

# رورملا ةم لك دادرتسا ءاطخا فاشك تسأ Cisco IOS و Cisco IOS XE تاهجوم يف اهال صاوا

## تايوت حمللا

[ةمدقملا](#)

[ةيساس الابلطت مللا](#)

[تابلطت مللا](#)

[ةمدختس مللا تانوك مللا](#)

[ةيساسا تامولعم](#)

[Cisco IOS و Cisco IOS XE تاهجوم يف رورملا ةم لك دادرتسا](#)

[ءاطقنا ءراشا ءاكاحم](#)


## ةمدقملا

ءاحسم Cisco IOS® و Cisco IOS® XE يف ءءاعتسا ةم لك زءني نأ ةي لمعلا ءقيثوا ذه فصبي ءي ءءخت.

## ةيساس الابلطت مللا

### تابلطت مللا

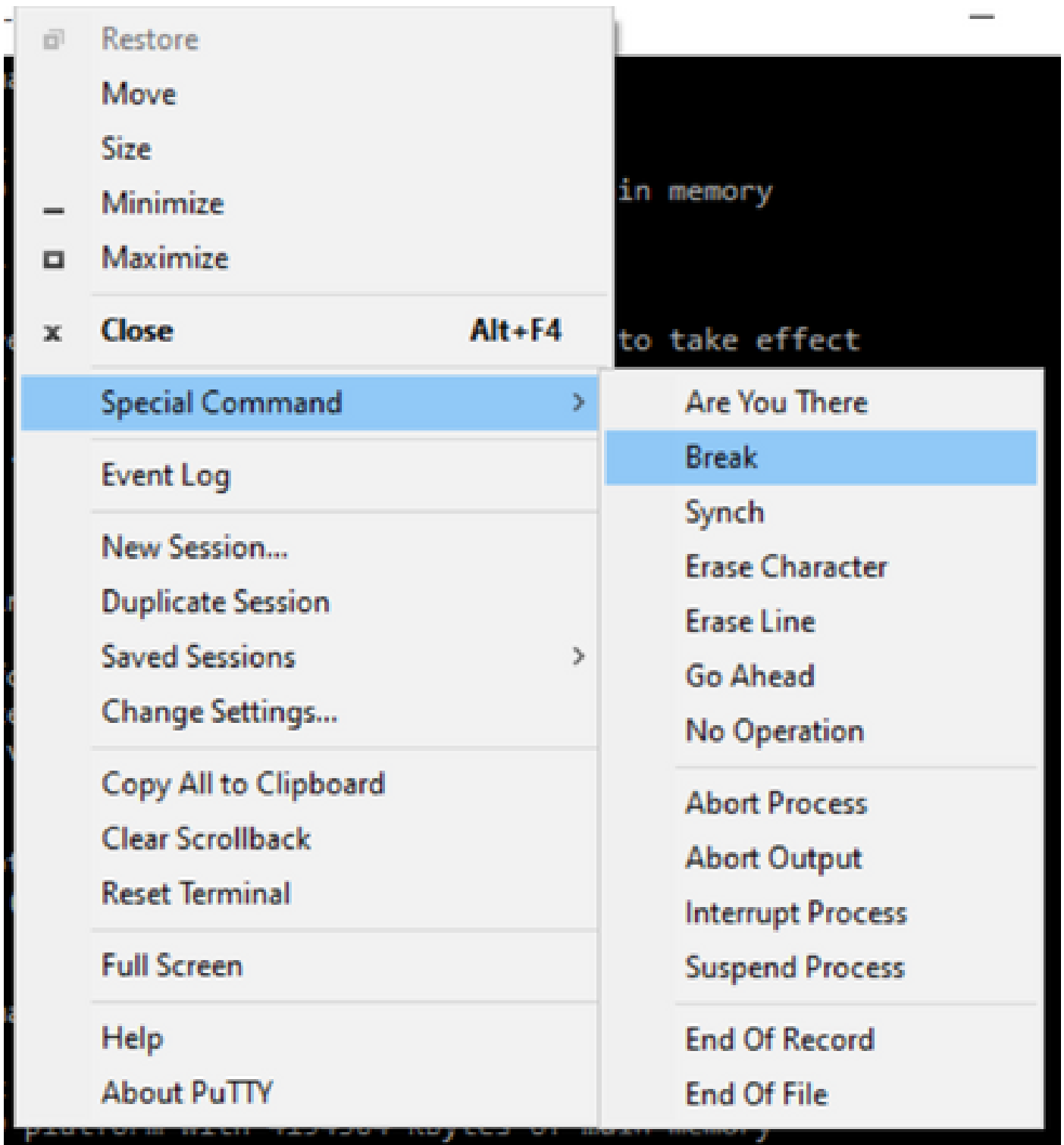
- و ASR1000 و ISR4000 و ISR2000 ءومءمللا نم Cisco تاهجوم يلع ءءتسمللا اءه قبطنبي ISR1000.
- Cisco IOS و Cisco IOS XE تالءاع لءشءت يءللا تاهجوم لل ءي لمعلا ريءت نأ نكمي ءفلءءمللا.
- مءءءلل ءي فرط ءءو ءاءأ يءلءتي يءبني ءنأ، ءءاعتسا ةم لك ءزءنأ in order to ءي صوء.

 ءي لمع ءي فنءل (Telnet أو SSH) زاءءلاب ءعب نع لاصءالا مءءءسا نكمي ال: ءظءالم لءمءء نلف، مءءءللا ءءو لاصءال يفرطال مءءءسا مء اذا. رورملا ءم لك ءءرتسا مءءءللا ءءو ب رءابملا لاصءالاب ي صوي. ءي لمعلا.

- ءءاطلا رءصم ءراءل رفوءللا ءي نءم و اءءاملا زاءءللا يلى لوصولل ءءءل نوكي نأ بءي رءءءملا زاءءلاب صاءءل ءعب نع.
- ل صاف لس لسءء لاس رال يفرط يءءم مءءءسا بءي.

 ءءؤملا فاءي الءاءءم يلع رءوي بمءللا ءزهءأ ءءءافم ءاءول ضعب يوءءء: ءظءالم ءراشال لاس رال مءءءسا نكمي و.





1. دام ريرمت دعب عاطقنالا قرأش إىل ع فرعتال متي .ةددعتم رسك تاراش إلسرت نأ كىل ع .  
ديهمتال ي ف قرشابم Cisco IOS ءاهتنا لبقورشنال

Initializing Hardware ...

Checking for PCIe device presence...done  
System integrity status: 0x610  
Rom image verified correctly

System Bootstrap, Version 16.12(2r), RELEASE SOFTWARE  
Copyright (c) 1994-2019 by cisco Systems, Inc.

Current image running: Boot ROM1

Last reset cause: LocalSoft  
ISR4331/K9 platform with 4194304 Kbytes of main memory

.....  
Located isr4300-universalk9.16.12.04.SPA.bin  
#####

Failed to boot file bootflash:isr4300-universalk9.16.12.04.SPA.bin

.....  
rommon 1 >

يلى ع نيوكتال لجس نيوكت بجي، ROMmon عرض وي ف. زاهجلا لى لوخدلا لجس 3. ةوطخل  
ي.ضارتفالا نيوكتال مادختساب ةللالات لىمحتلا ةداعا ةللمع ي ف ديهمتلا ءارجال 0x2142  
داتعملاك زاهجلا ةمزج كرتت نأ كيلي ع. reset. رمألا مادختساب لىمحتلا ةداعا كنكمي

rommon 1 > confreg 0x2142

You must reset or power cycle for new config to take effect  
rommon 2 > reset

Resetting .....

Initializing Hardware ...

Checking for PCIe device presence...done  
System integrity status: 0x610  
Rom image verified correctly

System Bootstrap, Version 16.12(2r), RELEASE SOFTWARE  
Copyright (c) 1994-2019 by cisco Systems, Inc.

Current image running: Boot ROM1

Last reset cause: LocalSoft  
ISR4331/K9 platform with 4194304 Kbytes of main memory

.....  
Located isr4300-universalk9.16.12.04.SPA.bin  
#####

Package header rev 3 structure detected  
IsoSize = 609173504  
Calculating SHA-1 hash...Validate package: SHA-1 hash:  
calculated 9E1353EB:8A02B6C4:C7B841DC:7A78BA24:5D48AA9B  
expected 9E1353EB:8A02B6C4:C7B841DC:7A78BA24:5D48AA9B  
RSA Signed RELEASE Image Signature Verification Successful.  
Image validated

Restricted Rights Legend

Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) of the Commercial Computer Software - Restricted Rights clause at FAR sec. 52.227-19 and subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS sec. 252.227-7013.

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, California 95134-1706

Cisco IOS Software [Gibraltar], ISR Software (X86\_64\_LINUX\_IOSD-UNIVERSALK9-M), Version 16.12.4, RELEASED FOR FIELD  
Technical Support: <http://www.cisco.com/techsupport>  
Copyright (c) 1986-2020 by Cisco Systems, Inc.  
Compiled Thu 09-Jul-20 21:44 by mcpre

This software version supports only Smart Licensing as the software licensing mechanism.

PLEASE READ THE FOLLOWING TERMS CAREFULLY. INSTALLING THE LICENSE OR LICENSE KEY PROVIDED FOR ANY CISCO SOFTWARE PRODUCT, PRODUCT FEATURE, AND/OR SUBSEQUENTLY PROVIDED SOFTWARE FEATURES (COLLECTIVELY, THE "SOFTWARE"), AND/OR USING SUCH SOFTWARE CONSTITUTES YOUR FULL ACCEPTANCE OF THE FOLLOWING TERMS. YOU MUST NOT PROCEED FURTHER IF YOU ARE NOT WILLING TO BE BOUND BY ALL THE TERMS SET FORTH HEREIN.

Your use of the Software is subject to the Cisco End User License Agreement (EULA) and any relevant supplemental terms (SEULA) found at <http://www.cisco.com/c/en/us/about/legal/cloud-and-software/software-terms.html>.

You hereby acknowledge and agree that certain Software and/or features are licensed for a particular term, that the license to such Software and/or features is valid only for the applicable term and that such Software and/or features may be shut down or otherwise terminated by Cisco after expiration of the applicable license term (for example, 90-day trial period). Cisco reserves the right to terminate any such Software feature electronically or by any other means available. While Cisco may provide alerts, it is your sole responsibility to monitor your usage of any such term Software feature to ensure that your systems and networks are prepared for a shutdown of the Software feature.

All TCP A0 KDF Tests Pass  
cisco ISR4331/K9 (1RU) processor with 1694893K/3071K bytes of memory.  
Processor board ID FLM1922W1BZ  
3 Gigabit Ethernet interfaces  
32768K bytes of non-volatile configuration memory.  
4194304K bytes of physical memory.  
3223551K bytes of flash memory at bootflash:.  
0K bytes of WebUI ODM Files at webui:.

Press RETURN to get started!

خسن عارج بچي. ةطقنل هذه دن ع يضارت فال نيوكتل ال ع هجوم ال يوتحي 4. ةوطخل  
startup-فلم في ن زخم ال نيوكتل مادختس كمل زي، running-config في نيوكتل ل يطايتح  
في running-config ال فلم لا خسن بچي، startup-config فلم مادختس ال. رخآ فلم و  
م اعلا عضول.

1. تانايب ةعجارم/ريغيغتو نيوكتل اعضو ال لاقنت ال كنكمي، اي طايتح خسن درجم بو.

دامت عال.

2. ادعاو تاريخي غتال ظفح كنكمي، كلذ دعب 0x2102 لى نيوكتال لجس ليدعت بجي.  
زاهجال ليغشت

```
Router#copy startup-config running-config
Destination filename [running-config]?
% Please write mem and reload
% The config will take effect on next reboot
```

```
2793 bytes copied in 0.363 secs (7694 bytes/sec)
```

```
Router#show running-config | sec password
enable password cisco
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#enable password cisco123
Router(config)#config-register 0x2102
```

```
Router(config)#exit
Router#show running-config | sec password
enable password cisco123
Router#write
Building configuration...
```

```
[OK]
Router#reload
```

show version رمألا ليغشت كنكمي، يحيص لكشب نيوكتال لجس ليدعت ديكأتل 5 ةوطخال  
show version جارخال نم ريخال رطسال نم ققحتلالو

```
Router#show version
Cisco IOS XE Software, Version 16.12.04
Cisco IOS Software [Gibraltar], ISR Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Version 16.12.4, RELEASED FOR PROD
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2020 by Cisco Systems, Inc.
Compiled Thu 09-Jul-20 21:44 by mcpre
```

```
Cisco IOS-XE software, Copyright (c) 2005-2020 by cisco Systems, Inc.
All rights reserved. Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0. The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY. You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0. For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.
```

```
ROM: 16.12(2r)
```

```
Router uptime is 19 minutes
Uptime for this control processor is 22 minutes
System returned to ROM by Reload Command at 21:14:19 UTC Tue Apr 13 2021
```

System image file is "bootflash:isr4300-universalk9.16.12.04.SPA.bin"  
Last reload reason: Reload Command

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:  
<http://www.cisco.com/wwl/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to [export@cisco.com](mailto:export@cisco.com).

Suite License Information for Module:'esg'

-----  
Suite Suite Current Type Suite Next reboot  
-----

FoundationSuiteK9 None Smart License None  
securityk9  
appxk9

AdvUCSuiteK9 None Smart License None  
uck9  
cme-srst  
cube

Technology Package License Information:

-----  
Technology Technology-package Technology-package  
Current Type Next reboot  
-----

appxk9 appxk9 Smart License appxk9  
uck9 uck9 Smart License uck9  
securityk9 None Smart License None  
ipbase ipbasek9 Smart License ipbasek9

The current throughput level is 300000 kbps

Smart Licensing Status: UNREGISTERED/EVAL MODE

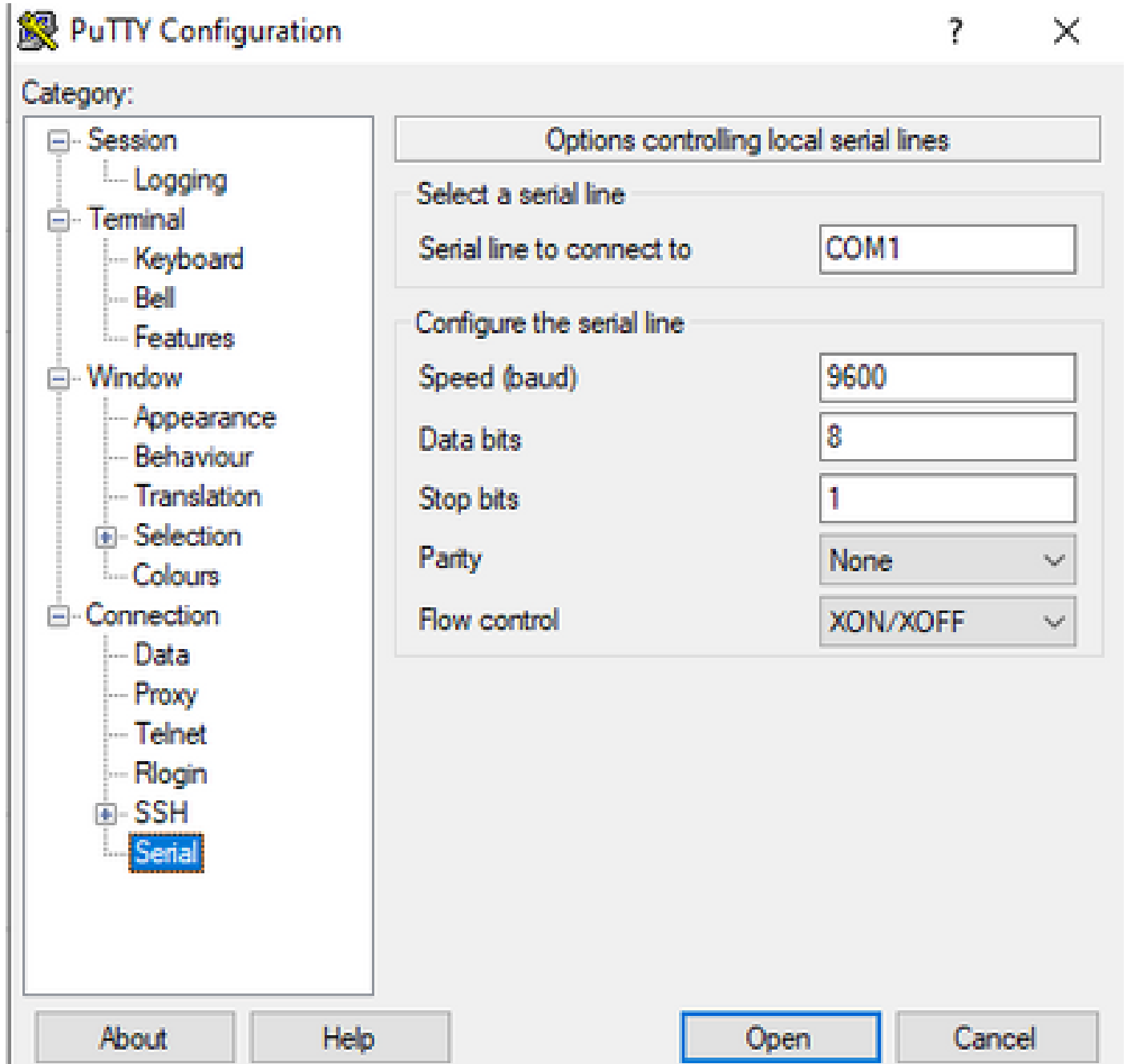
cisco ISR4331/K9 (1RU) processor with 1694893K/3071K bytes of memory.  
Processor board ID FLM1922W1BZ  
3 Gigabit Ethernet interfaces  
32768K bytes of non-volatile configuration memory.  
4194304K bytes of physical memory.  
3223551K bytes of flash memory at bootflash:.  
0K bytes of WebUI ODM Files at webui:.

Configuration register is 0x2142 (will be 0x2102 at next reload)

ةعقوتم ريغ تايكولس فلتخم نيوكت لجس نع جتني نأ نكمي :ةظالم

## عاطقنا ةراشا ةاكاحم

حضورم وه امك PuTTY نيوكت في يضارتفالا مكحتلا ةدحو/ةلسلسلا نيوكت ةعجارم نكمي ةروصلال في.



ةاكاحم كنكمي ف ،هجوملا ةطساوب حيحص لكشب عاطقنالال ةراشا يلع فرعتلا رذعت اذا ةاكاحم ROMmon عضو في لاقتنالال PuTTY عم ةراشالال.

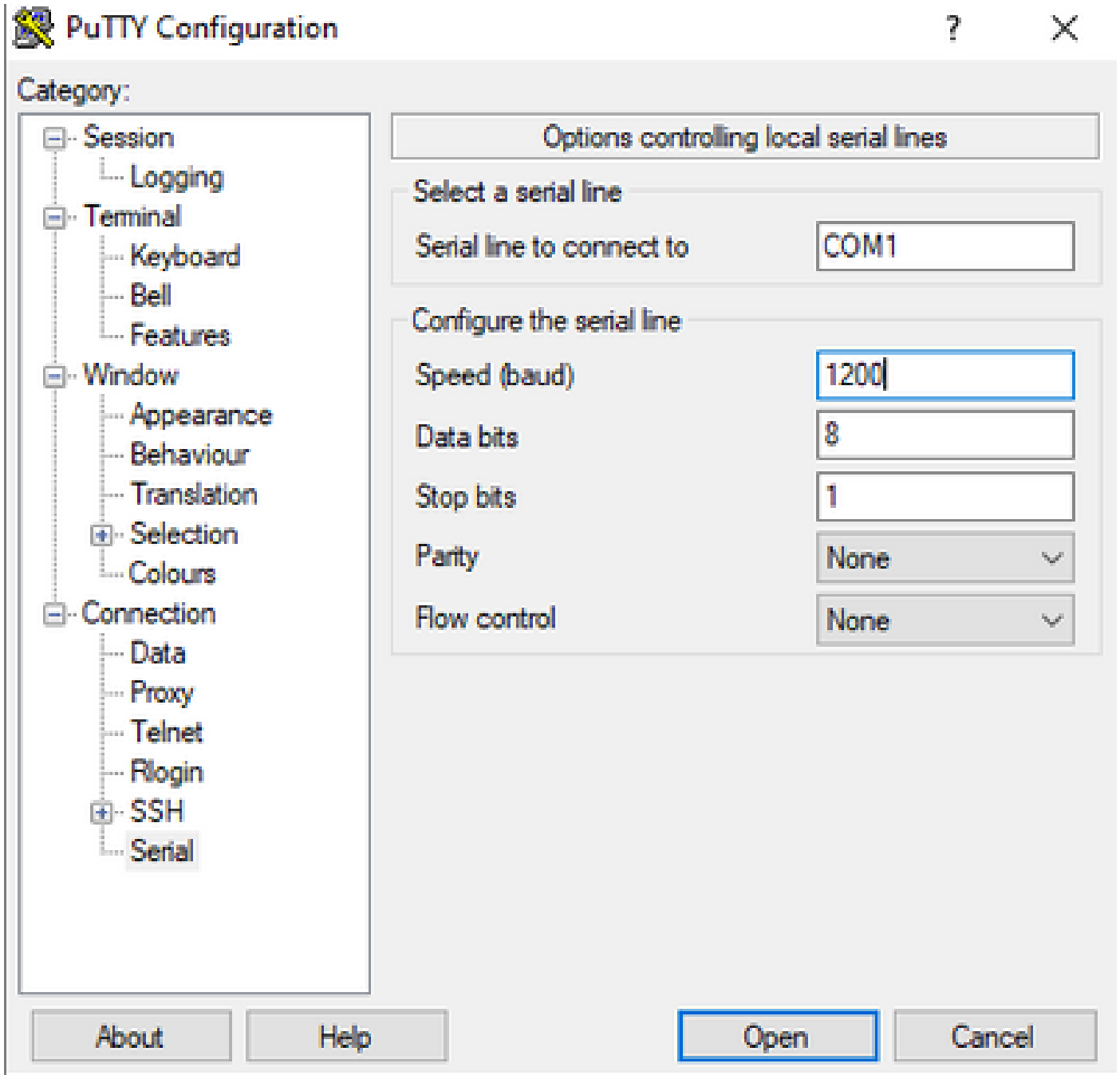
امك مكحتلا ةدحو/ةلسلسلا نيوكت نييعت كي لع بجي ،راسكنالال ةراشا ةاكاحم ل 1 ةوطخلال يلي:

- ةعرسالال : 1200.



- 8: تاناي ب ل ت ب ت ادحو
- 1: ت ب ت ادحو SROP
- ال ب: ل ثام ت ال
- ء. ش ال: ق ف د ت ال ي ف م ك ح ت ال

ة روص ال ي ف ح ض و م وه ام ك ي ل س ل س ت ال ن ي و ك ت ال ا ذه ن ي و ك ت م ت ي



كولس اذه .م ك ح ت ال ة د ح و ن م ج ا ر خ ا ي ا ر ت د ع ت م ل ، ق ب ا س ال ن ي و ك ت ال ا ب ز ا ه ج ال ل ي ص و ت د ر ج م ب ع ق و ت م .

10-15 ة د م ل ة ف ا س م ال ب ي ض ق ح ا ت ف م ي ل ع ط غ ض ل ا و ز ا ه ج ال ة ر و د ل ي غ ش ت ك ي ل ع ب ج ي 2. ة و ط خ ال ه ج و م ال ي ف ع ا ط ق ن ال ا ة ر ا ش ا ء ا ش ن ال ة ي ن ا ث .

ROMmon ه ج و م ة ي ؤ ر ك ن ك م ي ال ك ل ذ ع م و ، ROMmon ع ض و ي ف ه ج و م ال ن و ك ي ، ك ل ذ د ع ب

مكحتلا ةدحوب ىرخأ ةرم لاصتالا لواحو ةضارتفالا ميقلاب PuTTY ةسلج حتفا 3. ةوطخلا  
rommon. ةبلاطم ضرعي

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذه Cisco تچرت  
ملاعلاء انءمچ يف نيمدختسمل معدى وتحم مي دقتل ةيرشبل او  
امك ةقيد نوك تنل ةللأل ةمچرت لصف انءمچم اءمچرئى. ةصاأل مءتبل ب  
Cisco ةلخت. فرتحم مچرت مءم دقئى تلى ةى فارتحال ةمچرتل عم لاعل او  
ىل اءمءاد ةوچرلاب ي صوءو تامچرتل هذه ةقदन ةءىل وئسم Cisco  
Systems (رفوتم طبارل) ىل صأل اءمچرئى لءنل دن تسمل