

Troubleshoot Password Recovery in Cisco IOS and Cisco IOS XE Routers

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Password Recovery in Cisco IOS and Cisco IOS XE Routers](#)

[Simulate a Break Signal](#)


Introduction

This document describes the process to perform a password recovery in Cisco IOS® and Cisco IOS® XE Routers.


Prerequisites

Requirements

- This document applies to Cisco routers from the family ISRG2, ISR4000, ASR1000 and ISR1000. The process can change for routers running different Cisco IOS and Cisco IOS XE families.
- In order to perform a password recovery, you must have device console connection.

 **Note:** Remote connection to the device (SSH or Telnet) cannot be used to perform the password recovery process. If terminal server is used for console connection, the process cannot work. Direct console connection is recommended.

- You must have physical device access or availability to manage remotely the power source of the affected device.
- You must use a Terminal Emulator in order to send a break sequence.

 **Note:** Some PC keyboards have the break key, it can be used to send the signal.

Components Used

The information in this document is based on these software and hardware versions:

- Router ISR4331 running Cisco IOS XE 16.12.4
- Putty terminal session release 0.71

The information in this document was created from the devices in a specific lab environment. All of the

devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.


Background Information

This steps can be used to recover username and password credentials, as well as enable password. In base on the current device configuration, the password can be extracted or just replaced with a new one.

Cisco IOS and Cisco IOS XE Routers save the configuration in startup-config and running-config.

By default, the startup-config files are stored in the NVRAM and the running-config (actual device configuration) is stored in the DRAM.

The main purpose of the password recovery process is to boot the device with a default configuration, and once there is access to the device, load the current configuration and change the credentials.

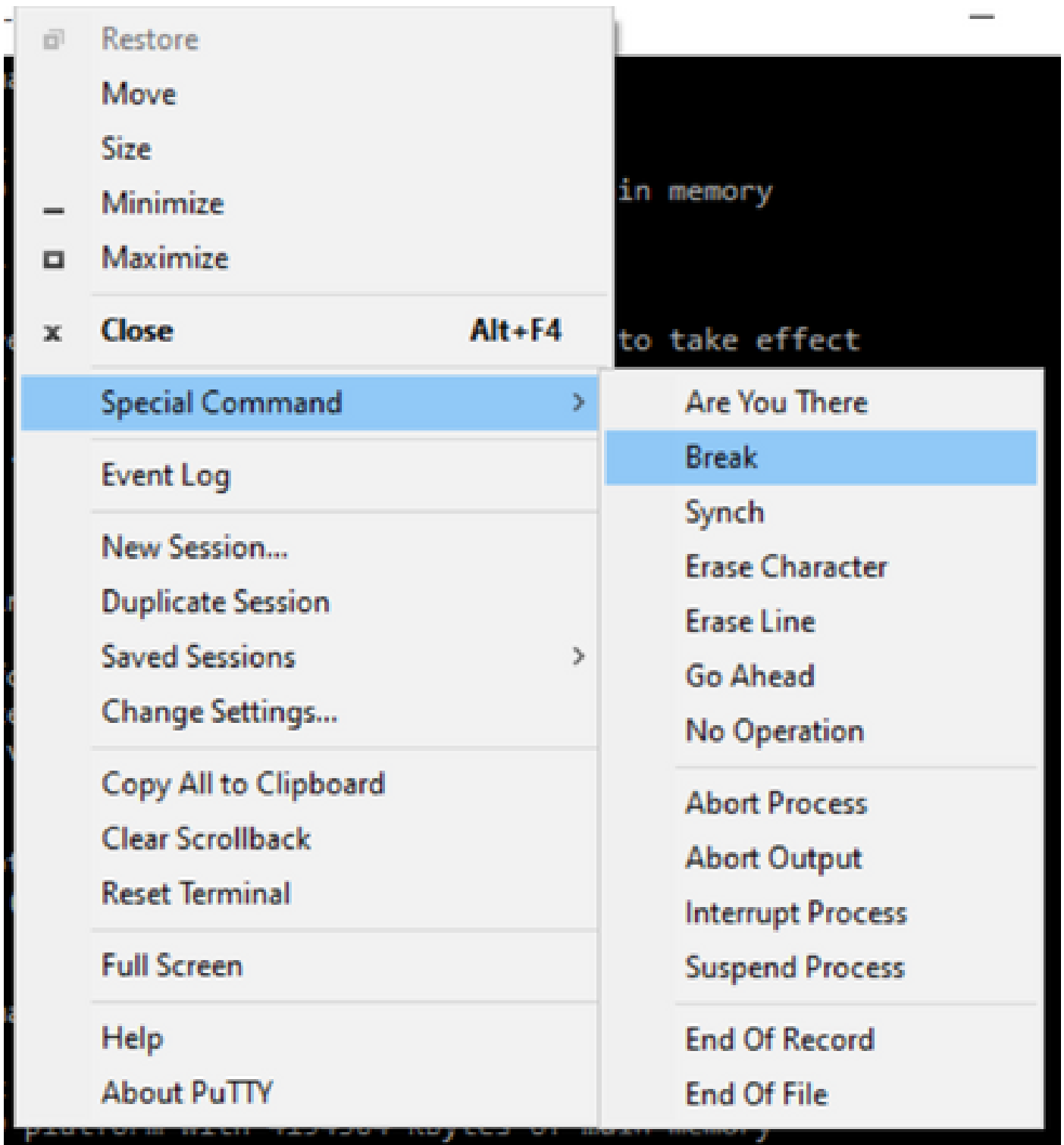
 **Note:** In case the router is configured with no service password-recovery feature, the password recovery can not be done. This configuration can be identified while the device is booting. You can review this document in order to get additional details regarding [No Service Password-Recovery](#) feature.

Password Recovery in Cisco IOS and Cisco IOS XE Routers

Step 1. Reboot the device. You are required to reboot the device from the power source/switch as you do not have access to the device via command line.

Step 2. While the device is booting, you have to issue the break sequence.

In the case of Putty, navigate to **Special Command > Break** option, as shown in the image.



1. You have to send multiple break signals. The break signal is recognized after the POST is passed and just before the Cisco IOS finishes to boot:

```
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 >

Step 3. Log in to device. In rommon mode, you have to configure the configuration register to 0x2142 in order to boot in the next reload with the default configuration.
You can reload with the **reset** command. You have to leave the device boots as usual.

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!

Step 4. The router has the default configuration at this point. You must backup the configuration in the running-config, you need to use the configuration stored in the startup-config file or another file. In order to use the startup-config file, you have to copy the file to the running-config in global mode.

1. Once it is backed up, you can move to the configuration mode and change/review the credentials.
2. The configuration register has to be modified to 0x2102. After this, you can save the changes and reboot the device.

```
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
```

Step 5. In order confirm the configuration register is correctly modified, you can run **show version** command and check the last line from the **show version** output.

```
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 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
```

```
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.

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

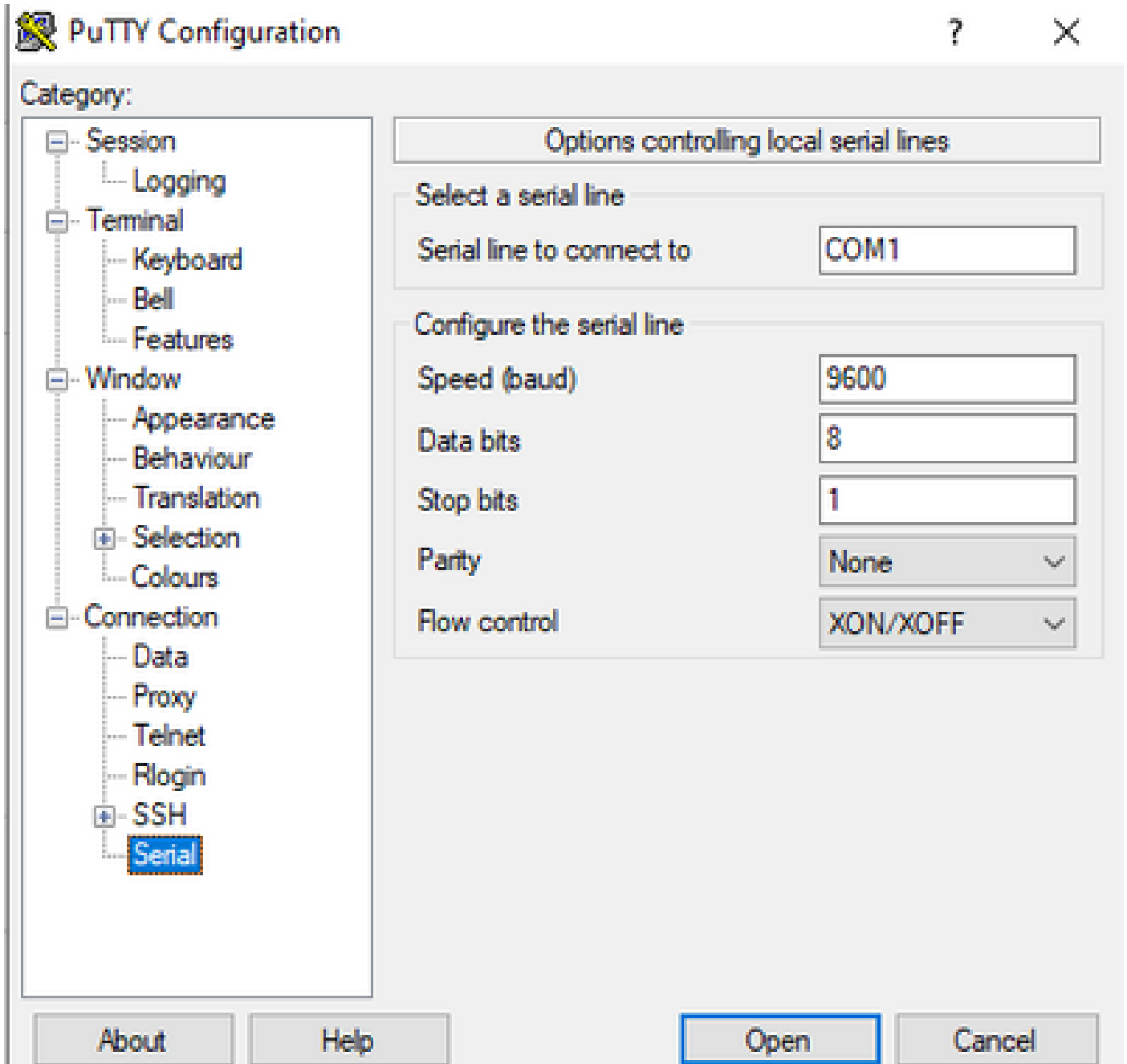
cisco ISR4331/K9 (1RU) processor with 1694893K/3071K bytes of memory.
Processor board ID FLM1922W1BZ
3 Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
3223551K bytes of flash memory at bootflash:.
0K bytes of WebUI ODM Files at webui:.

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

 **Note:** A different configuration register can produce unexpected behaviors.

Simulate a Break Signal

The default serial/console configuration can be reviewed in Putty configuration as shown in the image.

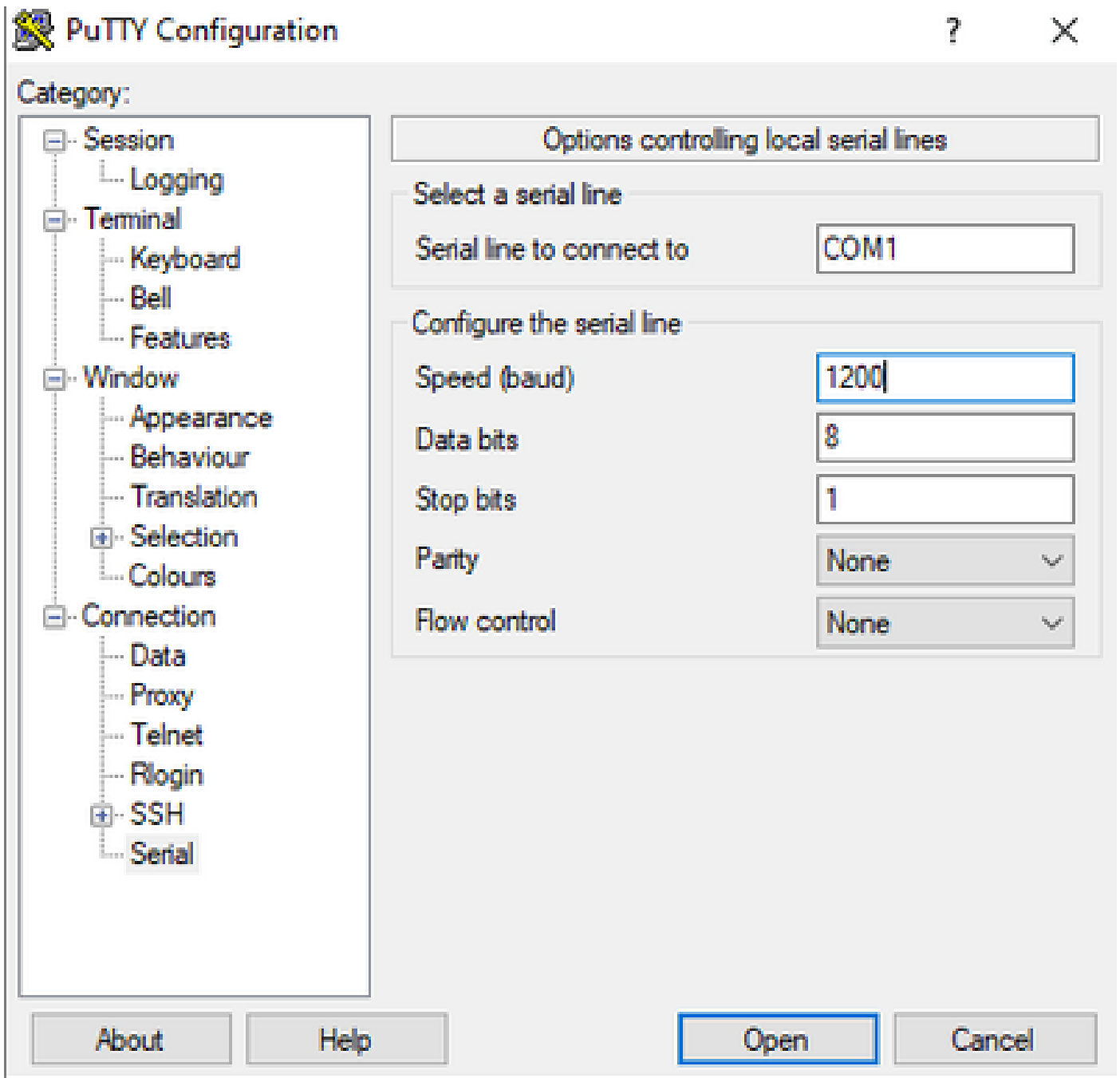


If the break signal cannot be properly recognized by the router, you can simulate the signal with Putty in order to go in rommon mode.

Step 1. In order to simulate the break signal, you have to set the serial/console configuration as follows:

- Speed: 1200.
- Data bits: 8.
- Srop bits: 1.
- Parity: none.
- Flow control: none.

This Serial configuration is configured as shown in the image.



Once you connect the device with the previous configuration, you no longer see any output from the console. This is an expected behavior.

Step 2. You have to power cycle the device and press the **spacebar key** for 10-15 seconds in order to generate the break signal in the router.

After that, the router is in rommon mode, however you are not able to see the rommon prompt.

Step 3. Open the Putty session with the default values and try to connect again to the console. It shows the **rommon** prompt.