

# نم ققحتلاو ETA و AVC و NetFlow نيوكت Catalyst 9000 Series Switches

## تايوتحمل

[عمدقمل](#)

[ةيساسأل تابلطتمل](#)

[تابلطتمل](#)

[عمدختسمل تانوكمل](#)

[ةيساسأ تامولعم](#)

[ةكبش ل ل يطيطختلا مسرلا](#)

[نيوكتلا](#)

[تانوكمل](#)

[قفدتلا لچس](#)

[قفدتلا ردصم](#)

[قفدتلا ةبقارم](#)

[\(يراي تخا\) قفدتلا تانيع ذخأ](#)

[دويقلا](#)

[ةحصللا نم ققحتلا](#)

[لققتسمل ايساسأل ماظنلا نم ققحتلا](#)

[ايساسأل ماظنلا دامتعا نم ققحتلا](#)

[NFL ميسقت لودج - NetFlow ةئيهت](#)

[قفدتلا ةبقارم](#)

[NetFlow \(ACL\) لوصولي فمكحتلا ةمئاق](#)

[قفدتلا عانق](#)

[ينمزلا عباطلا ليومت اغلا تانايبو قفدتلا تالاح](#)

[\(AVC\) اهيفمكحتلاو تاقيبطتلا ةيؤر ةينام](#)

[ةيساسأ تامولعم](#)

[روطتلاو عادال](#)

[ةيكلسلا AVC دويق](#)

[ةكبش ل ل يطيطختلا مسرلا](#)

[تانوكمل](#)

[NBAR2](#)

[نم ققحتلا AVC](#)

[\(ETA\) ةرفشمل رورملا ةكحتاليلحت](#)

[ةيساسأ تامولعم](#)

[ةكبش ل ل يطيطختلا مسرلا](#)

[تانوكمل](#)

[دويقلا](#)

[نيوكتلا](#)

[ةحصللا نم ققحتلا](#)

# مقدمة

هذه المقالة تشرح كيفية إعداد NetFlow على أجهزة Cisco IOS XE. كما تشرح كيفية إعداد NetFlow على أجهزة Cisco IOS XE. كما تشرح كيفية إعداد NetFlow على أجهزة Cisco IOS XE.

## أساسيات التثبيت

### التثبيت

الخطوات لإعداد NetFlow على أجهزة Cisco IOS XE:

- Netflow
- AVC
- التثبيت

### إعداد التثبيت

يتم إعداد NetFlow على أجهزة Cisco IOS XE باستخدام الأوامر التالية:

تتم إعداد NetFlow على أجهزة Cisco IOS XE باستخدام الأوامر التالية:

### الخطوات

الخطوات لإعداد NetFlow على أجهزة Cisco IOS XE:

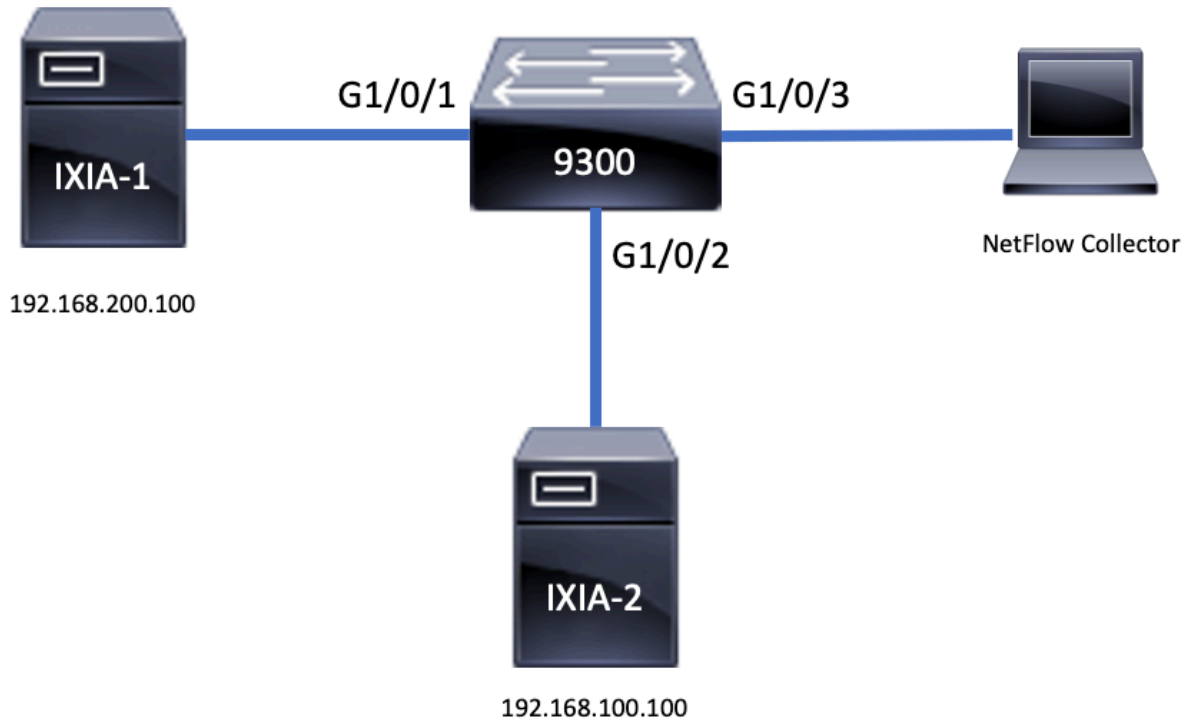
- 9200
- 9400
- 9500
- 9600
- إعدادات التثبيت على أجهزة Cisco IOS XE 16.12

## أساسيات التثبيت

- التثبيت على أجهزة Cisco IOS XE باستخدام الأوامر التالية:
- إعدادات التثبيت على أجهزة Cisco IOS XE باستخدام الأوامر التالية:
- إعدادات التثبيت على أجهزة Cisco IOS XE باستخدام الأوامر التالية:
- إعدادات التثبيت على أجهزة Cisco IOS XE باستخدام الأوامر التالية:
- إعدادات التثبيت على أجهزة Cisco IOS XE باستخدام الأوامر التالية:

show رمألا نوكي نأ نكمي (Fed) يساسألا ماظنلا رماوأ فلتخت نأ نكمي: **show platform fed <active|standby>** لباقم "show platform fed switch <active|standby>". اذإ رىغتملا ةبرجت ىجرىف ،ةلثمألا يف اهإلإ راشملا ةغايصلال عيزوت متي

## ةكبش لىل يطيختلا مسرلا



## نيوكتلا

### تانوكتلا

نم ديدعلا يه واعم اهم ادختسإ نكمي **قيس يئر تانوكم ةثالث** نم NetFlow نيوكت نيوكتي اهرىدصتو تانايبل رورم ةكرح لىلحت ءارجال تانايبتلا

### قفدتلا لىلس

- NetFlow تاللس صيصخت متي .ةيساسألا رىغو ةيساسألا لوقحلا نم جيزم وه لىلسلا نيزختل ةمدختسمل تقوؤملا نيزختلا ةركاذ ديدحتل ةنرملا NetFlow تاشاشل ةنرملا قفدتلا تانايب
- اهم ادختسإ نكمي يتلا اقبسمة ددحمل تاللسلا نم ديدعلا نرملا NetFlow نمضتتي رورملا ةكرح ةبقارملا
- ةبقارملا تقوؤملا نيزختلا ةركاذل صصخم تاللس ديدحت نرملا NetFlow حيتي امك صيصختل ةيساسألا رىغو ةيساسألا لوقحلا ديدحت قيرط نع ةنرملا NetFlow قفدت ةصاخلا كاتابلطتملا قفو تانايبلال ةومجم

قفدتلا لىلس نيوكت لىلصافت ،لاثملا يف حضوم وه امك

```
flow record TAC-RECORD-IN
match flow direction
match ipv4 source address
match interface input
match ipv4 destination address
match ipv4 protocol
collect counter packets long
collect counter bytes long
collect timestamp absolute last
collect transport tcp flags
```

```
flow record TAC-RECORD-OUT
match flow direction
match interface output
match ipv4 source address
match ipv4 destination address
match ipv4 protocol
collect counter packets long
collect counter bytes long
collect timestamp absolute last
collect transport tcp flags
```

## ق ف د ت ل ا ر د ص م

- تقؤم ل ا ن ي ز خ ت ل ا ة ر ك ا ذ ي ف ة د و ج و م ل ا ت ا ن ا ي ب ل ا ر ي د ص ت ل ق ف د ت ل ا ر ي د ص م م ا د خ ت س ا م ت ي ن ي ز خ ت ل ا و ل ي ل ح ت ل ل ، (NetFlow ع م ج م ك ل م ع ي م د ا خ) د ي ع ب م ا ط ن ي ل ا ق ف د ت ل ا ة ب ق ا ر م ل .
- ت ا ن ا ي ب ل ا ر ي د ص ت ة ي ن ك ا م ا ر ي ف و ت ل ق ف د ت ل ا ت ا ش ا ش ل ق ف د ت ل ا ر ي د ص م ن ي ي ع ت م ت ي ق ف د ت ل ا ت ا ش ا ش ل .

ق ف د ت ل ا ر د ص م ن ي و ك ت ل ي ص ا ف ت ، ل ا ث م ل ا ي ف ح ض و م و ه ا م ك :

```
flow exporter TAC-EXPORT
destination 192.168.69.2
source Vlan69
```

## ق ف د ت ل ا ة ب ق ا ر م

- ذ ي ف ن ت ل ت ا ه ج ا و ل ا ي ل ع ه ق ي ب ط ت م ت ي ذ ل ا ن ر م ل NetFlow ن و ك م ي ه ق ف د ت ل ا ت ا ش ا ش .
- ن ي ز خ ت ل ا ة ر ك ا ذ ي ل ا ا ه ت ف ا ض ا و ة ب ش ل ا ر و ر م ة ك ر ح ن م ق ف د ت ل ا ت ا ن ا ي ب ع ي م ج ت م ت ي ل و ق ح ل ا ي ل ع ة ل م ل ع م ل ا د م ت ع . ة ل م ل ع ل ل ي غ ش ت ا ن ا ث ا ق ف د ت ل ا ة ب ق ا ر م ل ت ق و م ل ا ق ف د ت ل ا ل ج س ي ف ة ي س ا س ا ل ا ر ي غ و ة ي س ا س ا ل ا .

ق ف د ت ل ا ة ب ق ا ر م ن ي و ك ت ل ي ص ا ف ت ، ل ا ث م ل ا ي ف ح ض و م و ه ا م ك :

```
flow monitor TAC-MONITOR-IN
exporter TAC-EXPORT
record TAC-RECORD-IN
```

```
flow monitor TAC-MONITOR-OUT
exporter TAC-EXPORT
record TAC-RECORD-OUT
```

```
Switch#show run int g1/0/1
Building configuration...
```

```
Current configuration : 185 bytes
```

```
!  
interface GigabitEthernet1/0/1  
switchport access vlan 42  
switchport mode access  
ip flow monitor TAC-MONITOR-IN input  
ip flow monitor TAC-MONITOR-OUT output  
load-interval 30  
end
```

## ق ف د ت ل ا ت ا ن ي ع ذ خ ا ( ي ر ا ي ت خ ا )

- ه ج و م ل ا ن ي و ك ت ي ف ة ل ص ف ن م ت ا ن و ك م ك ق ف د ت ل ا ج ذ ا م ن ا ش ن ا م ت ي .
- ز ا ه ج ل ا ي ل ع ل م ح ل ل ل ي ل ق ل ل ل ي ل ح ل ل ل ة د د ح م ل ا م ز ح ل ا د د ع ق ف د ت ل ا ت ا ن ي ع ذ خ ا ت ا د ح و د د ح ت .
- ن ر م ل ا N e t F l o w م د خ ت س ي ي ذ ل ا ز ا ه ج ل ا ي ل ع ل م ح ل ل ل ي ل ق ل ل ق ف د ت ل ا ج ذ ا م ن ا م ا د خ ت س ا م ت ي .
- ن ر م ل ا N e t F l o w م د خ ت ل ل ة د د ح م ل ا م ز ح ل ا د د ع د ح ل ل ا خ ن م ه ق ي ق ح ت م ت ي ي ذ ل ا .
- م ت ي ي ت ل ا م ز ح ل ا د د ع ي ف ض ا ف خ ن ا ك ا ن ه ن ا ك ا ذ ا . ه ج و م ل ا ا د ا ل ق ف د ت ل ا ت ا ن ي ع ل د ا ب ت ة ق د .
- ة ر ك ا ذ ي ف ة ن ز خ م ل ا ت ا م و ل ع م ل ا ة ق د ر ث ا ت ا ن ا ن ك م ي ، ق ف د ت ل ا ة ش ا ش ة ط س ا و ب ا ه ل ي ل ح ت .
- ق ف د ت ل ا ة ش ا ش ل ت ق و م ل ا ن ي ز خ ت ل ا .

ق ف د ت ل ا ت ا ن ي ع ذ خ ا ن ي و ك ت ، ل ا ث م ل ا ل ي ب س ي ل ع ، ل ا ث م ل ا ي ف ح ص و م و ه ا م ك

```
sampler SAMPLE-TAC  
description Sample at 50%  
mode random 1 out-of 2
```

```
Switch(config)#interface GigabitEthernet1/0/1  
Switch(config-if)#ip flow monitor TAC-MONITOR-IN sampler SAMPLE-TAC input  
Switch(config-if)#end
```

## د و ي ق ل ا

- م ت ي ذ ل ا N e t F l o w ن ا ف ا ل ا و ، ة ن و ر م ل ا ل م ا ك N e t F l o w ل D N A ق ح ل م ص ي خ ر ت ر ف و ت م ز ل ي .
  - ط ق ف ا ر ف و ت م ن و ك ي ه ر ا ب ت خ ا .
  - ر د ص م ك ة ر ا د ا ل ا ذ ف ن م ا د خ ت س ا ق ف د ت ل ا ي ر د ص م ل ن ك م ي ا ل .
- ن ي ب س ا ن م ل ا ز م ر ل ا و ي س ا س ا ل ا م ا ط ن ل ل ن ي و ك ت ل ا ل ي ل د ي ل ا ع ج ر ا ، ة ل م ا ش ة م ئ ا ق ت س ي ل ه ذ ه .

## ة ح ص ل ا ن م ق ق ح ت ل ا

### ل ق ت س م ل ا ي س ا س ا ل ا م ا ط ن ل ا ن م ق ق ح ت ل ا

ة ب و ل ط م ل a N e t F l o w ت ا ن و ك م د و ج و ن م د ك ا ت و ن ي و ك ت ل ا ن م ق ق ح ت

1. ق ف د ت ل ا ل ج س
2. ق ف د ت ل ا ر د ص م
3. ق ف د ت ل ا ة ب ق ا ر م
4. ق ف د ت ل ا ت ا ن ي ع ذ خ ا ( ي ر ا ي ت خ ا )

م ق ، د ح ا و ر م ا ي ف ق ف د ت ل ا ة ب ق ا ر م ج ر خ م و ، ق ف د ت ل ا ر د ص م و ، ق ف د ت ل ا ل ج س ض ر ع ل : ح ي م ل ت  
" s h o w r u n n i n g - c o n f i g f l o w m o n i t o r < f l o w m o n i t o r n a m e > e x p a n s i o n " ل ي غ ش ت ب

ه ب ة ط ب ت ر م ل ا ت ا ن و ك م ل ا و ل ا خ د ا ل ا ه ا ج ت ا ب ق ف د ت ل ا ة ب ق ا ر م ط ب ر م ت ي ، ل ا ث م ل ا ي ف ح ص و م و ه ا م ك

```
Switch#show running-config flow monitor TAC-MONITOR-IN expand
```

```
Current configuration:
```

```
!  
flow record TAC-RECORD-IN  
  match ipv4 protocol  
  match ipv4 source address  
  match ipv4 destination address  
  match interface input  
  match flow direction  
  collect transport tcp flags  
  collect counter bytes long  
  collect counter packets long  
  collect timestamp absolute last  
!  
flow exporter TAC-EXPORT  
  destination 192.168.69.2  
  source Vlan69  
!  
flow monitor TAC-MONITOR-IN  
  exporter TAC-EXPORT  
  record TAC-RECORD-IN  
!
```

هې ټپټرمل تان وكم ل او جاړخ ال ا ه اج ت اب ق ف د ت ل ا ټ ب ق ا ر م ط ب ر م ت ي ، ل ا ث م ل ا ي ف ح ض و م و ه ا م ك :

```
Switch#show run flow monitor TAC-MONITOR-OUT expand
```

```
Current configuration:
```

```
!  
flow record TAC-RECORD-OUT  
  match ipv4 protocol  
  match ipv4 source address  
  match ipv4 destination address  
  match interface output  
  match flow direction  
  collect transport tcp flags  
  collect counter bytes long  
  collect counter packets long  
  collect timestamp absolute last  
!  
flow exporter TAC-EXPORT  
  destination 192.168.69.2  
  source Vlan69  
!  
flow monitor TAC-MONITOR-OUT  
  exporter TAC-EXPORT  
  record TAC-RECORD-OUT  
!
```

ل ي ج س ت د ي ك ا ت ل د ي ف م ج ا ر خ ال ا ذ ه . <flow monitor name> show flow monitor ر م ا ل ل ي غ ش ت ب م ق ت ا ن ا ي ل ل :

```
Switch#show flow monitor TAC-MONITOR-IN statistics
```

```
Cache type: Normal (Platform cache)  
Cache size: 10000  
Current entries: 1  
  
Flows added: 1  
Flows aged: 0
```

ن ي ز خ ت ل ا ټ ر ك ا ذ ن ا د ي ك ا ت ل "show flow monitor <flow monitor name> cache ر م ا ل ل ي غ ش ت ب م ق

## جارخا ىلغى يوتحت NetFlow تقۇملا

```
Switch#show flow monitor TAC-MONITOR-IN cache
Cache type: Normal (Platform cache)
Cache size: 10000
Current entries: 1

Flows added: 1
Flows aged: 0

IPV4 SOURCE ADDRESS: 192.168.200.100
IPV4 DESTINATION ADDRESS: 192.168.100.100
INTERFACE INPUT: Gi1/0/1
FLOW DIRECTION: Input
IP PROTOCOL: 17
tcp flags: 0x00
counter bytes long: 4606617470
counter packets long: 25311085
timestamp abs last: 22:44:48.579
```

لاسراب ردصملا مایق دیکاتل `show flow source <source name> statistics` رمالا لیغش تب مق مزحلا:

```
Switch#show flow exporter TAC-EXPORT statistics
Flow Exporter TAC-EXPORT:
Packet send statistics (last cleared 00:08:38 ago):
  Successfully sent: 2 (24 bytes)

Client send statistics:
Client: Flow Monitor TAC-MONITOR-IN
  Records added: 0
  Bytes added: 12
  - sent: 12

Client: Flow Monitor TAC-MONITOR-OUT
  Records added: 0
  Bytes added: 12
  - sent: 12
```

## یساسأالا ماظنلا دامتعا نم ققحتلا

### NFL میسقت لودج - NetFlow ئیئەت

- لباقم لاخدا (هاتل لک اعاطق 16 لالغ نم ةفلتخم تازیمل NetFlow ماسقا ئیئەت متت جارخالا).
- متی یذلاو، میملال کنبال عیزوت ىل NetFlow میسقت لودج نیوکت میسقت متی جورخالاو لوخدلا قفدت کونب ىل ایضاً همیسقت

### ئیسیرلا لوقحلا

- ماسقأالا ددع
- مسقلا نیكمت ةلاح
- مسقلا دح
- یلاحلا مسقلا مادختسا

show platform software fed switch active|standby|member| fnf sw-table size asic <asic number> shadow 0

اهئاشن دن عةيساسألا ةاونللاو لوجملاب ةصاخ اهؤاشن متي يتلا تاقفدتلا :ةظحالم  
 متي يذلا ASIC مقرر طبر متي .كلذل اقفو (خلل ،يطايتح ،طشن) لوجمل مقرر ديدحت بجي  
**show platform software fed switch** مدختسأ ،ةلباقملا ةهجاوولاب هلاخدا  
 ،لظلا رايخل .ةهجاوول عم قفاوتي يذلا ASIC ديدحتل **active|standby|member ifm mappings**  
 "0" امئاد مدختسأ .

```
Switch#show platform software fed switch active fnf sw-table-sizes ASIC 0 shadow 0
```

```
-----  

Global Bank Allocation  

-----
```

```
Ingress Banks : Bank 0 Bank 1  

Egress Banks  : Bank 2 Bank 3  

-----
```

```
Global flow table Info                                     <--- Provides the number of entries  

used per direction  

INGRESS      usedBankEntry          0  usedOvfTcamEntry      0  

EGRESS      usedBankEntry          0  usedOvfTcamEntry      0  

-----
```

```
Flows Statistics
```

```
INGRESS      TotalSeen=0 MaxEntries=0 MaxOverflow=0  

EGRESS      TotalSeen=0 MaxEntries=0 MaxOverflow=0  

-----
```

```
-----  

Partition Table  

-----
```

##	Dir	Limit	CurrFlowCount	OverFlowCount	MonitoringEnabled	
0	ING	0	0	0	0	
<b>1</b>	<b>ING</b>	<b>16640</b>	<b>0</b>	<b>0</b>	<b>1</b>	<-- Current flow count in hardware
2	ING	0	0	0	0	
3	ING	16640	0	0	0	
4	ING	0	0	0	0	
5	ING	8192	0	0	1	
6	ING	0	0	0	0	
7	ING	0	0	0	0	
8	ING	0	0	0	0	
9	ING	0	0	0	0	
10	ING	0	0	0	0	
11	ING	0	0	0	0	
12	ING	0	0	0	0	
13	ING	0	0	0	0	
14	ING	0	0	0	0	
15	ING	0	0	0	0	
0	EGR	0	0	0	0	
<b>1</b>	<b>EGR</b>	<b>16640</b>	<b>0</b>	<b>0</b>	<b>1</b>	<-- Current flow count in hardware
2	EGR	0	0	0	0	
3	EGR	16640	0	0	0	
4	EGR	0	0	0	0	
5	EGR	8192	0	0	1	
6	EGR	0	0	0	0	
7	EGR	0	0	0	0	
8	EGR	0	0	0	0	
9	EGR	0	0	0	0	
10	EGR	0	0	0	0	
11	EGR	0	0	0	0	
12	EGR	0	0	0	0	
13	EGR	0	0	0	0	
14	EGR	0	0	0	0	
15	EGR	0	0	0	0	



## ق ف د ت ل ا ة ب ق ا ر م

ي ل ي ا م ق ف د ت ل ا ة ب ق ا ر م ن ي و ك ت ن م ص ت ي

1. ل خ ا د ل ا خ د ا ء ا ش ن ا ه ن ع ج ت ن ي ي ذ ل ا و ، NetFlow ل ا ل (ACL) ل و ص و ل ا ي ف م ك ح ت ل ا ة م ئ ا ق ن ي و ك ت .  
ACL TCAM ل و د ج

ن م ACL TCAM ل ا خ د ا ن و ك ت ي

- ق ب ا ط م ل ا ح ي ت ا ف م ن ع ث ح ب ل ا
  - ي ل ي ا م ن م ص ت ت ي ت ل ل ا و ، NetFlow ن ع ث ح ب ل ل ة م د خ ت س م ل ا ج ئ ا ت ن ل ا ت ا م ل م ع  
NetFlow ف ر ع م ف ي ر ع ت ل ا ف ل م ف ر ع م
2. و NflLookupTable ي ف ل ا خ د ا ء ا ش ن ا ه ن ع ج ت ن ي ي ذ ل ا و ، ق ف د ت ل ا ع ا ن ق ن ي و ك ت .  
NflFlowMaskTable.

- NetFlow ل ا ل (ACL) ل و ص و ل ا ي ف م ك ح ت ل ا ة م ئ ا ق ج ئ ا ت ن ت ا م ل م ع ة ط س ا و ب ه ت س ر ه ف ت م ت  
NetFlow ن ع ث ح ب ل ل ق ف د ت ل ا ع ا ن ق ي ل ع ر و ث ع ل ل

## ق ف د ت ل ا ة ب ق ا ر م (ACL) NetFlow ل و ص و ل ا ي ف م ك ح ت ل ا ة م ئ ا ق

show platform hardware fed switch active fwd-asic resource tcam table nfl\_acl asic <asic number>  
ر م ا ل ا ل ي غ ش ت ب م ق NetFlow ل (ACL) ل و ص و ل ا ي ف م ك ح ت ل ا ة م ئ ا ق ن ي و ك ت ض ر ع ل

ل ا خ د ا ل ا ء ا ش ن ا م ت ي س ، ذ ف ن م ل ل (PACL) ل و ص و ل ا ي ف م ك ح ت ة م ئ ا ق ك ا ن ه ت ن ا ك ا ذ ا : ح ي م ل ت  
ه ج و م ل ل ل و ص و ل ا ي ف م ك ح ت ل ا ة م ئ ا ق ة ل ا ح ي ف . ي ل ع ه ة ج ا و ل ا ن ي ي ع ت م ت ي ث ي ح ASIC ي ل ع  
(ة ص ا خ ل ل ل و ص و ل ا ي ف م ك ح ت ل ا م ئ ا و ق) ASIC ع ي م ج ي ل ع ا د و ج و م ل ا خ د ا ل ا ن و ك ي ، (RACL).

- م ق ، ف ي ص و ت ل ا ف ر ع م ب ا س ح ل . ت ب 4 ا ت م ي ق ا م ه و ، NFCMD0 و NFCMD1 ك ا ن ه ، ج ا ر خ ا ل ا ا ذ ه ي ف  
ة . ي ئ ا ن ث ي ل ل ه ل ي و ح ت د ن ع . 2 و ه NFCMD1 ، 1 و ه NFCMD0 ن و ك ي ، ج ا ر خ ا ل ا ا ذ ه ي ف
- ي ل و ا ل ا ت ب ت ا د ح و 4 ل ا ن ا ف ، ة م ج م ل ا ت ب ت ا د ح و 8 ل ا ن م ص ه د ع ب ا م و cisco IOS-XE 16.12 ي ف  
ل ا ث م ل ا ي ف ك ل ذ ل . ن ك م م ث ح ب ل ل ا ن ا ي ل ا ر ي ش ت ت ب ت ا د ح و 7 ل ا و ، ف ي ر ع ت ل ا ف ل م ف ر ع م ي ه  
00010010 ، 1 و ه ف ي ر ع ت ل ا ف ل م ف ر ع م ، 00010010
- ت ب ت ا د ح و 8 ل ا ن م ص ، ة م ج م ر ب ل ا ت ا م ي ل ع ت ل ل ن م م د ق ا ل ا ت ا ر ا د ص ا ل ا و Cisco IOS XE 16.11 ي ف  
ع ب ا س ل ل ا ت ب ل ا ر ي ش ي ا م ن ي ب ، ف ي ر ع ت ل ا ف ل م ف ر ع م ي ه 6 ي ل و ا ل ا ت ب ت ا د ح و ن و ك ت ، ة م ج م ل ل  
4 و ه ف ي ر ع ت ل ا ف ل م ف ر ع م ، 00010010 ، ل ا ث م ل ا ا ذ ه ي ف ك ل ذ ل . ث ح ب ل ل ن ي ك م ت ي ل ل

```
Switch#show platform hardware fed switch active fwd-asic resource tcam table nfl_acl asic 0
Printing entries for region INGRESS_NFL_ACL_CONTROL (308) type 6 asic 0
=====
Printing entries for region INGRESS_NFL_ACL_GACL (309) type 6 asic 0
=====
Printing entries for region INGRESS_NFL_ACL_PACL (310) type 6 asic 0
=====
TAQ-2 Index-32 (A:0,C:0) Valid StartF-1 StartA-1 SkipF-0 SkipA-0
Input IPv4 NFL PACL
```

Labels Port Vlan L3If Group

M: 00ff 0000 0000 0000  
V: 0001 0000 0000 0000

vcuResults l3Len l3Pro l3Tos SrcAddr DstAddr mtrid vrfid SH  
M: 00000000 0000 00 00 00000000 00000000 00 0000 0000  
V: 00000000 0000 00 00 00000000 00000000 00 0000 0000

RMAC RA MEn IPOPT MF NFF DF SO DPT TM DSEn l3m  
M: 0 0 0 0 0 0 0 0 0 0 0 0  
V: 0 0 0 0 0 0 0 0 0 0 0 0

SrcPort DstPortIITypeCode TCPFlags TTL ISBM QosLabel ReQOS S\_P2P D\_P2P  
M: 0000 0000 00 00 0000 00 0 0 0  
V: 0000 0000 00 00 0000 00 0 0 0

SgEn SgLabel AuthBehaviorTag l2srcMiss l2dstMiss ipTtl SgaclDeny  
M: 0 000000 0 0 0 0 0  
V: 0 000000 0 0 0 0 0

**NFCMD0 NFCMD1 SMPLR LKP1 LKP2 PID QOSPRI MQLBL MPLPRO LUT0PRI CPUCOPY**  
**1 2 0 1 0 0 0 0 0 0x0000f 0**

Start/Skip Word: 0x00000003  
Start Feature, Terminate

-----  
Printing entries for region INGRESS\_NFL\_ACL\_VACL (311) type 6 asic 0  
=====  
Printing entries for region INGRESS\_NFL\_ACL\_RACL (312) type 6 asic 0  
=====  
Printing entries for region INGRESS\_NFL\_ACL\_SSID (313) type 6 asic 0  
=====  
Printing entries for region INGRESS\_NFL\_CATCHALL (314) type 6 asic 0  
=====  
TAQ-2 Index-224 (A:0,C:0) Valid StartF-1 StartA-1 SkipF-0 SkipA-0  
Input IPv4 NFL RACL

Labels Port Vlan L3If Group  
M: 0000 0000 0000 0000  
V: 0000 0000 0000 0000

vcuResults l3Len l3Pro l3Tos SrcAddr DstAddr mtrid vrfid SH  
M: 00000000 0000 00 00 00000000 00000000 00 0000 0000  
V: 00000000 0000 00 00 00000000 00000000 00 0000 0000

RMAC RA MEn IPOPT MF NFF DF SO DPT TM DSEn l3m  
M: 0 0 0 0 0 0 0 0 0 0 0 0  
V: 0 0 0 0 0 0 0 0 0 0 0 0

SrcPort DstPortIITypeCode TCPFlags TTL ISBM QosLabel ReQOS S\_P2P D\_P2P  
M: 0000 0000 00 00 0000 00 0 0 0  
V: 0000 0000 00 00 0000 00 0 0 0

SgEn SgLabel AuthBehaviorTag l2srcMiss l2dstMiss ipTtl SgaclDeny  
M: 0 000000 0 0 0 0 0  
V: 0 000000 0 0 0 0 0

**NFCMD0 NFCMD1 SMPLR LKP1 LKP2 PID QOSPRI MQLBL MPLPRO LUT0PRI CPUCOPY**  
**0 0 0 0 0 0 0 0 0 0x00000 0**

Start/Skip Word: 0x00000003  
Start Feature, Terminate

-----  
TAQ-2 Index-225 (A:0,C:0) Valid StartF-0 StartA-0 SkipF-0 SkipA-0  
Input IPv4 NFL PACL

Labels Port Vlan L3If Group  
M: 0000 0000 0000 0000  
V: 0000 0000 0000 0000

vcuResults l3Len l3Pro l3Tos SrcAddr DstAddr mtrid vrfid SH  
M: 00000000 0000 00 00 00000000 00000000 00 0000 0000  
V: 00000000 0000 00 00 00000000 00000000 00 0000 0000

RMAC RA MEn IPOPT MF NFF DF SO DPT TM DSEn l3m  
M: 0 0 0 0 0 0 0 0 0 0 0 0  
V: 0 0 0 0 0 0 0 0 0 0 0 0

SrcPort DstPortIITypeCode TCPFlags TTL ISBM QosLabel ReQOS S\_P2P D\_P2P  
M: 0000 0000 00 00 0000 00 0 0 0  
V: 0000 0000 00 00 0000 00 0 0 0

SgEn SgLabel AuthBehaviorTag l2srcMiss l2dstMiss ipTtl SgaclDeny  
M: 0 000000 0 0 0 0  
V: 0 000000 0 0 0 0

NFCMD0 NFCMD1 SMPLR LKP1 LKP2 PID QOSPRI MQLBL MPLPRO LUT0PRI CPUCOPY  
0 0 0 0 0 0 0 0 0 0 0 0x00000 0

Start/Skip Word: 0x00000000

No Start, Terminate

-----  
TAQ-2 Index-226 (A:0,C:0) Valid StartF-0 StartA-0 SkipF-0 SkipA-0  
Input IPv6 NFL PACL

Labels Port Vlan L3If Group  
Mask 0x0000 0x0000 0x0000 0x0000  
Value 0x0000 0x0000 0x0000 0x0000

vcuResult dstAddr0 dstAddr1 dstAddr2 dstAddr3 srcAddr0  
00000000 00000000 00000000 00000000 00000000 00000000  
00000000 00000000 00000000 00000000 00000000 00000000

srcAddr1 srcAddr2 srcAddr3 TC HL l3Len fLabel vrfId toUs  
00000000 00000000 00000000 00 00 0000 00000 000 0  
00000000 00000000 00000000 00 00 0000 00000 000 0

l3Pro mtrId AE FE RE HE MF NFF SO IPOPT RA MEn RMAC DPT TMP l3m  
00 00 0 0 0 0 0 0 0 0 0 0 0 0 0  
00 00 0 0 0 0 0 0 0 0 0 0 0 0 0

DSE srcPort dstPortIITypeCode tcpFlags IIPresent cZId dstZId  
0 0000 0000 00 00 00 00  
0 0000 0000 00 00 00 00

v6RT AH ESP mREn ReQOS QosLabel PRole VRole AuthBehaviorTag  
M: 0 0 0 0 0 00 0 0 0  
V: 0 0 0 0 0 00 0 0 0

SgEn SgLabel  
M: 0 000000  
V: 0 000000

NFCMD0 NFCMD1 SMPLR LKP1 LKP2 PID QOSPRI MQLBL MPLPRO LUT0PRI CPUCOPY  
0 0 0 0 0 0 0 0 0 0 0 0x00000 0

Start/Skip Word: 0x00000000

No Start, Terminate

-----

TAQ-2 Index-228 (A:0,C:0) Valid StartF-0 StartA-0 SkipF-0 SkipA-0  
conversion to string vmr l2p not supported

-----  
TAQ-2 Index-230 (A:0,C:0) Valid StartF-0 StartA-0 SkipF-0 SkipA-0  
Input MAC NFL PAFL

Labels	Port	Vlan	L3If	Group
M:	0000	0000	0000	0000
V:	0000	0000	0000	0000

	arpSrcHwAddr	arpDestHwAddr	arpSrcIpAddr	arpTargetIp	arpOperation
M:	000000000000	000000000000	00000000	00000000	0000
V:	000000000000	000000000000	00000000	00000000	0000

	TRUST	SNOOP	SVALID	DVALID
M:	0	0	0	0
V:	0	0	0	0

	arpHardwareLength	arpHardwareType	arpProtocolLength	arpProtocolType
M:	00000000	00000000	00000000	00000000
V:	00000000	00000000	00000000	00000000

	VlanId	l2Encap	l2Protocol	cosCFI	srcMAC	dstMAC	ISBM	QosLabel
M:	000	0	0000	0	000000000000	000000000000	00	00
V:	000	0	0000	0	000000000000	000000000000	00	00

	ReQOS	isSnap	isLLC	AuthBehaviorTag
M:	0	0	0	0
V:	0	0	0	0

NFCMD0	NFCMD1	SMPLR	LKP1	LKP2	PID	QOSPRI	MQLBL	MPLPRO	LUT0PRI	CPUCOPY
0	0	0	0	0	0	0	0	0	0x00000	0

Start/Skip Word: 0x00000000  
No Start, Terminate

## ق ف د ت ال ع ان ق

د د ع ی ل ع ر و ث ع ال ن ك م ی ام ك . ز اه ج ل ا ی ف ق ف د ت ال ع ان ق ت ی ب ث ت ض ر ع ل 1 ا س ی ك <number> ا ن ی ق ل ی غ ش ت ب م ق  
ا ن ه ح ی ت ا ف م ل ل و ق ح

Switch#show platform software fed switch active fnf fmask-entry ASIC 1 entry 1

-----  
mask0\_valid : 1  
Mask hdl0 : 1  
Profile ID : 0  
Feature 0 : 148  
Fmask0 RefCnt: 1  
Mask M1 :  
[511:256] => :00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000  
[255:000] => :FFFFFFFF 00000000 FFFFFFFF 03FF0000 00000000 00FF0000 00000000 C00000FF  
Mask M2 :

Key Map :

Source	Field-Id	Size	NumPFields	Pfields
002	090	04	01	(0 1 1 1)
002	091	04	01	(0 1 1 0)
002	000	01	01	(0 1 0 7)
000	056	08	01	(0 0 2 4)
001	011	11	04	(0 0 0 1) (0 0 0 0) (0 1 0 6) (0 0 2 0)
000	067	32	01	(0 1 12 0)
000	068	32	01	(0 1 12 2)

## ينمزلل عباطلال لي محت اءاغل تانايبو قفدتل تالاح

ق show platform software fed switch active fnf flow-record asic <asic number> start-index <index number> num-flow <number of flow> كلك و netFlow تايئاصح اضرعل  
ة ينمزلل عباطلال

```
Switch#show platform software fed switch active fnf flow-record asic 1 start-index 1 num-flows 1
1 flows starting at 1 for asic 1:-----
Idx 996 :
{90, ALR_INGRESS_NET_FLOW_ACL_LOOKUP_TYPE1 = 0x01}
{91, ALR_INGRESS_NET_FLOW_ACL_LOOKUP_TYPE2 = 0x01}
{0, ALR_INGRESS_NFL_SPECIAL1 = 0x00}
{56, PHF_INGRESS_L3_PROTOCOL = 0x11}
{11 PAD-UNK = 0x0000}
{67, PHF_INGRESS_IPV4_DEST_ADDRESS = 0xc0a86464}
{68, PHF_INGRESS_IPV4_SRC_ADDRESS = 0xc0a8c864}
FirstSeen = 0x4b2f, LastSeen = 0x4c59, sysUptime = 0x4c9d
PKT Count = 0x00000000102d5df, L2ByteCount = 0x00000000ca371638
```

```
Switch#show platform software fed switch active fnf flow-record asic 1 start-index 1 num-flows 1
1 flows starting at 1 for asic 1:-----
Idx 996 :
{90, ALR_INGRESS_NET_FLOW_ACL_LOOKUP_TYPE1 = 0x01}
{91, ALR_INGRESS_NET_FLOW_ACL_LOOKUP_TYPE2 = 0x01}
{0, ALR_INGRESS_NFL_SPECIAL1 = 0x00}
{56, PHF_INGRESS_L3_PROTOCOL = 0x11}
{11 PAD-UNK = 0x0000}
{67, PHF_INGRESS_IPV4_DEST_ADDRESS = 0xc0a86464}
{68, PHF_INGRESS_IPV4_SRC_ADDRESS = 0xc0a8c864}
FirstSeen = 0x4b2f, LastSeen = 0x4c5b, sysUptime = 0x4c9f
PKT Count = 0x000000001050682, L2ByteCount = 0x00000000cbed1590
```

## اهي ف مكحتل او تاقيبطتلا ةيؤر ةينام (AVC)

### ةساس تامولعم

- ةزيم نم ةدافتسالال يلعل لمعي لحيه (AVC) اهي ف مكحتل او تاقيبطتلا ةيؤر ةينام اءاغل ةرادال او اءاغل او NetFlow v9 و (NBAR2) 2 رادصال ةكبشلال ال ةدنتسمل فرعتل قيمي علل صرقل ربق تاقيبطتلا فينصت في ةدعاسملل (Cisco Prime) ريراقتل دادع او مزجلل (DPI).
- تالوحملا تاسدكم و تالوحملا ةيكلسلال لوصولل ذفانم يلعل AVC نيوكت نكمي ةلقتسمل.
- تاقيبطتلا ديحتل Cisco نم ةيكلسلال مكحتل تادحو يلعل AVC مادختس نكمي امك سيسي اقم عمج ه نكمي امك. ةنيعم DSCP ةمي قيب اهلعل ةمالع عضو مث DPI ال اءانتسا تاقيبطتلا شيح نم يدرتلا قاطنل اضرعل مادختس لثم ةفلتخم ةيكلسلال اءاغل

ءال مع ل او

## ر و ط ت ل او ء اء ا ل ا

ءء و م اءء ت س ا ب (CPS) ء ء ن اء ل ا ف ل ا ص ت ا 500 ء ء ل ا ع م ل وء م ل ا ف و ض ع ل ل ء ن ء م ء : ء اء ا ل ا ء م ء ء ن ا م ء م ء ء ال ، ل ء ء م ل ا اء ء ء ن ء ت س ا ب و . 50% ن م ل ق ا ء ب س ن ب (CPU) ء ء ز ء ر م ل ا ء ء ل ا ع م ل ا AVC.

ء ف ن م 24 ل ل ء ه اء ء ا ل ا ء ء ء ن اء ل ا ت ا ق ف ء ت ل ا ن م 5000 ء ل ل ا ص ء ا م ء ء ل ا ع م ء ل ع ء ر ء ق ل ا : ق ا ط ن ل ا (ل و ص و ء ف ن م ل ل ء ق ف ء ت 200 ن م ب ر ق ء ا م) ل و ص و

## ء ء ء ل س ل ل AVC ء و ء ق

- س ف ن ف ا ع م (ETA) ء ر ف ش م ل ا ت ا ن ا ء ب ل ا ر و ر م ء ء ر ء ت ا ل ء ل ء ت و AVC ن ء و ء ت ن ء م ء ال ا ه س ف ن ء ه ء ا و ل ا ء ل ع ت ق و ل ا
- (TCP/UDP) ء ء اء ا ل ا ء ب ل ل IPv4 ر و ر م ء ء ر ء ل ط ق ف م و ع ء م ء م ز ء ل ا ف ء ن ص ت
- ء ء ء م ل ا ء ف ا ن م ل ا ء ل ع ط ق ف ء م ت ع م NBAR ء ل ل ء ن ت س م ل ا ء م ء ء ل ا ء ء و ء ه ن ن ء و ء ت ه ء و ت ء ف ا ن م و 2 ء ق ب ط ل ا ن م ل ا ص ت ا ل ا ط و ط ء و ل و ص و ل ا ء ف ا ن م ء ل ء ن م ء ت ء و . ء ء ء ل س ل ل 3. ء ق ب ط ل ا ن م
- ت ا ه ء ا و ء ا ء ف ن م ل ا ء ا ن ق ء ا ض ع ا ء ل ع م و ع ء م ر ء ء NBAR ء ل ل ء ن ت س م ل ا ء م ء ء ل ا ء ء و ء ه ن ن ء و ء ت ء ء ء ر ف ل ا ت ا ه ء ا و ل ا و ا (SVIs) ء ء ر ه ا ط ل ل ا ت ا ل و ء م ل ا
- ء م ء ء ل ا ء ء و ء ت ا ء ا ر ء ا ط ق ف م ع ء ت ، (ء ق ب ا ط م ل ا ل و ء و ت و ر ب) NBAR2 ء ل ل ء ن ت س م ل ا ت ا ف ن ص م ل ا ء ه ن ل ل ء ء ء ت و ت ا م ا ل ع ل ا ع ض و ب ء ص اء ل ا
- ء ء ت ا س ا ء س ل ل ا ع ء م ء ف ا ف ل ت ء ء م ا ل و ء و ت و ر ب 255 ء ل ع "ء ق ب ا ط م ل ا ل و ء و ت و ر ب" ر ص ت ق ء ء (ت ب 8 ء ز ه ء ا ل ا

ب س ا ن م ل ا AVC ن ء و ء ت ل ء ل ء ع ء ا ر ، ء و ء ق ل ا ع ء م ء ل ء ل م ا ش ء م ء ا ق ت س ء ل ه ء ه : ء ط ء ا ل م ز م ر ل ا ر ا ء ص ا و ء ء ء ل ء س ا س ا ل ا م ا ط ن ل ل

## ء ء ب ش ل ل ل ء ط ء ء ت ل ل م س ر ل ا



- قفدت لكل سيجل) ةمجملا رورملا ةكرح ىلع تاءارجإل ذيفنت متي
  - ةقباطمو ةئف ةطيرخ عاشنإ لالخنم قيبطتلال ىلإ ةدنتسملا ةمدخلال ةدوج قيقحت متي .  
ةسايس ةطيرخ عاشنإ مث ، لوكوتورب
  - ةهجاوب قيبطتلال ىلإ ةدنتسملا ةمدخلال ةدوج ةسايس قافرا متي .
- ىلإ ةدنتسملا (QoS) ةمدخلال ةدوج نيوكت ، لاثملا لىبس ىلع ، جارجإل ي فحضم وه امك قيبطتلال:

```
Switch(config)#class-map WEBEX
Switch(config-cmap)#match protocol webex-media
Switch(config)#end
```

```
Switch(config)#policy-map WEBEX
Switch(config-pmap)#class WEBEX
Switch(config-pmap-c)#set dscp af41
Switch(config)#end
```

```
Switch(config)#interface fi4/0/5
Switch(config-if)#service-policy input WEBEX
Switch(config)#end
```

```
Switch#show run int fi4/0/5
Building configuration...
```

```
Current configuration : 98 bytes
!
interface FiveGigabitEthernet4/0/5
service-policy input WEBEX
ip nbar protocol-discovery
end
```

## تاقيبطتلال ىلإ ةدنتسملا Flexible NetFlow ةئقنت

قفدت تالچس : اقبسم ةددحملال قفدتل تالچس نم نيعون يكلسل AVC FNF م عدي  
هجاتالاب ةديجل تانايبلال قفدت تالچسو هجاتالاب ةئانث ةميدقل تانايبلال

مداخلال/لمعلال قيبطت تايئاصحإ هجاتالاب ةئانث قفدتل تالچس عبتت

هجاتالاب ةئانث قفدت لچس نيوكت لثم ، جارجإل ي فحضم وه امك

```
Switch(config)#flow record BIDIR-1
Switch(config-flow-record)#match ipv4 version
Switch(config-flow-record)#match ipv4 protocol
Switch(config-flow-record)#match application name
Switch(config-flow-record)#match connection client ipv4 address
Switch(config-flow-record)#match connection server ipv4 address
Switch(config-flow-record)#match connection server transport port
Switch(config-flow-record)#match flow observation point
Switch(config-flow-record)#collect flow direction
Switch(config-flow-record)#collect connection initiator
Switch(config-flow-record)#collect connection new-connections
Switch(config-flow-record)#collect connection client counter packets long
Switch(config-flow-record)#collect connection client counter bytes network long
Switch(config-flow-record)#collect connection server counter packets long
Switch(config-flow-record)#collect connection server counter bytes network long
Switch(config-flow-record)#collect timestamp absolute first
Switch(config-flow-record)#collect timestamp absolute last
Switch(config-flow-record)#end
```



```
Switch#show flow record BIDIR-1
flow record BIDIR-1:
Description: User defined
No. of users: 0
Total field space: 78 bytes
Fields:
match ipv4 version
match ipv4 protocol
match application name
match connection client ipv4 address
match connection server ipv4 address
match connection server transport port
match flow observation point
collect flow direction
collect timestamp absolute first
collect timestamp absolute last
collect connection initiator
collect connection new-connections
collect connection server counter packets long
collect connection client counter packets long
collect connection server counter bytes network long
collect connection client counter bytes network long
جارجال/الخالل قيبطت تالاح يه هاجتال تالجال
```

جارجال او لخالل هاجتال تالجال نيوكتلا ةلثمأ، جارجال ي ف حضوم وه امك

**match interface** رمأل ددحي. لخالل ةهجال قباطت **match interface input** رمأل ددحي: **ةظحال** AVC. م عدل يمازلل **match application name** رمأل. جارجال ةهجال قباطت **match interface output**.

```
Switch(config)#flow record APP-IN
Switch(config-flow-record)#match ipv4 version
Switch(config-flow-record)#match ipv4 protocol
Switch(config-flow-record)#match ipv4 source address
Switch(config-flow-record)#match ipv4 destination address
Switch(config-flow-record)#match transport source-port
Switch(config-flow-record)#match transport destination-port
Switch(config-flow-record)#match interface input
Switch(config-flow-record)#match application name
Switch(config-flow-record)#collect interface output
Switch(config-flow-record)#collect counter bytes long
Switch(config-flow-record)#collect counter packets long
Switch(config-flow-record)#collect timestamp absolute first
Switch(config-flow-record)#collect timestamp absolute last
Switch(config-flow-record)#end
```

```
Switch#show flow record APP-IN
flow record APP-IN:
Description: User defined
No. of users: 0
Total field space: 58 bytes
Fields:
match ipv4 version
match ipv4 protocol
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
match interface input
match application name
collect interface output
```

```
collect counter bytes long
collect counter packets long
collect timestamp absolute first
collect timestamp absolute last
```

```
Switch(config)#flow record APP-OUT
Switch(config-flow-record)#match ipv4 version
Switch(config-flow-record)#match ipv4 protocol
Switch(config-flow-record)#match ipv4 source address
Switch(config-flow-record)#match ipv4 destination address
Switch(config-flow-record)#match transport source-port
Switch(config-flow-record)#match transport destination-port
Switch(config-flow-record)#match interface output
Switch(config-flow-record)#match application name
Switch(config-flow-record)#collect interface input
Switch(config-flow-record)#collect counter bytes long
Switch(config-flow-record)#collect counter packets long
Switch(config-flow-record)#collect timestamp absolute first
Switch(config-flow-record)#collect timestamp absolute last
Switch(config-flow-record)#end
```

```
Switch#show flow record APP-OUT
flow record APP-OUT:
Description: User defined
No. of users: 0
Total field space: 58 bytes
Fields:
match ipv4 version
match ipv4 protocol
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
match interface output
match application name
collect interface input
collect counter bytes long
collect counter packets long
collect timestamp absolute first
collect timestamp absolute last
```

## ق ف د ت ل ا ر د ص م

ر ي د ص ت ل ا ت ا م ل ع م د ي د ح ت ل ق ف د ت ر د ص م ء ا ش ن |

ق ف د ت ل ا ر د ص م ن ي و ك ت ل ا ث م ، ج ا ر خ ا ل ا ي ف ح ص و م و ه ا م ك :

```
Switch(config)#flow exporter AVC
Switch(config-flow-exporter)#destination 192.168.69.2
Switch(config-flow-exporter)#source vlan69
Switch(config-flow-exporter)#end
```

```
Switch#show run flow exporter AVC
Current configuration:
!
flow exporter AVC
destination 192.168.69.2
source Vlan69
!
```

## ق ف د ت ل ا ة ب ق ا ر م

ق ف د ت ل ج س ب ا ه ن ا ر ق ا ل ق ف د ت ة ب ق ا ر م ء ا ش ن ا

ق ف د ت ل ا ة ب ق ا ر م ن ي و ك ت ل ا ث م ، ج ا ر خ ا ل ا ي ف ح ض و م و ه ا م ك

```
Switch(config)#flow monitor AVC-MONITOR
Switch(config-flow-monitor)#record APP-OUT
Switch(config-flow-monitor)#exporter AVC
Switch(config-flow-monitor)#end
```

```
Switch#show run flow monitor AVC-MONITOR
Current configuration:
!
flow monitor AVC-MONITOR
exporter AVC
record APP-OUT
```

## ة ه ج ا و ب ق ف د ت ل ا ة ب ق ا ر م ط ب ر

ا ق ب س م ة ف ر ع م ة ف ل ت خ م ت ا ل ج س ب ن ي ت ف ل ت خ م AVC ي ت ش ا ش ا ل ا ل ص ي ا م ق ا ف ر ا ك ن ك م ي  
ت ق و ل ا س ف ن ي ف ة ه ج ا و ب .

ق ف د ت ل ا ة ب ق ا ر م ن ي و ك ت ل ا ث م ، ج ا ر خ ا ل ا ي ف ح ض و م و ه ا م ك

```
Switch(config)#interface fi4/0/5
Switch(config-if)#ip flow monitor AVC-MONITOR out
Switch(config-if)#end
```

```
Switch#show run interface fi4/0/5
Building configuration...
Current configuration : 134 bytes
!
interface FiveGigabitEthernet4/0/5
ip flow monitor AVC-MONITOR output
service-policy input WEBEX
ip nbar protocol-discovery
end
```

## NBAR2

ل ص ت م ل ا ر ي غ ي ك ي م ا ن ي د ل ا NBAR2 ل و ك و ت و ر ب ة م ز ح ة ي ق ر ت

ل ا د ب ت س ا ن و د ا م ز ا ه ج ا ل ع NBAR2 ل و ك و ت و ر ب م ع د ث ي د ح ت ب م و ق ت ج م ا ر ب م ز ح ي ه ل و ك و ت و ر ب ل ا م ز ح  
ي ت ل ا ت ا ق ي ب ط ت ل ا ل و ح ت ا م و ل ع م ا ل ع ل و ك و ت و ر ب ل ا ة م ز ح ي و ت ح ت . ز ا ه ج ا ل ا ل ع Cisco ج م ا ن ر ب  
ن م ض ت ت ، ق ي ب ط ت ل ل ك ل ة ب س ن ل ا ب . ا ع م ا ه د ش ح و ا ه ع ي م ج ت م ت ي ي ت ل ا و ا ي م س ر NBAR2 ا ه م ع د ت  
ن م ر ا د ص ا ل ك ي و ت ح ي . ق ي ب ط ت ل ا ت ا م س و ت ا ق ي ب ط ت ل ا ت ا ع ي ق و ت ل و ح ت ا م و ل ع م ل و ك و ت و ر ب ل ا ة م ز ح  
ر ا د ص ا ل ا ذ ه م ة ج م د م ة ج م د م ة ج م د م ل و ك و ت و ر ب ة م ز ح ا ل ع ج م ا ر ب ل ا

- ة م د خ ل ا و ا ر و ر م ل ا ة ك ر ح ي ف ع ا ط ق ن ا ي ا ن و د ل و ك و ت و ر ب ل ا ة م ز ح ث ي د ح ت ل ق ي ر ط NBAR2 ر ف و ي  
(ة ز ه ا ل ا) ز ا ه ج ا ل ا ل ع ج م ا ن ر ب ل ا ة ر و ص ل ي د ع ت ا ل ا ة ج ا ل ا ن و د و
- ا ذ ه URL ن ا و ن ع ن م Cisco ج م ا ر ب ز ك ر م ا ل ع ل ي ز ن ت ل ل NBAR2 ل و ك و ت و ر ب م ز ح ر ف و ت ت  
[https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos\\_nbar/prot\\_lib/config\\_library/nbar-prot-pack-library.html](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_nbar/prot_lib/config_library/nbar-prot-pack-library.html)

ل و ك و ت و ر ب ة م ز ح ة ي ق ر ت NBAR2

Flash ة ر ك ا ذ ا ل ل و ك و ت و ر ب ل ا ة م ز ح خ س ن ك ي ل ع ب ج ي ، ة د ي د ج ل و ك و ت و ر ب ة م ز ح ت ي ب ث ت ل ب ق

ip رمالا مدختسأ، ةديجالا لوكوتوربلا ةمزل ليحتل. تالوحملا عيجم يلع (ةتقؤملا ةركاذلا)  
nbar protocol-pack flash:<pack name>

NBAR2 ةيقرت ءارجال (تالوحملا) لوحملا ليحت ةداعإ يلا جاتحت ال

NBAR2 لوكوتورب ةمزل ليحت ةيفيكي نيوكت لثم، جارجالا يف حضوم وه امك

```
Switch(config)#ip nbar protocol-pack flash:newProtocolPack
```

يضارتفالا ip nbar protocol pack رمالا مدختسأ، ةجمدملا لوكوتوربلا ةمزل يلا ةدوعلل

ةجمدملا لوكوتوربلا ةمزل يلا ءوجرلا ةيفيكي نيوكت لثم، جارجالا يف حضوم وه امك

```
Switch(config)#default ip nbar protocol-pack
```

NBAR2 لوكوتورب ةمزل تامولعم ضرع

ةجمدملا رمالا مدختسأ لوكوتوربلا ةمزل تامولعم ضرع:

- show ip nbar version
- IP nbar لوكوتورب ةمزل ةطشنلا ليصافتلا

رمالالا هذه جارجالا لثم، جارجالا يف حضوم وه امك

```
Switch#show ip nbar version
```

```
NBAR software version: 37
```

```
NBAR minimum backward compatible version: 37
```

```
NBAR change ID: 293126
```

```
Loaded Protocol Pack(s):
```

```
Name: Advanced Protocol Pack
```

```
Version: 43.0
```

```
Publisher: Cisco Systems Inc.
```

```
NBAR Engine Version: 37
```

```
State: Active
```

```
Switch#show ip nbar protocol-pack active detail
```

```
Active Protocol Pack:
```

```
Name: Advanced Protocol Pack
```

```
Version: 43.0
```

```
Publisher: Cisco Systems Inc.
```

```
NBAR Engine Version: 37
```

```
State: Active
```

ةصصخملا NBAR2 تاقيبطت

معدت. ةصصخملا تاقيبطتلا فيرعتل ةصصخم تالوكوتورب مادختسإ NBAR2 معدت  
ايلا NBAR2 اهمعدت ال يتلا تاقيبطتلاو تالوكوتوربلا ةصصخملا تالوكوتوربلا

يولي ام كلذل لمشي نأ نكميو

- ةسسؤم يلع ددحم قيبطت
- ايفارغجالاب ةصاخ تاقيبطت

ip nbar رمالا لالخنم ايودي تاقيبطتلا صيصختل ةقيرط NBAR2 رفوي  
custom<myappname>.

## ةجمدملا تالوكوتوربلا ىلع ةصصخمل تاقىبطلتلا مدقت :ةظالم

قىبطلتلا صىصخت نم ةفلتخم عاونأ كانه

### ماعلا لوكوتوربلا صىصخت

- HTTP
- SSL
- DNS

مداخل مسا - ةددعتم تالوكوتوربلا ىلإ ادانتسا صىصختلا: بكم

### 4 ةقبطل/3 ةقبطل صىصخت

- IPv4 ناووع
- DSCP ميق
- TCP/UDP ذفانم
- ةهولوا وأ قفدتلا رصم هاجتا

ةلومحللا يف ةنعم تىاب ميق ىلإ ادانتسا صىصختلا: تىابللا ةحازا

### HTTP صىصخت

نم HTTP لوقح نم ةومجم ىلع HTTP صىصخت دامتعا نكمي

- HTTP طابترلا فيرعت فلم - طابترالا فيرعت فلم
- دروملا ىلع يوتحي يذلا لىلصألا مداخلل فيضملا مسا - فيضملا
- HTTP بولسا - ةقيرطالا
- هنم دروملا بلط ىلع لوصحللا مت ناووع - عجرملا
- دحوملا دراوملا عقوم دحوم راسم - url
- بلطلا لسري يذلا لىكولا ةطساوب مدختسملا جمانربلا - مدختسملا لىكولا
- HTTP رادصلا - رادصلا
- لقلل ربع HTTP - via

فرعمب "mydomain.com" HTTP فيضم مدختسي MYHTTP ىمسي صىصختلا قىبطلتلا لاثم 10. ددحلال

```
Switch(config)#ip nbar custom MYHTTP http host *mydomain.com id 10
```

### SSL صىصخت

رشم نم ةجرتسملا تامولعملالال خ نم ةرفشملا SSL رورم ةكرحل صىصختلا ءارج نكمي (CN). ءئاشلال مسالا وأ SSL (SNI) مداخ مسا

"mydomain.com" ديرفلا مسالا اب SSL مدختسي MYSSL ىمسي صىصختلا قىبطلتلا لاثم 11. ددحلال فرعمب

```
Switch(config)#ip nbar custom MYSSL ssl unique-name *mydomain.com id 11
```

### DNS صىصخت

متي. قيبطت DNS ةباجتسا طبر نكمي و، ةباجتسالا رورم ةكرحو DNS بلط NBAR2 صحفي ةقحلال مزحلل افاقفدل همادختسا واتقوم DNS ةباجتسا نم هعاجرا متي ذللا IP ناو نع نيزخت ددحمال قيبطتلا ك لذبة نرتقملا

صي صختل `NSDOMAIN-name` `id` `application-name` `customapplication-name` `nbar` رمألا مادختسا متي DNS. قيبطت دي دمتل `main-name` `domain-name` `customapplication-name` `nbar` رمألا مدختسا، قيبطت دي دمتل `Extendsexisting-application`.

فرعمب "mydomain.com" DNS لاجم مسا مدختسي MYDNS ميسي صصخم قيبطتلا لاثم 12 ددحمال

```
Switch(config)#ip nbar custom MYDNS dns domain-name *mydomain.com id 12
```

### بكرم صي صخت

يف رهظت يتللال تالاجملا عامسا لادانتسا افاقيبطتلا صي صختل ةقيرط NBAR2 رفوي DNS و SSL و HTTP.

DNS و SSL و HTTP لاجم مسا مدختسي MYDOMAIN ميسي صصخم قيبطتلا لاثم "mydomain.com" فرعمب 13 ددحمال

```
Switch(config)#ip nbar custom MYDOMAIN composite server-name *mydomain.com id 13
```

### صي صخت L3/L4

ةمزحلل لعل امئاد هتقباطم متي و مزحلال ةومجم لعل 4 ةقبطلا/3 ةقبطلا صي صخت دمتعي قفدتل نم لوالا

و IP 10.56.1.10 نيوانع قباطي ذللا CUSTOM ةصصخملا افاقيبطتلا ةقبطلا لاثم 10.56.1.11، TCP و DSCP EF فرعمب 14 ددحمال

```
Switch(config)#ip nbar custom LAYER4CUSTOM transport tcp id 14
Switch(config-custom)#ip address 10.56.1.10 10.56.1.11
Switch(config-custom)#dscp ef
Switch(config-custom)#end
```

### ةصصخملا افاقيبطتلا ةبقارم

ةجر دمل show رمألا مدختسي ةصصخملا افاقيبطتلا ةبقارم

ةصصخم Inc ةكرش | `show ip nbar protocol-id`

```
Switch#show ip nbar protocol-id | inc Custom
LAYER4CUSTOM          14          Custom
MYDNS                  12          Custom
MYDOMAIN               13          Custom
MYHTTP                 10          Custom
MYSSL                  11          Custom
```

`show ip nbar protocol-id CUSTOM_APP`

```
Switch#show ip nbar protocol-id MYSSL
Protocol Name          id          type
```

## AVC نم ققحتلا

لثام تاجرم ورم او مسقلا اذه رفوي، AVC فئاظو ةحص نم ققحتلل ةددعتم تاوطخ كانه.

show ip nbar control-plane رمالا ليغشت كنكمي، طشن NBAR نأ نم ققحتلل

ةيسيئرلا تالاجملا:

- حيحص ويراني س يف NBAR ةلاح طيشنت بجي
- حيحص ويراني س يف ةزهاج NBAR نيوكت ةلاح نوكت نأ بجي

```
Switch#show ip nbar control-plane
NGCP Status:
=====
```

```
graph sender info:
NBAR state is ACTIVATED
NBAR config send mode is ASYNC
NBAR config state is READY

NBAR update ID 3
NBAR batch ID ACK 3
NBAR last batch ID ACK clients 1 (ID: 4)
Active clients 1 (ID: 4)
NBAR max protocol ID ever 1935
NBAR Control-Plane Version: 37
```

<snip>

show platform software fed switch member wдавc function wдавc\_stile\_cp\_show\_info\_ui: رمالا مادختساب طشن تانايب يوتسم هي دل لوجملا يف وضع لك نأ نم ققحت

حيحص ويراني س يف TRUE نوكتي نأ بجي DP طيشنت مت له

```
Switch#show platform software fed switch active wдавc function wдавc_stile_cp_show_info_ui
```

```
Is DP activated : TRUE
MSG ID : 3
Maximum number of flows: 262144
Current number of graphs: 1
Requests queue state : WDAVC_STILE_REQ_QUEUE_STATE_UP
Number of requests in queue : 0
Max number of requests in queue (TBD): 1
Counters:
activate_msgs_rcvd : 1
graph_download_begin_msgs_rcvd : 3
stile_config_msgs_rcvd : 1584
graph_download_end_msgs_rcvd : 3
deactivate_msgs_rcvd : 0
intf_proto_disc_msgs_rcvd : 1
intf_attach_msgs_rcvd : 2
cfg_response_msgs_sent : 1593
num_of_handle_msg_from_fmanfp_events : 1594
num_of_handle_request_from_queue : 1594
num_of_handle_process_requests_events : 1594
```

وضع الاعداد لتسالا عضو اطنش لن لوجم ريفوت مت يذلا show platform software رمال مدختسا  
ةيساس الامل عمل ضرع wdavc قفدتسي:

```
Switch#show platform software fed switch active wдавc flows
```

```
CurrFlows=1, Watermark=1
```

```
IX |IP1 |IP2 |PORT1|PORT2|L3 |L4 |VRF |TIMEOUT|APP |TUPLE|FLOW |IS FIF |BYPASS|FINAL |#PKTS  
|BYPASS  
| | | |PROTO|PROTO|VLAN|SEC |NAME |TYPE |TYPE |SWAPPED | | | |PKT  
-----  
1 |192.168.100.2 |192.168.200.2 |68 |67 |1 |17 |0 |360 |unknown |Full |Real Flow|Yes |True |True  
|40 |40
```

ةيسيس رللا لوقحلا:

**CurrFlow:** AVC ةطساوب اهبقت متي يتلا ةطشنلا تاقفدتلا ددع حضوي

AVC ةطساوب ايخيرات اهبقت متي يتلا تاقفدتلا نم ددع ربكأ حضوي: **ةيسيس الامل ةم ال عمل**

ددحملل قيبطتلا لىل اذانتسا طاشنلا مدع ةلهم ءاهتنا: **ةلهملل ةيسيناثل**

ددحملل قيبطتلا: **قيبطتلا مسا**

ريشي. ةدراولا تانايب لل ةجيتن هؤاشن| مت اذه نأ لىل Real Flow ريشي: **قفدتلا عون**  
مادختسا متي. ةدراولا تانايب لل ةجيتنك قفدتلا اذءاشن| لىل قبسملل قفدتلا  
ةعقوتمل طئاسولا تاقفدتل ةقبسملل تاقفدتلا

تاقفدتلا امأ، ةلماك ةعومجم نع ةرابع ةيقي قحلا تاقفدتلا نوكت ام امئاد: **ةعومجم ال عون**  
ةموكحم فصن وأ ةلماك ةعومجم امأ يهف ةقباسلا

فيعرتل مزحلل نم ديزملا جم انربل بلطتي ال هنأ لىل ريشي، TRUE لىل عطبض مت اذا: **زواجت**  
قفدتلا اذه

قفدتلا اذهل ريغتي دعيل قيبطتلا نأ لىل ريشي هنإف، TRUE لىل عطبض مت اذا: **ةيسيناهن**

ةيسيناهنل فينصتلا لىل لوصولل ةبولطم تناك يتلا مزحلل ددع: **PKT زواجت**

قفدتلا اذهل جماربل لىل اهتبيثت مت يتلا مزحلل ددع مك: **#pkts**

show platform رمال مادختسا كنكمي، ةيلاحلا تاقفدتلا لوح ةيفاضا لىل صافات ضرع  
software fed switch active wдавc function wдавc\_ft\_show\_all\_flows\_seg\_ui

```
Switch#show platform software fed switch active wдавc function wдавc_ft_show_all_flows_seg_ui  
CurrFlows=1, Watermark=1
```

```
IX |IP1 |IP2 |PORT1|PORT2|L3 |L4 |VRF |TIMEOUT|APP |TUPLE |FLOW |IS FIF |BYPASS|FINAL |#PKTS  
|BYPASS  
| | | |PROTO|PROTO|VLAN|SEC |NAME |TYPE |TYPE |SWAPPED | | | |PKT  
-----  
1 |192.168.100.2 |192.168.200.2|68 |67 |1 |17 |0 |360 |unknown |Full |Real Flow|Yes |True |True
```



```
SEG IDX | I/F ID | OPST I/F | SEG DIR | FIF DIR | Is SET | DOP ID | NFL HDL | BPS PND | APP PND | FRST TS
| LAST TS | BYTES | PKTS | TCP FLGS
```

```
-----
0 | 9 | ---- | Ingress | True | True | 0 | 50331823 | 0 | 0 | 177403000 | 191422000 | 24252524 | 70094 | 0
```

## ةيسيسرلا لوقحلا

ةهجال اول فرعم ديدحت I/F: فرعم

seg dir: جرخم هاجت لخدم ددح

FIF DIR: ال مأ قفدتلا ئداب هاجت وه اذه ناك اذا ام ددح

NFL HDL: ةزهال ي قفدتلا فرعم

show platform software fed switch active fnf flow-record ASIC <number> start-index <number> num-flow <number of flow>  
ضرعل زاهجال ي ف دوجوملا لاخلال ضرعل

ASIC فيرعتل. هل ذفنملا نيينعت مت يذلا ASIC ليثم وه، ASIC رايتخال: **ةظجالم**  
"show platform software fed switch active|standby|member ifm mappings" رمال مدختسا  
نم دبالف، ال او. نيينعت قفدتلا متهم نكت مل اذا "0" يلع ةيادبال سرهف نيينعت نكمي  
يتلا تاقفدتلا ددح ددحت يتلا، num، تاقفدتلا ةبسنلاب. ةيادبال سرهف ديدحت  
10 ي صقال دحل، اهضرع نكمي.

```
Switch#show platform software fed switch active fnf flow-record ASIC 3 start-index 0 num-flows 1
1 flows starting at 0 for ASIC 3:-----
```

Idx 175 :

```
{90, ALR_INGRESS_NET_FLOW_ACL_LOOKUP_TYPE1 = 0x01}
{91, ALR_INGRESS_NET_FLOW_ACL_LOOKUP_TYPE2 = 0x01}
{0, ALR_INGRESS_NFL_SPECIAL1 = 0x00}
{11, PAD-UNK = 0x0000}
{94, PHF_INGRESS_DEST_PORT_OR_ICMP_OR_IGMP_OR_PIM_FIRST16B = 0x0043}
{93, PHF_INGRESS_SRC_PORT = 0x0044}
{67, PHF_INGRESS_IPV4_DEST_ADDRESS = 0xc0a8c802}
{68, PHF_INGRESS_IPV4_SRC_ADDRESS = 0xc0a86402}
{56, PHF_INGRESS_L3_PROTOCOL = 0x11}
```

FirstSeen = 0x2b4fb, LastSeen = 0x2eede, sysUptime = 0x2ef1c

PKT Count = 0x000000000001216f, L2ByteCount = 0x0000000001873006

## تانايبال راسم ي ف تاريذحتلا واطخال نم ديدحتلا نع ثحبل

show platform software fed switch active|standby|member wdv function  
wdvc\_ft\_show\_stats\_ui | inc| لف تاريذحت| ضرع ي ف ل ش ف تاريذحت|  
ةلمتحملا قفدتلا لودج واطخال

```
Switch#show platform software fed switch active wdv function wdv_ft_show_stats_ui | inc
err|warn|fail
```

```
Bucket linked exceed max error : 0
extract_tuple_non_first_fragment_warn : 0
ft_client_err_alloc_fail : 0
ft_client_err_detach_fail : 0
ft_client_err_detach_fail_intf_attach : 0
ft_inst_nfl_clock_sync_err : 0
ft_ager_err_invalid_timeout : 0
ft_intf_err_alloc_fail : 0
```

```
ft_intf_err_detach_fail : 0
ft_inst_err_unreg_client_all : 0
ft_inst_err_inst_del_fail : 0
ft_flow_seg_sync_nfl_resp_pend_del_warn : 0
ager_sm_cb_bad_status_err : 0
ager_sm_cb_received_err : 0
ft_ager_to_time_no_mask_err : 0
ft_ager_to_time_latest_zero_ts_warn : 0
ft_ager_to_time_seg_zero_ts_warn : 0
ft_ager_to_time_ts_bigger_curr_warn : 0
ft_ager_to_ad_nfl_resp_error : 0
ft_ager_to_ad_req_all_recv_error : 0
ft_ager_to_ad_req_error : 0
ft_ager_to_ad_resp_error : 0
ft_ager_to_ad_req_restart_timer_due_err : 0
ft_ager_to_flow_del_nfl_resp_error : 0
ft_ager_to_flow_del_all_recv_error : 0
ft_ager_to_flow_del_req_error : 0
ft_ager_to_flow_del_resp_error : 0
ft_consumer_timer_start_error : 0
ft_consumer_tw_stop_error : 0
ft_consumer_memory_error : 0
ft_consumer_ad_resp_error : 0
ft_consumer_ad_resp_fc_error : 0
ft_consumer_cb_err : 0
ft_consumer_ad_resp_zero_ts_warn : 0
ft_consumer_ad_resp_zero_pkts_bytes_warn : 0
ft_consumer_remove_on_count_zero_err : 0
ft_ext_field_ref_cnt_zero_warn : 0
ft_ext_gen_ref_cnt_zero_warn : 0
```

**أمدختسأ show platform software fed switch active wдавc function wдавc\_stile\_stats\_show\_ui | Inc err** في ةلمتحم ءاطخأ يأ ضرعل

```
Switch#show platform software fed switch active wдавc function wдавc_stile_stats_show_ui | inc
err
find_flow_error : 0
add_flow_error : 0
remove_flow_error : 0
detach_fo_error : 0
is_forward_direction_error : 0
set_flow_aging_error : 0
ft_process_packet_error : 0
sys_meminfo_get_error : 0
```

**ةيزكرملا ةجلاعمل ةدحوىلىل مزحلا خس ن م ققحتلا**

**ققحتلل "Inc" تم لتسأ | show platform software fed switch active punt cpuq 21** رمال م دختسأ  
NBAR: ةجلاعمل ةيزكرملا ةجلاعمل ةدحوىلىل مزحلا خس ن م

ديازتي مل مقرلا اذه لمعمل ي ف: ةظحالم

```
Switch#show platform software fed switch active punt cpuq 21 | inc received
Packets received from ASIC : 63
```

**ةيزكرملا ةجلاعمل ةدحوىلىل مزحلا ديحت**

WDAVC. ةي لمع لىلىل اهلاسرل لب ق مزحلا طاقسلى نكمي، ام دزالا تاقوا ي ف  
NBAR: "show platform software fed switch active wдавc function fed\_wдавc\_show\_ots\_stats\_ui" م ققحتلل

```
Switch#show platform software fed switch active wdavc function fed_wdavc_show_ots_stats_ui
OTS Limits
-----
ots_queue_max : 20000
emer_bypass_ots_queue_stress : 4000
emer_bypass_ots_queue_normal : 200
OTS Statistics
-----
total_requests : 40
total_non_wdavc_requests : 0
request_empty_field_data_error : 0
request_invalid_di_error : 0
request_buf_coalesce_error : 0
request_invalid_format_error : 0
request_ip_version_error : 0
request_empty_packet_error : 0
memory_allocation_error : 0
emergency_bypass_requests_warn : 0
dropped_requests : 0
enqueued_requests : 40
max_ots_queue : 0
```

show platform software fed switch active wdavc function fed\_wdavc\_clear\_ots\_stats\_ui  
رمأل مدختسې لعافل طاقسإل دادع حسم ل: حيملت

## ساي قمل لكاشم دي دحت

فېنصتلت تانايېل رورم ةكرح عضخت ال، ةزهجالا يف ةرح FNF تالاخل دا دوجو مدع ةلاح يف NBAR2. show platform software fed switch active fnf sw-table size asic <number> shadow 0  
مديكأتل:

اهئاشن دنع ةيساسال ةاونلاو لوجملاب ةصاخ اهؤاشن متي يتل تاقفدتلا: ةظحالم  
متي يذل ASIC مقر طبر متي. كلذل اقفو (خلل، يطايتح، طشن) لوجمل مقر دي دحت بجي  
show platform software fed switch active|standby|member ifm mappings" مدي دحت ل ASIC دي دحت ل  
لظلا رايخل. ةهجالا عم قفاوتي يذل ASIC دي دحت ل "0" امئاد مدي دتسأ.

```
Switch#show platform software fed switch active fnf sw-table-sizes asic 3 shadow 0
-----
Global Bank Allocation
-----
Ingress Banks : Bank 0
Egress Banks : Bank 1
-----
Global flow table Info
INGRESS usedBankEntry 1 usedOvfTcamEntry 0
EGRESS usedBankEntry 0 usedOvfTcamEntry 0 <-- 256 means TCAM entries are full
-----
Flows Statistics
INGRESS TotalSeen=1 MaxEntries=1 MaxOverflow=0
EGRESS TotalSeen=0 MaxEntries=0 MaxOverflow=0
-----
Partition Table
-----
## Dir Limit CurrFlowCount OverFlowCount MonitoringEnabled
```

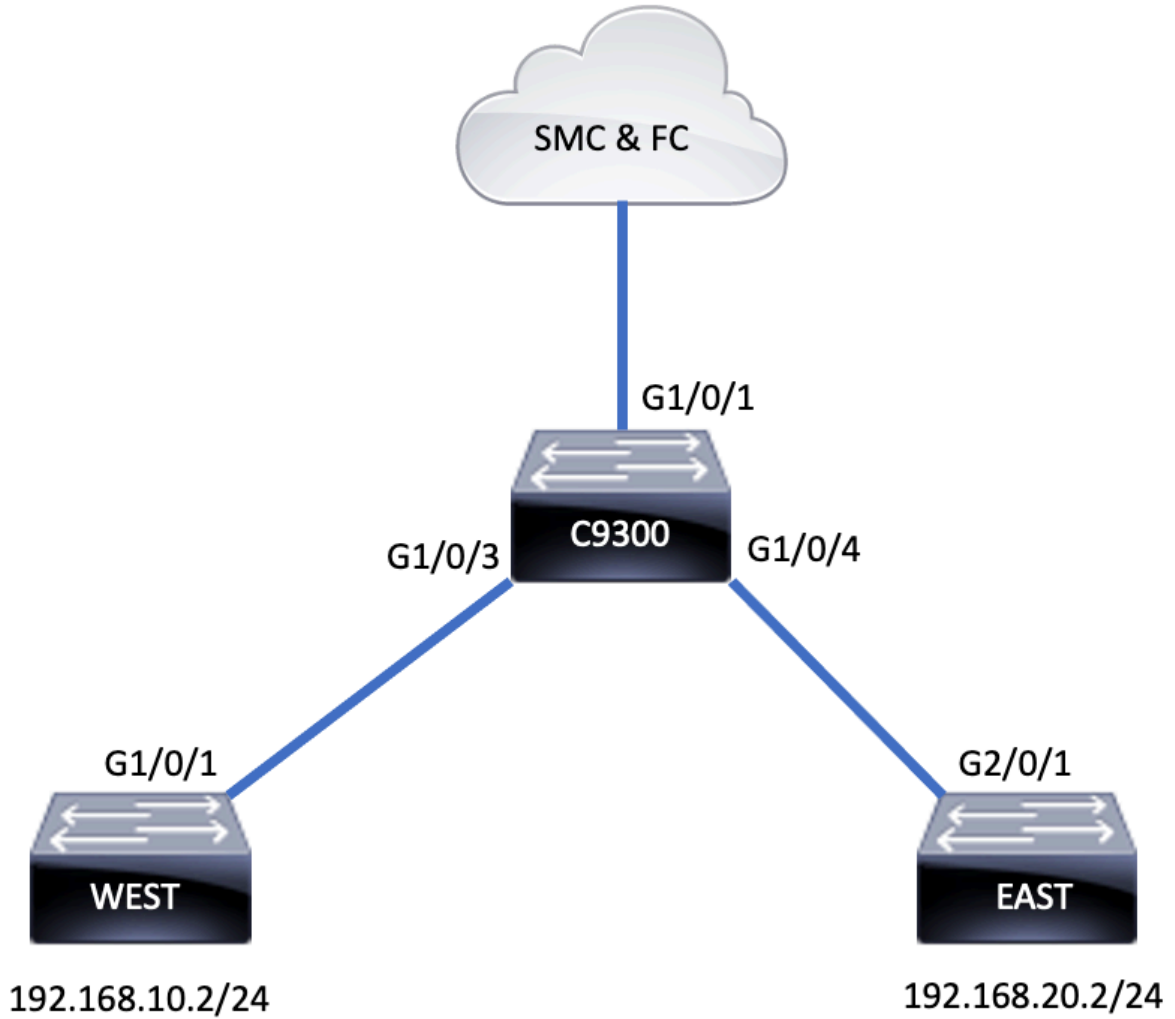
0 ING 0 0 0 0  
1 ING 16640 1 0 1  
2 ING 0 0 0 0  
3 ING 16640 0 0 0  
4 ING 0 0 0 0  
5 ING 8192 0 0 1  
6 ING 0 0 0 0  
7 ING 0 0 0 0  
8 ING 0 0 0 0  
9 ING 0 0 0 0  
10 ING 0 0 0 0  
11 ING 0 0 0 0  
12 ING 0 0 0 0  
13 ING 0 0 0 0  
14 ING 0 0 0 0  
15 ING 0 0 0 0  
0 EGR 0 0 0 0  
1 EGR 16640 0 0 1  
2 EGR 0 0 0 0  
3 EGR 16640 0 0 0  
4 EGR 0 0 0 0  
5 EGR 8192 0 0 1  
6 EGR 0 0 0 0  
7 EGR 0 0 0 0  
8 EGR 0 0 0 0  
9 EGR 0 0 0 0  
10 EGR 0 0 0 0  
11 EGR 0 0 0 0  
12 EGR 0 0 0 0  
13 EGR 0 0 0 0  
14 EGR 0 0 0 0  
15 EGR 0 0 0 0

## ةرفشملا رورملا ةكرح تاليلحت (ETA)

### ةيساسا تامولعم

- لالخ نم ةرفشملا رورملا ةكرح يف ةراضلا جماربلا نيب لاصتالا ديدحت ىلع ETA زكرت نم جيزم ىلإ ةفاضلاب ،ةلصللا تاذ تانايبلا رصانع جارختساو ةيبلسلا ةبقارملا تالكبشلا ىلع مئاقلا يملاعلا نمألا عم يلالا ملعتلاو ةيكولسلا ةجذمنلا
- فاشتكلا ىلإ ةفاضلاب NetFlow نم دعب نع سايقلا نم ةدافتسالا ىلع ETA لمعت Cisco ىلإ تانايبلا هذه لسرتو ريفشنتلا عم قفاوتلاو ةرفشملا ةراضلا جماربلا Stealthwatch.
- لوط لسلسلتو (IDP) ةيلوالا تانايبلا ةمزح :نيسيئر تانايب يرضنع ETA جرختست لوط لسلسلتو (SPLT) اهتقووةمزحلا

### ةكبشلا ليطيختلا مسرلا



## تانوكملا

ETA: لح عاشنإل نارتقالاب اهمادختسا متي ةفلتخم تانوكم ةدع نم ETA فلأتت

- فرصت يتلا ةكبشلا ةزهجأ ةطساوب ةردصملا تانايبلا رصانع ددحي راي عم - NetFlow - ةكبشلا ىلع تاقفدتلا
- يتلا ةكبشلا مادختسا عبتت تانايب ةقاط ريخست ىلع لمعي - Cisco Stealthwatch - ري فوئل - ماخلا مزحلل قيمي عملا صحفتلا وليكولا تالجسو IPFIX و NetFlow نمضتت تاليلحتلا و نامألا ءاكذو ةمدقتملا ةكبشلا ةيؤر ةيناكمإ
- يف مكحتلا رصانع زواجت يذلا راضلا طاشنلا نع ثحبلل - Cisco نم يف رعملا ءاكذلا ةسسؤملا ةئيب لخادو ةبقارملا ريغ تاونقلا لالخ نم هلاخدإ مت وأ نامألا
- تاي مزراوخ مدختست يتلا Cisco IOS XE ةزيم موقت - ةرفشملا رورملا ءكرح تاليلحت فيرعت تانايب ليلحت لالخ نم ةراضلا رورملا ءكرح طامناً ديدحتل ةمدقتملا كولسلا ةلمتحملا تاديدهتلا فاشتكاب، ةرفشملا رورملا ءكرح ب ءصاخلا تانايبلا قفدت ةرفشملا رورملا ءكرح يف ةيفخملا

امه نم ققحتلا و NetFlow و ETA نيوكت ىلع طقف دننتملا نم عزجلا اذه زكري: **ةظحالم** Stealthwatch (SMC) ةرادا مكحت ةدحو يطغي الو Catalyst 9000 Series Switch لوجم ىلع يف رعملا ءاكذلا ةباحس ىلا (FC) قفدتلا عمجم رشنو

## دويقلا

- لمعني كيونولل ضحلل ةيضم بلطتي ETA رشن
- هسفن لىل دناسي ال (نيتماعد نيب ةحسفف) رسي للحم لوحي (TX) و ETA نراق.

عيميحل زمرل رادصاو لوحملل بسانملا نيوكتل لىل عجرا، ةلماش ةمئاق تسيل هذه دويقل.

## نيوكتل

ريصت ةهجو دحو ماع لكشب لوحملا لىل ETA نيكم تب مق، جارخال ي فضوم وه امك قفدتل:

```
C9300(config)#et-analytics
C9300(config-et-analytics)#ip flow-export destination 172.16.18.1 2055
```

مقر ءانيم رخآ لمعتسي ال، 2055 ءانيم تلمعتسا يغبني تنأ: **حيملت**

جارخال ي فضوم وه امك ةنرملا NetFlow نيوكتب مق، كلذ دع

## قفدتل لفس نيوكت

```
C9300(config)#flow record FNF-RECORD
C9300(config-flow-record)#match ipv4 protocol
C9300(config-flow-record)#match ipv4 source address
C9300(config-flow-record)#match ipv4 destination address
C9300(config-flow-record)#match transport source-port
C9300(config-flow-record)#match transport destination-port
C9300(config-flow-record)#collect counter bytes long
C9300(config-flow-record)#collect counter packets long
C9300(config-flow-record)#collect timestamp absolute first
C9300(config-flow-record)#collect timestamp absolute last
```

## قفدتل ةبقارم نيوكت

```
C9300(config)#flow exporter FNF-EXPORTER
C9300(config-flow-exporter)#destination 172.16.18.1
C9300(config-flow-exporter)#transport udp 2055
C9300(config-flow-exporter)#template data timeout 30
C9300(config-flow-exporter)#option interface-table
C9300(config-flow-exporter)#option application-table timeout 10
C9300(config-flow-exporter)#exit
```

## قفدتل لفس نيوكت

```
C9300(config)#flow monitor FNF-MONITOR
C9300(config-flow-monitor)#exporter FNF-EXPORTER
C9300(config-flow-monitor)#record FNF-RECORD
C9300(config-flow-monitor)#end
```

## قفدتل ةبقارم قيبطت

```
C9300(config)#int range g1/0/3-4
C9300(config-if-range)#ip flow mon FNF-MONITOR in
```

```
C9300(config-if-range)#ip flow mon FNF-MONITOR out
C9300(config-if-range)#end
```

لوحمة لة جاول عى لة ETA نى كمة

```
C9300(config)#interface range g1/0/3-4
C9300(config-if-range)#et-analytics enable
```

## ةحصلا نم ققحتلا

سفن لى لة ETA و NetFlow نى وكى دنع. لة قؤملا نى زخمتلا ةركاذ ةئبعت نم ققحت "show flow monitor eta-mon" رمألا لال خ نم ةلألا صى صخت دى كأت. "eta-mon" ةشاش طى شنت نم ققحت "show flow monitor eta-mon"

```
C9300#show flow monitor eta-mon
Flow Monitor eta-mon:
Description: User defined
Flow Record: eta-rec
Flow Exporter: eta-exp
Cache:
Type: normal (Platform cache)
Status: allocated
Size: 10000 entries
Inactive Timeout: 15 secs
Active Timeout: 1800 secs
```

سفن لى لة ETA و NetFlow نى وكى دنع. لة قؤملا نى زخمتلا ةركاذ ةئبعت نم ققحت "show flow monitor <monitor name> cache" نم ال دب "show flow monitor eta-mon cache" نم جاولا، ةجاولا: اغراف "show flow monitor eta-mon cache" نم جارخال نوكى شى ح

```
C9300#show flow monitor FNF-MONITOR cache
Cache type: Normal (Platform cache)
Cache size: 10000
Current entries: 4
```

```
Flows added: 8
Flows aged: 4
- Inactive timeout ( 15 secs) 4
```

```
IPV4 SOURCE ADDRESS: 192.168.10.2
IPV4 DESTINATION ADDRESS: 192.168.20.2
TRNS SOURCE PORT: 0
TRNS DESTINATION PORT: 0
IP PROTOCOL: 1
counter bytes long: 500
counter packets long: 5
timestamp abs first: 21:53:23.390
timestamp abs last: 21:53:23.390
```

```
IPV4 SOURCE ADDRESS: 192.168.20.2
IPV4 DESTINATION ADDRESS: 192.168.10.2
TRNS SOURCE PORT: 0
TRNS DESTINATION PORT: 0
IP PROTOCOL: 1
counter bytes long: 500
counter packets long: 5
timestamp abs first: 21:53:23.390
timestamp abs last: 21:53:23.390
```

```
IPV4 SOURCE ADDRESS: 192.168.20.2
IPV4 DESTINATION ADDRESS: 192.168.10.2
```

TRNS SOURCE PORT: 0  
TRNS DESTINATION PORT: 0  
IP PROTOCOL: 1  
counter bytes long: 500  
counter packets long: 5  
timestamp abs first: 21:53:23.390  
timestamp abs last: 21:53:23.390

IPV4 SOURCE ADDRESS: 192.168.10.2  
IPV4 DESTINATION ADDRESS: 192.168.20.2  
TRNS SOURCE PORT: 0  
TRNS DESTINATION PORT: 0  
IP PROTOCOL: 1  
counter bytes long: 500  
counter packets long: 5  
timestamp abs first: 21:53:23.390  
timestamp abs last: 21:53:23.390

**show flow source eta-exp statistics** **رمأل مادختساب FC و SMC لى اتاقتدال ري دصت نم ققحت**

```
C9300#show flow exporter eta-exp statistics
Flow Exporter eta-exp:
Packet send statistics (last cleared 03:05:32 ago):
Successfully sent: 3 (3266 bytes)
```

```
Client send statistics:
Client: Flow Monitor eta-mon
Records added: 4
- sent: 4
Bytes added: 3266
- sent: 3266
```

**show platform software fed switch active fnf et-analytics-flows** **رمأل مادختساب ةيفي لل ةانقلا لى IDP و SPLT ري دصت نم دكأت**

```
C9300#show platform software fed switch active fnf et-analytics-flows
```

```
ET Analytics Flow dump
```

```
=====
Total packets received : 20
Excess packets received : 0
Excess syn received : 0
Total eta records added : 4
Current eta records : 0
Total eta splt exported : 2
Total eta IDP exported : 2
```

**show platform software et-analytics interfaces** **رمأل مادختساب et تاليلحتلل اهنوك متي يتل اتاهاولا ةحص نم ققحتلا**

```
C9300#show platform software et-analytics interfaces
ET-Analytics interfaces
GigabitEthernet1/0/3
GigabitEthernet1/0/4
```

```
ET-Analytics VLANs
```

**show platform software et-analytics global** **رمأل مدختسأ** **ETA: ل ةماع ةلاح ضرعل**



C9300#**show plat soft et-analytics global**

ET-Analytics Global state

=====

All Interfaces : Off

IP Flow-record Destination : 10.31.126.233 : 2055

Inactive timer : 15

ET-Analytics interfaces

GigabitEthernet1/0/3

GigabitEthernet1/0/4

ET-Analytics VLANs

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذہ Cisco تچرت  
ملاعلاء انءمچي فني مدختسمل معدى وتحم مي دقتل ةيرشبلاو  
امك ةقيقد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچري. ةصاغل مهتغب  
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحل وه  
ىلإ أمئاد عوچرلاب ي صؤت وتامچرتل هذه ةقد نع اهتيلوئسم Cisco  
Systems (رفوتم طبارلا) ي لصلأل يزي لچنل دن تسمل