

# ىلع اه حال صإو Rommon ءاطخأ فاشك ت سا ة ل س ل س ل ا ت ال د ب م Catalyst 9000 Series

## تايوت حمل ا

[ةمدقم ل ا](#)

[ةيس اساس ال ا تابل ط ت م ل ا](#)

[تابل ط ت م ل ا](#)

[ةمدخت س م ل ا تانوك م ل ا](#)

[ةيس اساس ا تامول عم](#)

[دي همت ل ا لي محت ة ادا جراخ ل د ب م ل ا دي همت ت ارايخ](#)

[Flash تافل م ماظن يف ةدوجوم ل ا تافل م ل ا نم دي همت ل ا: 1 رايخ ل ا](#)

[USB / TFTP نم رشاب م ل ا دي همت ل ا: 2 رايخ ل ا](#)

[نراوطل ا تالاج يف تيبث تال ا عم عيس وتلاوخ س ن ل ا: 3 رايخ ل ا](#)

[رورم ةم لك ب ي محم جات فم تدرت سا](#)

[رورم ل ا ةم لك ةداعت س ال فق زواج ت ةيل ا](#)

[ةلص تاذا تامول عم](#)

## ةمدقم ل ا

bootloader رم او ا هجوم نم Catalyst 9000 Series تال د ب م دي همت ةي فيك دن ت س م ل ا اذه فص ي رورم ةم لك دادر ت سا ةي فيك و (rommon).

## ةيس اساس ال ا تابل ط ت م ل ا

### تابل ط ت م ل ا

دن ت س م ل ا اذه ل ةصاخ تابل ط ت م ل ا دجوت ال

### ةمدخت س م ل ا تانوك م ل ا

ةيل ل ا ةي دامل ا تانوك م ل ا و جمار ب ل ا تاراد ص ا ل ا دن ت س م ل ا اذه يف ةدراول ا تامول عم ل ا دن ت س ت

- Catalyst 9200
- Catalyst 9300
- Catalyst 9400
- Catalyst 9500
- Catalyst 9600

تازي م ل ا هذه ني ك م ت ل ةمدخت س م ل ا رم او ال ا ةفر عم ل ب س ان م ل ا ني وك ت ل ا ل ي ل د ع جار : ةظح ال م ى ر خ ال ا ةيس اساس ال ا Cisco ةم ظن ا ل ع

ةصاخ ةي لمعم ةئيب ي ف ةدوجوم ل ةزهجال نم دنتسمل اذ ف ةدراول تامولعمل عاشنم تناك اذا . (يضا رتفا) حوسمم نيوكتب دنتسمل اذ ف ةمدختسمل ةزهجال عيمج تادب رمل يال لمحتحمل ريثأتلل كمهف نم دكأتف ، ليغشتلا ديقتك تبش

## ةيساسأ تامولعم

ديهمت رمل هجوم وهو rommon، ي ف Catalyst 9000 switch لوجم ديهمت متي ، تالاحل ضع ب ي وأ ، ةلماك Cisco IOS®Software جم انرب ةروص لي محت لوجملل نكمي ال ام دنع اما احتام حبصي ةملك دادرتسا لثم تاعارج ذيفنتل ايودي ةيداعال ديهمتلا ةيلمع ةعطاقمب موقت ام دنع رورمل .

ةوجم boot loader رفوي . rommon / bootloader عضو ي ف زاهجال نأ ل رملال : switch هجوم ري شي هجوم ي ف رملال ؟ رادصاب مق ، ةحاتملا تاعارجال ةمئاق ىرتل . زاهجال ةرادال تاعارجال نم ةدودجم رملال : switch .

```
switch: ?
-----
alias          Set and display aliases command
boot           Load and boot an executable image
cat            Concatenate (type) file(s)
copy           Copy a file
date           Show or Set system date
delete         delete file(s)
dir            List files in directories
dns-lookup     Send DNS standard query packets
emergency-install Initiate Disaster Recovery
help           Present list of available commands
history        Monitor command history
md5            Compute MD5 checksum of a file
mkdir          Create directory(ies)
meminfo        Main memory information
net-show       Display current network configuration
ping           Send ICMP ECHO_REQUEST packets to a network host
rename         Rename a file/directory
reset          Reset the system
rmdir          delete directory(ies)
set            Set or display environment variables
unalias        Unset an alias
unset          Unset one or more environment variables
version        Display boot loader version
-----
```

## ديهمتلا لي محت ةادأ جراح لدبملا ديهمت تاراخي

تاراخي ةثالث دجوت:

1. ماظن دربم قربل ي ف دوجوم نوكي نأ دربم نم ةمزج .
2. USB وأ TFTP ربع رشابملا ديهمتلا .
3. (Flash فلم ماظن عارجال اذ وحمي) ئراوطلال تيبتت .

## Flash تافل ماطن في ةدوجومل تافل ملل نم ديهمت ال: 1 رايل


ةلباق ةلمك تافل مكي دل نوكت ام دنع اهاذختا بجي يتل تاوطلال مسقلا اذه فصلي  
لى ديهمتلاب ماق يذلا لدبملاب صاخال Flash تافل ماطن في لعفلاب ةدوجوم ديملت لل  
تنك اذا وا، ايلخا ةظوفحم تافل لولم لول نكي مل اذا. rommon / ديملت لولمحت اءا رماوا هجوم  
رايل اذه نم ال دب 3 رايل وا 2 رايل مدختسا، تافل ملل كلت ةلاح نم دكأتم ريغ.

رملال: dir flash: ليغشتب مق. 1 ةوطلال


امه ناعونلوا. لدبمل ديملت تافل ملل يعون دحا دح. 2 ةوطلال

- Catalyst 9000 تالوحم (فلملال bin قحلمب هيل راشي) ديملت لل لباق يئانث ةروص فلم  
Series Switches. يلالال وحنل لىلع فلملال اذه ةيؤر نكمي: cat9k\_iosxe\_

.SPA.bin

 ةماعل ةروصلال س فن Catalyst 9200 Series switches تالوحم ل مدختست ال: ةظحال  
ةيئانثلال ةروصلال يوتحت. 9600 Series Switches و 9500 و 9400 و 9300 تالوحم ل  
ل فلملال مسال لثامم حالطصا لىلع Catalyst 9200 Series Switch لولم لول  
cat9k\_lite\_iosxe...SPA.bin

- ةمزح فلم نم اقبسم اهازختسا مت يتل مزحل ددحي (.conf) ديملت لل لباق نيوكت فلم  
في ةنيعم (pkg) مزح تافل ماضي كيدل نوكي نا بجي، اذه فلملال عون ديملت. بسانم  
Flash.

 فرعي، ةقيرط ةمزح نانثا اذه نيب ةيلغشتلال قورفال دشرم اذه يطيغلي ال: ةظحال  
ديملتال اعاضوا قباطت نا بجي، لدبملال ةمزح في. بولسا بكري بولسا ةمزح مساب  
جوز ليغشت بجي، قيبطلل ةلباقلال تاصلنملل ةبسنلاب. ةمزحلاءاضع ربع  
exec رمال هجوم نم show version رمال ليغشتب مق. تيبتلال عضوي فس دكم يضارتفا  
ليغشتلل لباق لولم لولم ليلاجل ديملتال عضو ديحتل.

بولسا ةمزح لخا حاتفلال دهمي نا تلمعتسا تنك عيطتسي نا دربم bin. نم لالم

<#root>

switch:

dir flash:

<snip>

cat9k\_iosxe.16.12.04.SPA.bin

يه هذه نا نم ققحتلال ةي فيك ةيلالال ةوطلال فرصت). Flash في مزح هب فلم .conf لىلع لالم

ة.) ححصلا مزحلل

```
<#root>
```

```
switch:
```

```
dir flash:
```

```
<snip>
```

```
14464008 -rw- cat9k-cc_srdriver.16.12.04.SPA.pkg
89134084 -rw- cat9k-espbase.16.12.04.SPA.pkg
1684484 -rw- cat9k-guestshell.16.12.04.SPA.pkg
531063808 -rw- cat9k-rpbase.16.12.04.SPA.pkg
41799673 -rw- cat9k-rpboot.16.12.04.SPA.pkg
31478788 -rw- cat9k-sipbase.16.12.04.SPA.pkg
60392448 -rw- cat9k-sipspace.16.12.04.SPA.pkg
23217156 -rw- cat9k-srdriver.16.12.04.SPA.pkg
7560 -rw- packages.conf <-- .conf file calls a group of packages
12907520 -rw- cat9k-webui.16.12.04.SPA.pkg
9216 -rw- cat9k-wlc.16.12.04.SPA.pkg
```

ف ة ححصلا ة نرت ق م ل ا مزحلل ك يدل نوكي نأ ب ج ي ف ، فلم .conf دي همت ترتخأ اذا 2أ ة و ط خ ل ا  
ري غ فلم "conf" ل ا و ا ة مزحلل ف ل ت ل ا ل ش ف ي ذ ل ا ع و ن ل ا ا ذ ه دي همت ري شي نأ ن ك مي Flash.  
ص (flash) ة ت ق و م ل ا ة ر ك ا ذ ل ا ي ف مزحلل ححص

راد ص ا ب م ق ، ة ت ق و م ل ا ة ر ك ا ذ ل ا ي ف ة ن م ض م ل ا مزحلل ق با ط ي فلم conf ك يدل ن ا ك اذا م ق ق ح ح ل ل  
cat flash:

```
.conf
```

ه ل ا د ب ت س ا و ة ل ص ل ا ت ا ذ ة مزحلل ن ي و ك ت فلم م س ا  
packages. فلم ل ا ا ع ا د ت س ا م ت ي ، ة ل ا ح ل ا ه ذ ه ي ف . ه ب

---

 ت ا ع ا ر ج ا ض ع ب ن ا و ه ة مزحلل ن ي و ك ت فلم ل packages.conf .conf ي ض ا ر ت ف ا ل ا م س ا ل ا : ة ظ ح ا ل م  
ة . ف ل ت خ م ت ا ف ل م ا م س ا ا ه ن ع ج ت ن ي ن ا ن ك م ي ة ي ق ر ت ل ل

---

ي ف ة ب و ل ط م ل ا ت ا ف ل م ل ا ن م ( ة مزحلل ) .pkg ا م ل ا ر ي ش ت ي ت ل ا و ، packages.conf ة ص ا خ ل ا ص ن ل ا ت ا ج ر خ م  
ححص ل ك ش ب دي همت ل ل ل و ح م ل ل Flash فلم م ا ظ ن

```
<#root>
```

```
switch:
```

```
cat flash:packages.conf
```

```
#!/usr/bin/sh
```

```
sha1sum: fb7ea5ea75a0cbf14ce81cecf110e5a6d526df86
```

# sha1sum above - used to verify that this file is not corrupted.

#  
# package.conf: provisioned software file for build 2020-07-09\_21.53  
#

# NOTE: Editing this file by hand is not recommended.

<snip>

# This is for CAT9k

boot rp 0 0 rp\_boot cat9k-rpboot.16.12.04.SPA.pkg <-- package files are for version 16.12.4

iso rp 0 0 rp\_base cat9k-rpbase.16.12.04.SPA.pkg

iso rp 0 0 rp\_daemons cat9k-rpbase.16.12.04.SPA.pkg

iso rp 0 0 rp\_iosd cat9k-rpbase.16.12.04.SPA.pkg

iso rp 0 0 rp\_security cat9k-rpbase.16.12.04.SPA.pkg

iso rp 0 0 rp\_wlc cat9k-wlc.16.12.04.SPA.pkg

iso rp 0 0 rp\_webui cat9k-webui.16.12.04.SPA.pkg

iso rp 0 0 srdriver cat9k-srdriver.16.12.04.SPA.pkg

iso rp 0 0 guestshell cat9k-guestshell.16.12.04.SPA.pkg

<snip>

boot flash: رم أال وأ رم أال رادصإب مق 3. ةوطخأل

.bin

boot flash: سب سأن مأل <filename> م ادخت سإب

.conf

.

<#root>

switch:

```
boot flash:packages.conf
```

```
boot: attempting to boot from [flash:packages.conf]
```

```
boot: reading file packages.conf
```

```
#####...<snip>
```

## USB / TFTP نم رشابم ال ديهمت ال: 2 رايخل

ديهمت ال لي محت اءا رم او اءوم نم Catalyst 9000 Series لءبم ديهمت اءرء مسقلا اءه فص ي ديهمت نكم ي ؁ ءقيرطلا هءه ي ف TFTP مءاخ و ا لومءم USB صارق ا كءم مءءءسا ب rommon ال اءه ديهمت ب موقت يءل اءللم ال ءسن ب لومءم ال موق ي ال ءمءم ءءو ي ف طقف لءبم ال اءءءللم ال ءسن ب لءبم ال لوؤسم موق ي ن ا بء ي رايءل رفوء ي ال امك ؁ Flash ءءلم مءظن ام مقف ؁ ءي بءءل ءءو ال ءءءب ءنك اءا لءبم ال ديهمت ءءب Flash ءءءل ءل ءلصل ي ف ءءءوم ال ءاوءءم مءءءسا و ا ؁ ءمءم ءءو ي ف ءءءنل ال ديهمت ال ءءب لءبم ال لي وءءب 3 رايءل.

ءلءم) cisco.com ءقووم نم Catalyst 9000 Series Switch ءمءنرب ليءنءب مق 1 ءووءم ال اقءال مءءءءسا ل (MD5) 5 مقرة مءءم ال ءلءس رل ءءءءءل ءلءءءءم نوء (cat9k\_iosxe.16.12.4.bin).

TFTP مءاخ و ا لومءم USB صارق ا كءم ي ال اءلءنء مء يءل ءرءصلا لءن. 2 ءووءم ال

نم ءءءو: dir usbflash0 رم ا ل لي ءءءب مق لءبم اب USB لي صوءب مق (طقف USB). 3 ءووءم ال ءءءءصلا لءم ال رءءن اءل

```
<#root>
```

```
switch:
```

```
dir usbflash0:
```

Size	Attributes	Name
805827585	-rw-	cat9k_iosxe.16.12.04.SPA.bin

لومءم ل نكم ي ءءءب ءارءم ن يءل ءءلء بء ي ؁ TFTP مءءءءسا ل (طقف TFTP). 3 ءووءم ال TFTP مءاخ ب لءءءل ءلءل ءلءم ال IP ءءبءل ءلء لءصءال

نءونء ن يءل ءلءومءم مءءءسا

```
switch: set IP_ADDRESS 192.168.1.2
```

ةي عرف ةكبش عانق نيي عتل ةومجم مدختسأ:

```
switch: set IP_SUBNET_MASK 255.255.255.0
```

ةيضارتفا ةباوب نيي عتل set مدختسأ:

```
switch: set DEFAULT_GATEWAY 192.168.1.1
```

TFTP: مداخل لاصتال رابتخال لاصتال رابتخال مدختسأ:

```
switch: ping 192.168.1.10
Pinging 192.168.1.10, 4 time(s), with packet-size 16
service type : 0
total length : 9216 bytes
identification : 56580
fragmentation : 0
time to live : 254
protocol : 1
source : 192.168.1.2
destination : 192.168.1.10
<snip>
```

usbflash0: TFTP نم ةروصل ديهمتل ديهمتل مدختسأ 4. ةوطخلال

<#root>

switch:

```
boot tftp://192.168.1.10/cat9k_iosxe.16.12.04.SPA.bin
```

```
boot: attempting to boot from [tftp://192.168.1.10/cat9k_iosxe.16.12.04.SPA.bin]
```

h/w (environment):

```
mac : aa:bb:cc:dd:ee:ff
```

n/w (environment):

```
ip : 192.168.1.2
```

```
mask : 255.255.255.0
```

```
gateway : 192.168.1.1
```

h/w:

```
interface : eth0 (Ethernet)
```

```
mac : aa:bb:cc:dd:ee:ff
```

n/w (ip v4):

```
ip : 192.168.1.2
```

```
mask : 255.255.255.0
```

```
route(s) : 0.0.0.0 -> 192.168.1.0/255.255.255.0
```

n/w (ip v6):

```
ip(s) : FE80::1234:5678:9123:4567/64
```


```
      : 2001:111:2222:333:4444:5555:6666:7777/64
route(s) : :: -> 2001:111:2222:333::/64
          : :: -> FE80::/64
          : FE80::999:8888:7777:6666 -> ::/

tftp v4:
server   : 192.168.1.10
file     : cat9k_iosxe.16.12.04.SPA.bin
blocksize : 1460
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
<snip>
```

### ئراوطلال تالاح ي ف تي بثتال عم عيسوتل اوخسنال: 3 رايخلال

packages بوغرم لا ام دنع بولسا ب كرى ي ف حات فملا ده مي نا تنأ اارجا حمسي ب كرى ئراط لا، الا بولسا م زح ي ف ده مي نا دي رت ال تنأ ام دنع وا، ماظن دربم قربلا ي ف يوتحي ال نو كى دي همت متي، ئراوطلال ةلاح ي ف تي بثتال ةقيرط مادختساب. بولسا ب كرى نا ل وحي كلذ دعبو لىل ع دي همتال ري غتمو، ةمزال نيوكت فلمو، ةبسانملا ةمزال تافل م مادختساب ل وحملا لوال دي همتال.

---

 وا قباس نيوكت ي ا حسم متي. امامت Flash تافل م ماظن وحم ت اوطلال هذه: ري ذحت ةظوفحم تافل م.

---

 install-ئراط حات فم sery 9200 ةزافح ةدام دناسي ال: ةطحال م.

---

ل واصلل USB او TFTP ربع هيل ل واصل ونا نكمي ي ئانث (.bin) ةروص فلم لىل لصح 1. ةوطلال USB / TFTP نم رشابم لي حمت: 2 رايخلال نم 3 لىل 1 نم ت اوطلال عجار، تامولعمل نم ديزم لىل لىل دلل اذه ي ف.

رمال: dir sda9: مادختساب فطاخ دادرتسا مسق لىل دادرتسا فلم رفوت نم ققحت 2. ةوطلال

ءارجال cisco.com نم هلي زنتب موقت ي ذلا جم انربلا فلم عم نارتيق ال اب دادرتسالال فلم لم عي ةعسوتل اوخسنال ةي لم ع.

<#root>

switch:

dir sda9:

Size Attributes Name

-----  
21656489 -rw-

cat9k-recovery.SSA.bin <-- Recovery Image

-----



emergency-install مَادخْتَسَاب ئِرَاطَلَا تِيْبَثَلَا ءَارْجَا أَدْبَا 3. ةَوْطَخَلَا

رِظْتَنَا. تَانُوَكْمَلَا مَزْحِي فِ ةَوْصَلَا عَسُوِي وَ Flash فَلَم مَاطْن قِيَسْنَتَب رَمَالَا اذَه مَوْقِي. رَمَالَا  
ةَمَلْعَلَا لَمْتَكْت يْتَح تَقْوَلَا ضَعْب.

```
<#root>
```

```
switch:
```

```
emergency-install tftp://192.168.1.10/cat9k_iosxe.16.12.04.SPA.bin
```

```
WARNING: The system partition (bootflash:) can be erased during the system recovery install process.
```

```
Are you sure you want to proceed? [y] y/n [n]: y
```

```
Starting system recovery (tftp://192.168.1.10/cat9k_iosxe.16.12.04.SPA.bin) ...
```

```
boot: attempting to boot from [sda9:cat9k-recovery.SSA.bin]
```

```
boot: reading file cat9k-recovery.SSA.bin
```

```
#####
```

```
<snip>
```

```
Downloading bundle tftp://192.168.1.10/cat9k_iosxe.16.12.04.SPA.bin...
```

```
curl_vrf=2
```

% Total	% Received	% Xferd	Average	Speed	Time	Time	Time	Current			
			Dload	Upload	Total	Spent	Left	Speed			
100	768M	100	768M	0	0	5522k	0	0:02:22	0:02:22	--:--:--	7646k

```
<snip>
```

```
Preparing flash....
```

```
Flash filesystem unmounted successfully /dev/sda3
```

```
Syncing device....
```

```
Emergency Install successful... Rebooting
```

```
can reboot now
```

boot لِيْغَشْتَب مَق. bootloder / rommon(switch:). رَمَالَا هَجُوم يَلَا لَوْحَمَلَا دَوْعِي نَأْنِكْمِي 4. ةَوْطَخَلَا  
flash:packages.conf رَمَالَا .

```
<#root>
```

```
switch:
```

```
boot flash:packages.conf
```

```
boot: attempting to boot from [flash:packages.conf]
```

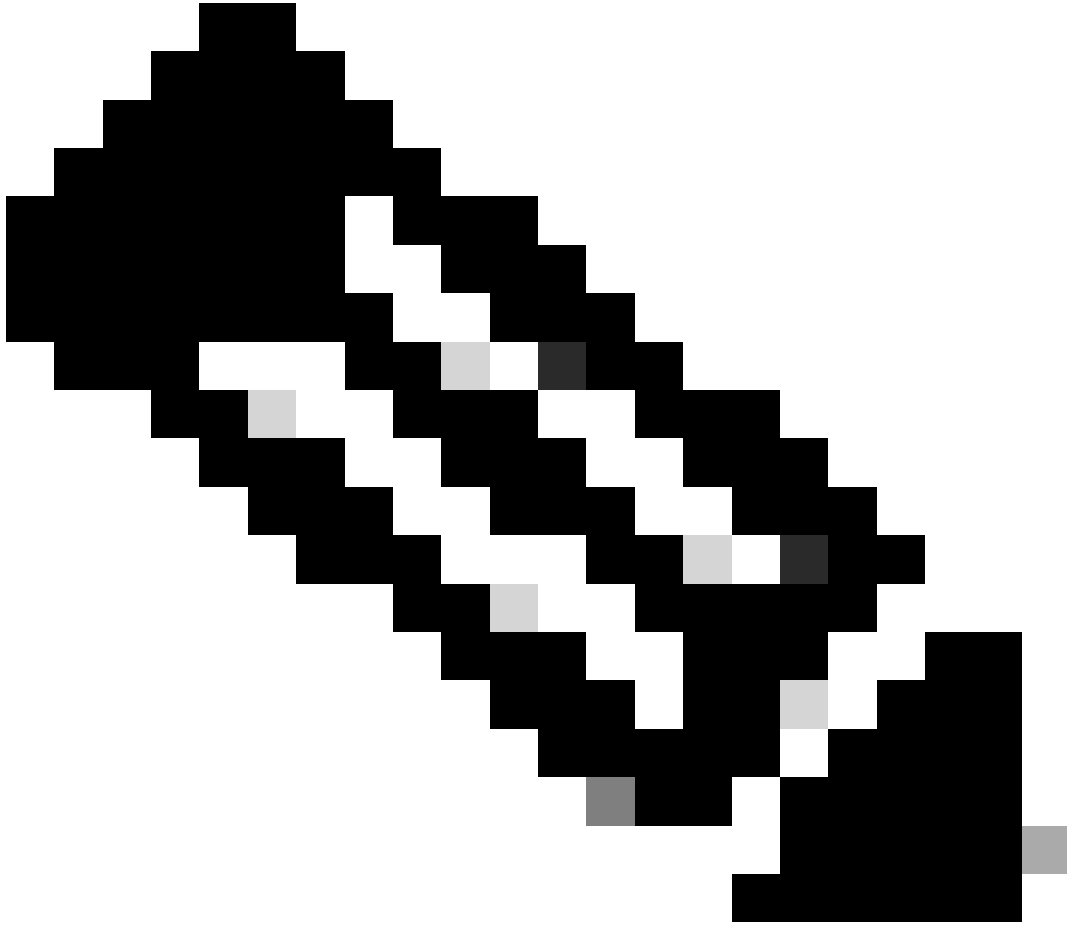
```
boot: reading file packages.conf
```

```
#
```

```
#####
```

## رورم ةم لك ب ي محم حات فم تدرت سا

رِيْغْتَم طَبْضَب مَق. لِيْغَشْتَلَا ءَدْب نِيْوَكْت لَهَا جْت كْنِكْمِي، رورم ةم لك ب ي محم لَوْحَم دَادْرْتَسَا ل  
رورم ةم لك يَلَع يَوْتَحِي يَذَلَاو، startup-config يَطْخَتَل bootloder ةَبَلَا طَم ةَذَفَان يَف.



دادرستسإءارجإ دنع ،(نافرشم) ىلالعلا رفوتلا تاذ Catalyst 9400 تالوحم ىف :ةظحال م نكمى ،الءو .لىغشتلا لبق ىوناثلا فرشملا ءلازا كىلع بىجى ،رورملا ءم لك رورملا ءم لك نىوكت ءعب .ىوناثلا فرشملا نم ىلالعلا نىوكتلا لىمحت ىساسألل نىوكتلا بىحست نأ نكمى و ،ىوناثلا فرشملا ءارءا ك نكمى ،بولطملا وحنلا ىلع ىساسألل فرشملا نم ىلالعلا

رمأل SWITCH\_IGNORE\_STARTUP\_CFG=1 لىغشتب مق ،(switch:) bootloader رمأل ءوم ىف

<#root>

switch: SWITCH\_IGNORE\_STARTUP\_CFG=1

ءىمئل تارائى نونعملا مسقلا ىف ءفوصوم ءقىرط ربع لوحملا ءىمئل ءىمئل مءءتسأ (ءىمئل لىمحت ءاءا) bootloader ءبلطملا نم لوحم

لىغشتلا ءءب نىوكت ءءاعتسال نوكملا رىغ لوحملا مءءتسإ ك نكمى ،لوحملا ءىمئل ءعب

Flash، فلم ماظن نم كيدل copy:startup-config ربح،  
no system ignore startupconfig switch all رمال رادصاب مق، ةبغرل بسح لوحملا نيوكتب تمق نأ دعب .  
يلى ليغشتلا ادب نيوكتب لوحملل حامس لل exec رمال هجوم نم write memory رمال او  
لبق تسملال في ديهمتلا.

---

 نم ام عم ةمزج حاتفملا write memory، و no system ignore startupconfig switch all تنأ ردي ال نإ: ريذحت  
لبق تسملال في reload يلى ليكشت.

---

## رورملا ةملك ةداعتسا لفق زواجت ةيلا

ةادأ يلى لوصول او ديهمتلا ةيلعم ةعطاقم لوحات ام دنع أطخ ةلاس رلدبملا ضرعي نأ نكمي  
ديهمتلا ليحمت.

رورملا ةملك دادرستسا لي طعت يلى ةلاس رللا ريشت

```
<#root>
```

The

```
password-recovery mechanism has been triggered, but
```

```
is currently disabled
```

```
. Access to the boot loader prompt  
through the password-recovery mechanism is disallowed at  
this point. However, if you agree to let the system be  
reset back to the default system configuration, access  
to the boot loader prompt can still be allowed.
```

```
Would you like to reset the system back to the default configuration (y/n)?
```

يلى لوصول اب حمست و يضارتفالا نيوكتبلا يلى لوحملا طبض ةداع y يلى ةباجتسالا يدؤت  
bootloader / rommon رمال هجوم.

ليغشتلا ادب ليكشت و يلاحللا ديهمتلا نايب عم حاتفملا n ةباجتسالا دهمي.

## ةلص تاذا تامولعم

- [تادنتسملال او يبقنقتلا معدلا - Cisco Systems](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة م ادخت ساب دن تسمل اذة Cisco ت مچرت  
ملاعلاء انء مچ م ن م دخت سمل م عد ى وت م م دقت ل م رشب ل و  
امك ة قى قد نوك ت نل ةللأل مچرت ل ضفأ نأ ة ظحال م ى چرئى . ة صاأل م هت غل ب  
Cisco مچرت م م دقت م تى ل ة فارت حال ة مچرت ل م لاعل و  
ى ل أمئ اد وچرل اب ى صؤت و ت امچرتل هذه ة قد ن ع اهت ل وئ س م  
Systems (رفو تم طبارل) ل صأل ل ى زى ل چن إل دن تسمل