

ةبل اظملا ديهمتلا MDS9000 تدرتسلا

تايوتحمل

[ةمدقملا](#)

[ةيساسلا تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[ةيساسا تامولعم](#)

[لوحملا ديهمت لسلسلت](#)

[ليديتلاب ةبل اظملا](#)

[دادرتسالا عارج](#)

ةمدقملا

هجوم نم (MDS) تاقبطلاددعتم تانايب زكرم لوحمةداعتسلا ةيفيك دنتسملا اذه حضوي ديهمتلا عوضوو ديهمتلا ليحت.

ةيساسلا تابلطتملا

تابلطتملا

ةيلاتلا عيضاوملاب ةفرعم كي دل نوكت ناب Cisco ي صوت:

- MDS9000 CLI نيوكت رماوا
- MDS لوحمب مكحت ةدحو لاصتا دادعلا ةيفيك
- اهب صاخلا ةرادلا ذفنم لالخ نم ةكبشب هلي صوت و MDS لوحم دادعلا ةيفيك
- TFTP عم هباشتلا

ةمدختسملا تانوكملا

تارادصل او 6.2(9) رادصلال جماربل تابلطتملا دنتسملا اذه يف ةدراولا تامولعملا دنتست 48 ىلا 12 نم معددي ذل switchname tempest و MDS9148S لوحم دنتسملا اذه مدختسي .ثدحألا ةيناثلا يف تباچي 16 ةعرسب ةيفيل ةانق ذفنم

ةصاخ ةيلمعم ةئيب يف ةدوجوملا ةزهجال نم دنتسملا اذه يف ةدراولا تامولعملا عاشنإ مت تناك اذإ .(يضارتفا) حوسمم نيوكتب دنتسملا اذه يف ةمدختسُملا ةزهجالا عيمجتأ دب رمايأ لمتحمل ريثأتلل كمهف نم دكأتف ،ليغشتلا ديقتككشب

ةيساسا تامولعم

فلات ريغ حل اص Kickstart ليغشت ادب MDS تالوحم بلطتت ،حيحص لكشب لمعلال لجا نم عنمت ةدوقم وأ ةفلات وأ ةحيحص ريغ Kickstart روص .لماك لكشب ديهمتلل ماطنلا ةروصو

ةحل اص Kickstart ةروص عم حاتفم .ديهمتال ليمحت رمأ هجوم ي ف فقوتتو ديهمتال نم لوحمل
ديهمتال عضو ي ف فاطمال هب يهتني ،ةدوقفم وأ ةحيحص ريغ ماطن ةروص نكلو

لوحمل ديهمت لسلسلت

ماظنل ةروص > Kickstart ةروص > ليمحت ةادأ > BIOS

- ليمحتل ةادأ ليمحتب (BIOS) يساسأل لاخذال جارخا ماطن موق ي .
- أدبتو (RAM) يئاوشعل لوصول ةركاذ ي ف Kickstart ةروص ليمحتب ليمحتل ةادأ موقت .
Kickstart ةروص ليغشت
- اهليغشتو ماطنل ةروص ليمحتب Kickstart ةروص موقت .
- ليغشتل ادب نيوكت فلم ماطنل ةروص أرت .

ليدبتلاب ةبالاطمال

روط	رماو هجوم	فصولا
BIOS	لباق ريغ ديهمتلل	ليغشتب (BIOS) يساسأل جارخال او لاخذال ماطن أدبي ةركاذل رابتخاو يتاذل رابتخال
لمحم	>ليمحت زاهج	جماربلا طغض اغلاب ديهمتال ليمحت ةادأ موق ي Kickstart ةروص ديهمتل ةلمحمل رمأ هجوم لاخذال (C حاتفم و مكحتل حاتفم) Ctrl + C ديهمتال ليمحت .
تراتسكيك	switch(boot)#	Ctrl ىلع طغضا ،ديهمتال ليمحت ةادأ ةلحرم اهتنا دنع لاخذال (نميال سوقل حاتفم و مكحتل حاتفم) + — ديهمتال عضو
ماظنل	ليجست لوخدال:	ادب نيوكت فلم ليمحتب ماطنل ةروص موقت ةبالاطمك لوخدال ليجستل لوحم عاجراو ليغشتل

دادرتسال اارجا

لوحمل مكحت ةدحو لمع ةسلج نم

>ليمحت زاهج

TFTP مداخل ليلد ي ف اهعضوو ،لوحملاب ةصاخال System و Kickstart روص ليزنتب مق 1. ةوطخل

10.104.204.100 وه TFTP مداخل IP ناونع ،لاثمل اذه ي ف

هتباوبو ةيعرفال ةكبشلل عانقو لوحمل ةرادل IP ناوع نيوكتب مق 2. ةوطخل
ةيضارفال.

<#root>

Check config options in loader prompt using help option

```
loader> help
help      - print online help
boot      - Boot image
cmdline   - <arguments>
dir       - List Directory
help      - print online help

network - Set network communication settings

reload    - Reboot the board.
serial    - Set serial console settings
show      - Show loader configuration
```

<#root>

```
loader>
net --ip=10.66.78.80 --nm=255.255.255.128 --gw=10.66.78.4
```

لالم اذه في:

- mgmt0 IP 10.66.78.80 255.255.255.128 لوحمل ةهجاو ناوع نوكي
- 10.66.78.4 وه لوحمل ةيضارفال ةرابعلل IP ناوع

وأ

لوحمل ةزهجال زرط عم اليلق ليحتل ةادأ ةبلاطم في IP نييعت ةنمازم فلتيخي

T&V-Series ةنبل تالوحم ةلاح في انه جردمل لالم.

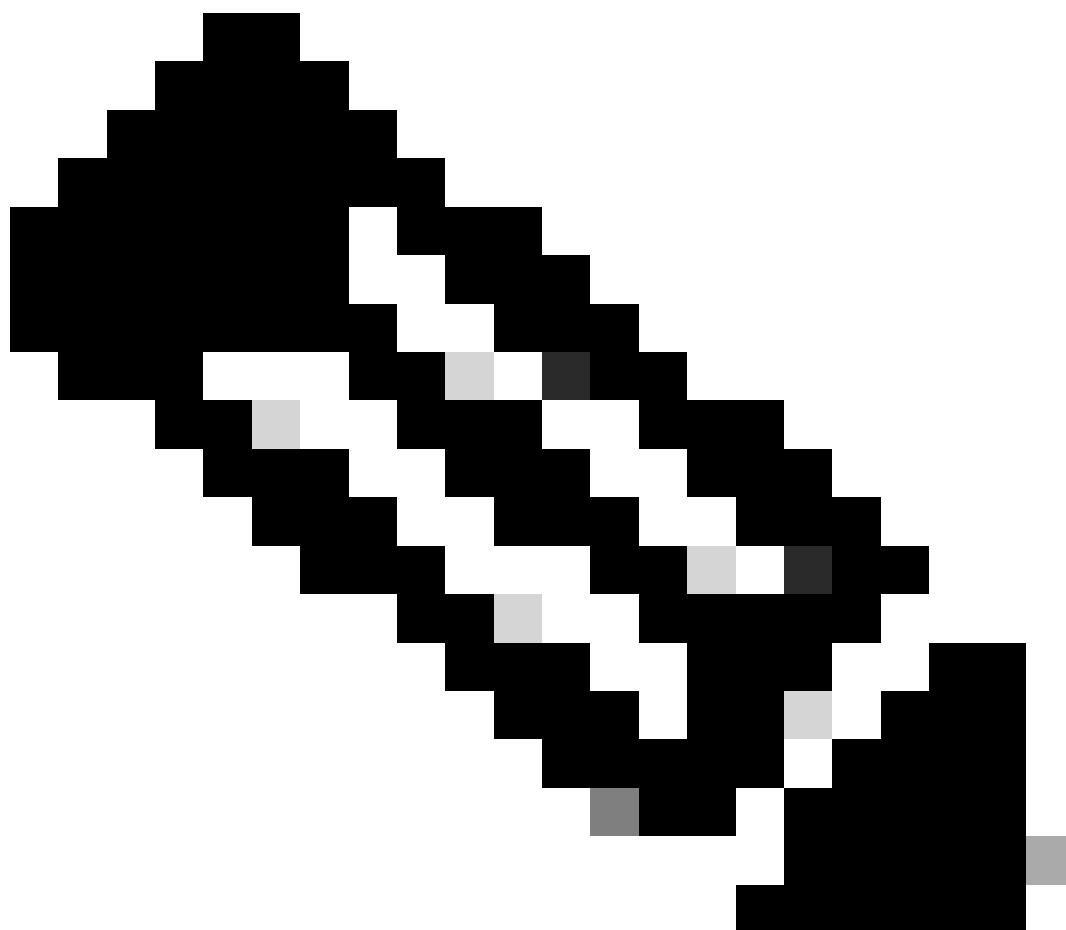
<#root>

```
loader> set ip
```

10.66.78.80

255.255.255.128

```
loader> set gw
```



ةرم لولل لوحمل ديمتب موقت تنك اذ بلولطم config 2 ةوطخل :ةطخلالم
erase boot. ةباتك مت دق لوحمل نأ وأ

عضو ىلا لوحمل راضلالم ،TFTP مداخل لىلد ف ةدووملالم Kickstart ةروص ديمتب مق 3. ةوطخلالم
ديمتلالم.

```
loader> boot tftp://10.104.204.100/m9100-s5ek9-kickstart-mz.8.3.1.bin
eTSEC2: Speed 1000, full duplex
Using eTSEC2 device
TFTP from server 10.104.204.100; our IP address is 10.66.78.80; sending through gateway 10.66.78.4
Filename 'm9100-s5ek9-kickstart-mz.8.3.1.bin'.
Load address: 0x8000000
Loading:      *#####
              #####
```

```
[ 0.060378] Host controller irq 26
[ 0.103390] Assign root port irq 26
[ 0.144046] Host controller irq 24
[ 0.193691] Assign root port irq 24
[ 0.810630] physmap-flash physmap-flash.0: Could not reserve memory region
[ 1.084751] Enabling all PCI devices
INIT: Checking all filesystems...r.r.r.retval=[1]
r done
WARNING: Image sync is going to be disabled after a loader netboot.
Loading system software
No system image is specified
/etc/init.d/functions: li
INIT: Sending processes the KILL signal
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2018, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
```

```
http://www.opensource.org/licenses/lgpl-2.1.php
switch(boot)#
```

ب. ولساً ةمزال نم حاتفملا تدرتسا 4. ةوطخل

لوحمل ديهتم رماً هجوم في IP نيوكت نم ققحت 1.

```
switch(boot)# sh ip
ip routing is disabled
Management Interface: ip address 10.66.78.80/25
                        ip default-gateway 10.66.78.4
```

IP ناوعو ةهجال ةرادال IP ناوع نيوكتب مقف، IP نيوكت ىلع روثعل متي مل اذإ
حضم وه امك ىرخأ ةرم ةرابعلل يضارثفالا

```
switch(boot)# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(boot)(config)# interface mgmt 0
switch(boot)(config-if)# ip address 10.66.78.80 255.255.255.128
switch(boot)(config-if)# no shut
switch(boot)(config-if)# exit
switch(boot)(config)# ip default-gateway 10.66.78.4
switch(boot)(config)# exit
```

هجوم في لاصتالا رابتخا ةباجتسا رفوتت ال) لوحمل او TFTP مداخل ني ب IP لاصتالا رابتخا 2.
(للمحتال رمأ

للدان TFTP ال نم ناوع ةرادال حاتفملا زؤي.

```
C:\Users\mpandika> ping 10.66.78.80
Pinging 10.66.78.80 with 32 bytes of data:
Reply from 10.66.78.80: bytes=32 time=2ms TTL=60
Reply from 10.66.78.80: bytes=32 time=3ms TTL=60
Reply from 10.66.78.80: bytes=32 time=3ms TTL=60
Reply from 10.66.78.80: bytes=32 time=3ms TTL=60

Ping statistics for 10.66.78.80:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 3ms, Average = 2ms

C:\Users\mpandika>
```

3. لوحملاب ةصاخلا ديهمتلا ةركاذى لى TFTP م داخ نم ماظنلا روصو Kickstart لىزنتب مق.

```
switch(boot)# copy tftp://10.104.204.100/m9100-s5ek9-kickstart-mz.8.3.1.bin bootflash:
Trying to connect to tftp server.....
Connection to server Established. Copying Started.....
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...
switch(boot)#
```

```
switch(boot)#copy tftp://10.104.204.100/m9100-s5ek9-mz.8.3.1.bin bootflash:
Trying to connect to tftp server.....
Connection to server Established. Copying Started.....
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...
switch(boot)#
```

4. لوحملاب ةصاخلا ديهمتلا ةركاذى لى حاجناب ماظنلا روصو Kickstart لىزنت نم ققحت.

```
switch(boot)# dir bootflash:
 4096  Dec 22 2002 01:38:31  .partner/
  297  Nov 09 2017 07:18:54  MDS201711091818530370.lic
  297  Nov 09 2017 07:28:42  MDS201711091828418770.lic
 4096  Jul 23 2018 14:44:25  lost+found/
26027008 Aug 08 2018 02:55:31 m9100-s5ek9-kickstart-mz.8.3.1.bin
109635731 Aug 08 2018 02:53:38 m9100-s5ek9-mz.8.3.1.bin
 3430222 Feb 01 2000 02:31:30 moonlake.1.f.xsvf
 23467  Jul 30 2018 12:40:56  mts.log
 347607  Jul 28 2017 04:46:31  portchannel
  4096  Dec 22 2002 02:38:54  scripts/
 31812  Jun 30 2018 05:07:27  snmp.pcap
```

```
Usage for bootflash: filesystem
1264746496 bytes used
2106781696 bytes free
3371528192 bytes total
switch(boot)#
```

5. ماظنلا ةروص لىمحت.

```
switch(boot)# load bootflash:m9100-s5ek9-mz.8.3.1.bin
Uncompressing system image: bootflash:/m9100-s5ek9-mz.8.3.1.bin
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
Load plugins that defined in image conf: /isan/plugin_img/img.conf
No Patching support on this platform
```

```
Loading plugin 0: core_plugin...
No Patching support on this platform
Enter pboot_chk_compatibility
num srgs 1
0: swid-core-s5ek9m, swid-core-s5ek9m
num srgs 1
0: swid-sup-mini-ks, swid-sup-mini-ks
INIT: Switching to runlevel: 3
INIT: Sending processes the TERM signal
switch(boot)#
INIT:
```

```
2018 Aug 8 03:13:03 %SYSLOG-2-SYSTEM_MSG : Syslogs wont be logged into logflash until logflash is onl
2018 Aug 8 03:13:06 %KERN-0-SYSTEM_MSG: [ 1.084751] Enabling all PCI devices - kernel
2018 Aug 8 03:14:13 switch %CARDCLIENT-2-REG: OK
System is coming up ... Please wait ...
System is coming up ... Please wait ...
2018 Aug 8 03:14:22 switch %ASCII-CFG-2-CONFIG_REPLAY_STATUS: Bootstrap Replay Started.
System is coming up ... Please wait ...
```

User Access Verification

```
10.66.78.80 login: 2018 Aug 8 03:14:41 switch %ASCII-CFG-2-CONFIG_REPLAY_STATUS: Bootstrap Replay Done
2018 Aug 8 03:14:44 switch %PMON-SLOT1-2-PMON_CRIT_INFO: Port Monitor Critical Information: Config down
2018 Aug 8 03:14:45 switch %ASCII-CFG-2-CONFIG_REPLAY_STATUS: Ascii Replay Started.
2018 Aug 8 03:14:45 switch %PMON-SLOT1-2-PMON_CRIT_INFO: Port Monitor Critical Information: Policy (sl
2018 Aug 8 03:14:46 switch %PLATFORM-2-PS_OK: Power supply 1 ok(Serial number QCS18242L8D)
2018 Aug 8 03:14:46 switch %PLATFORM-2-PS_FANOK: Fan in Power supply 1 ok
2018 Aug 8 03:14:46 switch %PLATFORM-2-PS_FAIL: Power supply 2 failed or shut down(Serial number QCS18
2018 Aug 8 03:14:46 switch %PLATFORM-2-FAN_OK: Fan module ok
2018 Aug 8 03:14:46 switch %PLATFORM-2-FAN_OK: Fan module ok
2018 Aug 8 03:14:46 switch %PLATFORM-2-FAN_OK: Fan module ok
2018 Aug 8 03:14:46 switch %PLATFORM-2-FAN_OK: Fan module ok
2018 Aug 8 14:15:35 tempest %ASCII-CFG-2-CONFIG_REPLAY_STATUS: Ascii Replay Done.
User Access Verification
tempest login:
```



لوحمل مسالسلست مادختساب اقبسملوحمل نيوكت مت:ةظالم

لوحمل إلى لودلد لجس.

```
tempest login: admin
Password:
Last login: Wed Aug 8 14:20:01 on pts/0
```

```
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2018, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
```

<http://www.opensource.org/licenses/lgpl-2.1.php>
tempest#

7. ديهم تل تاريختم نم ققحتل.

```
tempest# show boot
Current Boot Variables:
kickstart variable = bootflash:/m9100-s5ek9-kickstart-mz.8.1.1.bin
system variable = bootflash:/m9100-s5ek9-mz.8.1.1.bin
Boot POAP Disabled
No module boot variable set

Boot Variables on next reload:
kickstart variable = bootflash:/m9100-s5ek9-kickstart-mz.8.1.1.bin
system variable = bootflash:/m9100-s5ek9-mz.8.1.1.bin
Boot POAP Disabled
No module boot variable set
tempest#
```

8. ةحاصل ةروصل ال ع ديهم تل تاريختم طبضا.

```
tempest# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Documents: http://www.cisco.com/en/US/products/ps9372/tsd\_products\_support\_series\_home.html
Copyright (c) 2002-2018, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained herein are owned by
other third parties and are used and distributed under license.
Some parts of this software are covered under the GNU Public
License. A copy of the license is available at
http://www.gnu.org/licenses/gpl.html.
```

Software

```
BIOS:      version 2.1.17
loader:    version N/A
kickstart: version 8.3(1)
system:    version 8.3(1)
BIOS compile time:      01/08/14
system image file is:   bootflash:///m9100-s5ek9-mz.8.3.1.bin
system compile time:    7/30/2018 12:00:00 [07/12/2018 19:32:46]
```

Hardware

```
cisco MDS 9148S 16G 48 FC (1 Slot) Chassis ("2/4/8/16 Gbps FC/Supervisor")
Motorola, e500v2 with 4088556 kB of memory.
Processor Board ID JAE18250A8C
```

```
Device name: tempest
bootflash:   4018896 kB
```

Kernel uptime is 0 day(s), 0 hour(s), 47 minute(s), 44 second(s)

Last reset at 362296 usecs after Wed Aug 8 13:02:31 2018

Reason: Reset Requested by CLI command reload

System version: 8.1(1)

Service:

plugin

Core Plugin

tempest# config t

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

tempest(config)# boot kickstart bootflash:m9100-s5ek9-kickstart-mz.8.3.1.bin

Performing image verification and compatibility check, please wait....

tempest(config)# boot system bootflash:m9100-s5ek9-mz.8.3.1.bin

Performing image verification and compatibility check, please wait....

tempest(config)#

9. ديهتم لال تاريغتم نييغت نم ققحت.

tempest# show boot

Current Boot Variables:

kickstart variable = bootflash:/m9100-s5ek9-kickstart-mz.8.3.1.bin

system variable = bootflash:/m9100-s5ek9-mz.8.3.1.bin

Boot POAP Disabled

No module boot variable set

Boot Variables on next reload:

kickstart variable = bootflash:/m9100-s5ek9-kickstart-mz.8.1.1.bin

system variable = bootflash:/m9100-s5ek9-mz.8.1.1.bin

Boot POAP Disabled

No module boot variable set

10. لال running-config لولحمل ظفح.

tempest# copy running-config startup-config

[#####] 100%

Copy complete.

tempest#

11. ديهتم لال تاريغتم نييغت نم ققحت copy running-config startup-config.

```
tempest# show boot
Current Boot Variables:
kickstart variable = bootflash:/m9100-s5ek9-kickstart-mz.8.3.1.bin
system variable = bootflash:/m9100-s5ek9-mz.8.3.1.bin
Boot POAP Disabled
No module boot variable set
```

```
Boot Variables on next reload:
kickstart variable = bootflash:/m9100-s5ek9-kickstart-mz.8.3.1.bin
system variable = bootflash:/m9100-s5ek9-mz.8.3.1.bin
Boot POAP Disabled
No module boot variable set
```

ةمچرتل هذه ل و ح

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