

Out of Band Site Management with ISR LTE via Console, Telnet, HTTP

For All Verizon Wireless LTE Services

Revision 1.3

November 2014

Overview

Out-of-band management has long been used to access a remote site or device, as a way to monitor, restore service or determine an issue affecting service. In the past, the most popular method of out-of-band access was the PSTN (Public Switched Telephone Network), via analog POTS lines (Plain Old Telephone Service) or ISDN lines (Integrated Switched Digital Network). Dial-up modems or ISDN equipment attached to remote site devices would accept incoming calls from an administrator at the main site. These lines are still in common use today.

The PSTN lines were sometimes also used to support backup to the primary WAN path.

The challenges of using the PSTN for out-of-band and backup WAN include:

- Aging modem or ISDN hardware, often unchecked until needed
- Slow speeds (9.6-53.3 or 64-128 kbps) affect response time and the ability to download patches, upload logs, or support user traffic if used as the active WAN path
- High costs include monthly recurring charges and potential additional usage costs
- Physical cabling may be run alongside primary WAN cabling; a break may affect both.
- Vulnerable to hacking attacks from the PSTN (public network)

4G LTE is an option for out-of-band management and backup WAN function, and can provide an improved solution for remote sites. LTE Advantages for these functions include:

- Multi-megabit speeds, providing improved response and transfer times
- LTE plans are flexibly priced, allowing for lower cost (low byte plans for out-of-band only), or similar cost with greater performance (multi-GB plans for out-of-band and WAN backup, generally 100x faster).
- Wireless connection provides protection against physical cable plant outages (e.g. the “backhoe disconnect”)
- Traditional IP security methods can be applied, in addition to using a Mobile Private Network service (separates the LTE connection from the public network)

The Router Best Practices for LTE Guide (under “Real World Examples” section) includes additional uses and links to available apps for ISRs with LTE. Below is a link to the guide.

www.cisco.com/c/dam/en/us/td/docs/routers/access/interfaces/software/deployment/guide/lte_access_011414.pdf

WAN Backup with LTE

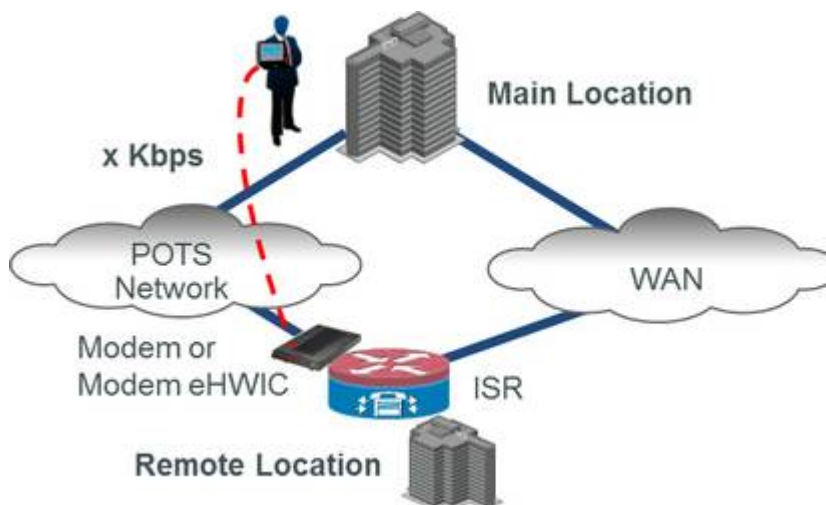
This configuration guide is focused on Out-of-Band access with LTE. Although use cases will include WAN backup, no backup configurations will be detailed. Configuration guides are available for using LTE as backup for Verizon Mobile Private Network and public network services, available at the link below under “Verizon LTE Deployment Guides for Cisco 4G LTE ISR 819/1900/2900/3900”.

www.cisco.com/c/en/us/support/interfaces-modules/high-speed-wan-interface-cards/products-installation-and-configuration-guides-list.html

Traditional Out-of-Band Access with PSTN

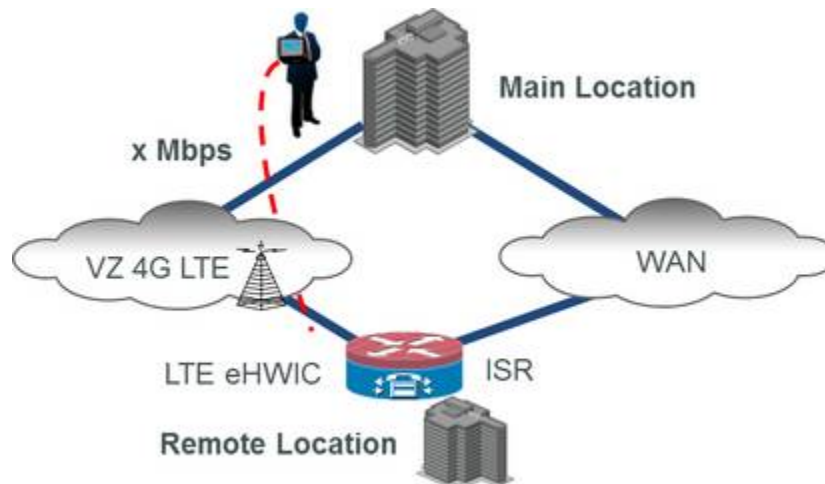
In order to provide a management path that does not depend on or affect the data path, organizations deploy out-of-band management access to remote sites. In the past this was done by installing a PSTN line along with a modem at the remote site router. The modem can be external, or embedded in the Cisco ISR router with a module (HWIC or eHWIC).

By using a PC with dial-up function or a dial-out terminal server at the main site, an administrator can gain access to a command line interface on the remote site router. In addition to troubleshooting and recovering (if needed) the router, an administrator can also access other equipment at the remote site (by either a Telnet or SSH session, or by serial connection if the remote site router has been appropriately configured). Below is a diagram representing traditional out-of-band access via the PSTN.



Out-of-Band Access with LTE

With the ubiquity and pricing of cellular wireless services and equipment, LTE offers an improved out-of-band management option compared to the PSTN. Greatly increased speed, quick provisioning, easy moves, and alternate access methods (such as SMS) make LTE a compelling option. Below is a diagram representing out-of-band access via LTE.



For new deployments, LTE is a compelling choice for out-of-band management. For existing deployments, LTE offers an opportunity to update equipment, reduce line charges, and greatly improve performance. The improved performance allows for:

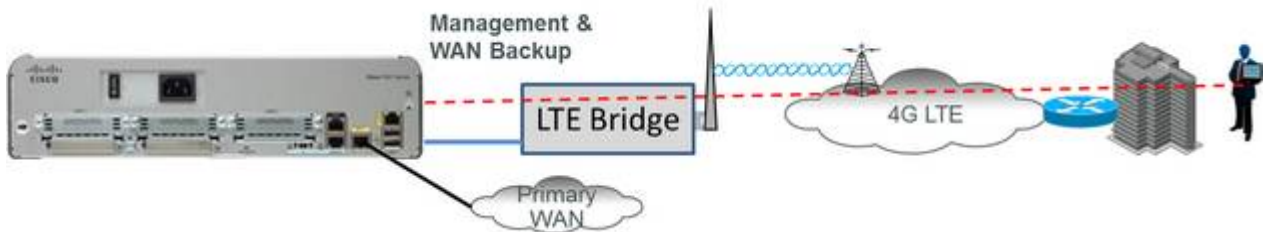
- Faster response to/from the device for management
- As the LTE connection is high performance IP versus serial/Async, Telnet, SSH, HTTP, HTTPS and API access are available, greatly expanding management options
- Log files and IOS images can be transferred more quickly to/from the managed ISR
- As the LTE connection can be a routed path, access to other remote site equipment is enhanced, including the ability to transfer log file and images to/from other devices.

LTE access can be terminated at the remote ISR in 3 ways.

The first option uses an external LTE device, connected to the ISR via Ethernet. The advantages and considerations include:

- Allows placement away from the ISR, for best reception, with inexpensive cabling
- Can be used with an older ISR, which may not have an integrated LTE module option
- It's another device to manage, which may not have the same LTE interface or debugging ability as an ISR
- Under normal operating conditions, the ISR is not aware of the state of LTE upstream of the external device. This may be important if LTE is also used as the backup path
- The device may not provide redundancy for the remote site ISR (HSRP, VRRP); if it has this ability, features needed to become the primary router may be missing.

Below is a diagram representing out-of-band LTE via external device.



The second option uses an ISR integrated LTE interface. The advantages and considerations include:

- LTE functions such as LTE monitoring, debugging, alerting and tuning are fully integrated into the ISR. LTE is simply another ISR interface
- A single remote device; no additional device to cable, configure, manage and separately cover under maintenance contracts.
- Capabilities such as advanced routing, automation, site surveys, location based services, geo-fencing, LTE QoS, etc. are already available or feasible.
- Antenna placement via extension cables have a higher cost due to low loss RF cables (various LTE antennas and cables are available as standard ISR SKUs)
- Cannot be supported with older Cisco ISRs (1800, 2800, 3800 series). Note that these older models were released 9 years ago, and are end-of-sale and soon end-of-support, with improved replacement models available (1900, 2900, 3900 series).

Below is a diagram representing out-of-band LTE via ISR integrated/embedded LTE.

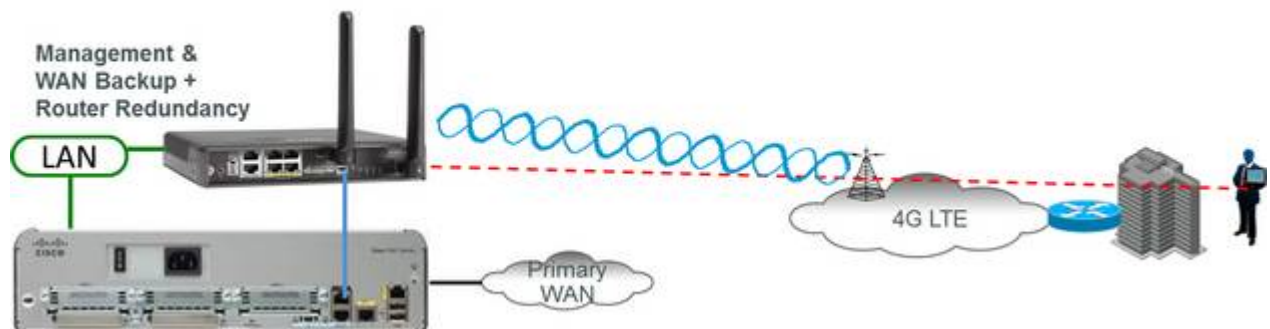


The third option combines the advantages of an ISR integrated LTE interface with an external device that provides for full redundancy of the primary ISR. The existing ISR remains in place with an 819G-4G ISR added. The 819 is a small, low cost, high function, fixed port ISR with embedded LTE and serial port.

The 819's built-in serial port is connected to the AUX or console port of the primary ISR for out-of-band management. Both the primary ISR and the 819 can be configured for router redundancy using either HSRP or VRRP. This provides out-of-band management WAN backup and full router redundancy, offering higher availability compared to the previous options. The advantages and considerations include:

- Allows for placement away from the primary ISR, where reception is best, with inexpensive cabling. There is an available splitter to allow power to the 819 over the Ethernet cable.
- Can be used with an older ISR, which may not have an integrated LTE module option
- It's another device to manage, but provides the same interface and routing, QoS, and programmability features as modular ISRs
- The 819 is aware of the detailed state of the LTE connection. This may be important if LTE is also used as the backup path; tuning and debugging are available the same as with an LTE eHWIC in a modular ISR
- The 819 can also provide router redundancy for the remote site (HSRP, VRRP)
- Cost is higher than an external LTE bridge or LTE eHWIC, weighed along with its ability to provide redundancy for the primary router, improved diagnostics and debugging, and programmability

Below is a diagram representing out-of-band LTE via 819G-4G ISR alongside an existing ISR.



Out-of-Band Management with LTE: Configuration

Option 1 (external LTE bridge):

This configuration is dependent on the non-Cisco equipment used for the bridge, and is not documented in this guide.

Option 2 (ISR integrated LTE):

This option does not require special configuration for out-of-band, as LTE access is direct to the ISR. LTE Configuration guides are available here:

www.cisco.com/c/en/us/support/interfaces-modules/high-speed-wan-interface-cards/products-installation-and-configuration-guides-list.html

Option 3 (819G-4G ISR for out-of-band management and router redundancy):

The out-of-band configuration is provided for two scenarios below. The LTE configuration is not included, as it is provided in documents available at the link above.

For both the following scenarios, appropriate console cabling is required. The cable between the 819 smart serial port and the primary WAN router console port is SKU CAB-SS-RJ45=. This cable is shown below.

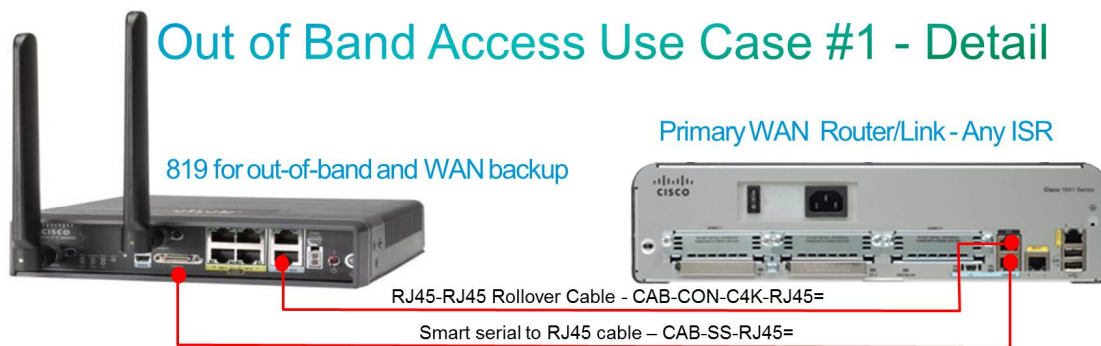


The console cable between the 819 RJ45 console port and the console or AUX port of the primary router or switch is part no. CAB-CON-C4K-RJ45=. This cable is shown below.



Option 3 - First Scenario:

The first scenario allows the 819 to provide out-of-band management for the primary ISR and for the primary ISR to provide out-of-band management for the 819. If the primary ISR becomes unreachable via the primary WAN link, it can be reached from the 819 via LTE. And if the 819 becomes unreachable via the LTE connection, it can be reached from the primary WAN. Thus both WAN and out-of-band management are fully redundant. Along with a router redundancy configuration, this provides higher availability as both the WAN links and routers are redundant. The first scenario is depicted below.



The smart serial port of the 819 is connected to the console port of the primary router. This provides the out-of-band access to the primary router via the 819 with LTE. The AUX port of the primary router is connected to the console port of the 819.

Configuration for the 819:

```

### The next stanzas provide console access to the primary router
### by telnetting to a local interface of the 819 with port number of 2007
### e.g. with a loopback address of 10.0.0.1, "telnet 10.0.0.1 2007" and hit <enter>
### AAA should be defined for userid/password prompt on all interfaces supporting CLI
### this example uses locally defined userid and password
Username <theusername> privilege 15 secret <thepassword>
### Enables the serial interface and create a line for console access
interface serial 0
  physical-layer async
  no ip address
  encapsulation slip
### Enables outbound console access from the line created by the serial commands
line 7
  transport input telnet
### Allows inbound console access. Default timeout is 10 minutes
line con 0
  login local
  no modem enable
##### Provides for telnet access to the 819 via the LTE connection
line vty 0 4
  login local
  
```


Configuration for the primary ISR:

```

### The next stanzas provide inbound console access and outbound console access to the 819
### by telnetting to a local interface of the primary ISR with port number of 2001 (AUX port)
### e.g. with a loopback address of 10.0.0.1, "telnet 10.0.0.1 2001" and hit <enter>
### AAA should be defined for userid/password prompt on all interfaces supporting CLI
### this example uses locally defined userid and password
Username <theusername> privilege 15 secret <thepassword>
## Allows inbound console access. Default timeout is 10 minutes
### Additional commands can provide timeout and security options
line con 0
  login local
  no modem enable
### Enables outbound console access from the AUX port of a modular ISR
line aux 0
  transport input telnet
  telnet transparent
  
```

Sample Operation of Bidirectional Console Access – 819 to Primary Router:

Connecting to a device’s console from the console session of an intermediate device is called “reverse telnet”. The scenario below entails accessing the 819 via Telnet over LTE. Once on the 819 command line interface, access to the primary router console is accomplished via an internal Telnet session from the 819 to itself using the port number for the serial port (the port number is the line number of 7 + 2000).

```

C819V_pod1#sh ver | i IOS
Cisco IOS Software, C800 Software (C800-UNIVERSALK9-M), Version 15.4(3)M, RELEASE SOFTWARE (fc1)
  
```

```

C819V_pod1#sh run int s0
Building configuration...
  
```

```

Current configuration : 82 bytes
!
interface Serial0
  physical-layer async
  no ip address
  encapsulation slip
end
  
```

```

C819V_pod1#sh run | s line
line con 0
  login local
  no modem enable
line aux 0
line 2
  no activation-character
  no exec
  transport preferred none
  transport input all
  stopbits 1
  
```

```

line 3
 script dialer LTE
 modem InOut
 no exec
 transport input all
 transport output all
 rxspeed 100000000
 txspeed 50000000
line 7
 transport input telnet
 transport output none
 stopbits 1
line vty 0 4
 login local
 length 0
 transport input all

```

C819V_pod1#**sh line**

	Tty	Typ	Tx/Rx	A	Modem	Roty	AccO	AccI	Uses	Noise	Overruns	Int
	0	CTY		-	-	-	-	-	0	0	0/0	-
	1	AUX	0/0	-	-	-	-	-	0	0	0/0	-
	2	TTY	9600/9600	-	-	-	-	-	0	0	0/0	-
A	3	TTY		-	inout	-	-	-	0	0	0/0	Ce0
	7	TTY	9600/9600	-	-	-	-	-	0	0	0/0	Se0
*	10	VTY		-	-	-	-	-	1	0	0/0	-
	11	VTY		-	-	-	-	-	0	0	0/0	-
	12	VTY		-	-	-	-	-	0	0	0/0	-
	13	VTY		-	-	-	-	-	0	0	0/0	-
	14	VTY		-	-	-	-	-	0	0	0/0	-

Line(s) not in async mode -or- with no hardware support:
4-6, 8-9

C819V_pod1#**sh ip int brie | i Lo**

```

Loopback100          10.0.0.11          YES NVRAM  up          up

```

C819V_pod1#

C819V_pod1#**clear line 7**

[confirm]

[OK]

C819V_pod1#**telnet 10.0.0.11 2007**

Trying 10.0.0.11, 2007 ... Open

User Access Verification

Username: **cisco**

Password:

C2911#

C2911#

C2911#

C2911#

<< console access is now on the primary router>>

<<to return the interface to the 819 console...>>

<<hold down the 3 keys "control-shift-6" together, then release and type "x" >>

```

<<commands can now be entered for the 819.>>
<<If just <enter> is hit, console access to the primary router returns>>
<<to end the (reverse Telnet) console session, after "control-shift-6 x" type "disconnect" >>
C819V_pod1#disconnect
Closing connection to 10.0.0.11 [confirm]
C819V_pod1#
C819V_pod1#

```

Sample Operation of Bidirectional Console Access – Primary Router to 819:

Connecting to a device’s console from the console session of an intermediate device is called “reverse telnet”. The scenario below entails accessing the primary router via Telnet over the primary WAN connection or the LAN. Once on the primary router’s command line interface, access to the 819 console is accomplished via an internal Telnet session from the primary router to itself using the port number for the AUX port (the port number is the line number of 1 + 2000).

```

C2911#sh ver | i IOS
Cisco IOS Software, C2900 Software (C2900-UNIVERSALK9-M), Version 15.1(4)M2, RELEASE SOFTWARE (fc1)
C2911#
C2911#sh run | s line
line con 0
  login local
line aux 0
  no exec
  transport input telnet
  telnet transparent
line 2
  no activation-character
  no exec
  transport preferred none
  transport input all
  transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
  stopbits 1
line vty 0 4
  login
  transport input all
C2911#
C2911#sh ip int brie
Interface                IP-Address      OK? Method Status          Protocol
Embedded-Service-Engine0/0 unassigned      YES unset    administratively down down
GigabitEthernet0/0       unassigned      YES unset    administratively down down
GigabitEthernet0/1       unassigned      YES unset    administratively down down
GigabitEthernet0/2       unassigned      YES unset    administratively down down
Loopback1                1.2.3.4         YES manual  up              up
C2911#
C2911#sh line
  Tty Line Typ      Tx/Rx    A Modem  Roty Acc0 AccI  Uses  Noise Overruns  Int
*   0   0 CTY          - -      - -      - -    0     0     0/0     -
    1   1 AUX      9600/9600 - -      - -      - -    0     0     0/0     -
    2   2 TTY      9600/9600 - -      - -      - -    0     0     0/0     -
  388 388 VTY          - -      - -      - -    0     0     0/0     -

```

389	389	VTY	-	-	-	-	-	0	0	0/0	-
390	390	VTY	-	-	-	-	-	0	0	0/0	-
391	391	VTY	-	-	-	-	-	0	0	0/0	-
392	392	VTY	-	-	-	-	-	0	0	0/0	-

Line(s) not in async mode -or- with no hardware support:
3-387

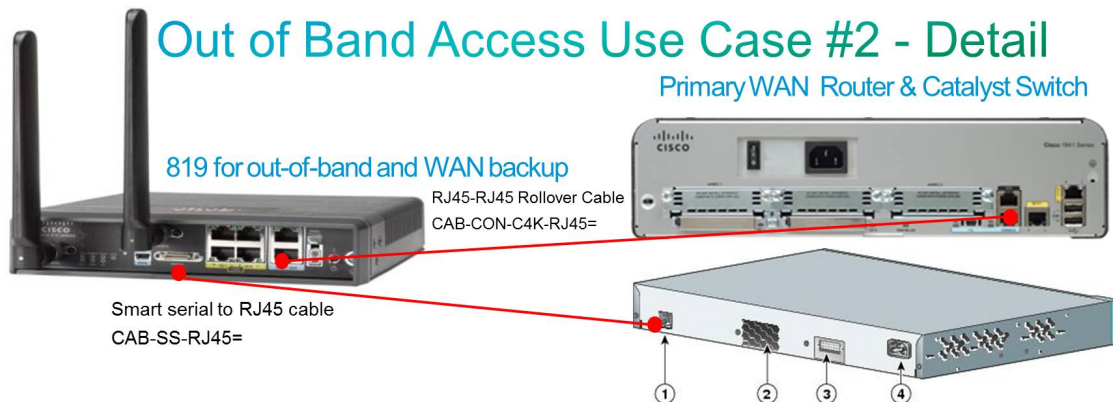
```
C2911#clear line 1
[confirm]
[OK]
C2911#telnet 1.2.3.4 2001
Trying 1.2.3.4, 2001 ... Open
```

User Access Verification

```
Username: cisco
Password:
C819V_pod1#
C819V_pod1#
C819V_pod1#
<< console access is now on the 819>>
<<to return the interface to the primary router console>>
<<hold down the 3 keys "control-shift-6" together, then release and type "x" >>
<<commands can now be entered for the primary router>>
<<If just <enter> is hit, console access to the 819 returns>>
<<to end the (reverse Telnet) console session, after "control-shift-6 x" type "disconnect" >>
C2911#disconnect
Closing connection to 1.2.3.4 [confirm]
C2911#
```

Option 3 - Second Scenario (819 Supporting console access to two devices):

The second scenario allows the 819 to provide out-of-band management for the primary ISR and for a second device (in this case the site Ethernet switch). If the primary ISR becomes unreachable from the primary WAN, it along with the Ethernet switch can be reached can be reached from the 819 via LTE. The second scenario is depicted below.



Configuration for the 819:

```

#### The next 3 stanzas provide console access from the 819 to the primary router and switch
#### by telnetting to a local interface of the 819 with port number 2007 (router access)
#### and by telnetting to a local interface of the 819 with port number 2001 (switch access)
#### e.g. with a loopback address of 10.0.0.1, "telnet 10.0.0.1 2001" and hit <enter>
#### AAA should be defined for userid/password prompt on all interfaces supporting CLI
#### this example uses locally defined userid and password
Username <theusername> privilege 15 secret <thepassword>
#### Enables the serial interface and creates a line for console access interface serial 0
physical-layer async
no ip address
encapsulation slip
#### Enables outbound console access from the line created by the serial commands
line 7
transport input telnet
#### Enables console port to support the AUX port function (819 has no physical AUX port)
line con 0
login local
modem enable
#### Enables outbound console access from the virtual AUX port
line aux 0
transport input telnet
telnet transparent
#### Provides for telnet access to the 819 via the LTE connection
line vty 0 4
login local
    
```

Configuration for the primary ISR or Switch:

```
### Provides console access into the primary ISR or switch from the 819
### This is the standard configuration for console access
### Additional commands can provide timeout and security options
line con 0
  login local
  no modem enable
```

Sample Operation of Bidirectional Console Access – 819 to Primary Router or Switch:

Connecting to a device’s console from the console session of an intermediate device is called “reverse telnet”. The scenario below entails accessing the 819 via Telnet over LTE and then:

- access to the primary router console is accomplished via an internal Telnet session from the 819 to itself using the port number for the serial port (the port number is the line number of 7 + 2000)
- access to the primary switch console is accomplished via an internal Telnet session from the 819 to itself using the port number for the virtual AUX port (the port number is the line number of 1 + 2000)
- The second console interface can be used for devices other than a switch, such as a secondary router or other network equipment with a serial/async console port

<<The 819 configuration lines for interface serial 0, line 7, and line vty 0-4 are identical to the first <<option but still shown below for completeness. The changed or added lines are in bold>>

```
C819V_pod1#sh ver | i IOS
```

```
Cisco IOS Software, C800 Software (C800-UNIVERSALK9-M), Version 15.4(3)M, RELEASE SOFTWARE (fc1)
```

```
C819V_pod1#sh run int s0
```

```
Building configuration...
```

```
Current configuration : 82 bytes
```

```
!
interface Serial0
  physical-layer async
  no ip address
  encapsulation slip
end
```

```
C819V_pod1#sh run | s line
```

```
line con 0
  login local
  modem enable
line aux 0
  transport input telnet
  transport output none
  telnet transparent
line 2
  no activation-character
  no exec
  transport preferred none
  transport input all
  stopbits 1
```

```

line 3
 script dialer LTE
 modem InOut
 no exec
 transport input all
 transport output all
 rxspeed 100000000
 txspeed 50000000
line 7
 transport input telnet
 transport output none
 stopbits 1
line vty 0 4
 login local
 length 0
 transport input all

```

C819V_pod1#sh line

Tty	Typ	Tx/Rx	A	Modem	Roty	AccO	AccI	Uses	Noise	Overruns	Int
0	CTY		-	-	-	-	-	0	0	0/0	-
1	AUX	0/0	-	-	-	-	-	0	0	0/0	-
2	TTY	9600/9600	-	-	-	-	-	0	0	0/0	-
A 3	TTY		-	inout	-	-	-	0	0	0/0	Ce0
7	TTY	9600/9600	-	-	-	-	-	0	0	0/0	Se0
* 10	VTY		-	-	-	-	-	1	0	0/0	-
11	VTY		-	-	-	-	-	0	0	0/0	-
12	VTY		-	-	-	-	-	0	0	0/0	-
13	VTY		-	-	-	-	-	0	0	0/0	-
14	VTY		-	-	-	-	-	0	0	0/0	-

C819V_pod1#sh ip int brie | i Lo

```

Loopback100          10.0.0.11          YES NVRAM  up          up
C819V_pod1#

```

<<the example for reverse Telnet to the primary router via the serial interface is identical to the>>
 <<first scenario and omitted here>>

```

C819V_pod1#telnet 10.0.0.11 2001
Trying 10.0.0.11, 2001 ... Open

```

```

CAT2960#
CAT2960#
CAT2960#

```

<<there was no prompt for password when the session was opened as the previous console session was not>>
 <<closed by logging out, and the session was reopened before the session timed out (10 minute default)>>
 << console access is now on the primary switch. to return the interface to the 819 console>>
 <<hold down the 3 keys "control-shift-6" together, then release and type "x" >>
 <<commands can now be entered for the 819.>>

C819V_pod1#disconnect

```

Closing connection to 10.0.0.11 [confirm]
C819V_pod1#

```