

ةطشننل-ةطشننل VRRP ءاطخأ فاشكتسا Viptela نم SD-WAN هجوم يف اهحالصا و

تاوت حمل

[ةمدقملا](#)

[ةيساسأل تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[ايجولوبوط](#)

[طشننل-طاشننل ءلاخ يف VRRP 1. ضرعلا](#)

[ححص ريغ DNS لىلا هيبتنت ليدبتلا 2. ضرعلا](#)

[رركم عضو يف لقتنا APs 3. ضرعلا](#)

[اهحالصا وءاطخأل فاشكتسا](#)

[لحلا](#)

ةمدقملا

Viptela (VRRP) يرهاظال SD-WAN هجوم راركت لوكوتورب لح ءيفيك دنتسملا اذه حصوي طاشننل ءلاخ يف قلاعال.

ةيساسأل تابلطتملا

تابلطتملا

ةيلال عيضاوملاب ءفرعم كيدل نوكت ناب Cisco ي صوت:

- Meraki لولحب ءيساسأل ءفرعم
- VRRP ب ءيساسأل ءفرعم

ةمدختسملا تانوكملا

ةيلال ءيدامل تانوكملا وءلاوملاب تارادصل لىلا دنتسملا اذه يف ءدراول تامولعمل دنتست:

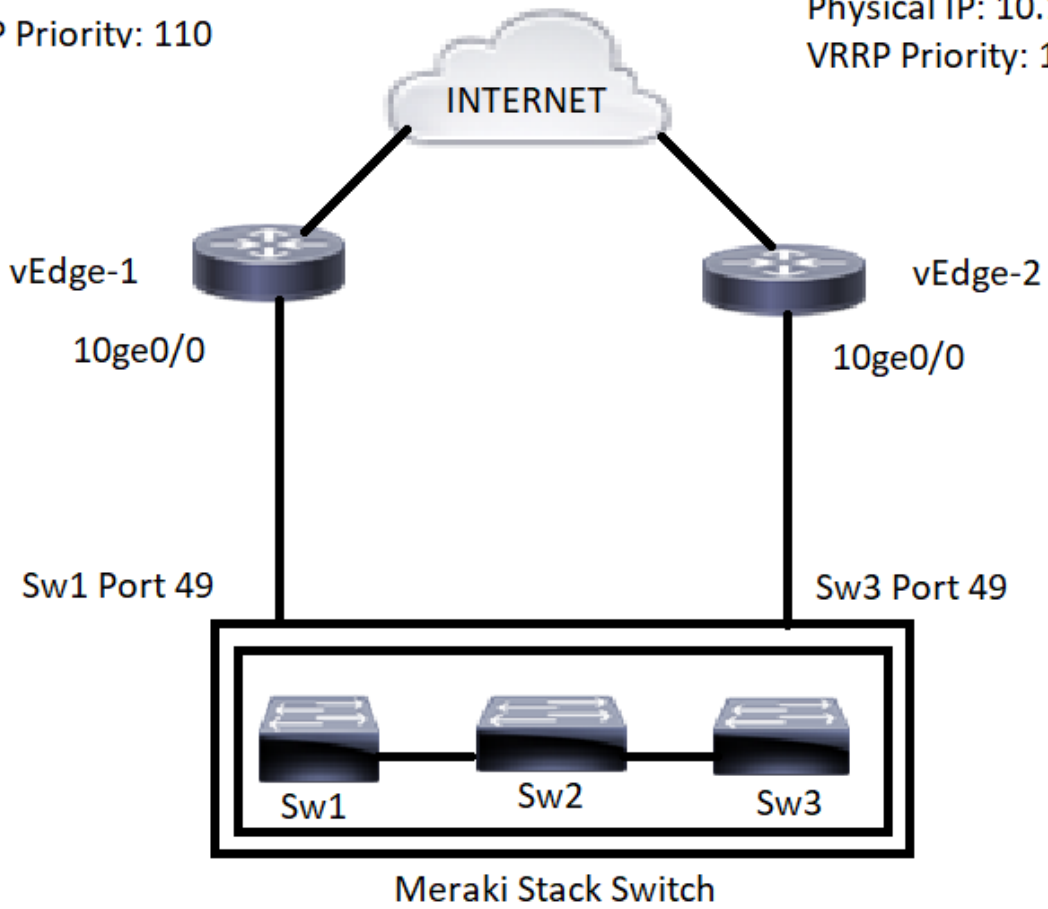
- vEdge 2000، رادصلال 19.2.3
- MS250-48FP، ءسن MS 12.28

ءصاخ ءيلمعم ءئيب يف ءدووملا ءزهأل نم دنتسملا اذه يف ءدراول تامولعمل ءاشننل مت تناك اذلا. (يضارفتلا) حوسمم نيوكتب دنتسملا اذه يف ءمدختسملا ءزهأل عيمج تءب رمأ لىلا لمحمل ريثائل كمهف نم دكأتف، لىغشتلا ديقتك تبش.

ايجولوبوط

VRRP VIP: 10.17.69.x
Physical IP: 10.17.69.x
VRRP Priority: 110

VRRP VIP: 10.17.69.x
Physical IP: 10.17.69.x
VRRP Priority: 100



طشننل-طاشننل ةلاح في VRRP 1. ضرعلا

زاهك Meraki سدكم تالوحم ىلى لفسألأب ةلصتملا مداخل ةرابعل vEdge ةزهجأ نم لك لمعت VRRP لوكتوربل ىساسأ

```
VE1# show vrrp MASTER PREFIX GROUP VRRP OMP ADVERTISEMENT DOWN LIST VPN IF NAME ID VIRTUAL IP
VIRTUAL MAC PRIORITY STATE STATE TIMER TIMER LAST STATE CHANGE TIME TRACK PREFIX LIST STATE ----
-----
----- 11 10ge0/0.670 1
10.17.69.1 00:00:5e:00:01:01 110 master up 1 3 2021-10-12T02:16:49+00:00
Default_Route_Prefix_List resolved
VE2# show vrrp MASTER PREFIX GROUP VRRP OMP ADVERTISEMENT
DOWN LIST VPN IF NAME ID VIRTUAL IP VIRTUAL MAC PRIORITY STATE STATE TIMER TIMER LAST STATE
CHANGE TIME TRACK PREFIX LIST STATE -----
-----
----- 11 10ge0/0.670 1 10.17.69.1 00:00:5e:00:01:01 100 master up 1 3 2021-10-
12T02:16:40+00:00 Default_Route_Prefix_List resolved
```

ححص ريغ DNS ىلى هيبنت ليدبتلا 2. ضرعلا

تامولعم ةحول في "ححص ريغ لكشب DNS نيوكت" ىلى VE2 ب لصلتملا 2 لوحملا هيبنت م Meraki.

The screenshot shows the Meraki switch management interface for a switch model MS250-48FP. A red error banner at the top states "DNS is misconfigured - How to resolve this error". Below the error, there is a location pin icon with the text "Set a location for this switch". The main interface displays a "Ports" section with a grid of 48 ports, each with a status indicator (green for up, red for down). A "Historical device data" section shows a "Connectivity" bar graph for the last day, indicating the switch has been online for most of the time.

رركم عضو في لقتنا APs 3. ضرعلا

ال لوحملا نأل ارظن لاسرلال ةداعل عضو ىلى 2 لوحملا ب ةلصتملا (APs) لوصولا طاقن تبهذ ةباوبلا ىلى لوصولا ةيلباق ىلى وحتي.

The screenshot shows the Meraki network dashboard. On the left, there is a "NETWORK" dropdown menu. The main dashboard displays four status categories: "OFFLINE" with 0 devices, "ALERTING" with 0 devices, "ONLINE" with 6 devices, and "REPEATERS" with 2 devices. Each category is represented by a colored dot and a number.

اهال صاوا ءاطخال فاشكتسا

1. vEdges نم VRRP كولس نم ققحت.

تظحال، ءالخال هذو فو VRRP ءمزح ءلخال نم ققحتل او vEdges نم لك نم "tcpdump" عو مءمءب مق لىل VE1 نم VRRP مزح لىقلى مءى ال هنا رىغ. VE1 ءطساوب ل سرتو لىقلىل VRRP مزح نا فو لكاشم ءووم ءىءكء كنعكو، لىلالابو. VE1 نم هسفن رمالا لاسرا مء، كلذ عم و. ءرابعلل vEdges ءفظو.

نم VE1:

```
10.17.69.3 > 224.0.0.18: vrrp 10.17.69.3 > 224.0.0.18: VRRPv2, Advertisement, vrid 1, prio 100,
authtype none, intvl 1s, length 20, addrs: 10.17.69.1 08:57:12.744406 80:b7:09:32:e5:02 >
01:00:5e:00:00:12, ethertype IPv4 (0x0800), length 54: (tos 0xc0, ttl 255, id 6968, offset 0,
flags [DF], proto VRRP (112), length 40) 10.17.69.2 > 224.0.0.18: vrrp 10.17.69.2 > 224.0.0.18:
VRRPv2, Advertisement, vrid 1, prio 110, authtype none, intvl 1s, length 20, addrs: 10.17.69.1
08:57:13.708034 00:00:5e:00:01:01 > 01:00:5e:00:00:12, ethertype IPv4 (0x0800), length 56: (tos
0xc0, ttl 255, id 29924, offset 0, flags [DF], proto VRRP (112), length 40)
```

نم VE2:

```
10.17.69.3 > 224.0.0.18: vrrp 10.17.69.3 > 224.0.0.18: VRRPv2, Advertisement, vrid 1, prio 100,
authtype none, intvl 1s, length 20, addrs: 10.17.69.1 08:57:50.644532 80:b7:09:31:82:a2 >
01:00:5e:00:00:12, ethertype IPv4 (0x0800), length 54: (tos 0xc0, ttl 255, id 31817, offset 0,
flags [DF], proto VRRP (112), length 40)
```

لمعو لطمع VE1 نا VE2 ضرءف لىلالابو، (10.17.69.2) VE1 نم VRRP ءمزح ءءو ال لىسسا VRRP لوكو ءورب.

2. Meraki سدكم كولس نم ققحت.

ءب رلا لوءمب ل صءملا لاسرالا ءءاع لءسو فو AP3 و AP4 نا لىل Meraki ءامو لعم ءءول رىشء ءلالءل DNS لىل هىبءنءل لىل ل صءى لءل 2.

ل ءقو ءىءرم سدكملا لاصءا لىسرنوكء ءىء Meraki TAC ءءفا، سدكملا ءلخال ءىءكءءل ءالوءملا نىب سدكملا لءءالءل لكاشم نا ءىءءمءى، ققءءل ءنء. Meraki TAC سدكملا فو ءىءونءءل او ءىسسا.

اهىل لءوول مءى مل لىءل VE1 نم VRRP ءمزح نع ءءءن ءلءشملا هذو نا Meraki ءءكءءم ءوورعم ءلءشم هذو. 2. سدكملا وءع لءلء نم (لىسسا) 1. سدكملا وءع لوءم رءع VE2 لىل لىل 12.28 لىل فو.

لءل

1. (ءقووملا ءالصال) سدكملا فو ءاضءالءالوءملا عىمء لىمءء ءءاع لىل.

2. رءءسم مءىم صءءءءء لىل Meraki لوءم لءبءءلءءءم ان رءل ءىءقءءب مق.

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا اذ ه Cisco ت مچرت
م ل ا ل ا ا ن ا ع مچ 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 ل ا ة مچرت ل ض ف ا ن ا ة ظ 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 مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ي ل ا م ا ة ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
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 دن ت س م ل ا