

Connecting External Encryption Equipment (KG-194, KV-19) to NM-4T, PA-4T+, PA-8T, and FSIP Cisco Serial Interfaces

Document ID: 14097

Contents

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Cables

- Red Cable – Cable Pinout Option 1
- Red Cable – Cable Pinout Option 2
- Red Cable – Cable Pinout Option 3
- Black Cable – Cable Pinout

Testing Results

Related Information

Introduction

This document contains configuration and resolution information about connecting external encryption equipment (crypto) to Cisco 36xx/NM-4T, Cisco 72xx/PA-4T+, and Cisco 75xx/PA-4T+/PA-8T serial interfaces. When you use Cisco IOS® Software Release 11.2(x) and later with the Fast Serial Interface Processor (FSIP) on the 75xx router platform, as well as the NM-4T, PA-4T+, and PA-8T on any hardware platform, the crypto equipment, while connected to any of the stated Cisco hardware combinations, could fail to successfully establish synchronization after a circuit interruption or an equipment reset. The only option is to remove the **pulse-time x** command. This command controls how data terminal ready (DTR) functions on the serial interface. Also, in some instances, on the Cisco 75xx platform, the router has to be reloaded. Since hardware configurations vary according to customer-specific security requirements, different EIA-530 cabling pinouts are used. These different wiring combinations have caused different variations of the problem, which results in several Cisco bugs being opened.

Cisco Bug ID	Description
CSCds44777 (registered customers only)	Cisco 7500: PA-4T+, PA-8T, and FSIP glitch Request to Send (RTS).
CSCds26771 (registered customers only)	Cisco 7000: RSP-3-RESTART when the pulse-time command is set.
CSCds36893 (registered customers only)	Cisco 7200: If DTR pulse is turned on. PA-4T+ RTS goes full low correspondingly.
CSCdr96683 (registered customers only)	Cisco 7000: RTS signal dropped in duration of pulse time.

CSCdk74881 (registered customers only)	Cisco 3600: RTS tied to DCD prevents DTR pulse.
CSCdr41395 (registered customers only)	Cisco 3600: If DTR pulse is turned on NM-4T RTS goes full low correspondingly.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Cables

Customers who typically experience this problem use EIA-530 cables to interconnect their crypto equipment to the Cisco NM-4T, PA-4T+, and PA-8T serial interfaces. This section describes the cables necessary to connect the KG-194 and KIV-19, using the Pulse Engineering Cryptographic Equipment Enclosure, to the Cisco serial interfaces previously mentioned in this document. Due to customer specific hardware applications, different EIA-530 cable pin outs are used on the "red," or unencrypted side of the cryptographic unit. The "red" side of the cryptographic unit connects to the Cisco serial interface on the router.

Red Cable – Cable Pinout Option 1

Router DTE EIA-530 Side			Pulse Engineering (KG FPA RED I/O #1-J2 or #2-J1)	
Pin	Signal	Direction	Pin	Signal
1	Frame/Chassis Gnd	<-->	1	Shield
2	TXD+	-->	2	TXPT+
14	TXD-	-->	14	TXPT-
15	TXC+	<---	15	RSC+
12	TXC-	<---	12	RSC-
3	RXD+	<---	3	RXPT+
16	RXD-	<---	16	RXPT-
17	RXC+	<---	17	RPTC+
9	RXC-	<---	9	RPTC-

4-5-6-8	RTS+/CTS+/DSR+/DCD+			
19-13-22-10	RTS-/CTS-/DSR-/DCD-			
23	DTR-	-->	18	(Resync+/Prep+)
20	DTR+	-->	21	(Resync-/Prep-)
7	Signal Ground	<-->	7	Logic Ground

Red Cable – Cable Pinout Option 2

Router DTE EIA-530 Side			Pulse Engineering (KG FPA RED I/O #1-J2 or #2-J1)	
Pin	Signal	Direction	Pin	Signal
1	Frame/Chassis Gnd	<-->	1	Shield
2	TXD+	-->	2	TXPT+
14	TXD-	-->	14	TXPT-
15	TXC+	<--	15	RSC+
12	TXC-	<--	12	RSC-
3	RXD+	<--	3	RXPT+
16	RXD-	<--	16	RXPT-
17	RXC+	<--	17	RPTC+
9	RXC-	<--	9	RPTC-
4-5	RTS+/CTS+			
19-13	RTS-/CTS-			
6-8-20	DSR+/DCD+/DTR+			
22-10-23	DSR-/DCD-/DTR-	-->	18	(Resync+/Prep+)
7	Signal Ground	<-->	7	Logic Ground

Red Cable – Cable Pinout Option 3

Router DTE EIA-530 Side			Pulse Engineering (KG FPA RED I/O #1-J2 or #2-J1)	
Pin	Signal	Direction	Pin	Signal
1	Frame/Chassis Gnd	<-->	1	Shield
2	TXD+	-->	2	TXPT+
14	TXD-	-->	14	TXPT-
15	TXC+	<--	15	RSC+
12	TXC-	<--	12	RSC-
3	RXD+	<--	3	RXPT+

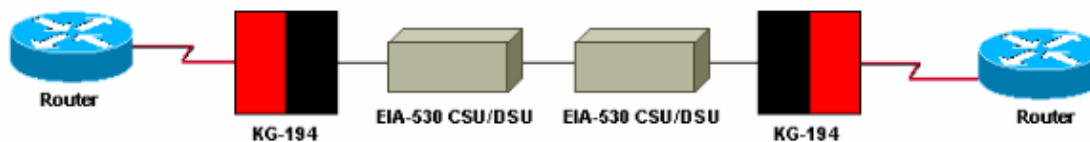
16	RXD	<---	16	RXPT
17	RXC+	<---	17	RPTC+
9	RXC-	<---		RPTC-
4-5-8	RTS+/CTS+/DCD+			
19-13-10	RTS-/CTS-/DCD-			
6-20	DSR+/DTR+			
22-23	DSR-/DTR-	-->	18	(Resync+/Prep+)
7	Signal Ground	<-->	7	Logic Ground

Black Cable – Cable Pinout

CSU/DSU/MUX EIA-530 Side			Pulse Engineering (KG FPA BLK I/O #1- J6 or #2- J4)	
Pin	Signal	Direction	Pin	Signal
1	Frame/Chassis Gnd	<-->	1	Shield
2	TXD+	-->	2	TXCT+
14	TXD-	-->	14	TXCT-
15	TXC+	-->	15	BSC+
12	TXC-	-->	12	BSC-
3	RXD+	<---	3	RXCT+
16	RXD-	<---	16	RXCT-
17	RXC+	<---	17	RCTC+
9	RXC-	<---	9	RCTC-
7	Signal Ground	<-->	7	Logic Ground

Testing Results

Testing of the resync problem consists of using different lab setups with the Cisco 7507/FSIP, 7507/PA-8T, 7507/VIP2-50/PA-4T+, 7206/PA-4T+, and 3640/NM-4T equipment. Platforms using the PA-4T, WIC-1T, and WIC-2T did not appear to be affected during testing. The lab connectivity consisted of:



The DTR control signal is used to resync, or "prep" a crypto unit after synchronization is lost. The **pulse-time x** command must be entered in the serial interface configuration, or the crypto unit has no way to know the data that is received by the router is corrupt.

The problem encountered on the Cisco 75xx platform is when a circuit disruption or crypto resync takes place. The configured **pulse-time x** command caused DTR to transition only once, therefore the resynchronization of the external encryption gear could not take place.

The problem encountered on the Cisco 72xx/36xx platforms is when a circuit disruption or crypto resync takes place. The configured **pulse-time x** command caused RTS to glitch every 1.5 ms, as seen with a digital oscilloscope. This occurred until the **pulse-time x** command was taken out of the serial interface configuration. This glitch is detrimental because the cabling scheme calls for the control signals to be tied together. This results in continuous interface resets.

Related Information

- [Technical Support – Cisco Systems](#)
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2014 – 2015 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Jan 19, 2006

Document ID: 14097
