

GBPPR 'Zine



Issue #89 / The Monthly Journal of the American Hacker / September 2011

"Every child in America entering school at the age of five is mentally ill because he comes to school with certain allegiances to our founding fathers, toward our elected officials, toward his parents, toward a belief in a supernatural being, and toward the sovereignty of this nation as a separate entity. It is up to you as teachers to make all of these sick children well – by creating the international child of the future."

---- Quote from Dr. Chester M. Pierce, Professor of Education at Harvard, addressing the Association for Childhood Education International in April, 1972.

Do *NOT* send your kids to public school!

Table of Contents

- ◆ **Page 2 / Lawfully Authorized Electronic Surveillance / 5ESS (Part 5)**
 - ◆ Procedures for the provisioning, maintenance, and troubleshooting of the 5ESS switch for CALEA applications.
- ◆ **Page 36 / GBPPR MIL-SPEC Laser Dazzler**
 - ◆ Improvements on the laser dazzler project in Issue #86.
- ◆ **Page 61 / Motorola STF2520A 900 MHz Power Amplifier Modifications**
 - ◆ Modifying a surplus Motorola STF2520A cellular-band RF amplifier for 150 watts in the 900 MHz ham band.
- ◆ **Page 74 / 5 Watt RF Power Amplifier for 900 MHz**
 - ◆ Simple pre-driver stage for the Motorola STF2520A amplifier using an old Radio Shack cellular phone.
- ◆ **Page 83 / Bonus**
 - ◆ Teacher Union Propaganda
- ◆ **Page 84 / The End**
 - ◆ Editorial and rants.

Lawfully Authorized Electronic Surveillance / 5ESS (Part 5)

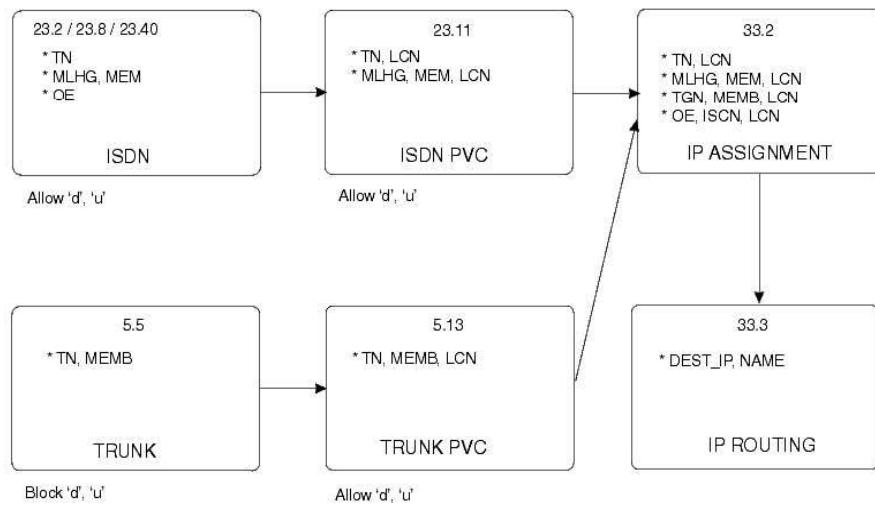
Provisioning, Troubleshooting, and Maintenance

235-200-400

June 2003

ISDN and trunk PVC views.

Each of the six "screens" depicted in the flowchart contains several lines of text. The first line lists the applicable view numbers. The lines denoted with an asterisk (*) are the key fields for each of these views. The last line tells whether the view is used for ISDN line or trunk assignments.



Key: 'd' refers to the 'delete' operation via Recent Change
'u' refers to the 'update' operation via Recent Change

Note: updates and deletes are only allowed if the CALEA IN USE bit is not set for underlying data present on RCV view 33.2

Figure 3-11 Recent Change View Interactions

3.11 CALEA CASE PROVISIONING

Specific surveillance case provisioning is performed by the Surveillance Administrator and is outside the scope of this document.

Lawfully Authorized Electronic Surveillance / 5ESS (Part 5)

Provisioning, Troubleshooting, and Maintenance

235-200-400

June 2003

4. NETWORK TROUBLESHOOTING

4.1 OVERVIEW

A call can fail for many reasons including called party interface busy, destination address is out of order, network busy, etc. When the call fails, the switch will initiate call clearing. Surveillance CDC messages are sent to the SAS terminal to indicate the failures encountered by a monitored call.

If an error condition such as an assert or audit is encountered as a result of this feature set, the normal operation of the subscriber's service will be protected as the first priority.

4.2 UNUSUAL EVENTS HANDLING

Unusual events will be handled by sending reports to the CALEA TTY describing the unusual event and in some cases logging the administrator of the CALEA system if the event was linked to their login session.

4.3 CALL CONTENT CHANNEL (CCC)

4.3.1 CCC TRUNK IS 'OOS'

When a CCC trunk is out of service (OOS), an autonomous report, RMV TRK, is sent to the SAS terminal. The RST:TRK command must be executed from a non-CALEA terminal to put the trunk back in service (IS). A RST TRK report is generated when a CCC is placed back in service.

4.3.2 CCC NOT AVAILABLE

If the switch attempts to access and use a CCC for a given subject and all CCCs provisioned for the surveillance subject are in use, the switch denies allocation of a CCC and the intercepted call content is not transmitted. The switch continues to provide CDC messages (except for CCOpen and CCClose) for the call even if a CCC is not available.

4.3.3 C-TONE FAILURE

Failure to apply the continuity signal to an idle CCC circuit associated with a surveillance is reported using the ContentChannelSetupFailure administration message sent to the Surveillance Administration System. The channel(s) on which the failure occurred and one of the following failure causes are reported:

- * Switch blockage - cannot set up CCC for a surveillance
- * Resource unavailable - cannot set up CCC for a surveillance
- * Other - span failure on the CCC

4.4 CALEA SYSTEM PROCESS (CASP)

4.4.1 OVERVIEW

The CALEA System Process (CASP) is responsible for performing resource allocation for a new surveillance, delivering specific CDC messages to the SAS, and requesting the bridge process (CABR) to perform a bridge action.

A failure detected in or by the CASP will not impact a call in progress.

4.4.2 ERRORS

Lawfully Authorized Electronic Surveillance / 5ESS (Part 5)

Provisioning, Troubleshooting, and Maintenance

235-200-400

June 2003

Requests to the CALEA System Process (CASP) can result in (but are not limited to) the following conditions:

4.4.2.1 Unable to allocate RLcal_info tuple.

If no tuples are available in the idle list, the CASP will not be able to begin a new surveillance for a new call, or extend a surveillance for an existing call ID. This will result in an assert indicating that the limit has been reached in new surveillances or added call legs for existing surveillances. The CASP will report this condition to the surveillance administration ROP.

4.4.2.2 Unable to create a bridge process (CABR).

This condition assumes a CDC channel has already been created for a Level I surveillance. A sanity timer has expired before an acknowledgement has been received from the newly-created CABR. In this case, the required Level II surveillance cannot be established. The surveillance level of the terminal process will be lowered to Level I and a failure report will be sent to the surveillance administration ROP.

4.4.2.3 CABR is unable to create/move a bridge.

This condition should be handled primarily by the CABR, and is noted here only to indicate that the CASP should perform the same recovery actions as the CABR process creation above, that is, the surveillance level of the terminal process will be lowered to Level I and a failure report will be sent to the surveillance administration ROP.

4.4.2.4 ASN.1 encoding failure.

If a message to be sent to the LEA cannot be encoded correctly by ASN.1, an assert will be invoked and the failing message will be discarded.

4.4.2.5 Unknown message received.

The CASP will print out a debug message detailing the "unknown" message and its contents, and then ignore the message and continue with more message reception and processing.

4.4.2.6 Socket-related failure.

Socket-related failures will be handled by the Socket Manager, which will assert and report the failure to surveillance administration ROP. The CASP will not take any further action.

4.5 SOCKETS

4.5.1 OVERVIEW

Sockets is a widely used application program interface to the IP network. A socket is a path that is defined by a pair of addresses; the local internet protocol (IP) address and port number for the transmission control protocol (TCP), and the foreign IP address and port number. Each address/port combination is referred to as a "socket address." Together, both address/port combinations are referred to as a "socket pair" of addresses.

4.5.2 ERRORS

Any socket-related failure will be handled by the Socket Manager by sending a CDC Communications Alarm message to the SAS detailing the failure. The CASP will not assert when a socket failure is encountered.

Lawfully Authorized Electronic Surveillance / 5ESS (Part 5)

Provisioning, Troubleshooting, and Maintenance

235-200-400

June 2003

4.5.2.1 CDC COMMUNICATIONS ALARM MESSAGES

For the CDC alarm messages, see the report:

- REP CALEA SAS ERROR

4.5.2.2 CCC COMMUNICATIONS ALARM MESSAGES

For the CCC alarm messages see the reports:

- RMV TRK
- RST TRK
- REPT CALEA SAS ERROR

4.6 CDC/PDC ERRORS

Problems associated with a surveillance CDC or PDC are reported on the SAS ROP.

NOTE: * = Unexpected, software problems which would cause an assert if encountered.

- * The socket is non-blocking and a previous connection attempt has not yet been completed.
- + The connection was refused.
- * The domain is not supported.
- * Insufficient global memory is available.
- * The socket is non-blocking and a connection can not be completed immediately.
- * Socklen is not the size of a valid address for the specified address.
- *The socket is already connected.
- *The socket is of type SO_DGRAM, requiring the data be sent automatically, however the message exceeded internal buffer space.
- + Call establishment error. The TCP/IP platform has received an ICMP_UNREACH message.
- * Insufficient global memory to allocate a socket{} structure.
- + The specified socket is not connected.
- * The socket does not refer to a valid socket structure.
- * The application has requested to send out of band data, however the protocol does not support this functionality.
- * The operation requested is not supported for this socket.
- * The protocol type or the specified protocol is not supported within this domain.
- * Insufficient user memory is available for the socket send queue.
- * The socket is marked as non-blocking and the call would block.

These alarm messages will be generated with a "handling priority" equivalent to major alarm but without the audible alarms.

4.7 PH

4.7.1 OVERVIEW

Lawfully Authorized Electronic Surveillance / 5ESS (Part 5)

Provisioning, Troubleshooting, and Maintenance

235-200-400

June 2003

The packet handler (PH) contains the TCP/IP software that routes the PDC subject content to the LEA.

4.7.2 ERRORS

Protocol Monitoring (PM) can be triggered by the following:

- The IP datagram length,
- the IP version,
- checksum error,
- illegal IP source address,
- illegal IP destination address,
- invalid IP header,
- invalid protocol field (not supported),
- no outgoing route available,
- invalid IP option was received, or
- the source IP address (from the received IP datagram perspective).

NOTE: The local IP address mentioned above is actually the destination IP address in received datagrams and the source IP address in IP datagrams that are sent out. If only the local IP address is specified, then the first IP datagram with the local address is received will fire the trigger. As just stated, the default trigger is the local IP address which is a required parameter.

4.8 CALEA PACKET ERRORS

When packet errors occur in the CMP, SMP, or PH, the **REPT CALEA SAS** report is sent to the surveillance terminal. The report contains information regarding

- the processor environment where the error message originated (PSUPH or SM)
- the event number
- the time of day
- the description of the error type

ERROR 14 = Protocol Handler Resource CAL_INFO Exhaustion

ERROR 15 = Invalid Protocol Handler CAL_INFO attribute value

ERROR 17 = RLCASE_IDX data inconsistency

ERROR 18 = RLCASE_IDX tuple missing

Lawfully Authorized Electronic Surveillance / 5ESS (Part 5)

Provisioning, Troubleshooting, and Maintenance

235-200-400

June 2003

ERROR 19 = RLLAESCASE tuple missing

ERROR 22 = Attempted to add monitoring station when 5 already exist

ERROR 23 = Attempt to send a CALEA message to a CALEA process failed

ERROR 24 = PSLAESCASE tuple missing when adding new monitoring station

- a description of the data type associated with the error type
- and, the data value(s) in hexadecimal format associated with a specific data type

For the complete report description, see Chapter 6.

4.9 TONE DECODER OVERLOAD (5E15 and later)

Excessive UTD usage can block originations from lines and multi-frequency (MF) trunks. This may cause an unacceptable level of dial tone delay or failed calls. Corrective actions may include:

- Growing additional UTD circuits. Refer to 235-105-231, *Hardware Change - Growth*, for the procedures.
- Re-designating some subjects from DTMF STATUS=ESSENTIAL to DTMF STATUS=STANDARD on view C.4. This view can only be accessed by the Surveillance Administrator.
- Reducing the value of "TD LIMIT" on RC/V view 8.1. Note that the value of "TD LIMIT" on view 8.1 has no effect on cases marked DTMF STATUS=ESSENTIAL on view C.4.
- Re-assign subjects to SMs with a lighter UTD usage (where physically possible).

4.10 TONE DECODER ALARM MESSAGE (5E15 and later)

The switch sends a REPT CALEA SAS report to the SAS terminal whenever a tone decoder is dropped from a surveillance or cannot be attached to a surveillance.

The alarm message contains the caseID and one or more of the following error type messages:

- **Tone Decoder Dropped Due to Load**

CALEA tone decoder threshold was exceeded. See Section 3.7 for procedures covering tone decoder threshold modification.

- **Digit Surge Tone Decoder Dropped**

A burst of digits greater than 100 digits in 20 seconds occurred. No action required.

- **Tone Decoder Dropped**

Tone decoder dropped due to other failure/maintenance.

- **No Tone Decoder Available**

Lawfully Authorized Electronic Surveillance / 5ESS (Part 5)

Provisioning, Troubleshooting, and Maintenance

235-200-400

June 2003

Additional tone decoders may need to be provisioned in the office.

The alarm report is generated with a handling priority equivalent to 'PHMNORM' (a normal priority message requiring some action to be taken by switch personnel).

For the complete report description, see Chapter 6 .

4.11 AUDITS

4.11.1 OVERVIEW

Audits are responsible for detecting lost resources and data structure inconsistencies. If an error is detected, audits take actions (either directly or indirectly) to recover the lost resources and correct inconsistencies before they adversely affect the system. The following is an overview of the audit changes in the SM and the PH that ensure the integrity of data added and modified.

4.11.2 NEW AND MODIFIED AUDITS

The following is an overview of the audit changes in the SM that ensure the integrity of data added and modified by this feature set.

- BRGDB

The BRGDB audit ensures the integrity of the RLBRGDB relation.

- CALINFO

The CALINFO audit ensures the integrity of the new RLCAL_INFO relation.

- CCBCOM and CHDB

The CCBCOM and CHDB audits are modified to recognize the new linkage from the RLCCBCOM relation to the RLBRGDB relation.

- CRECORD

The CRECORD audit is modified to recognize the new linkage from the RLCRECORD relation to the new RLCAL_INFO relation.

- PORTLA

The PORTLA audit is modified to ensure the integrity of the new attributes added to the RLPORTLA relation by this feature.

The following is an overview of the audit changes in the PH that ensure the integrity of data added and modified by this feature set.

- LAESCASE

The LAESCASE audit ensures the integrity of the new PSlaescase[0] array and its associated headcell (PSrlaescasehd).

Lawfully Authorized Electronic Surveillance / 5ESS (Part 5)

Provisioning, Troubleshooting, and Maintenance

235-200-400

June 2003

- CALINFO

The CALINFO audit ensures the integrity of the new PScal_info[0] array and its associated headcell (PSrcal_infod).

- ALDB

The ALDB audit has been modified to ensure the integrity of the new semantic linkage between the PSaldb[0] array and the PSlاءescase[0] array.

- LCCB

The LCCB audit has been modified to ensure the integrity of the new semantic linkage between the PSllcb[0] array and the PScal_info[0] array.

4.11.3 KEEP ALIVE AUDITING

There are several scenarios in which the CALEA bridge process (CABR) can become stuck in a busy state. It may be that the CABR terminal process did not receive a mgIDLE_PT message, the corresponding originating terminal process (OTP) or terminating terminal process (TTP) is purged, SM selective or full initialization has occurred, or due to audit recovery. Therefore, keep alive auditing is performed between the CABR terminal process and the CALEA system process (CASP).

The TCP socket application turns on the keep-alive mechanism by setting the keep-alive timer to 5 minutes to detect the failure cases. Once a failure case is detected, a error handling function (provided by the application) is invoked by the TCP/IP platform to perform the error handling.

4.12 OVERLOAD CONTROL (OC)

4.12.1 SRE RESOURCES

Overload Control (OC) is the SRE resource exhaustion reporting mechanism. All SRE resources under OC have at least one idle list which is managed by the application using specialized Dynamic Access (DA) primitives created explicitly for the dynamic relation. When a monitored resource exhausts due to no more idle resources available, DA calls Integrity Monitor (IM). IM schedules a immediate audit to attempt to recover any resources that may have been idled incorrectly, left dangling, etc. IM sets a bit in the OCrcmon[] table for the resource. This tells OC to start monitoring this resource every six-seconds until the overload has cleared. The audit probably will not recover any resources. The resource will be in overload for a minimum of 18 seconds. If this is the first overload in the particular SM during the current 15 minute interval, an OP OVRLD message will be output to the ROP.

4.12.1.1 CALINF RESOURCE EXHAUSTION

In the case of CALINF resource exhaustion, OP OVRLD reports will appear on the MCC TTY, for example:

```
* OP OVRLD SM=2
    REAL TIME NONE
    RESOURCE CALINF
    CONTROLS DNET
    CONTROLS AVRT
```

Lawfully Authorized Electronic Surveillance / 5ESS (Part 5)

Provisioning, Troubleshooting, and Maintenance

235-200-400

June 2003

NOTE: The control AVRT (Avoidance Routing) applies to calls involving one-way trunks and is administered by RTA. DNET (Defer Non-Essential Task) is a "maintenance" control looked at by only a very few maintenance tasks (REX, certain diagnostics, etc.) These controls, by design, do not block calls but attempt to route around the problem, but will NOT fail a call specifically due to the overload.

In addition, REPT CALEA SAS reports will appear on the Surveillance Administration System TTY, for example:

```
REPT CALEA SAS ERROR SM=2 EVENT=37 TIME=21:07:20
ERROR TYPE=Surveillance not started due to SM RLCAL_INFO Exhaustion
DATA1 TYPE=RLCASE_IDX Relation Key Value
00060000
DATA2 TYPE=NONE
DATA3 TYPE=NONE
DATA4 TYPE=NONE
```

4.12.1.2 BRGDB RESOURCE EXHAUSTION

In the case of BRGDB resource exhaustion, OP OVRLD reports will appear on the MCC TTY, for example:

```
* OP OVRLD SM=2
REAL TIME NONE
RESOURCE BRGDB
CONTROLS DNET
CONTROLS AVRT
```

and craft asserts print on the MCC TTY, such as:

```
A REPT MANUAL ACTION ASSERT=23063 SM=2 EVENT=3
PCallocbrg.c AT LINE 65
Bridging Data Blocks Exhausted
```

In addition, REPT CALEA SAS reports will appear on the Surveillance Administration System TTY, for example:

```
REPT CALEA SAS ERROR SM=2 EVENT=37 TIME=21:07:20
ERROR TYPE=Bridge Resource Failure
DATA1 TYPE=SM Process Identification value
00060000
DATA2 TYPE=NONE
DATA3 TYPE=NONE
DATA4 TYPE=NONE
```

4.12.1.3 RESOURCE EXHAUSTION RECOVERY

When a CALINF or BRGDB resource exhaustion occurs, Recent Change view 8.40, SRE INCREMENTAL GLOBAL PARAMETERS, must be updated via the normal Recent Change terminal (not the SAS) to increase the number of resources on the switching module listed in the reports.

```
5ESS SWITCH
RECENT CHANGE 8.40
(5547) SRE INCREMENTAL GLOBAL PARAMETERS
*1. MODULE
```

Lawfully Authorized Electronic Surveillance / 5ESS (Part 5)

Provisioning, Troubleshooting, and Maintenance

235-200-400

June 2003

*2. SOFTWARE RESOURCE _____
#3. TUPLES TO ADD _____

INCREMENTAL VALUE _____
CURRENT TOTAL VALUE _____

WARNING: This form should not be used to make changes to dynamic memory without first contacting your next level of support. Refer to the Administration Guideline Section for Software Resource Engineering.

For CALINF, set:
MODULE = switching module that ran out of resources.
SOFTWARE RESOURCE = CAL_INF
TUPLES TO ADD = the number of tuples by which you want this resource increased or decreased (-50 to 50). The default number of total resources is 25.

For BRGDB, set:
MODULE = switching module that ran out of resources.
SOFTWARE RESOURCE = BRGDB
TUPLES TO ADD = the number of tuples by which you want this resource increased or decreased (-50 to 50). The default number of total resources is 64.

If the resource is not increased, subsequent surveillances will not occur.

4.12.2 PH RESOURCES

An overload condition occurs due to too many surveillances on a subject PH or too much traffic on a delivery PH. PH resource exhaustion is reported as always, via OP OVRLD reports to the MCC TTY. Refer to 235-600-750, *5ESS® Switch Output Messages*, for an explanation of the output message(s) and the appropriate action(s) to be taken.

Lawfully Authorized Electronic Surveillance / 5ESS (Part 5)

Provisioning, Troubleshooting, and Maintenance

235-200-400

June 2003

5. MAINTENANCE

5.1 OVERVIEW

The CALEA feature set will block routine maintenance activities (100-108 and digital loopback) for CCCs.

When either a resource is not restored properly or the far end equipment is not restored, leaving the resource out of service preventing its use in delivering content, the SAS will be notified of any out of service condition on a CCC, CDC or PDC.

5.2 PORT STATUS ADMINISTRATION (PSA)

PSA is responsible for maintaining and reporting the status of ports on the switch. The RMV TRK report is sent to the SAS whenever a CCC trunk is placed out of service (OOS). This output message will generate an alarm with a "handling priority" equivalent to a major alarm but without the audible alarms.

An autonomous report, sent to the SAS, will also be generated when a CCC is placed back in-Service (IS) using the same "handling priority" and message class.

5.3 ODBE ACCESS TO CALEA DATA

For the purposes of troubleshooting and maintenance, ODBE will have update access to all data except the global parameter GLCALIPADR. GLCALIPADR is viewable, but has been blocked from ODBE update. Any attempt to change GLCALIPADR via ODBE will result in the response: **You are not allowed to update this office parameter using ODBE.**

5.4 SM INITIALIZATIONS (FULL/SELECTIVE)

If a monitored call is dropped by an initialization, there is no notification to the LEA, and there is no attempt to re-establish surveillance on the current call. The surveillance will be established starting with the subject's next call. All the surveillance-related information shall be preserved. All the SM dynamic data will be reset during a full SM initialization. Full initializations with or without pump will reestablish the PDC socket connections.

In 5E15 and later software releases, tone decoders are dropped from post cut-through surveillance calls during a selective initialization on an SM.

For Level I subjects, if the tone decoder is dropped, a message announcing the drop is sent to the SAS terminal and the LEA collection facility, but CDC communication continues as normal. For Level II subjects, if the tone decoder is dropped, a message announcing the drop is sent to the SAS terminal and the LEA collection facility, however, CCC and CDC communication continue as normal.

5.5 AM INITIALIZATIONS

During a manual and automatic full AM initialization up through and including D4 level (init 54), all surveillance static data is preserved. An active call and the surveillance are dropped, but the surveillance is established again when the subject initiates a new call. All the AM dynamic data will be reset during a full AM initialization and need to be re-initialized.

5.6 PH INITIALIZATIONS

Lawfully Authorized Electronic Surveillance / 5ESS (Part 5)

Provisioning, Troubleshooting, and Maintenance

235-200-400

June 2003

During PH selective initialization (soft switch), CDC/PDC connections are preserved and any queued data for both transmit and receive remains unaffected.

A PH full initialization (hard switch), results in PDC socket connections being re-established after initialization.

5.7 TRUNK OOS/IS

The switch will send an alarm message to the SAS whenever a CALEA trunk is taken out of service and restored to service. This report will be the same as the existing RMV TRK output message that reports trunk port status. There is no audible alarm.

5.8 SOFTWARE RELEASE RETROFIT AND LARGE TERMINAL GROWTH

During a software release retrofit, the monitored calls will not be impacted by the CALEA feature. The monitoring connections (CCC and CDC channels) will be dropped. Since all the existing dynamic data for the stable calls is reset, the monitored calls are not considered as monitored calls anymore during and after retrofit.

5.9 TRUNK & LINE WORK STATION (TLWS)

5.9.1 TREATMENT FOR CCC TRUNKS

TLWS will block all tests on CCC trunks.

5.9.2 TREATMENT OF SUBSCRIBER LINES UNDER SURVEILLANCE

With one exception, TLWS test calls will not have a CALEA surveillance occurring. Since tests do not create a call record, CALEA will not monitor these lines. The one exception is monitor busy idle.

When the talk and monitor phone (also called callback) is added, the callback (CBAK) process is created and associated with the port under test (PUT). The T&M can be added several ways. The various ways the T&M phone can be accessed are:

- The most straight forward case has the T&M phone added as part of process of testing the line either directly by the command requesting it or indirectly as an automatic operation of another test. Once the T&M phone is added, the T&M could be put in the following modes:
 - Talk (equivalent to double bridge)
 - Monitor (equivalent to single bridge)
 - Hold (equivalent to single bridge)

Simply adding the T&M to a subject's line via these methods (pokes 4301, 4302, 4303 or 4304), would not cause LEA monitoring to occur since the subject does not go offhook, but the potential for activating the surveillance bridge is there especially since the TLWS can ring the line.

- 101TL calls.

The 101TL call begins when the 101TL DN is dialed from the subject's line. The 101TL call is initially processed in POTS call processing. TMlotck() is called to start the terminal maintenance portion of the

Lawfully Authorized Electronic Surveillance / 5ESS (Part 5)

Provisioning, Troubleshooting, and Maintenance

235-200-400

June 2003

101TL setup. Since the subject's line is placing a call, LEA monitoring will occur.

- Monitor Busy (poke 4600) and Monitor Busy Idle (poke 4601)

If the TLWS attempts to seize a line that is busy, the message "DO MNTR BUSY(4600) OR B&I(4601) ONLY" will be displayed. The craft person can then do 4600/4601 (specific actions found starting in T Mtmon.c) to add the T&M.

When the line is idle and the 4601 poke is done, the port is released for the subscriber to use. Any calls to or from that line activates the CBAK process. Monitor Busy Idle does not interfere with the customer's ability to make and receive calls. This means that LEA monitoring can occur during the time monitor busy idle is active.

NOTE: The above cases can be done with either local or remote callback. The remote T&M case goes through call processing code (RTrtereq) as part of the creation of the CBAK process.

5.10 CDC/PDC TRUNK TESTS

Routine or scheduled trunk tests for CDCs and PDCs are handled in the same way as regular packet trunk channel tests. Note that RMV/RST TRK reports are sent to the SAS ROP.

Lawfully Authorized Electronic Surveillance / 5ESS (Part 5)

Provisioning, Troubleshooting, and Maintenance

235-200-400

June 2003

6. INPUT AND OUTPUT MESSAGES

6.1 INPUT COMMAND AND OUTPUT REPORT DESCRIPTIONS

This chapter contains a full description of each input command (also known as an input message) and output report (also known as an output message) referenced within this document. The commands and reports are listed in alphabetical order.

NOTE: These CALEA-specific commands and reports are documented in this information product only.
They are not documented in 235-600-700, *Input Messages*.

Input messages are used to control, maintain, and monitor the switching system, including the processors, peripherals, and other software. Output reports are generated either in response to input messages, or to inform support personnel of system conditions or automatic operations that have been performed by the system.

A brief overview of the manual page layout follows. For more information on commands and their usage, refer to 235-600-700, *Input Messages*. For more information on reports and their usage, refer to 235-600-750, *Output Messages*.

6.1.1 INPUT COMMAND DESCRIPTIONS

For the purposes of security and surveillance administration, the following sections of each input command description are of the most value:

The "PURPOSE" section of the manual page contains a brief explanation of the purpose of the message and includes the explanation of any associated warnings.

The "FORMAT" section contains the command format including all options. Parameter values are represented by lowercase letters which are defined in the "EXPLANATION OF MESSAGE" section. Optional parameters are surrounded by brackets '[]'. An OR bar '|' separates a selection of entries enclosed by brackets. Only one of the entries separated by OR bars may be selected.

NOTE: Brackets and OR bars are never used when entering a command. They are only used in message formats to show you how a message must be constructed.

The "EXPLANATION OF MESSAGE" section explains the meaning of the various parameter names, parameter values, and variables in the format. Parameter values are represented by lowercase letters in the command format.

The "SYSTEM RESPONSE" section defines acknowledgments that appears one space after the terminating character of the command. This will normally happen about five seconds after the command is entered.

The "REFERENCES" section contains a list of all related input and output messages.

6.1.2 OUTPUT MESSAGE DESCRIPTIONS

For the purposes of security and surveillance administration, the following sections of each output message description are of the most value:

The "FORMAT" section contains the layout of each output report.

Lawfully Authorized Electronic Surveillance / 5ESS (Part 5)

Provisioning, Troubleshooting, and Maintenance

235-200-400

June 2003

The "REASON FOR OUTPUT" section contains a brief summary of why the message appeared.

The "VARIABLE FIELD DEFINITIONS" section contains the meaning of the various keywords, arguments, and variables shown in the format.

The "ACTION TO BE TAKEN" section contains a brief summary of any actions that should be taken in response to the output message.

The "ALARMS" section contains any alarms that are associated with the output message.

The "REFERENCES" section contains all related input and output messages.

6.2 ASGN:SECRTY command

ID.....ASGN:SECRTY
RELEASE.....5E14 and later
COMMAND GROUP..AUTH
APPLICATION....5
TYPE.....Input

1. PURPOSE

This command will be used by the switch System Administrator to assign a default user ID and password to be used by the Surveillance Administration System (SAS) Security Administrator. The switch System Administrator will have to execute this command from a non-SAS terminal.

2. FORMAT

ASGN:SECRTY,USRID="a";

3. EXPLANATION OF MESSAGE

a = The user ID (3 to 8 characters in length).

4. SYSTEM RESPONSE

PF = Printout follows.

5. REFERENCES

Output Message(s) :
ASGN SECRTY

6.3 ASGN SECRTY report

ID.....ASGN:SECRTY

Lawfully Authorized Electronic Surveillance / 5ESS (Part 5)

Provisioning, Troubleshooting, and Maintenance

235-200-400

June 2003

RELEASE.....5E14 and later
MESSAGE CLASS..NOCLASS
APPLICATION....5
TYPE.....Output

1. FORMAT

ASGN SECRTY
a

2. REASON FOR OUTPUT

To report the result of assigning a Security Administrator user ID and password to the Surveillance Administration System.

3. VARIABLE FIELD DEFINITIONS

a = Status of the command:

COMMAND COMPLETED SUCCESSFULLY
FAILED, TUPLE COUNT EXCEEDED
USER ID MUST BE 3-8 CHARACTERS
PASSWORD MUST BE 6-12 CHARACTERS
A SYSTEM ERROR OCCURRED TRY AGAIN
THE USER ID ENTERED ALREADY EXISTS

4. ACTION TO BE TAKEN

If "COMMAND COMPLETED SUCCESSFULLY", no action needs to be taken.
If "FAILED, TUPLE COUNT EXCEEDED", the maximum number of users has been exceeded; a user must be deleted to add a new user.
If "USER ID MUST BE 3-8 CHARACTERS", enter a valid user ID.
If "PASSWORD MUST BE 6-12 CHARACTERS", enter a valid password.
If "A SYSTEM ERROR OCCURRED TRY AGAIN", try command again later.
If "THE USER ID ENTERED ALREADY EXISTS" enter a different user ID.

5. ALARMS

None.

6. REFERENCES

Input Message(s) :
ASGN:SECRTY

Lawfully Authorized Electronic Surveillance / 5ESS (Part 5)

Provisioning, Troubleshooting, and Maintenance

235-200-400

June 2003

6.4 DEL:SECRTY command

ID.....DEL:SECRTY
RELEASE.....5E14 and later
COMMAND GROUP..AUTH
APPLICATION....5
TYPE.....Input

1. PURPOSE

This command is used by the switch System Administrator to delete a user ID and password of Surveillance Administration System (SAS) Security Administrator. The switch System Administrator will have to execute this command from a non-SAS terminal.

2. FORMAT

DEL:SECRTY, USRID="a";

3. EXPLANATION OF MESSAGE

a = The user ID (from 3 to 8 characters in length).

4. SYSTEM RESPONSE

PF = Printout follows.

5. REFERENCES

Output Message(s):
DEL SECRTY

6.5 DEL SECRTY report

ID.....DEL:SECRTY
RELEASE.....5E14 and later
MESSAGE CLASS..NOCLASS
APPLICATION....5
TYPE.....Output

1. FORMAT

DEL SECRTY
a

2. REASON FOR OUTPUT

Lawfully Authorized Electronic Surveillance / 5ESS (Part 5)

Provisioning, Troubleshooting, and Maintenance

235-200-400

June 2003

To report the result of deleting a Security Administrator user ID from the Surveillance Administration System.

3. VARIABLE FIELD DEFINITIONS

a = Status of the command:

COMMAND COMPLETED SUCCESSFULLY
USER ID DOES NOT EXIST
USER ID IS NOT A SECURITY TYPE
A SYSTEM ERROR OCCURRED TRY AGAIN

4. ACTION TO BE TAKEN

If "COMMAND COMPLETED SUCCESSFULLY", no action needs to be taken.
If "USER ID DOES NOT EXIST", check user ID spelling.
If "USER ID IS NOT A SECURITY TYPE", cannot delete a surveillance administrator.
If "A SYSTEM ERROR OCCURRED TRY AGAIN", try again later.

5. ALARMS

None.

6. REFERENCES

Input Message(s) :
DEL:SECRTY

6.6 EXC:PING command

MESSAGE NAME...EXC:PING
RELEASE.....5E14 and later
COMMAND GROUP..TRKLN
APPLICATION....5
TYPE.....Input

1. PURPOSE

The Packet Internet Groper (PING) is used to verify a Transmission Control Protocol/Internet Protocol (TCP/IP) connection between the Source Internet Protocol (SRCIP) address and the Internet Protocol Destination (IPDEST) address. PING sends a request message with data to the IPDEST address and expects a reply from IPDEST, returning the data sent in the request.

Lawfully Authorized Electronic Surveillance / 5ESS (Part 5)

Provisioning, Troubleshooting, and Maintenance

235-200-400

June 2003

Note: Only one EXC:PING input message is allowed per SM or CHNG until the EXC:PING processing is complete. The system response will indicate when the EXC:PING is still in progress. The response message is RL - PING IN PROGRESS. To enter a valid EXC:PING, repeat the input message after a EXC:PING output.

2. FORMAT

```
[1]   EXC:PING,SM=a[,SRCIP=e.f.g.h][,BYTES=i]...
      ...[,TIMEOUT=j][,REPEAT=k],IPDEST=l.m.n.o;
[2]   EXC:PING,CHNG=a-b-c-d[,SRCIP=e.f.g.h][,BYTES=i]...
      ...[,TIMEOUT=j][,REPEAT=k],IPDEST=l.m.n.o;
```

3. EXPLANATION OF MESSAGE

- a = SM number.
- b = PSU unit number. Refer to the APP:RANGES appendix in the Appendixes section of the Input Messages manual.
- c = PSU shelf number. Refer to the APP:RANGES appendix in the Appendixes section of the Input Messages manual.
- d = Channel group (CHNG) number. Refer to the APP:RANGES appendix in the Appendixes section of the Input Messages manual.
- Note: Source IP (SRCIP) is the address the PING is sent from. Each entry (e-i) is part of the SRCIP address. The default is the SRCIP of the SM or CHNG.
- e = SRCIP. This is the address the PING is sent from. The range is 0-255.
- f = SRCIP. The range is 0-255.
- g = SRCIP. The range is 0-255.
- h = SRCIP. The range is 0-255.
- i = BYTES to send in PING Message. This is the number of bytes that will be sent to the IPDEST and the same number of bytes received from the IPDEST. The range is 1-126. The default is 126.
- j = TIMEOUT in seconds waiting from a reply from IPDEST. The range is 1-10. The default is 5.
- k = REPEAT the number of times to send the message to IPDEST.

Lawfully Authorized Electronic Surveillance / 5ESS (Part 5)

Provisioning, Troubleshooting, and Maintenance

235-200-400

June 2003

The range is 1-5. The default is 3.

Note: IP Destination (IPDEST) is the address the PING is sent to.
Each entry (l-o) is part of the IPDEST address.

l = IPDEST. The range is 0-255.

m = IPDEST. The range is 0-255.

n = IPDEST. The range is 0-255.

o = IPDEST. The range is 0-255.

4. SYSTEM RESPONSE

NG = No good. The message was not accepted because the SM is isolated or the equipment does not exist.

NG - NOT VALID FOR PH = No Good. The EXC:PING is not valid for this PH. The feature is not equipped on this PH.

NG - NOT VALID FOR SM = No Good. The EXC:PING is not valid for this SM. The feature is not equipped for this SM.

NG - NOT VALID PROCESSOR = No Good. An invalid processor type was requested, other than SM or PH.

PF = Printout follows. The message was accepted and a printout will follow.

RL - PING IN PROGRESS = Retry Later - Only one ping input message is allowed to execute on the same SM or PH.

RL - CREATE PING TP FAILED = Retry Later - Failed to create the PING Terminal Process.

RL - MESSAGE TO PING TP FAILED = Retry Later - Message sent to the PING Terminal Process Failed.

RL - TIMEOUT WAITING TO PROCESS PINGDATA = Retry Later - A timeout occurred waiting for the PING DATA message in the PING Terminal Process.

RL - BAD DEFAULT = Retry Later - An incorrect message was received in the PING Terminal Process.

RL - SOCKET NOT CREATED = Retry Later - A socket could not be created.

RL - BIND FAILED = Retry Later - A BIND to the socket could not be completed.

Lawfully Authorized Electronic Surveillance / 5ESS (Part 5)

Provisioning, Troubleshooting, and Maintenance

235-200-400

June 2003

RL - SOCKOPT FAILED(BLKING) = Retry Later - When setting BLOCKING for this application, a failure occurred.

RL - SOCKOPT FAILED(TO) = Retry Later - When setting the TIMEOUT for this application, a failure occurred.

5. REFERENCES

Output Message(s):
EXC:PING

Other Manual(s):
235-105-110 System Maintenance Requirements and Tools

6.7 EXC PING report

MESSAGE NAME...EXC PING
RELEASE.....5E14 and later
MESSAGE CLASS..TRKLN
APPLICATION....5
TYPE.....Output

1. FORMAT

[1] EXC PING REPLY FROM SM=a

[2] EXC PING REPLY FROM CHNG=a-b-c-d
PH IMAGE TYPE = e
SOURCE IP = f
DESTINATION IP = g
BYTES SENT = h
TIMEOUT = i

PING TIME STATUS
j k l
.
.
.
.

2. REASON FOR OUTPUT

To output PING information that is sent from an SM or PH.

Format 1 is printed in response to an EXC:PING input message where an SM is INPUT. Format 2 is printed in response to an EXC:PING input message where a CHNG is INPUT.

3. VARIABLE FIELD DEFINITIONS

Lawfully Authorized Electronic Surveillance / 5ESS (Part 5)

Provisioning, Troubleshooting, and Maintenance

235-200-400

June 2003

- a = SM number.
- b = PSU unit number.
- c = PSU shelf number.
- d = Channel group (CHNG) number.
- e = The image type of the PH. If not a PH, this field will read NULL IMAGE.
- f = Source IP address. If zero is displayed the default source address is used.
- g = Destination IP Address.
- h = Bytes sent.
- i = The timeout value, in seconds.
- j = The number of PINGs sent.
- k = The time it takes to receive the PING, in milliseconds.
- l = Status of the PING request.

4. ACTION TO BE TAKEN

None

5. ALARMS

None.

6. REFERENCES

Input Messages
EXC:PING

6.8 OP:TCPIP:RTDMP command

MESSAGE NAME...OP TCPIP RTDMP
RELEASE.....5E14 and later
COMMAND GROUP..TRKLN
APPLICATION....5
TYPE.....Input

Lawfully Authorized Electronic Surveillance / 5ESS (Part 5)

Provisioning, Troubleshooting, and Maintenance

235-200-400

June 2003

1. PURPOSE

The TCP/IP route dump input message is used to verify TCP/IP routing tables in an SM or PH.

2. FORMAT

[1] OP:TCPIP:RTDMP,SM=a;
[2] OP:TCPIP:RTDMP,CHNG=a-b-c-d;

3. EXPLANATION OF MESSAGE

a = SM number.
b = PSU unit number.
c = PSU shelf number
d = Channel group (CHNG) number.

4. SYSTEM RESPONSE

NG = No good. The message was not accepted because the SM is isolated or the equipment does not exist.

NG - NO ROUTE TABLES FOUND = No Good. No entries were found in the ROUTE TABLE on the SM or PH requested.

PF = Printout follows. The message was accepted and a printout will follow.

5. REFERENCES

Output Message(s) :
OP TCPIP RTDMP

Other Manual(s) :
System Maintenance Requirements and Tools

6.9 OP TCPIP RTDMP report

MESSAGE NAME...OP TCPIP RTDMP
RELEASE.....5E14 and later
MESSAGE CLASS..TRKLN
APPLICATION....5
TYPE.....Output

Lawfully Authorized Electronic Surveillance / 5ESS (Part 5)

Provisioning, Troubleshooting, and Maintenance

235-200-400

June 2003

1. FORMAT

[1] OP TCPIP RTDMP ROUTE TABLE DUMP FOR SM=a PAGE e OF f
PH IMAGE TYPE = g

ROUTE NUMBER	DESTINATION IP ADDR	DESTINATION IP MASK	GATEWAY IP ADDR
h	i	j	k
.	.	.	.
.	.	.	.
.	.	.	.

ROUTE METRIC NUMBER	INTERFACE	NEXT ROUTE PTR	PREVIOUS ROUTE PTR
l	m	n	o
.	.	.	.
.	.	.	.
.	.	.	.

[2] OP TCPIP RTDMP ROUTE TABLE DUMP FOR CHNG=a-b-c-d PAGE e OF f
PH IMAGE TYPE = g

ROUTE NUMBER	DESTINATION IP ADDR	DESTINATION IP MASK	GATEWAY IP ADDR
h	i	j	k
.	.	.	.
.	.	.	.
.	.	.	.

ROUTE METRIC NUMBER	INTERFACE	NEXT ROUTE PTR	PREVIOUS ROUTE PTR
l	m	n	o
.	.	.	.
.	.	.	.
.	.	.	.

2. REASON FOR OUTPUT

To output TCP/IP routing information that is contained on an SM or PH.

Format 1 is printed in response to an OP:TCPIP:RTDMP input message where an SM is INPUT. Format 2 is printed in response to an OP:TCPIP:RTDMP input message where an CHNG is INPUT.

The Route Number pertains to all values in ('h'-'o').

3. VARIABLE FIELD DEFINITIONS

Lawfully Authorized Electronic Surveillance / 5ESS (Part 5)

Provisioning, Troubleshooting, and Maintenance

235-200-400

June 2003

- a = SM number.
- b = PSU unit number.
- c = PSU shelf number.
- d = Channel group (CHNG) number.
- e = Current page number.
- f = Total number of pages for this output.
- g = The image type of the PH.
If not a PH this field will read NULL IMAGE.
- h = The route number.
The physical position of the route in the route table.
- i = Destination IP Address.
- j = Destination IP Mask.
- k = Gateway IP Address.
- l = The route metric.
- m = Interface Number for this route.
- n = The Next Route Pointer. If this field has an ENTRY other than 0xffffffff, it will point to the next route entry.
If the field has 0xffffffff as an entry, there is no Next Route.
- o = The previous route pointer. If this field has an ENTRY other than 0xffffffff, it will point to the previous route entry. If the field has 0xffffffff as an entry, there is no Previous Route.

4. ACTIONS TO BE TAKEN

None.

5. ALARMS

None.

6. REFERENCES

Lawfully Authorized Electronic Surveillance / 5ESS (Part 5)

Provisioning, Troubleshooting, and Maintenance

235-200-400

June 2003

Input Message(s):
OP:TCPIP:RTDMP

6.10 REPT CALEA SAS report

MESSAGE NAME...REPT CALEA SAS
RELEASE.....5E14 and later
MESSAGE CLASS..SECLEA
APPLICATION....5
TYPE.....Output

1. FORMAT

```
REPT CALEA SAS ERROR a [f] EVENT=h TIME=ii:ii:ii
ERROR TYPE = et
DATA1 TYPE = d1
[j1 j2 j3 j4 j5 j6 j7 j8]
DATA2 TYPE = d2
[k1 k2 k3 k4 k5 k6 k7 k8]
DATA3 TYPE = d3
[l1 l2 l3 l4 l5 l6 l7 l8]
DATA4 TYPE = d4
[m1 m2 m3 m4 m5 m6 m7 m8]
```

2. REASON FOR OUTPUT

To report the occurrence of a TCP/IP connection breakdown.
When the CDC or PDC connection is down, or the socket interface
is broken, a communication alarm message is sent to the SAS.
For a given MS IP address, only one alarm message is sent to
the SAS for any failure cases.

3. VARIABLE FIELD DEFINITIONS

a = The processor environment where the error message originated.
The environment can either be the Packet Switching Unit
Protocol Handler (PSUPH) which is also referred to as the
physical PH address, or the Switching Module (SM).

Valid values(s):

PSUPH=b-c-d-e
b = Switching module (SM) number.
c = Packet switching unit (PSU) number.
d = PSU shelf number.
e = PSUPH number.

SM=b
b = Switching module (SM) number.

Lawfully Authorized Electronic Surveillance / 5ESS (Part 5)

Provisioning, Troubleshooting, and Maintenance

235-200-400

June 2003

f = The Channel Group (CHNG) assignment if and only if the error message originated from the PH whose PSUPH address is indicated above. The CHNG value is also referred to as the logical PH address. If the error message did not generate from the PSU, then this field is left blank.

Valid values(s) :

CHNG=b-c-d-g
b = Switching module (SM) number.
c = Packet switching unit (PSU) number.
d = PSU shelf number.
g = Channel Group (CHNG) number.

h = Event number

i = Time of the day the message was generated, in the form hours:minutes:seconds.

et = Description of ERROR TYPE message that was sent to the SAS:
For a more detailed description of the CALEA SAS error report, see section 6.15.

Valid types(s) :

Attempt to send a CALEA message to a CALEA process failed
Attempted to add monitoring station when 5 already exist
Bridge Resource Failure
Bridge Loop Channel Unavailable
CCC Dial Out Answer Timeout
CCC Dial Out connection dropped
CCC Dial Out fanout not supported
CCC Dial Out RCV path failed
CCC Dial Out retry failed
CCC Dial Out three port conference circuit dropped
CCC Dial Out three port conference circuit unavailable
CCC Dial Out unsupported supplementary service encountered
CCC Dial Out XMIT path failed
CCCTP can not activate port, can not add
CCCTP can not close network path
CCCTP can not idle all ports
CCCTP can not merge ports on different SMs
CCCTP can not release all ports
CCCTP could not remove CTONE
CCCTP couple port failed, can not add
CCCTP port access failed, can not add
CCCTP port limit exceeded, can not add
CCCTP port limit exceeded, can not merge

Lawfully Authorized Electronic Surveillance / 5ESS (Part 5)

Provisioning, Troubleshooting, and Maintenance

235-200-400

June 2003

CCCTP port move failed, can not merge
CCCTP received MGINTERRUPT on port
CCCTP rcv can not be accessed
CCCTP trunk hunt failed, can not add
CDC Dial Out connection dropped
CDC Dial Out message queue corrupt
CDC Dial Out message queue full
CDC Dial Out setup failed due to invalid data
CDC Dial Out setup failed, will attempt retry
CDC message dropped, GR30 interface send failed
CDC or PDC Message length invalid
Can not create surveillance bridge
Could not apply CTONE
Destination GR30 LEA CDC DN not recognized by digit analysis
Digit Surge Tone Decoder Dropped
Discarding buffered CDC messages due to inactivity
Error return from close application program interface
Error return from connect application program interface
Error return from getsockdesc application program interface
Error return from getsockname application program interface
Error return from select application program interface
Error return from send application program interface
Error return from setsockopt application program interface
Error return from shutdown application program interface
Error return from socket application program interface
Failed to route to GR30 LEA CDC DN
Failed to send GR30 CDC message to link SM
Found socket data inconsistency
GR30 CAGS TP received MGINTERRUPT
GR30 CAGS/CAGR TP cannot be created
GR30 CDC Connection dropped
GR30 CDC message discarded. Link occupancy above threshold
GR30 Internal Failure
GR30 Length of CDC message too large for OSDS
GR30 msg queue full, oldest message discarded
HEARTBEAT message dropped, GR30 interface send failed
IAP times out waiting for login digits
Invalid IP route
Invalid LOGIN digits received
Invalid Protocol Handler CAL_INFO attribute value
IP datagram fragment received
LOGIN message dropped, GR30 interface send failed
LOGIN Successful
No FSK or UTD resources available for GR30 interface
No IP route
No Tone Decoder Available
PDC collection facility IP address not obtained
PSLAESCASE tuple missing when adding new monitoring station
Protocol Handler Resource CAL_INFO Exhaustion
RLCASE_IDX data inconsistency
RLCASE_IDX tuple missing

Lawfully Authorized Electronic Surveillance / 5ESS (Part 5)

Provisioning, Troubleshooting, and Maintenance

235-200-400

June 2003

```
RLEQUIPDSL tuple missing
RLFC_LINE tuple missing
RLGR30INTF tuple missing
RLLAESCASE tuple missing
RLLAESPROF tuple missing
RLOFFICECODE tuple missing
RLPORTLA tuple missing
RLPR_DNTRAN tuple missing
RLRTDNMOD tuple missing
RLRT_DNTRAN tuple missing
Resource Unavailable
Socket not found
Surveillance not started due to SM RLCAL_INFO Exhaustion
Tone Decoder Dropped
Tone Decoder Dropped Due to Load
Too many IP datagrams received
WARNING: GR30 buffered messages will be discarded in 15 minutes
```

```
d1      = Description of DATA1 TYPE associated with the ERROR TYPE above:
d2      = Description of DATA2 TYPE associated with the ERROR TYPE above:
d3      = Description of DATA3 TYPE associated with the ERROR TYPE above:
d4      = Description of DATA4 TYPE associated with the ERROR TYPE above:
```

Valid types(s) :

```
DC Dial Out discarded message
CDC Dial Out message queue pointers
CDC or PDC Message length
CDC event
CDC LEA DN port status value
CDC SVC setup request result
CDC SVC setup response result
CDC SVC setup state result
CDC SVC state value
Collection facility IPv4 address value
Collection facility TCP port value
Data collected for collection facility
Destination SM value
Error return from sockets application program interface
Failure return value
Global Trunk Port value
Highest socket descriptor value
IP datagram count
IP interface identifier
Lawfully authorized electronic surveillance case data
LEA destination DN
Local Trunk Port value
Logical Protocol Handler Number
Msg or value
```

Lawfully Authorized Electronic Surveillance / 5ESS (Part 5)

Provisioning, Troubleshooting, and Maintenance

235-200-400

June 2003

NONE (see Note at end of list)
NUMBER OF PORTS value
Partial IP datagram dump
Party Identifier
Peripheral Control failure value
PH subscriber CALEA information block
Protocol Handler Channel Number
Q.931 Cause Value
Relation ID Value
Relation Key Value
RLCASE_IDX Relation Key Value
RLLAESCAPE Relation Key Value
RLLAESPROF Relation Key Value
Routing and Termination failure value
SM Process Identification value
Socket descriptor list length
Socket descriptor value
Source SM value
Trunk Group value
Trunk Member value

j1 - j8 = Data value(s) in hexadecimal format associated
with a specific DATA1 TYPE above.
Anywhere from 0 to 8 Data Values can appear.

k1 - k8 = Data value(s) in hexadecimal format associated
with a specific DATA2 TYPE above.
Anywhere from 0 to 8 Data Values can appear.

l1 - l8 = Data value(s) in hexadecimal format associated
with a specific DATA3 TYPE above.
Anywhere from 0 to 8 Data Values can appear.

m1 - m8 = Data value(s) in hexadecimal format associated
with a specific DATA4 TYPE above.
Anywhere from 0 to 8 Data Values can appear.

For each ERROR TYPE there will always be 4 DATA TYPE lines.
However, for each non-existent DATA TYPE, "NONE" will print
instead of a valid data type.

For each existing DATA TYPE there can be anywhere from 0 to 8
Data Values. For a non-existing Data TYPE there will be no Data Values.

Each Data Value consists of a 32-bit word of data associated with
its corresponding DATA TYPE in the previous line.

Note that one or more DATA TYPE(S) can be associated with one ERROR
TYPE, and any particular DATA TYPE can be associated with more than
one ERROR TYPES.

Lawfully Authorized Electronic Surveillance / 5ESS (Part 5)

Provisioning, Troubleshooting, and Maintenance

235-200-400

June 2003

Even though each Data Value can be up to 32 bits in length, some data values will be less, and thus their corresponding output value will be LEFT JUSTIFIED. One needs understanding of the DATA TYPE associated with the Data Values to interpret those values correctly. For example, a 16-bit value of h'001A will appear as h'001A0000.

4. ACTION TO BE TAKEN

Consult field expert to determine the cause/solution of the error in question.

5. ALARMS

None.

6. REFERENCES

None.

6.11 UPD:SECRTY command

ID.....UPD:SECRTY
RELEASE.....5E14 and later
COMMAND GROUP..AUTH
APPLICATION....5
TYPE.....Input

1. PURPOSE

This command will be used by the switch System Administrator to update the Security Administrator's password to a new password. The 5ESS System Administrator will have to execute this command from a non-SAS terminal.

2. FORMAT

UPD:SECRTY,USRID="a";

3. EXPLANATION OF MESSAGE

a = The user ID (from 3 to 8 characters in length).

4. SYSTEM RESPONSE

Lawfully Authorized Electronic Surveillance / 5ESS (Part 5)

Provisioning, Troubleshooting, and Maintenance

235-200-400

June 2003

PF = Printout follows.

5. REFERENCES

Output Message(s) :
UPD SECRTY

6.12 UPD SECRTY report

ID.....UPD:SECRTY
RELEASE.....5E14 and later
MESSAGE CLASS..NOCLASS
APPLICATION....5
TYPE.....Output

1. FORMAT

UPD SECRTY
a

2. REASON FOR OUTPUT

To report the result of updating a Security Administrator password.

3. VARIABLE FIELD DEFINITIONS

a = Status of the command:

COMMAND COMPLETED SUCCESSFULLY
PASSWORD MUST BE 6-12 CHARACTERS
USER ID DOES NOT EXIST
UPDATE FAILED

4. ACTION TO BE TAKEN

If "COMMAND COMPLETED SUCCESSFULLY", no action needs to be taken.
If "PASSWORD MUST BE 6-12 CHARACTERS", select a valid password.
If "USER ID DOES NOT EXIST", check user ID spelling.
If "UPDATE FAILED", try again later.

5. ALARMS

None.

6. REFERENCES

Lawfully Authorized Electronic Surveillance / 5ESS (Part 5)

Provisioning, Troubleshooting, and Maintenance

235-200-400

June 2003

Input Message(s) :
UPD:SECRTY

6.13 VFY SECRTY command

ID.....VFY:SECRTY
RELEASE.....5E14 and later
COMMAND GROUP..AUTH
APPLICATION....5
TYPE.....Input

1. PURPOSE

This command is used by the switch System Administrator to list all the Security Administrators user IDs entered into the Surveillance Administration System (SAS). The switch System Administrator will have to execute this command from a non-SAS terminal.

2. FORMAT

VFY:SECRTY;

3. EXPLANATION OF MESSAGE

No variables.

4. SYSTEM RESPONSE

PF = Printout follows.

5. REFERENCES

Output Message(s) :
VFY SECRTY

6.14 VFY SECRTY report

ID.....VFY:SECRTY
RELEASE.....5E14 and later
MESSAGE CLASS..NOCLASS
APPLICATION....5
TYPE.....Output

1. FORMAT

Lawfully Authorized Electronic Surveillance / 5ESS (Part 5)

Provisioning, Troubleshooting, and Maintenance

235-200-400

June 2003

VFY SECRTY
a

USER ID	TYPE
b	SECURITY ADMINISTRATOR
.	.
.	.
.	.

2. REASON FOR OUTPUT

To report the list of Security Administrators user IDs.

3. VARIABLE FIELD DEFINITIONS

a = Status of the command:

COMMAND COMPLETED SUCCESSFULLY
THERE ARE NO ADMINISTRATORS ASSIGNED
A DATA BASE ERROR HAS OCCURRED TRY AGAIN

4. ACTION TO BE TAKEN

If "COMMAND COMPLETED SUCCESSFULLY", no action needs to be taken.
If "THERE ARE NO ADMINISTRATORS ASSIGNED", information only.
If "A DATA BASE ERROR HAS OCCURRED TRY AGAIN", try command again.

5. ALARMS

None.

6. REFERENCES

Input Message(s) :
VFY:SECRTY

6.15 CALEA SAS ERROR TYPE DEFINITION

6.15.1 Introduction

This document provides more detailed description of the CALEA SAS error report. It should be considered as supplementary information to the CALEA document 235-200-400. The customers are encouraged to contact Lucent Technical Support and Service Personnel to resolve any issue that may occur.

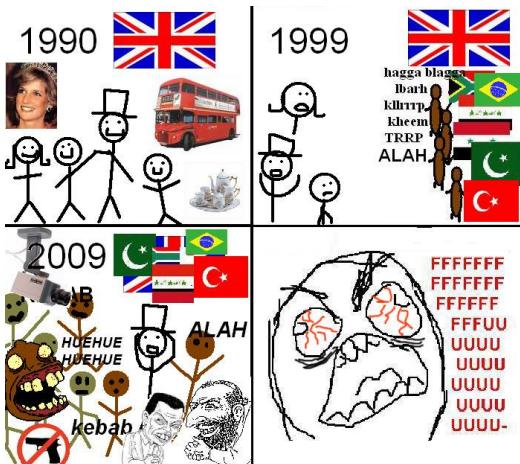
6.15.2 CALEA SAS Error Types

GBPPR MIL-SPEC Laser Dazzler

Overview

The summer of 2011 saw a large amount of rioting and "flash mob" violence committed by non-Whites all over the world. This *just* might be the trigger needed to finally start waking people up...

In the mean time, you may need some non-lethal weapons to help protect yourself, your family, or your business, from these savage beasts.



This project is an improvement on the laser dazzler project from Issue #86. The goal of this laser dazzler is to make it a little more "MIL-SPEC." The physical ruggedness of the overall laser dazzler design will be improved, along with an increase of the laser output power to around 100 milliwatts. An optional 15 Hz laser pulse circuit will also be used to further increase the effectiveness of the laser dazzler.

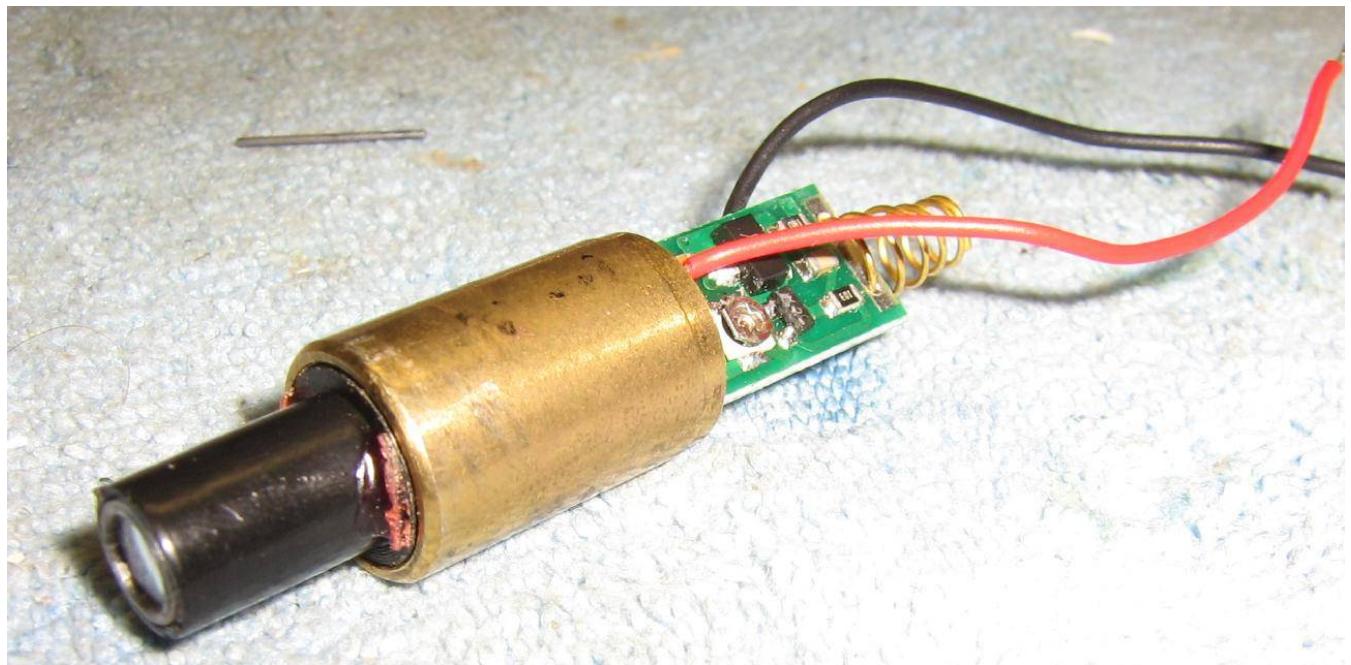
The 100 mW / 532 nm green laser diode module used in this project is the same one which is often available on eBay by various sellers out of Baton Rouge, Louisiana. The laser diode module by itself isn't very rugged, with the main lens assembly being made from plastic and secured using a dab of glue, but for the low-cost (bidding usually starts at 1 cent and will go up to around \$10), this laser diode module will work just fine.

The main body of the laser dazzler will be made from standard PVC pipe components and the laser diode module will be housed in a short piece of copper pipe. This design significantly increases the ruggedness of the laser dazzle and the small copper pipe section acts as a heatsink to help prolong the life of the laser diode.

The dazzler will be powered from two "AA" size batteries providing a total of +3 VDC. The current draw of the laser diode will be around 300 mA. Note that the brass body of the laser diode module will be at a *positive* voltage potential and may require additional isolation from any other circuitry.

The 15 Hz flasher circuit will be made from a CMOS 555 timer and TIP42 PNP pass transistor, all of which will be housed in the PVC handle. 15 Hz was chosen as this is near the "seizure" frequency, but you may wish to experiment with other flashing frequencies. Note that when using the 555 timer for flashing circuits, adding a single diode across one of the timing resistors will give the output a 50% duty cycle.

Pictures & Construction Notes

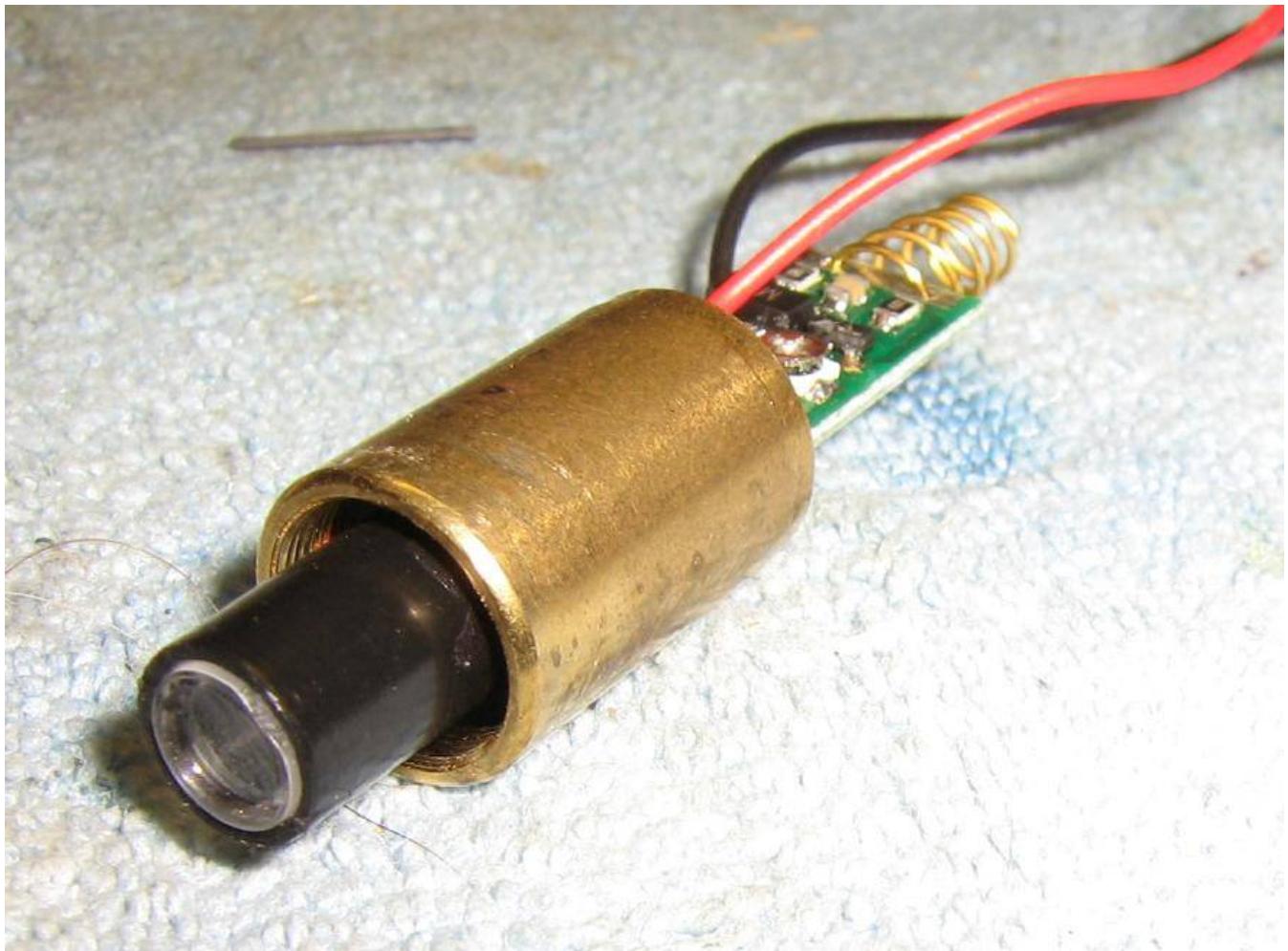


Overview of the stock 100 milliwatt green laser diode module as purchased from eBay for around \$10.



Removing the black plastic lens assembly.

There is a little bit of glue (that red stuff) on the threads which will need to be "broken" in order to adjust the lens assembly.



The stock lens focal setting provides a single point, like a regular laser pointer.

In order to user this laser diode module as a "dazzler," you'll need to expand the beam a bit.

Do this by *carefully* screwing the lens assembly all the way into the brass body.



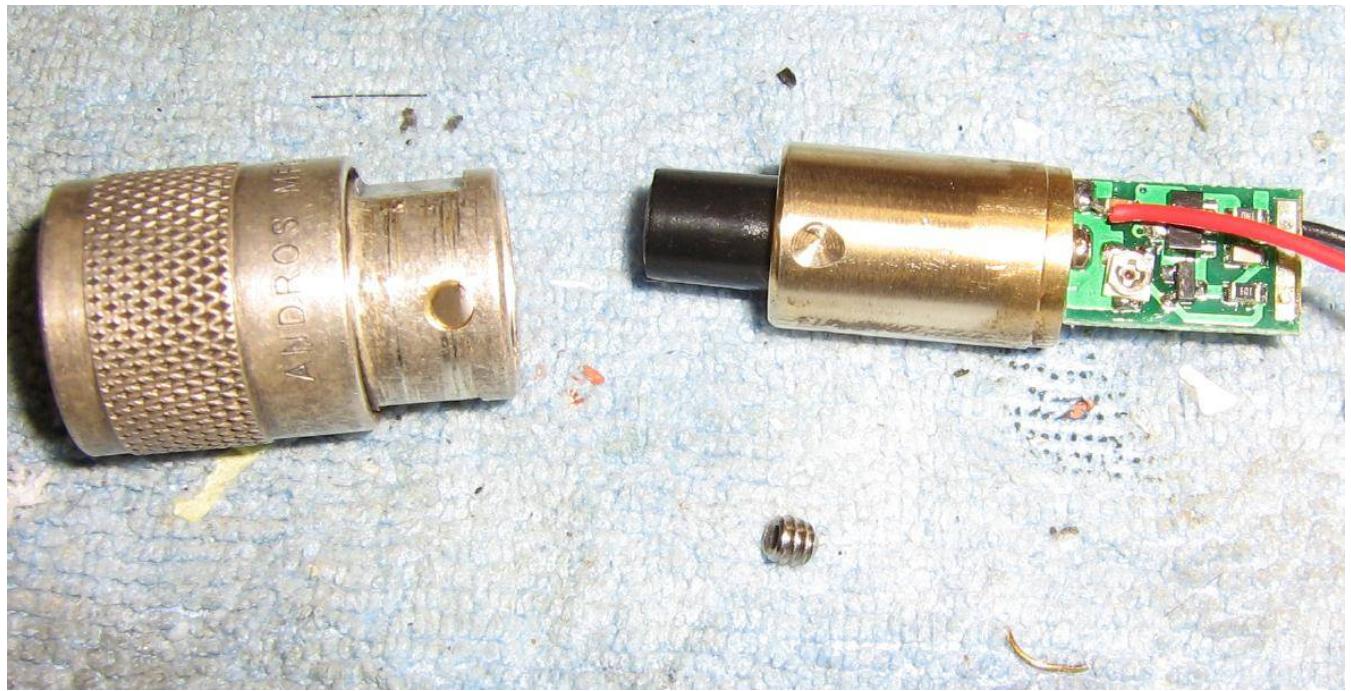
To hold the laser diode module, we'll be using the front section from a 2-piece Andros N connector.

These Andros N connectors are available at most ham radio swapfests or from Tower Electronics (www.pl-259.com) in Green Bay, Wisconsin.



You'll need to drill out the center section and tines of the Andros connector with a 21/64-inch drill bit.

The rubber washer should also be removed.



Next, drill a #43 hole into one side of the thicker section of the Andros connector, as shown above.

Tap the hole for #4–40 thread. *Carefully* make a matching divot in the brass body of the laser diode module.

A #4 set screw will secure the laser diode module into the rear of the Andros connector.



The front-end of the laser dazzle will be made from a 3-inch long piece of 1-inch diameter copper pipe and two matching end caps.

Drill 5/8-inch diameter holes in each of the end caps.

A panel-mount double-female N connector will be used as the attachment point to hold the laser diode module in the Andros connector. It will also be an attachment point for any additional external lenses.

You'll need to drill (or burn out) the center conductor and insulator material of the panel-mount double-female N connector.



Attach the panel-mount double-female N connector to one of the copper pipe end caps.

Note the internals of the N connector have been removed.



On the other copper pipe end cap, drill a 1/8-inch hole all the way through (near the end) and through the matching 3-inch piece of copper pipe.

Solder an old panel-mount N jack to the end cap. This jack should also have its internal center conductor and insulator material removed.

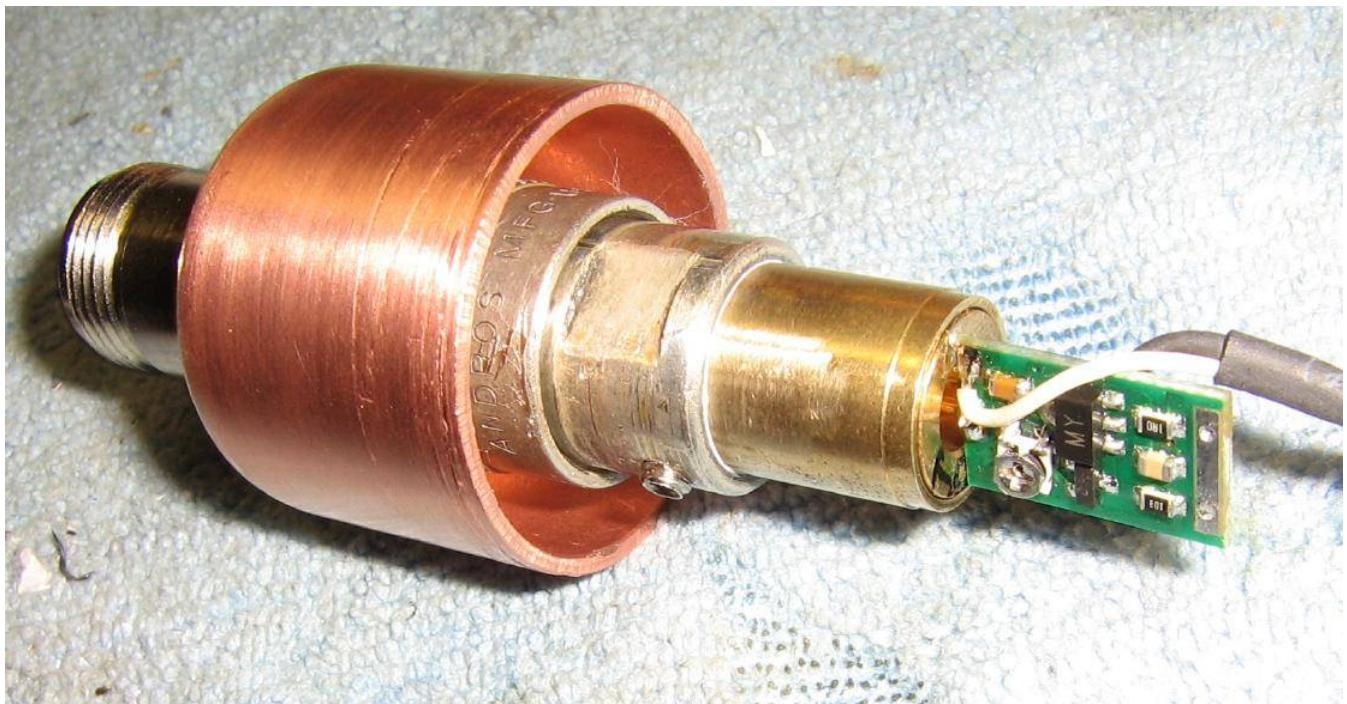
This will be the attachment point to secure the copper pipe front-end to the PVC handle.



Internal view of the soldered panel-mount N jack.

Note the internals of the panel-mount N jack have been removed.

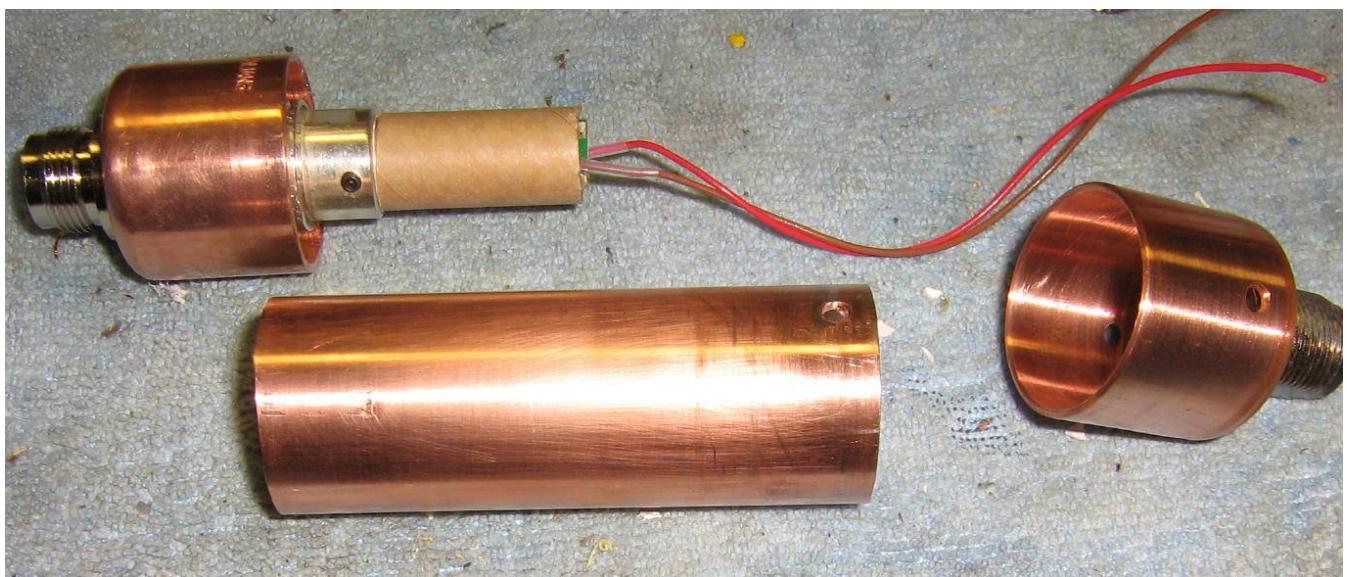
You'll need to use a propane torch in order to provide enough heat solder the N jack.



Attach the laser diode module connector to the panel-mount double-female N connector, as shown above.

You'll also want to solder two longer power wires to the laser diode module at this time. Teflon wire is recommended.

A dab of Loctite on the threads of the N connectors is also recommended.



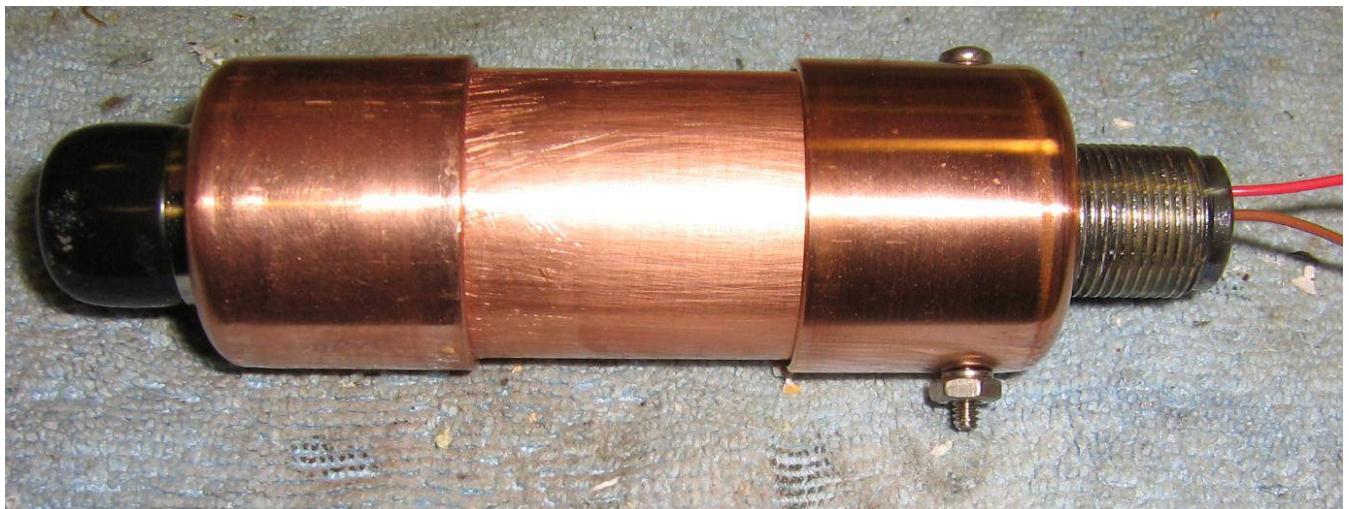
Prepare and clean the the copper pipe sections with Copper Glo and a scrub pad.

An optional short piece of cardboard tube from a model rocket was slipped over the laser diode module driver board.



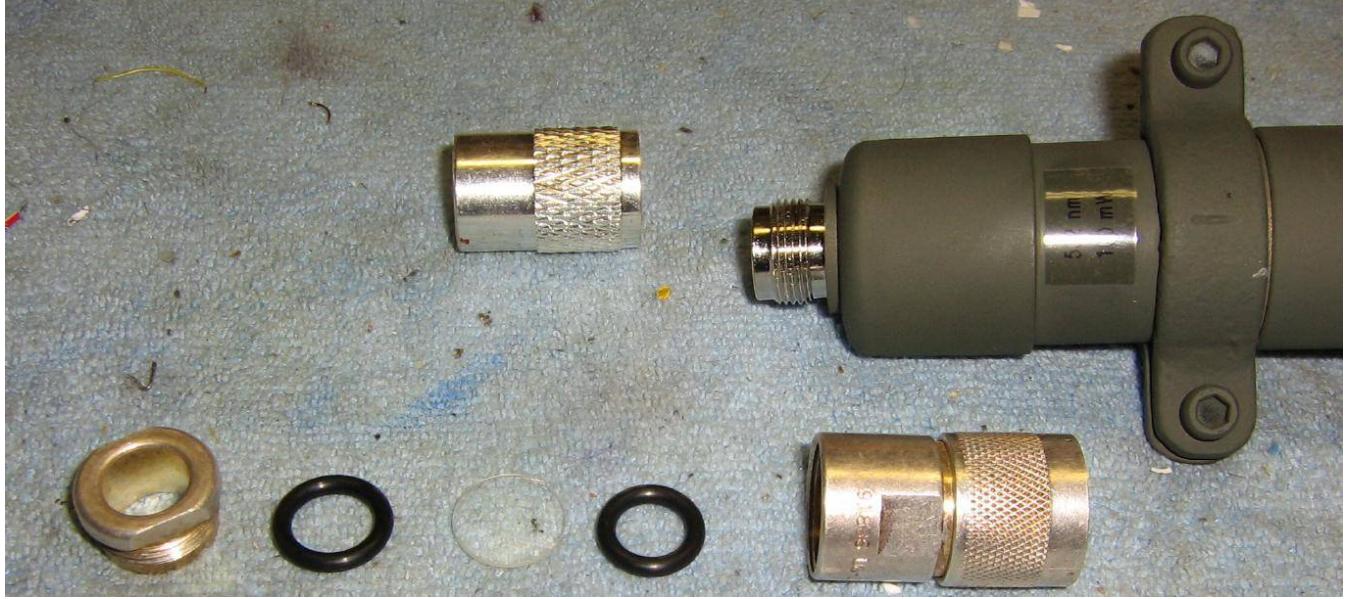
The front copper pipe end cap will be attached to the 3-inch long piece of copper pipe using some JACO Just-For-Copper solderless bonding glue.

Each section which the JACO Just-For-Copper is to be applied should be cleaned with emory cloth.



Completed laser diode module section.

The rear copper pipe end cap is held on using a long #4 bolt to make removal easier.



Optionally, to make an external beam expansion lens, use an old RG-8 compression male N connector to hold the lens between two neoprene O-rings.

Experiment with different lenses to get different beamwidths. You can salvage small lenses from some older video cameras.

A protective cap was made from the shell of an old PL-259 connector with tape over the open end.



Completed beam expansion lens mounted inside an old RG-8 male N connector.



To use the beam expansion lens, just screw it onto the matching N jack of the laser dazzler.

A plain piece of glass can also be used to make a optically-transparent protective cap for the laser dazzler.



If the lens requires an extended focal length, you can use long pieces of double SO-239 connectors when attaching the beam expansion lens.



To remove the center conductor and insulator material, heat them up using a propane torch and the internal center connector should just slide out.



Connect the double SO-239 connector to the laser dazzle with a cut down section from an old PL-259 connector shell.



Example of a lens which required a longer focal length attached to the laser dazzle.



Next is constructing the PVC body for the handle section of the laser dazzler.

You'll need one 1.25-inch diameter PVC cap (Genova 30159), one 5-inch long section of 1.25-inch diameter PVC pipe, one 1.25-inch diameter PVC female adapter (Genova 70314), and one 1.25-inch diameter PVC threaded plug MIP (Genova 31814).

A small piece of aluminum channel stock was cut for use as an optional switch guard.

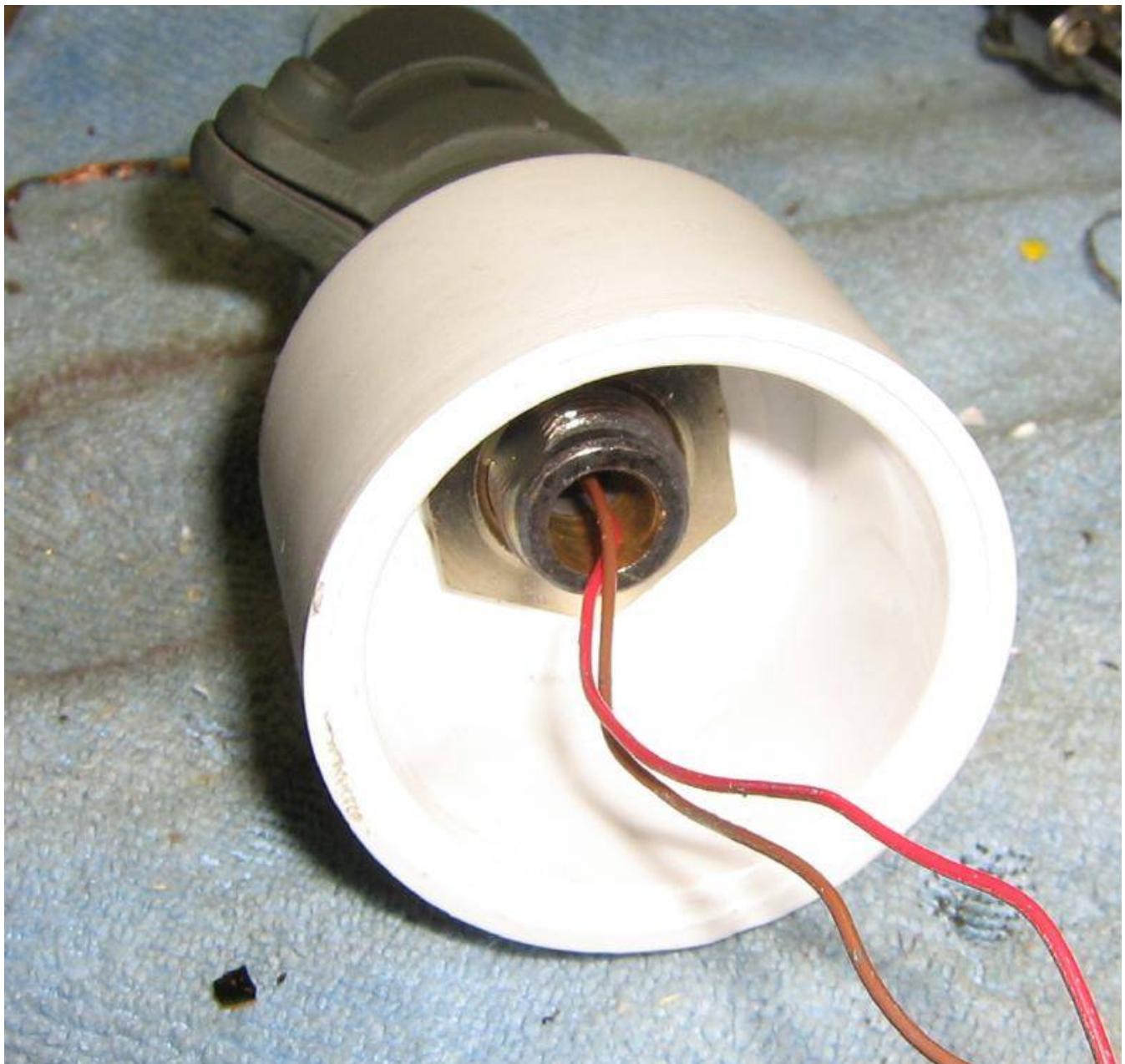


The laser dazzle will be powered via two "AA" 1.5 volt batteries.

To secure the battery holder inside the PVC pipe handle, a couple of rubber grommets will be slid over a bolt which is then mounted inside the PVC pipe handle.

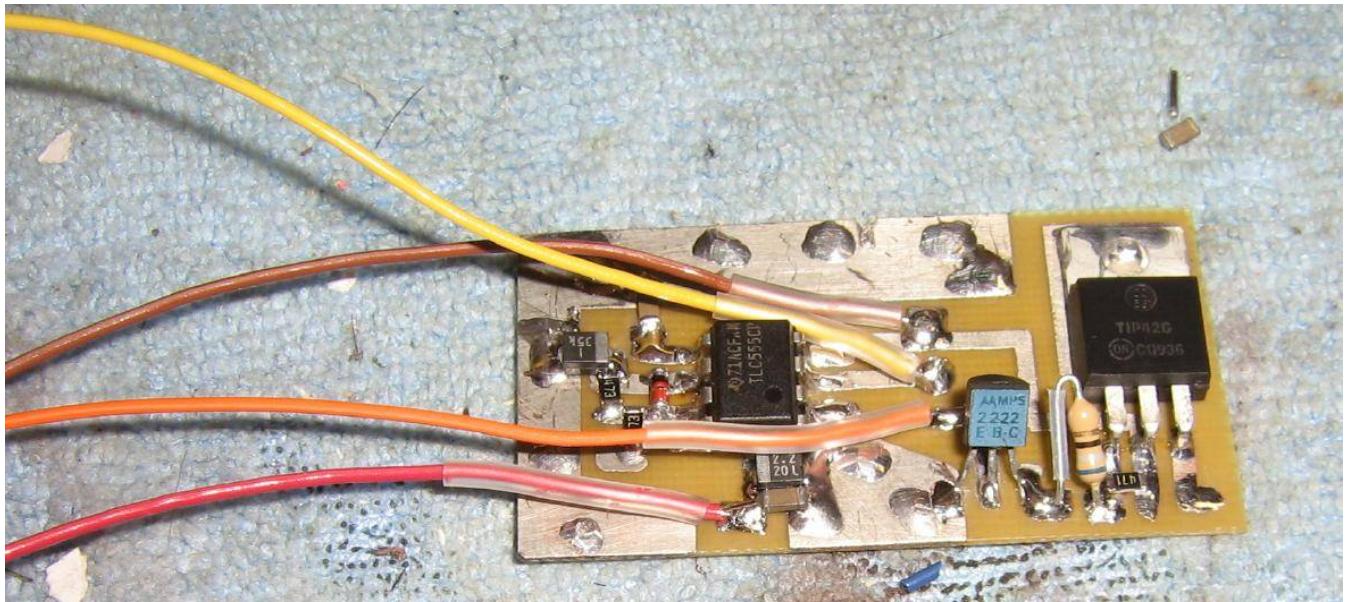
Note the threaded PVC plug was cut down a bit so it doesn't stick out so far.

A 1/4-inch hole should be drilled into the PVC pipe handle for the selector switch.



Drill a 5/8–inch hole in the center of the 1.25–inch diameter PVC cap.

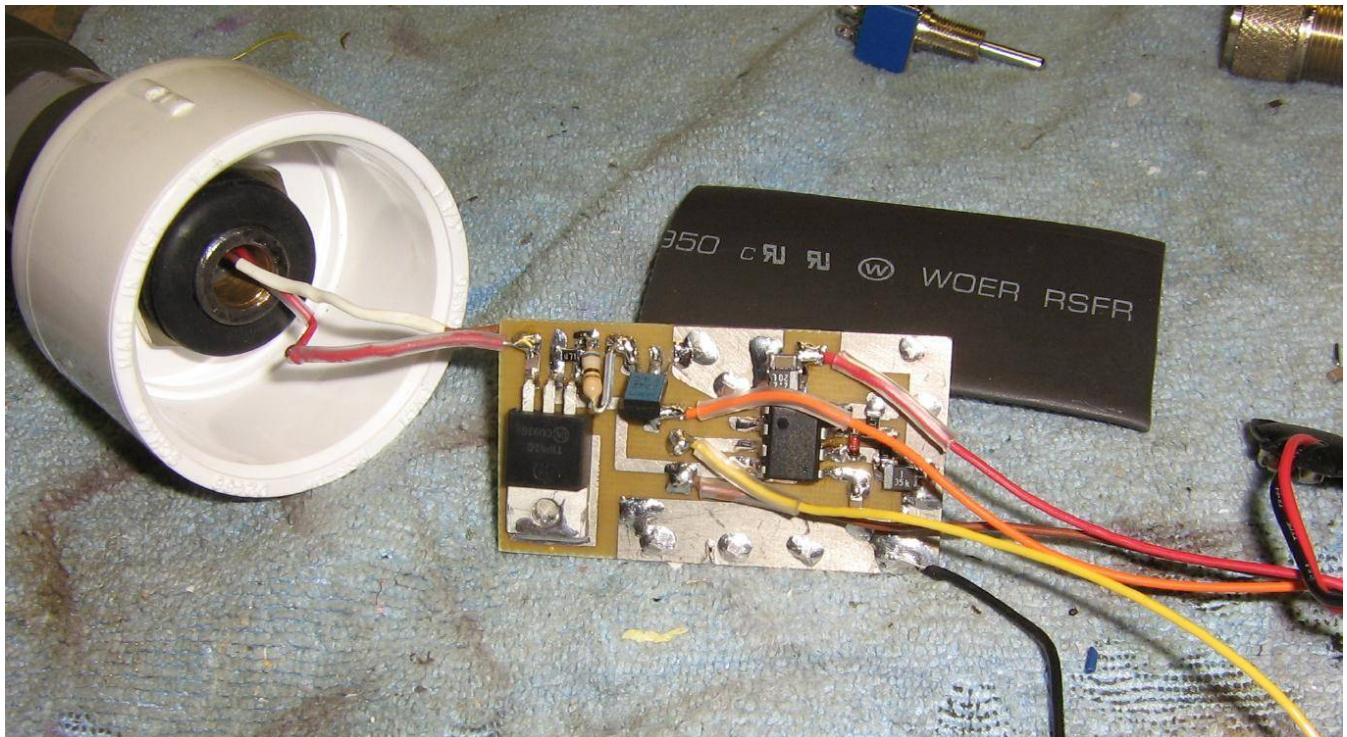
Attach the cap to the laser diode section via the modified N connector and a matching nut, also salvaged from an old panel–mount N or SO–239 connector.



Overview of the laser diode flasher circuit.

A CMOS 555 timer pulses a TIP42 transistor at around 15 Hz, this in turn controls the +3 volts going to the laser diode module.

A center-off DPDT switch controls the "15 Hz," "CW," or "OFF" settings and main flasher circuit power.



Preparing the circuit board to be mounted in the PVC pipe handle.



The circuit board was slid inside a piece of heat-shrink tubing.

Note that the circuit board should *not* touch any metal parts on the front laser diode section which are at a positive voltage potential.

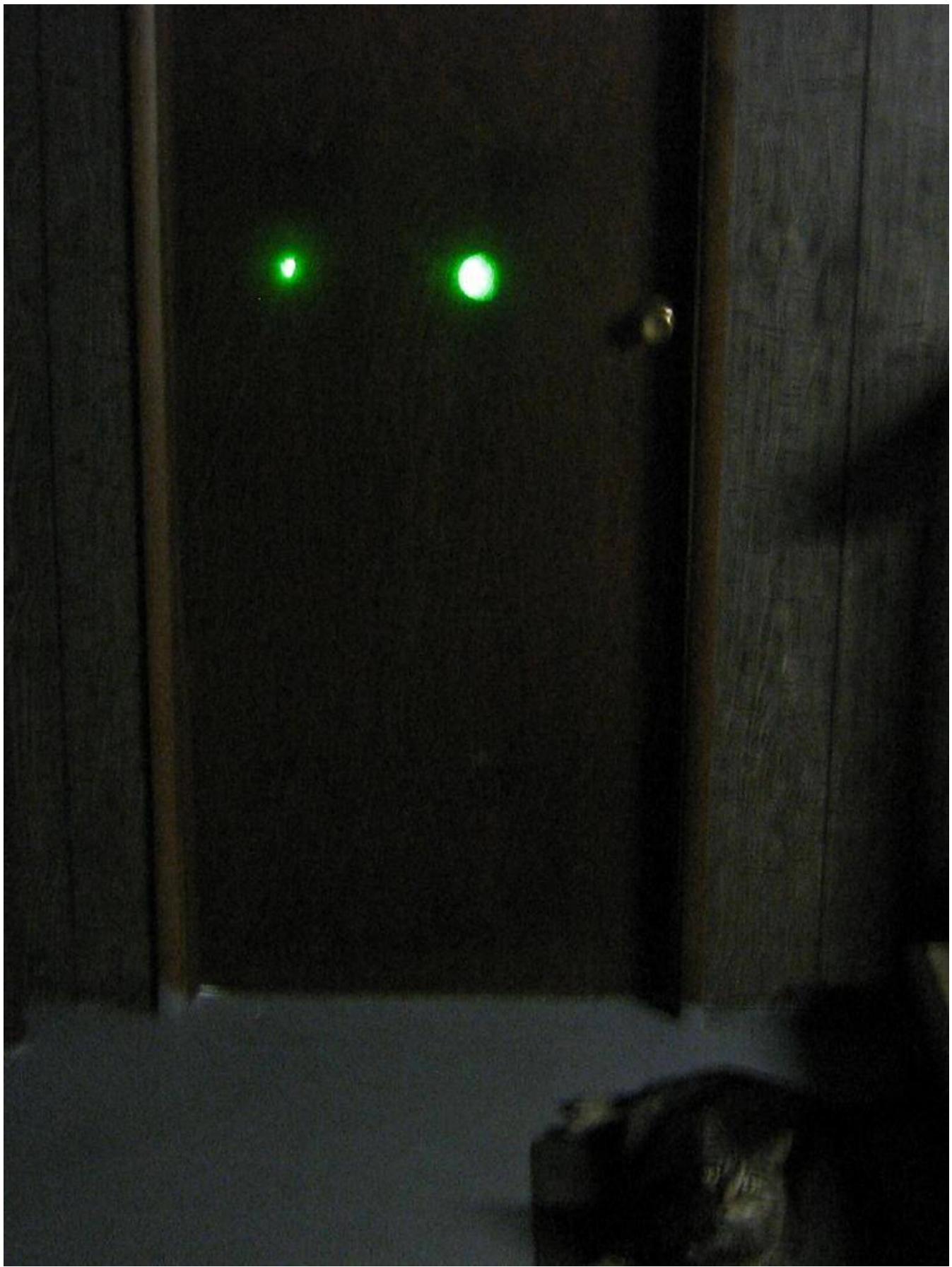


Internal handle view showing the rubber grommets on the bolt which the battery holder will press up against.



Completed laser dazzler.

Note that a 1-inch diameter copper pipe hanger mount was added to the front laser section to act as an additional heatsink and as a mounting point.

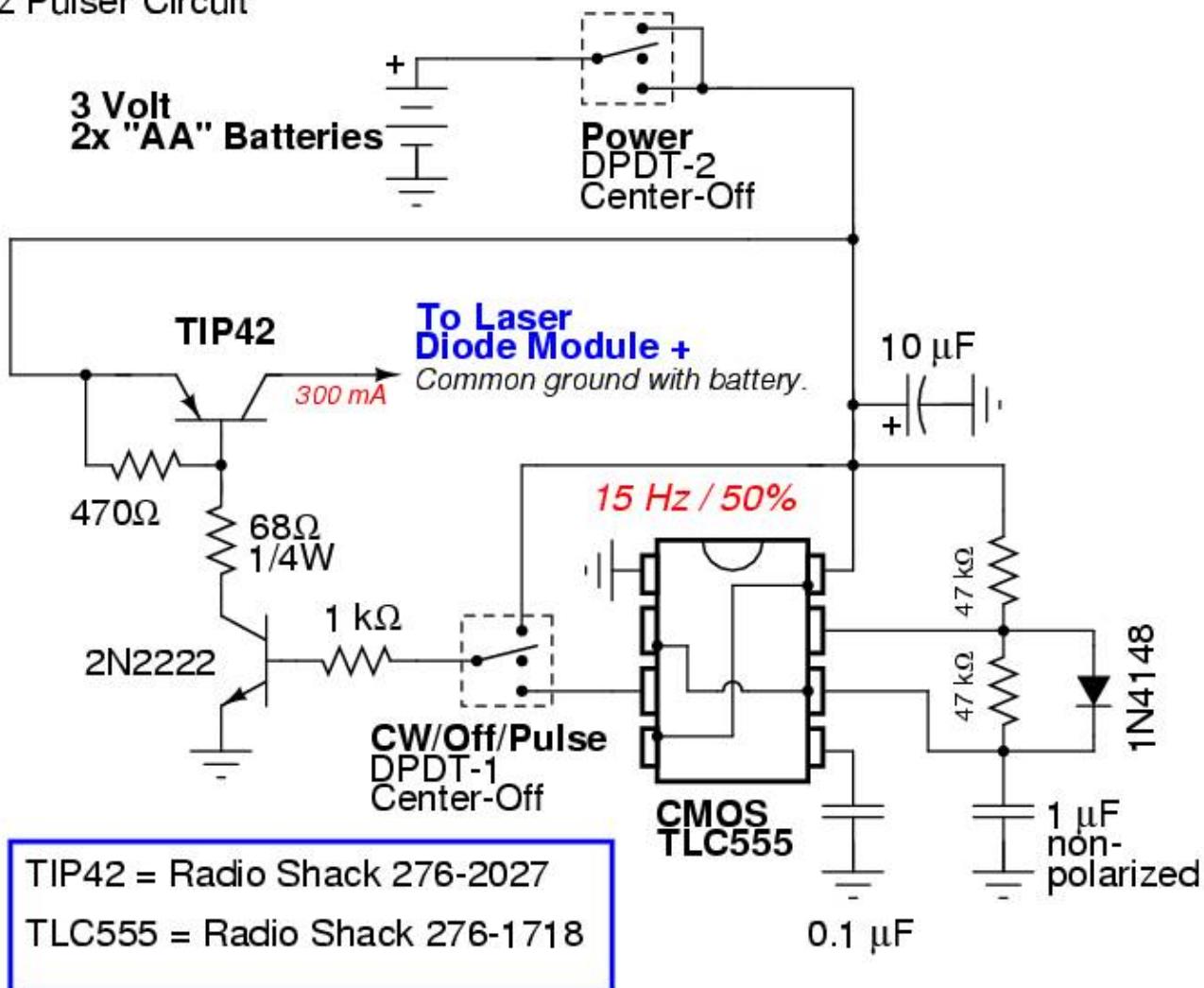


Laser dazzler beam (right) compared to a regular laser pointer (left) from around 10 feet.

Schematic

GBPPR MIL-SPEC Laser Dazzler

15 Hz Pulser Circuit



Motorola STF2520A 900 MHz Power Amplifier Modifications

Overview

This is a project to modify a surplus Motorola STF2520A 800 MHz cellular-band RF amplifier for use in the 900 MHz amateur radio band. Note that this is a "low power" cellular amplifier, but it has a RF output of around 150 watts with only a few watts of drive.

The Motorola STF2520A's +24 volts at 15 amps DC power requirements are non-standard for ham gear, and this may be difficult to supply. Two decent-sized, 12 volt lead-acid batteries wired in series will work fine if you don't have a proper power supply. You can keep the batteries topped off with a trickle charger. Note that this amplifier has a *maximum* voltage rating of +28 VDC, and it's best to run it at only +24 VDC.

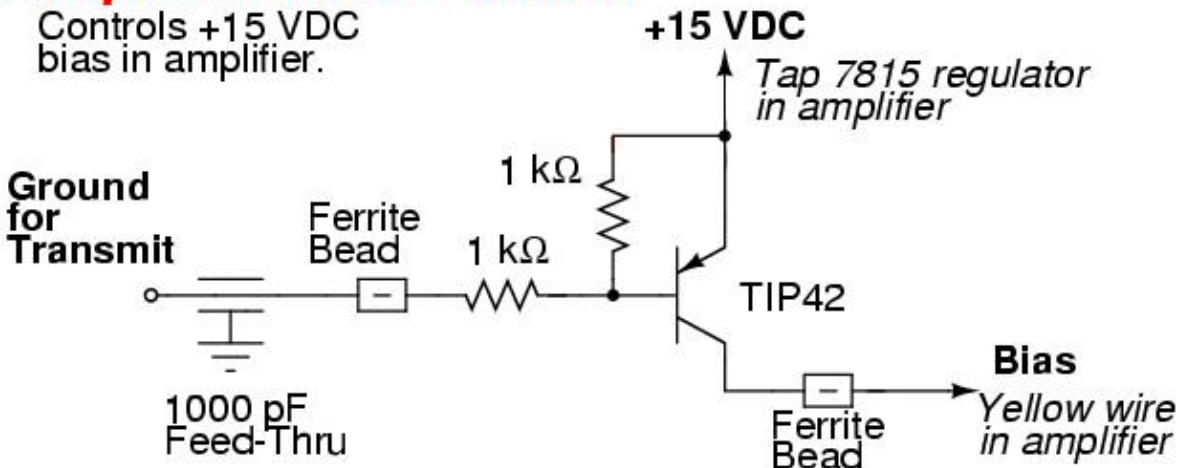
The stock Motorola STF2520A amplifier doesn't really require any board-level changes to operate in the 900 MHz region, but it does help (in some cases) to remove the output RF isolator, and you'll also need to add some new RF connectors for the RF input and output.

An optional "ground for transmit" bias control circuit will be added to this amplifier. This is handy if your application needs to power down the amplifier during a receive cycle. By default, the amplifier is always biased on. This +15 VDC bias voltage is provided via the **YELLOW** wire inside the amplifier.

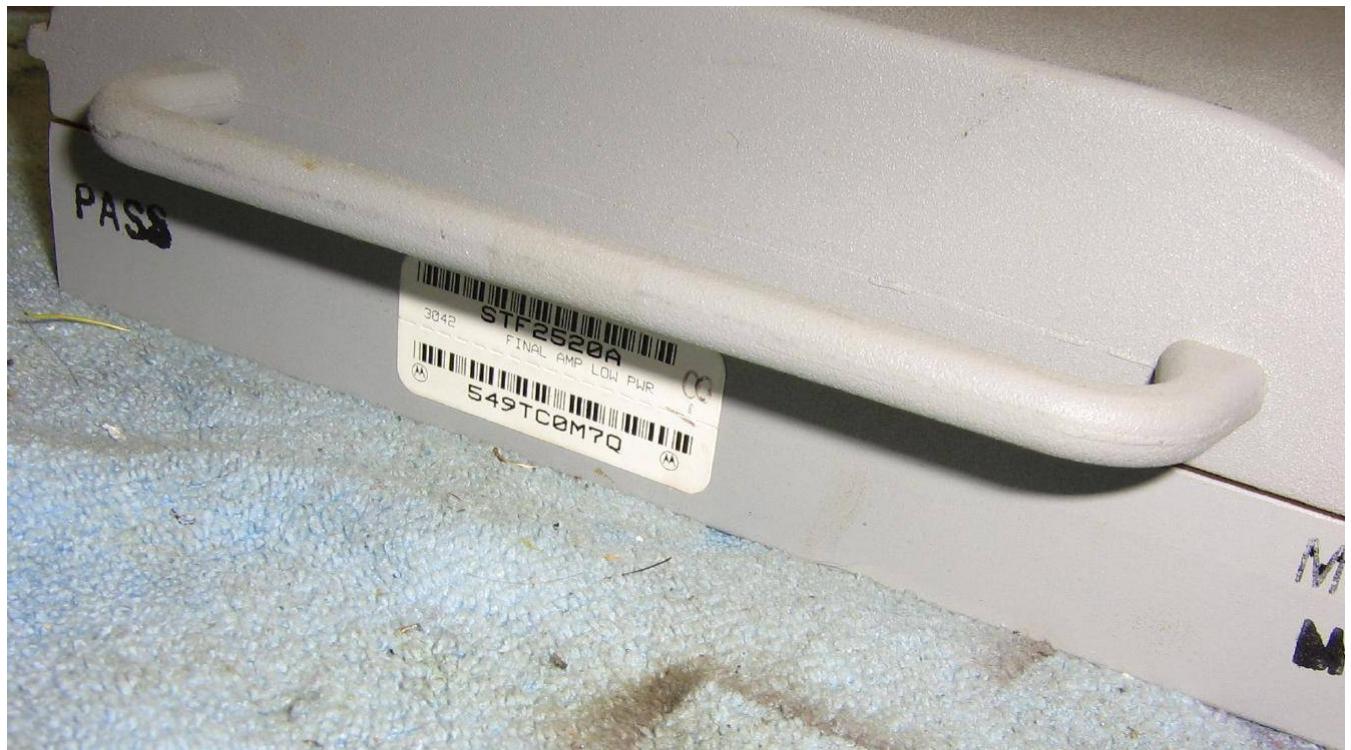
The stock Motorola STF2520A 800 MHz cellular-band amplifier requires 2 – 5 watts of RF drive power for 150 watts output. The amplifier is biased for class AB, so it is slightly linear. Back off the RF input power to prevent any more distortion. Since this amplifier was designed for 100% duty cycle operation, it has a very rugged physical construction. You'll just want to make sure the fins of the heatsink are *vertical* to help with the heat dissipation to prevent overheating.

Amplifier Bias Control

Controls +15 VDC bias in amplifier.



Pictures & Construction Notes



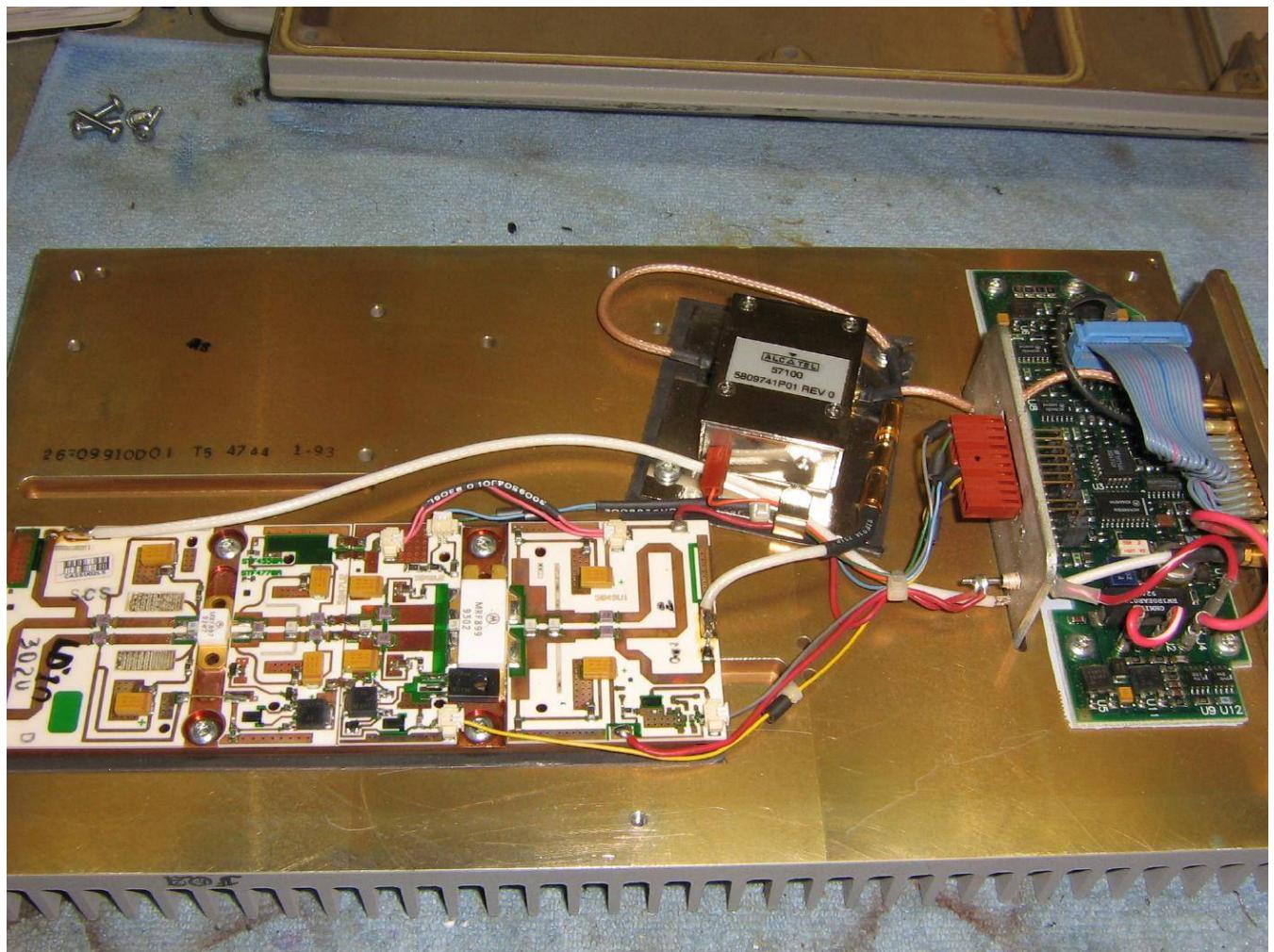
Overview of the label on a stock Motorola STF2520A 800 MHz cellular-band amplifier.

You can find these amplifiers on eBay or at ham radio swapfests at very low prices.



Overview of the main connector on a stock Motorola STF2520A 800 MHz cellular-band amplifier.

This connector provides both the RF input and output and the DC power for the amplifier.



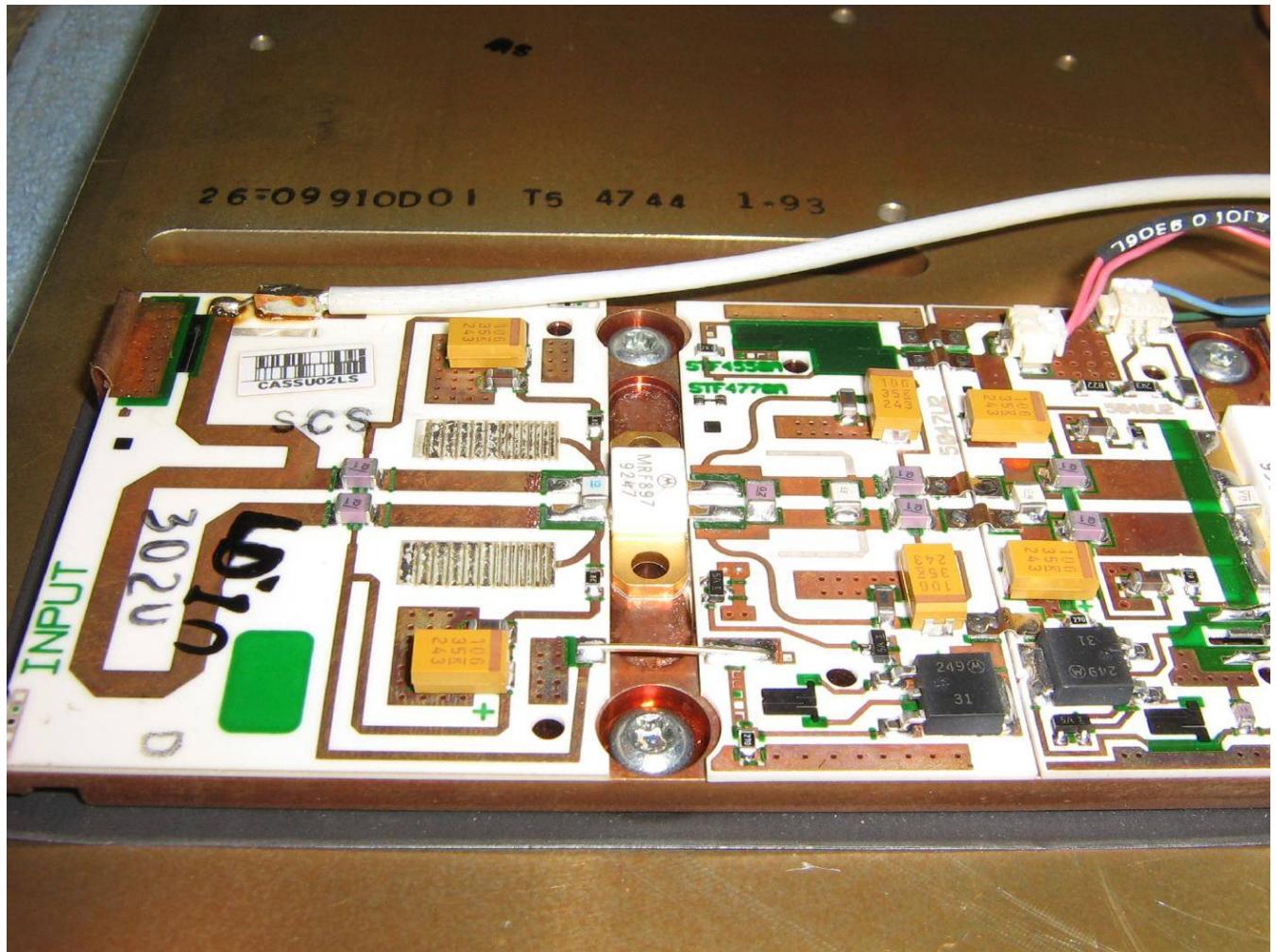
Internal view of a stock Motorola STF2520A 800 MHz cellular-band amplifier.

The low-power version of this amplifier is quite minimal in components.

The RF isolator is the silver box in the upper-middle.

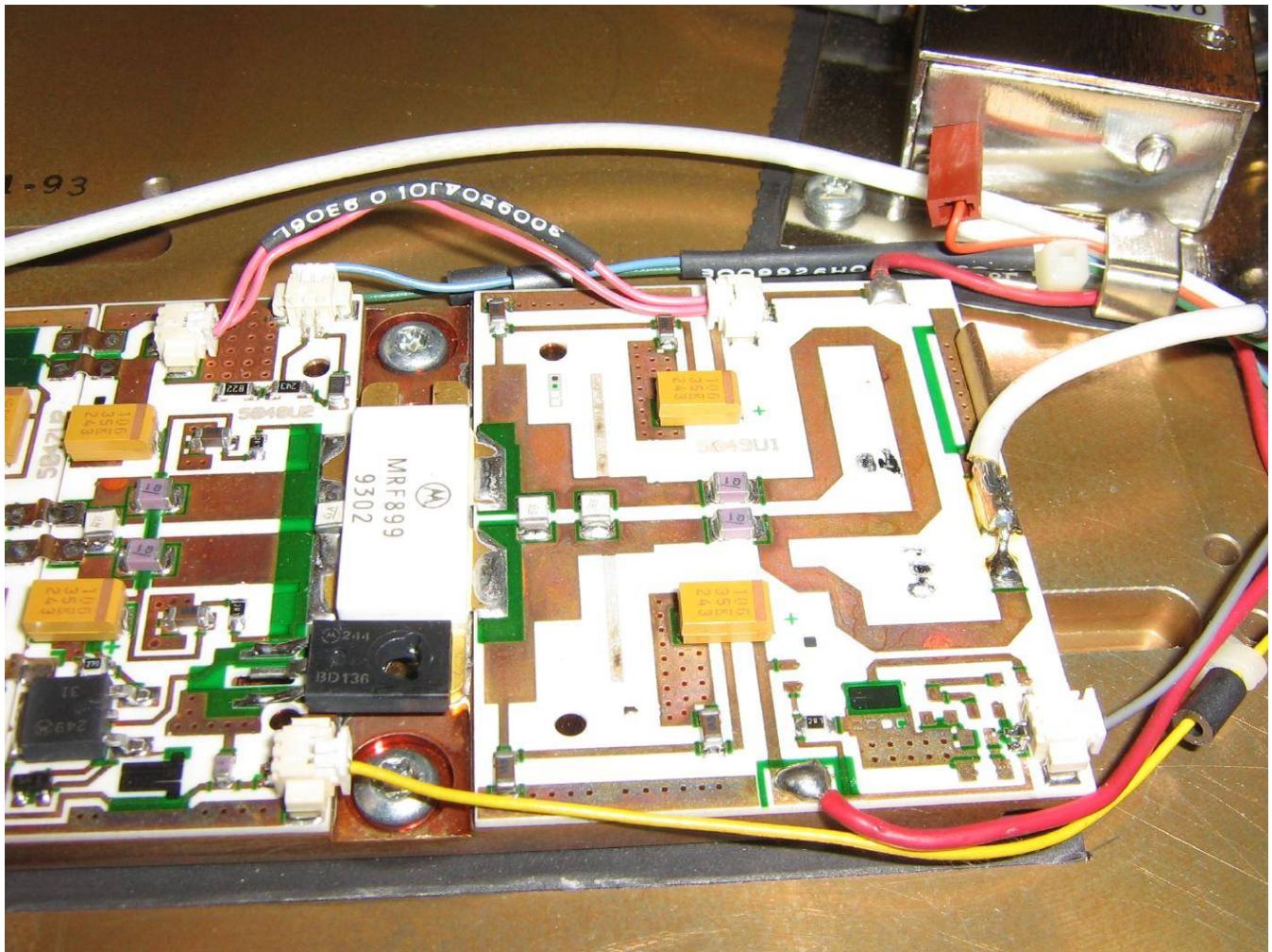
RF input is on the left side of the circuit board, RF output on the right, going through the isolator.

The power supply circuit board is on the far-right.



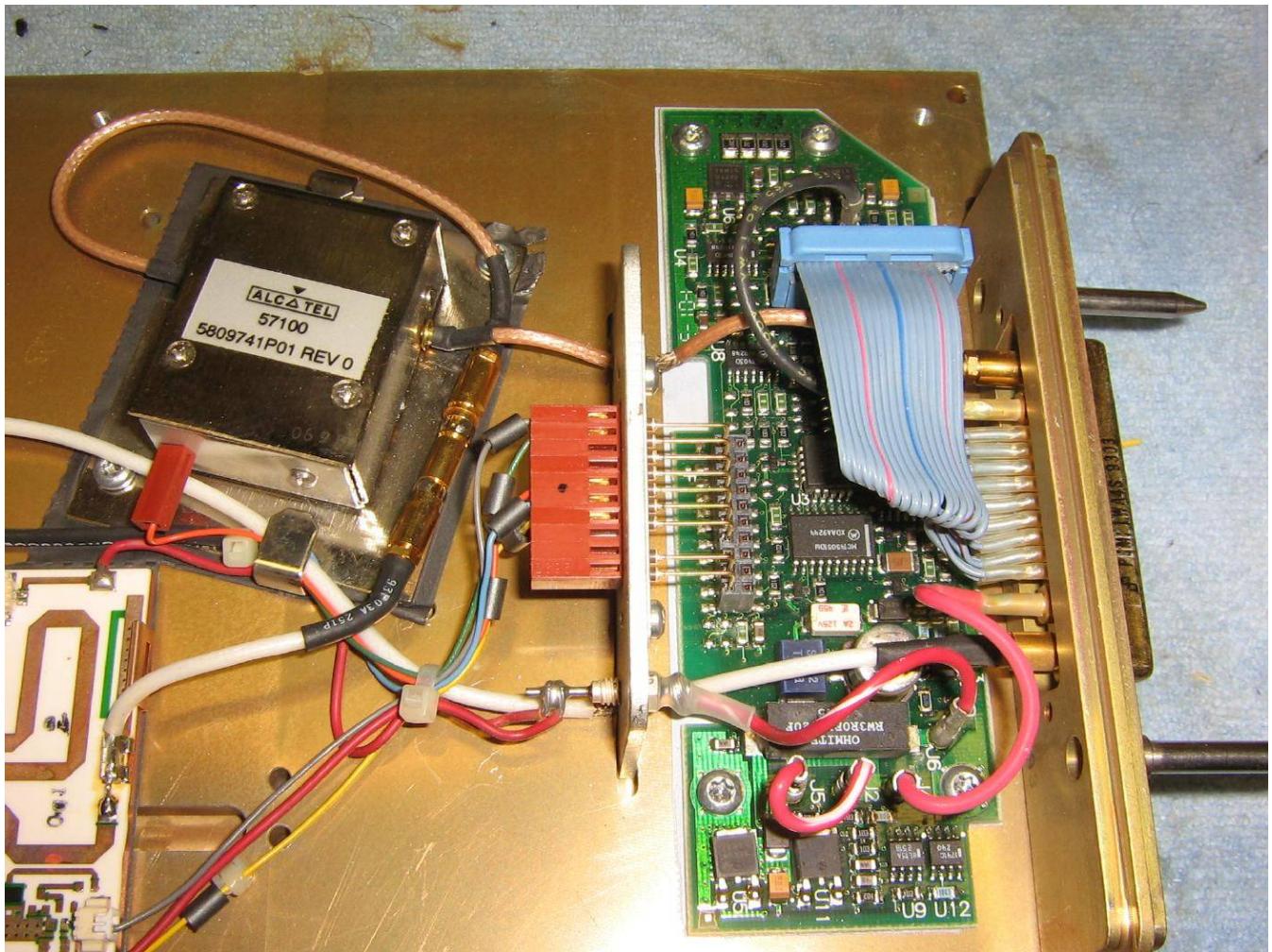
RF input section of the Motorola STF2520A 800 MHz cellular-band amplifier.

The input RF transistor is a Motorola MRF897. At 900 MHz, it provides around 12 dB of gain and will give around 30 watts RF output with around 2 watts input.



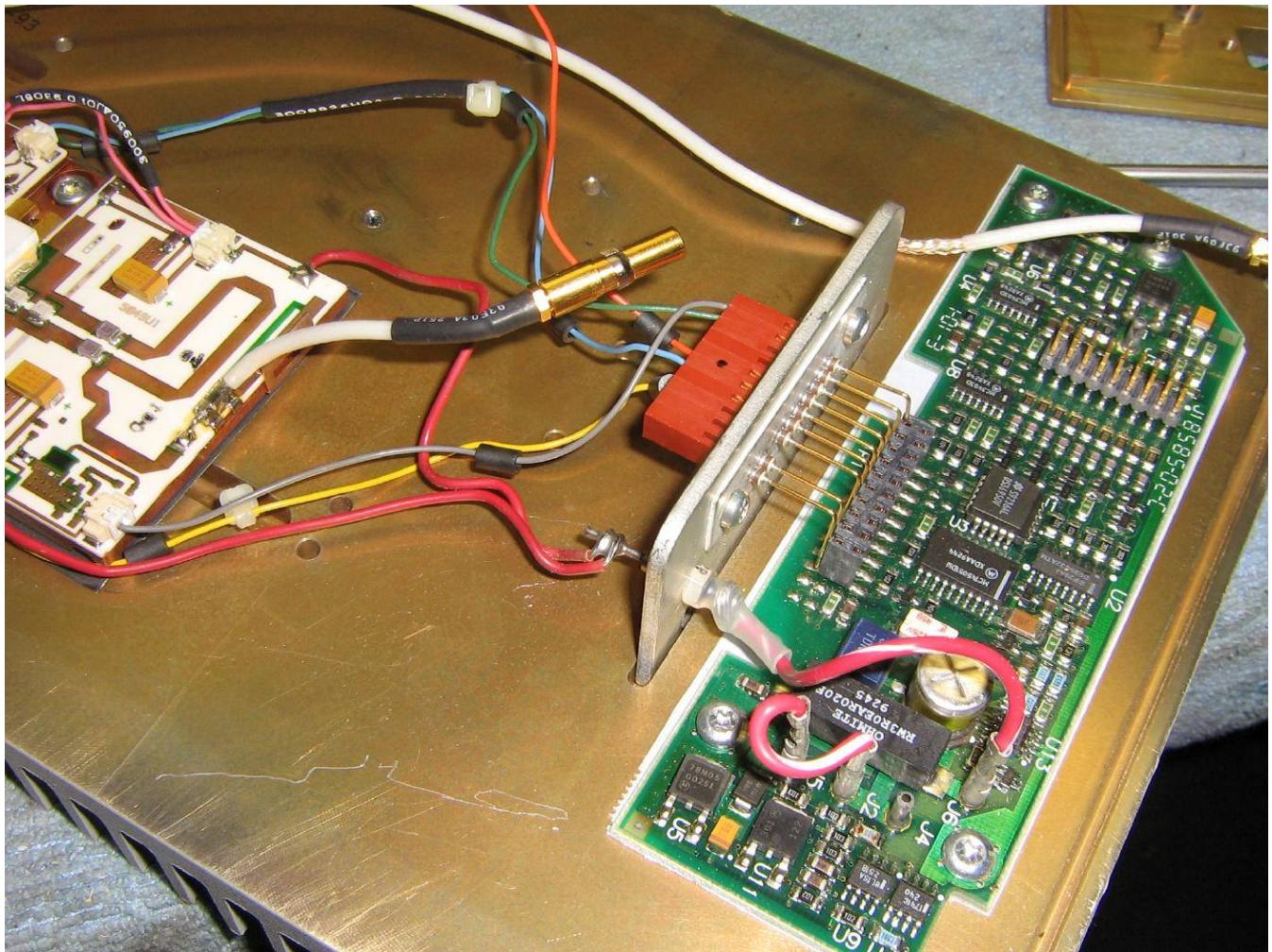
RF output section of the Motorola STF2520A 800 MHz cellular-band amplifier.

The output RF transistor is a Motorola MRF899. At 900 MHz, it provides around 9 dB of gain and will give around 150 watts RF output with around 20 watts input.



Overview of the output RF isolator and DC power control circuit board of the Motorola STF2520A 800 MHz cellular-band amplifier.

The stock RF isolator has a fairly poor response in the higher portion of the 900 MHz band, so it should be removed. Adding an external RF isolator is highly recommended.



Removing the RF isolator.

You'll need to add longer coaxial cables on the RF input and output.

Only the **RED** wires and **YELLOW** wire going to the amplifier are required.

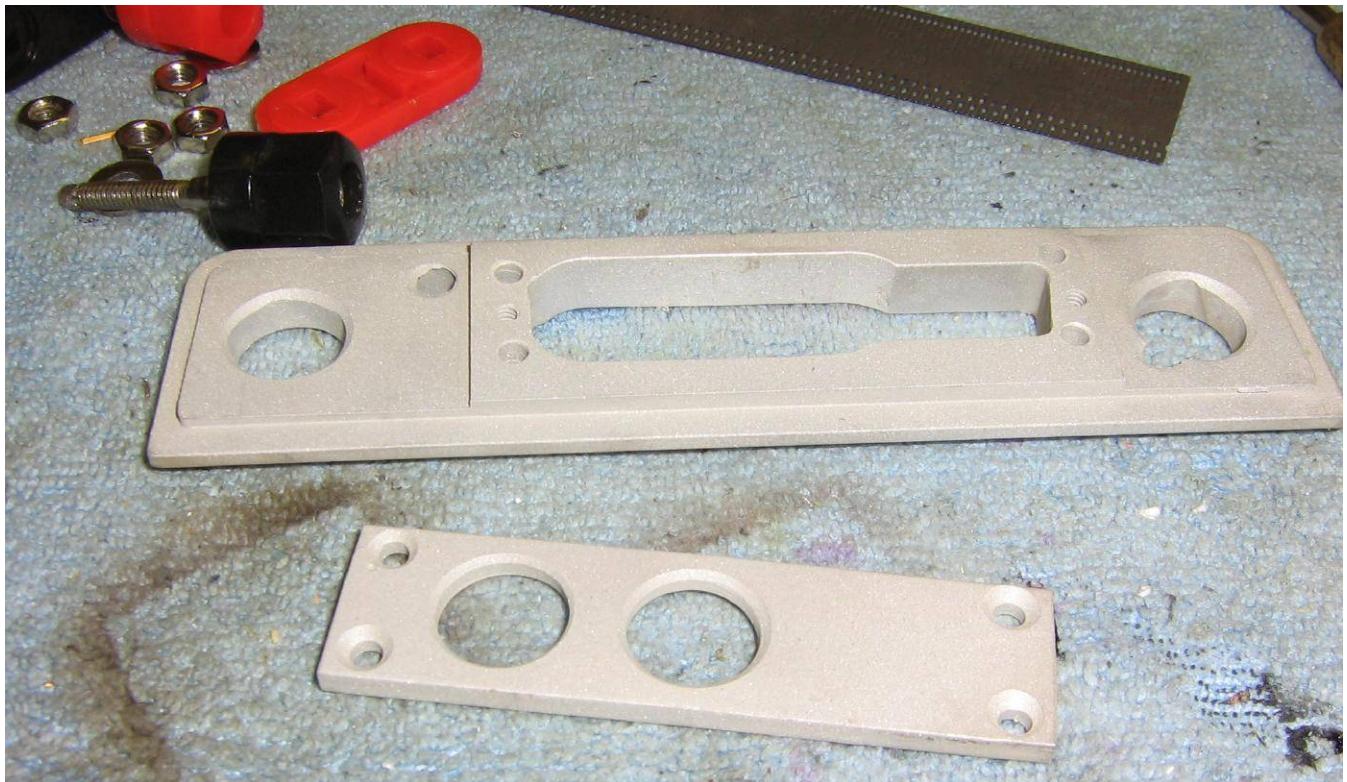
The **RED** wires carry the +24 VDC and the **YELLOW** wire is the +15 VDC bias control. By controlling the application of the bias voltage you can power down the amplifier, if so required.

You can trim the other wires (gray, blue, green, & orange), saving the ferrite beads for other uses.



Removing the connector faceplate.

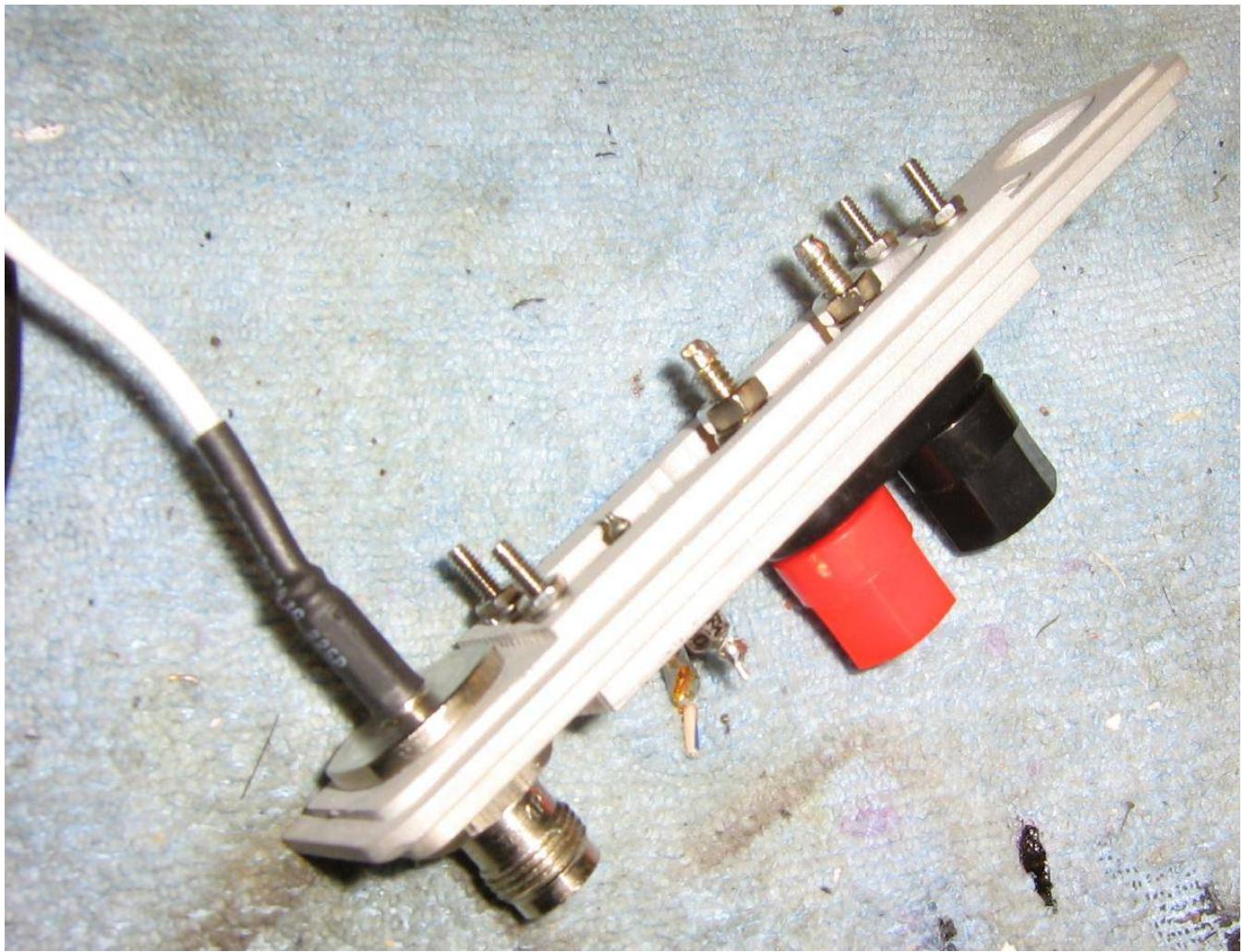
The faceplate will be slightly modified by adding new RF input and output jacks and banana jacks for DC power.



Cleaning up the faceplate.

The ends where machined down a bit and two 1/2-inch holes were drilled for adding panel-mount TNC connectors.

A small aluminum plate was made to fit over the original faceplate connector hole. This little plate will hold the banana jacks for DC power.

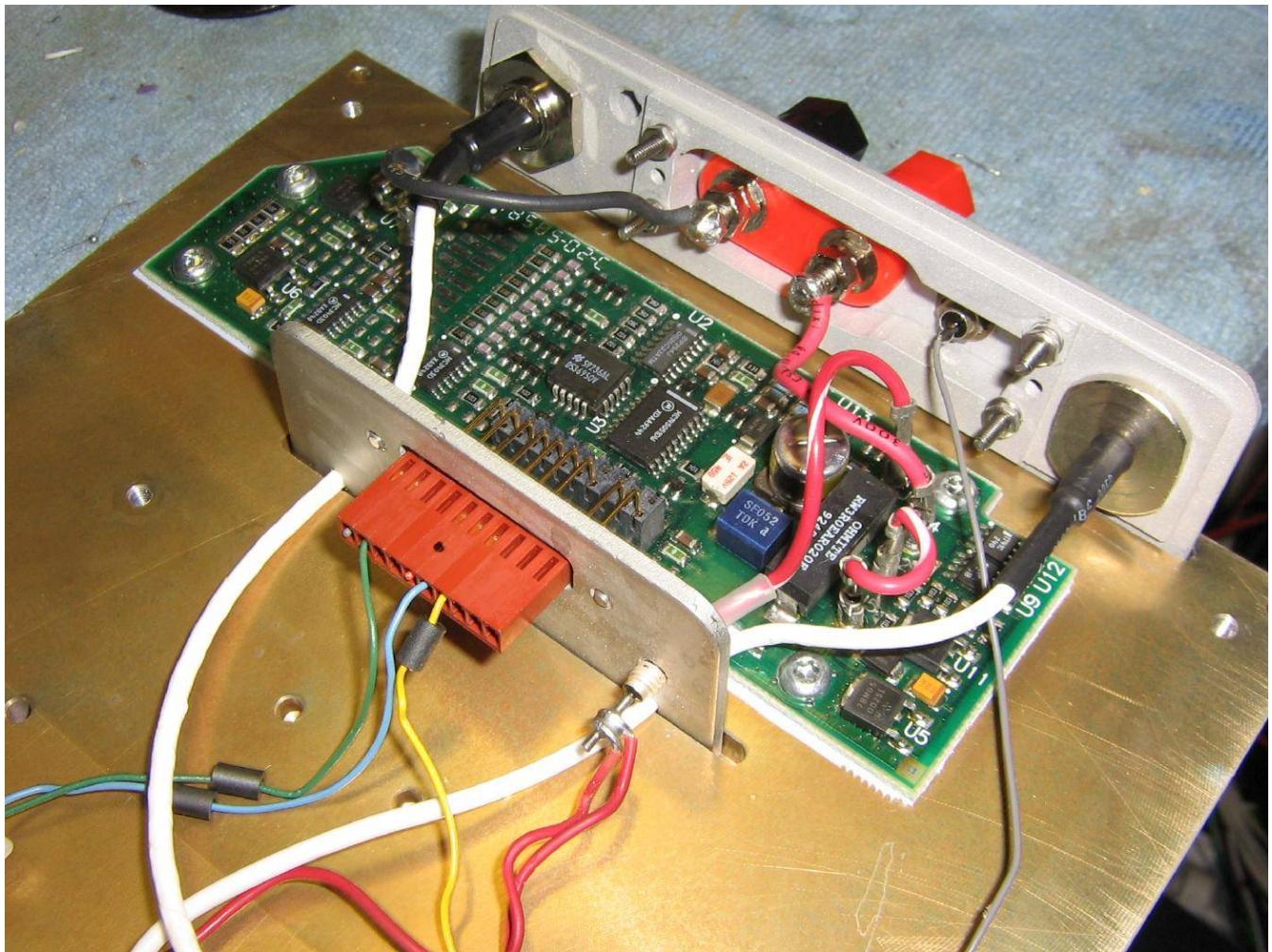


Constructing the new faceplate.

Panel-mount TNC connectors are used for the RF input and output.

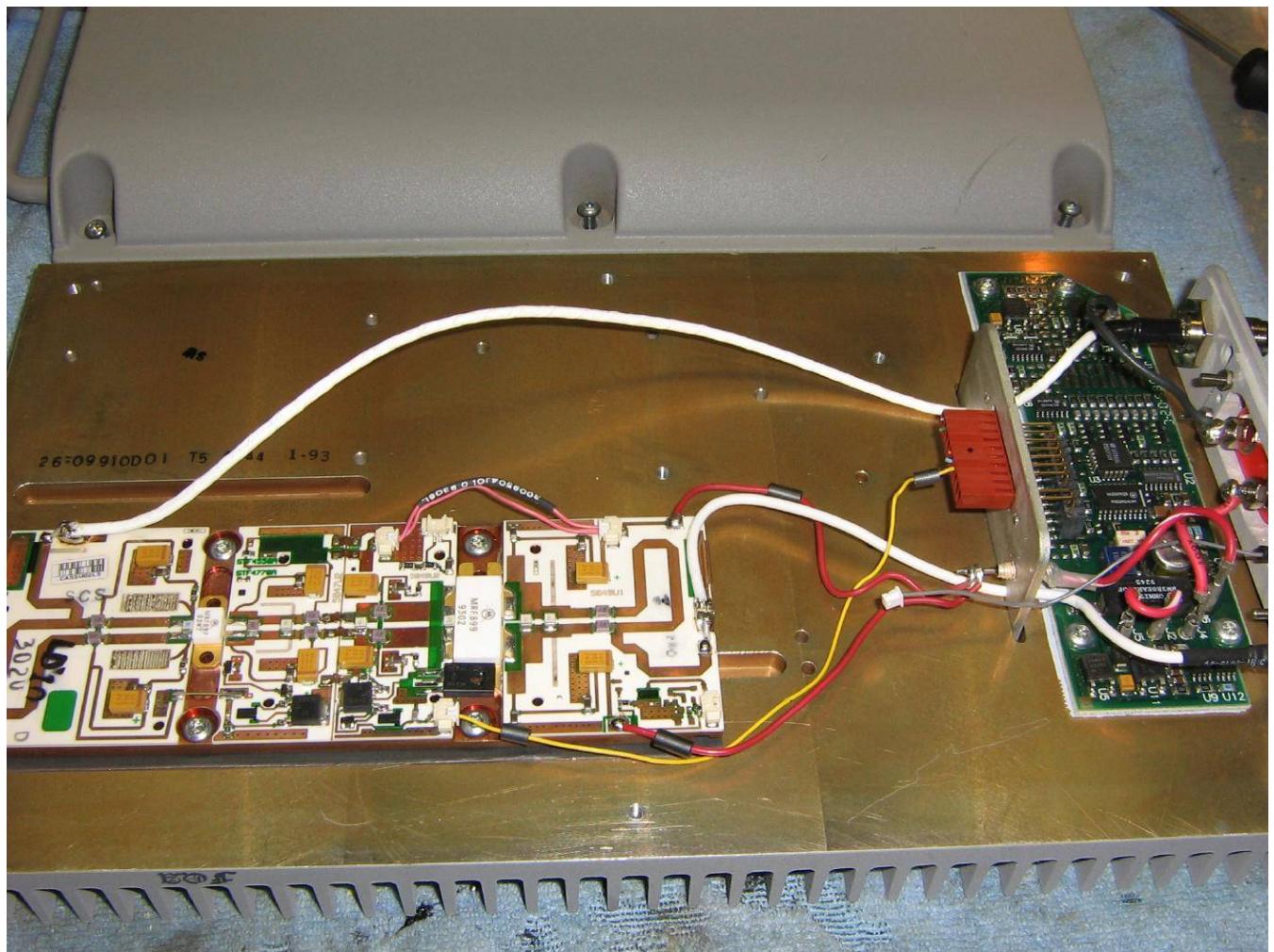
An optional 1,000 pF feed-thru capacitor is used for the "ground for transmit" line.

The banana jacks are for the +24 VDC power.



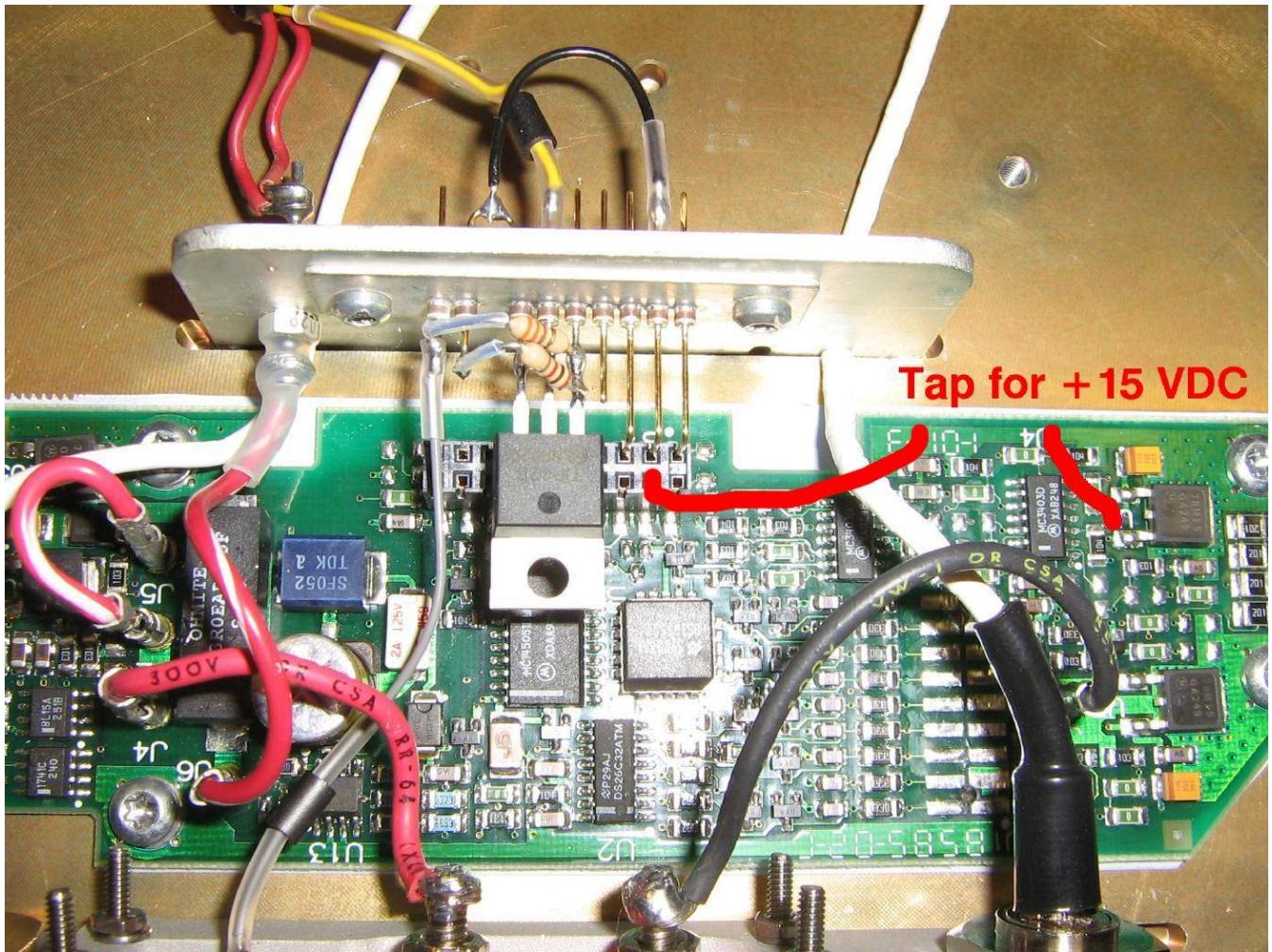
Installing the new faceplate connector.

The **RED** wire on the stock DC power control circuit board connects to the **RED** (positive) banana jack. The **BLACK** wire connects to the **BLACK** (negative) banana jack.



Overview of the completed Motorola STF2520A amplifier with the RF isolator and unnecessary wiring removed.

New pieces of 50 ohm Teflon coax were added for the RF input and output.

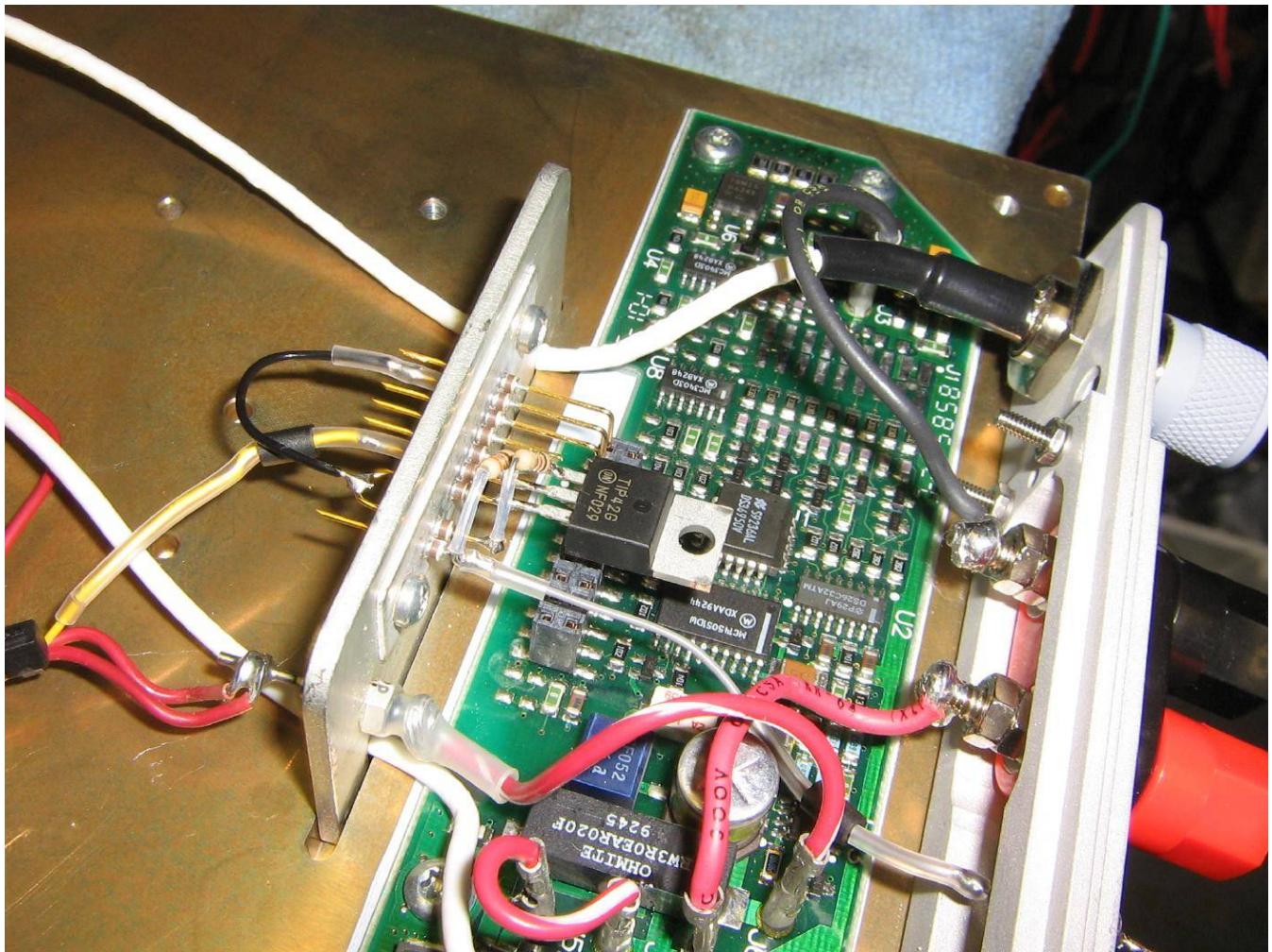


Optional bias control circuit.

Since those wires on the bulkhead connector are not required, I cut a few of the pins down and soldered the TIP42 transistor directly to them.

The other pins hold the biasing resistors and a tap for the required +15 VDC.

You can take the +15 VDC output directly from one of the 7815 voltage regulators (on the lower-right), or from the "second from the right" pin on the bulkhead.



Overview of the completed bias control circuit.

5 Watt RF Power Amplifier for 900 MHz

Overview

This is a project for a simple 5 watt, 900 MHz RF power amplifier which can be used stand-alone or as the driver stage for the Motorola STF2520A 150 watt amplifier project.

Construction of this amplifier will be very easy, as we'll be using the RF power amplifier module from an old Radio Shack CT-1050 800 MHz (analog) cellular phone. These old cellular phones, and other models using the same RF power amplifier module, show up from time-to-time at various ham radio swapfests. The Radio Shack CT-1050 is ideal for this project as they use a Hitachi PF0030 RF power module mounted on its own little heatsink.

The Hitachi PF0030 RF power module is designed for 824 – 849 MHz and has a maximum RF input of 20 mW (+13 dBm). It has over 30 dB of gain in that frequency range and the compression point is around 6 watts (+38 dBm) at +12 VDC. The PF0030 is non-linear biased, so it's only useful for constant envelope modulations – like FM, FSK, or CW. The PF0030's frequency range is fairly wideband, with its gain dropping off 10 dB at around 780 MHz on the low side and 915 MHz on the high side. There is over 3 dB of gain difference over the entire 902 – 928 MHz ham band, so keep this in mind. That isn't a big deal in most ham radio applications since the convenience and low cost of the Hitachi PF0030 RF power module makes up for any downfalls.

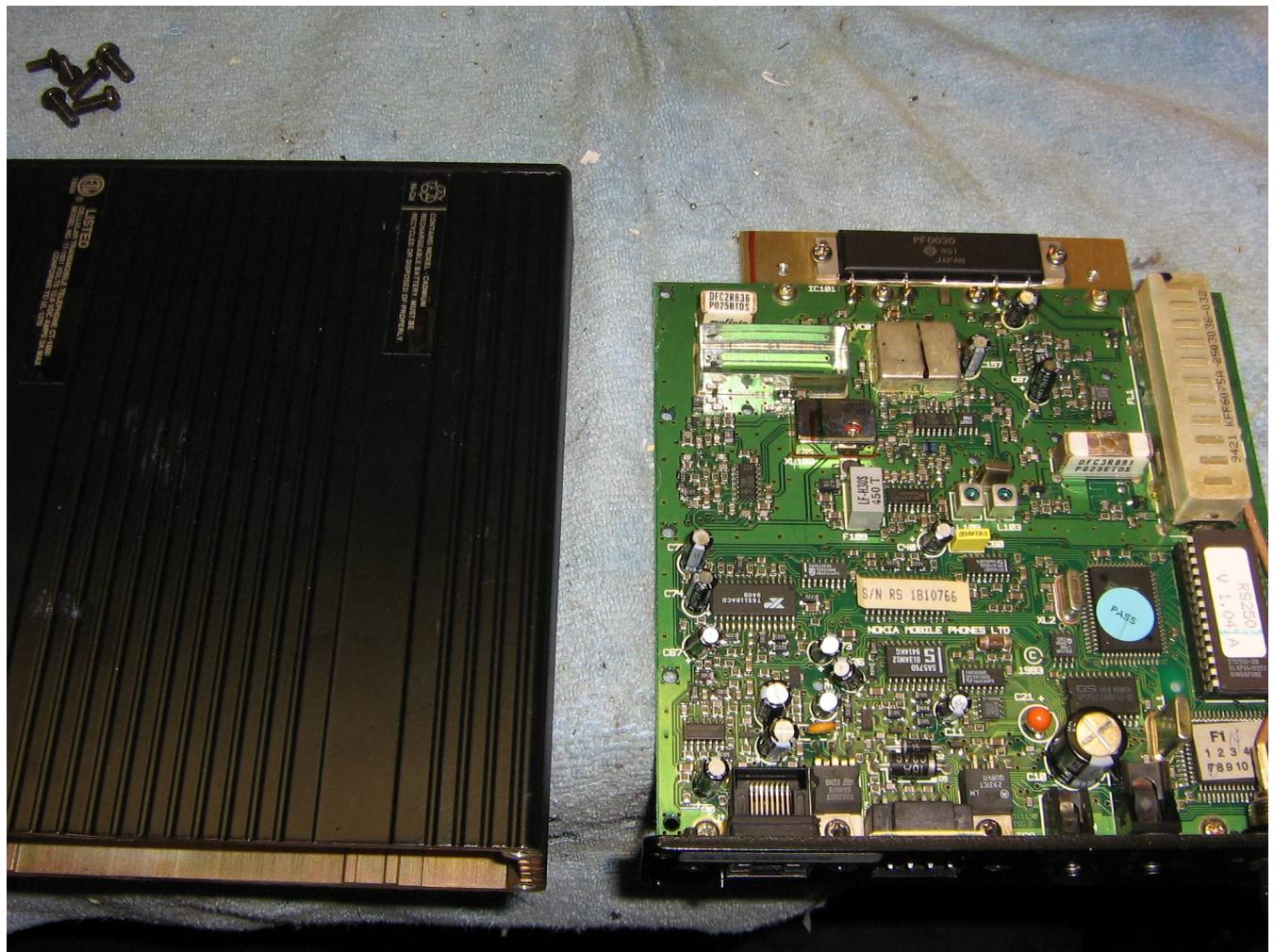
The Hitachi PF0030 RF power module itself is also fairly rugged. You can run them at +15 or +18 VDC and increase the RF input power for a little bit of extra gain. The PF0030 does get fairly hot, and this will require proper heatsinking. This is often overlooked when working with these RF power modules as the mounting flange is also the ground. Adding heatsink thermal compound to the flange often causes the RF power module to break into oscillation, in certain instances. The key to prevent oscillation is to have a common ground connection between the RF power module's flange and its RF input/output and DC power connections, and this can't be done with thermal compound under the flange. You'll then need to mount this first heatsink onto another one for additional heatsinking.

An optional transistor circuit will be added to this amplifier to toggle the RF power control voltage. This is useful for powering down the amplifier during a receive cycle. Since the current draw of the PF0030's control pin is minimal, we can just use a regular 2N3906.

Hitachi PF0030 Amplifier Specifications

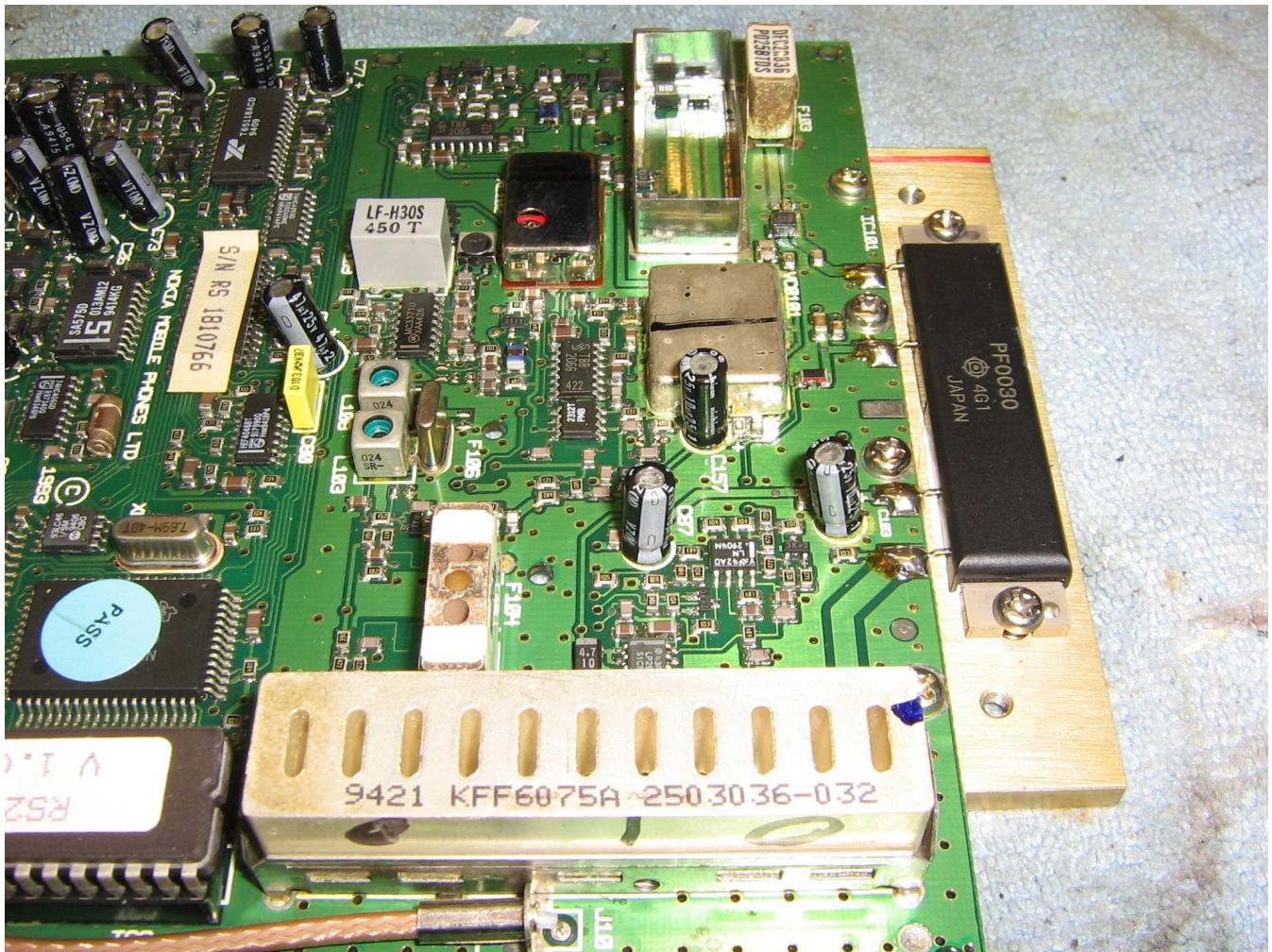
RF Frequency (MHz)	RF Input (dBm)	RF Output (dBm) (Watts)
830–850	-3	+38 (6.3)
780	-3	+28 (0.6)
880	-3	+36 (4.0)
902	-3	+33 (2.0)
915	-3	+28 (0.6)

Pictures & Construction Notes



Stock Radio Shack CT-1050 (Model No. 17-1021) analog cellular phone with its internal circuit board removed. This phone's FCC ID is: GML-C250

Note how the Hitachi PF0030 RF power module is mounted to its own little heatsink.

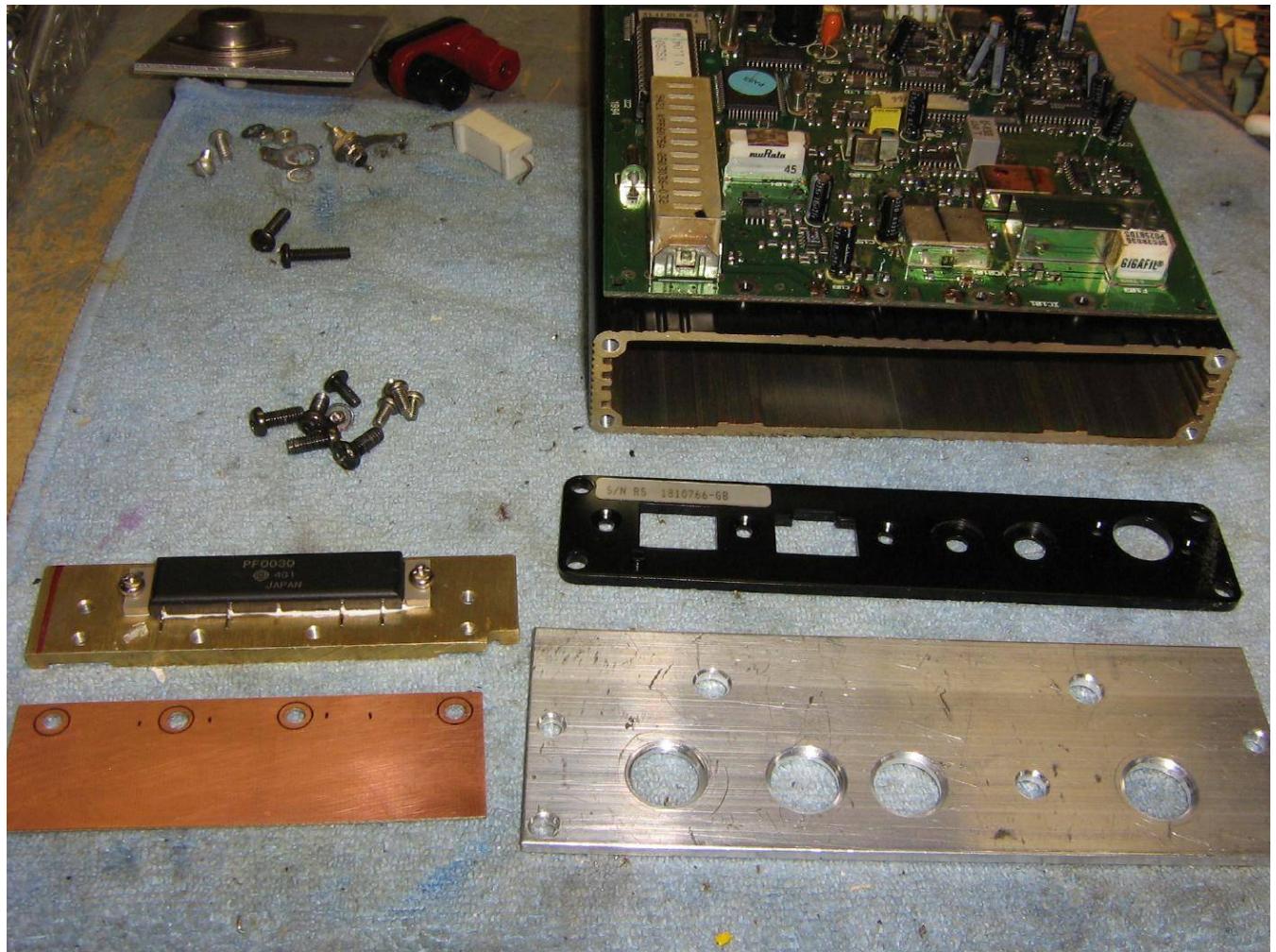


Alternate view of the Hitachi PF0030 RF power module and its heatsink.

We'll be making our own circuit board to connect up to the PF0030.

The PF0030 requires only five connections:

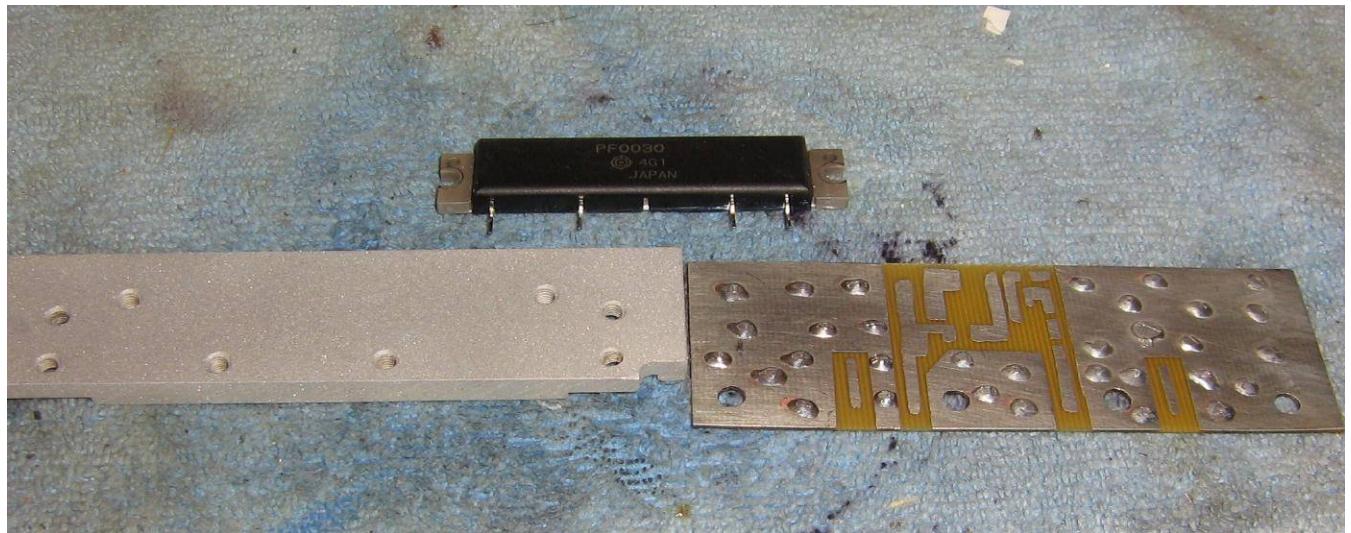
- RF input and RF output (50 ohm).
- +12 VDC at 3 amps Vcc power.
- RF power control voltage, which can be varied to control output RF power. We'll be using a fixed +5 VDC through a transistor control circuit.
- A common ground via the PF0030's flange.



Making a new faceplate for the front of the amplifier's case.

It's a piece of 2-inch wide aluminum stock with a few 1/2-inch diameter holes drilled in it for the TNC RF input/output connectors and DC power banana jacks.

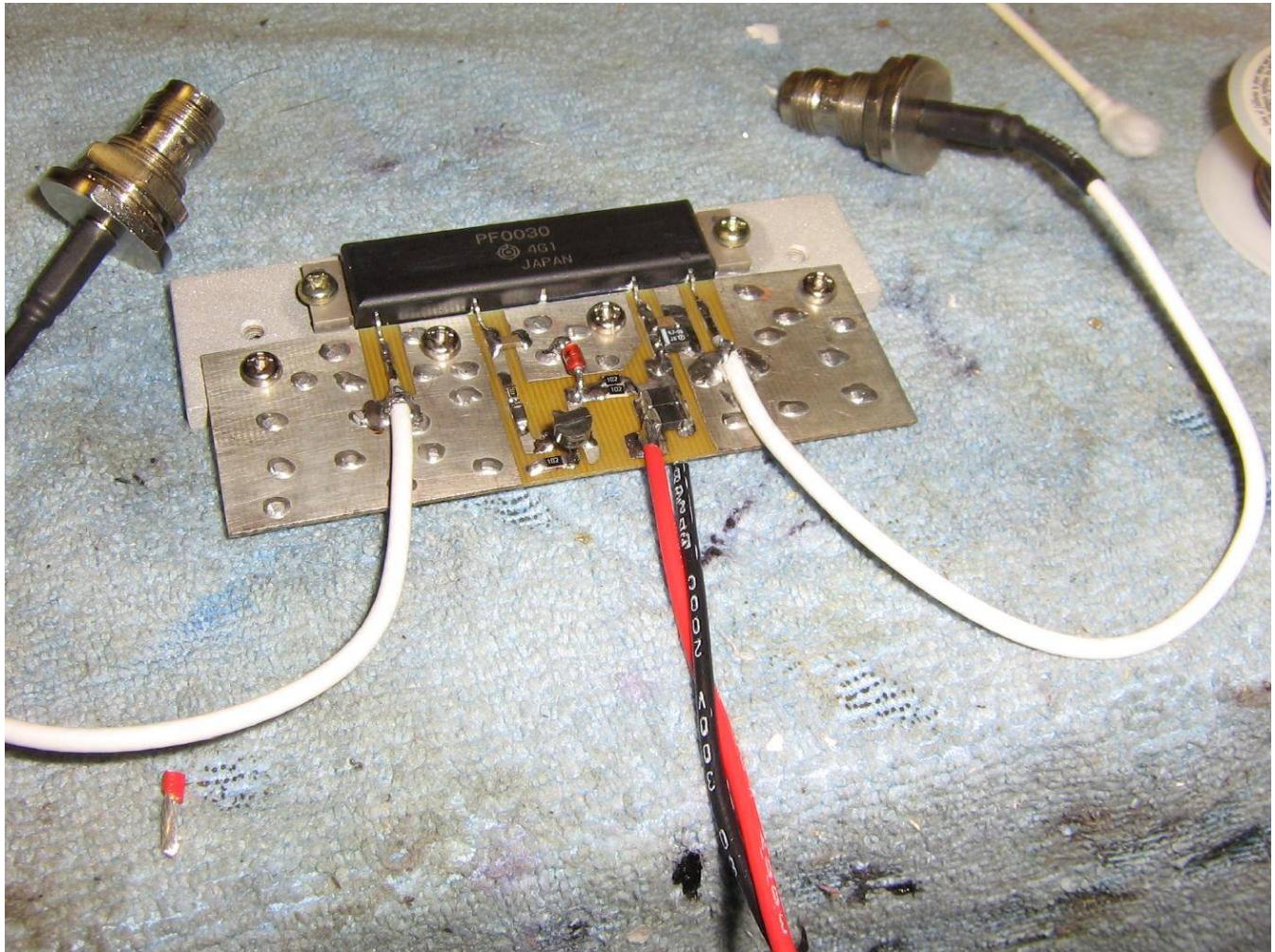
A new circuit board was also made for the PF0030 RF power module. This will hold the coaxial cable on the RF input/output, the power control transistor, and the voltage conditioning components.



Cleaning up the PF0030's heatsink and making the PC board.

I removed all the old thermal compound and sandblasted the heatsink to help clean it up a bit.

The PC board is double-sided and should have a large ground plane which is common to the heatsink.



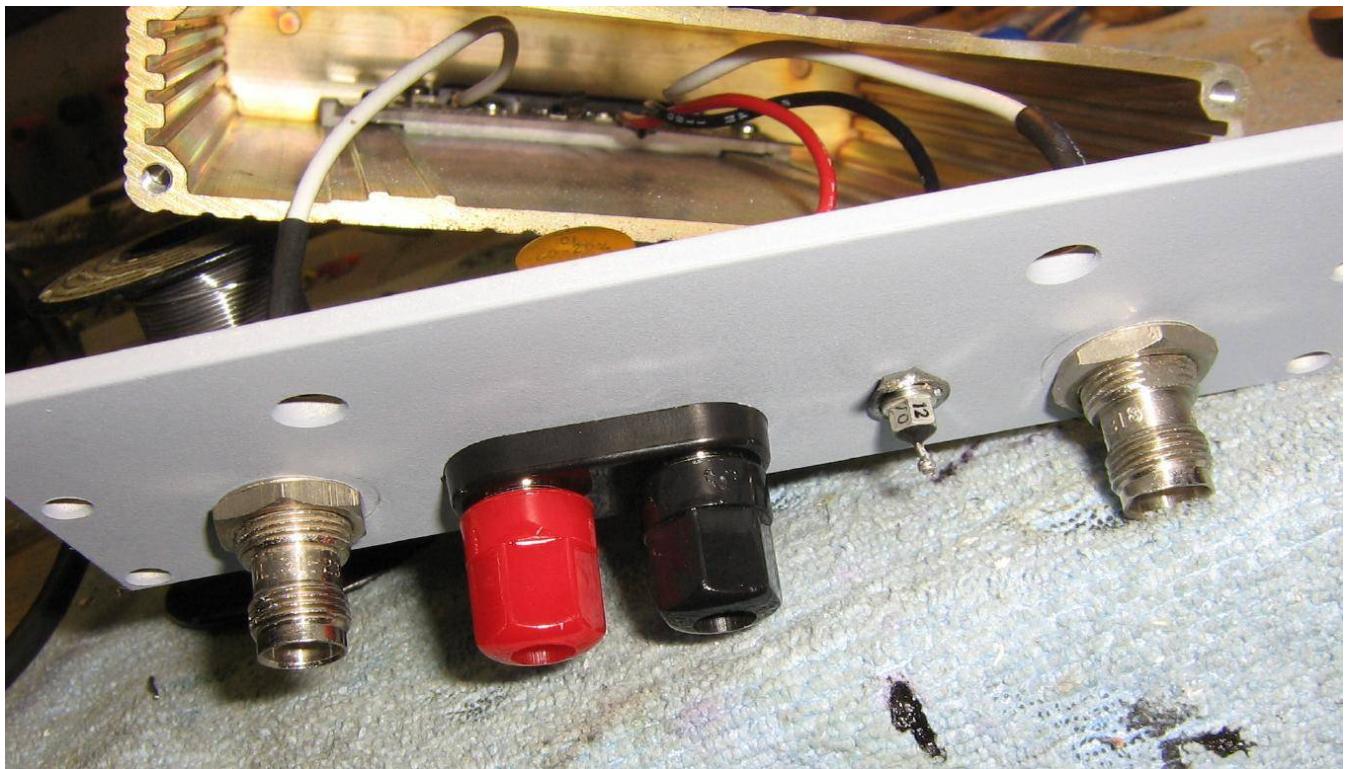
Completed Hitachi PF0030-based amplifier.

RF input is on the left, RF output is on the right via the TNC jacks.

There is *NO* heatsink thermal compound between the PF0030 and the aluminum mounting block. This keeps a strong common ground between the PF0030 and the circuit board holding the other components.

The +12 VDC for the Hitachi PF0030 is provided via the **RED** and **BLACK** wires which connect to the banana jacks on the amplifier's front panel.

Be sure not to over tighten the mounting screws for the PF0030 or the stress can crack the internal circuit board.



Amplifier internal view.

The PF0030 is mounted to the aluminum base *without* using any heatsink compound under its flange.

Then the aluminum base holding the PF0030 is mounted inside the case using a very thin amount of heatsink compound.



Finished 5 watt, 900 MHz amplifier.

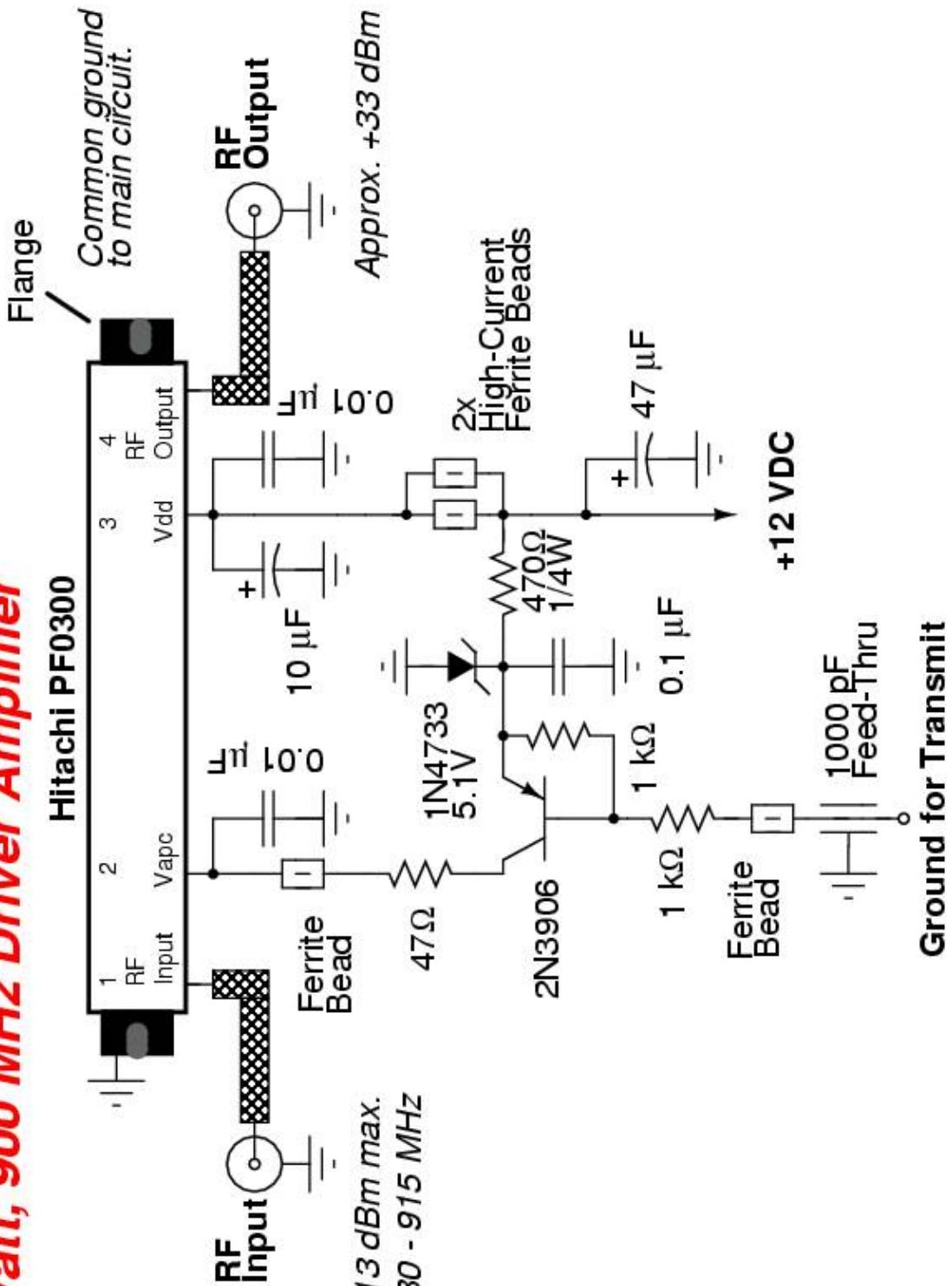
RF input of around 1 mW (0 dBm) is via the TNC connector on the left.

RF output of around 2 watts (+33 dBm) is via the TNC connector on the right.

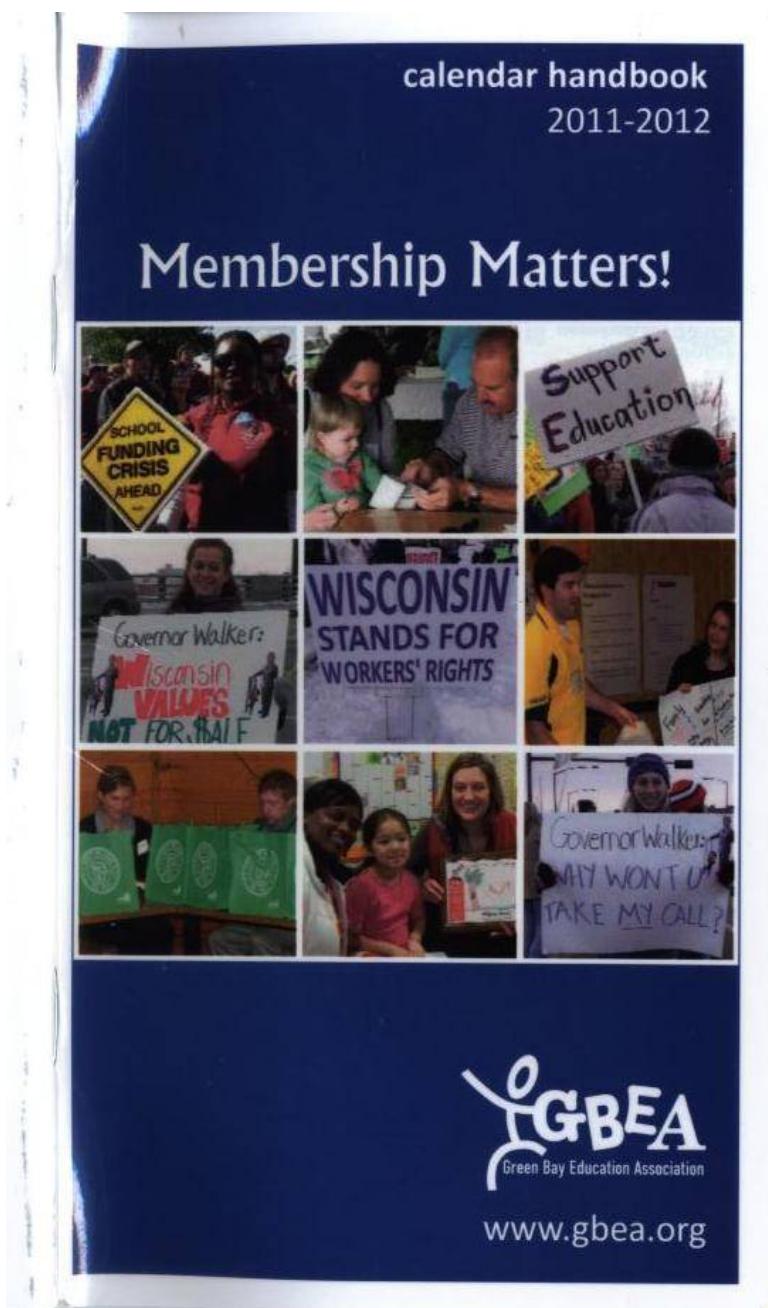
The banana jacks are for the +12 VDC power. **RED** is positive and **BLACK** is negative. Current draw is under 3 amps.

The optional 1,000 pF feed-thru capacitor is used for the "ground for transmit" line.

5 Watt, 900 MHz Driver Amplifier



Bonus



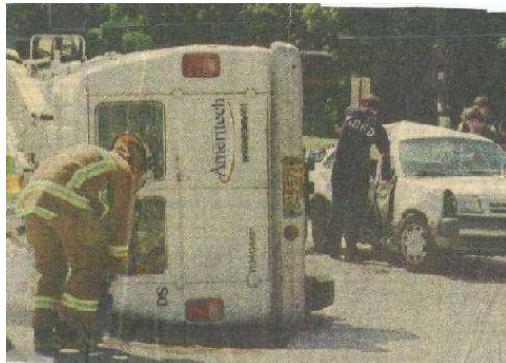
Since when is it up teachers to tell US who to vote for?

Contact the Green Bay Education Association's nigger president and let her know what you think:

Margaret "Toni" Lardinois
3000 Nooyer Ln.
Green Bay, WI 54311
(920) 866-9834

Be sure to ask why the Green Bay Public School District just wasted almost a million dollars installing over 500 video surveillance cameras in all the schools, then turned around and whined about "budget cuts."

End of Issue #89



Any Questions?

Editorial and Rants

If you live in Chicago, you better pray to God your house doesn't start on fire!

Fred Reed on Affirmative Action: "If you are good enough, you don't need it. If you need it, you aren't good enough."

City to Pay \$30 Million, Hire 111 Black Firefighters

August 17, 2011 – From: suntimes.com

by Fran Spielman

Chicago will hire 111 bypassed black firefighters by March 2012 and pay at least \$30 million in damages to some 6,000 others who will never get that chance, under a court order expected to be approved Wednesday by a federal judge.

Last year, the U.S. Supreme Court unanimously agreed that African-American candidates did not wait too long before filing a lawsuit that accused the city of discriminating against them for the way it handled a 1995 firefighter's entrance exam.

A federal appeals court affirmed that ruling in May and remanded the case back to the trial court to implement a hiring remedy the city had been stalling.

Now, both sides have agreed on that plan and how it should be implemented.

"We're extremely pleased that, after all these years, this long-running legal fight is coming to an end," said plaintiffs' attorney Matt Piers.

Noting that Chicago taxpayers are liable for an additional \$500,000 in back pay for every month the hiring is delayed, Piers said, "The attitude of the Emanuel administration has been to attempt to resolve this as quickly as possible."

The court order, to be presented to U.S. District Judge Joan Gotschall on Wednesday, calls for the city begin by sending postcards to all 6,000 black bypassed black candidates.

Those who indicate they are still interested in becoming Chicago firefighters will be entered into a "jobs lottery" to identify 750 candidates who will take a physical abilities test in October and undergo background checks, drug tests and medical exams.

From that group, the city will select 111 candidates who will enter the fire academy for training by the end of March 2012.

Would-be firefighters who have moved on to other careers or choose to bypass the jobs lottery for other reasons will receive cash awards of at least \$5,000 per person. Chicago taxpayers will also be on the hook for \$10 million to \$20 million in back pension contributions for those who get jobs. That means the total cost could approach \$50 million.

The Chicago Fire Department's age limit for new hires is 38, but that will not apply to the 111 black firefighters because the discrimination occurred before the cut-off was established.

"I don't think we'll have a problem coming up with 111 who still want the job and are fully qualified to have it," said Joshua Karsh, another attorney representing the plaintiffs.

"Some of these people are older than 38. But, better than half the department is older than 38."

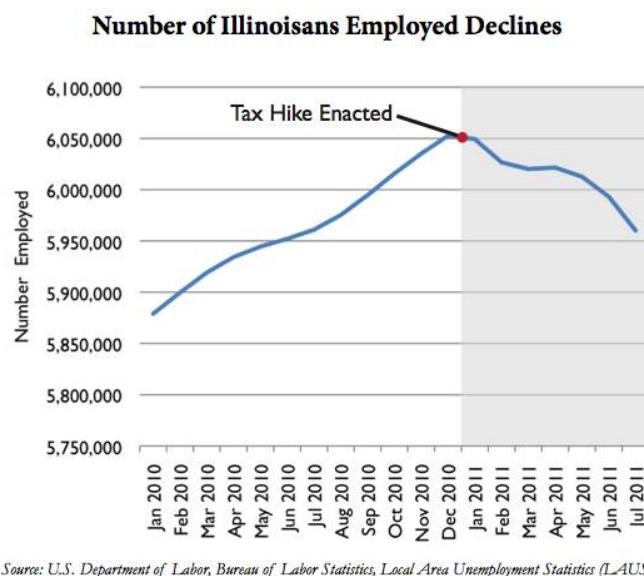
When results from the 1995 entrance exam were disappointing for minorities, the city established a cut-off score of 89 and hired randomly from the top 1,800 "well-qualified" candidates.

In 2005, a federal judge ruled that the city's decision had the effect of perpetuating the predominantly white status quo, since 78 percent of those "well-qualified" candidates were white.

Currently 19 percent of Chicago's 5,000 firefighters and paramedics are African-American. The force is 68 percent white and 11 percent Hispanic.

"By comparison to the Police Department, African-Americans are dramatically under-represented. There will [now] be 111 additional African-Americans. That's a very good thing," Karsh said.

He added, "This is the remedy for violating the law. Hopefully, this will deter the city from ever violating the law in this fashion again."



Finally! Obama is going to get more hard-working, high-IQ, educated Whites into government positions to put an end to all the bureaucracy!

Oh wait... Get ready for that kind of "diversity." Change!

Obama Creates Office of Diversity, Inclusion

August 24, 2011 – From: judicialwatch.org

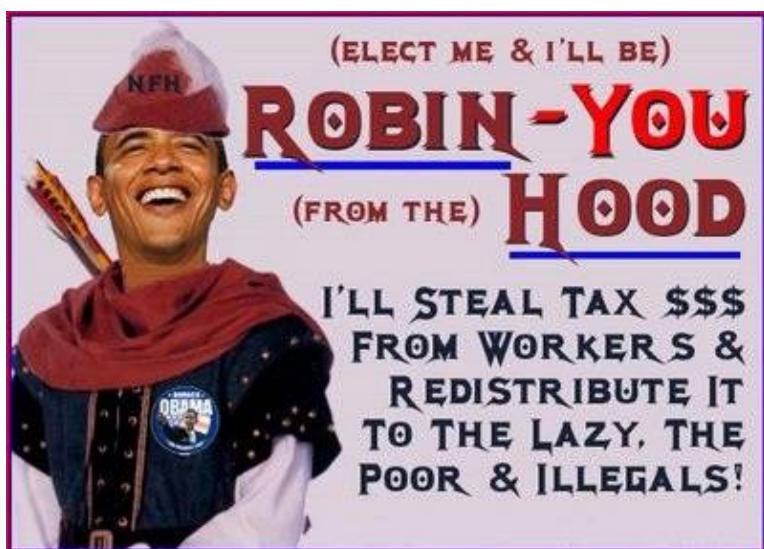
The economy remains in shambles yet President Obama keeps wasting taxpayer dollars expanding an already bloated U.S. government, this month launching a new office to help build a "diverse and inclusive workforce" at all federal agencies.

The new Office of Diversity and Inclusion will ensure that the entire U.S. government develops comprehensive strategies to drive and integrate diversity and inclusion practices. It will assist the different agencies in building a workforce that "respects individual and organizational cultures" by examining policy options, data trends and employee survey findings.

The goal is to eliminate demographic group imbalances in targeted occupations and improve workforce diversity. To attain this, special initiatives have been created targeting specific groups, including Hispanics, African Americans, American Indians, women and gays and lesbians. The idea is to create a workforce that truly reflects America's diversity, according to the Obama Administration.

In fact, the Obama executive order creating the new agency assures that it will promote the federal workplace as a model of equal opportunity, diversity and inclusion. It will also establish a coordinated government-wide initiative to promote the cause. The investment is worth it because a commitment to equal opportunity, diversity and inclusion is critical for the federal government as an employer, according to the commander-in-chief.

The president's new plan will force agencies to identify and remove barriers to equal employment opportunities that may exist in the federal government's recruitment, hiring, promotion, retention, professional development and training policies and practices.



And it continues... Non-White students too stupid to pass a simple test? Just have Obama issue the school a waiver!

Kinda makes you wonder how we put a fucking man on the moon... Oh yeah, that's right... No niggers!

Obama Administration Exempting Schools From Federal Law's Testing Mandate

August 8, 2011 – *From: cnsnews.com*

By Donna Gordon Blankinship

(AP) – State and local education officials have been begging the federal government for relief from student testing mandates in the federal No Child Left Behind law, but school starts soon and Congress still hasn't answered the call.

Education Secretary Arne Duncan says he will announce a new waiver system Monday to give schools a break.

The plan to offer waivers to all 50 states, as long as they meet other school reform requirements, comes at the request of President Barack Obama, Duncan said. More details on the waivers will come in September, he said.

The goal of the No Child Left Behind law is to have every student proficient in math and reading by 2014. States have been required to bring more students up to the math and reading standards each year, based on tests that usually take place each spring. The step-by-step ramping up of the 9-year-old law has caused heartburn in states and most school districts, because more and more schools are labeled as failures as too few of their students meet testing goals.

Critics say the benchmarks are unrealistic and brands schools as failures even if they make progress. Schools and districts where too few kids pass the tests for several years are subject to sanctions that can include firing teachers or closing the school entirely.

Through the waivers, schools will get some relief from looming deadlines to meet testing goals as long as they agree to embrace other kinds of education reforms such as raising standards, helping teachers and principals improve, and focusing on fixing the lowest performing schools.

Duncan and Melody Barnes, director of the Domestic Policy Council at the White House, said the administration will encourage every state to apply and will work with them to meet the requirements.

Nothing in this plan for temporary relief from some aspects of the federal law will undermine what Congress is still discussing in terms of revising federal education laws, Duncan said. The long-awaited overhaul of the law began earlier this year in the U.S. House, but a comprehensive reform appears far from the finish line.

"What we do in terms of flexibility can be a bridge or transition," he said. "We all want to fix the law. This might help us get closer to that."

The chairman of the House Committee on Education and the Workforce, however, says he is worried about Duncan's waiver plan.

"I remain concerned that temporary measures instituted by the department, such as conditional waivers, could undermine the committee's efforts to reauthorize the Elementary and Secondary Education Act," said Rep. John Kline, R-Minn., in a statement, referring to the formal name of the No Child Left Behind law.

The Obama administration requested a revision more than a year ago. Duncan said another school year is about to start and state education officials have told him they can't keep waiting for relief from the mandates.

"I can't overemphasize how loudly the outcry is to do something now," Duncan said.

Duncan has warned that 82 percent of U.S. schools could be labeled failures next year if No Child Left Behind is not changed. Education experts have questioned that estimate, but state officials report a growing number of schools facing sanctions under the law.

Montana Schools Superintendent Denise Juneau said she welcomed the waiver proposal, as long as it offers relief from the 2014 deadline. She said her state isn't afraid of high standards and education reform but needs enough time to reach those standards and freedom to institute change in a way that works for Montana.

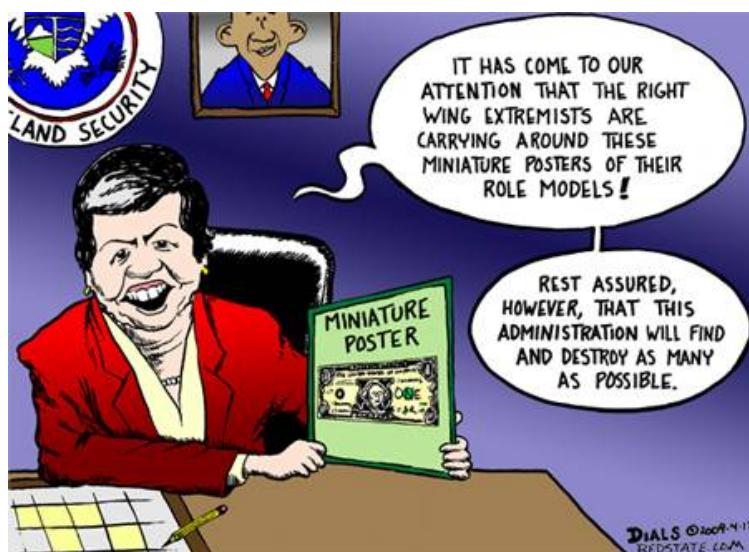
Montana decided to skip a planned increase in its testing goals this past school year.

"I don't mind the goals and we're certainly not afraid of accountability. They can set the bar wherever they want. They just have to let us have the flexibility to get there," Juneau said. "We can definitely meet any bar they throw at us."

The chairman of the Senate Health, Education, Labor and Pensions Committee said he understands why it was time for the administration to take action.

"This Congress faces real challenges reaching bipartisan, bicameral agreement on anything," said Sen. Tom Harkin, D-Iowa, in a written statement. "Given the ill-advised and partisan bills that the House majority has chosen to move, I understand Secretary Duncan's decision to proceed with a waiver package to provide some interim relief while Congress finishes its work."

Harkin said he remains committed to keep working toward a bipartisan solution to reform the federal education law.



Here's how the Jew media has been portraying the recent spat of nigger-on-human "flash mob" violence. Note how their story includes pictures of White kids just having a good time...

For flash mobsters, crowd size a tempting cover

[Email this Story](#)

Aug 9, 8:01 AM (ET)

By ERIC TUCKER and THOMAS WATKINS

The July 4 fireworks display in the Cleveland suburb of Shaker Heights was anything but a family affair.

As many as 1,000 teenagers, mobilized through social networking sites, turned out and soon started fighting and disrupting the event.

Thanks to social networks like Twitter and Facebook, more and more so-called flash mobs are materializing across the globe, leaving police scrambling to keep tabs on the spontaneous assemblies.

"They're gathering with an intent behind it - not just to enjoy the event," Shaker Heights Police Chief D. Scott Lee said. "All too often, some of the intent is malicious."



(AP) In this photo taken July 14, 2011, actors dressed in beach attire participate in a flash mob as...

[Full Image](#)



(AP) In this photo taken July 14, 2011 actors dressed in beach attire participate in a flash mob as part...

[Full Image](#)

Flash mobs started off in 2003 as peaceful and often humorous acts of public performance, such as mass dance routines or street pillow fights. But in recent years, the term has taken a darker twist as criminals exploit the anonymity of crowds, using social networking to coordinate everything from robberies to fights to general chaos.

In London, recent rioting and looting has been blamed in part on groups of youths using Twitter, mobile phone text messages and

From: apnews.myway.com/article/20110809/D9P0I3AG0.html

Now, here's a 911 call excerpt and timeline from the recent nigger "flash mobs" which struck the Wisconsin State Fair:

"I mean this is what I gotta go through, I pay taxes and I'm walking down the fucking street -- really? -- and this is what the fuck happens, some stupid fucking black motherfuckers, they think they can just punch people, really?"

--- Excerpt from one of the 911 calls during the Wisconsin State Fair nigger riots. LOL!

Wisconsin State Fair Calls for Support Timeline

22:48 ~ State Fair P.D. advised us that they shut the park down early because of a large amount of fights. They report large groups of people leaving the grounds.
22:49 ~ Walgreens reports lots of people in the area.
22:59 ~ 9-1-1 call received in regards to group of 25 black youths assaulting State Fair worker around 81/Greenfield.
23:00 ~ 9-1-1 call received in regards to fight at front entrance of State Fair.
People are everywhere. Groups of people chasing white people.
23:01 ~ Call received indicating people are leaving State Fair and heading to 84/Greenfield.
23:08 ~ State Fair P.D. reports that people are walking on cars near 84/Schlinder.
23:10 ~ Groups jumping on cars at 84/Schlinder.
23:11 ~ Angry mob, fights, wrong way drivers, people running in traffic, at 84/Schlinder.
23:12 ~ Fight at 1000 S. 84 St.
23:14 ~ Kids obstructing traffic and hitting cars.
23:15 ~ Person assaulted and has a knot on the head at 84/Schlinder.
Party going to hospital on own.
23:16 ~ Victim punched in face at 84/Walker by group. Medical denied.
23:17 ~ State Fair P.D. reports fights and people jumping on cars at 84/Greenfield.
23:18 ~ Mob pulled male and female from motorcycle at 84/Adler.
Female was dragged and has fat lip.
23:18 ~ Mobs hitting cars at 84/Schlinder.
23:21 ~ Victim jumped and almost robbed at 87/McMyron.
23:24 ~ Group of guys have a gun in a car near 85/Walker.
23:25 ~ Group of guys jumping people near 85/Walker. One had a gun.
23:26 ~ People running through yards. One bike stolen.
23:30 ~ Kids hitting cars at 84/Walker.
23:30 ~ Police report large fight at 84/Greenfield.
23:30 ~ Group attack male at 88/Greenfield.
23:33 ~ Kid getting pummeled by a group at 84/Schlinder.
23:34 ~ Kids jump guy at 76/Washington.
23:34 ~ State Fair P.D. report fight at 84/Greenfield.
23:35 ~ Fight reported at 85/Greenfield.
23:37 ~ Riot at 84/Greenfield. Wife has black eye and bloody lip. Refuse to report incident.
23:37 ~ Possible beating and man with gun at 76/Walker.
23:38 ~ Fight and theft at 87/McMyron.
23:39 ~ Police requesting help at McDonald's. Under control at 2340.
23:39 ~ Victim got hit by group of kids at 76/Walker.
23:40 ~ Teenagers assaulted male at 76/Walker.
23:43 ~ Fight at 76/Walker.
23:44 ~ Male assaulted by group. Bleeding, but medical refused.
23:51 ~ Homeless person beat up at 76/Greenfield.
23:51 ~ Caller got hit in face by group.
23:51 ~ Fight at 86/Greenfield.
23:51 ~ Fight at 76/Washington.
23:53 ~ 20-25 people ran in and out of gas station at 76/Greenfield at stole stuff.
23:55 ~ Mutual aid requested - MCSO. MCSO is responding.
23:57 ~ Male assaulted by group at 86/Greenfield.
23:57 ~ Caller was almost robbed by group at 87/McMyron.

"The incidents Thursday night come as the State Fair board over the last decade has worked to increase diversity at the annual fair, expanding its entertainment lineup and marketing to appeal to a younger, more multicultural audience. Diversity was a priority for State Fair Park Chairman Martin Greenberg, who spoke often of making it 'truly the people's park' – a 'place of inclusion, not exclusion.'"

Ever wonder just whose idea is was to allow niggers into the Wisconsin State Fair in the first place? (www.jsonline.com/news/milwaukee/126828998.html)

See the Jew...



London, 1960



London, 2011



Obongo's Magical Misery Tour Bus



Sarah Palin's Tour Bus