

VLAN تالابش نيب هيچوتلا نيوكت يجراخ هجوم مادختساب

تايوتحمل

[عمدقملا](#)

[سيساسال تابلطتملا](#)

[تابلطتملا](#)

[عمدختسملا تانوكملا](#)

[تالاطصالا](#)

[سيساسا تامولعم](#)

[نيوكتلا](#)

[كيشلل ليطيطختلا مسرلا](#)

[تانويكتلا](#)

[عمديفم رماوا](#)

[رماوالا جالخلا جذومن](#)

[Catalyst Switch](#)

[Cisco هجوم](#)

[قلص تاذا تامولعم](#)

عمدقملا

VLAN تالابش نيب هيچوتلا دادعإل عمزاللا تانويكتلا ميظنت عميفي كنننسملا اذه فصي
يجراخ Cisco هجوم مادختساب.

سيساسال تابلطتملا

تابلطتملا

يالاتلا عوضوملاب وفرعم كيذل نوكت ناب Cisco ي صوت

- سساسال هيچوتلا وفرعم

عمدختسملا تانوكملا

يالاتلا جماربلا تارادصإل كنننسملا اذه في دراولا تامولعمل كنننست

- Catalyst Switch Cisco IOS® 15.2E
- Cisco Router Cisco IOS 17.3

صاخ عمي لمعم عمي في دوجوملا زهجالا نم كنننسملا اذه في دراولا تامولعمل عاشنإ مت
تناك اذإ. (يضا رتفا) حوسمم نيوكتب كنننسملا اذه في عمدختسملا زهجالا عمي متا دب

رماً يأل لم تحملا ريثأتلل كمهف نم دكأتف ،ليغشتلا ديق كتكبش

تاحالطصلا

[تاجيملت تاحالطصلا](#) ىلا عجرا ،تادنتسملا تاحالطصلا لوح تامولعمل نم ديزم ىلع لوصحلل [في نقتلا Cisco](#).

ةيساسأ تامولعمل

Cisco هجوم مادختساب VLAN تاكبش نيي هي جوتلا دادعإل تانيوكتلا دنتسملا اذه فص ي رماً لك جئاتن ضرع متي ؛802.1Q لىصوت ىلع تانيوكتلا جذومن مادختساب هجرشيو يجرخا في Catalyst switch لذبم يأو ،ةفلتخملا Cisco ةلسلس تاهجوم مادختسا نكمي .اهذيفنت دنع اهسفن جئاتنلا ىلع لوصحلل دنتسملا اذه في ةمدقملا تاهويراني سلا

ربع (VLAN) ةيضارتفا ةيلحم تاكبش ةدع نم رورملا ةكرح لقنل ةلېسو وه لىصوتلا ذيفنتل ناتقيرط كانه تناك ،ةيادبلا في .ني زاهجلا نيي ةطقن ىلا ةطقن نم طابترلا Ethernet لىصوت:

- Cisco ةكرشل كولملا (ISL) InterSwitch Link لوكوتورب
- 802.1Q (IEEE) تانيورتكلال او عابرهكلا يس دنهم ده عم راي عم

،رثكأ وأ VLAN ي تكبش نم رورملا ةكرح لقنل هم مادختساو لاصتالا ةانق طبار عاشنا متي Cisco هجوم وأ Catalyst تالذبم نيي دحاو طبار ربع VLAN2 و VLAN1 ،لاثملا لىبس ىلع

VLAN-X ةكبش نيي VLAN تاكبش نيي ام هي جوتلاب مايقلل Cisco هجوم مادختسا متي Catalyst ةلسلس تالذبم نوكت امدنع اديفم نيوكتلا اذه نوكتي نأ نكمي .VLAN-Y ةكبشو VLAN تاكبش نيي لاصتالا وأ هي جوتلا اهنكمي الو طقف (L2) 2 ةقبطلا نم

ةكبش ىمسئتو .ةدحاو VLAN ةكبش ىلع ةمالع عضو متي ال ،802.1Q لىصوتل ةبسنلاب ريغ رورملا ةكرحل ةيلصلال VLAN ةكبش مادختسا متي .ةيلصلال VLAN ةكبش هذه VLAN ،802.1Q لاصتالا طخ نيوكت اناثأ .802.1Q لىصوتلا عضو في ذفنملا نوكتي امدنع ةزيمملا ب بناج لك ىلع اهسفن ةقيرطلاب ةيلصلال VLAN ةكبش نيوكت بجي هنأ ركدت نيوكت دنع ةيلصلال VLAN تاكبش ةقباطم مدع ةعئاشلا عاڤخالأ نم .لاصتالا ةانق طابترلا لذبملاو هجوملا نيي 802.1Q تاونق

لك ىلع ،يضارتفا لكشب ،VLAN1 يه ةيلصلال VLAN ةكبش نوكت ،اذه نيوكتلا جذومن في مادختسا كنكمي ،كب ةصاخلا ةكبشلا تاجايتحا ىلع انا .Catalyst لذبم و Cisco هجوم نم في رماوالا ركذمت .VLAN1 ةكبش ،ةيضارتفا ال VLAN ةكبش فالخب ةيلصلال VLAN ةكبش هذه ىلع ةيلصلال VLAN ةكبش رييغت ةيفيك لوح دنتسملا اذه في [تانيوكتلا](#) مسق ةزهجال

Cisco تاهجوم ةلسلس ىلع دنتسملا اذه في ةمدقملا تانيوكتلا جدامن مادختسا نكمي 802.1Q راي عمب VLAN ةكبش لىصوت معدت يتللا ةفلتخملا

 ةرورضللاب هب ىصوملا رادصلا وه دمتعملال لقألا رادصلا نوكتي نأ نكمي ال :ةظحالما بسح ةجرڈملا عاڤخالأ نع ثحبا ،كب صاخلا Cisco جتنملا ةنايص رادصلا لصفأ ديدحتل

✎ عا طخأل تاودأ ةعومجم يف جتنملا نوكم

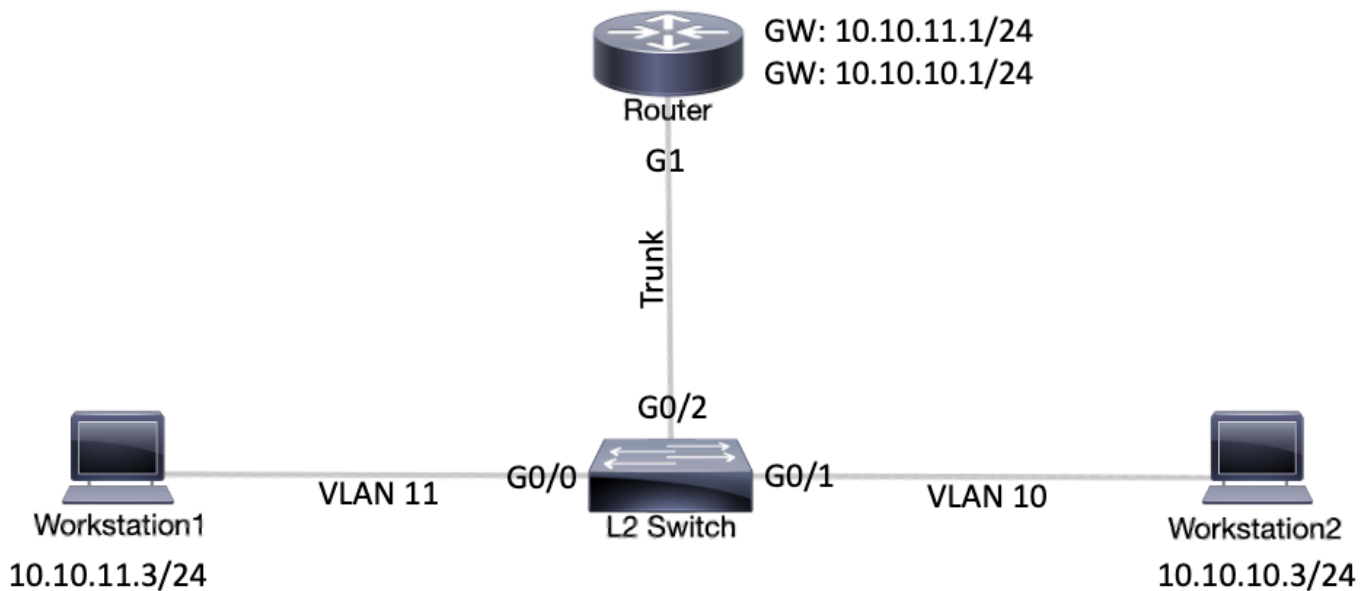
✎ تاودأل او تادن تسمل الى لوصول ني ل ج سمل Cisco ي مدخت سمل طقف نكمي :ةظحال مة.ةي ل خادل تامول عمل او

نيوكتلا

دنت سمل اذه يف ةحصولم تازيمل نيوكت تامول عمل كل مّدقّت، مسقلا اذه يف

ةكبش لل يطي طختلا مسرلا

ي نايبل ططخملا اذه يف حصولم ةكبشلا دادعإ دنت سمل اذه مدخت سي



ةكبش لل يطي طختلا مسرلا

تانيوكتلا

Catalyst L2 Switch
<pre><#root> !-- (Optional) Set the IP address and default gateway for VLAN1 for management purposes. L2_Switch# configure terminal Enter configuration commands, one per line. End with CNTL/Z. L2_Switch(config)# interface vlan 1 L2_Switch(config-if)#</pre>

```
ip address 10.10.0.2 255.255.255.0
```

```
L2_Switch(config-if)#no ip directed-broadcast
```

```
L2_Switch(config-if)#no ip route-cache
```

```
L2_Switch(config-if)#exit
```

```
L2_Switch(config-if)#
```

```
ip default-gateway 10.10.0.1
```

```
!-- (Optional) Set the VTP Mode. In our example, we have set the mode to be transparent.
```

```
!-- Depending on your network, set the VTP Mode accordingly.
```

```
L2_Switch(config)#
```

```
vtp mode transparent
```

```
Setting device to VTP Transparent mode for VLANs.
```

```
L2_Switch(config)#
```

```
!-- Adding VLAN10 and VLAN11.
```

```
L2_Switch(config)#
```

```
vlan 10-11
```

```
L2_Switch(config-vlan)#exit
```

```
L2_Switch(config)#
```

```
!-- Enable trunking on the interface GigabitEthernet 0/2.
```

```
!-- Enter the trunking encapsulation as dot1q.
```

```
L2_Switch(config)#
```

```
interface gigabitEthernet 0/2
```

```
L2_Switch(config-if)#
```

```
switchport trunk encapsulation dot1q
```

```
L2_Switch(config-if)#
```

```
switchport mode trunk
```

```
!-- In case of dot1q, you need to make sure that the native VLAN matches across the link.
```

```
!-- On Catalyst Switches, by default, the native VLAN is 1.
```

```
!-- It is very important that you change the native VLAN on the router accordingly.
```

```
!-- The following set of commands can place on the interfaces connecting to the workstations.
```

```
L2_Switch(config)#
```

```
interface gigabitEthernet 0/0
```

```
L2_Switch(config-if)#
```

```
switchport mode access
```

```
L2_Switch(config-if)#
```

```
switchport access vlan 11
```

```
L2_Switch(config-if)#exit
```

```
L2_Switch(config)#
```

```
interface gigabitEthernet 0/1
L2_Switch(config-if)#
switchport mode access

L2_Switch(config-if)#
switchport access vlan 10
L2_Switch(config-if)#exit

!-- Remember to save the configuration.

L2_Switch#
write memory

Building configuration...
```

هجوم ال

 مت Cisco هجوم ىلع اهل اخدا مت يت ال رماو الة لة شاش ال تاطقل رهظت :ةظالم مة نة عم تاوطخو رماو ا حرشل لئام طخب رماو ال نيب تاقي لعت الة فاضا

```
<#root>

Router#
configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

!-- Select GigabitEthernet 1 for the trunk configuration.
!-- No Layer 3 (L3) configuration is done here.

Router(config)#

interface GigabitEthernet 1

Router(config-if)#

no shut

Router(config-if)#

exit

!-- Enable dot1q on the sub-interface one for each VLAN.
!-- Configure L3 information on the sub-interface for each gateway.

Router(config)#

interface gigabitEthernet 1.10
```

```
Router(config-subif)#
encapsulation dot1Q 10

Router(config-subif)#
ip address 10.10.10.1 255.255.255.0

Router(config-subif)#
exit

Router(config)#
interface gigabitEthernet 1.11

Router(config-subif)#
encapsulation dot1Q 11

Router(config-subif)#
ip address 10.10.11.1 255.255.255.0

Router(config-subif)#
exit

!-- (Optional) For the management VLAN 1 make sure that the native VLAN matches across the link.
!-- On the switch, by default, the native VLAN is 1.
!-- On the router, configure VLAN1 as the native VLAN.

Router(config)#
interface gigabitEthernet 1.1

Router(config-subif)#
encapsulation dot1Q 1 native

Router(config-subif)#
ip address 10.10.0.1 255.255.255.0

Router(config-subif)#
end

!-- Remember to save the configuration.

Router#write memory
Building configuration...
[OK]
Router#
```

✎ ج.ي.ح.ص.ل.ك.ش.ب.ل.م.ع.ل.ا.ت.ا.ط.ح.م.ى.ل.ع.ة.ي.ض.ا.ر.ت.ف.ا.ل.ا.ت.ا.ب.ا.و.ب.ل.ا.د.ا.د.ع.إ.ن.م.د.ك.أ.ت.ل.ا.ك.م.ز.ل.ي.، 2 ل.م.ع.ل.ا.ة.ب.س.ن.ل.ا.ب.و. 10.10.11.1 ة.ي.ض.ا.ر.ت.ف.ا.ل.ا.ة.ر.أ.ب.ع.ل.ا.ن.و.ك.ت.ن.أ.ب.ج.ي.، 1 ل.م.ع.ل.ا.ة.ط.ح.م.ل.ة.ب.س.ن.ل.ا.ب. 10.10.10.1. ة.ي.ض.ا.ر.ت.ف.ا.ل.ا.ة.ر.أ.ب.ع.ل.ا.ن.و.ك.ت.ن.أ.ب.ج.ي.، 2 ل.م.ع.ل.ا.ة.ط.ح.م.ل.

ة.د.ي.ف.م.ر.م.ا.و.أ

ع.ق.و.ت.م.ل.ا.و.ح.ن.ل.ا.ى.ل.ع.ل.م.ع.ي.ك.ب.ص.ا.خ.ل.ا.ن.ي.و.ك.ت.ل.ا.ن.أ.ن.م.د.ك.أ.ت.ل.ا.ى.ل.ع.م.س.ق.ل.ا.ا.ذ.ه.ك.د.ع.ا.س.ي.

ق.ق.ح.ت.ل.ا.ي.ف.ة.د.ع.ا.س.م.ل.ل.ة.ي.ل.ل.ا.ت.ل.ا.ر.م.ا.و.أ.ل.ا.م.ا.د.خ.ت.س.ا.ك.ن.ك.م.ي.، Catalyst ل.د.ب.م.ي.ف.

- show interface {FastEthernet | GigabitEthernet} <module/port> switchport
- show vlan
- show vtp status

ة.ي.ل.ل.ا.ت.ل.ا.ر.م.ا.و.أ.ل.ا.م.د.خ.ت.س.ا.، Cisco ة.ج.و.م.ى.ل.ع.

- show ip route
- show interface

ر.م.ا.و.أ.ل.ا.ج.ا.ر.خ.إ.ج.ذ.و.م.ن

Catalyst Switch

م.ت.ي.ه.ن.أ.م.ك.ذ.ف.ن.م.ل.ل.ة.ي.ل.ي.غ.ش.ت.ل.ا.و.ة.ي.ر.ا.د.إ.ل.ا.ة.ل.ا.ح.ن.م.ق.ق.ح.ت.ل.ل.ي.ل.ل.ا.ت.ل.ا.ر.م.أ.ل.ا.م.ا.د.خ.ت.س.ا.م.ت.ي.م.ت.ي.ل.ا.ص.ت.ا.ل.ا.ة.ا.ن.ق.ي.ب.ب.ن.ا.ج.ا.ل.ك.ى.ل.ع.ة.ي.ل.ل.ص.أ.ل.ا. VLAN ة.ك.ب.ش.ق.ب.ا.ط.ت.ن.م.د.ك.أ.ت.ل.ل.ه.م.ا.د.خ.ت.س.ا.ع.ض.و.ي.ف.ذ.ف.ن.م.ل.ا.ن.و.ك.ي.ا.م.د.ن.ع.ة.ز.ي.م.م.ل.ا.ر.ي.غ.ر.و.ر.م.ل.ا.ة.ك.ر.ح.ل.ة.ي.ل.ل.ص.أ.ل.ا. VLAN ة.ك.ب.ش.م.ا.د.خ.ت.س.ا.802.1Q. ل.ي.ص.و.ت.ل.

ج.ا.ر.خ.إ.ل.ا.ر.م.أ.ض.ر.ع.ي.، 802.1Q ل.ي.ص.و.ت.ى.ل.ل.ة.ب.س.ن.ل.ا.ب.

<#root>

L2_Switch#

show interfaces gigabitEthernet 0/2 switchport

Name: Gi0/2

Switchport: Enabled

Administrative Mode: trunk

Operational Mode: trunk

Administrative Trunking Encapsulation: dot1q

Operational Trunking Encapsulation: dot1q

Negotiation of Trunking: On

Trunking Native Mode VLAN: 1 (default)

VLAN 10 كېش ىلى (ذفانملا) تاهاولا نأ نم ققحتلل يلاتل رملأ مادختسا متي
 كېش ىلى gi0/0 يمتنيو VLAN10 كېش ىلى gi0/1 ةهاولا يمتنت ،لاثملا اذه ي .ةححصلا
 VLAN1. كېش ىلى فاضعأ مهف يقابلأ .VLAN11

L2 Switch#

VLAN	Name	Status	Ports
1	default	active	Gi0/3
10	VLAN0010	active	Gi0/1
11	VLAN0011	active	Gi0/0
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

يُعالج VLAN عبءًا من لي صو ت ل و ك و ت و ر ب ن ي و ك ت ن م ق ق ح ت ل ل ي ل ا ت ل ر م ا ل م ا د خ ت س ا م ت ي ل ك ي ه ي ل ع ح ي ح ص ل V T P ع ض و د م ت ع ي . ف ا ف ش ل ع ض و ل م ا د خ ت س ا م ت ي ، ل ا ث م ل ا ذ ه ي ف . ل د ب م ل . ك ت ك ب ش .

L2 Switch#

show vtp status

```
VTP Version capable      : 1 to 3
VTP version running      : 1
VTP Domain Name          :
VTP Pruning Mode         : Disabled
VTP Traps Generation     : Disabled
Device ID                : 5254.0000.8000
Configuration last modified by 0.0.0.0 at 3-1-24 15:21:18
```

Feature VLAN:

```
VTP Operating Mode       : Transparent

Maximum VLANs supported locally : 1005
Number of existing VLANs      : 7
Configuration Revision       : 0
MD5 digest                  : 0x9F 0x7D 0x8D 0x10 0xB1 0x22 0x2F 0xE7
                             0x29 0x77 0x42 0xA7 0x95 0xE7 0x68 0x1C
```

هجوم Cisco

هجوم على امني وكتمت في التل اية عرف ال تاهاج اول لوج L3 هي جوت تامول عمب في التل رم ال ربخي

<#root>

Router#

show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
H - NHRP, G - NHRP registered, g - NHRP registration summary
o - ODR, P - periodic downloaded static route, l - LISP
a - application route
+ - replicated route, % - next hop override, p - overrides from PfR
& - replicated local route overrides by connected

Gateway of last resort is not set

```
10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
C    10.10.0.0/24 is directly connected, GigabitEthernet1.1
L    10.10.0.1/32 is directly connected, GigabitEthernet1.1

C    10.10.10.0/24 is directly connected, GigabitEthernet1.10
L    10.10.10.1/32 is directly connected, GigabitEthernet1.10
C    10.10.11.0/24 is directly connected, GigabitEthernet1.11
L    10.10.11.1/32 is directly connected, GigabitEthernet1.11
```

ةبسننل اب .ةهجالولل ةيليغشتلاو ةيرادلإا ةلاحلا نم ققحتلل يلاتل رملأا مادختسا متي
جارجالإا رملأا ضرعي ،ةجوملا ةهجالو ةلاحلا

<#root>

Router#

show interfaces

GigabitEthernet1 is up, line protocol is up

Hardware is CSR vNIC, address is 5254.0000.004d (bia 5254.0000.004d)
MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
 reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Full Duplex, 1000Mbps, link type is auto, media type is Virtual
output flow-control is unsupported, input flow-control is unsupported
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:00, output 00:14:10, output hang never
Last clearing of "show interface" counters never
Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
 5338 packets input, 361563 bytes, 0 no buffer
 Received 0 broadcasts (0 IP multicasts)
 0 runs, 0 giants, 0 throttles
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
 0 watchdog, 0 multicast, 0 pause input
 13 packets output, 1248 bytes, 0 underruns
 Output 0 broadcasts (0 IP multicasts)
 0 output errors, 0 collisions, 2 interface resets
 57 unknown protocol drops
 0 babbles, 0 late collision, 0 deferred
 1 lost carrier, 0 no carrier, 0 pause output
 0 output buffer failures, 0 output buffers swapped out

GigabitEthernet1.1 is up, line protocol is up

Hardware is CSR vNIC, address is 5254.0000.004d (bia 5254.0000.004d)
Internet address is 10.10.0.1/24
MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
 reliability 255/255, txload 1/255, rxload 1/255
Encapsulation 802.1Q Virtual LAN, Vlan ID 1.
ARP type: ARPA, ARP Timeout 04:00:00
Keepalive set (10 sec)
Last clearing of "show interface" counters never

GigabitEthernet1.10 is up, line protocol is up

Hardware is CSR vNIC, address is 5254.0000.004d (bia 5254.0000.004d)
Internet address is 10.10.10.1/24

MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
 reliability 255/255, txload 1/255, rxload 1/255
Encapsulation 802.1Q Virtual LAN, Vlan ID 10.
ARP type: ARPA, ARP Timeout 04:00:00
Keepalive set (10 sec)
Last clearing of "show interface" counters never

```

GigabitEthernet1.11 is up, line protocol is up
  Hardware is CSR vNIC, address is 5254.0000.004d (bia 5254.0000.004d)
  Internet address is 10.10.11.1/24

  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation 802.1Q Virtual LAN, Vlan ID 11.
  ARP type: ARPA, ARP Timeout 04:00:00
  Keepalive set (10 sec)
  Last clearing of "show interface" counters never
GigabitEthernet2 is administratively down, line protocol is down
  Hardware is CSR vNIC, address is 5254.0000.004e (bia 5254.0000.004e)
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full Duplex, 1000Mbps, link type is auto, media type is Virtual
  output flow-control is unsupported, input flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo

```

ةلص تاذا تامولعم

- [Catalyst تالددبمو Catalyst 3550/3750 لددبم نيي 802.1q لاصتالا ةانق نيوكت](#)
- [Catalyst تالددبم لالخ نم VLAN تاكبش نيي هيچوتلا نيوكت](#)
- [Cisco Systems - تاليزنت لاوي نفلل معدلا](#)

ةمچرتل هذه لوح

ةيلآل تاي نقتل نم ةومجم مادختساب دنتسمل اذه Cisco تمچرت
ملاعلا اناء عي مجي في ني مدختسمل معدى وتحم مي دقتل ةيرشبلاو
امك ةقيقد نوكت نل ةيلآ ةمچرت لصفأ نأ ةظحال ميجري. ةصاخلا مهتغلب
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحا وه
ىلإ أمئاد عوچرلاب يصوت و تامچرتل هذه ةقदन ع اهتيلوئسم Cisco
Systems (رفوتم طبارلا) يلصلأال يزيلچنلإا دنتسمل