#)

[م د خ ت س م ل ا ض ا ر ع أ](#)

[ا ه ج ا ل ص ا و عاطخأ ل ا فاش ك تسأ ا ر ج ا م ت](#)

[ا ل ا ن ع ن ا](#)

[ل م ع ل ا ة ط خ](#)

[ق ق ح ت ل ا / ر ا ر ق ل ا](#)

[LAN ة ك ب ش ن ي ا ه م ي ف ة ل ك ش م - 4 و ي ر ا ن ي س ل ا](#)

[ة ل ك ش م ل ا ف ص و](#)

[ض ا ر ع أ ل ا](#)

[ا ه ج ا ل ص ا و عاطخأ ل ا فاش ك تسأ ت ا و ط خ](#)

[ا ل ا ن ع ن ا](#)

[ل م ع ل ا ة ط خ](#)

[ق ق ح ت ل ا / ر ا ر ق ل ا](#)

[ق ب ا ط ت م ر ي غ MTU - 5 و ي ر ا ن ي س ل ا](#)

[ة ل ك ش م ل ا ف ص و](#)

[م د خ ت س م ل ا ض ا ر ع أ](#)

[ا ه ج ا ل ص ا و عاطخأ ل ا فاش ك تسأ ا ر ج ا م ت](#)

[ا ل ا ن ع ن ا](#)

[ل م ع ل ا ة ط خ](#)

[ق ق ح ت ل ا / ر ا ر ق ل ا](#)

[IPDT ة ي ا م ح - 6 و ي ر ا ن ي س ل ا](#)

[ة ل ك ش م ل ا ف ص و](#)

[م د خ ت س م ل ا ض ا ر ع أ](#)

ةمدقملا

اهل لولحل رفوتو APIPA نيوانعب ةقلعتمل لئاسملا ةقيثولا هذه فصت

ةمدختسملا تانوكملا

- Catalyst 9000 switches تالوحملا
- 5516 لثم ASA ةيامح نارديج
- عون يأ نم DHCP مداخ
- SDA دادعإ يف 9300 ةزافح ةدام
- رفوتم ريغ: جماربلا

بابسأل

، تاهويرانيسللا هذه ءانثأ APIPA نويئاهنلا نومدختسملا نيغي

- رفوتم ريغ DHCP مداخ
- اهلبق وأ ةيلاحلا ةوطخل لبق DHCP ضرع طاقسإ متي
- رركم IP لثمت ةباجتسإ لىع ARP Probe لصحي

اهحل الصاوعاطخأل افاشك تساو تاهويرانيسللا

ةيامحل رادج ليكو نيوكت - 1 وييرانيسلا



ASA 5516

ةلكشملا فصو:

- ممدختسملا لاصتاو APIPA IP ناونع ىقلتت يتلا ممدختسملا ةزهجأ تراثأت

ةلکشمل ضارعأ

1. ناونع نوقلتي شيح ةعطقتم لكاشم ةني عم VLAN ةكبش ىلع نومدختسمال هجاوي ةكبشلاب لاصتال نودقفي وAPIPA.
2. دحاولا يئاهنل مدختسملل MAC ناونعل ةددعتم ARP تالخدإ ىلع ةياملال ناردي وتحت اذه لثم:

<#root>

```
Firewall/pri/act# show arp | include abcd.abcd.abcd
```

```
inside 10.1.1.12 abcd.abcd.abcd 30
```

```
inside 10.1.1.13 abcd.abcd.abcd 40
```

```
inside 10.1.1.14 abcd.abcd.abcd 51
```

```
inside 10.1.1.15 abcd.abcd.abcd 53
```

اهالصلإو ءاطخألا فاشكتسأ تاوطخ

1. ىلإ ةباجتسالال لسري يذلا ةياملال رادج ىلإ ةياملال رادج ىلع ءاطخألا حيحصت ري شي ARP Probe. نبيئاهنل نيمدختسمال

<#root>

```
DHCPD/RA: creating ARP entry (10.1.1.12, abcd.abcd.abcd).
```

```
DHCPRA: Adding rule to allow client to respond using offered address 10.1.1.12
```

رركم ناونع هنأ يف ركفي يف رطل زاهال لعج ىلإ اذه يدؤي.

ةياملال رادج وأ يف رطل زاهال ىلع طاقتل.

ةيلمع لامتكأ درجمب DHCP ضمزم لسري يذلا يف رطل زاهال طاقتلال تايلمع رهظت DORA.

Source	Destination	Info
0.0.0.0	255.255.255.255	DHCP Discover
10.1.2.3	10.1.1.1	DHCP Offer
0.0.0.0	255.255.255.255	DHCP Request
10.1.2.3	10.1.1.1	DHCP ACK
0.0.0.0	255.255.255.255	DHCP Decline

الازعنا

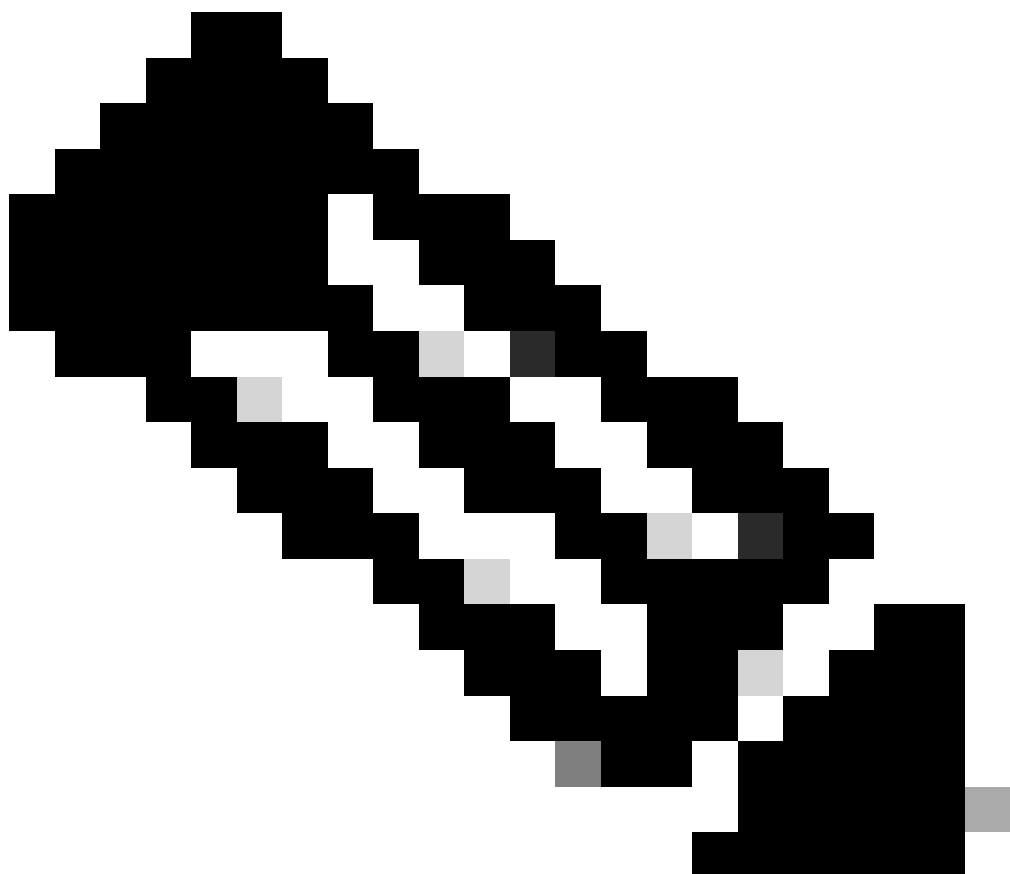
- درج م ب ، ليكوك لمعمل قيرط ن ARP قيقحت ىل اةلخادل اةيامحل رادج اةج او بيحتست
ضفر DHCP لسري نأ pc ل لعجي اذه DORA. اةلمع لامتك

لمعمل اةطخ

- رمأل مادختساب اةجاول لxad اةيامحل رادج ىل ع ليكولل ARP ليطلع ب مق
"sysopt noproxyYarp inside"

ققحتل/رارقل

- ليكولل نيوانع ل ليحت لوكوتورب ليطلع دب IP ناونع اةفرطال اةجأل ىقلتت



- ARP تافشك تسمل ةباجت سا لاسرا وأ ليكوك زاهج يا لمع مدع نم دكأت :ةطحال م
يئاهنلا مدختس ملل

DHCP مداخ قاطن - 2 ويراني سلا



DHCP Server

فصل كشم ال فصول:

- م دختسم ال لاصت او APIPA IP ناونع ى قلتت ي ت ال م دختسم ال ةزهجأ ت رثأت

ضارعالا

1. نودق فو و طق ف APIPA IP ناونع ة ني عم VLAN ة كبش ى ل ع نوم دختسم ال ى قلتت ي .
ة. كبش ل اب ل لاصت ال

اهال ص او اعاطخ ال فاشكت س أ عارج م ت

- ناونع م ادختساب ه ني وكت م تو ني يئاهن ال ني م دختسم ال ى ل DHCP ض فر ل اسرا م ت
APIPA

الازعنا

- ه ني عت م تي ي ذل ال IP ناونع س ف نو A قاطن ال نم ادخ او IP ناونع DHCP م داخ ني عي

DHCP: ضافخنا بېسې اذه. قاطنل س فن هل B قاطنل نأل رخآ لومحم رتويېمكل

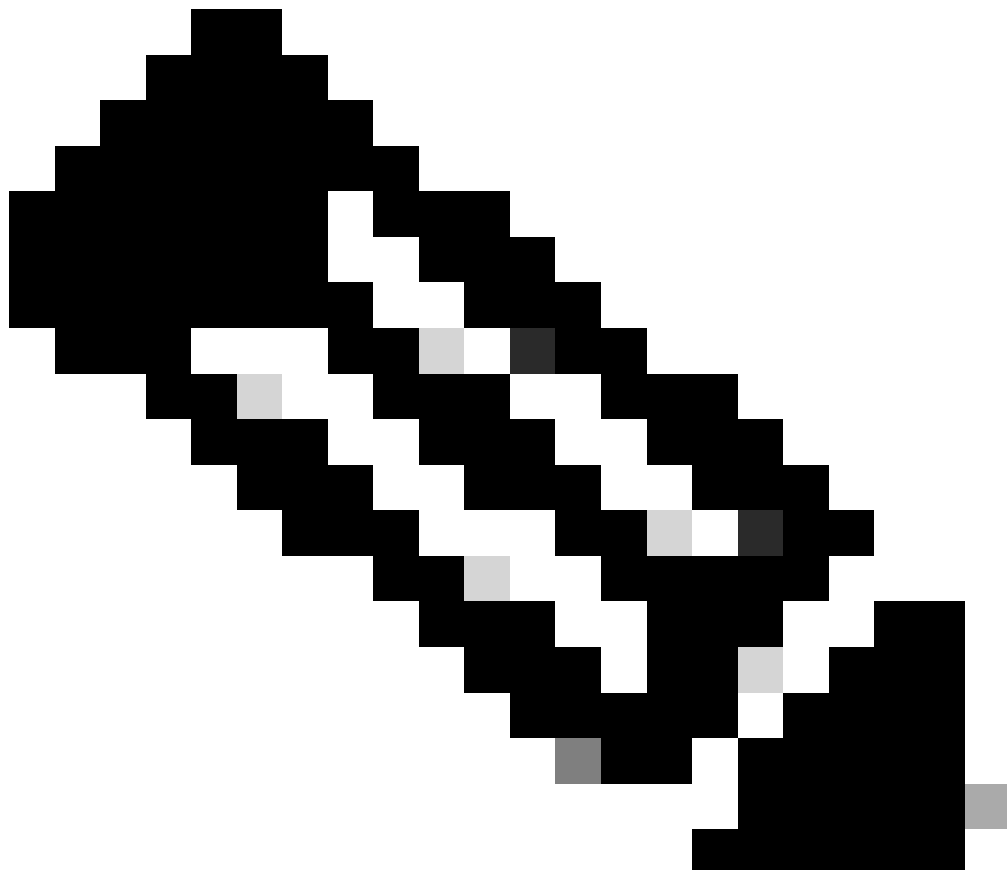
Source	Destination	Info
0.0.0.0	255.255.255.255	DHCP Discover
10.1.2.3	10.1.1.1	DHCP Offer
0.0.0.0	255.255.255.255	DHCP Request
10.1.2.3	10.1.1.1	DHCP ACK
0.0.0.0	255.255.255.255	DHCP Decline

لمعلا ةطخ

- دېرفال DHCP قاطن قاطن قاطن نېيغت

ققحتل/رارقل

- قاطنل رېيغت دع ب IP ناو نع ةي ف رطلا ةزهجأل ى قلتت



• اهنوكت مت ةرركم تاقاطن ىلع يوتحي ال DHCP مداخل نا نم دكأت: ةطخال م

C9300-3 وي رانيسي ل ل SDA ني وكت



Cat9300 in SDA

ةل كش م ال ف ص و:

- م د خ ت س م ال ل ا ص ت ا و IP APIPA ن ا و ن ع ي ق ل ت ت ي ت ال م د خ ت س م ال ة ز ه ج أ ت ر ث أ ت

م د خ ت س م ال ض ا ر ع أ

1. DHCP ن ي و ا ن ع ي ل ع ل و ص ح ال ة ن ي ع م VLAN ة ك ب ش ي ف ن ي م د خ ت س م ال ض ع ب ع ي ط ت س ي ال ة .
ة ي ك ل س ال ال ل و ص و ال ة ط ق ن ل ال خ ن م
2. د ح ا و ي ئ ا ه ن م د خ ت س م ال MAC ن ا و ن ع ل ة د د ع ت م ARP ت ال ا خ د ا ي ل ع ة ي ا م ح ال ر ا د ج ي و ت ح ي .

<#root>

```
Firewall# show arp | i abcd
```

```
Inside 10.1.1.22 abcd.abcd.abcd 48
```

```
Inside 10.1.1.23 abcd.abcd.abcd 49
```

```
Inside 10.1.1.24 abcd.abcd.abcd 50
```

ا ه ا ل ص ا و ا ط ا ل ا ف ا ش ك ت س ا ا ر ج ا م ت

- ل و ح م ال ة ط س ا و ب DHCP ض ر ع ط ا ق س ا م ت
- DHCP م د ا خ ن م ر د ا ص ال DHCP ض ر ع ي ل ا ا د ا ن ت س ا ARP ع ل م ب FTD م و ق ي .

<#root>

DROP Broadcast to Access-Tunnel disallowed (accessTunnelBroadcastDrop)

الازعنإ

- غلبې ال ملع ثب عم طبر ضرع، setup، كلسال SDA ل نوکې L2-only VLAN تلکش نإ
يضا رتفا لكش ب مزحل ثب ب حمسي ال Access-tunnel نأ ام ب AP.

لمعل طخ

- LISP. ةئې ل خاد "ناضي فال ةينام" ب حامس ال

<#root>

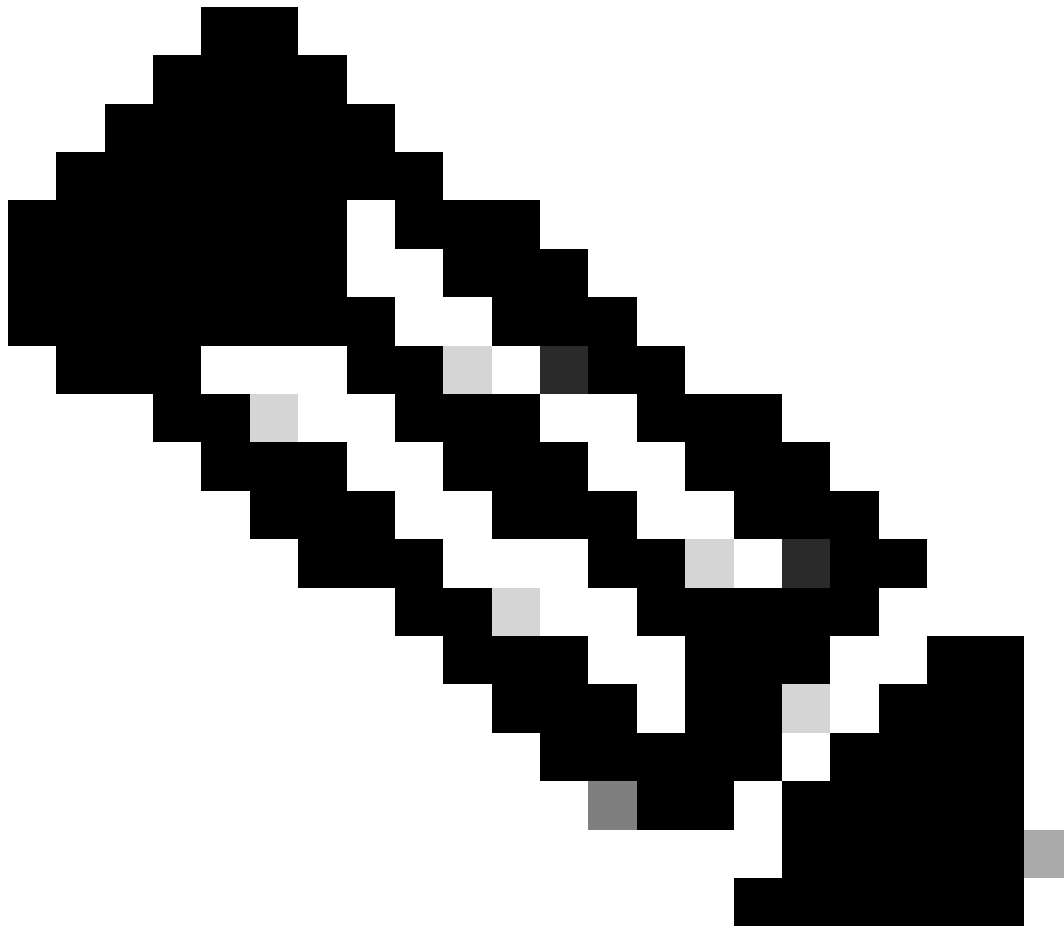
router lisp

instance-id 8456

flood access-tunnel

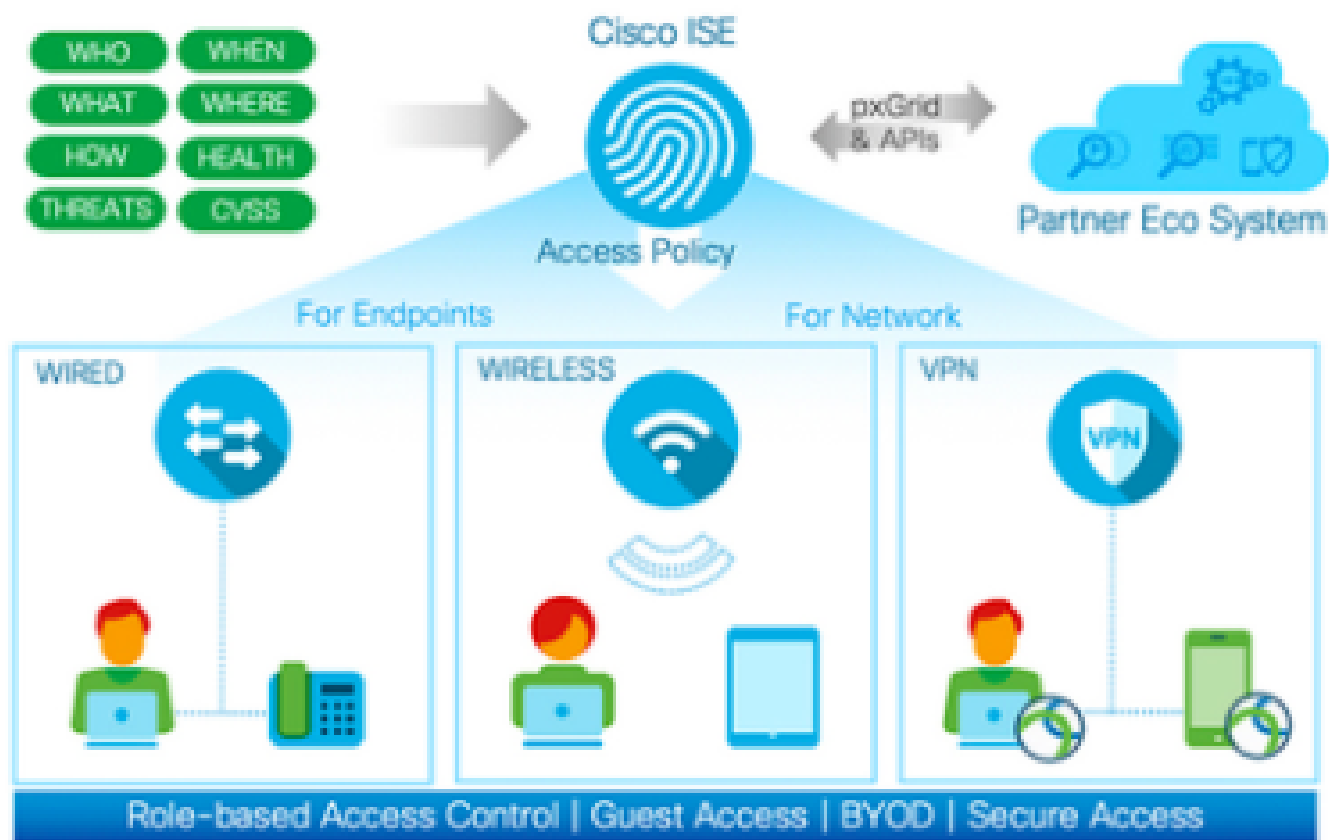
ققحتل/رارقل

- ة، ل خادل ةهاولا ىل ل صتم ال C9300 ي ف "ناضي فال ىل ل وصولا قفن" نيوكت دعب
DHCP. نيوانع ءالمعل ملتسي



نيوكت ةلاح يف ،زمرلا تحت ناضي فالإ لوصولا قفن نيكم ت نم دكأت :ةطحال م
ثبلا ضرع يقلتلفرطالا زاهجلا

LAN ةكبش ئيها م يف ةلكشم - 4 ويراني سللا



cisco ISE

ةلكشمال فصوصو

- مدختسمال لاصتاو IP APIPA ناوع ىقلتت يتال مدختسمال ةزهجأ تثرأت

ضارأل

1. "drop" تاذا تالخالإال MAC نيوانع لودج رهظي.

<#root>

```
#show mac address-table interface gigabitethernet1/0/20
```

Mac Address Table

Vlan	Mac Address	Type	Ports
----	-----	-----	-----

10 0000.0001.000a DYNAMIC Drop

10000 ىتح وأ 2000 نم رثكأ امبر ،تالاخلال نم ديدعل ةقداصلم ةسلج ضرع رهظي 2.

<#root>

switch2#show authentication sessions

Gi1/0/1 0000.0001.1234 N/A UNKNOWN Unauth 0AFF0B8D000000EC000000AF

Gi1/0/1 0000.0001.2345 N/A UNKNOWN Unauth 0AFF0B8D000000F00016B7D7

Gi1/0/1 0000.0001.3456 N/A UNKNOWN Unauth 0AFF0B8D0028DE3500000000

اهحالصاوا ءاطخال فاشكتسا تاوطخ

- MAC نيوانع مادختساب يف رطل زاهال نم ةدراوال مزحل نم ديدعل ةمزال طاقتال رهظي ردصم لل ةفلتخم.
- ةكبشال يف ةعقوتم ريغ لكاشم أشنت دحل زواجت درجمبو 2000 وه ةقداصلم ةسلج دح
- https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3650/software/release/16-12/configuration_guide/sec/b_1612_sec_3650_cg/configuring_ieee_802_1x_port_based_authentication.html

الازعن

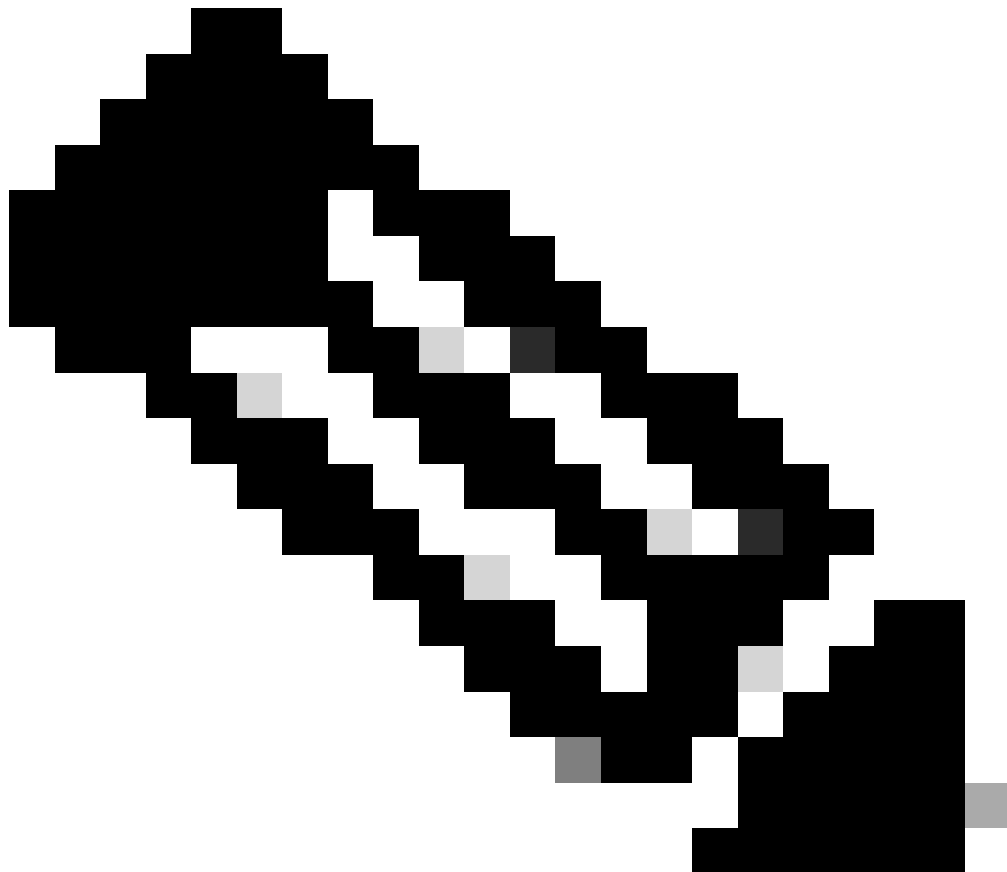
- لكشب ةنوكم مزح اذه لسري. يئاهنل مدختسمال ئيهاهم يف ةلكشم دوجو ىلع رشؤم اذه يئاولشعلا ردصم لل MAC نيوانع اهنأ ىلع لوحمل اهمه في حيحص ريغ.

لمعل ةطخ

- MAC نيوانع ب حمسي يذلا "تالاجمل ددعتم فيضملا عضو ةقداصلم" نيوكتب مق طقف نينثإ.
- هلزعو لوؤسمال زاهج ىلع فرعتال.

ققحتل/رارقل

- اهتظالم نكمي ةلكشم دجوت ال لجال اذه نيوكت دعب.



- Dot1x auth session host-mode multi-domain. وأذفنملا نامأ اما نيكم ت نم دكأت :ةطحالم

MTU قباطت مدع - 5 ويراني سل

Wired 802.1X Authentication failed.

Network Adapter: Intel(R) Ethernet Connection (13) I219-LM

Interface GUID: {83db9d6a-f8af-4f25-b133-a464ba980ffe}

Peer Address: F875A4EFA979

Local Address: 0892042D68CB

Connection ID: 0xe

Identity: NULL

User: 12345

Domain: ABC

Reason: 0x50007

Reason Text: There was no response to the EAP Response Identity packet.

Error Code: 0x0

مداخل إلى ليع أطلال اذه ISE لثمي

ةلكشمال فصول:

- مدختسمال لاصتاو IP APIA ناونع ىقلتت يتال مدختسمال ةزهجأ تراثأت

مدختسمال ضارعا

1. ةمزال لوط (3736: لاثم) نم ىلعا ةمزال لوط عم EAP ةباجتسا ىفرطال لىمعال لسري . 1492 عقوقمالي لعلال

Extensible Authentication Protocol

Code: Response (2)

Id: 4

Length: 1492

Type: TLS EAP (EAP-TLS) (13)

• EAP-TLS Flags: 0xc0

..0. = Start: False

EAP-TLS Length: 3736

اهالصالوا عاخال فاشكتسا عارجا مت

- ىلعا لاخداك لوحمال ىلعا لقا مچح ىلعا (MTU) لقنلل ىصقأال دحالا ةدحو نييعة مت (تياپ 1998: لاثمال لىبس ىلعا). ماظنالا ىوتسم
- (تياپ 9198: لاثمال لىبس ىلعا). ربكأ مچحب جورخال ةهجاو نيوكت مت

الازعنا

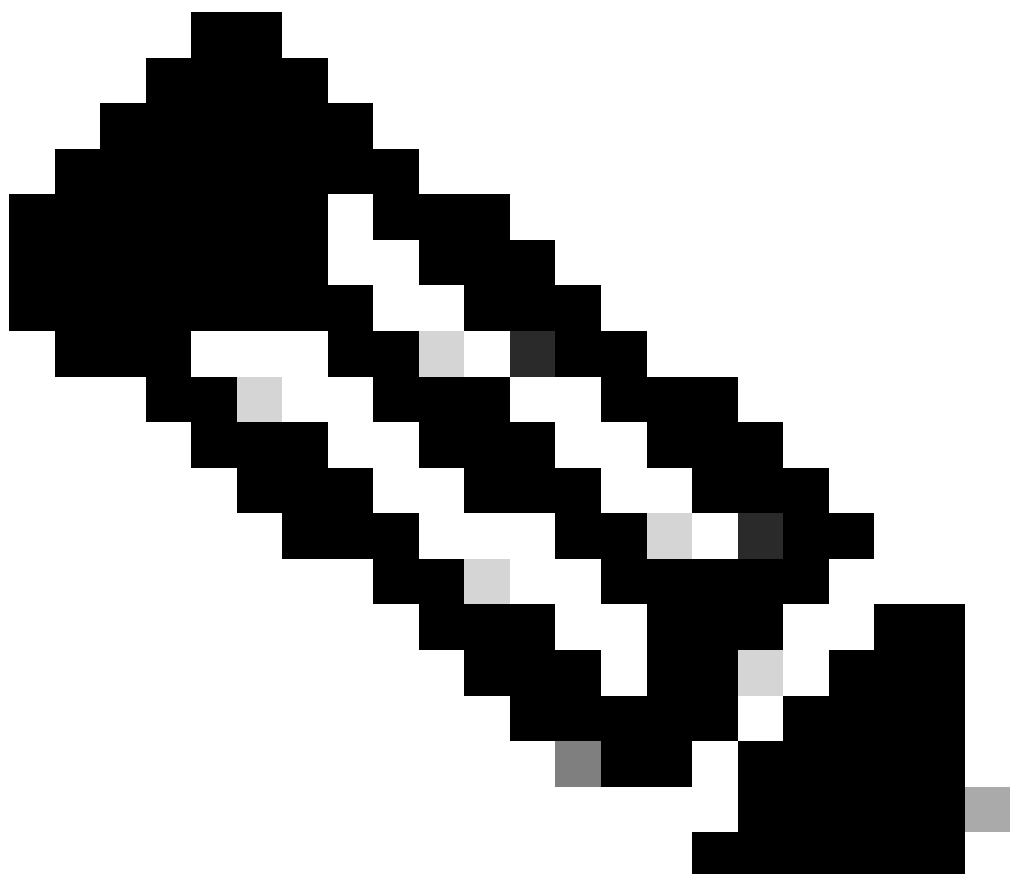
- ةلكشمال بىبسي راسمال ربع MTU ىف قباطتال مدع.

لمعال ةطخ

- لوحمال لىمحت دعاو 1500 ىلا ماظنلل (MTU) لقنلل ىصقأال دحالا ةدحو رييغت ب مق

ققحتال/رارقال

- ةحجان ةقداصمال حبصت ،تاداعإال هذو نيوكت دعب .



- راسم ربع (MTU) لقنل لى صقألا دحلأا ءءو سفن نى كمأ نم ءكأأ :ةظءالم ءمزلأا قفءأ.

IPDT ءىءء - 6 وىرانىسلا

ءلءشملا فصول:

- مءءسملا لاصأا و APIPA IP ناوئع ىقلأأ ءىءلا مءءسملا ءزهءأ ءرأأ.

مءءسملا ضارءأ

- ءهءاولا ىف اقبطم ءهنلا اءه ءىءل نا ءا، HA ىف ءىضارءفالا ءزهءألا ءوءو ءئع

IPDT_POLICY ءزهءألا ءبأأ ءهن

UDP لوكوآورب ءووىال

بقلأأ نى كمأ

- لالځ نم (ARP) نږوانعلا لېلحت لوكوتورب ىلع درلا طاقسإ متي ،لشفال زواجت دعب .لوصولا لوحم

اهحالصإو عاځأل فاشكتسأ عارج مت

1. لوحملا عطساوب تافشكتسملل ARP تاباجتسا طاقسإ متيس .
2. IPDT يقاو مادختساب لوحملا نيوكت مت .
3. APIPA ىلع لوصحلا يفرطال زاوجل او ARP قيقحت طاقسإ عيامح - IPDT .

الازعنإ

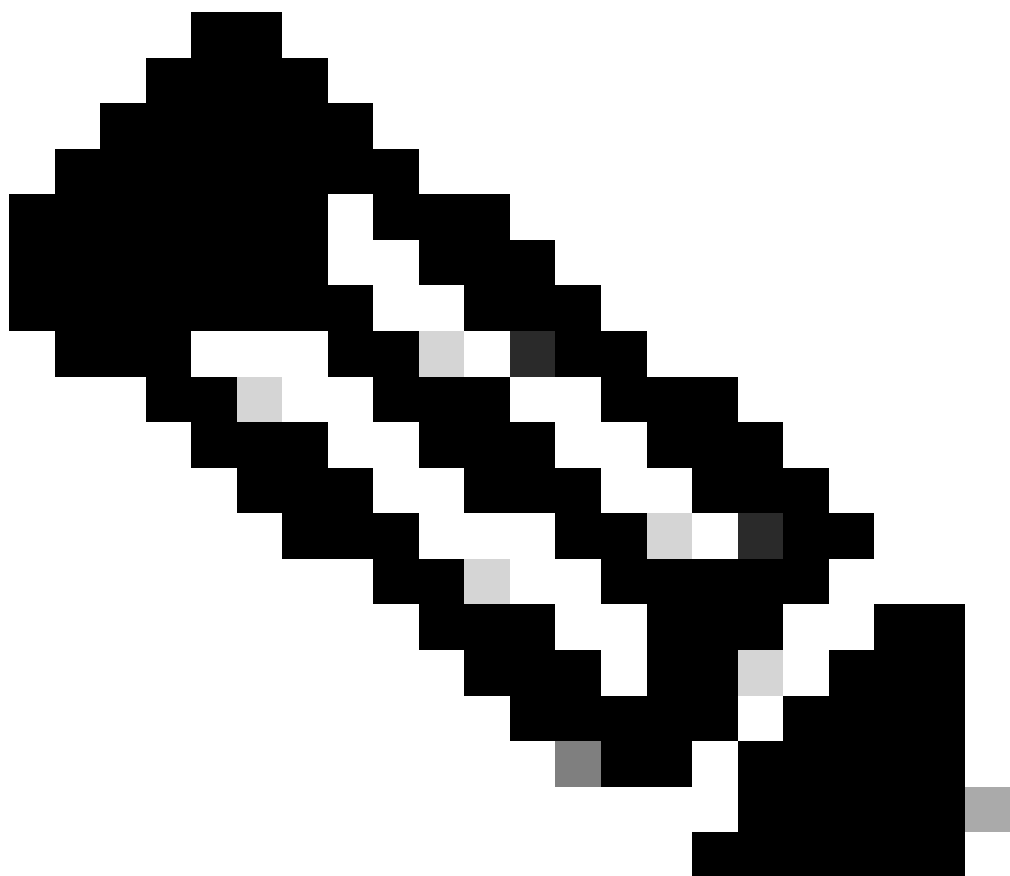
- "يځاولا" عزي م ببسب اهطاقسإ متي و IPDT ىلإ لصت يتي ال ARP مزح .
- امم ARP مزح "نامأل ىوتسم عيامح" نيوكت مادختساب اهنوكت متي يتي ال IPDT عسايس طقس ت اهي مچ وأ عي فرطال عزهجأل نم ليلقلال ىوس ىلإ لوصولا عيناكمإ مدع يف ببستي

لمعلال عځ

- Glean ىلإ Guard نم دادعإل رييغت ب مق .
- IPDT جهن يف "نامأل ىوتسم جهن نيوكت

ققحتل/رارقلال

- لحت متي و ARP عي لمع عطساوب ARP رباسم عجلاعم متت glean تاداعإ نيوكت دعب .
- علكشملا



- تارادص إالو 17.15.1 رادص إالو ف هحالص إا م تيسو اديج فورعم بي ع اذه :ةطحالم
ةقحالل
-

ةمچرتل هذه ل و ح

ةيلآل ا تاي ن ق ت ل ا ن م ة و م ج م ا د خ ت س ا ب د ن ت س م ل ا ا ذ ه Cisco ت م چ ر ت
م ل ا ع ل ا ا ح ن ا ع م ج ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل و
ا م ك ة ق ي ق د ن و ك ت ن ل ة ي ل آ ة م چ ر ت ل ض ف ا ن ا ة ط ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح م م چ ر ت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة م چ ر ت ل ا ع م ل ا ح ل ا و ه
ي ل ا م ا ء ا د ع و ج ر ل ا ب ي ص و ت و ت ا م چ ر ت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Systems
(ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا د ن ت س م ل ا