SLC® Series 5 Carrier System

AUA180 Remote Provisioning Unit — 5SPQAB9

Features/Functions

- Remote provisioning of *SLC*-5 channel banks
- Multiple security levels:
  - Login/Password
  - Call back
  - Caller ID
  - Security lockout.
- Nonvolatile storage of security information
- Local faceplate access via RS-232
- Supports multiple channel banks with a single AUA180 RPU
- Daisy chaining of multiple AUA180 RPUs
- Built-in self diagnostics.

Description

This data sheet describes the AUA180 remote provisioning unit (RPU) (COMCODE 107191165) and is intended for the end-user of the unit. The AUA180 RPU is used in the *SLC* Series 5 Carrier System.

The AUA180 Remote Provisioning Unit is a *SLC* Series 5 plug-in designed to be used for remote access to *SLC*-5 channel banks. The AUA180 RPU provides an electrical interface between external provisioning equipment and the *SLC* Series 5 channel bank. When used in conjunction with a compatible software package, the AUA180 RPU will allow provisioning and inventory administration of *SLC* channel banks virtually anywhere a bank is installed.

The AUA180 RPU and associated support software provide a suitable and cost-effective replacement for the provisioning function of the craft interface unit.

A PROCOMM PLUS[1] script has been written and is available free of charge via the SCAT website. The script, provides an automated installation and setup procedure at http://www.lucent.com-ade.com/scat.

The following are features of the AUA180 RPU:

- Modem access via VF pair
- Direct RS-232 access via faceplate
- Four levels of security:
  - 10-character login
  - 10-character password
  - dial back capability
  - security threshold lockout feature.
- Caller identification (ID) for break-in attempts[2]
- Real time clock with National Information Services (NIS) auto set feature
- Remote (modem) access compatible with SCAT-II[3] software
- Direct (RS-232) link compatible with SCAT-II software or terminal emulator
- EEPROM for nonvolatile storage of login, password, callback number, etc.
- On board diagnostics and user-selectable initialization
- RPU hardware/software sanity timer
- Hardware fanout supports multiple channel bank service by one RPU
- RS-232 daisy chaining for multiple AUA180 RPUs.

This data sheet is being reissued to clarify some technical information in the specification.

[1] Registered trademark of Datastorm Technologies, Inc.

[2] The caller ID feature attempts to log the phone number of anyone trying to break the security of the RPU. Caller ID is a subset of the AUA180 RPU security but is not service-affecting; that is, if caller ID is not available, the RPU operation is unaffected. The data transmission interface for caller ID [Calling Number Delivery (CND)] is a service feature *CLASS (Class is a Service Mark of Bell Communication Research, Inc.)* and must conform to Bellcore TR-NWT-000030/”Voiceband Data Transmission Interface Generic Requirements.”

[3] SCAT-II (Special Channel Administration Tool II) is a software product of Lucent Technologies included with the AUA180 RPU. Upgrades to SCAT-II can be obtained via the Internet at http://www.lucent-ade.com/scat.

Description of Figures and Tables

- Figure 1 shows the AUA180 RPU ’CTU’ faceplate connector.
- Figure 2 shows the AUA180 RPU ’T-R/RS232’ faceplate connector.
- Figure 3 shows the AUA180 RPU Functional Block Diagram.
- Figure 4 shows the typical AUA180 RPU daisy chain topology
- Figure 5 shows the AUA180 RPU faceplate diagram
- Table 1 lists the environmental specifications.
- Table 2 lists the power drain of the AUA180 RPU.
- Table 3 lists the edge connections for the AUA180 RPU.

Compatibility

The AUA180 RPU is designed for a dedicated channel bank POTS phone line. The appropriate protection networks have been designed into the hardware, but the device is not FCC approved for direct connection to the Public Switched Telephone Network (PSTN). A tip/ring pair from a POTS channel unit should be dedicated for this purpose.

Table 1. Environmental Specifications

A. Temperature Range (Ambient)

1. Operating, per TR-NWT-000057: in Lucent Technologies cabinet mounted RT, outside ambient temperatures of -40° F (-40° C) with no solar load to +115° F (46° C) with maximum solar load and maximum power dissipation. Lucent Technologies cabinets are designed to assure that the components within do not exceed their rated temperatures for the above conditions.
2. Storage, per TR-NWT-000057: ambient temperatures of -40° to 140° F (-40° to 60° C).

B. Relative Humidity

1. Operating, per TR-NWT-000057. For outside ambient temperature 84° F (29° C) or less, relative humidity of 5% to 95%. For ambient temperatures above 84° F (29° C), the relative humidity is limited to that corresponding to a specific humidity of 0.024 pounds of water per pound of dry air.
2. Storage, per TR-NWT-000057: ambient temperatures 84° F (29° C) or less, 10% to 95%. For ambient temperatures above 84° F (29° C), the relative humidity is limited to that corresponding to a specific humidity of 0.024 pounds of water per pound of dry air.

Table 2. Power drain of the AUA180 RPU

Condition	Maximum Value
+ 5 Volts dc	300 mW

Circuit Description

Purpose

The AUA180 RPU is a *SLC* Series 5 plug-in designed to provide a remote electrical interface for the *SLC* Series 5 channel bank for provisioning and inventory purposes. The interface is accessible over a POTS phone line or via a direct RS-232 interconnection. The AUA180 RPU is specifically designed to work in conjunction with the SCAT-II software package.

General

The AUA180 RPU is composed of a single board which is plugged into the sixth line interface unit (LIU) slot of the WHITE bank in a *SLC* Series 5 channel bank. The AUA180 RPU performs mainly as a communications interface for access to the *SLC* channel bank channel test unit (CTU) for provisioning via an RS-232 faceplate connection or over a VF pair (phone line). The AUA180 RPU has a built-in 1200 baud modem for this purpose.

The AUA180 RPU has two faceplate jacks, a T-R/RS-232 (8-pin) jack and a CTU (10-pin) jack, which serve dual purposes. Pin 4 and pin 5 of the 8-pin modular jack connect the AUA180 RPU to a dedicated POTS channel phone line. The other pins (1, 2, 3, and 8) are used for a direct RS-232 connection to a laptop computer. Refer to Figure 2 for the T-R/RS-232 faceplate modular connector. The 10-pin connector is used to connect the AUA180 RPU to the BLUE bank CTU via a ribbon cable and provides a multiple bank fanout and an RS-232 interface to other AUA180 RPUs. Refer to Figure 1 for the CTU faceplate connector.

Security

The AUA180 RPU has multiple levels of security. In addition to a login and password, the AUA180 RPU has a customer callback feature. The AUA180 RPU also has a caller ID chip that will attempt to identify all calls to the AUA180 RPU. Any call that results in a failed attempt to access the AUA180 RPU will result in logging of the caller ID.

The caller ID feature is dependent upon the availability of the service. A security lockout feature can be optioned to lock out the AUA180 RPU from external access if too many security breach attempts are encountered.

External access via the direct connect RS-232 feature does not enforce security and may be used by craft to initialize or reinitialize the AUA180 RPU or as an interface to other AUA180 RPUs in a daisy chain.

All login and password information is written into serial EEPROM. If enabled, a reset of the AUA180 RPU clears out this memory and writes a default login and password. A movable jumper ('NORM/CONFIG') on the surface of the AUA180 RPU may be placed in the 'CONFIG' position to enable initialization. Once initialization is performed, the movable jumper is installed in the 'NORM' position to ensure that power resets do not clear memory.

Onboard Diagnostic

The AUA180 RPU has a self-diagnostic feature, which is executed each time the AUA180 RPU is reset. The diagnostics check the real time clock, memory, the modem, and CTU interface. Provision is made in the code for intermittent power resets. Should a power reset occur due to power interruptions; for example, thunder storms or human intervention, the AUA180 RPU will enter the diagnostic feature and will fail the CTU interface code during this test because jumper cables are usually used to complete the loop around during this test. The reason the CTU code does not cause a halt during the CTU loop around test is that to pass the test requires the craft to install a loop around plug or short two pins on the front of the AUA180 RPU. Since it expected that periodic power resets will occur and the craft cannot be dispatched each time, this provision allows the AUA180 RPU to enter service despite a 'failure'. The AUA180 RPU will flash the failure state but will continue and enter the idle state (failures in the diagnostic code are identified by flashes of the 'FAIL' LED). All failures except the CTU loop around will halt the AUA180 RPU with the 'FAIL' LED flashing the failure code.

The AUA180 RPU has a built-in real time clock to aid in the security aspect of the device. The real time clock may be set using an RPU command. The AUA180 RPU has provision for an auto set feature which may be enabled by providing the dialing sequence to the NIS in Boulder, Colorado (currently, this number is 303-494-4774).

After this dialing sequence is installed, the AUA180 RPU will dial (after the customer logs off) the NIS in Boulder and set the real time clock using the information provided by the Automated Computer Time Service. If this feature is enabled and the 'NORM/CONFIG' header is in the 'NORM' position, the AUA180 RPU will call the NIS to update the time after a reset condition.

The real time clock is used when the AUA180 RPU fails to receive a caller ID during a break-in attempt. The date and time of the attempt will be provided by the real time clock and the information will be logged into serial EEPROM. If a caller ID is present, however, the time supplied by the caller ID string will be used.

There is no provision in the AUA180 RPU for intelligent interface to the CTU. All intelligence; that is, 'keep alive' must be provided by the host software. In the case of the AUA180 RPU, it is expected that SCAT-II or other customer provided software will provide this capability. Access to the AUA180 RPU built-in command set can be obtained via a directly connected laptop computer or over a phone line, but it is not expected that this will be used. The AUA180 RPU commands are somewhat obtuse (like talking to the CTU directly), and it is expected that craft will use only those commands required to turn up an AUA180 RPU. An automated software procedure exists to aid the craft in RPU initialization/maintenance and is available free of charge.

General Description

Major Components

The AUA180 RPU consists of the following major components:

- ***Microcontroller —*** The microcontroller used in the AUA180 RPU contains 8K of internal code space and 256 bytes of internal RAM. All code for the RPU is contained onboard the microcontroller. The microcontroller mainly controls the actions of the CTU serial link, the modem/UART (universal asynchronous receiver transmitter), and the serial memory. The microcontroller receives characters from the host via the modem/UART and passes CTU commands through to the CTU interface. The AUA180 RPU commands are intercepted and processed.
- **Modem/UART—** The AUA180 RPU contains a dual purpose modem/UART chip whose sections may be used independently at different times. This chip performs the following functions:
  1. After detection of ringing, the microcontroller enables the modem circuitry to begin receiving FSK. The voice frequency signal is decoded by the modem section and sent to the UART section and on to the processor via the data bus. Modem protocol is 1200 baud, 7 bits, even parity.
  2. After detection of the first ringing interval, the RX input of the UART section is enabled to receive an ASCII character bit stream from the caller ID chip. Decoded ASCII characters are sent to the processor over the data bus.
  3. If the processor detects DTR on the RS-232 direct connect port, the modem section input to the UART section is disabled and the RS-232 signals are routed directly to the UART RX lead for processing. The ASCII characters are sent to the processor via the data bus as before. The UART TX lead supplies ASCII serial bit stream return. The protocol for the direct connection is 1200 baud, 7 bits, even parity.
- ***Real Time Clock (RTC)—*** The real time clock chip runs autonomously and, once set, will supply accurate time information to the security feature on demand. The real time clock may be set using an AUA180 RPU command or can be set automatically as stated before. If set by the NIS automatically, the real time clock gives coordinated universal Greenwich mean time (GMT) time.

Time stamps read from memory will indicate whether the time is universal coordinated time (U) or local (L). The isolated, backed up power supply for the

RTC allows the RPU to be removed and reinserted for short periods of time without loss of time on the real time clock.

Serial EEPROM

The AUA180 RPU is equipped with a 256-byte serial EEPROM with a 100-year data retention specification. All nonvolatile information is written to this EEPROM. This includes login, password, call back number, security threshold count, and security log.

Caller ID

The AUA180 RPU is equipped with a caller ID chip which is used in the following way. All calls into the AUA180 RPU will enable a call ID window between the first and second rings. The caller ID chip will examine the caller ID interval and, if caller ID is available, store the incoming number in processor memory. If caller ID is not available, a default date/time stamp from the RTC along with the word NONE is written to processor memory. If the subsequent login or password attempt fails, a security breach attempt is assumed and the information in processor memory is written to EEPROM in the security log. Five such locations are provided in EEPROM and are erased by initialization or with an AUA180 RPU command to clear the security log. Security information is written in a circular manner, with the oldest entry being overwritten by the newest.

Processor Reset/Sanity Timer

The AUA180 RPU is equipped with a power reset circuit that will cause initialization upon a manual remove and reinsert (r&r) of the circuit pack or a power failure. In addition to power reset, the AUA180 RPU is equipped with a sanity timer. The sanity timer is selectively enabled in firmware to provide an approximate 20-second time-out interval. The time-out interval is gated to be approximately 800 ms in duration. Users must be aware that the AUA180 RPU will not perform a manual reset function while the 'CTU' access cable is plugged into a channel bank CTU. This is because a back power condition between the CTU and the RPU will inhibit the reset circuitry of the AUA180 RPU. A reset condition that is triggered by a bank power failure or by a sanity timer reset will, however, succeed.

Detailed Description

The AUA180 RPU begins from a reset condition in response to either a power reset or a sanity timer reset. The sanity timer reset occurs on condition of a hardware fault or software insanity condition. Once the processor resets and restarts, the sanity timer is selectively disabled, depending on where in the code execution is taking place. During those intervals where timing is not critical, the sanity timer is enabled.

The processor continues execution by performing a series of diagnostics which checks the modem sanity, EEPROM sanity, real time clock operation, and communications loop around. After the diagnostics are run, the processor initializes the modem/UART chip to respond to a direct connection on the RS-232 input of the faceplate. This input condition is monitored by looking at the data terminal ready (DTR) input. If and when this condition occurs, the AUA180 RPU indicates that a link is established by lighting the 'BUSY' LED on the faceplate.

At this point, a dialog string is issued along with a prompt at which point communication with the host begins without benefit of security. If the SCAT-II software package is being used, provisioning of the bank may now take place along with AUA180 RPU transactions that set the login, password, call back number, etc. Direct connection to the AUA180 RPU may also take place without benefit of SCAT-II, however, access to the bank will be difficult at best because of the obtuse command protocol. The AUA180 RPU commands, however, may be issued with little difficulty.

If a ringing detection is encountered, the AUA180 RPU opens a caller ID software window. If the caller ID chip detects a valid caller ID FSK signal between rings 1 and 2, an interruption is generated to the processor. The processor then enables gating for the caller ID chip data lead into the UART section of the modem (rx lead). The UART processes the serial bit stream, and the caller ID ASCII information is gathered into memory along with the associated time stamp. If caller ID is not detected, a date time stamp along with the word NONE is placed into memory and held for the security activity.

After the caller ID activity, if any, the processor inhibits the call ID data lead gating and closes the on-hook relay. The modem circuitry is then enabled to begin a standard modem handshake with the caller. If the caller modem answers properly, the AUA180 RPU will establish a communications protocol and hand off to the security activity. After the modem connection is made, the 'BUSY' LED will light. The 'BUSY' LED is an indication of communications activity on the AUA180 RPU.

The security activity first looks at the lockout threshold to see if a lockout is enabled. If a lockout is enabled, the AUA180 RPU responds with a denial message to the caller and hangs up. If a lockout is not enabled, the AUA180 RPU enters a login and password routine. Upon successful receipt of login and password, the AUA180 RPU will, if callback is enabled, notify the user of impending hang-up and then hang-up. The user is expected to have the calling modem in the auto answer mode by this time. Shortly, the AUA180 RPU dials the callback number to reestablish communications. If callback is not enabled, session management begins immediately. The AUA180 RPU establishes a session with the user (not the CTU) by sending a copyright and version number message along with a single '>' prompt. At this point the AUA180 RPU enters an idle mode waiting to process characters to/from the CTU. No further prompting is done after the initial '>' prompt (just as the CTU, the AUA180 RPU silently ignores nonrecognized character sequences).

If **either** the login or password activities fail, the AUA180 RPU logs the caller ID or derived date time stamp into EEPROM then hangs up (up to three attempts each will be allowed to enter a login or password). The faceplate 'FAIL' LED will also flash to indicate the failure for visual test purposes. Up to five caller ID/date time stamps may be logged in a circulating memory in EEPROM. This information is accessible to the craft upon command. If the security lockout feature is enabled, the security count is incremented. If the count reaches the user’s preset threshold, a flag is set in EEPROM that will cause the AUA180 RPU to block access on all subsequent calls as noted previously. If this occurs, craft must be dispatched to the site of the AUA180 RPU to obtain direct access and reinitialize. Users attempting to log in to a locked out AUA180 RPU are notified of a lockout condition prior to hanging up.

As characters are received over the VF pair or via direct RS-232 access, valid CTU commands are transmitted over the CTU fanout as well as the RS-232 daisy chain. The daisy chain enables one AUA180 RPU to control access to other AUA180 RPUs in the direct connect mode. The architecture of the channel bank allows the fanout and daisy chain to work; that is, the bank does not echo characters, and only the bank to which a message packet is valid will respond properly to bank commands.

As long as the user is connected to the AUA180 RPU, character transmission is enabled, that is, there is no character time-out initiated by the AUA180 RPU. Only the sanity timer will cause a system reset, and this will only be in response to some system hardware or software sanity problem.

The AUA180 RPU will hang-up when the modem no longer detects a valid carrier signal, when the RPU hang-up command is issued, or when the RS-232 direct connect DTR lead is dropped. In the case of a direct connection, if the RPU hang-up command is issued (**:R1O!**), the AUA180 RPU will immediately reissue the initial connection dialog unless DTR is dropped.

Connector Wiring

The RPU is shipped with a single access cable that allows one AUA180 RPU to communicate with a single dual channel bank. To take advantage of the AUA180 RPU fanout capability, it will be necessary to fashion suitable cabling to allow this. The following connector wiring information will aid in this.

CTU connector wiring

The *SLC*-5 channel test unit (CTU) is equipped with a 25-pin 'D' connector on the faceplate. Communication with peripheral maintenance equipment is through this connector.

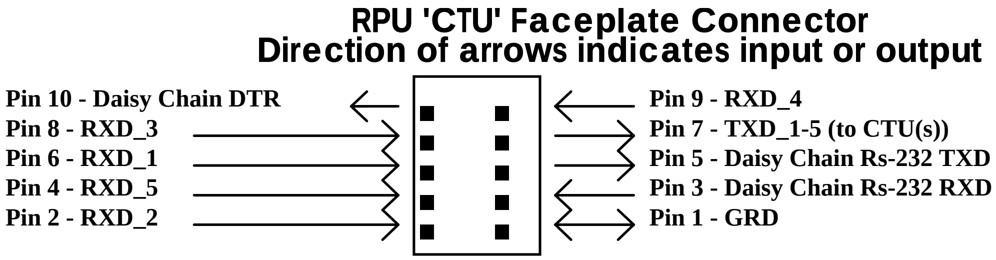
The AUA180 RPU communicates through this connector as well. The AUA180 RPU only uses three pins on this connector. The pins are as follows:

1. pin 21: ground (wires to pin 1 of the RPU 10-pin faceplate connector)
2. pin 20: CTU out (wires to one of the RPU RXD_x pins on the faceplate 10 pin connector.
3. pin 8: CTU in [wires to pin 7 of the RPU faceplate 10-pin connector (TXD)].

RPU Faceplate Pinouts

The AUA180 RPU is equipped with two connectors to the outside environment. The connectors are as follows:

1. The 'CTU' connector pins are numbered from 1 through 10 starting at the lower right-hand side to the upper left-hand side. Refer to Figure 1 for lead designations.
2. The 'T-R/RS232' connector is an 8-pin modular jack that numbers from bottom to top. Refer to Figure 2.


RPU 'CTU' Faceplate Connector
Direction of arrows indicates input or output
Pin 10 - Daisy Chain DTR
Pin 8 - RXD_3
Pin 6 - RXD_1
Pin 4 - RXD_5
Pin 2 - RXD_2
Pin 9 - RXD_4
Pin 7 - TXD_1-5 (to CTU(s))
Pin 5 - Daisy Chain Rs-232 TXD
Pin 3 - Daisy Chain Rs-232 RXD
Pin 1 - GRD

RXD_1 thru RXD_5 are TTL level inputs from up to 5 CTUs

TXD_1-5 is a common TTL level output to up to 5 CTUs

Figure 1. RPU ‘CTU’ Faceplate Connector

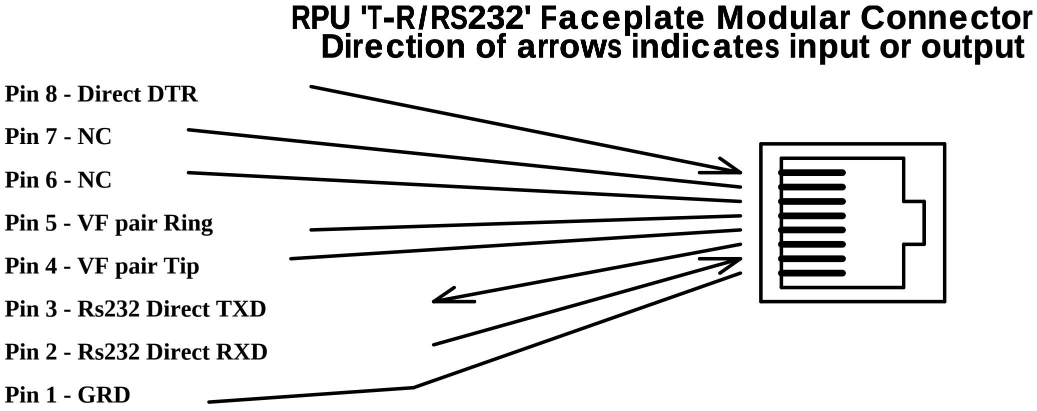


Figure 2. **RPU ’T-R/RS232’ Faceplate Connector**

Direct Connect Cable Construction

In the event that a direct connect cable is needed, the construction of an RS-232 direct connect cable is explained below. The following guide may be used:

1. Procure an 8-conductor cable with at least one RJ45 connector on one end. A Lucent comcode 102796976 cable can be used. If the cable is equipped with an RJ45 on each end, cut one of the connectors off close to the end of the cable.
2. Procure one 9-pin amphenol 'D' connector, female gender.
3. Determine the cable colors of following pins: 1, 2, 3, & 8 using the diagram shown in Figure 2, RPU 'T-R/RS232' Faceplate Modular Connector.
4. Wire the following:
   a. RJ45 pin 1 to 9-pin connector pin 5
   b. RJ45 pin 2 to 9-pin connector pin 3
   c. RJ45 pin 3 to 9-pin connector pin 2
   d. RJ45 pin 8 to 9-pin connector pin 4
   e. Wire 9-pin connector pin 1 to pin 4

This cable will be suitable for direct connection via a laptop communications (COM) port to the faceplate of the AUA180 RPU.

Installation and Verification Procedure

Installation and verification of the AUA180 RPU consists mainly of inspecting the product and performing a few basic procedures to bring the AUA180 RPU on-line. What follows is an abbreviated procedure for installation/verification of the AUA180 RPU. Detailed installation procedures may be found in Lucent Modification Implementation Procedure (MIP) MIP0060MV *SLC Series 5 Carrier System* AUA180 Remote Provisioning Unit Installation Procedure. The manual procedures found in this data sheet will suffice for bringing an AUA180 on line if the installation document is unavailable.

Automated Installation/Verification

Automated installation/verification procedures are contained in a PROCOMM PLUS script written for the express purpose of automating the installation and maintenance of the AUA180 RPU. The script is meant to augment the SCAT-II tool, which is the main *SLC*-5 channel bank administration interface to the AUA180 RPU. The listing for the script is, approximately 15 pages and cannot be listed in this document. The script is however, available on the original software diskette for Releases 2.0 and later or via the SCAT website at http://www.lucent-ade.com/scat. This service is offered free of charge to purchasers and users of the AUA180 RPU. The script is also available on the COACH software tools data base maintained by Lucent Technologies Technical Support. In order to use this facility you must have a login on the COACH system. To obtain a login on the COACH system call Lucent Technologies Regional Technical Assistance Center (RTAC) on 1-800-225-RTAC.

Manual Installation/Verification

Prior to starting the following manual procedure, you must identify a dedicated VF channel for AUA180 RPU operation. A dedicated tip/ring pair off the backplane of the channel bank is the normal mode of operation. The AUA180 RPU is equipped with phone line protection circuitry; however, FCC approval has not been sought for operation with a PSTN phone line.

1. Remove the AUA180 RPU from the shipping container and inspect it for obvious damage to gold fingers or board components. Verify that the 'NORM/CONFIG' header is in the 'CONFIG' position.
2. Verify that you have one CTU single access cable.
3. Plug the CTU end of the CTU access cable into the BLUE bank CTU. Leave the other end hanging free at this time.

4. Insert the AUA180 RPU into the spare dual slot between the WHITE bank LSU and LIU-P. Never remove and reinsert the AUA180 RPU while the CTU access cable is plugged into the CTU. Power being drawn from the CTU will prevent the AUA180 RPU from resetting properly.
5. Verify that the AUA180 RPU 'FAIL' (red) LED lights for approximately 4 seconds.
6. Verify that the AUA180 RPU 'BUSY' (green) LED lights for approximately 2 seconds.
7. Verify that the 'BUSY' LED extinguishes and that the 'FAIL' LED begins flashing five groups of five flashes. This signals a failure of the CTU communications link.
8. Plug in a shorting plug into the jack on the AUA180 RPU marked 'CTU'. If you do not have a shorting plug, short pins 6 & 7 of the 10-pin jack with a clip lead. The pins count from 1 in the lower right to 10 in the upper left in a zigzag pattern. Pin 6 is the third pin up from the lower left and pin 7 is the fourth pin up from the lower right. Failure to perform items 8 and 9 will not affect performance but may mask a hardware failure.
9. Remove and reinsert (r&r) the AUA180 RPU and wait for all LEDs to extinguish. As before, the 'FAIL' LED will light for 4 to 5 seconds as diagnostics are being performed. The busy light will light for a second or two during this time. Eventually, both LEDs should extinguish.
10. If the 'FAIL' LED flashes, count the repetitions (reps) and match the number against the following:

    1 rep - EEPROM Sanity Failure
    2 reps - MODEM/UART Insane
    3 reps - MODEM Time-out Failure
    4 reps - MODEM Loop Around (internal) Failure
    5 reps - CTU Communications Loop Time-out Failure
    6 reps - CTU External Loop Around Failure
    7 reps - Real Time Clock Failure

    If the AUA180 RPU fails with one of the above indications, remove and reinsert the AUA180 RPU and try again to validate the failure. If you still receive a failure indication, tag the AUA180 RPU as bad and perform this procedure with another circuit pack.

    If you do not receive a failure indication, remove and reinsert the circuit pack a third time to verify the integrity of the pack.
11. Remove the shorting plug. Remove and reinsert the AUA180 RPU and wait for all LEDs to extinguish. At this time, plug in the RJ11 plug from the dedicated POTS VF pair.

12. To verify access to the AUA180 RPU, place a telephone call to the phone number dedicated to the AUA180 RPU and verify that a modem 'squeal' is heard after no more than two rings. Observe that the 'BUSY' may flash on for approximately 1 second prior to connection. This is an indication that the caller ID window is open, but not that a caller ID is being received. Note that the AUA180 RPU 'BUSY' LED lights when the AUA180 RPU answers. Hang up the phone and verify that the AUA180 RPU hangs up after a few seconds.

13. Using a personal computer or laptop computer and a computer-based terminal emulator (Microsoft® Windows works well as a terminal emulator, also programs such as PROCOMM PLUS, VT100, CTRM or equivalent.), place a modem call to the AUA180 RPU (1200 baud, 7 bit, even parity) and verify that the AUA180 RPU connects and that a 'Login:' message appears on the screen. You should be aware that the AUA180 RPU **does not** echo characters. If you make a typing mistake, the AUA180 RPU will ignore any conventional efforts to recover, short of retyping the correct character sequence. In some instances, like entering the login or password, the AUA180 RPU will respond immediately to invalid input with an error message.

14. Log in to the AUA180 RPU by typing the following exactly - **AUA180 RPU!**

15. Verify that the AUA180 RPU responds with a 'Password:' message.

16. Enter the following exactly - **AT&T SLC-5!**

17. Verify that the AUA180 RPU responds with the following:

    Remote Provisioning Unit, copyright 1994 by AT&T, Version X.xx
    >
    where X.xx = the version number.

18. After the '>' prompt, you may now enter the three security parameters.

    a. To enter your login type the following exactly:

       :R1L<login_string>!

       where <login_string> must be at least 6 but not more than 10 characters long.

    If entered correctly, the AUA180 RPU will respond with:

    1<login_string>C%<cksum>
    where <cksum> is a checksum byte calculated by the RPU.

    If entered incorrectly, the AUA180 RPU will respond with a deny message of the form:

    1D@@@D%^

If this happens, you should retry the procedure.

b. To enter your password, type the following exactly:

:R1P<password_string>!

where <password_string> must be at least 6 but not more than 10 characters long. <password_string> must contain at least 2 alpha characters and 1 numeric or special character.

If entered correctly, the AUA180 RPU will respond with: 1<password_string>C%<cksum> where <cksum> is a checksum byte calculated by the RPU.

If entered incorrectly, the AUA180 RPU will respond with a deny message of the form:

1D@@@D%^ (not enough characters) or

1A@@@D%[(wrong form)

If this happens, you should retry the procedure.

c. If you desire to have the AUA180 RPU call back after logging in you may enter a callback telephone number. This is a security feature which ensures that the AUA180 RPU is being accessed by a valid source. To enter a callback phone number, type the following exactly:

:R1C<phone_number>!

where <phone_number> is the exact dialing sequence to be used by the RPU to call back the user. <phone_number> may be up to 15 digits long. If entered correctly, the RPU responds with a message of the form: 1<phone_number>C%<cksum>

If entered incorrectly or if any characters are not digits, the RPU will respond with a deny message of the form:

1D@@@D%^

d. You may verify you login, password, and callback number by sending the following AUA180 RPU query commands and noting the responses.

To query the login:**R1L?!** The response will be: 1<login_string>C%<cksum>

To query the password:**R1P?!** The response will be:

1<password_string>C%<cksum>

To query the callback number:**R1C?!** The response will be: 1<phone_number>C%<cksum>

19. If you are satisfied with your login, password, and call back number entries, you may secure the AUA180 RPU by doing the following:

a. Remove the AUA180 RPU from the bank.

b. Place the 'NORM/CONFIG' header in the 'NORM' position.

c. Reinsert the AUA180 RPU into the bank and wait for all LEDS to extinguish.

d. Plug the AUA180 RPU end of the CTU access cable into the RPU jack marked 'CTU'.

e. The AUA180 RPU is now ready for use. As long as the 'NORM/CONFIG' header is in the 'NORM' position, the AUA180 RPU will be inhibited from overwriting nonvolatile RAM, should a power failure cause a reset condition.

20. Removing and reinserting the AUA180 RPU with the 'NORM/CONFIG' header in the 'CONFIG' position will clear the nonvolatile memory and rewrite the default login and password. It will also clear the call back phone number.

21. Provisioning may take place via phone connection or via the face plate direct connect using the SCATT-II software package. The AUA180 RPU commands are accessible either via direct connect or phone connection.

22. The real-time clock is used in conjunction with the caller ID function to produce a date/time stamp in memory of failed attempts which do not have an associated call ID. This clock may be set automatically by initiating the following procedure while logged in and just prior to hanging up.

    First type:

    ```
    :R1N<long_distance_access>3034944774!
    ```

    where <long_distance_access> is the digit sequence to get into the U.S. long distance network.

    Then type the following:

    ```
    :R1TA!
    ```

    This enables the autoset feature. The autoset procedure will run once only after you initiate a hang up from the AUA180 RPU. This procedure will initiate a call to the on-line time service, 'ACTS', supported by the NIS, in Boulder, Colorado.

    The AUA180 RPU will initiate the call after you hang up from your login session. This call will take place each time you execute the above command should you so desire. There is no provision for periodic setting of the real time clock. When the clock is set by the NIS the time will be Coordinated Universal Time. The clock may also be set via command line, in which case the time will be your local time.

23. To hang up, you may type the following:

    ```
    :R1O!
    ```

A hang up may also be initiated by simply turning off your modem or exiting from the terminal emulator.

24. The AUA180 RPU should also be accessed in the direct connect mode to verify that the RS-232 interface is working. To do this, you may again use a suitable terminal emulator to connect directly to one of the COM ports. The direct connect protocol is 1200 baud, 7 bits, even parity. The AUA180 RPU does not supply any handshake but does require a DTR signal from the communications port. The 8-pin modular jack on the AUA180 RPU faceplate is also used as an RS-232 direct access port.

    Starting from the bottom, the pins number from 1 through 8. Pin 1 is signal ground, pin 2 is RS-232 in (RXD), pin 3 is RS-232 out (TXD), and pin 8 is DTR. As soon as the AUA180 RPU sees the DTR go high, the sign on prompt will be sent to the terminal emulator. It should look something like this:

    ```
     Remote Provisioning Unit, copyright 1994 by AT&T, Version X.xx

       >
    ```

25. After the above prompt is received, type the following command:

    ```
    :R1XS!
    ```

    This will invoke the sanity timer test function. After approximately 20 seconds the sanity timer will cause a reset. As soon as this happens, the sign on prompt will again be issued, provided you have not caused the DTR to drop.

AUA180 RPU Instruction Set

The instruction set of the AUA180 is designed to look much like the CIU/*SLC*-5 channel bank interface language implemented by SCAT-II. Information contained in this instruction set may be used for manual AUA180 RPU installation or maintenance. All commands have the form:

:R1<opt><arg>!

The '**1**' is actually superfluous to the AUA180 RPU but is used to maintain consistency with the channel bank command set.

The '**!**' character is the command terminator and must always be used.

New lines/carriage returns are ignored except in the case of the login and password activities. These two characters may be used as valid special characters for login or password purposes. In keeping with the convention used on the *SLC*-5 channel bank, the AUA180 RPU commands **are not** echoed. Refer to Table 1 for the list of instruction sets and responses.

Table 1. Instruction Set and Responses

synopsis	opt	arg	successful response
1. set security threshold	S	single numeric 0-9	1<arg>C%<cksum>
2. query threshold	S	'?'	1<digit1><digit2>C%<cksum>[1]
3. clear security count	S	'C'	1<digit1><digit2>C%<cksum>[1]
4. set login	L	up to 10 char string	1<arg>C%<cksum>
5. query login	L	'?'	1<login>C%<cksum>
6. set password	P	up to 10 char string	1<arg>C%<cksum>
7. query password	P	'?'	1<password>C%<cksum>
8. set callback number	C	up to 15 digit phone number	1<arg>C%<cksum>
9. clear call back number	C	'C'	1C%]
10. query call back number	C	'?'	1<phone number>C%<cksum>
11. set time	T	up to 12 digits	1<arg>C%<cksum>[2]
12. query time	T	'?'	1<time>C%<sum>[3]
13. query call id fields	I	'?'	1<string>C%<cksum>[4]
14. reset call id fields	I	'C'	1C%]
15. hangup	O		1C%]
16. set NIS phone number	N	up to 15 digit phone number	1<arg>C%<cksum>
17. activate NIS call	T	'A'	1C%]
18. activate sanity reset	X	'S'	none, system reset on completion
19. activate loopback test	X	'L'	"TEST COMPLETE"

Notes for superscripted responses:

1. Digit1 of the threshold query is the current threshold number setting, digit2 is the current number of failed attempts registered if the lockout feature is enabled. The security lockout feature is enabled by submitting a digit other than 0 to the set security threshold command; in other words, a 0 will disable the security lockout. Once security lockout is enabled, if the threshold is exceeded, the craft must manually clear the security count in the direct connect mode. The security count is cleared with the **:R1SC!** command.
2. <arg> consists of the string submitted, which is in the following order of submission:

   secl,sech,minl,minh,hrl,hrh,dayl,dayh,monl,monh,yrl,yrh.

   This is the order of the digits necessary to set the clock.
3. <time> will be a human readable time stamp of the form:

   monh,monl,dayh,dayl,hrh,hrl,minh,minl,yrh,yrl - This is a typical UNIX[1] computer program -like time stamp.

   If the time was set locally, the string '(L)' will also appear. If the time was set by the NIS, the string '(U)', indicating coordinated universal time, will appear.
4. Caller ID <string> will be packed thusly - the first field will be the caller ID of the call in progress. This will be followed by up to 5 ':' separated fields with a time stamped caller ID. If the RPU is unable to determine a call ID a field will consist of at least a time determined by the real time clock setting and possibly the string 'NONE'; for example, a caller ID field might look like this:

1071009204055941211:070911094053415932:07061317NONE:::C%<cksum>

If the incoming line is equipped with call ID capability and the caller ID is available, the first part of the call ID string should always be seen; that is, a call ID query should always show the phone number of your incoming call to the AUA180 RPU. Other fields will only appear if someone has tried to call into the RPU and failed to log in properly. Thus, a safe and secure the AUA180 RPU will respond to a call ID query with something resembling the following:

1<your call id data>:::::C%<cksum>

[1] UNIX is a registered trademark of Novell, Inc.

Refer to Figure 3 for the AUA180 RPU functional block diagram.

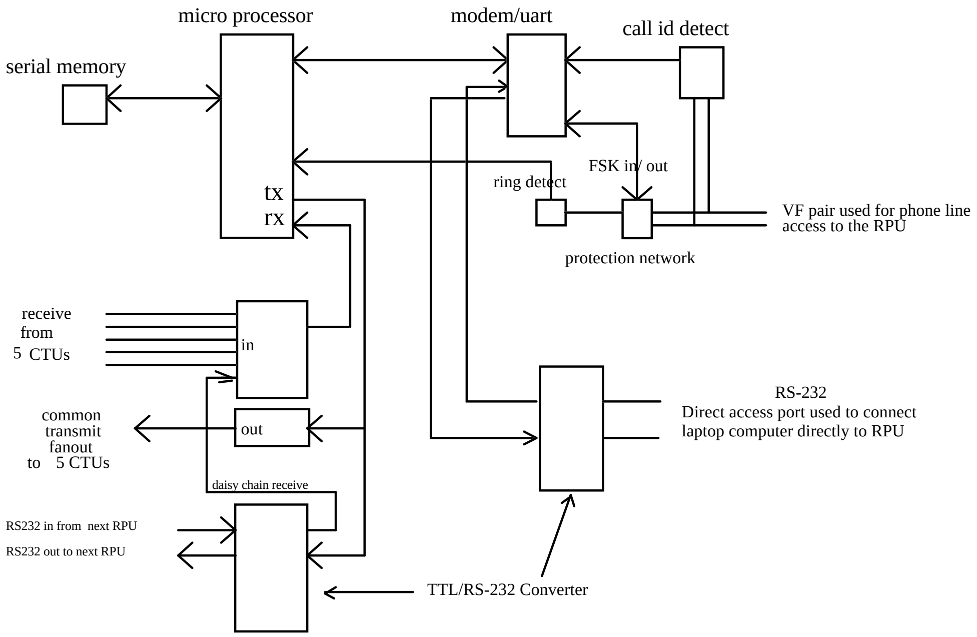


Figure 3. AUA180 RPU Functional Block Diagram

A single AUA180 RPU can be used to access up to five dual channel banks via the multiple bank fanout. If access to more banks is desired, an AUA180 RPU may be daisy chained to a second AUA180 RPU via an RS-232 daisy chain port. This second AUA180 RPU may then be used to access 5 additional AUA180 RPUs, and so on.

If direct access to an AUA180 RPU is desired, an RS-232 direct access port may be used. This port is used for AUA180 RPU turnup and verification. It is conceivable that an AUA180 RPU installed in a central office terminal (COT) in a central office could be hard wired to an RS-232 port to give access on demand for provisioning and inventory purposes at the COT. The AUA180 RPUs may be used either at the COT or remote terminal (RT) end.

Refer to Figure 4 for typical AUA180 RPU daisy chain topology

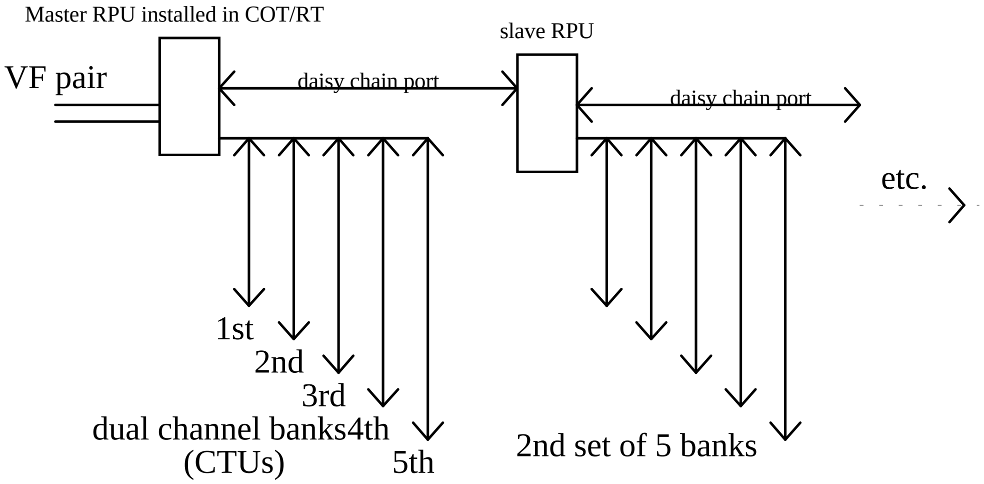


Figure 4. Typical AUA180 RPU Daisy Chain Topology

Faceplate Features

The AUA180 RPU faceplate has two faceplate jacks, a T-R/RS232 (8-pin) jack and a CTU (10-pin) jack, and two LED indicators. Refer to Figure 5 for a faceplate diagram. The 8 pin modular jack serves as the input for the tip and ring for the VF pair. The other pins are used for a direct RS-232 connection to the laptop computer. The 10-pin connector serves as the interface for the *SLC* Series 5 Channel Test Unit (CTU) and also it is used as an RS-232 daisy chain to another AUA180 RPU.

The faceplate also has BUSY and FAIL LED indicators. When the AUA180 RPU is in the inactive state, both indicator lights will be off. The LEDs may also be used to indicate a transient condition. For more detailed information, refer to Detailed Description, and Installation and Verification Procedure sections.

BUSY (green LED): The green LED when lit indicates that the AUA180 RPU is running a communication path loop around. It is also lit to indicate a busy status.

FAIL (red LED): The red LED lights when the onboard diagnostic feature is enabled or during an installation/power-up or an abnormal condition.

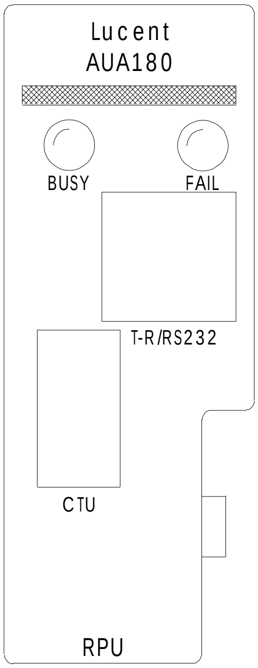


Figure 5. AUA180 RPU Faceplate Diagram

Table 3. Edge Connections For AUA180 Remote Provisioning Unit

Finger	**Function**
1	Frame Ground
6, 7, 10, 12, 13, 25	Circuit Ground
18	+5R Volts dc

References

The following documents provide additional information about the use of this channel unit in the *SLC Series 5 Carrier System* and the *SLC*-2000 Access System:

363-205-010	*SLC Series 5 Carrier System Applications and Planning Guide*
363-205-402	*SLC Series 5 Carrier System Channel Unit Installation and Testing*
363-208-000	*SLC*-2000 *Access System Applications, Planning, and Ordering Guide*
363-208-001	*SLC*-2000 *Access System User/Service Manual*
363-208-003	*SLC*-2000 *Access System Command and Message Manual*
915-710-116	*SLC Series 5 Carrier System Channel Unit Application and Prescription Setting.*
MIP 0060MV	*SLC Series 5 Carrier System AUA180 Remote Provisioning Unit Installation Procedure*.

Technical Assistance

Follow local procedures for obtaining technical assistance. Lucent Technologies also provides in-hours or emergency out-of-hours help for the *SLC* Series 5 Carrier System and the *SLC*-2000 Access System. Call the Lucent Technologies Regional Technical Assistance Center at 1-800-225-RTAC.

Ordering Information

Additional copies of this document (363-005-315) are available from the Customer Information Center — call 1-888-582-3688.

Comments

Comments about this document can be directed to:

Lucent Technologies
Customer Training and Information Products (CTIP)
Documentation Services
2400 Reynolda Road
Winston-Salem, NC 27106-4606

Copyright Information

For permission to reproduce or distribute, please call: 1-888-584-6366.