GBPPR 'Zine

Issue #32 / The Monthly Journal of the American Hacker / November 2006

"The men said that their actions were inspired by an urge to avenge the suffering of Muslims in Bosnia and Chechnya."

––– Excerpt from *Al–Qaeda Video Takes Credit for 9/11* at:
http://www.sweetness–light.com/archive/911–hijackers–wanted–to–avenge–bosnia

Yes, that is right. The ragheads are pissed–off because those fucking *Eurosavages* can't go 10 years without killing each other.

Special "Kill All Europeans" Issue

Table of Contents

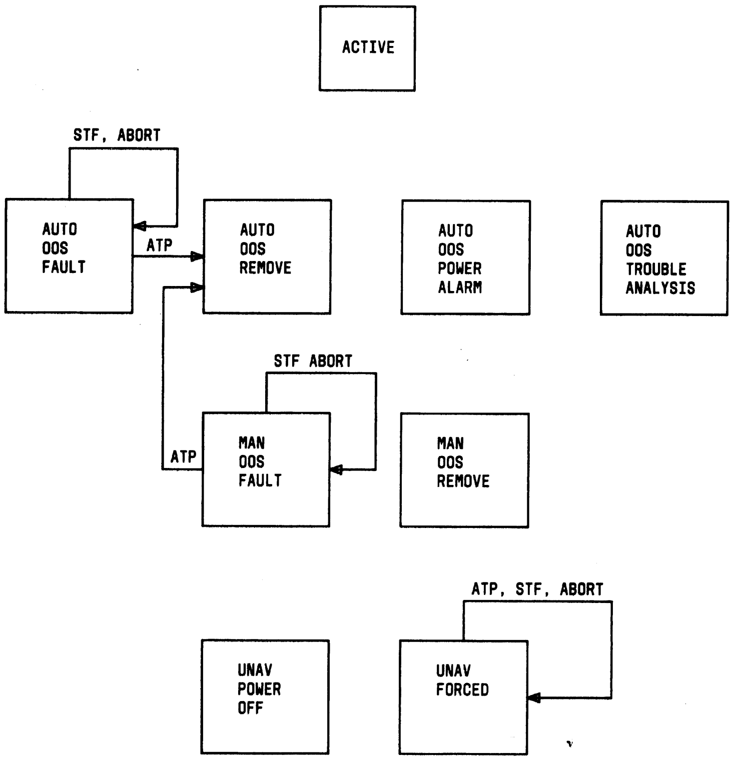


Fig. 23—➧Manually Requested DTRM Diagnostics➧

- Disposition of maintenance procedure(ie, pass, fail, in-progress, completed, etc)
- Sequence number of message
- DTRM/MODEM maintenance state
- Last processor notification processed
- VFL maintenance state
- VFL to DTRM connection indicator
- VFL transmission test status
- Whether or not VFL is in synchronization
- Whether or not VFL test relay is operated.

10.04 Using the information provided by the LS01 printout, it is possible to identify the data link in trouble. All data links should be placed in the ACTIVE state as soon as possible. Any data links out of service should be repaired and rediagnosed.

LS02 OUTPUT MESSAGE

10.05 The LS02 output message is printed each quarter hour when data link errors exceed a predetermined warning level, but are not high

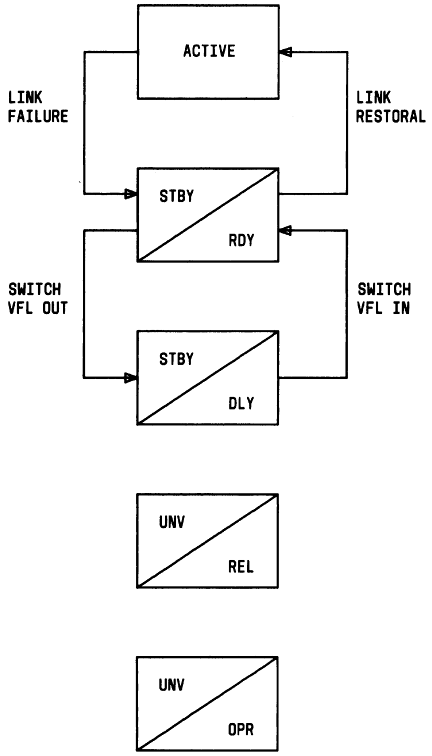


Fig. 24—▶Automatic VFL State Transitions◀

enough to cause automatic removal of the link from service.

10.06 The following information is provided in the LS02 printout.

- Terminal pair to which the DTRM is assigned
- Member of terminal pair to which the DTRM is assigned
- DTRM type indication
- Member number of DTRM
- Which VFL (a or b) is connected through to the DTRM
- Number of SUs received in error
- Number of received repeated acknowledgment control units
- Number of received skipped acknowledgment control units.

10.07 Based on the information provided by the LS02 printout, appropriate action may be taken. High error rates may indicate impending data link failure. High counts of SUs received in error and/or retransmission requests received indicate transmission problems. High counts of received repeated acknowledgment control units and/or received skipped acknowledgment control units indicate near-end and far-end modem clocks are not synchronized.

LS03 OUTPUT MESSAGE

10.08 The LS03 output message is printed in response to the DTRM-REQ-AUD input message. The printout shows those DTRM, VFL, and band status indicators that are currently being used to perform the CCIS data link I/O function in addition to data link maintenance control.

10.09 The data contained in the LS03 printout may be used to provide additional status information if the LS01 printout is not sufficient.

LS04 OUTPUT MESSAGE

10.10 The LS04 output message is printed whenever the CCIS link security bootstrap routine is entered. This can occur via an internal program request or manual request using the DTRM-REQ-FRC input message. The printout shows all the status information and current input data for the DTRM being bootstrapped before all software and hardware for that DTRM is reinitialized.◀

11. DTRM STATE CONTROL

11.01 ▶Control of the DTRM maintenance states is accomplished automatically or manually. Automatic state control is initiated entirely by the system, without human intervention, based on the results of automatic transmission tests and status

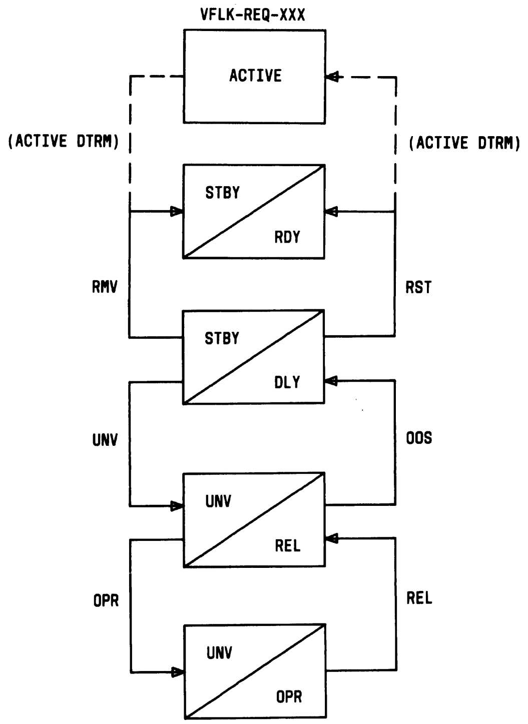


Fig. 25—♦Manual VFL State Transitions♦

♦TABLE H♦

VOICE FREQUENCY LINK (VFL) STATES

STATE	VFL FUNCTION
ACTIVE	Carrying call traffic
STBY/RDY	Standby: ***Not*** carrying call traffic Ready: Connected to DTRM
STBY/DLY	Standby: ***Not*** carrying call traffic Delay: ***Not*** connected to DTRM
UNV/REL	Unavailable: ***Not*** available for service Released: VFL access circuit ***released***
UNV/OPR	Unavailable: Not available for service Operated: VFL access circuit ***operated***

checks. Manual state control is initiated via teletypewriter input messages, frame controls, or maintenance data link messages, when configurations must be established for maintenance purposes. Table I shows the DTRM state transitions that are allowed (from one state to another).

AUTOMATIC DTRM STATE TRANSITIONS

A. Normal Link Recovery

Note: Refer to the state diagram in Fig. 20.

11.02 The normal link recovery procedure is initiated when a single link failure occurs or when a link is released from an unavailable condition and the mate link is currently active. The DTRM must always enter the AUTO OOS REMOVE state before being restored to active service. This allows the recovering link to be monitored for 18 seconds to insure acceptable transmission quality and allows a CCIS signaling network status update to be completed.

11.03 If transmission quality is found to be unacceptable for 3 minutes, the DTRM is automatically placed in the AUTO OOS TROUBLE ANALYSIS state and a diagnostic is initiated. If an all-test-pass occurs, the DTRM is returned to the AUTO OOS REMOVE state, from which the normal link recovery routine will attempt to restore it to the ACTIVE state.

11.04 If the automatically initiated diagnostic has some-tests-failing or aborts, the DTRM is placed in the AUTO OOS FAULT state. In this state, the DTRM is marked unavailable for service and manual troubleshooting procedures should be initiated as soon as possible. Manually initiated diagnostics can be run from this state. (See paragraph 11.16.)

11.05 Any automatically initiated link recovery procedures are reported on the maintenance teletypewriter via the LS01 output message.

B. Emergency Link Recovery

Note: Refer to the state diagram in Fig. 21.

11.06 The emergency link recovery procedure is automatically initiated when a double link failure occurs or when a link is released from an unavailable condition and the mate link is not currently active. The DTRM enters the AUTO OOS REMOVE state and, before being restored to ACTIVE service, the recovering link is monitored for only 3 seconds and an abbreviated restoral sequence is followed.

11.07 As for normal link recovery, emergency link recovery procedures are reported via the LS01 output message.

MANUAL DTRM STATE TRANSITIONS

Note: Refer to the state diagram in Fig. 22.

11.08 Manual control of the DTRM maintenance states is accomplished via the maintenance teletypewriter using the DTRM-REQ-XXXX input message. These messages allow maintenance personnel to establish various maintenance states or request some action to be taken on the DTRMs. The use of this message is described in the following paragraphs.

A. Removing a DTRM from Service

11.09 To manually remove a DTRM from ACTIVE service, type in:

DTRM-REQ-RMV bbbb.

bbbb = Decimal number between 0 and 1023 identifying the DTRM.

System responds with PF followed by an LS01 output message indicating the request has been implemented. The DTRM is now in the MAN OOS REMOVE state (T/M state 38) and operating for maintenance-only but is available if the mate DTRM fails.

11.10 If the problem is solved, the DTRM may be restored to ACTIVE service, using the DTRM-REQ-RST input message. (See paragraph 11.11.) If the problem is of such a nature that manually requested diagnostics are required to obtain further information, the DTRM must first be placed in the MAN OOS FAULT state using the DTRM-REQ-OOS message. (See paragraph 11.12.)

B. Restoring a DTRM to Service

11.11 To manually restore a DTRM to service, type in:

DTRM-REQ-RST bbbb.

bbbb = Decimal number between 0 and 1023 identifying the DTRM to be restored to service.

▶TABLE I◀

DTRM STATE TRANSITIONS ALLOWABLE OR NOT ALLOWED

FROM T/M STATE NO.	TO T/M STATE NO.	ACTIONS OR EVENTS CAUSING STATE CHANGE
32	32 33 34 35 36 37 38	Don't Care Not allowed Automatically initiated if single link failure or if DTRM inaccessible Blown fuse Automatically initiated if single link failure Not allowed Initiated by ***DTRM-REQ-RMV*** input message
	39	DTRM should be in one of OOS states before power removed
	40	Initiated by ***DTRM-REQ-UNV*** input message
33	32 33	Not allowed Don't care
	34	Automatic if diagnostic is ATP or initiated by ***DTRM-REQ-RST*** input message
	35 36 37 38 39 40	Blown fuse Not allowed Initiated by ***DTRM-REQ-OOS*** input message Initiated by ***DTRM-REQ-RMV*** input message Power manually removed Initiated by ***DTRM-REQ-UNV*** input message
34	32 33 34 35	Automatically initiated by link recovery routine Not allowed Don't care Blown fuse
	36	Automatically initiated by link recovery routine
	37 38 39 40	Initiated by ***DTRM-REQ-OOS*** input message Not allowed Power manually removed Initiated by ***DTRM-REQ-UNV*** input message
35	32 33	Not allowed Not allowed
	34	Automatically initiated if single link failure or if DTRM inaccessible
	35 36 37 38 39 40	Don't care Not allowed Initiated by ***DTRM-REQ-OOS*** input message Initiated by ***DTRM-REQ-RMV*** input message Power manually removed Initiated by ***DTRM-REQ-UNV*** input message

▶TABLE I◀ (Contd)

DTRM STATE TRANSITIONS ALLOWABLE OR NOT ALLOWED

FROM T/M STATE NO.	TO T/M STATE NO.	ACTIONS OR EVENTS CAUSING STATE CHANGE
36	32	Not allowed
	33	Initiated automatically if diagnostics aborts or results in STF
	34	Automatic if diagnostics is ATP or initiated by ***DTRM-REQ-RST*** input message
	35 36 37 38 39 40	Blown fuse Don't care Initiated by ***DTRM-REQ-OOS*** input message Initiated by ***DTRM-REQ-RMV*** input message Power manually removed Initiated by ***DTRM-REQ-UNV*** input message
37	32 33	Not allowed Not allowed
	34	Automatic if diagnostics is ATP or initiated by ***DTRM-REQ-RST*** input message
	35 36 37 38 39 40	Not allowed Not allowed Don't care Initiated by ***DTRM-REQ-RMV*** input message Power manually removed Initiated by ***DTRM-REQ-UNV*** input message
38	32 33 34 35 36 37 38 39 40	Not allowed Not allowed Automatic if diagnostics is ATP Not allowed Not allowed Initiated by ***DTRM-REQ-OOS*** input message Don't care Power manually removed Initiated by ***DTRM-REQ-UNV*** input message
39	32 33	Not allowed Not allowed
	34	Automatic if diagnostics is ATP or initiated by ***DTRM-REQ-RST*** input message
	35	Not allowed
	36	Power manually restored; diagnostics automatically initiated
	37 38 39 40	Initiated by ***DTRM-REQ-OOS*** input message Initiated by ***DTRM-REQ-RMV*** input message Don't care Initiated by ***DTRM-REQ-UNV*** input message

TABLE I (Contd)

DTRM STATE TRANSITIONS ALLOWABLE OR NOT ALLOWED

FROM T/M STATE NO.	TO T/M STATE NO.	ACTIONS OR EVENTS CAUSING STATE CHANGE
40	32	Not allowed
	33	Not allowed
	34	Initiated by ***DTRM-REQ-RST*** input message
	35	Not allowed
	36	Not allowed
	37	Initiated by ***DTRM-REQ-OOS*** input message
	38	Initiated by ***DTRM-REQ-RMV*** input message
	39	Not allowed
	40	Don't care

System responds with PF followed by an LS01 output message indicating the request has been implemented. The DTRM is placed in the AUTO OOS REMOVE (T/M state 34) from which the automatic link recovery routine will attempt to restore the unit to the ACTIVE state.

C. Taking a DTRM Out of Service

11.12 To take a unit out of service, type in:

DTRM-REQ-OOS bbbb.

bbbb = Decimal number from 0 through 1023 identifying the DTRM to be taken out of service.

This request is not honored on an active terminal. The system responds with PF followed by an LS01 output message indicating the request has been implemented. The DTRM is now in the MAN OOS FAULT state (T/M state 37). In this state, the DTRM is not operating but is available if the mate DTRM fails. Diagnostics may be run using the DTRM-REQ-DGN (paragraph 11.16) or DTRM-REQ-DGR (paragraph 11.17) input messages.

11.13 The DTRM may be restored to ACTIVE service from this state by using the DTRM-REQ-RST message as explained in paragraph 11.11. If additional maintenance is required with the DTRM operational but not carrying normal call traffic, the DTRM may be returned to the MAN OOS REMOVE state by using the DTRM-REQ-RMV input message as explained in paragraph 11.09.

D. Marking a DTRM Unavailable for Service

11.14 If major maintenance is required, a DTRM may be marked unavailable for service by typing in:

DTRM-REQ-UNV bbbb.

bbbb = Decimal number from 0 to 1023 identifying the DTRM to be marked unavailable for service.

System responds with PF followed by an LS01 output message indicating the request has been implemented. The DTRM is now in the UNAV FORCED state (T/M state 40). In this state, the DTRM is not operating and not available if the mate DTRM fails. This state is useful for major maintenance requiring power on the unit but assurance that the system will not attempt to place the unit into service.

E. Reinitializing a DTRM

11.15 If a DTRM must be fully reinitialized, type in:

DTRM-REQ-FRC bbbb.

bbbb = Decimal number between 0 and 1023 identifying the DTRM to be forced active.

System responds with an LS04 output message showing all the status information and current input data for the DTRM being forced before all software and hardware for that DTRM is reinitialized. An LS01 message is also printed indicating when the initialization is completed. Repeated LS04 messages may indicate software problems.

MANUAL DTRM DIAGNOSTICS, STATUS CHECKS AND AUDITS

> ***Note:*** See Fig. 23 for a diagram indicating from which maintenance states diagnostic results will be meaningful.

A. Diagnosing a DTRM (Normal Printout)

11.16 To diagnose a DTRM and obtain a normal printout, type in:

DTRM-REQ-DGN bbbb.

bbbb = Decimal number between 0 and 1023 identifying the DTRM to be diagnosed.

System responds with a DR01 output message containing diagnostic results for the DTRM. No trouble numbers will be printed if all tests pass is printed; otherwise, use the printed trouble numbers to access the appropriate trouble locating manual section and follow the procedure indicated.

B. Diagnosing a DTRM (Raw Data Printout)

11.17 To diagnose a DTRM and obtain a raw data printout of the diagnostic results, type in:

DTRM-REQ-DGR-bbbb.

bbbb = Decimal number from 0 to 1023 identifying DTRM to be diagnosed.

System responds with a DR02 message containing the raw data of a diagnostic result in octal form. Refer to the raw data tables given in PK-xxxxx. Trouble numbers are also printed and may be matched with numbers in the appropriate trouble locating manual.

C. Requesting DTRM Status

11.18 To request a printout of the status of a DTRM, type in:

DTRM-REQ-STS bbbb.

bbbb = Decimal number between 0 and 1023 identifying the DTRM to be checked.

System responds with an LS01 message containing the current status and configuration of a DTRM and its associated voice frequency links (VFLa and VFLb).

D. Requesting an Audit of a DTRM

11.19 To request a copy of the DTRM data base, type in:

DTRM-REQ-AUD bbbb.

bbbb = Decimal number between 0 and 1023 identifying the DTRM to be audited.

The system responds with an LS03 message showing those DTRM, VFL, and band status indicators that are currently being used to perform the CCIS data link I/O function in addition to data link maintenance control.◆

12. VFL STATE CONTROL

12.01 ◆Manual control of the VFL maintenance states is accomplished via the maintenance TTY using the VFLK-REQ input message. This message is functionally similar to the DTRM-REQ message described in Part 11; ie, it can be used to establish various maintenance states and/or configurations or request some action to be taken on the VFL.

MANUAL VFL STATE TRANSITIONS

12.02 The following paragraphs describe the various VFLK-REQ input messages required to manually change the state of the VFL. There is a definite sequence which must be followed when going from one state to another, as shown in the state diagram in Fig. 25. After determining which state the VFL is in (using the VFLK-REQ-STS input message, as described in paragraph 12.09), start at that state and type in the appropriate VFLK-REQ-xxx messages to allow progression through the required number of states until the desired VFL state is reached. The following descriptions of the various VFLK-REQ-xxx input messages correspond to the sequence given in the state diagram.

A. Removing a VFL from Service

12.03 To remove a VFL from service, type in:

VFLK-REQ-RMV bbbb c.

bbbb = Decimal number between 0 and 1023 identifying the DTRM

c = A or B identifying the VFL.

System responds with a PF followed by an LS01 output message indicating the system has implemented the request. The VFL is removed from the ACTIVE state and placed in the STBY/DLY state. In this state, the VFL is not carrying call traffic and is not connected to the DTRM. The mate VFL is placed in the ACTIVE state.

B. Marking a VFL Unavailable for Service

12.04 To mark a VFL unavailable for service, type in:

VFLK-REQ-UNV bbbb c.

bbbb = Decimal number between 0 and 1023 identifying the DTRM

c = A or B identifying the VFL

System responds with OK indicating the request has been implemented. The VFL has been changed from the STBY/DLY state to the UNV/REL state. In this state, the VFL is not available for service and cannot be automatically switched into service by the system. Also, the VFL access circuit is released (not connected); however, before the access circuit can be operated (connected), the VFL must be in this state.

C. Operating a VFL Access Circuit

12.05 To operate the VFL access circuit for a specified VFL, type in:

VFLK-REQ-OPR bbbb c.

bbbb = Decimal number between 0 and 1023 identifying the DTRM

c = A or B identifying the VFL

System responds with OK indicating the specified VFL access circuit has been operated. The VFL has been moved from the UNV/REL state into the UNV/OPR state. In this state, the VFL is connected to the network appearance of the shared maintenance bus used for manual VFL testing. In this state, the VFL is not available for service and transmission tests may be performed.

D. Releasing a VFL Access Circuit

12.06 To release the VFL access circuit for a specified VFL, type in:

VFLK-REQ-REL bbbb c.

bbbb = Decimal number between 0 and 1023 identifying the DTRM

c = A or B identifying the VFL

The system responds with OK indicating the specified VFL access has been released. The VFL is now in the UNV/REL state and has been disconnected from the maintenance bus.

E. Placing a VFL in the Manual Out-of-Service State

12.07 To place the VFL in the manual OOS state, type in:

VFLK-REQ-OOS bbbb c.

bbbb = Decimal number between 0 and 1023 identifying the DTRM

c = A or B identifying the VFL.

System responds with OK indicating the request has been implemented. This causes a transition from the UNV/REL state to the STBY/DLY state. The automatic VFL test may be initiated only from this state. (See paragraph 12.10.)

F. Restoring a VFL to Service

12.08 To manually restore a VFL to service, type in:

VFLK-REQ-RST bbbb c.

bbbb = Decimal number between 0 and 1023 identifying the DTRM

c = A or B identifying the VFL.

The system responds with PF followed by an LS01 output message indicating that the request has been implemented. The VFL is restored to the ACTIVE state, carrying call traffic. If the associated DTRM is not active, the VFL is restored to the STBY/RDY state. The mate VFL is removed from service.

MANUAL VFL STATUS CHECKS, TESTS, AND AUDITS

A. Requesting VFL Status

12.09 To request a printout of the status of a VFL, type in:

VFLK-REQ-STS bbbb c.

bbbb =Decimal number between 0 and 1023 identifying the DTRM

c = A or B identifying the VFL to be checked.

The system responds with an LS01 message containing information on the current status and configuration of the specified DTRM and associated VFLs.

B. Initiating the Automatic Standby VFL Test

Note: The VFL must be in the STBY/DLY state to perform this test.

12.10 To initiate the automatic VFL test, type in:

VFLK-REQ-TST bbbb c.

bbbb = Decimal number between 0 and 1023 identifying the DTRM

c = A or B identifying the VFL to be tested.

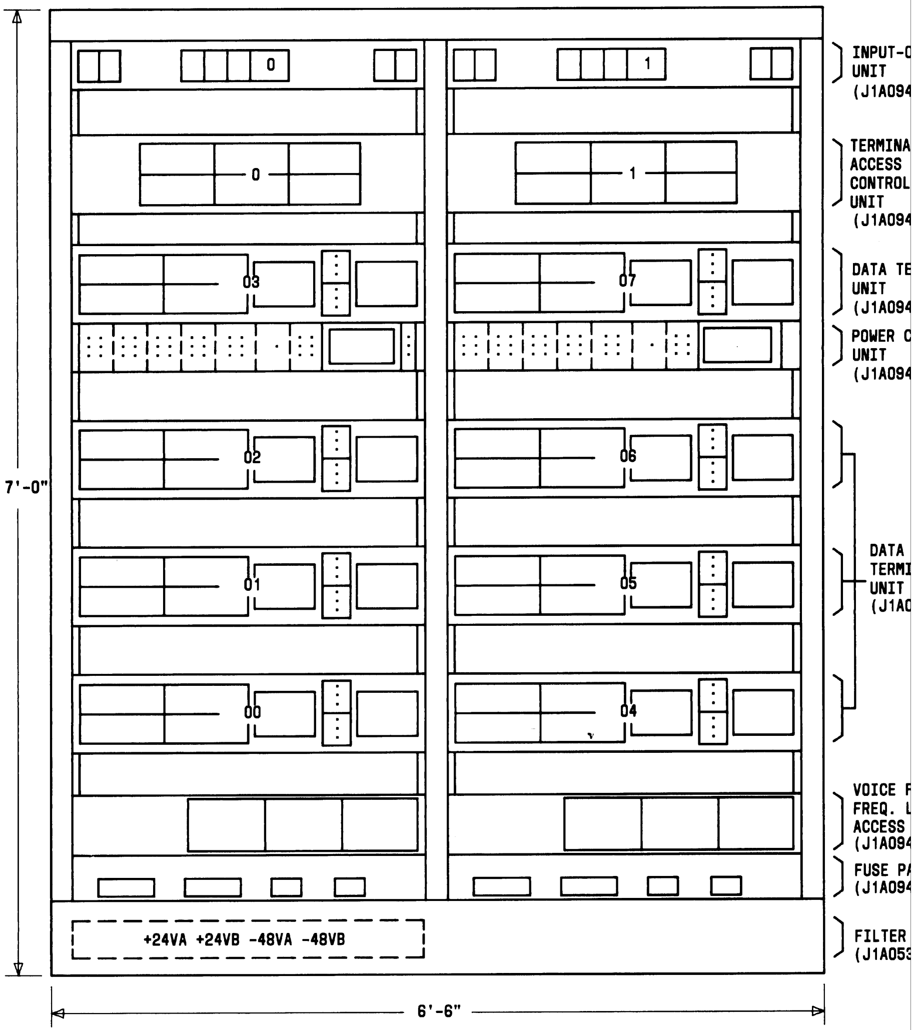
System responds with an LS01 message giving the results of the test. The switching office (via the link security routine) applies a loop to the VFL and sends a test-standby VFL signal to the STP. The STP then performs the loop-around test and returns the results to the switching office via a VFL test-passed signal or a VFL test-failed signal.◀

13. ABBREVIATIONS AND ACRONYMS

13.01 The following abbreviations and acronyms are used in this section.

ALT	Automatic Link Test
AUTO	Automatic
CCIS	Common Channel Interoffice Signaling
CONT	Controller
CP	Circuit Pack
CPD	Central Pulse Distributor
DEN	Data Enable
DS	Data Set
DTRM	Data Terminal
ESS	Electronic Switching System
FA	Fuse Alarm
IGFET	Integrated Field Effect Transistor
I/O	Input/Output
LBP	Lock Babble Protect
LSU	Lone Signal Unit
MCT	Master Clock Time
MN	Minor Alarm
MUM	Multiple Unit Message
NADRGO	Data-Register-Gate-Out(Bits 1 through 12)
NBDRGO	Data-Register-Gate-Out(Bits 13 through 24)
OEN	Opcode Enable
OOS	Out Of Service
PUAB	Peripheral Unit Address Bus
RQ	Reset Quarantine Enable
SCAB	Scanner Answer Bus
SQ	Set Quarantine Enable
STP	Signal Transfer Point
SU	Signal Unit
TASW	Terminal All-Seems-Well
TD	Terminal Data
UBP	Unlock Babble Protect

VFL	Voice Frequency Link
VFLA	Voice Frequency Link Access
WRMI	We-Really-Mean-It.


0
1
0
1
03
07
02
06
01
05
00
04
7'-0"
6'-6"
+24VA +24VB -48VA -48VB
INPUT-O
UNIT
(J1A094
TERMINA
ACCESS
CONTROL
UNIT
(J1A094
DATA TE
UNIT
(J1A094
POWER C
UNIT
(J1A094
DATA
TERMI
UNIT
(J1AO
VOICE F
FREQ. L
ACCESS
(J1A094
FUSE PA
(J1A094
FILTER
(J1A053

]

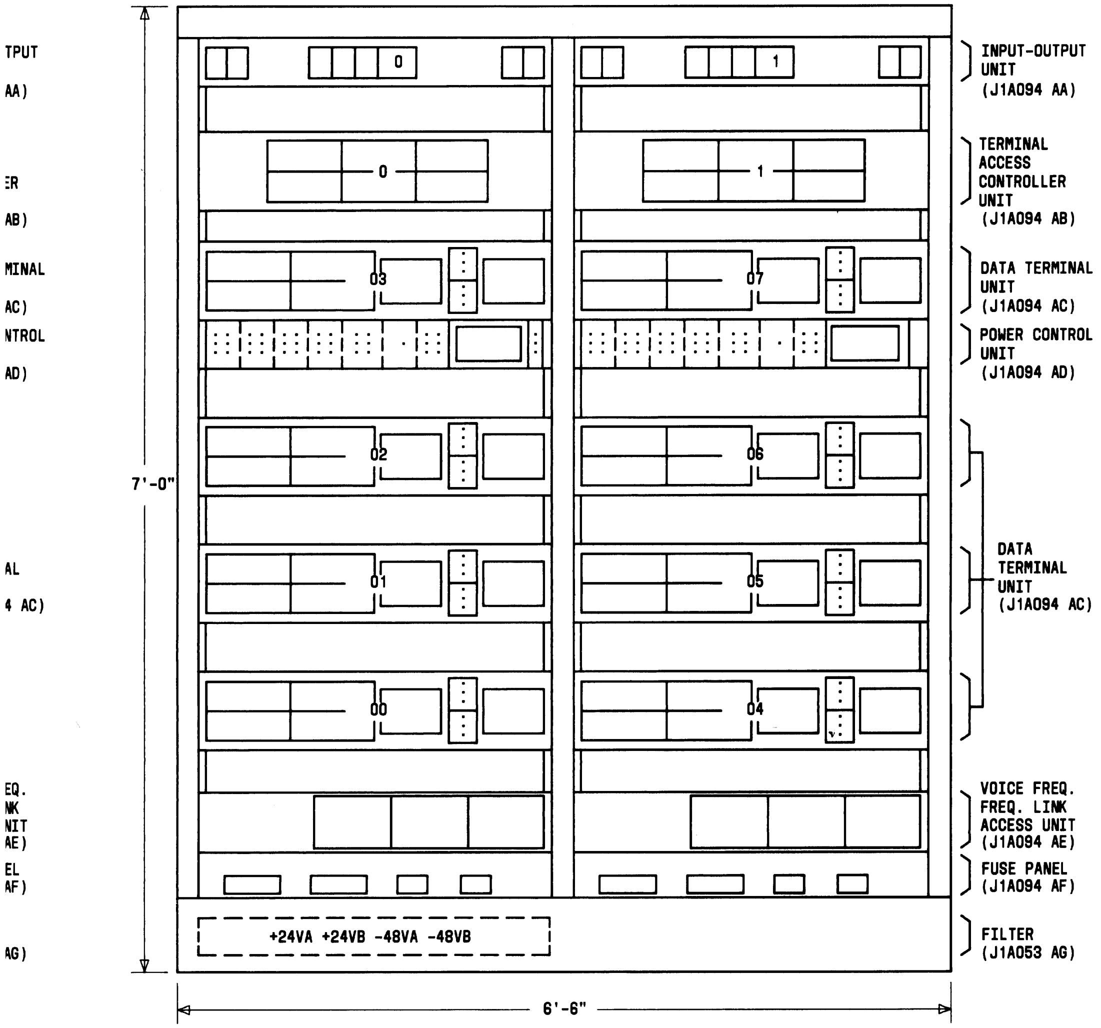
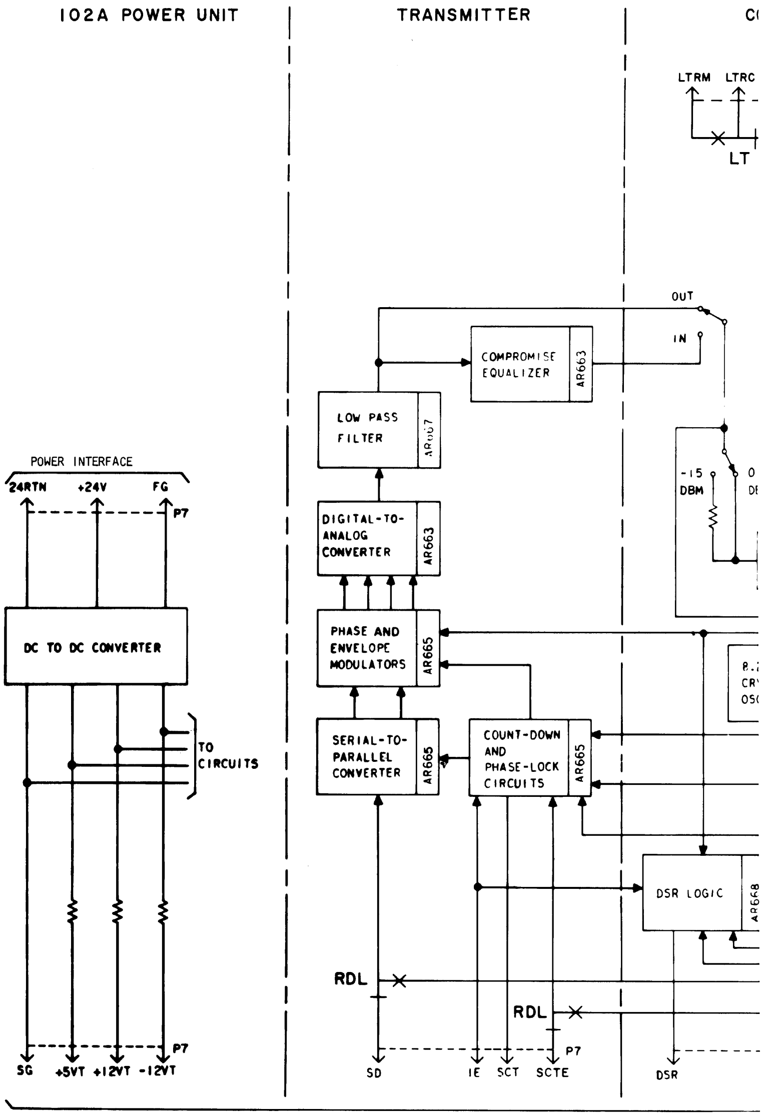

TPUT
AA)
ER
AB)
MINAL
AC)
NTROL
AD)
AL
4 AC)
EQ.
NK
NIT
AE)
EL
AF)
AG)
0
1
0
1
03
07
02
06
01
05
00
04
7'-0"
+24VA +24VB -48VA -48VB
6'-6"
INPUT-OUTPUT UNIT (J1A094 AA)
TERMINAL ACCESS CONTROLLER UNIT (J1A094 AB)
DATA TERMINAL UNIT (J1A094 AC)
POWER CONTROL UNIT (J1A094 AD)
DATA TERMINAL UNIT (J1A094 AC)
VOICE FREQ. FREQ. LINK ACCESS UNIT (J1A094 AE)
FUSE PANEL (J1A094 AF)
FILTER (J1A053 AG)

Fig. 26—Data Terminal Base Frame J1A094A


102A POWER UNIT
TRANSMITTER
C
LTRM
LTRC
LT
OUT
IN
COMPROMISE EQUALIZER
AR663
LOW PASS FILTER
AR667
-15 DBM
0
D
POWER INTERFACE
24RTN
+24V
FG
P7
DIGITAL-TO-ANALOG CONVERTER
AR663
PHASE AND ENVELOPE MODULATORS
AR665
DC TO DC CONVERTER
TO CIRCUITS
SERIAL-TO-PARALLEL CONVERTER
AR665
COUNT-DOWN AND PHASE-LOCK CIRCUITS
AR665
DSR LOGIC
AR668
RDL
RDL
P7
P7
SG
+5VT
+12VT
-12VT
SD
IE
SCT
SCTE
DSR

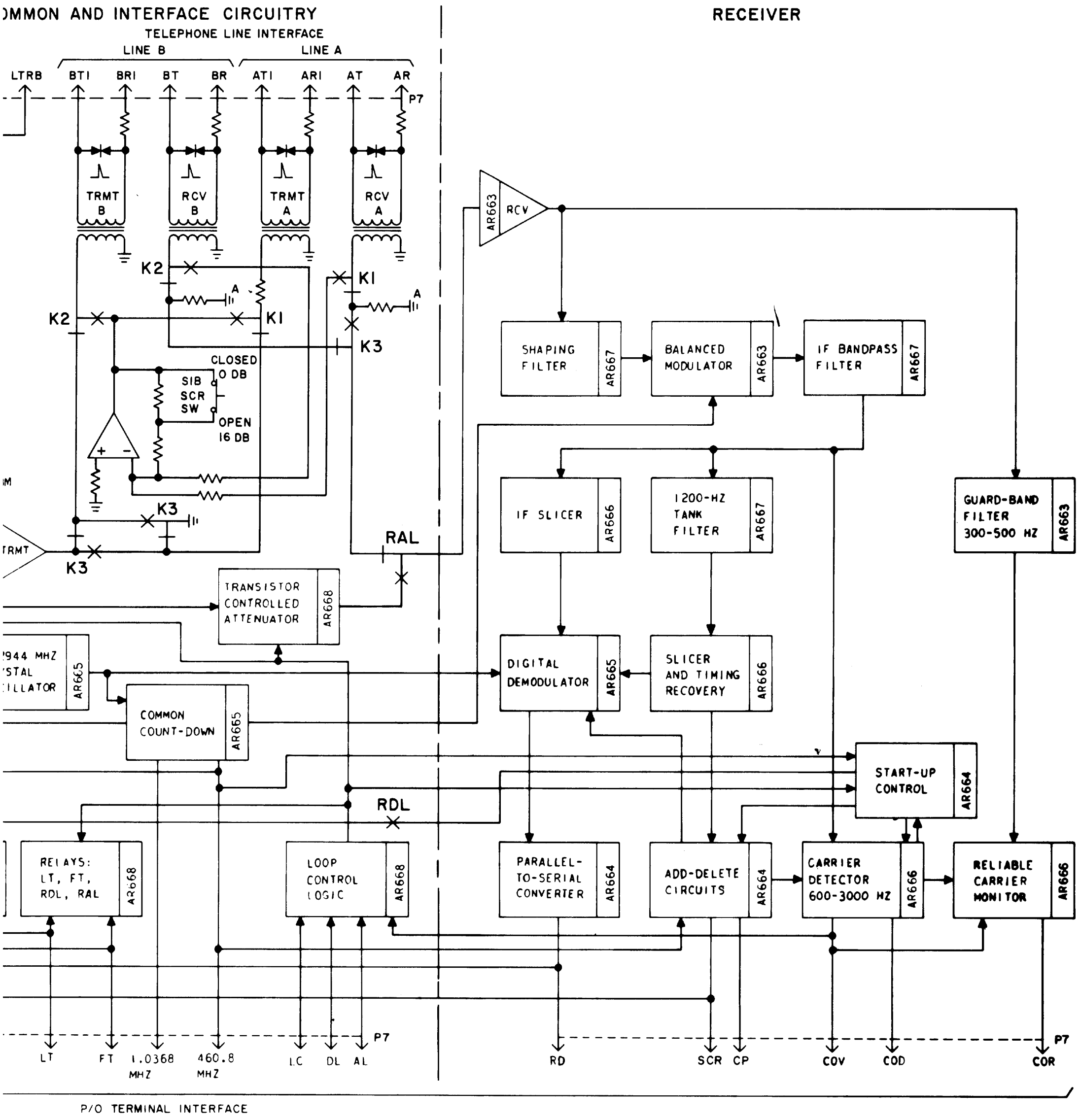
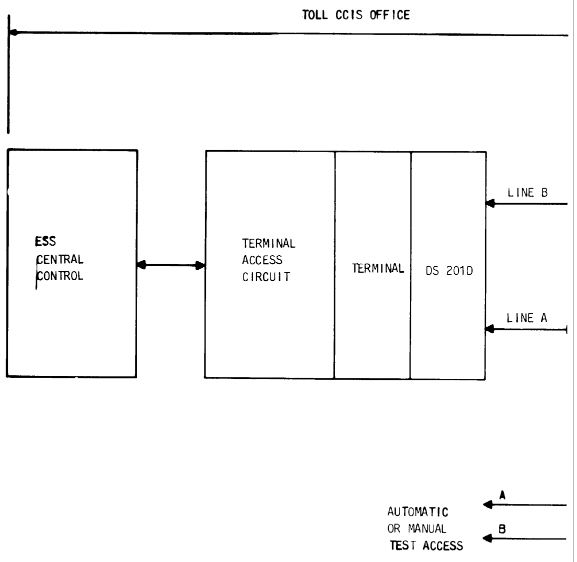


Fig. 27—Data Set DS 201D—Simplified Functional Schematic


TOLL CCIS OFFICE
ESS
CENTRAL
CONTROL
TERMINAL
ACCESS
CIRCUIT
TERMINAL
DS 201D
LINE B
LINE A
AUTOMATIC
OR MANUAL
TEST ACCESS
A
B

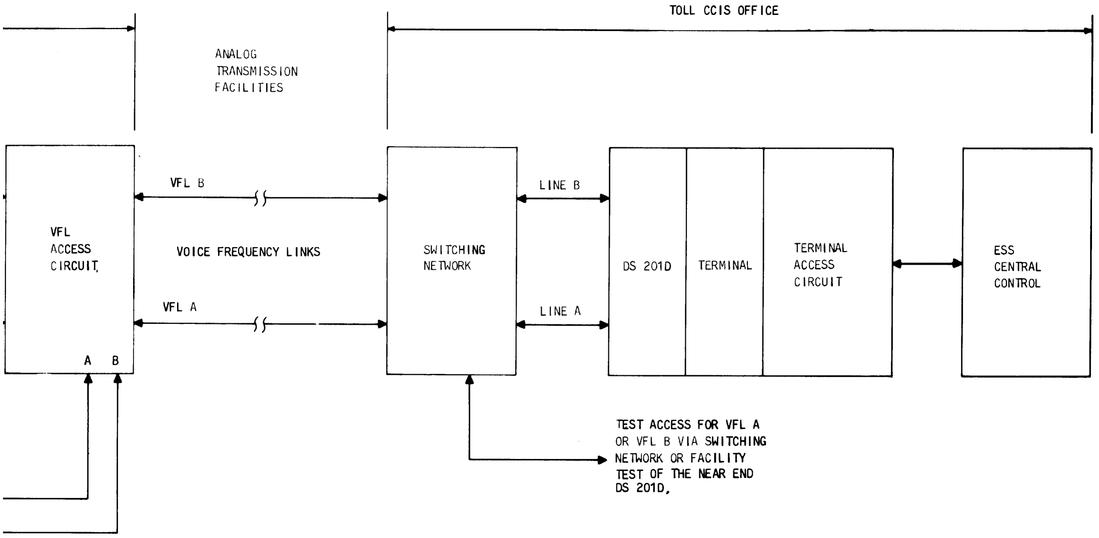
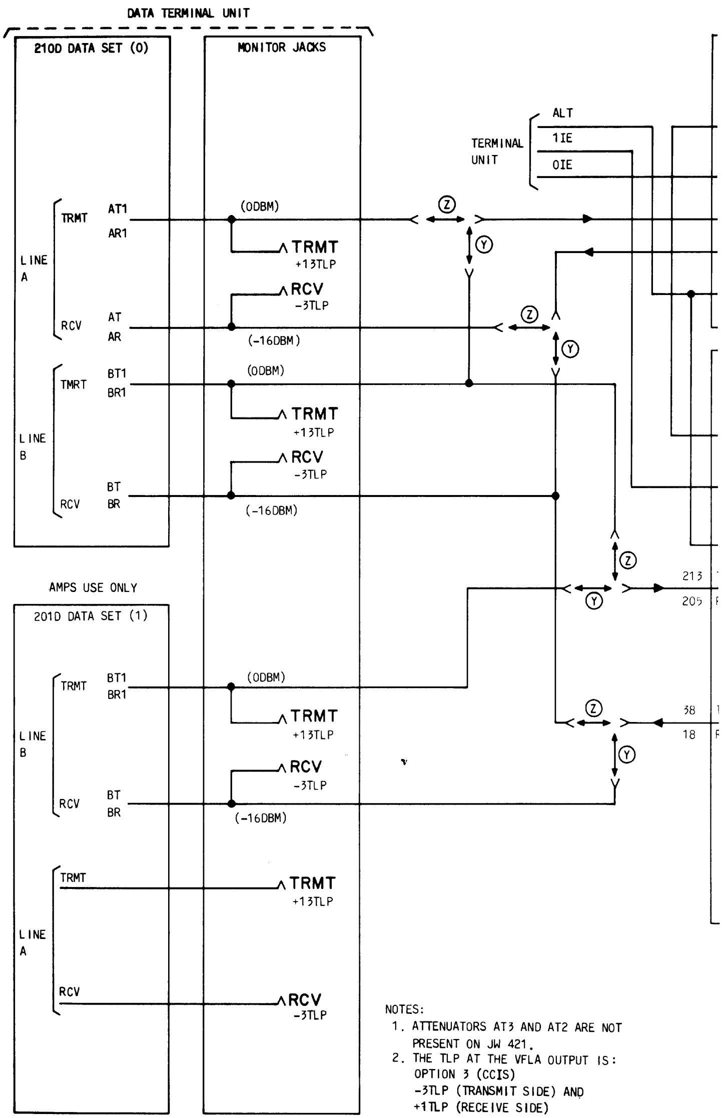


Fig. 28—Basic CCIS Configuration



NOTES:
1. ATTENUATORS AT3 AND AT2 ARE NOT PRESENT ON JW 421.
2. THE TLP AT THE VFLA OUTPUT IS:
OPTION 3 (CCIS)
-3TLP (TRANSMIT SIDE) AND
+1TLP (RECEIVE SIDE)
OPTION 2 (AMPS)
+13TLP (TRANSMIT SIDE) AND
-3TLP (RECEIVE SIDE)

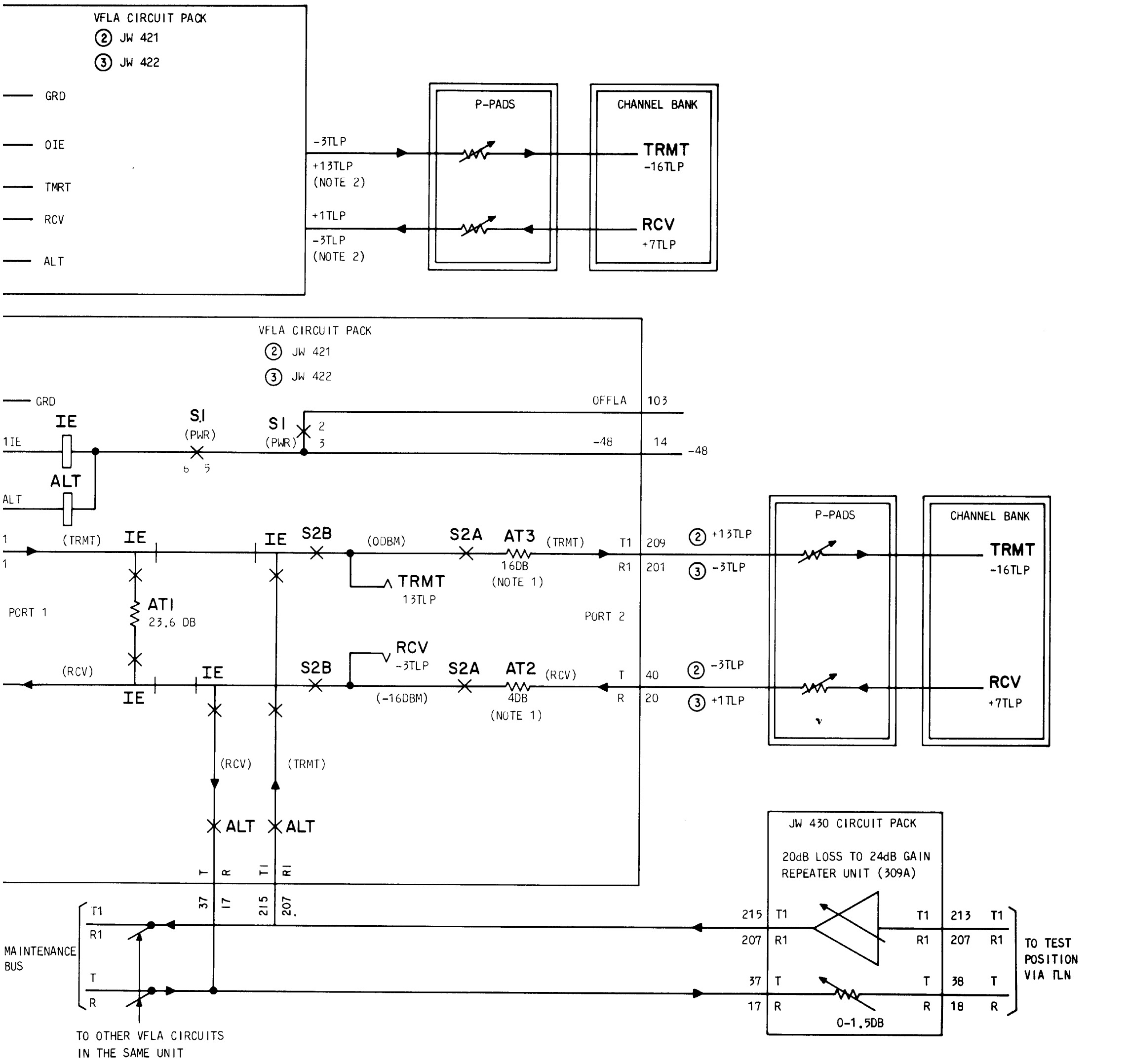
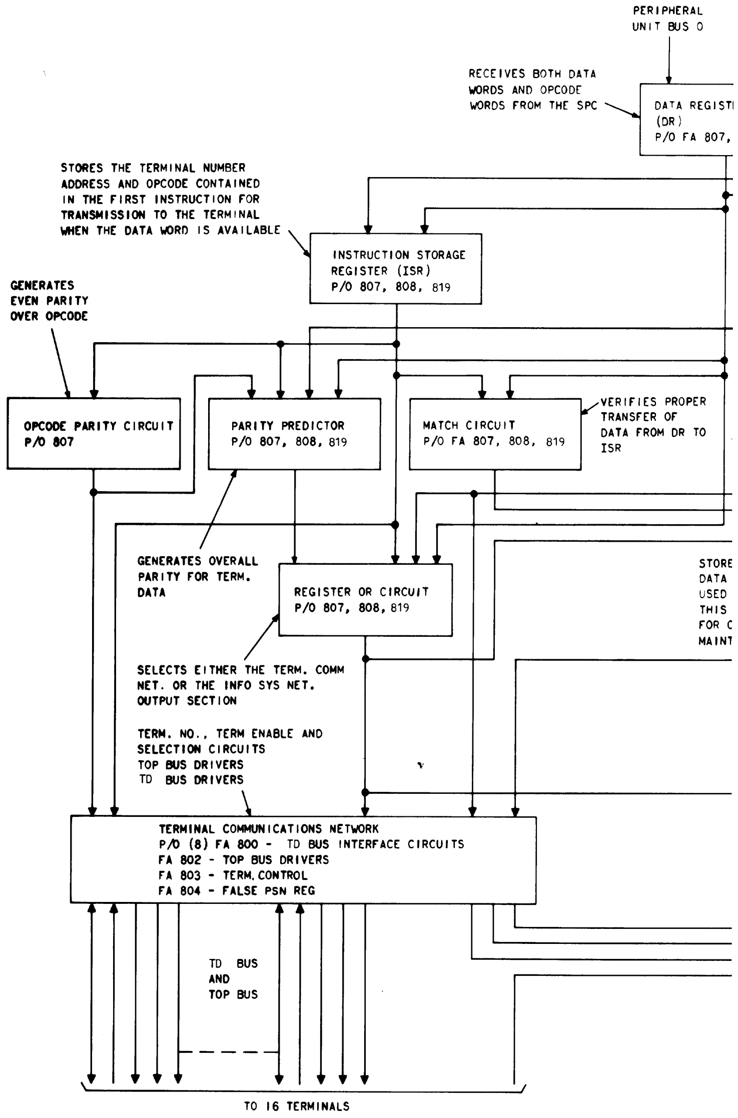


Fig. 29—Voice Frequency Link Access Unit—Block Diagram


PERIPHERAL
UNIT BUS 0
RECEIVES BOTH DATA
WORDS AND OPCODE
WORDS FROM THE SPC
DATA REGISTI
(DR)
P/O FA 807,
STORES THE TERMINAL NUMBER
ADDRESS AND OPCODE CONTAINED
IN THE FIRST INSTRUCTION FOR
TRANSMISSION TO THE TERMINAL
WHEN THE DATA WORD IS AVAILABLE
INSTRUCTION STORAGE
REGISTER (ISR)
P/O 807, 808, 819
GENERATES
EVEN PARITY
OVER OPCODE
OPCODE PARITY CIRCUIT
P/O 807
PARITY PREDICTOR
P/O 807, 808, 819
MATCH CIRCUIT
P/O FA 807, 808, 819
VERIFIES PROPER
TRANSFER OF
DATA FROM DR TO
ISR
GENERATES OVERALL
PARITY FOR TERM.
DATA
REGISTER OR CIRCUIT
P/O 807, 808, 819
STORE
DATA
USED
THIS
FOR C
MAINT
SELECTS EITHER THE TERM. COMM
NET. OR THE INFO SYS NET.
OUTPUT SECTION
TERM. NO., TERM ENABLE AND
SELECTION CIRCUITS
TOP BUS DRIVERS
TD BUS DRIVERS
TERMINAL COMMUNICATIONS NETWORK
P/O (8) FA 800 - TD BUS INTERFACE CIRCUITS
FA 802 - TOP BUS DRIVERS
FA 803 - TERM. CONTROL
FA 804 - FALSE PSN REG
TD BUS
AND
TOP BUS
TO 16 TERMINALS

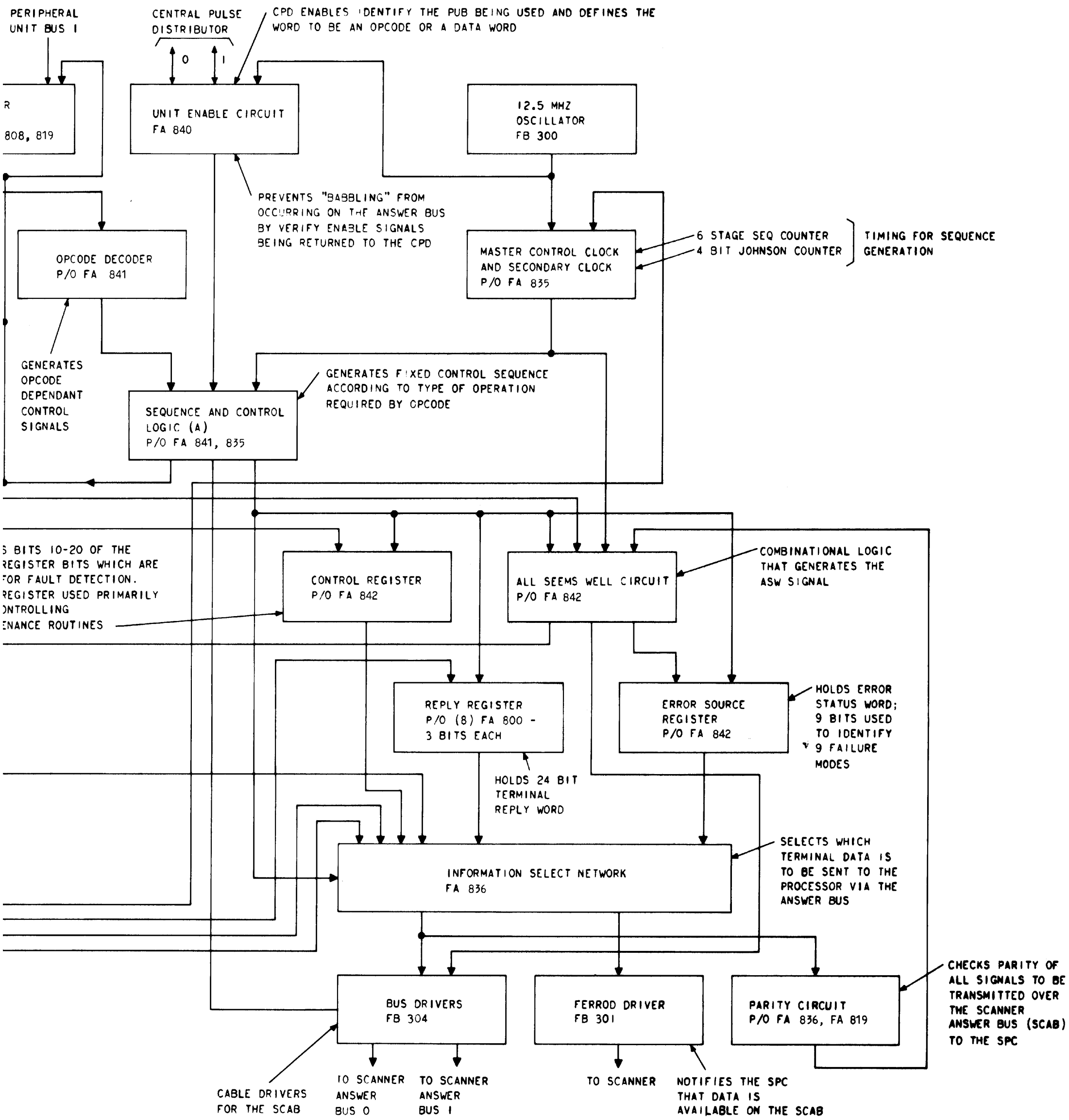
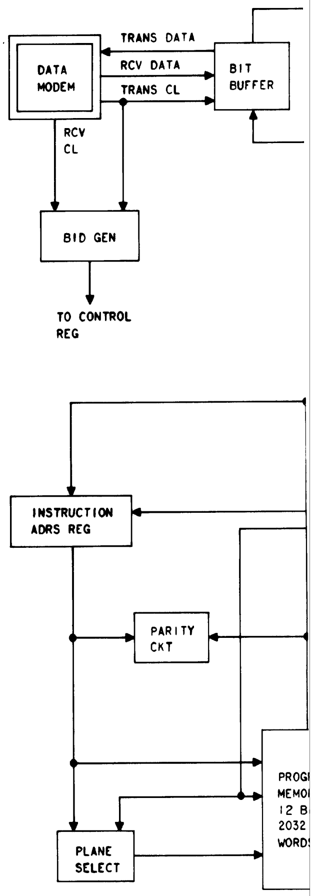

PERIPHERAL UNIT BUS I
CENTRAL PULSE DISTRIBUTOR
0
I
CPD ENABLES IDENTIFY THE PUB BEING USED AND DEFINES THE WORD TO BE AN OPCODE OR A DATA WORD
R
808, 819
UNIT ENABLE CIRCUIT FA 840
12.5 MHZ OSCILLATOR FB 300
PREVENTS "BABBLING" FROM OCCURRING ON THE ANSWER BUS BY VERIFY ENABLE SIGNALS BEING RETURNED TO THE CPD
OPCODE DECODER P/O FA 841
MASTER CONTROL CLOCK AND SECONDARY CLOCK P/O FA 835
6 STAGE SEQ COUNTER
4 BIT JOHNSON COUNTER
TIMING FOR SEQUENCE GENERATION
GENERATES OPCODE DEPENDANT CONTROL SIGNALS
SEQUENCE AND CONTROL LOGIC (A) P/O FA 841, 835
GENERATES FIXED CONTROL SEQUENCE ACCORDING TO TYPE OF OPERATION REQUIRED BY OPCODE
S BITS 10-20 OF THE
REGISTER BITS WHICH ARE
FOR FAULT DETECTION.
REGISTER USED PRIMARILY
ONTROLLING
ENANCE ROUTINES
CONTROL REGISTER P/O FA 842
ALL SEEMS WELL CIRCUIT P/O FA 842
COMBINATIONAL LOGIC THAT GENERATES THE ASW SIGNAL
REPLY REGISTER P/O (8) FA 800 - 3 BITS EACH
ERROR SOURCE REGISTER P/O FA 842
HOLDS ERROR STATUS WORD; 9 BITS USED TO IDENTIFY 9 FAILURE MODES
HOLDS 24 BIT TERMINAL REPLY WORD
INFORMATION SELECT NETWORK FA 836
SELECTS WHICH TERMINAL DATA IS TO BE SENT TO THE PROCESSOR VIA THE ANSWER BUS
BUS DRIVERS FB 304
FERROD DRIVER FB 301
PARITY CIRCUIT P/O FA 836, FA 819
CHECKS PARITY OF ALL SIGNALS TO BE TRANSMITTED OVER THE SCANNER ANSWER BUS (SCAB) TO THE SPC
CABLE DRIVERS FOR THE SCAB
TO SCANNER ANSWER BUS 0
TO SCANNER ANSWER BUS I
TO SCANNER
NOTIFIES THE SPC THAT DATA IS AVAILABLE ON THE SCAB

Fig. 30—CONT Functional Block Diagram


TRANS DATA
DATA MODEM
RCV DATA
TRANS CL
BIT BUFFER
RCV CL
BID GEN
TO CONTROL REG
INSTRUCTION ADRS REG
PARITY CKT
PROG
MEMO
12 B
2032
WORDS
PLANE SELECT

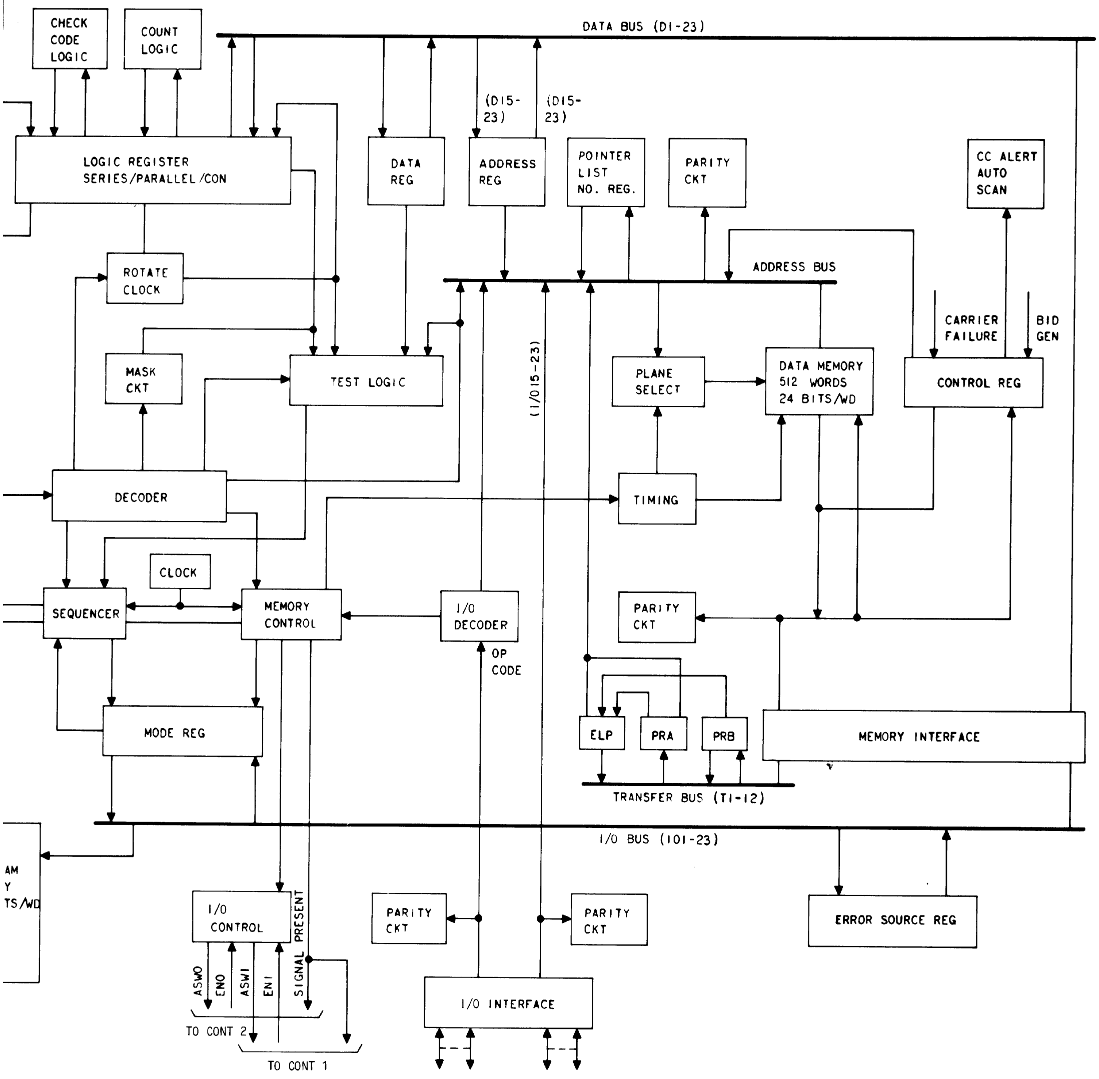


Fig. 31—CCIS Terminal—Block Diagram

GBPPR Hot Pack

Overview

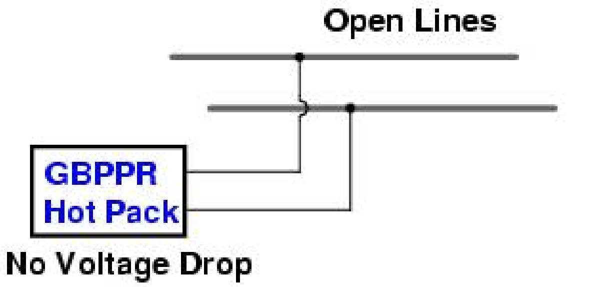
The *GBPPR Hot Pack* is a handy TSCM device which uses a high-voltage power source to check the integrity of any *unconnected* wiring. The *GBPPR Hot Pack* provides an approximate voltage output of 700 VDC, but with very little current. This is then connected to the device or wiring under test via some hook-up wires or an integrated outlet. Once connected, any measured reduction in voltage is an indication that there is something connected to the line or that the line is "leaking" in some way. Two internal digital multimeters measure both the voltage and current draw at the same time. Each of these meters needs to be powered via an external power source, 9 volt batteries in this case.

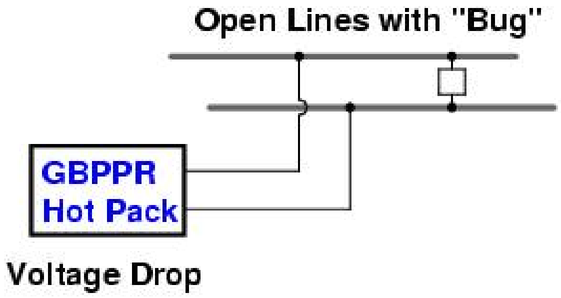
A good example of an item to test is a normal, everyday table lamp. When you remove the lightbulb, the wiring *should* show up as an "open" circuit. That is, no current should flow through the wiring. If you connect the power cord up to the *GBPPR Hot Pack*, and it shows a slight reduction in high-voltage output, then you know there is an "unknown" device connected in parallel with the lamp's internal wiring, or it could be the power cord is bad, you never know. Always perform a good *visual* overview of everthing as you perform a TSCM sweep.

Other good items to check are mechanical hook-switches inside phones, intercom/furnace/doorbell wiring, conference or boardroom speaker systems, and overhead lighting systems. All of these are targets to a potential eavesdropper.

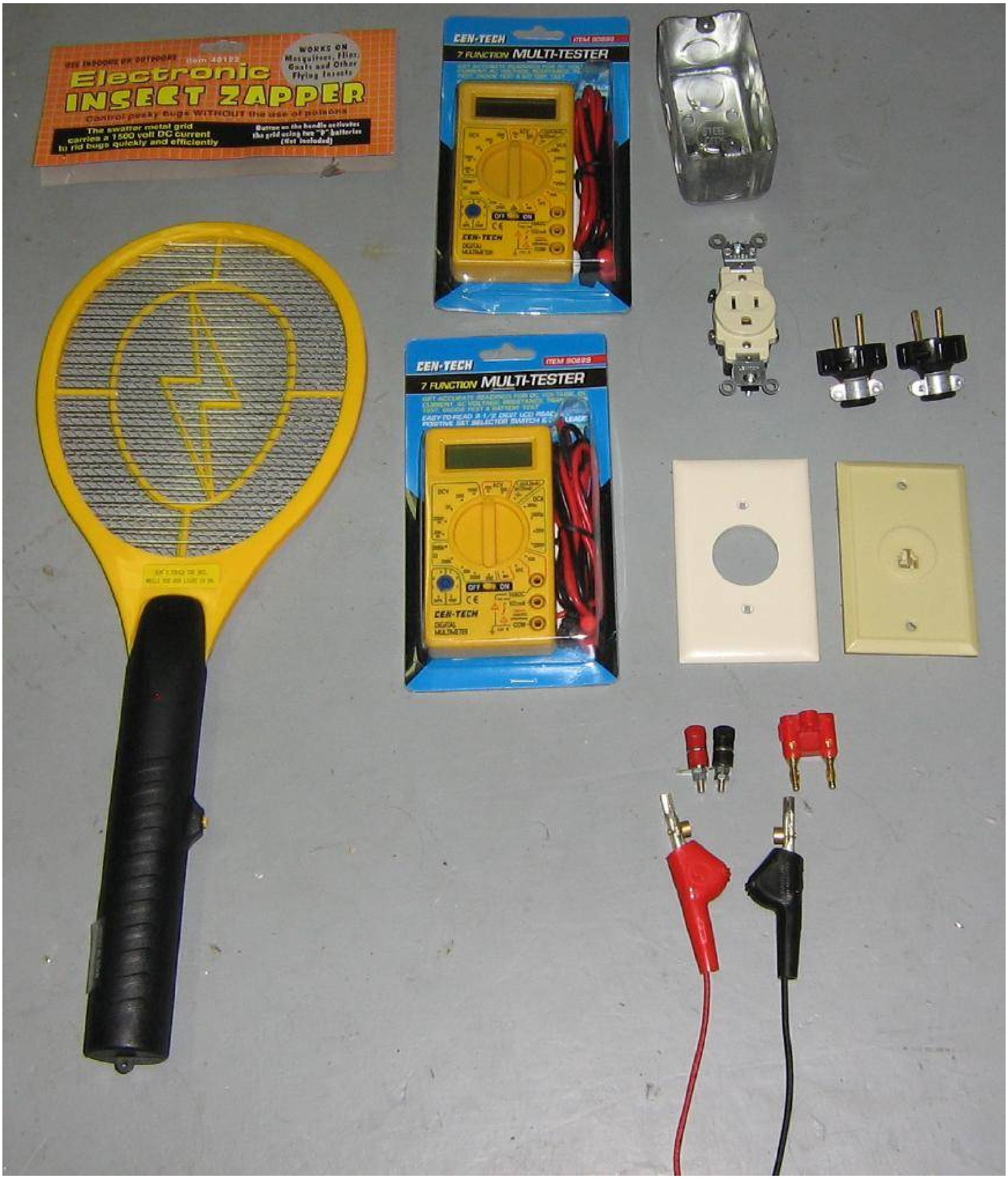
This is also ideal for checking telephone lines. Parallel telephone taps or automatic tape recorder starters can be easily detected, even if they are positioned after a "loading coil" as some professionals will do. You will need to disconnect the telephone line from the Main Distribution Frame (MDF) at the local central office though. This can be done by using the various remote test systems (Proctor, DATU, Recent Change) or by dialing an "open termination" test number. Social engineering a frame technician is also possible.

Example

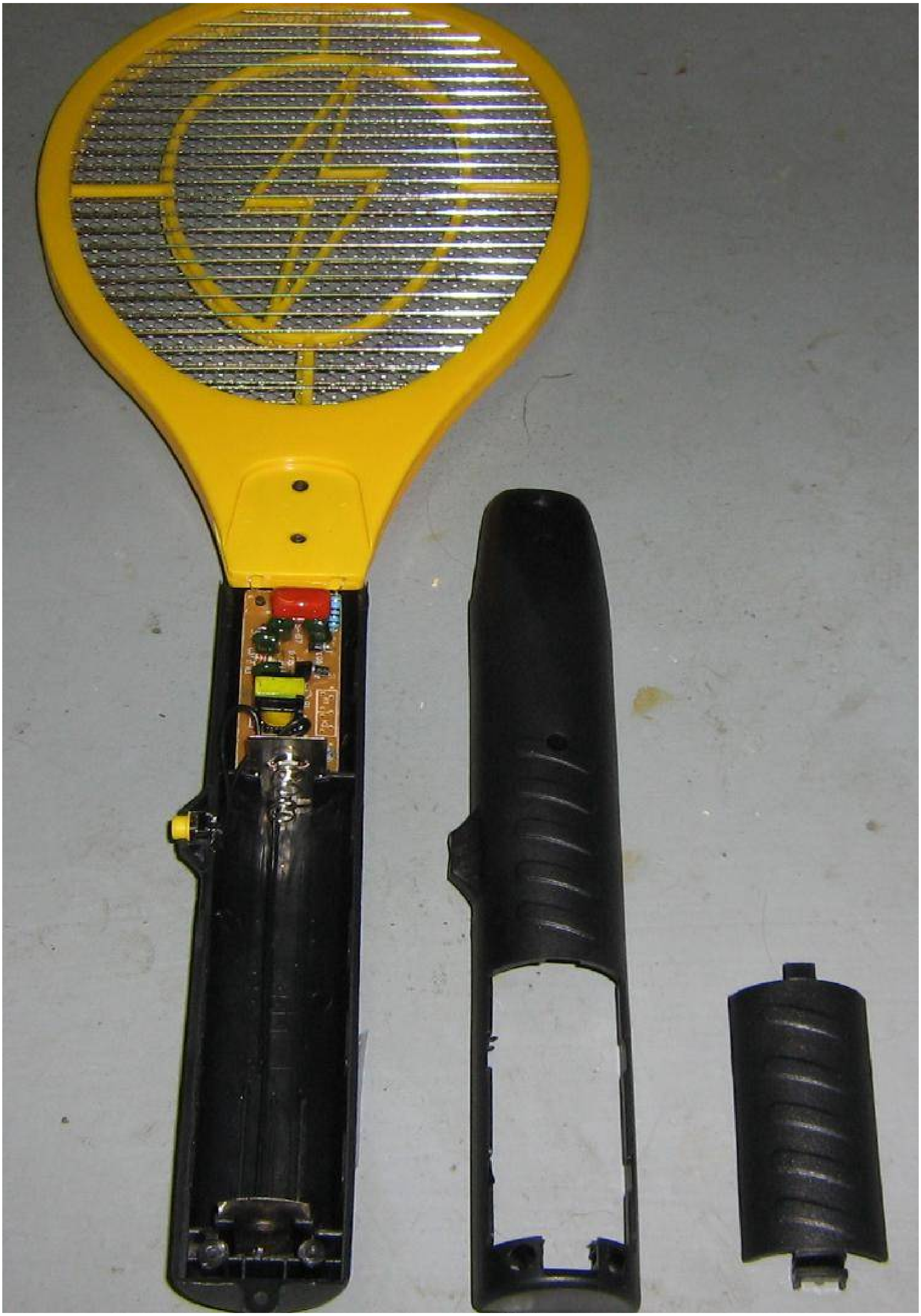




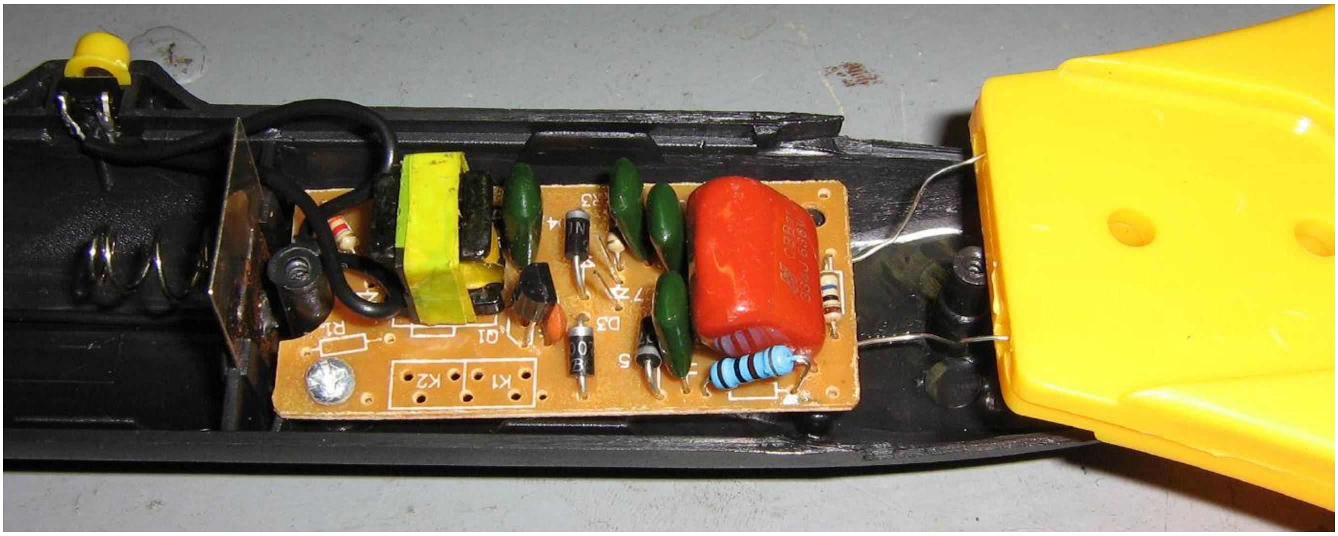
Pictures & Construction


USE INDOORS OR OUTDOORS
Item 40122
WORKS ON Mosquitoes, Flies, Gnats and Other Flying Insects
Electronic
INSECT ZAPPER
Control pesky bugs WITHOUT the use of poisons
The swatter metal grid carries a 1500 volt DC current to rid bugs quickly and efficiently
Button on the handle activates the grid using two "D" batteries (Not Included)
CEN-TECH
ITEM 90899
7 FUNCTION MULTI-TESTER
CEN-TECH
ITEM 90899
7 FUNCTION MULTI-TESTER
CEN-TECH
DIGITAL MULTIMETER
OFF
ON
COM

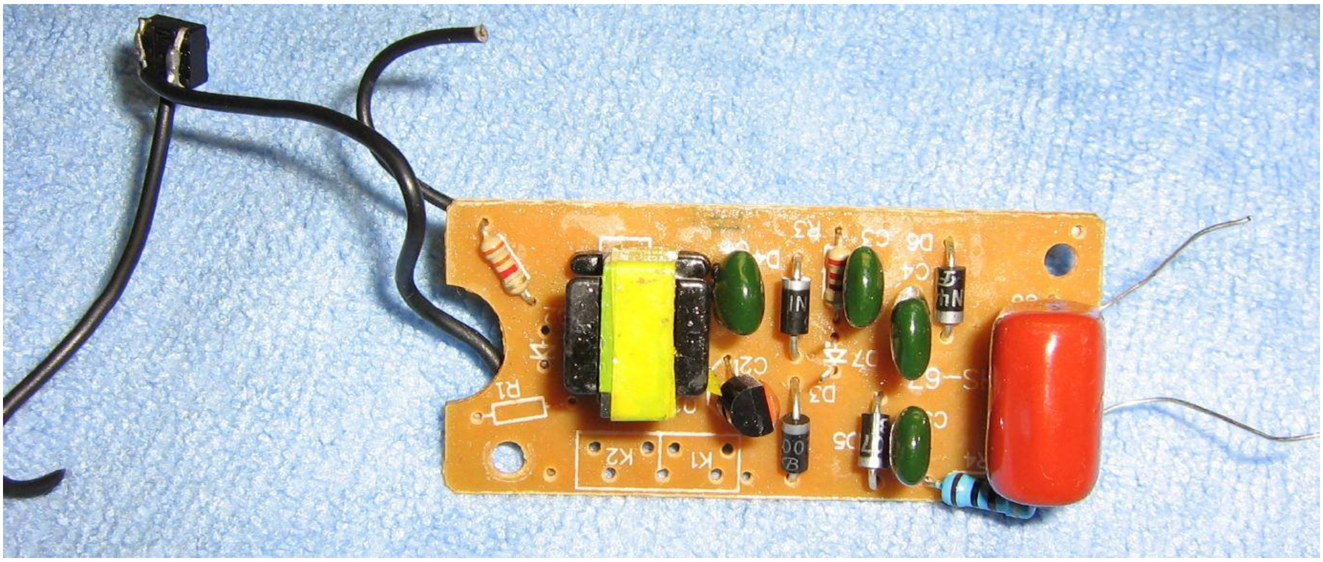
Components you'll need. The source for the high−voltage power supply will come from a Harbor Freight Tools Electronic Insect Zapper (#40122). The two Cen−Tech multimeters are also from Harbor Freight Tools (#90899). To the right of the meters are the parts needed for the outlet and also banana jacks for connecting a pair of J.S. Popper clips. A wall mounted RJ−11 telephone jack is shown to the right of the outlet plate.



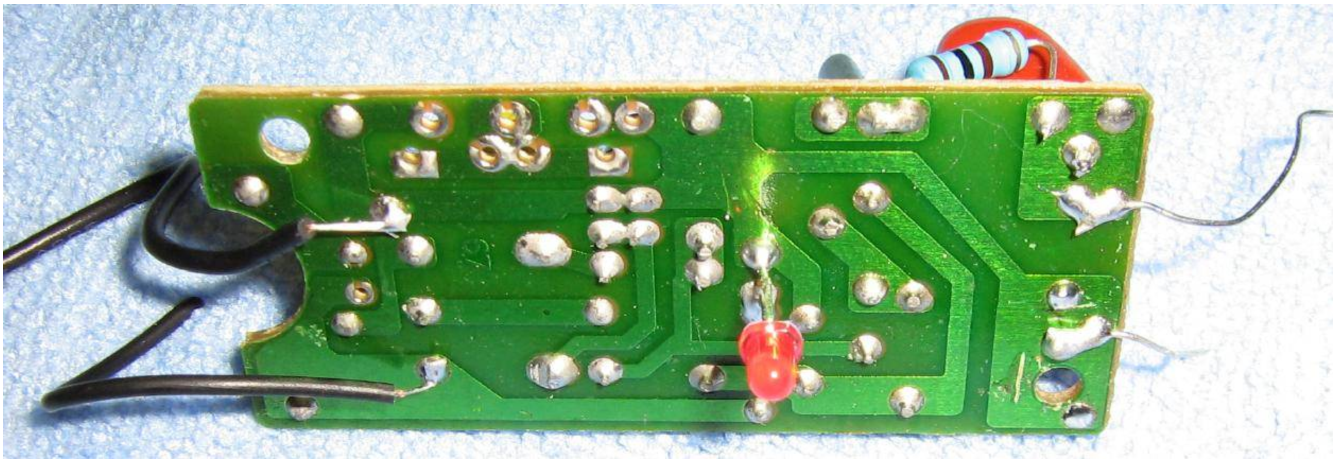
Taking the electronic insect zapper apart. It runs from two "D" size batteries. It says it generates 1,500 VDC, but its output will vary with the load under test.



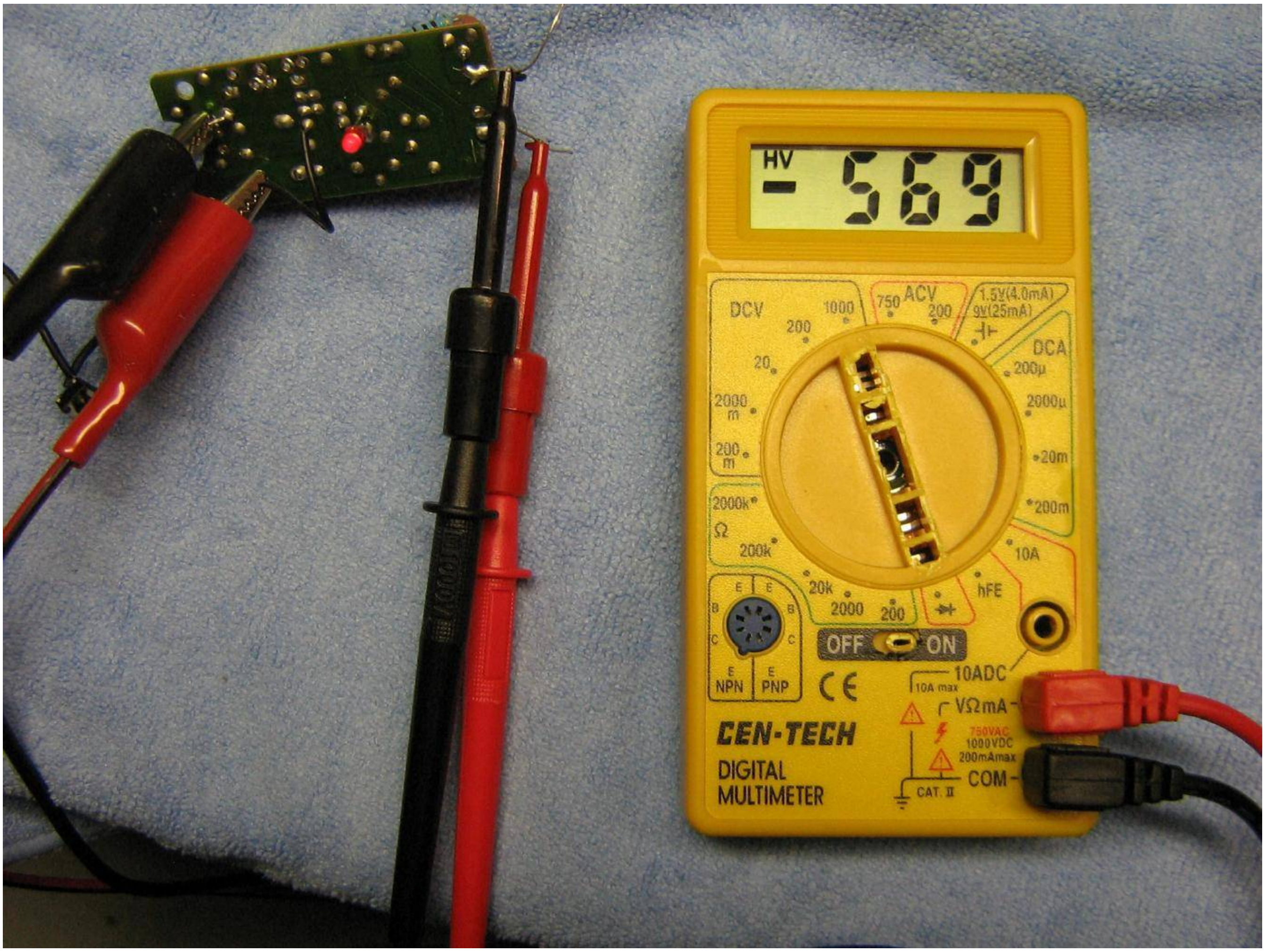
High−voltage power supply mounted inside the electronic insect zapper. Be careful to note the wiring when you remove it.



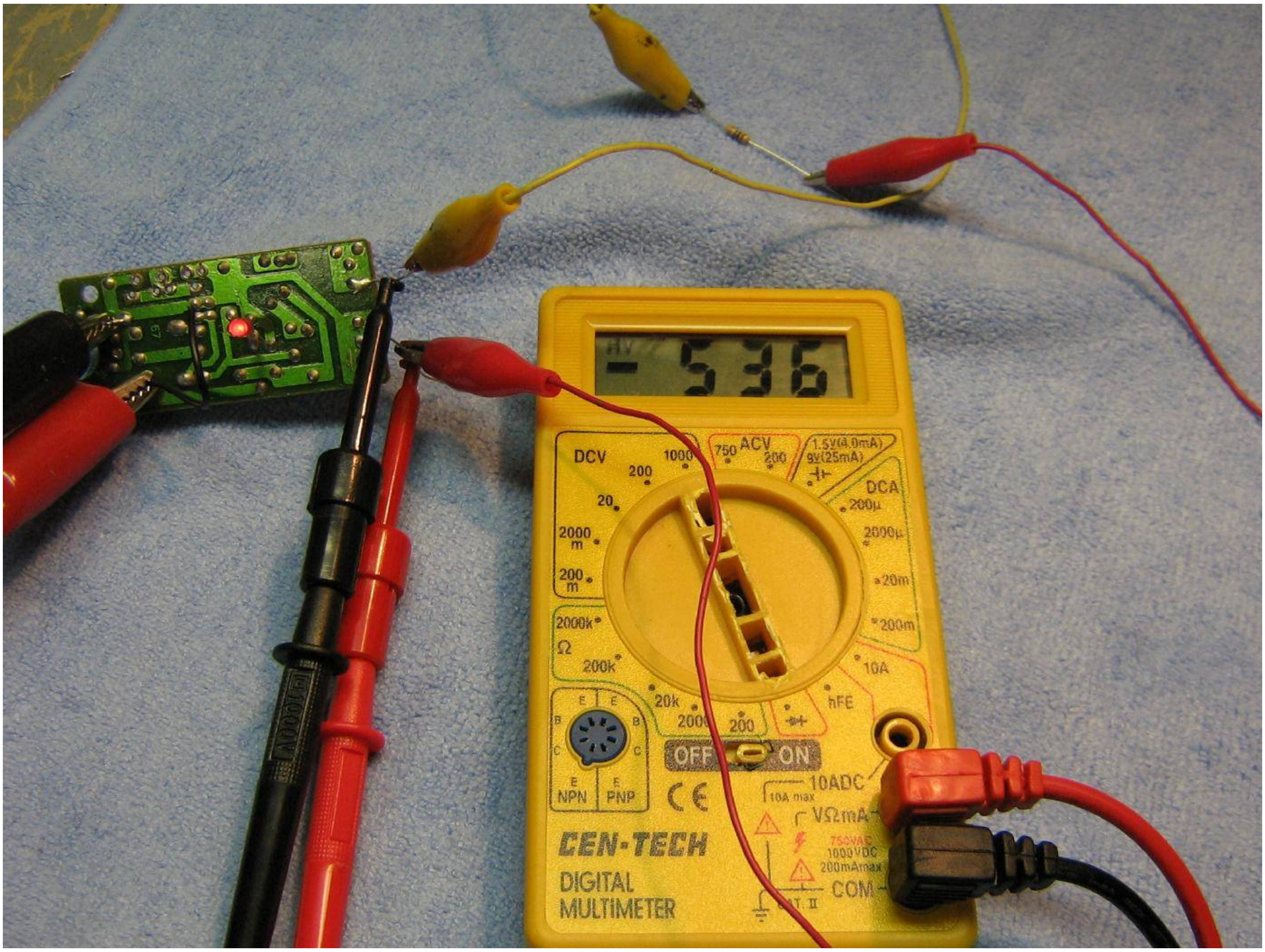
The high−voltage power supply is now removed. It uses a simple DC−to−DC converter to increase the incoming 3 VDC to over 1,000 VDC. A 10 Mohm resistor across the output high−voltage capacitor will drain the capacitor when powered off to prevent getting shocked. It is also a good idea to replace the 100 ohm current−limiting resistor (the blue, 1/2 watt one) with a 10 kohm resistor. This will help to protect the high−voltage power supply from short circuits.



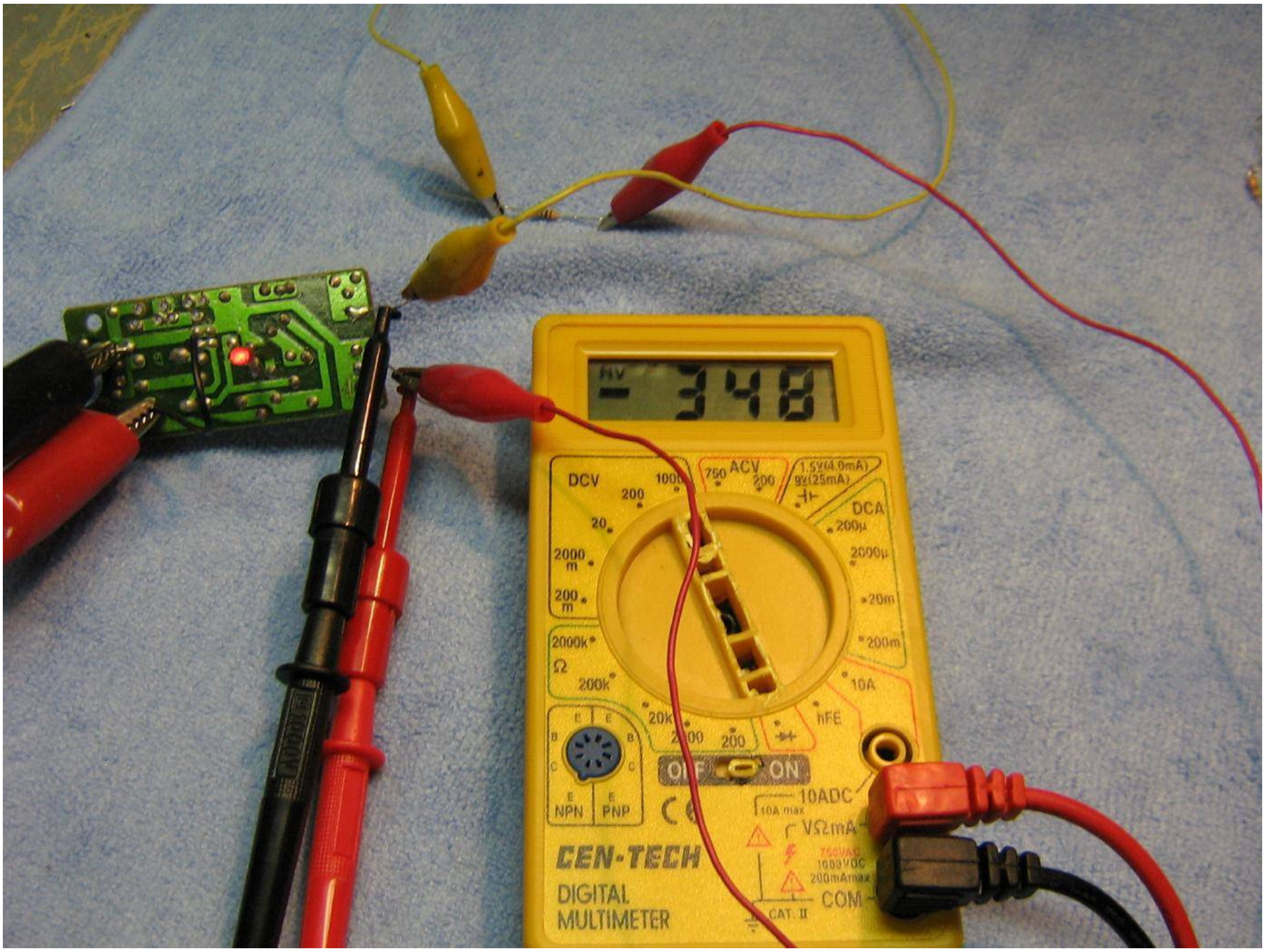
Underside of the high−voltage power supply's PC board. The top−left wire is ground, the bottom−left wire is the +3 VDC battery input. A power−indicating LED is in the middle. The high−voltage output is on the right. It shares a common ground with the DC input.



Test operation. The high−voltage output of this particular power supply when loaded with just the Cen−Tech multimeter is 569 VDC.

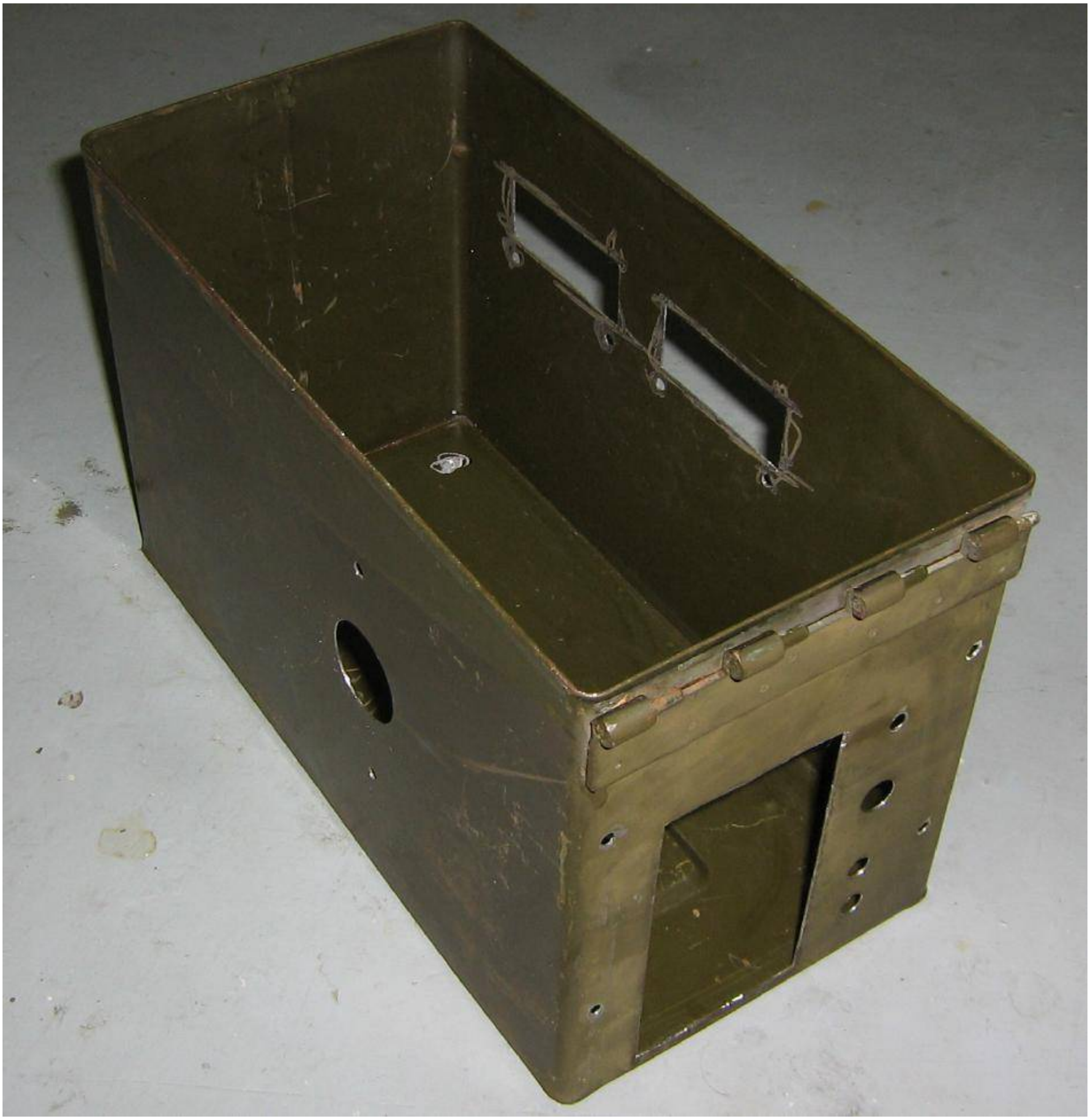


Now a 10 megaohm resistor is placed in *parallel* with the high−voltage output and the meter. It drops to 536 VDC.

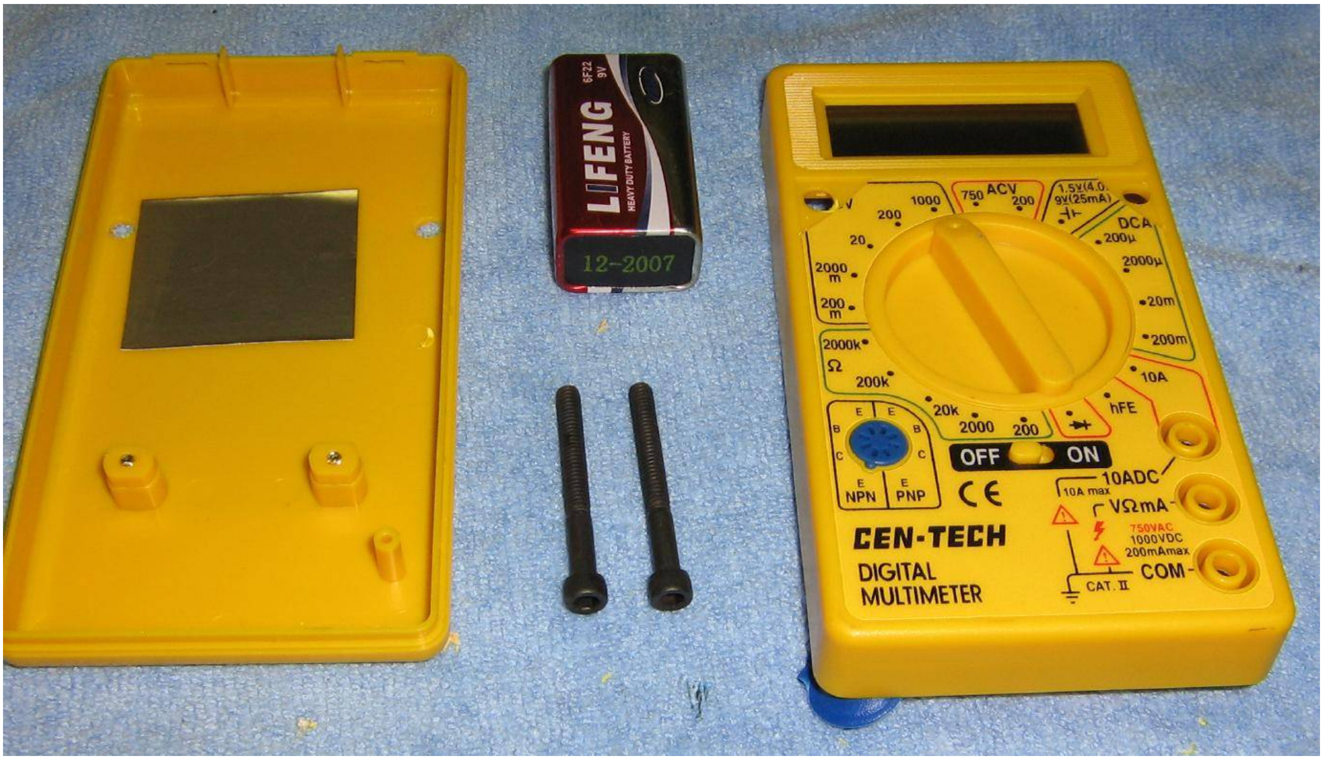


Now a 1 megaohm resistor is placed in *parallel* with the high−voltage output and the meter. It drops even lower to 348 VDC.

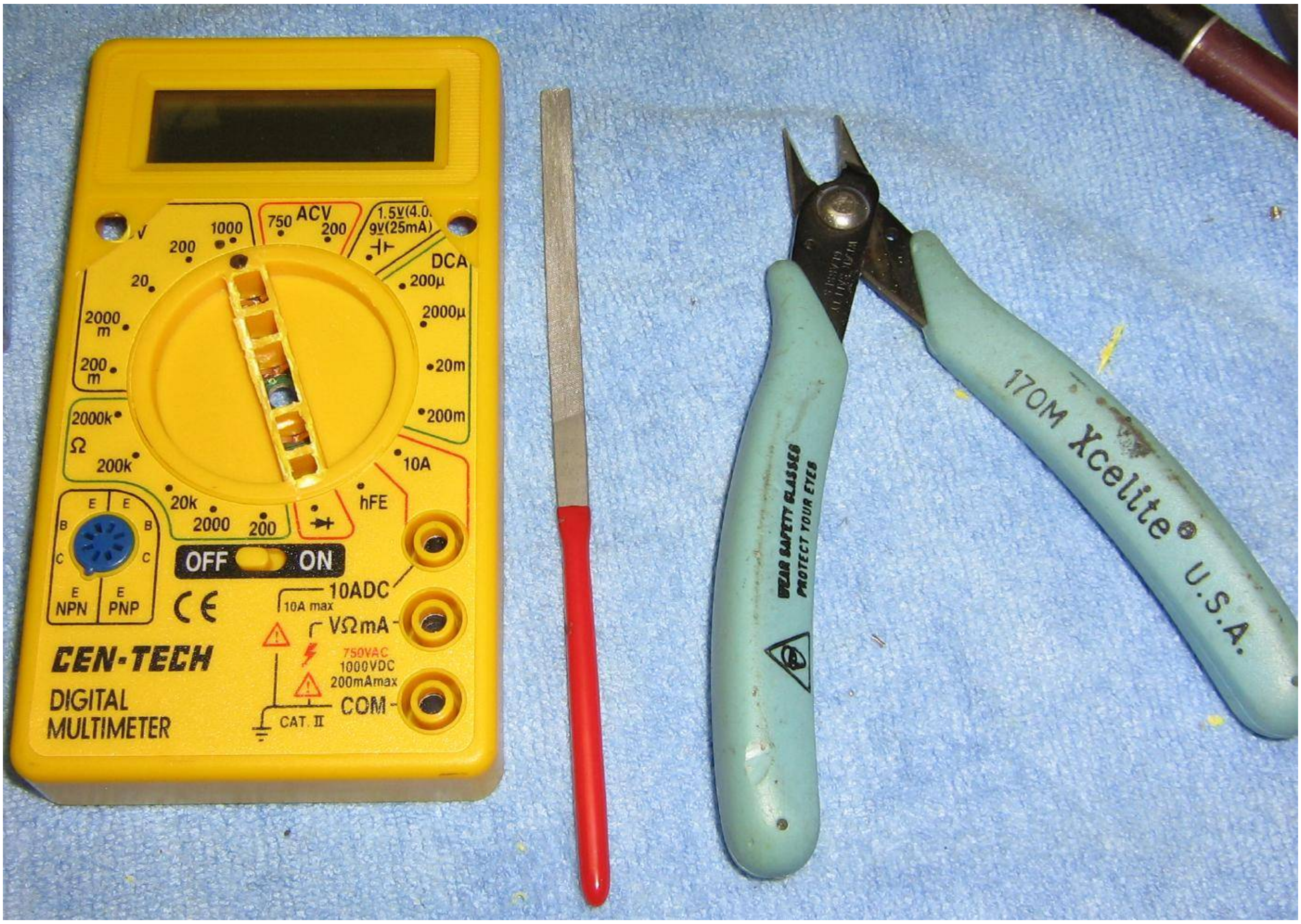
As you can see, even very high−impedance "bugging" devices can be detected with this device. And as a useful bonus, the high−voltage can even destroy them, in some cases.



Project case overview. It's an old ammo box, as usual. The two large rectangular holes are for the meter's display and the large 1.25–inch hole (left side) is for a RJ–11 wallplate. The large cutout on the front is for an outlet box.

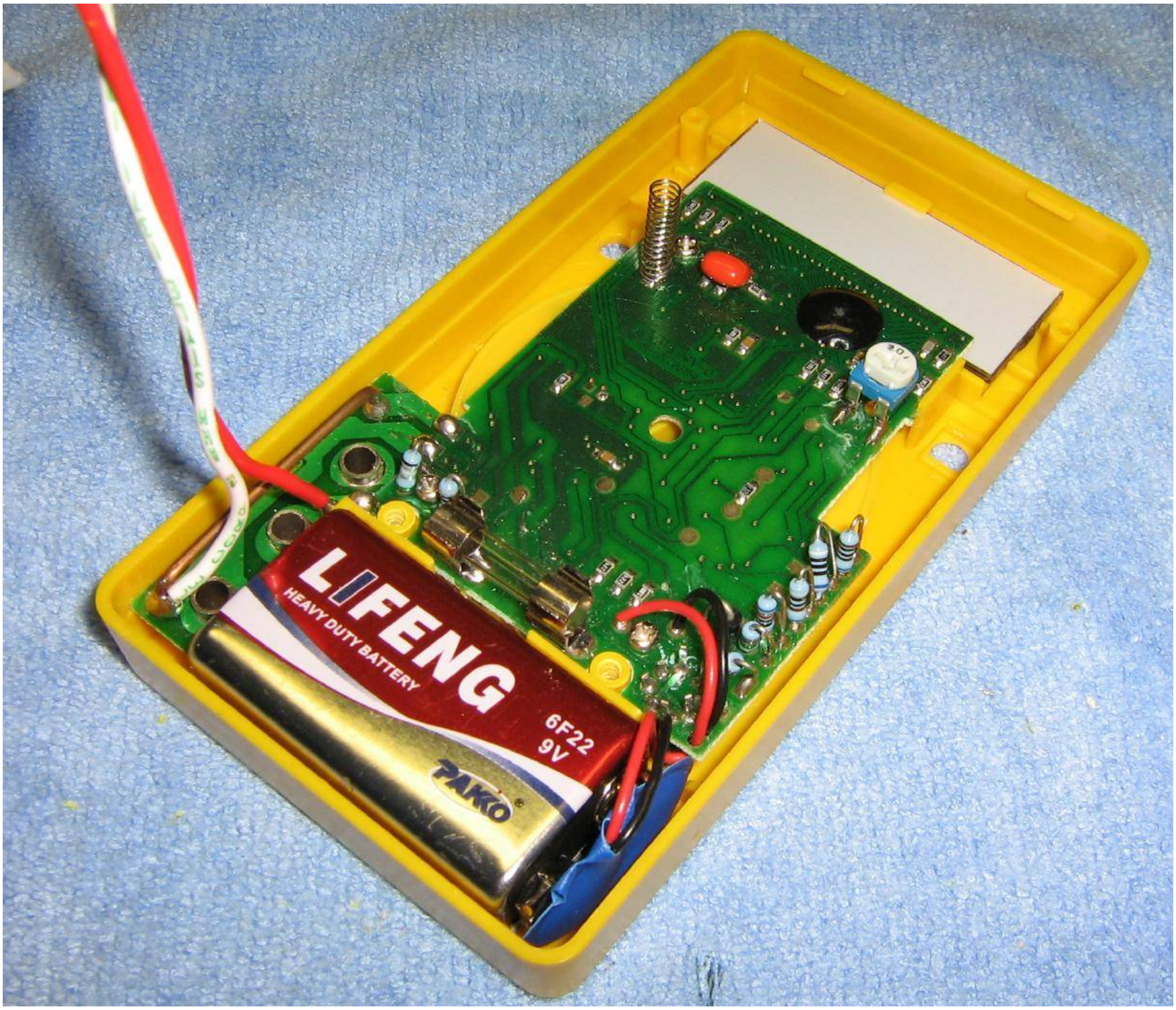


Preparing the digital multimeters. Two 3/16–inch holes are drilled through both plastic covers. They will be mounted to the case using two 1.5–inch long #8 screws and locking hardware. They'll need to be removable to replace the internal 9 volt batteries.

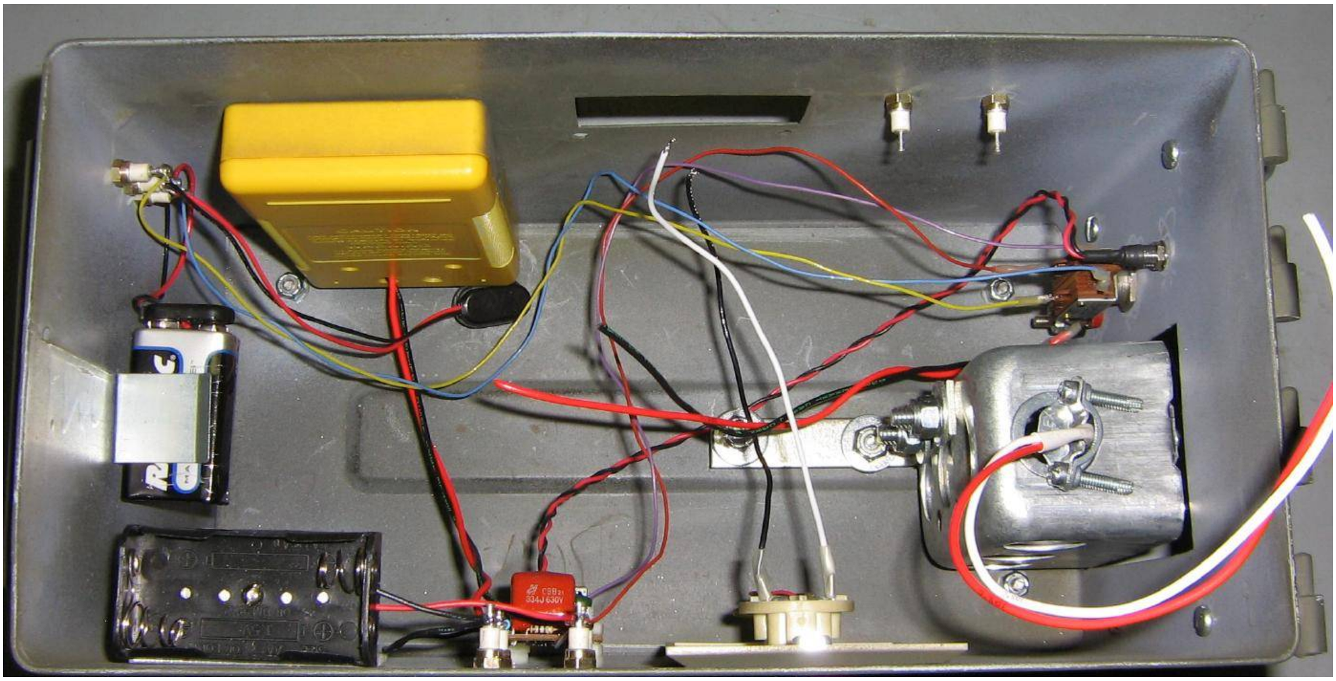


Cut and file down the large plastic selector switch on the meter's front so it can rest along the inside of the project case. Leave the on/off switch as it is.

Be sure to set (and mark) the meters to their proper ranges. The meter reading the current draw should be set to "DCA – 2000µ" and the meter reading voltage should be set to "DCV – 1000".

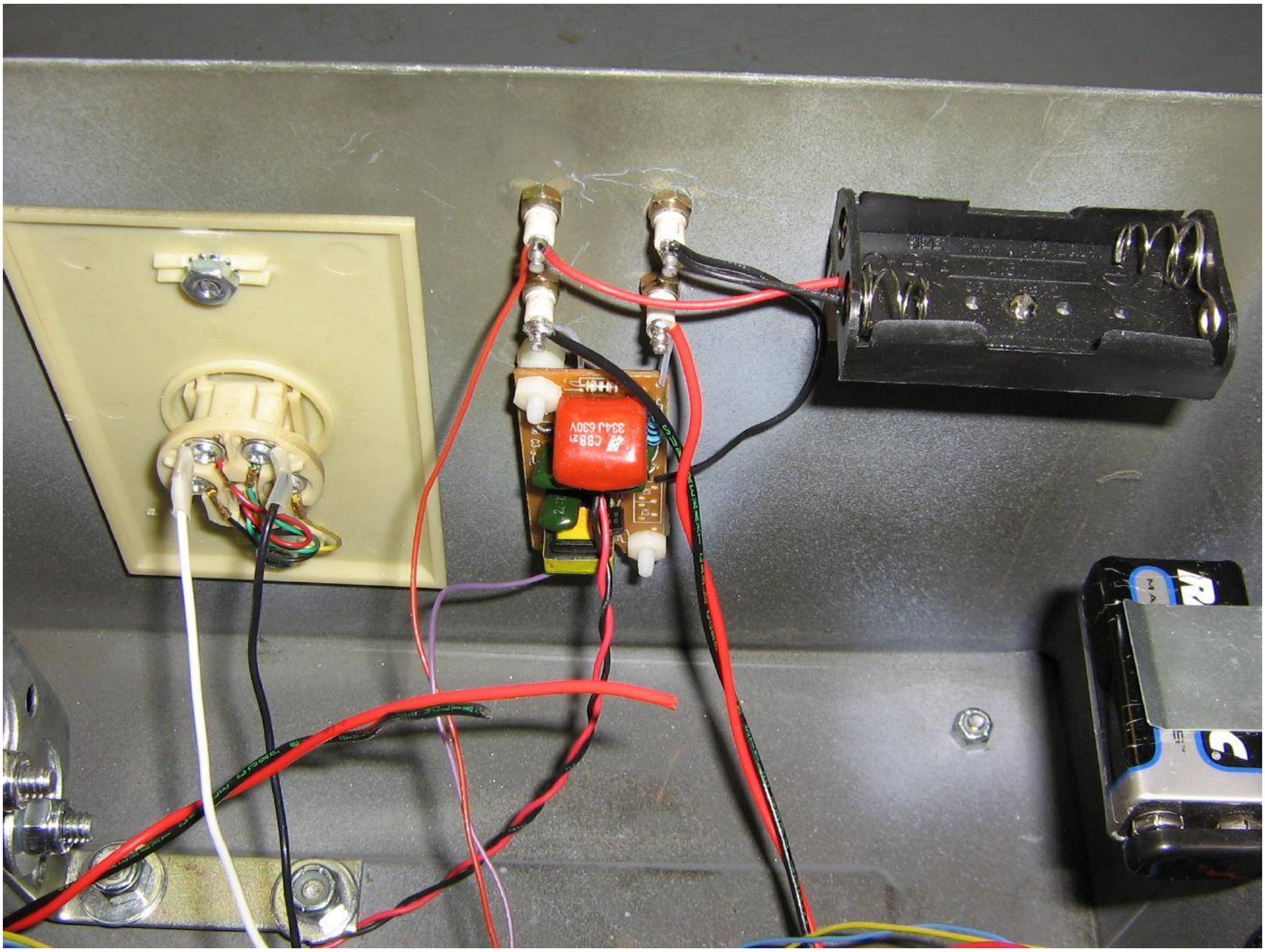


Inside of the meter. Solder two wires to the meter's terminals. Both the meters can be soldered in the same place. Drill a hole on the rear cover to pass the wires through.

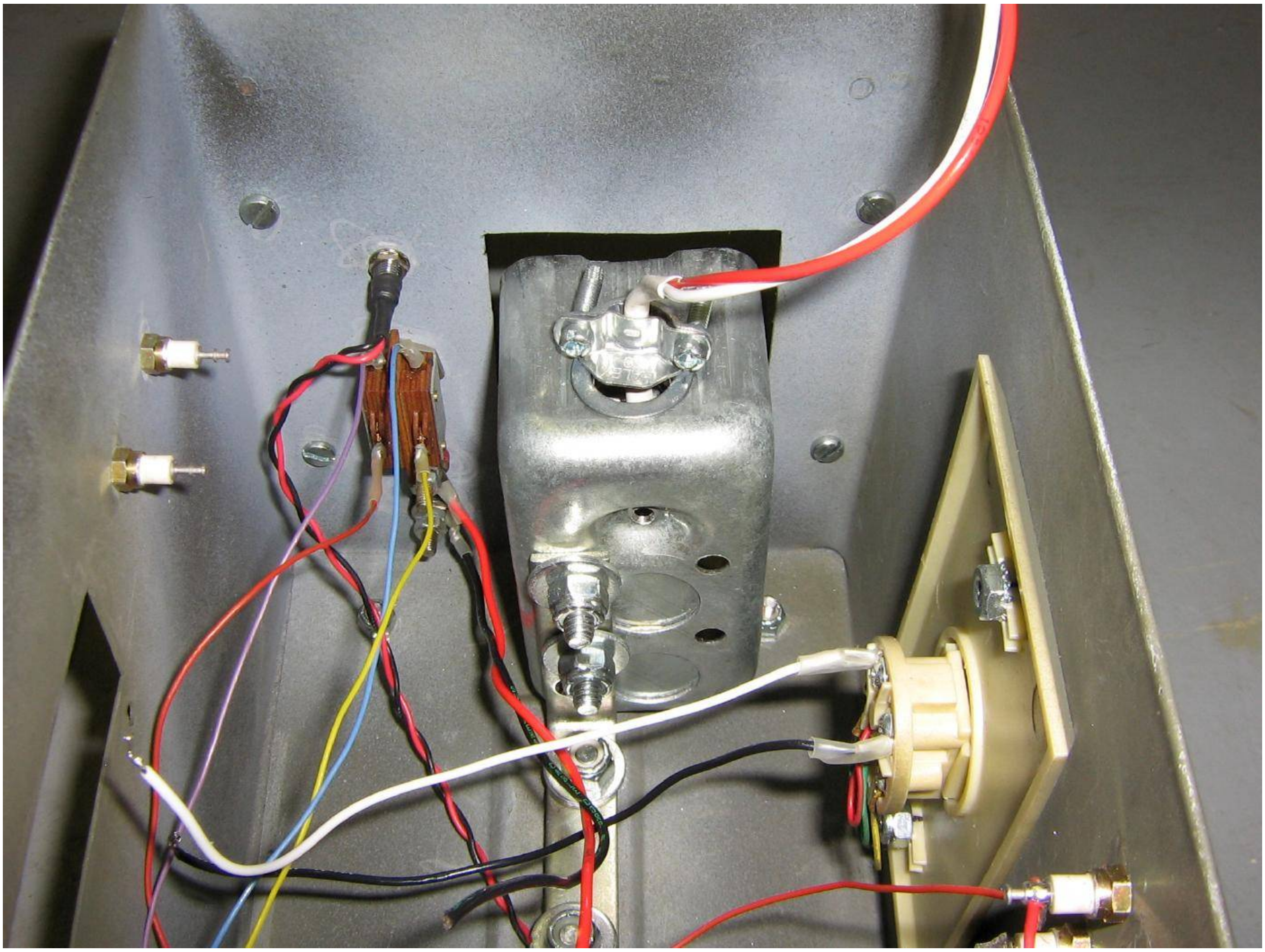


Overview – putting everything together.

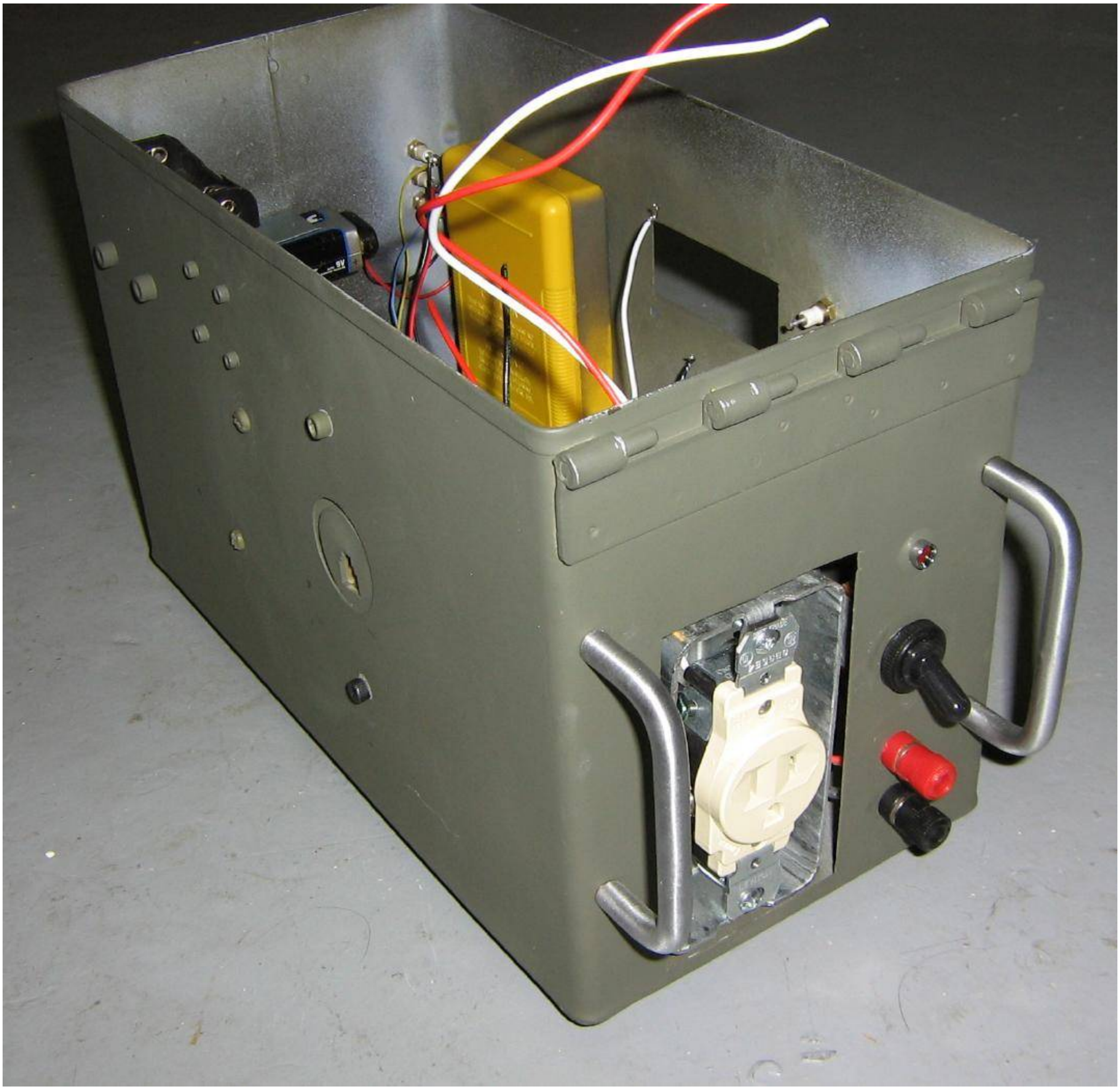
The initial version was going to have the 9 volt batteries externally mounted, but it's not worth it. The plastic battery holder on the lower–left holds two "AA" batteries to power the high–voltage power supply, which is mounted next to it. The high–voltage power supply is mounted to the case using nylon hardware. Its high–voltage output is connected to two isolation terminals. To the right of the high–voltage power supply is a RJ–11 wallplate. This provides a handy RJ–11 jack for testing phone lines. The large silver–colored metal box is a single AC outlet. This is very useful for checking disconnected (pull the fuses) AC power wiring and appliances. Underneath the power switch are two banana jacks. These are for connecting a set of "popper" alligator clips. The two isolation terminals on top are for the final high–voltage output after it passes through the two meters.



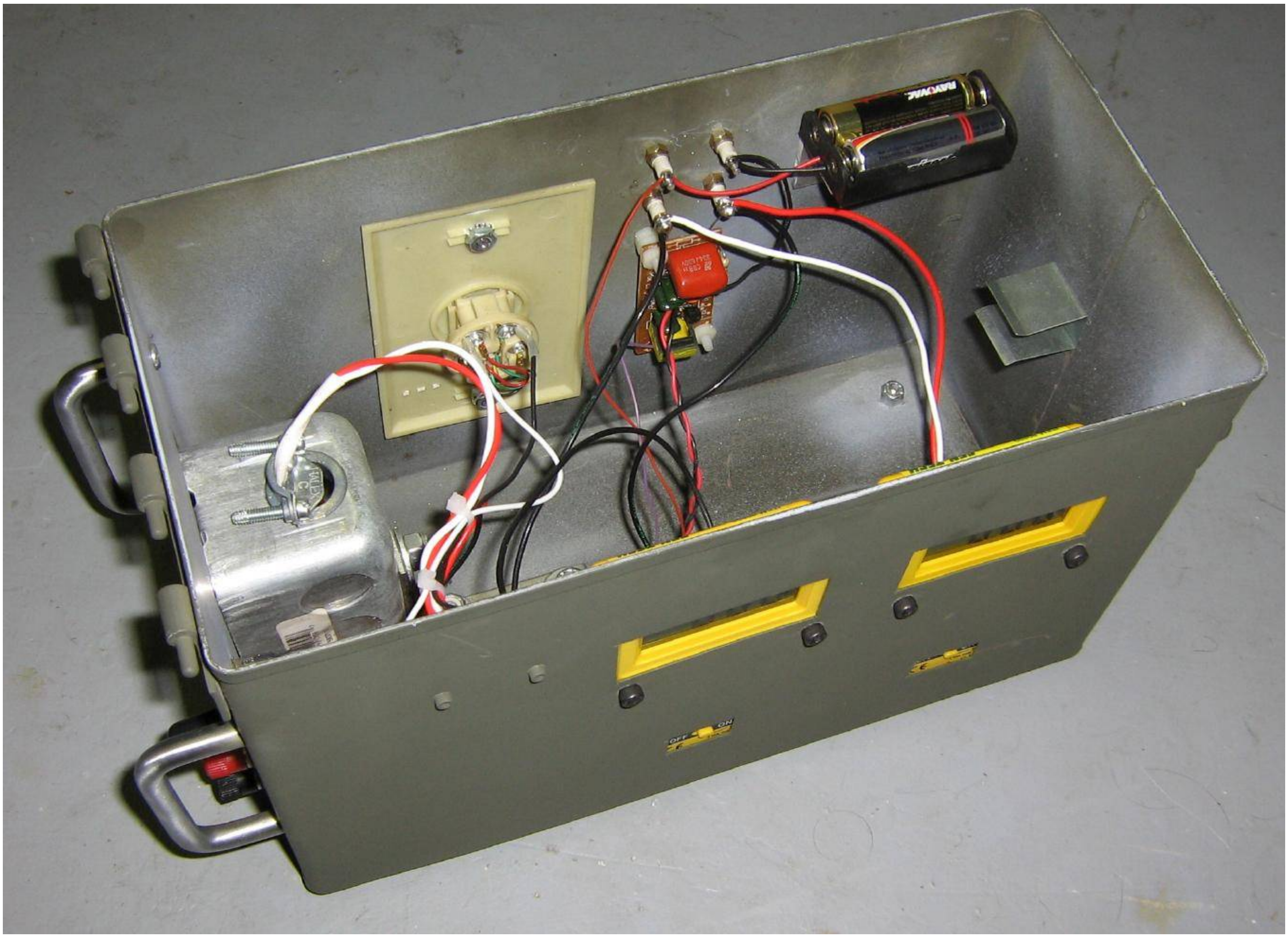
Close up picture of the high−voltage power supply and RJ−11 wallplate mounting. Teflon dielectric wiring is used for all the wires carrying high−voltage. This is optional, but helps to prevent any stray leakage current. The battery holder is mounted on a little L−bracket.



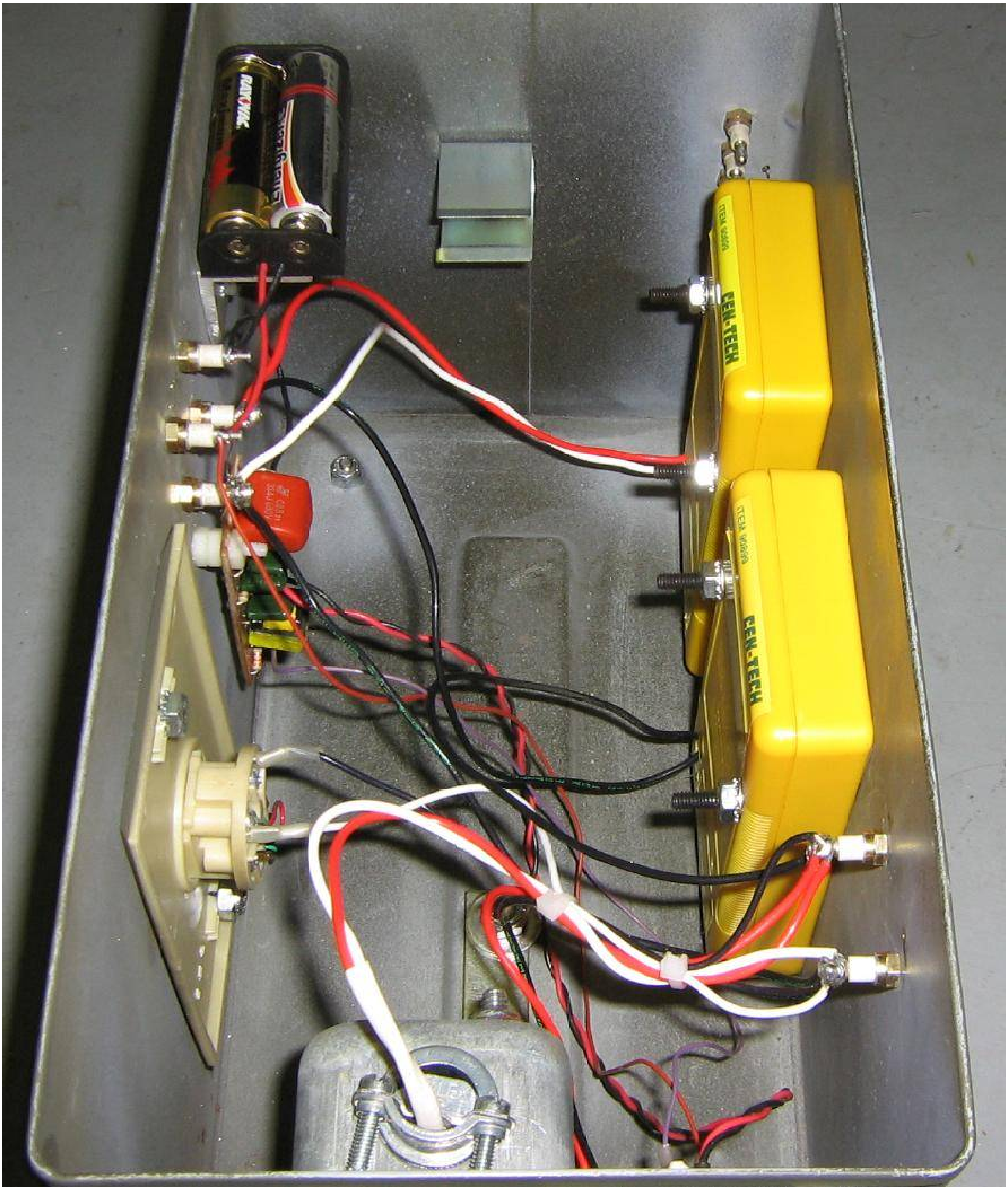
Close up picture behind the front panel.



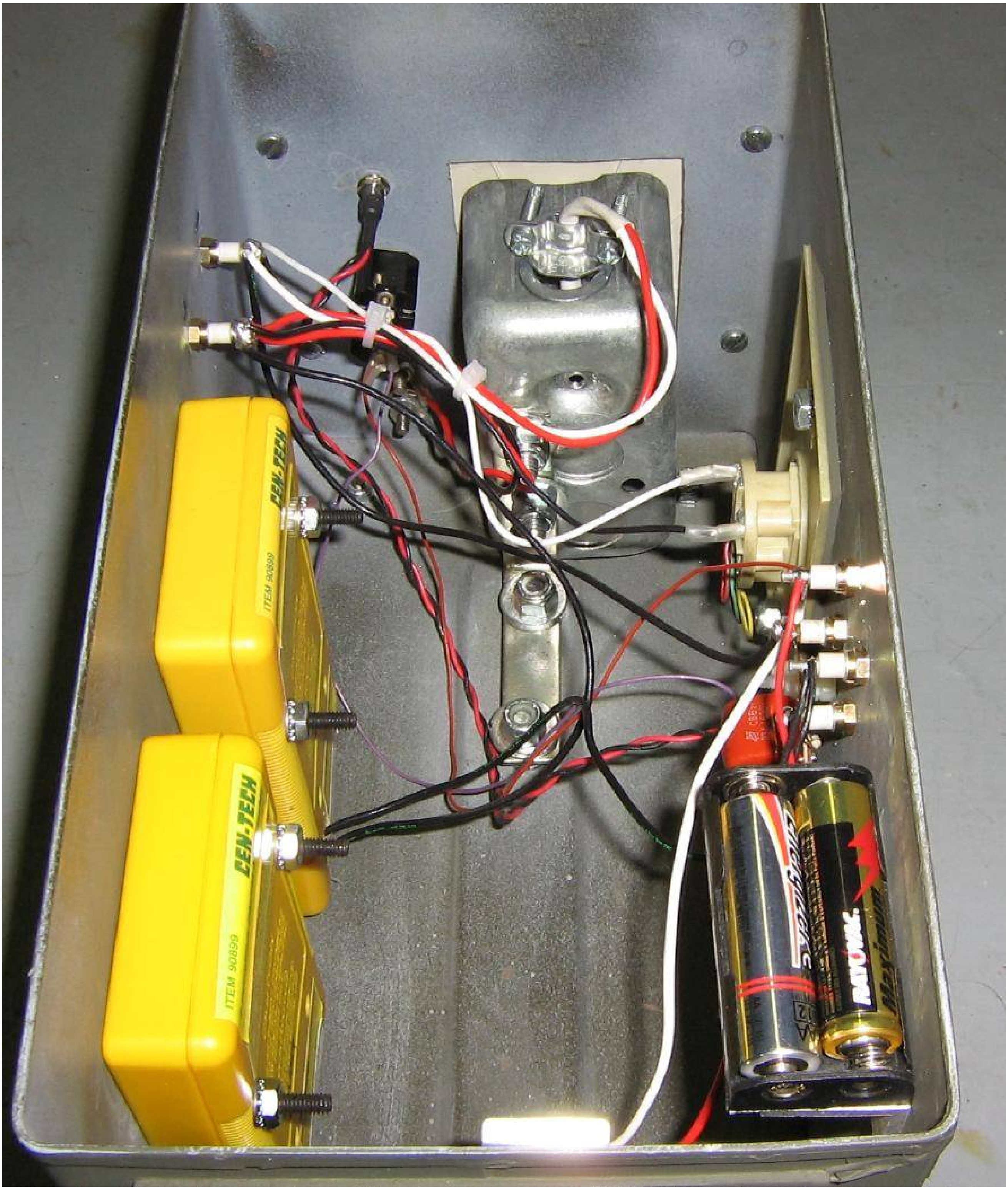
Under construction external view.



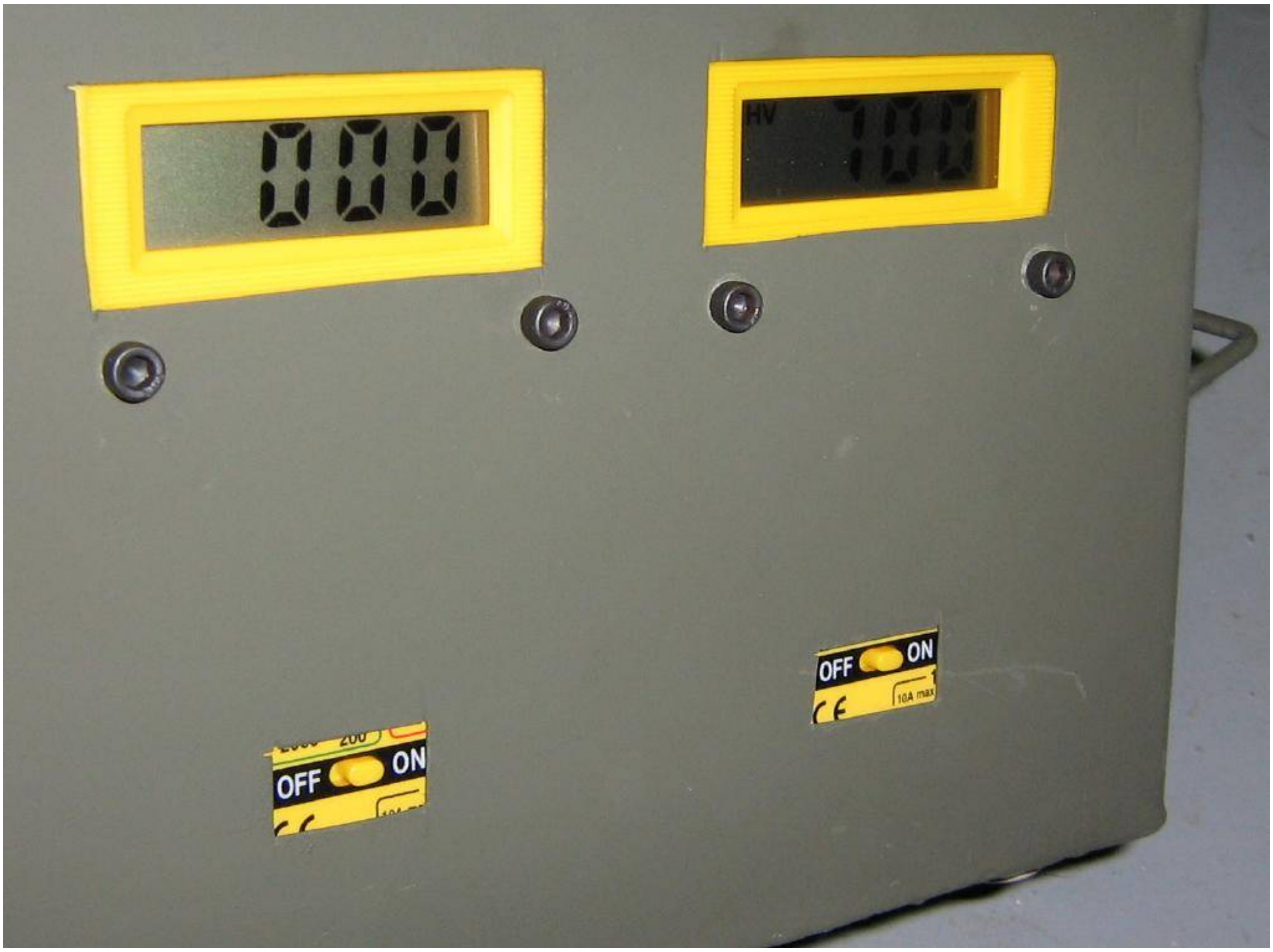
Top view with the meters added. Two small, rectangular holes are cut on the side of the case to access the meter's power switches.



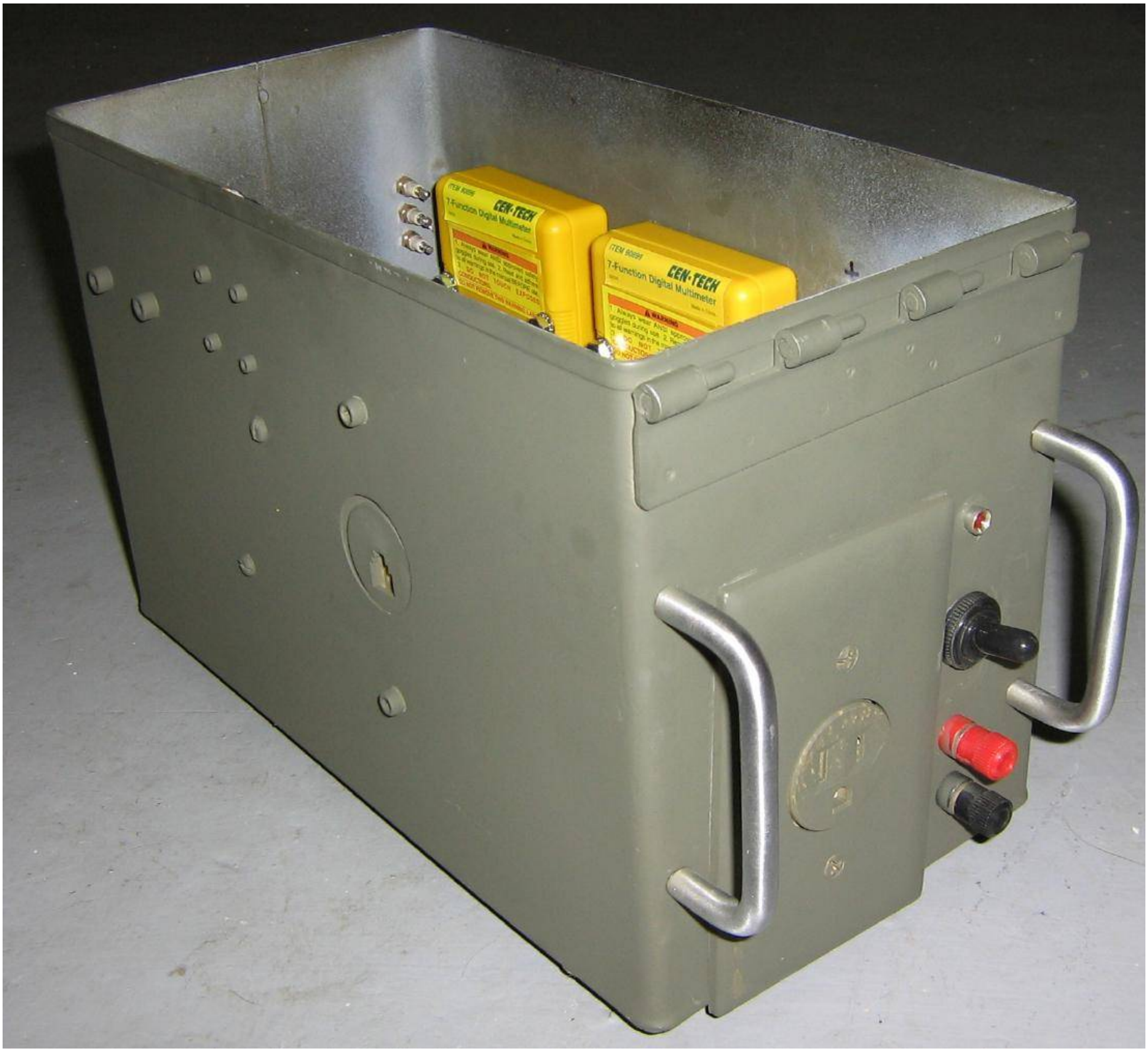
Completed top view.



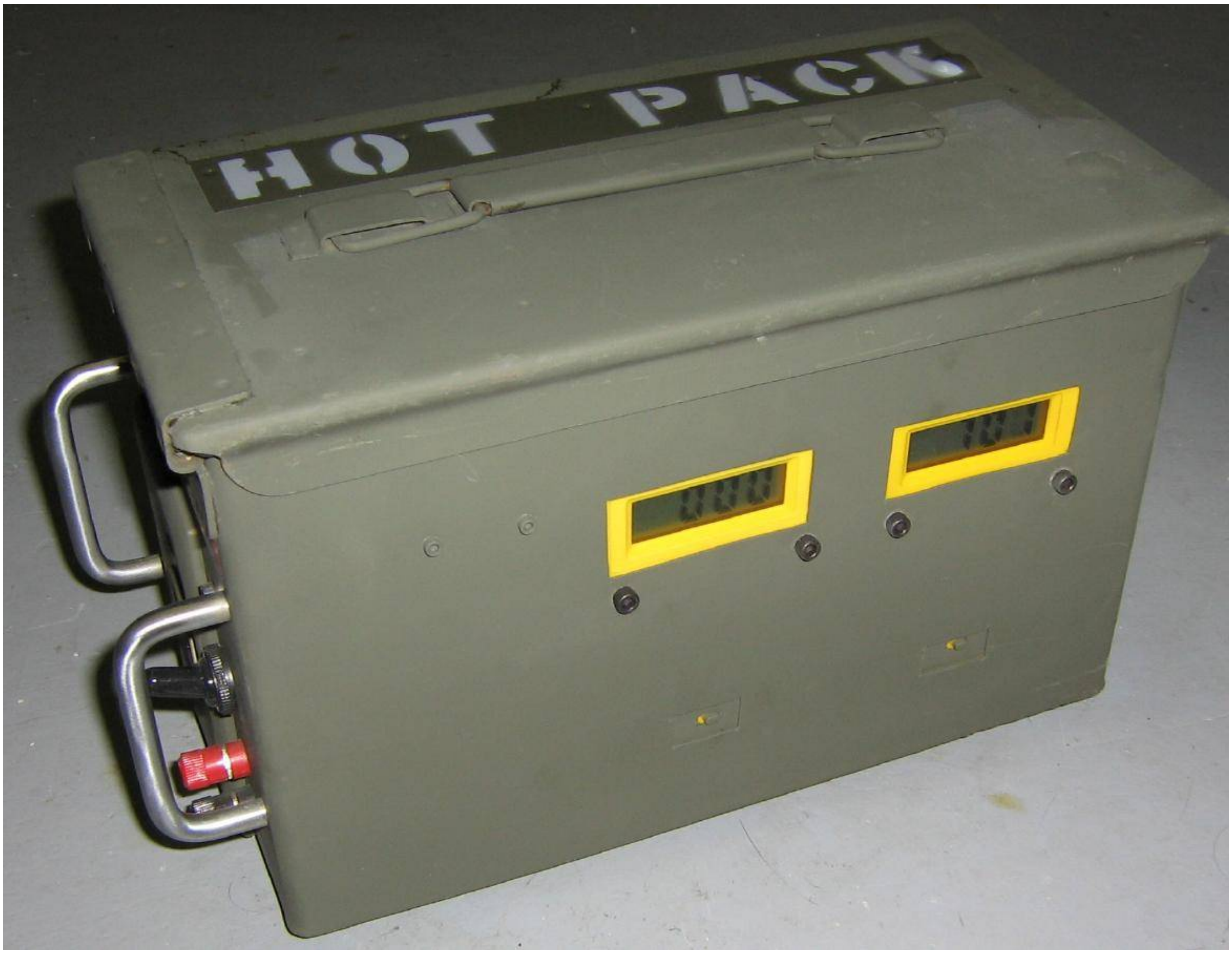
Alternate view.



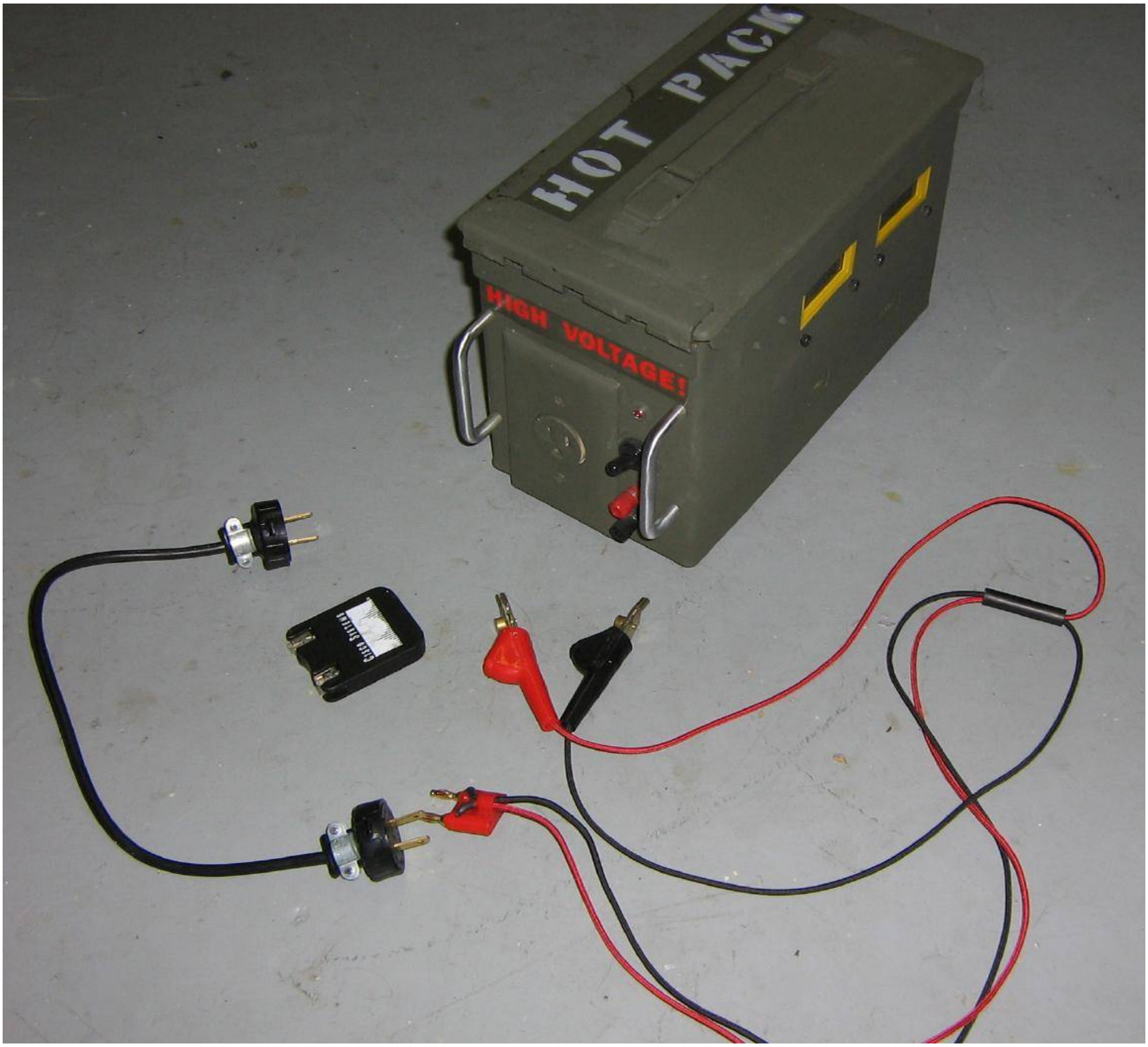
Main power is on. Meter close up picture. The meter on the left is reading the current draw (none) and the meter on the right is reading the high−voltage output (700 volts).



Completed external view. Everything is spray painted "Kill All Eurosavages" green.

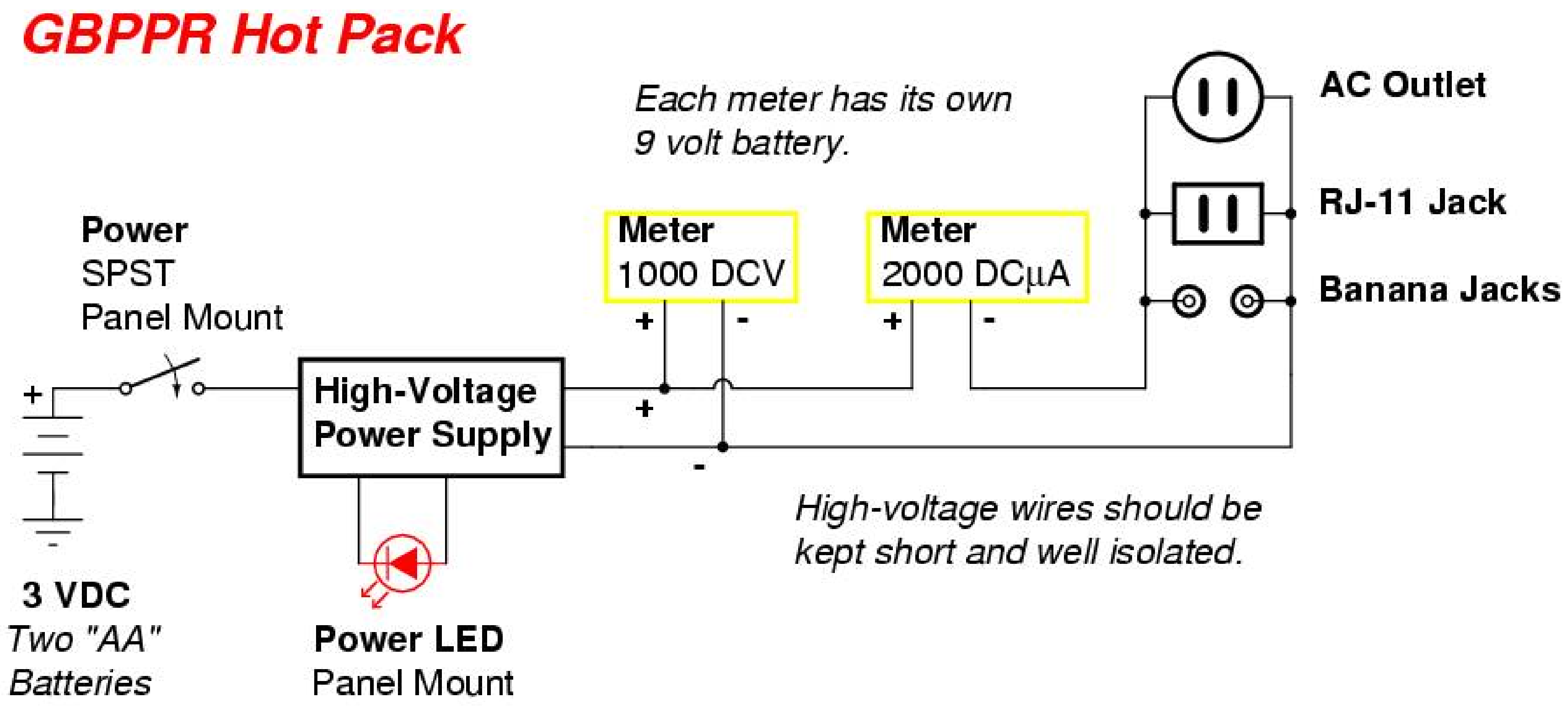


Completed side view.



Accessory overview. A small AC plug−to−plug adapter is shown on the lower−left, the black square thing is a retractable RJ−11 phone extesion, and finally a set of J.S. Popper clips connected to a dual−banana plug.

Schematic / Block Diagram



Each meter has its own 9 volt battery.

High-voltage wires should be kept short and well isolated.

Nortel DMS–100 Trunk–to–Trunk Translations

Description

The system elements whose operation and translations are described below are specific to trunk–to–trunk translations.

Operation

Trunk–to–trunk calls can be traced using a simplified block diagram, representing the major functions within the translation process, as shown below.

```
++++++++++       +++++++++++++       +++++++++++       ++++++++++
+ Trunks + ----> + Screening + ----> + Routing + ----> + Trunks +
++++++++++       +++++++++++++       +++++++++++       ++++++++++
```

The *trunks* tables contain detailed information about trunks originating and terminating in the switch. Each trunk connected to the office is represented by entries in the trunk tables. These tables include information about the following:

- Type of trunk group.
- Type of signaling.
- Hardware location of each trunk.
- Screening information for incoming call from trunks to define the next logical step in translation.

The *screening* tables contain the information used to analyze the digits that the DMS–100 receives. This screening process tests the digits dialed prior to continuing to the next routing stage, to determine, for example, whether this call is local or non–local.

The screening tables establish the call type based on the digits received. The three basic call types are:

- Operator Assisted (OA)
- Direct Dial (DD)
- No Prefix (NP)

The *routing* tables route the calls to their final destination. The information found in these tables dictates how and where a call will be completed, or if the call will route to a recorded announcement or treatment.

The trunk–to–trunk translations process is shown in the flowchart that follows.

Translations Table Flow for Trunk–to–Trunk Translations

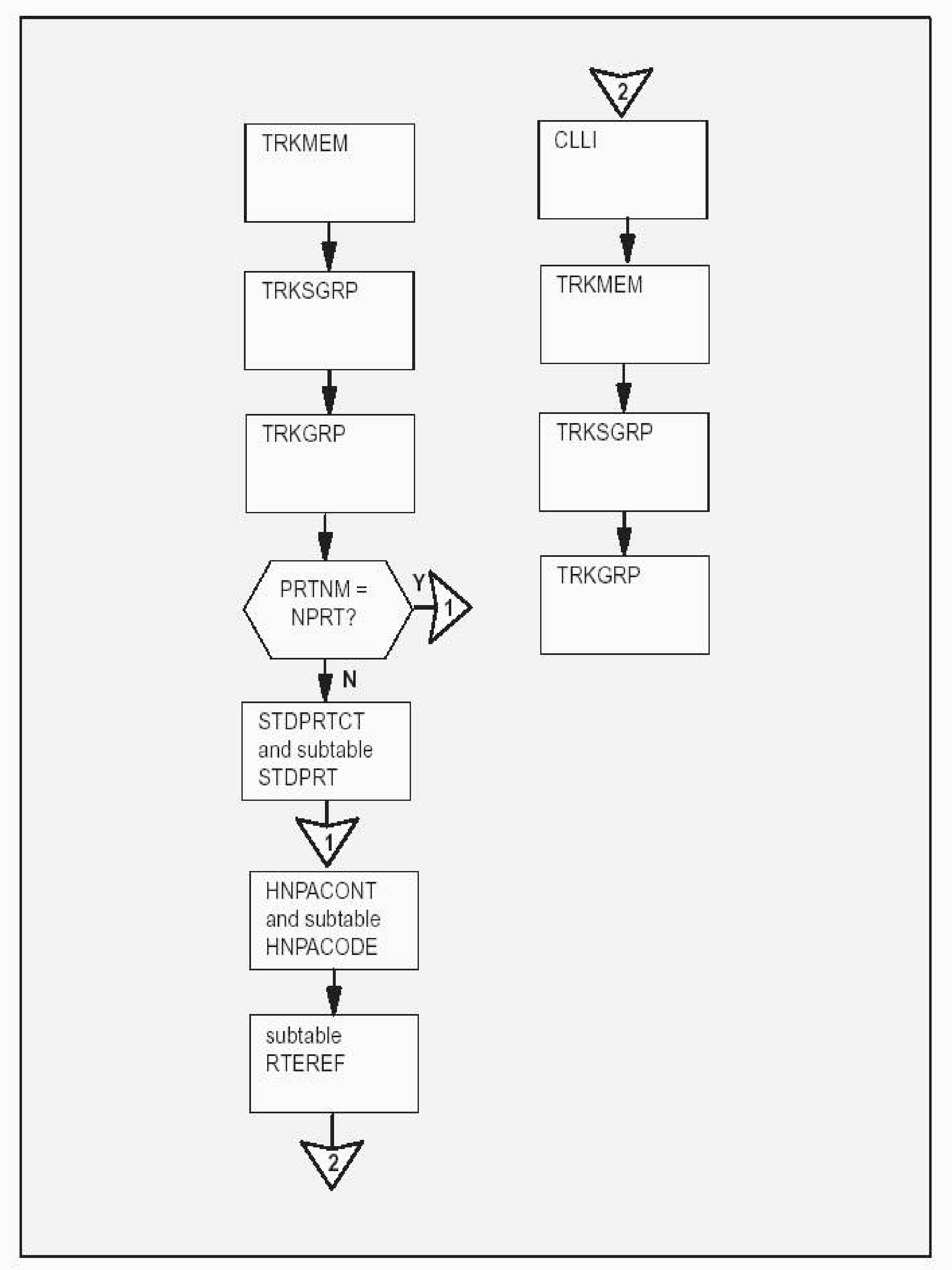
The call originates from a particular hardware location on an incoming trunk member listed in table TRKMEM. Signaling information is obtained from table TRKSGRP.

For an incoming trunk, table TRKGRP lists the Serving Numbering Plan Area (SNPA) in subfield SNPA and the pre–translator subtable name in subfield PRTNM.

If a pre–translator subtable name is specified, translation continues with table STDPRTCT and its subtable STDPRT. If no pre–translator is specified, the entry in subfield PRTNM is NPRT and the call routes to table HNPACONT and its subtable HNPACODE.

At this point, call processing will continue through table HNPACONT and its subtables. The Common Language Location Identifier (CLLI) of the trunk datafilled in subtable HNPACONT.RTEREF is listed in table CLLI. Trunk group type and screening information are provided in table TRKGRP. Table TRKSGRP defines the signaling and control information and table TRKMEM contains the physical location of each trunk member.

<u>Table Flow for Trunk–to–Trunk Translations</u>



The following table lists the datafill content used in the flowchart:

Datafill Example for Trunk-to-Trunk Translations

Datafill Table	**Example Data**
CLLI	F514T13TISIT048 1527 1 SSP5_TACISUP_TRAF_TRUNKS
TRKMEM	F514T13TISIT048 1 0 DTC 13 19 24
TRKSGRP	F514T13TISIT048 0 DS1SIG C7UP 2W N N UNEQ NONE Q764 2W 2W 0 TATSTAC $ TACTIMER CIC
TRKGRP	F514T13TISIT048 IT 0 NPDGP NCIT 2W NIL MIDL 514 NPRT NSCR 514 000 Y N $
HNPACONT	514 98 0 (72) (1) (24) (0)
subtable HNPACODE	819457 819457 FRTE 23
subtable RTEREF	23 (N D S1514819TISIT 3 N N) $
CLLI	S1514819TISIT 239 48 S5_450_TO_S1_819_LAMA
TRKMEM	S1514819TISIT 0 0 DTC 2 10 1
TRKSGRP	S1514819TISIT 0 DS1SIG C7UP 2W N N UNEQ NONE Q764 THRH 0 DMS26 $ NIL CIC
TRKGRP	S1514819TISIT IT 0 NPDGP NCIT 2W IT MIDL 819 P514 NSCR 514 000 N N $

The following table lists the datafill content used in the flowchart. In this example, pre−translator P807 is specified and the call routes through table STDPRTCT and its subtable:

Datafill Example for Trunk−to−Trunk Translations Using a Pre−translator

Datafill Table	**Example Data**
CLLI	S5AAA807IPTLA 346 40 S5AAA_TO_S5807_IC_PTS_LAMA
TRKMEM	S5AAA807IPTLA 0 0 DTC 5 1 1
TRKSGRP	S5AAA807IPTLA 0 DS1SIG STD IC DP WK N 10 10 NO NO N N Y M UNEQ
TRKGRP	S5AAA807IPTLA IT 0 NPDGP NCRT IC DD MIDL 000 P807 NSCR 807 000 N N $
STDPRTCT	P807 (1) (65021)
subtable STDPRT	807 807 N DD 3 NA
HNPACONT	807 201 1 (31) (1) (14) (0)
subtable HNPACODE	514978 514978 FRTE 9
subtable RETEREF	9 (N D S1807819TISIT 0 N N) $
CLLI	S1807819TISIT 238 48 S5_450_TO_S1_819_LAMA
TRKMEM	S1807819TISIT 0 0 DTC 4 2 1
TRKSGRP	S1807819TISIT 0 DS1SIG C7UP 2W N N UNEQ NONE Q764 THRH 0 DMS26 $ NIL CIC
TRKGRP	S1807819TISIT IT 0 NPDGP NCIT 2W IT MIDL 819 P807 NSCR 807 000 N N $

Datafilling Office Parameters

The following table shows the office parameters used by trunk–to–trunk translations. For more information about office parameters, refer to the *DMS–100 Office Parameters Reference Manual*, NTP 297–8021–855:

Office Parameters Used by Trunk-to-Trunk Translations

Table Name	Parameter Name	Explanation and Action
OFCENG	AIN_ACTIVE	This parameter controls the activation of the Advanced Intelligent Network (AIN). Enter "Y" to activate AIN software. Enter "N" to deactivate AIN software. If this parameter is set to "N", parameter AIN_OFFICE_TRIGGRP in table OFCVAR is disregarded.
OFCVAR	AIN_OFFICE_TRIGGRP	This parameter is used to subscribe trigger behaviors on an office-wide basis. The entry in field AINGRP in table TRIGGRP is entered here. The default value is "NIL".

Datafill Sequence

The following table lists the tables that require datafill to implement trunk–to–trunk translations. The tables are listed in the order in which they are to be datafilled:

Datafill Tables Required for Trunk-to-Trunk Translations

Table	Purpose of Table
CLLI	The common language location identifier table lists the name that uniquely identifies each trunk group, tone, or announcement.
TRKGRP	The trunk group table contains customer-defined data associated with each trunk group.
TRKSGRP	The trunk subgroup table specifies supplementary information for each trunk group.
TRKMEM	The trunk member table gives the physical location of each trunk assigned to one of the trunk groups.
OFRT	The office route table lists up to eight alternate routes in order of preference. This table lists tones or announcements for calls requiring treatment.
HNPACONT	The home numbering plan area control table lists all the home or serving area NPAs for a particular area.
subtable HNPACODE	The home numbering plan area code subtable lists the route treatment or table to which the translation routes for each of the assigned NPAs.
STDPRTCT	The standard pre-translator table lists the names of the standard pre-translator subtables.
subtable STDPRT	The standard pre-translator subtable determines the next stage of translation, based on the range of leading digits.

Datafilling Table CLLI

Table CLLI must contain a tuple for the originating and terminating office.

The following table shows the datafill specific to trunk–to–trunk translations for table CLLI. Only those fields that apply directly to trunk–to–trunk translations are shown:

Datafilling Table CLLI

Field	Subfield or Refinement	Entry	Explanation and Action
CLLI		Alphanumeric (1 to 16 characters)	*Common Language Location Identifier* Enter a CLLI code to uniquely identify the far–end of each ann., tone, or trunk group

The following example MAP display shows sample datafill for table CLLI:

CLLI	ADNUM	TRKGRSIZ	ADMININF
F514T13TISIT048	1527	1	SSP5_TACISUP_TRAF_TRUNKS
S1514819TISIT	239	48	S5_450_TO_S1_819_LAMA

Datafilling Table TRKGRP

Table TRKGRP must contain a tuple for the originating and terminating office.

The following table shows the datafill specific to trunk–to–trunk translations for table TRKGRP. Only those fields that apply directly to trunk–to–trunk translations are shown:

Datafilling Table TRKGRP

Field	Subfield or Refinement	Entry	Explanation and Action
GRPKEY		See subfield	*Group Key* This field consists of subfield CLLI.
	CLLI	Alphanumeric (1 to 16 characters)	*Common Language Location Identifier* Enter the CLLI code assigned to the trunk group in table CLLI.

The following example MAP display shows sample datafill for table TRKGRP:

GRPKEY	GRPINFO
F514T13TISIT048	IT 0 NPDGP NCIT 2W NIL MIDL 514 NPRT NSCR 514 000 Y N $
S1514819TISIT	IT 0 NPDGP NCIT 2W IT MIDL 819 P514 NSCR 514 000 N N $

Datafilling Table TRKSGRP

Table TRKSGRP must contain a tuple for the originating and terminating office.

The following table shows the datafill specific to trunk–to–trunk translations for table TRKSGRP. Only those fields that apply directly to trunk–to–trunk translations are shown:

Datafilling Table TRKSGRP

Field	Subfield or Refinement	Entry	Explanation and Action
SGRPKEY		See subfields	*Subgroup Key* This field consists of subfields CLLI and SGRP.
	CLLI	Alphanumeric (1 to 16 characters)	*Common Language Location Identifier* Enter the code that is assigned in table CLLI to the trunk group to which the subgroup belongs.
	SGRP	0 or 1	*Subgroup Number* Enter the number assigned to the trunk subgroup.

The following example MAP display shows sample datafill for table TRKSGRP:

```
SGRPKEY             CARDCODE   SGRPVAR
_____________________________________________________________________________
F514T13TISIT048 0   DS1SIG     C7UP 2W N N UNEQ NONE Q764 2W 2W 0 TATSTAC $ TACTIMER CIC

S1514819TISIT 0     DS1SIG     C7UP 2W N N UNEQ NONE Q764 THRH 0 DMS26 $ NIL CIC
```

Datafilling Table TRKMEM

Table TRKMEM must contain a tuple for the originating and terminating office.

The following table shows the datafill specific to trunk–to–trunk translations for table TRKMEM. Only those fields that apply directly to trunk–to–trunk translations are shown:

Datafilling Table TRKMEM

Field	Subfield or Refinement	Entry	Explanation and Action
CLLI		Alphanumeric (1 to 16 characters)	*Common Language Location Identifier* Enter the CLLI code that is assigned to the trunk group of which the trunk is a member. This CLLI code is assigned in table CLLI.

EXTRKNM		0 to 9,999	*External Trunk Number* Enter the external trunk number that is assigned to the trunk. For members of trunk groups using the AIOD option, the external trunk number must be unique over all trunks and lines using the same AIOD group.
MEMVAR		See subfield	*Variable Data for Members* This field consists of subfield PMTYPE and refinements.
	PMTYPE	DTC	*Peripheral Module Type* Enter the Peripheral Module (PM) type on which the trunk is mounted and datafill the refinements associated with this entry value. Enter DTC for a digital trunk controller and complete subfields DTCNO, DTCCKTNO, and DTCCKTTS.
	DTCNO	0 to 511	*Digital Trunk Controller Number* Enter the number of the DTC to which the trunk group member is assigned.
	DTCCKTNO	0 to 19	*Digital Trunk Controller Circuit Number* Enter the number of the DTC circuit card to which the trunk group member is assigned.
	DTCCKTTS	1 to 24	*Digital Trunk Controller Circuit Time-Slot* Enter the number of the circuit card DS-1 time-slot to which the trunk group member is assigned.

The following example MAP display shows sample datafill for table TRKMEM:

CLLI	EXTRKNM	SGRP	MEMVAR
F514T13TISIT048	1	0	DTC 13 19 24
S1514819TISIT	0	0	DTC 2 10 1

Datafilling Table STDPRTCT

The following table shows the datafill specific to trunk–to–trunk translations for table STDPRTCT. Only those fields that apply directly to trunk–to–trunk translations are shown:

Datafilling Table STDPRTCT

Field	Subfield or Refinement	Entry	Explanation and Action
EXPRTNM		Alphanumeric (up to 8 characters)	*External Standard Pre-Translator Name* Enter the key defined by the operating company to represent the standard pre-translator subtable.

STDPRT		See note	*Standard Pre-Translator* The field is an index into subtable STDPRT. **Note:** This field does not accept any input.

The following example MAP display shows sample datafill for table STDPRTCT:

```
EXPRTNM    STDPRT    AMAPRT
___________________________
P807       (   1)    (65021)
```

Datafilling Subtable STDPRTCT.STDPRT

The following table shows the datafill specific to trunk–to–trunk translations for subtable STDPRTCT.STDPRT. Only those fields that apply directly to trunk–to–trunk translations are shown:

Datafilling Subtable STDPRTCT.STDPRT

Field	Subfield or Refinement	Entry	Explanation and Action
FROMDIGS		Numeric (up to 18 digits)	*From Digits* Enter the digit or digits to be translated. If the entry represents a block of consecutive numbers, enter the first number in the block.
TODIGS		Numeric (up to 18 digits)	*To Digits* If field FROMDIGS represents a block of consecutive numbers, enter the last number in the block.
PRETRTE		See subfield	*Pre-Translation Route* This field consists of subfield PRERTSEL and its refinements, TYPECALL, NOPREDIG, TRANSYS, and POS.
	PRERTSEL	N	*Pre-Translator Route Selector* Enter "N".
	TYPCALL	DD, OA, NP, or NL	*Type of Call* Enter the type of call: DD (Direct Dial), NP (No Prefix), OA (Operator Assisted), or NL (Nil). For Traffic Operator Position System (TOPS) calls, there can be a mixture of 0 and 1 (OA and DD) call types. Enter "NL" for these cases.
	NOPREDIG	0 to 7	*Number of Prefix Digits* Enter the number of digits that are to be interpreted as prefix digits.

	TRANSYS	IN, IP, or NA	*Translation System* Enter "IN" if the translation routes to international translations (on a local and toll combined switching unit only). Enter "IP" if the translation routes to international partitioned translations (DMS–250 only). Enter "NA" if the translation routes to national translations.

The following example MAP display shows sample datafill for subtable STDPRTCT.STDPRT:

FROMDIGS	TODIGS	PRETRTE
807	807	N DD 3 NA

Datafilling Table HNPACONT

The following table shows the datafill specific to trunk–to–trunk translations for table HNPACONT. Only those fields that apply directly to trunk–to–trunk translations are shown:

Datafilling Table HNPACONT

Field	Subfield or Refinement	Entry	Explanation and Action
STS		0 to 9,999,999	*Serving Translation Scheme* Enter a SNPA or STS code.
HNPACODE		See note	*Home Numbering Plan Area Code* This field is an index into subtable HNPACODE. **Note:** This field does not accept any input.

The following example MAP display shows sample datafill for table HNPACONT:

STS	NORTREFS	NOAMBIGC	RTEREF	HNPACODE	ATTRIB	RTEMAP
514	98	0	(72)	(1)	(24)	(0)
807	201	1	(31)	(1)	(14)	(0)

Datafilling Subtable HNPACONT.HNPACODE

The following table shows the datafill specific to trunk–to–trunk translations for subtable HNPACONT.HNPACODE. Only those fields that apply directly to trunk–to–trunk translations are shown:

Datafilling Subtable HNPACONT.HNPACODE

Field	Subfield or Refinement	Entry	Explanation and Action
FROMDIGS		Numeric (3 digits)	*From Digits* Enter the number representing a single code or the first in a block of consecutive codes that have the same input data.
TODIGS		Numeric (3 digits)	*To Digits* If field FROMDIGS represents a single code, enter the same single code as in field FROMDIGS. If field FROMDIGS represents the first number of a block of consecutive numbers, enter the last number in the block.
CDRRTMT		See subfield	*Code Type, Route Reference, or Treatment* This field consists of subfield CD.
	CD	DN	*Code Type* Enter DN for terminating office code and datafill refinements SNPA and NXX.
	SNPA	Numeric (3 digits)	*Terminating Serving Numbering Plan Area* Enter the SNPA of the called terminating line DN. If the operating company uses screening to intraswitch SNPAs, translation of the dialed digits proceeds to table TOFCNAME, using SNPA and NXX as the key.
	NXX	Numeric (3 digits)	*Terminating NXX* Enter three digits for the NXX code of the called terminating line DN.

The following example MAP display shows sample datafill for subtable HNPACONT.HNPACODE:

FROMDIGS	**TODIGS**	**CDRRTMT**
819457	**819457**	**FRTE 23**
514978	**514978**	**FRTE 9**

Datafilling Subtable HNPACONT.RTEREF

The following subtable shows the datafill specific to trunk–to–trunk translations for subtable HNPACONT.RTEREF. Only those fields that apply directly to trunk–to–trunk translations are shown:

Datafilling Subtable HNPACONT.RTEREF

Field	Subfield or Refinement	Entry	Explanation and Action
RTE		1 to 1,023 or blank	*Route Reference Index* Enter the route reference number assigned to the route list.
RTELIST		See subfield	*Route List* This field consists of a vector of up to nine multiples of subfield RTESEL and refinements CONNTYPE, CLLI, DELDIGS, PRFXDIGS, and CANCNORC. Enter "$" to signify the end of the vector.
	RTESEL	N	*Route Selector* Enter "N" if the outgoing or two-way trunk group is intertoll. Enter "T" if translation routes to table OFRT.
	CLLI	Alphanumeric (1 to 16 characters)	*Common Language Location Identifier* Enter the code in table CLLI to which translation is routed.

The following example MAP display shows sample datafill for subtable HNPACONT.RTEREF:

```
RTE   RTELIST
_____________________________________
23     (N D S1514819TISIT 3 N N)  $

9      (N D S1807819TISIT 0 N N)  $
```

Translation Verification Tools

The following example shows the output from TRAVER when it is used to verify trunk−to−trunk translations.

```
>TRAVER tr S5AAA807IISLA 8194573075 b
TABLE TRKGRP
S5AAA807IISLA IT 0 NPDGP NCRT IC DD MIDL 000 P807 NSCR 807 000 N N $
TABLE OFCVAR
AIN_OFFICE_TRIGGRP NIL
TABLE STDPRTCT
P807 ( 1) (65021) 0
 . SUBTABLE STDPRT
WARNING: CHANGES IN TABLE STDPRT MAY ALTER OFFICE
BILLING. CALL TYPE DEFAULT IS NP. PLEASE REFER TO
DOCUMENTATION.
 . 807 807 N DD 3 NA
 . SUBTABLE AMAPRT
 . KEY NOT FOUND
 . DEFAULT VALUE IS: NONE OVRNONE N
TABLE HNPACONT
807 201 1 ( 31) ( 1) ( 14) ( 0) 0
 . SUBTABLE HNPACODE
 . 514978 514978 FRTE 9
AIN Info Collected TDP: no subscribed trigger.
AIN Info Analyzed TDP: no subscribed trigger.
 . SUBTABLE RTEREF
 . 9 (N D S1807819TISIT 0 N N)
 . EXIT TABLE RTEREF
EXIT TABLE HNPACONT

+++ TRAVER: SUCCESSFUL CALL TRACE +++

DIGIT TRANSLATION ROUTES

1 S1807819TISIT 8194573075 ST

TREATMENT ROUTES. TREATMENT IS: GNCT
1 120T0

+++ TRAVER: SUCCESSFUL CALL TRACE +++
```

Introduction to Trunk Tables

Understanding Trunks Translations

Digital Multiplex System (DMS) translations is based on the following information:

- The digits received by the switch.
- Which trunk is the incoming trunk.
- Signaling information received from the incoming trunk.

The translation process involves reading specific tuples in designated data tables to determine the path that a call takes to its destination, as well as the termination point of a call.

The number and sequence of tables accessed by a given call varies according to several factors: for example, the origin and destination of the call, the number of digits dialed, and the signaling system used on the incoming trunk group.

Translation on a call is complete when the call has been screened and sent to treatment, or when it is ready for transmission. The route that the call takes depends on the route list.

The data tables required to complete the translation process are classified as follows:

- Information Tables
- Analysis, Conversion, and Routing Tables
- Trunk Tables

Information tables provide all the trunk names, pretranslator codes, screening class codes, and other names and codes that are used by the analysis, conversion, and routing tables, and the trunk tables.

Analysis, conversion, and routing tables are the tables that perform the functions required for processing and routing calls. These functions include the translation of incoming digits, call screening, and the selection of outgoing trunk group routes or call treatments. Analysis, conversion, and routing tables reference data in the information and trunk tables.

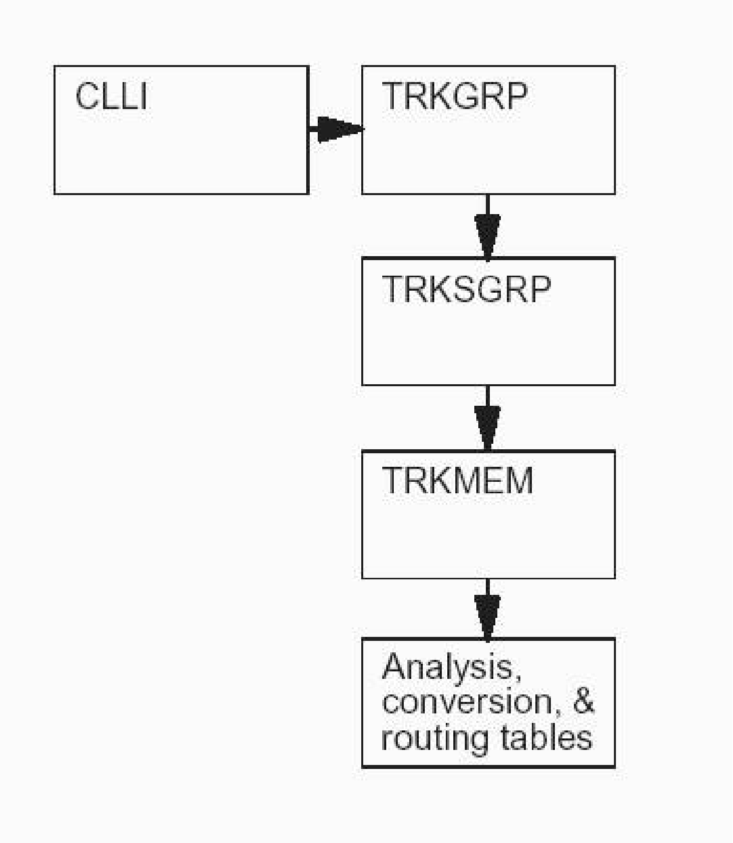
Trunk tables provide information concerning both originating and terminating trunk groups and trunk subgroups. The type of information includes the following:

- The type of trunk group (for example, intertoll, Super CAMA, and operator).
- The direction of traffic flow on the trunk group (incoming, outgoing, or two−way).
- The type of signaling handled by the trunk group (for example, multifrequency or dial−pulse).
- The mapping of individual trunk group members to physical circuits in the switch.

The trunk tables use key fields to direct calls on incoming trunks to applicable translations steps. For each call, information in the trunk tables indexes one of the translation tables to begin analysis, conversion, and routing. Each translation table, in turn, indexes another table until the call is fully translated and can be routed.

The trunk tables translations process is shown in the following flowchart. To build trunks in translations, the following tables must be datafilled in order: CLLI, TRKGRP, TRKSGRP, and TRKMEM. Additional tables may require datafill dependent on the trunk group type.

Translations Table flow for Trunk Tables



Nortel DMS−100 Office Security

General

In today's environment, with the challenge of illegal access to computer systems, the security of our telephone network should be one of the highest priorities within any communications company. There is a need to safeguard telephone service to the customer, Automatic Message Accounting (AMA) billing records, credit card numbers, communications equipment, and databases by restricting access only to authorized personnel. These safeguards require constant monitoring and 24 hour year−round commitment.

Some safeguards have been described in previous areas of this manual. Those safeguards dealt with office images, maintaining office logs for AMA tapes and dial−up access, and retaining hard copies of translation tables, office parameters, and Store File Device (SFDEV) files. In addition to those safeguards, this subsection describes security features and safeguards for:

- Human−Machine Access
- Input Command Screening
- Audit Trail
- Dial−Up Access Ports

All dial−up access ports should be arranged for customer controlled access. This control may consist of manual answer on the data set, call transfer to a restricted Centrex group, access through a central minicomputer system, or a dial−back feature. All dial−up accesses should be logged. Periodic checks should be made to ensure that all dial−up access is being controlled by responsible personnel, whether it is through a control center or within the switch.

LOGINCONTROL Command

It is recommended that the Command Interpreter (CI) level `LOGINCONTROL` feature be used to provide security for the use of dial−up ports into the switch. This feature allows the automatic disabling of a port after disconnect by a user, as well as limiting the time and number of attempts at logging into an enabled port.

This can be a valuable enhancement to switch security and reduces the possibility of ports being left in an accessible state. We suggest `LOGINCONTROL` responsibility be under control of a security supervisor or manager. You may consider "privclassing" `LOGINCONTROL` for additional security. More is provided on the `LOGINCONTROL` command later within this subsection.

Human−Machine Access

The following are general security safeguards regarding human−machine access:

- Logout I/O devices (i.e., MAPs, PRTs) during extended periods when not in use and unattended.
- Change user passwords every month or more frequently.
- Follow local procedures for disposing of printout paper, documentation, and CD−ROM.

Input Command Screening

All commands should be Privilege Classed (PRIVCLASS) to restrict commands to selected users and all commands should be DUMPSAFE or DUMPUNSAFE as required. It is suggested that the PRIVCLASS screening process be controlled only by the control center (i.e., SCC, NOC, NRC). More is provided later within this subsection.

Security Log

When the parameter TABLE_ACCESS_CONTROL is set to "Y" and table CUSTPROT (Customer Protection) is datafilled, a security log is generated each time a table is changed. It records who, when, and what was changed. See table CUSTPROT later within this subsection.

Access Control for Tables

When equipped with the appropriate software, it is possible to control who may change translation data by using table CUSTPROT. Three levels of security may be provided: read only, update, and all privileges. TABLXXX logs produce an audit trail if they are set up in the log system.

Log Trails and Security Alarms

Any security log reports described within this subsection may be alarmed if desired. Various alarm levels for the SECUXXX and TABLXXX logs may be assigned by using table AUDALARM (Audible Alarm). The security logs can be used as an audit trail for regular and unauthorized operations. More is provided later within this subsection.

Security Software Packages

One or more of the following software packages must be present in the switching system to implement enhanced security:

- NTX292AB (BASE0001) Enhanced Security Package (Password Encrytion)
- NTX292BA (BASE0001) Enhanced Security Package (Non−Encrytion)
- NTX293AA (BASE0001) Enhanced Security Package II (Auto Dial−Back)

Office Security Parameters

The following office parameters are associated with the Enhanced Office Security software packages NTX292AB, NTX292BA, and NTX293AA.

Table OFCOPT: ENHANCED_COMMAND_SCREENING

This parameter should have a value of "Y" if the switching unit has the Enhanced Security Package (with password encryption – NTX292AB).

The feature associated with this parameter allows commands to be assigned any subset of 31 classes. Command screening then becomes a matter of ensuring that a user's command classes have a nonempty intersection with the classes of any command they wish to use.

Table OFCOPT: ENHANCED_PASSWORD_CONTROL

This option should be set to "Y" if the switching unit has the Enhanced Password Control Package (NTX292AB/NTX292BA).

If set to "Y", it creates the following parameters in table OFCENG:

- EXPIRED_PASSWORD_GRACE
- MIN_PASSWORD_LENGTH
- PASSWORD_LIFETIME

Use of the Enhanced Password Control feature disables all automatic login features.

This feature must have a value of "Y" in order for the Automatic Dial–Back Feature (NTX293AA) to function properly.

Table OFCOPT: MONITOR_TABLE_ACCESS

This option specifies whether the switching unit has the Security Table Enhancement Feature (NTX292AB/NTX292BA).

The operating company can activate or deactivate this feature by changing the value of parameter TABLE_ACCESS_CONTROL in table OFCVAR.

The operating company may activate or deactivate this feature on a table basis by changing the value of fields READPROT, UPDTPROT, or ALLPROT in table CUSTPROT.

Table OFCOPT: PASSWORD_ENCRYPTED

This parameter specifies whether the `SHOWPW` command is to be suppressed or not. The command `SHOWPW` is not optional and is available in switching units with the Password Encryption Package (NTX292AB).

Table OFCOPT: DIALBACKPW_ENCRYPTED

This parameter is required in a switching unit with the Automatic Dial–Back Feature (NTX293AA) and specifies whether the `SHOWDBPW` (Show Dial–Back Password) command is to be suppressed or not.

Table OFCOPT: MODEM_DIALBACK_CONTROL

This option specifies whether automatic dial–back is allowed on modems.

The Enhanced Password Control Package (NTX292AB/BA) is required for dial–back to function properly.

The `LOGINCONTROL` command is used to specify whether a modem is to be used as an answer modem or a dial–out modem when DIALBACK is active.

Table DIALBACK stores the dial–back related data.

Table OFCOPT: SUPPRESS_USERNAME

This appears only if ENHANCED_PASSWORD_CONTROL in table OFCOPT is set to "Y".

This parameter specifies if the username is suppressed during MAP VDU and printer sessions.

Set the parameter to "Y" if the username is to be suppressed.

Table OFCENG: EXPIRED_PASSWORD_GRACE

This appears only if ENHANCED_PASSWORD_CONTROL in table OFCOPT is set to "Y".

The number of logons for which a password may be used if the password is older than the value of parameter PASSWORD_LIFETIME:

```
Minimum : 0
Maximum : 32,767
Default : 3
```

Table OFCENG: MIN_PASSWORD_LENGTH

This parameter appears only if the switching unit has the option ENHANCED_PASSWORD_CONTROL in table OFCOPT set to "Y" and the Enhanced Security Package (NTX292AB) is present.

This parameter specifies the minimum number of characters allowed for logon passwords:

```
Minimum : 0
Maximum : 16
Default : 6
```

Table OFCENG: PASSWORD_LIFETIME

Appears only if ENHANCED_PASSWORD_CONTROL in table OFCOPT is set to "Y".

Determines the duration, in number of days, for which a password may be used.

```
Minimum : 0
Maximum : 32,767
Default : 30
```

Table OFCVAR: TABLE_ACCESS_CONTROL

This parameter is required if the switching unit has the Security Table Enhancement Feature (NTX292AB/NTX292BA) office option MONITOR_TABLE_CONTROL set to "Y" in table OFCOPT.

This parameter allows the operating company to activate or deactivate the feature by changing the value of this parameter.

When this parameter has the value of "Y", the operating company can activate or deactivate this feature on a table basis by changing value of fields READPROT, UPDTPROT, or ALLPROT in table CUSTPROT.

Associated Data Tables

The following tables are associated with enhanced security as described in NTP 297–XXXX–350, *Translations Guides*.

Terminal Device Table (TERMDEV)

This table lists the assignments for terminal devices. Table TERMDEV provides the ability to PRIVCLAS a terminal device restricting the device to a specific set or class of commands specified in table CMDS. There can be any combination of classes between 0 through 31 or "ALL".

This table also stipulates the type of modem that is connected to the corresponding port and thus determines which set of procedures are used for controlling the modem.

Where the Enhanced Password Control (Automatic Dial–Back) feature is present, the type of modem must be specified.

Access to table TERMDEV can be restricted by datafilling table CUSTPROT.

> **WARNING!** – *Be aware that a lockout condition exists if all the commands are "privclassed" out for all users and terminals.* The only way out is to use the user ID called ADMIN. An ADMIN user ID is neither displayed nor restricted in any way. It is always available, provided the ADMIN password is known and the terminal is not in the "autologin" mode.

Command Screening Table (CMDS)

Office parameter ENHANCED_COMMAND_SCREENING determines if the feature is turned on. This office parameter may be set only once: that is, at datafill time.

When office parameter ENHANCED_COMMAND_SCREENING is turned on, the table is automatically datafilled by the system.

The table is initially datafilled with default values.

> **WARNING!** – If tuples are added to this table through table control, a restart is required to activate the change, particularly if the tuple is deleted and then readded. To avoid a restart, modify the tuples in table CMDS using the `CHANGE` or `REPLACE` command (or via the `PRIVCLAS` command) instead of the `DELETE` and `ADD` commands.

The `PRIVCLAS` command allows for setting multiple command classes.

Four fields are present in table CMDS that specifies whether command use or command abuse is to be logged or alarmed. Those fields are:

Datafilling Table CMDS

Field	**Entry**	**Explanation and Action**
LOGONUSE	Y or N	Enter "Y" when a log is to be created on every use of this command. Default value is "N".
USEALARM	CR, MJ, MN, or NA	Enter the type of alarm to raise on every use of this command. Default value is "NA" (No Alarm).
LOGABUSE	Y or N	Enter "Y" when a log is to be created when a user with the wrong command set tries to use this command. Default is "N".
ALRMABUS	CR, MJ, MN, or NA	Enter the type of alarm to raise when a user with the wrong command set tries to use this command. Default value is "NA" (No Alarm).

Customer Protection Table (CUSTPROT)

This table defines the command class of users able to read, change, add, or delete tuples respectively for each table assigned in the switching unit.

The initial input for table CUSTPROT is automatically produced by table control, and maintains this value unless changed by the operating company. The initial values produce by table control for privilege classes are 15.

The privilege class that has the *read* protect capability is allowed to read, but *not* allowed to update, add, or delete tuples from the table.

The privilege class that has the *update* protection capability is allowed to read and update, but not allowed to add or delete tuples from the table.

The privilege class that has the *all* protection capability, is allowed to read, update, add, or delete tuples from the table.

All completed or aborted attempts to access a table is recorded in the form of log reports for examination later.

The log reports are generated on a per table basis when attempting to read a tuple and have it displayed, and on a tuple basis when attempting to write the tuple.

The log TABLXXX that is introduced by this feature is a secret log. All secret type logs are automatically routed to SYSLOG.

Following are the fields and associated datafill:

Datafilling Table CUSTPROT

Field	Entry	Explanation and Action
READPROT	0 - 30	Enter the privilege class that is allowed to read this table.
UPDTPROT	0 - 30	Enter the privilege class that is allowed to read the table and update tuples. Not allowed to add or delete tuples from the table.
ALLPROT	0 - 30	Enter the privilege class that is allowed to read, update, add, or delete tuples from the table.
VALACC	OFF, ALL, or WRITE	If the switching unit has the Security Enhancements Feature, and TABL101 logs are required, enter "WRITE", if TABL100 and TABL101 logs are required, enter "ALL", otherwise if the feature is not provided, or logs TABL100 and TABL101 are not required, enter "OFF".
DENACC	OFF, ALL, or WRITE	If the switching unit has the Security Enhancements Feature, and TABL103 logs are required, enter "WRITE", if TABL102 and TABL103 logs are required, enter "ALL", otherwise if the feature is not provided, or logs TABL102 and TABL103 are not required, enter "OFF".

Audible Alarm Table (AUDALARM)

This table is used to specify the alarm level for security log reports, which are *secret*. These reports are secure, that is, seeing them and manipulating them is restricted. The operating company can specify alarm levels to flag these reports.

Alarms can be specified in the following two ways:

- For report of the valid or invalid use of commands, the operating company can specify whether a report and alarm are to be generated for each command separately. This is specified in table CMDS.
- For other reports, the operating company can optionally specify an alarm level for each report separately. This is specified in table AUDALARM.

Secret alarms are not printed by log devices. To aid the operating company in determining the cause of alarms, any time a secret report causes an alarm, a *nonsecret* log is generated by the alarm system. This nonsecret log only reports that an alarmed secret report has occurred.

Tuples can not be added or deleted from the table with `LOGUTIL`. Tuples are added automatically by the log system at restart time, and each log report has the alarm level set to "No Alarm" by the default. The only valid user operation on this table is to change the alarm level on an existing tuple.

Following are the fields and associated datafill:

Datafilling Table AUDALARM

Field	Entry	Explanation and Action
LOGREP	Alphanumeric (16 characters)	This is the key field in the form: 'logname$report number' Only lognames and report numbers of secret logs are keys to their table.
ALARM	NA, MN, MJ, or CR	This sets the alarm to raise whenever the report is logged.

Automatic Dial–Back Table (DIALBACK)

The table DIALBACK enhances the security of dial–up ports. Requires feature package NTX293AA.

The special dial–back login sequence is performed only if the correct hardware and firmware are available, and the DIALBACK flag associated with the modem is set.

The `LOGINCONTROL` command permits the operating company to turn DIALBACK on or off for a specific port as well as change three dial–out related values:

- Number of rings per dial–back attempt.
- Number of dial–back attempts.
- Type of dial line.

Command `DIALBACKPW` allows the operating company to change dial–back passwords. This should be a privileged command to prevent security violations.

Login Control Table (LGINCTRL)

The table LGINCTRL is provided to enable the login control data to be dumped and restored during the software application process. This enables data to be preserved between software loads. This table is an extension to table TERMDEV that controls the addition or deletion of tuples for table LGINCTRL.

The operating companies can change the tuples if they so desire, but it is *highly recommended* that they use the CI command `LOGINCONTROL`.

Associated Commands

Following are the commands associated with the Enhanced Office Security software packages:

PASSWORD

```
      >PASSWORD [username] [newpw]
```

Changes a user's own password. Only the ADMIN user can change another user's password. (*See Note 1*)

Where:

- `[username]` – Is an 8–character (max.) name, defined by the operating company. Use the `SHOW USERS` command to display a list of current usernames. Required only when ADMIN user is changing another user's password.

- `[newpw]` – Is the new password that is to replace the current password associated with the username.

Password characteristics are controlled by the following parameters (default values) in table OFCENG:

```
   MIN_PASSWORD_LENGTH : 6 characters
     PASSWORD_LIFETIME : 30 days
EXPIRED_PASSWORD_GRACE : 3 logons (See Notes 2 & 3)
```

Responses:

```
PASSWORD: ENTER NEW LOGON PASSWORD
```

Explanation: Normal system prompting before `[newpw]` is entered.

```
PASSWORD: ENTER YOUR CURRENT PASSWORD TO VERIFY
```

Explanation: Normal system prompting after valid `[newpw]` has been entered.

```
PASSWORD FOR XXXXXXXX HAS BEEN CHANGED.  IT MUST BE CHANGED AGAIN WITHIN
30 DAYS
```

Explanation: Normal response when the new password has replaced the old password.

```
PASSWORD: SORRY THAT PASSWORD SHOULD BE AT LEAST 6 CHARACTERS LONG
```

Explanation: A new password has been entered that does not conform to the office parameter MIN_PASSWORD_LENGTH. Select a proper password and reenter it.

```
*****WARNING*****
YOUR LOGON PASSWORD HAS NOT BEEN CHANGED IN 30 DAYS.  YOU HAVE 3 MORE LOGON SESSIONS TO
CHANGE YOUR PASSWORD AFTER WHICH YOU WILL *NOT* BE ABLE TO LOGON
```

Explanation: Reminder to a user at login time that office parameter PASSWORD_LIFETIME has been exceeded, and that EXPIRED_PASSWORD_GRACE parameter is in effect.

Notes:

1. PASSWORD is only present and active when the Enhanced Office Security software package is provisioned, and the ENHANCED_PASSWORD_CONTROL parameter in table OFCENG is set to "TRUE".
2. PASSWORD should first be entered alone. The system then prompts the user to enter [newpw].
3. PASSWORD must be used periodically to change passwords. Users are automatically reminded to change their passwords when PASSWORD_LIFETIME has expired. The new password *must* be different from the old password.

PERMIT

```
>PERMIT [username] [password] {priority} {stksize} {language} {cmdclass}
```

Assigns command classes, previously defined by PRIVCLAS, to specified users. It also alters previous assignments to a user, or defines new users.

Where:

- [username] – An 8–character (max.) name for a user class that is defined by the operating company. Use the SHOW USERS command to display a list of current usernames.
- [password] – The DMS–100 user password that is to be associated with the username. Required when a user initially logs on. Passwords are defined by the operating company. The number of characters permissible in a password is governed by the parameter MIN_PASSWORD_LENGTH in table OFCENG, if ENHANCED_PASSWORD_CONTROL is set to "TRUE".
- {priority} – Value 1 to 4. The default is 4. Sets the priority level of the user's process.
- {stksize} – Sets the number of words of memory that are assigned to the specified user's processes at log on. The range available is 1,500 to 10,000. The default is 4,000.
- {lang} – Values: FRENCH, GERMAN. Selects the language of input commands and system outputs. If human–machine interface is required in a language other than default value (ENGLISH), then set in the DEFAULTLANGUAGE field of table OFCENG. Bilingual human–machine interface software must be provided.
- {cmdclass} – Command class number(s) value 0 to 30, NONE, or ALL. The default is NONE. Terminal designation associated with each of 31 class numbers are entered in the COMCLASS field of table TERMDEV, and are assigned by the operating company.

PRIVCLAS

```
>PRIVCLAS ALL [cmdname] [modname] [cmdclass] [cmdlist]
```

Adds, changes, or deletes the privilege class for specified command(s) or program module(s). Lists all current privilege commands and their classes. Sets DUMPSAFE state for specified command(s) or module(s).

Where:

- ALL – Provides a display listing all command and module names, with their assigned command class(es) and DUMPSAFE states. Unrestricted commands are not listed. Default value if PRIVCLAS only is entered.
- [cmdname] – Is the name of any valid DMS–100 family command. Specifies command name to be assigned privilege class(es) and DUMPSAFE state.
- [modname] – Is the name of the program module that is to be assigned a privilege class, or the name of the module in which the specified [cmdname] resides. Also referred to as "increment" (INCR).

- [cmdclass] – Specifies the class number to be assigned to a [cmdname] or [modname]. Also used to set DUMPSAFE state. Used with systems having regular command screening.

- [cmdlist] – Used only when the Enhanced Command screening feature is turned on. Specifies a list of command classes to be assigned to a [cmdname] or [modname]. Also sets DUMPSAFE state for the specified command classes.

Values:

- 0 - 30 – Terminal designations associated with each of the 31 class numbers are entered in COMCLASS field of table TERMDEV and are assigned by the operating company.

- NONE – Deletes any privilege class already assigned, so that any user can execute the specified [cmdname].

- DUMPSAFE – Sets the specified [cmdname], or commands associated with a specified [modname], to DUMPSAFE.

- DUMPUNSAFE – Sets the specified [cmdname] or [modname] to DUMPUNSAFE (cannot be executed during office image production).

LOGINCONTROL

```
>LOGINCONTROL [console_name, {ALL}] [option]
```

Control login access to consoles.

Option Descriptions:

QUERY

Displays the current settings and current state of a console (port). The BRIEF option causes only the current enable state and the current user to be displayed. The FULL option displays the state of all options that can be set by the other parameters.

ENABLE

Allows login attempts on a port to be accepted by the system.

DISABLE [disabletime]

Causes the system to refuse any login attempt. The optional subparameter, [disabletime], specifies how long (in minutes) the port is unavailable for logins. Range is 1 to 32,767 or FOREVER (default).

> **Note:** Currently logged in ports cannot be disabled. If the LOGINCONTROL command is used to set *all* ports disabled, only those ports that are not currently logged in are disabled.

AUTODISABLETIME [disabletime]

Determines how long a port is disabled if it is disabled automatically by the system. The optional subparameter, [disabletime], specifies how long (in minutes) the port is unavailable for logins. Range is 1 to 32,767 or FOREVER (default).

MAXLOGINTIME [seconds]

Determines the maximum time (in seconds) a user may take to login on a specific port. If the timeout is exceeded, the login sequence is canceled and the port is optionally disabled (see DISABLEON parameter). Range is 1 to 32,767. The default is 60 seconds.

MAXIDLETIME [minutes]

Determines the maximum time (in minutes) a user may leave a port unattended. If timeout is exceeded, the user is forced out and the port is optionally disabled (see DISABLEON parameter). Range is 2 to 546 or FOREVER (default).

LOGINRETRIES [retries]

Determines the number of times a user has to login correctly before the login sequence is canceled. If the login sequence is canceled, the port may also be optionally disabled (see DISABLEON parameter). Range is 1 to 32,767. The default is 4.

OPENCONDITIONFORCEOUT [true/false]

Indicates that the user at the reported terminal should be logged out when a line open condition is detected. The port may optionally be disabled.

DISABLEON [add/set/remove] [action]

Determines the events that cause a port to be automatically disabled. The DISABLEON parameter takes two subparameters. The first subparameter is either ADD, SET, or REMOVE that specifies what to do with the second `[action]` subparameter, which is any number of entries from the following list:

- **LOGINFAIL** – The port is to be disabled if the user cannot supply a valid user ID and password in MAXLOGINRETRIES attempts.
- **LOGONTIMEOUT** – The port is to be disabled when the login sequence of a user is canceled when the user takes more than MAXLOGINTIME to login.
- **IDLETIMEOUT** – Specifies that the port is to be disabled when an idle user is forced out on that port.
- **LOGOUT** – Specifies that the port is to be disabled upon the user logout.
- **OPENCOND** – Specifies that the port is to be disabled if the user is logged out due to the detection of a line open condition.
- **DIALBACKLOGINFAIL** – Specifies that the port is to be disabled upon a dial–back login failure.
- **DIALBACKCALLFAIL** – Specifies that the port is to be disabled upon a failed dial–back call.

DIALBACK [state]

Disables dial–back for specified port or enables the port as a dial–out or answer modem. Where `[state]` is: OFF, ANSWER, or DIAL.

DIALOUT [max_calls] [dialtype]

Sets the maximum number of rings the modem is to wait for an answer before aborting the call, the maximum number of dial–back calls that the modem will attempt, and the line type associated with the modem (dial pulse or tone). Range for `[max_calls]` is 1 to 7 and `[dialtype]` is AUTO, PULSE, or TONE.

Examples:

To enable a port:

```
>LOGINCONTROL DIALUP1 ENABLE
```

To enable all ports:

```
>LOGINCONTROL ALL ENABLE
```

To disable a port temporarily:

```
>LOGINCONTROL DIALUP1 DISABLE MINS 10
```

To set a port to force out a user if the user has been idle for ten minutes:

```
>LOGINCONTROL DIALUP1 MAXIDLETIME MINS 10
```

To set the port to disable if the user does not login in two attempts:

```
>LOGINCONTROL DIALUP1 LOGINRETRIES 2
>LOGINCONTROL DIALUP1 DISABLEON LOGINFAIL
```

To turn off disable on IDLETIMEOUT for all terminals:

```
>LOGINCONTROL ALL DISABLEON REMOVE IDLETIMEOUT
```

To set the disable options of a port to a specific list:

```
>LOGINCONTRL DIALUP1 DISABLEON SET LOGINFAIL IDLETIMEOUT LOGOUT
```

To turn off all disable options for a port:

```
>LOGINCONTROL DIALUP1 DISABLEON REMOVE LOGINFAIL IDLETIMEOUT LOGOUT LOGINTIMEOUT
```

To display current settings:

```
>LOGINCONTROL ALL QUERY
```

To forceout a terminal when a line open condition is detected:

```
>LOGINCONTOL DUALUP1 OPENCONDITIONFORCEOUT
```

To set the terminal to disable if a line open condition exists:

```
>LOGINCONTROL DIALUP1 OPENCONDITIONFORCEOUT DISABLEON ADD OPENCOND
```

To turn off all disable options for a terminal:

```
>LOGINCONTROL DIALUP1 DISABLEON REMOVE LOGINFAIL IDLETIMEOUT LOGOUT LOGINTIMEOUT OPENCOND
```

Login Banner

The login banner feature (NTXS07AA) displays a banner immediately following a successful login. The banner will appear after a successful login – on the initial login, not a remote login – and will survive all restarts. The customer can define the banner by using the SETBANNER command to replace the current login banner with a user–defined banner file. The user banner file may be no longer than 22 lines, 80 characters per line. A file that exceeds this limit will be truncated before being copied. The user banner file must not be blank or have its first 22 lines blank. A blank file will not be copied. The device where the user banner file is stored, and the name of that file must be provided. The device on which the user file is located must be listed so that SETBANNER can locate that file.

It is suggested that the customer PRIVCLAS the SETBANNER command using the CMDS table. Until the customer replaces the default login banner text, it will read:

```
This is a private database.  All activity is subject to monitoring.
Any UNAUTHORIZED access or use is PROHIBITED, and may result in PROSECUTION.
```

Associated Logs

The following SECUXXX, SOSXXX, and TABLXXX logs are associated with the Enhanced Office Security software packages:

Log Report	Description
SECU101	The Security (SECU) subsystem generates this report when a valid user logs on or off a terminal using normal login or logoff procedures.
SECU102	Generated when a user attempts to login on a terminal using an invalid identification or password.
SECU103	Generated when one user forces another user off their logged–in terminal.
SECU104	Generated when a user changed the commandset class for a privileged command or the automatic logging of command use or abuse in table CMDS.
SECU105	Generated when one user changes the password for another user.
SECU106	Generated when a user with the proper command class set issues a command datafilled in table CMDS, and the command is executed.
SECU108	Generated when a user without the proper command class set attempts to access a table, and the table is not accessed.
SECU109	Generated when a valid user logs on a terminal using Priority Login (PLOGIN) procedures.
SECU110	The security subsystem generates this report when a user attempts a Priority Login (PLOGIN) on a terminal using an invalid identification or password.
SECU111	The security subsystem generates this report when a user changes the command class set for a terminal defined in customer data table TERMDEV.
SECU112	Generated when one user adds or changes the security profile for another user.
SECU113	Generated when an attempt is made to login on a terminal that is not enabled.

SECU114 Generated when a console is manually enabled or disabled.

SECU115 Generated when the maximum login time specified by the LOGINCONTROL command is exceeded, and the terminal is disabled.

SECU116 The security subsystem generates this report when the maximum number of invalid login attempts specified by the LOGINCONTROL command is exceeded, and the console is disabled.

SECU117 Generated when a terminal is automatically enabled by the system as specified by the LOGINCONTROL command.

SECU118 Generated when a user is idle too long or a line open condition is detected. The user is automatically logged off the terminal, and the terminal is disconnected, depending on the terminal's security profile defined in table TERMDEV and by LOGINCONTROL.

SECU119 The security generates this report when a terminal is disabled by the system after the user has logged out, or the terminal has been busied out.

SECU120 Generated when a user attempts to login on a dial-up terminal using an invalid identification or password.

SECU121 Generated when a valid user logs on a dial-up terminal using normal login procedures.

SECU122 Generated when an attempt to logon on a dial-up terminal fails.

SECU123 Generated when an attempt to login on a dial-up terminal succeeds, the dial-back call is successful, and the login is completed.

SECU124 Generated when a user changes the dial-back password for a user.

SECU125 Generated when dial-back is enabled for a dial-up terminal.

SECU126 Generated when dial-back is disabled for a dial-up terminal.

SECU127 Generated when a START, STOP, REMOVE, or OVERRIDE command is used in the Automatic Line Testing (ALT) MAP levels. This log is also generated when changes are made to the start field.

SECU128 Generated when the system of ADMIN user activates of deactivates the AUTOLOG feature.

SECU129 Generated when the AUTOLOG CLASS command is issued by the ADMIN user.

SOS600 Informs the customer that a hung login process has been killed. It captures status information of the login process to help debug the hung login process.

TABL100 The table subsystem generates this report to indicate that an authorized user has accessed the customer data table in read mode, and displayed a tuple. It is generated once per table entry.

TABL101 Generated to indicate that an authorized user has accessed the specified customer data table in write mode. This report is generated once per tuple update.

TABL102 Generated to indicate that an unauthorized user has attempted to access the specified customer data table. This report is generated once per table entry attempt only.

TABL103 Generated to indicate that an unauthorized user has accessed the customer data table in write mode. This report is generated once per tuple update.

Arrangement of User Classes

Switch *users* should be organized into classes that define a specific set of functions they are required to perform. These functional needs in turn dictate the command requirements for each user class. The assignment of user commands and table access is made flexible to meet telephone company operational requirements. The rule is: the division of tasks shall provide the purpose for each users' class.

The following are the names and descriptions for some typical users' classes.

Administration (ADMIN)

Provides the user with unlimited access from any device to all command classes (see PRIVCLAS). ADMIN is assigned the highest priority level. The password associated with ADMIN cannot be displayed, and cannot be changed by any other user.

Switch Maintenance (SMTCE)

Enables the user to maintain the DMS−100 switch by performing regular maintenance and fault correction for the following:

- Central Control/Computer Module (CC/CM)
- Central Message Controller/Message Switch (CMC/MS)
- Input/Output Device (IOD)
- Network Module (NM)
- Peripheral Module (PM)

The SMTCE user also performs all database changes to administer the switch. SMTCE monitors the switch status, runs diagnostic programs, and replaces equipment. This class has commands associated with table editor and the Support Operating System (SOS). SMTCE class also includes control center positions for analyzers and office control responsibilities.

Trunk Maintenance (TMTCE)

Enables the user to perform regular maintenance and fault correction for trunk circuits, trunk facilities, and trunk translations (maintenance and input). The user monitors the trunk status, runs diagnostic programs, and performs hardware tests.

The TMTCE use is limited to the input commands available only to the user's class. TMTCE has only those commands associated with testing and maintaining trunks and trunk facilities. The user has access to the table editor commands, but is restricted in the changing of specific tables as required by the position profile. The TMTCE functions are performed from a Trunk Test Position (TTP). This class of user also includes the control center position for trunk analysis control responsibilities.

Network Management (NM)

Enables the user to make optimum use of available facilities and equipment by exercising routing control over traffic oriented switch resources. The user monitors traffic levels, applies manual controls, adjusts automatic controls, and receives Operational Measurement (OM) traffic reports.

NM has interactive capabilities to execute only those input commands assigned to its class. The user is allowed data table query capabilities, but is restricted to changes for specific data tables.

Dial Administration (DADMIN)

This class enables the user to monitor OM traffic reports. DADMIN can alter OM scheduling, assignments, and thresholds.

The DADMIN user has access to the table editor repertoire of commands when altering data associated with OMs. Full data table query capabilities are also afforded the user (in particular, traffic register assignment and readings).

Service Analysis (SA)

Enables the user to monitor, on a random basis, customer dialed and operation assisted toll calls to obtain information on the quality of service provided by the equipment and personnel.

The SA user has access to the table editor repertoire of commands, but is screened on a table basis to change only those data tables associated with this class. The SA user has access to the "SAselect" area of the MAPCI commands.

Technical Assistance Center (TAC)

The TAC, or equivalent technical support group (i.e., Electronic Systems Assistance Center [ESAC]), enables the user to monitor unattended switching units and provide technical assistance to switching center personnel as required. The TAC is a centralized maintenance group of highly trained and experienced personnel.

This user class has interactive capabilities to execute all input commands that are applicable to switch maintenance.

Emergency Technical Assistance Service (ETAS)

Nortel Network's ETAS provides assistance to customers TAC groups when they are having difficulty correcting switching problems.

This user class is restricted to those input commands required for system interrogation, data dumps, etc. No machine operating parameters including tables OFCOPT, OFCENG, OFCVAR, OFCSTD, CUSTPROT, TERMDEV, CMDS, AUDALARM, and equipment inventory tables should be allowed to be altered from this position.

Line Maintenance (LMTCE)

Enables the user to monitor the status of line cards, run diagnostics on line cards, sectionalize troubles, test and diagnose troubles with the office, query and change subscriber data, and schedule automatic line card diagnostics.

Repair Service Bureau (RSB)

Enables the user to sectionalize troubles, test and diagnose facility troubles, schedule Automatic Line Insulation Testing (ALIT), receive ALIT outputs, and query or change subscriber data.

Traffic Administration (TA)

Enables the user to receive automatic periodic summary reports of traffic statistics accumulated by the switching system. These reports reflect traffic peg counts, overflows, usage of the switching units, and OMs. The TA user can modify the schedule and output of these reports.

Minimum Security Implementation

There are four key areas in implementing minimum security: (1) passwords, (2) ports, (3) tables, and (4) commands.

Listed below is a step−by−step example for implementing minimum security for the DMS−100 family of switches. The scheme is to reserve classes 1 thru 13 for *commands* and 15 thru 29 for *tables*. Classes 14 and 30 are reserved for the *administrator*. Class assignment is flexible and any command or table can be assigned any or all of the 31 allowable classes.

Commands are automatically written into table CMDS, upon their first use, with a class of 0. Therefore, command class 0 should not be assigned to a user after all user classes have been designated.

Steps 1 & 2 show the office parameters associated with enhanced security.

Step 3 shows the recommended settings for password security.

Steps 4 & 5 shows the use of the command `LOGINCONTROL` and how to secure port access.

Steps 6 thru 13 show an example of restricting ports and users to table access.

Steps 14 thru 16 show the restriction of specific command to specific users.

Step 17 shows the assignment of an external alarm and log to specific secret logs that are not alarmed in tables CMDS and CUSTPROT.

1. Check the following parameters in table OFCOPT for correct settings as listed:

```
ENHANCED_COMMAND_SCREENING = Y
 ENHANCED_PASSWORD_CONTROL = Y
         SUPPRESS_USERNAME = Y
      MONITOR_TABLE_ACCESS = Y
```

2. Check the following parameter in table OFCVAR for the correct setting as listed:

```
TABLE_ACCESS_CONTROL = Y
```

3. The following tuples in table OFCENG set the parameters associated with user passwords, provided are the recommended minimum and maximum values. These parameters appear only if the table OFCOPT parameter ENHANCED_PASSWORD_CONTROL is set to "Y":

```
     PASSWORD_LIFETIME = 30
   MIN_PASSWORD_LENGTH = 4
EXPIRED_PASSWORD_GRACE = 1
```

4. Review the existing login control parameters set for all ports. Input the following command to print out these parameters:

```
>LOGINCONTROL ALL QUERY FULL
```

5. Set login control parameters for all ports. For more information on the `LOGINCONTROL` command, see NTP 297−1001−822, *Commands Reference Manual*. The following are the suggested login control parameters:

```
>LOGINCONTROL ALL DISABLE                 # Disables all idle ports
>LOGINCONTROL ALL AUTODISABLETIME FOREVER
>LOGINCONTROL ALL MAXLOGINTIME SECS 60
>LOGINCONTROL ALL MAXIDLETIME MINS 15
>LOGINCONTROL ALL LOGINRETRIES 3
>LOGINCONTROL ALL DISABLEON SET LOGINFAIL
>LOGINTIMEOUT IDLETIMEOUT
```

Note: A secret log SECUXXX is generated.

6. Print a hard copy of tables CUSTPROT and TERMDEV and the output of the `SHOW USERS` command. These will be needed for reference with the remaining implementation examples.

7. Logout and login as the ADMIN user.

8. Review table TERMDEV for devices that should be restricted access to tables.

9. Change field COMCLASS from "ALL" to "0 1 2 3 4 5 6 7 8 9 10 11 12 13 15".

10. Review the `SHOW USERS` printout for users to be restricted from accessing tables.

11. Using the command `PERMIT`, change the command class of the users to be restricted from "ALL" to "0 1 2 3 4 5 6 7 8 9 10 11 12 13 15".

12. Enter table CUSTPROT and change the entries for the following tables and fields. Default values for this table are "15, 15, OFF, OFF":

TABLE	UPDTPROT	ALLPROT	VALACC	DENACC
OFCENG	28	29	WRITE	WRITE
OFCSTD	28	29	WRITE	WRITE
OFCOPT	28	29	WRITE	WRITE
OFCVAR	28	29	WRITE	WRITE
CUSTPROT	30	30	WRITE	WRITE
CMDS	30	30	WRITE	WRITE
AUDALARM	30	30	WRITE	WRITE
TERMDEV	30	30	WRITE	WRITE
DIALBACK	30	30	WRITE	WRITE
LGINCTRL	30	30	WRITE	WRITE

13. Assign class 28 to users that are allowed to update the above tables and assign class 29 to those users allowed complete access to the above tables.

Notes:

- Class 30 is reserved for ADMIN.
- Assigning "WRITE" to field VALACC and DENACC provides a secret log TABLXXX. When an authorized user writes to the above tables a TABL101 log is generated. A TABL103 log is generated when an unauthorized user attempts to write to the above tables.

14. Access table CMDS and perform the following changes to fields LOGONUSE, USEALARM, LOGABUSE, and ALRMABUS:

COMMAND	LOGONUSE	USEALARM	LOGABUSE	ALRMABUS	CLASS
ENGWRITE	Y	NA	Y	NA	13
JFFREEZE	Y	MJ	Y	CR	14
LOGINCONTROL	Y	NA	Y	NA	13
MODEDIT	Y	MJ	Y	MJ	13
PRIORITY	Y	NA	Y	NA	13
PROIRITY	Y	NA	Y	NA	13
PRIVCLAS	Y	NA	Y	NA	14
PRIVERAS	Y	NA	Y	NA	14
RESTART	Y	CR	Y	CR	13
RESTARTBASE	Y	CR	Y	CR	13
RWOK	Y	NA	Y	MN	13
SHOWDBPW	Y	NA	Y	NA	14
SHOWPW	Y	NA	Y	NA	14
SLEEP	Y	MJ	Y	MJ	13
SLEEPTIL	Y	NA	Y	NA	13
PERMIT	Y	NA	Y	NA	14
UNPERMIT	Y	NA	Y	NA	14
LOGUTIL:					
OPENSECRET	Y	NA	Y	NA	14

15. Using the command `PRIVCLAS`, assign the above commands to their respective class:

```
>PRIVCLAS ENGWRITE $ 13
>PRIVCLAS OPENSECRET LOGUTIL 14
```

16. Assign command class 13 to those users allowed the above commands:

```
>PERMIT [username] [password] 1 4000 ENGLISH 0 1 2 3 4 5 6 7 8 9 10 11 12 13 15
```

Notes:

- Class 14 is reserved for ADMIN.
- The fields LOGONUSE and LOGABUSE set to "Y" causes the following two logs to be generated: TABL106 for valid command use, and TABL107 for invalid command use.

17. Enter table AUDALARM and change the following records:

Log Report	Alarm	Reason
SECU103	Minor	One user forces another out.
SECU107	Major	Command abuse.
SECU111	Minor	Changes to port class in table TERMDEV.
SECU124	Major	Dial-back password changed for a user.

Notes:

- The alarm generated by a secret log or commands use or abuse turn themselves off after approximately 15 seconds.
- An EXT108 log is printed for critical alarms, an EXT107 log is printed for major alarms, and an EXT106 log is printed for minor alarms. EXTXXX log reports are not generated for "NA" (No Alarm).

Security Recommendations

It is extremely difficult to provide specific security recommendations without knowledge of a company's requirements. Below are general recommendations that provide basic security for DMS−100 family switches. It is recommended that security measures be implemented to safeguard switch integrity.

1. PRIVCLASS all devices and user passwords according to the needs of the device and user.
2. Establish password aging.
3. Change the password for user ADMIN and it should be known only by the office and/or control center supervisor.
4. All dial−up modems should be set to "DISABLE" upon logout.
5. Institute a manual log form of all requests for dial−up access. When a request for dial−up access is received, the requester should be called back to verify the validity of the their phone number.
6. PRIVCLASS all sensitive data tables such as: CUSTPROT, OFCENG, OFCVAR, OFCOPT, OFCSTD, TERMDEV, CMDS, and AUDALARM.
7. Restrict access command use by user need. The following commands should only be available to the switch administrator (ADMIN): `SHOWDBPW`, `SHOWPW`, `PERMIT`, `UNPERMIT`, `PRIVCLAS`, and `PRIVERASE`.
8. All I/O devices (MAPS, TTPs, LTPs, etc.) should be logged out during extended periods when not in use and unattended.
9. User passwords should be changed every three months or more often.
10. Local procedures should be followed for disposing of printout paper, documentation, and CD−ROMs. This may require recycling or shredding to meet local and Technical Information Agreement (TIA) security requirements.

Nortel Networks Security Service

To assist operating companies with their switch security, Nortel Networks Global Professional Services Group provides a Standardized Security Service. There is a nominal charge for this service. This service provides a review of the operating company's switch security. If an operating company requests this service, security will be set up based upon information provided by the operating company and recommendations from Nortel Networks. A special program developed by Nortel Networks will be provided to the operating company for implementation on their switches. Nortel Networks lab testing and a VO switch designated by the operating company will provide preliminary program testing before implementation. For further information on this service or obtaining this special service, contact Nortel Networks, Global Professional Services, Manager – Technical Services at 1−(919)−465−0434.

Surreptitious Entry Tips

Overview

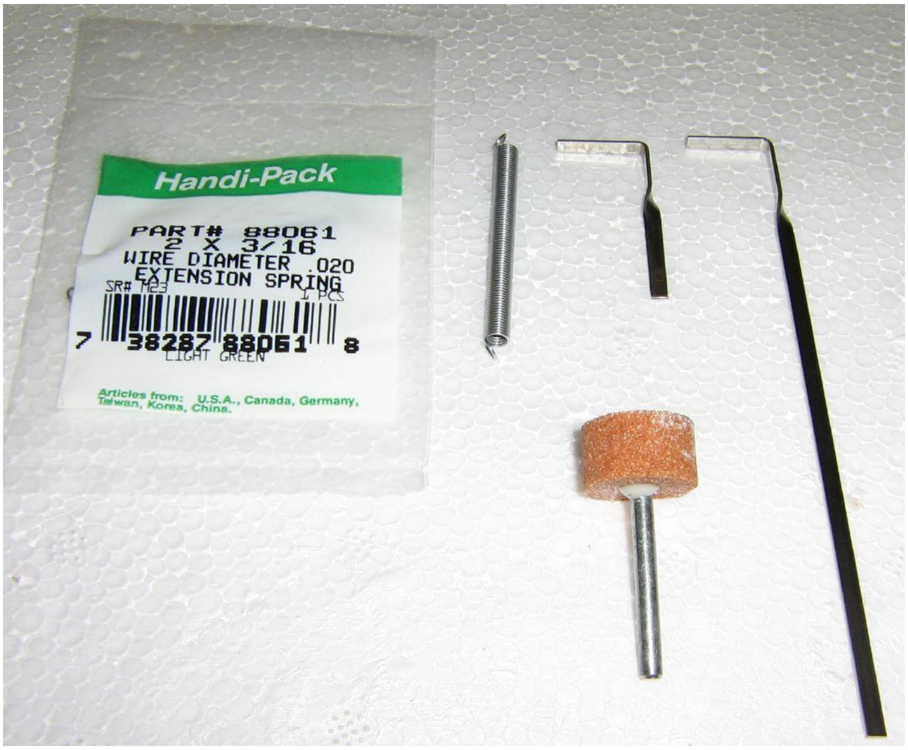
Here are some useful tips and tricks one can use when breaking into a "forbidden" target area. A person should, at least once in their lifetime, break into a Democratic National Committee office to plant surveillance bugs to monitor any illegal "call girl" operations. Just don't screw it up, dumbass...

If you're in the FBI, a good target area is *$2600 Magazine's* "little boys" room. I get scared just *thinking* about what goes on in there! You should too...

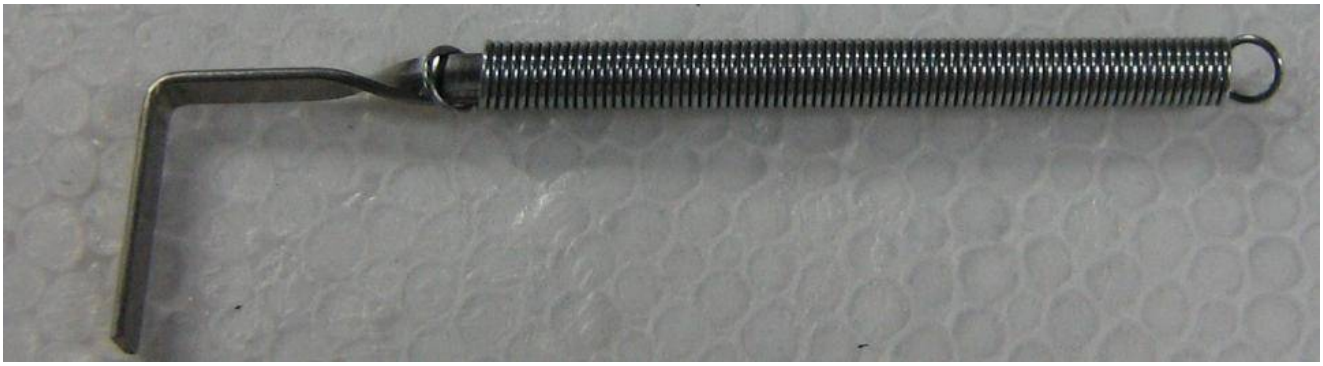
A new favorite game to play is breaking into the "homes" of illegal aliens to take back the money they steal from taxpayers. Be just like Robin Hood! Other places of interest are Mosques (duh!), any Eurosavage country's embassy, the United Nations headquarters, and ACLU offices.

Covered are a few lock picking tension wrench tricks for aiding in one–handed operations and a method of polishing your lock picks for a better "feel" inside the lock. Also covered is the use of an old blood pressure arm cuff which acts as an inflatable blatter for raising doors off the floor. There is also a really neat trick for determining keypad–based alarm or safe combinations – and it only costs $20! Finally, there is a simple project for building a magnetic–mount magnifying glass.

Feather Tension Wrench

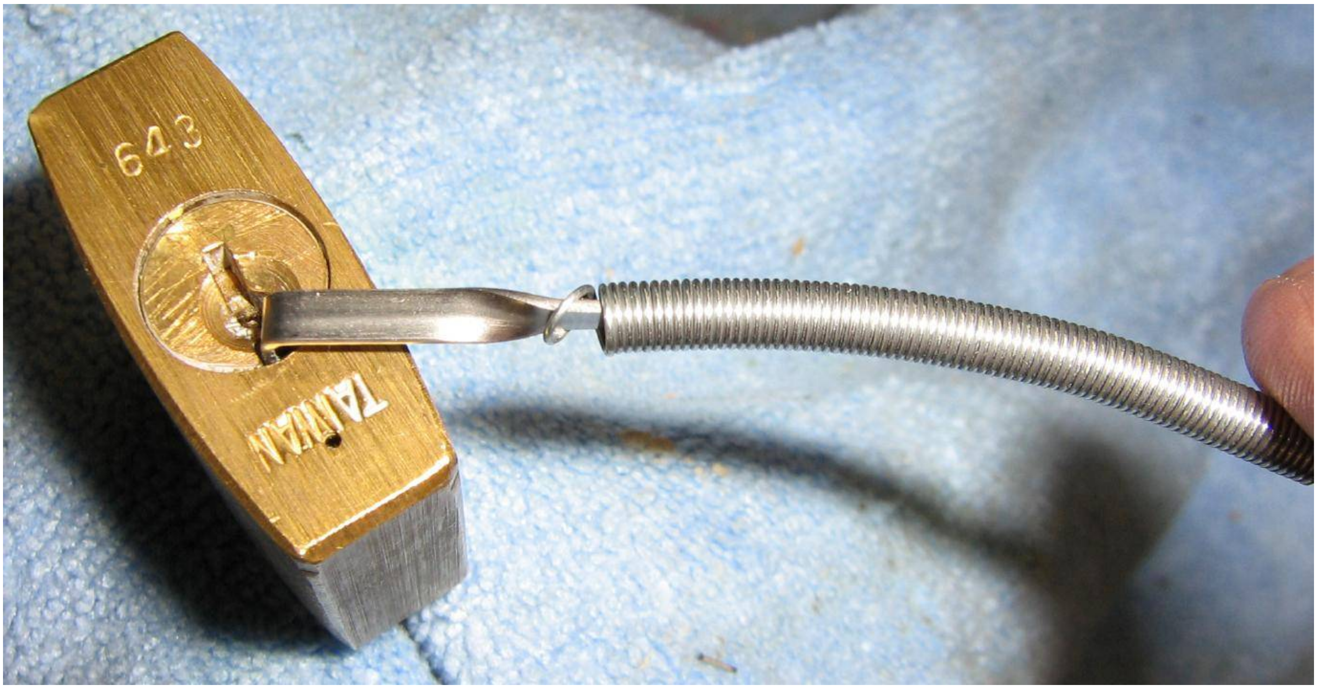


Feather tension wrench parts overview. A stock Southern Ordnance, Long Twist–Flex (TW–03) tension wrench is shown on the far–right. Cut the handle down so it is approximately one inch long. Use a Dremel tool with a cut–off wheel attachment, then debur the cut end with an abrasive wheel attachment.



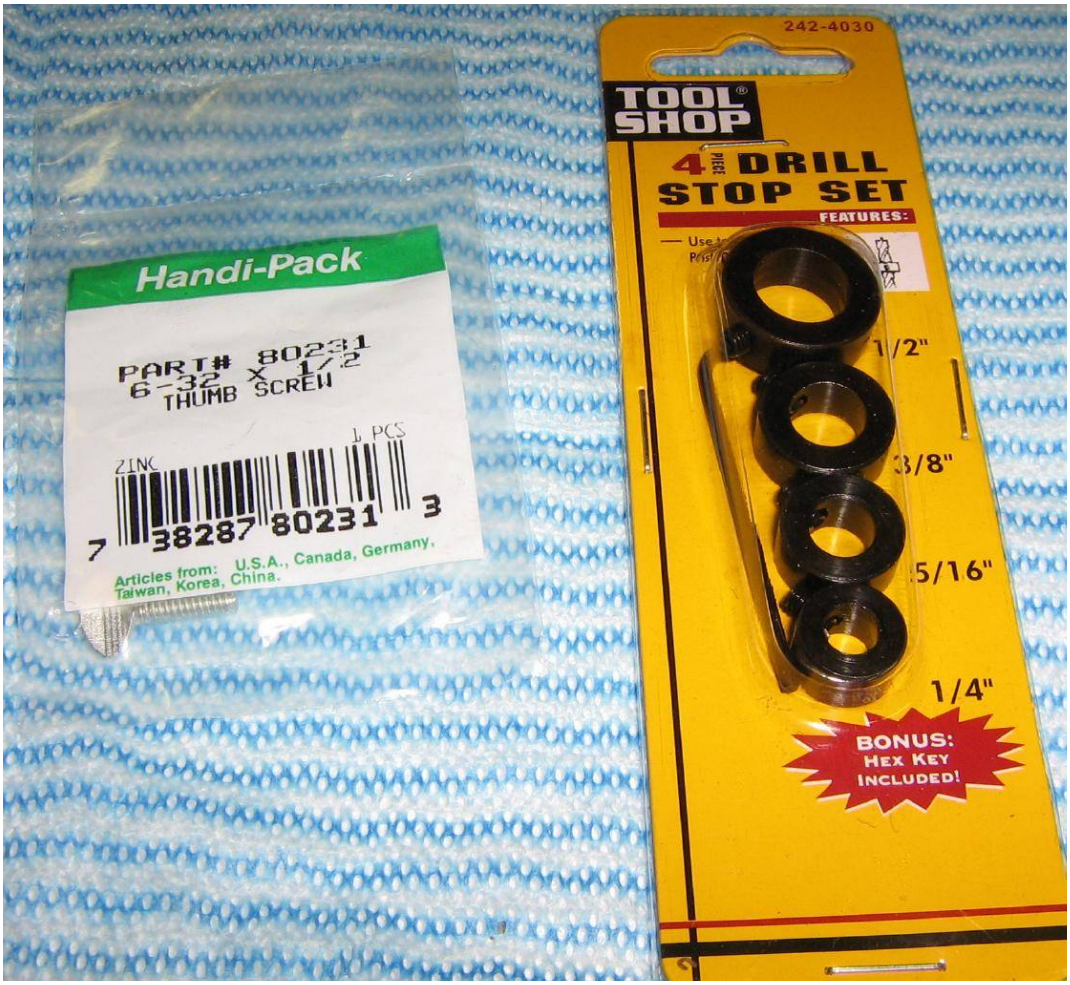
Push a small–diameter spring onto the shortened tension wrench handle. The spring used for this particular wrench is 2–inches long with a 3/16–inch inside diameter. It fits the wrench perfectly. You'll want to purchase a vast assortment of different spring lengths and spring tensions to experiment with.

Be careful not to push the spring up too far on the handle. It needs to maintain its "flex."



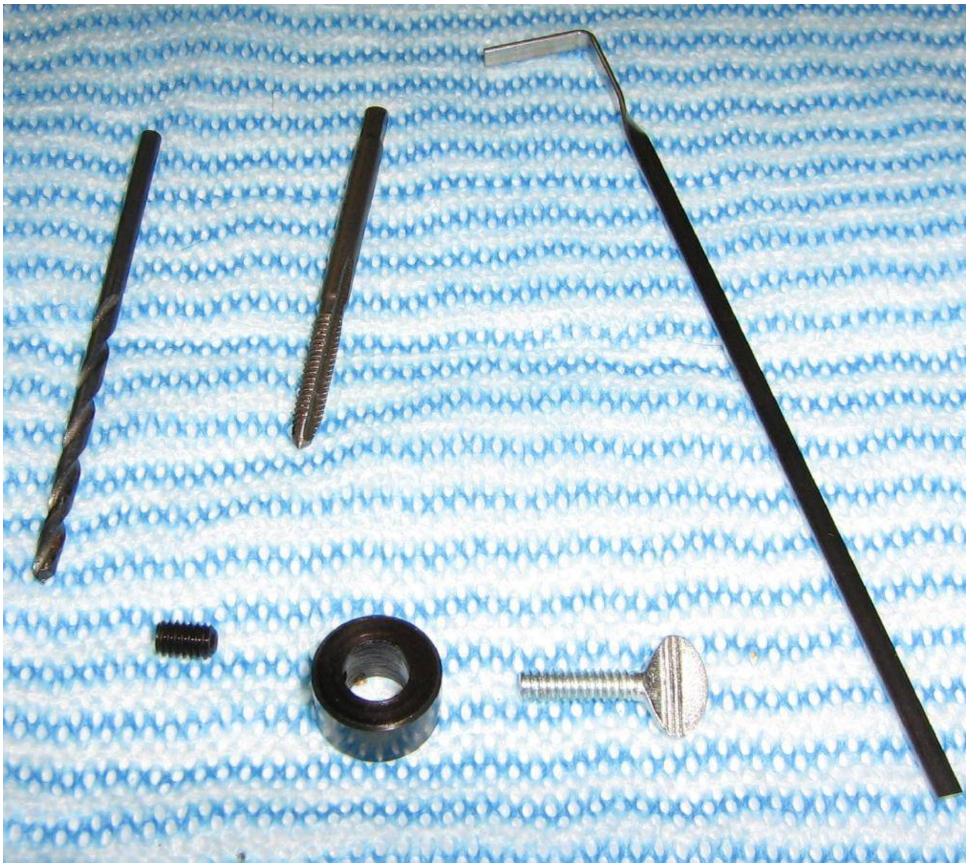
Feather tension wrench in operation. This tension wrench is useful for applying a *very light* turning pressure, which is handy for picking pin tumbler locks with security (i.e., spool or mushroom) pins.

Adjustable Tension Wrench Weight

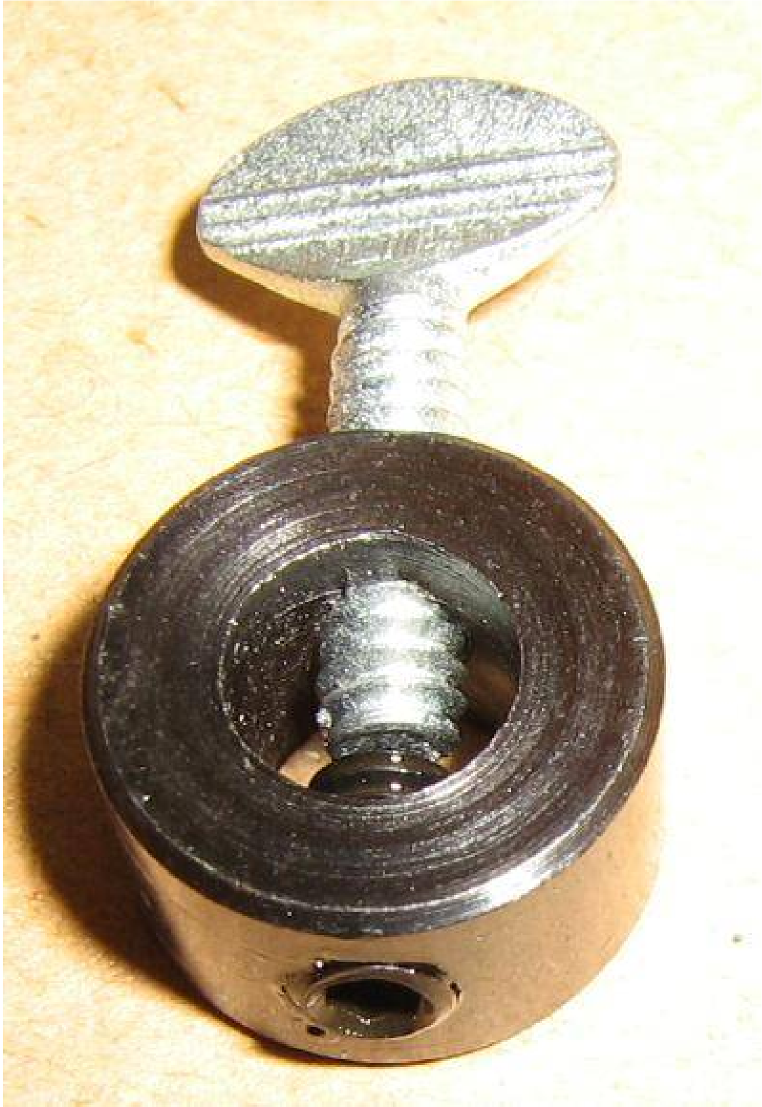


To ease one−handed lock picking or raking, a small adjustable weight can be added to the tension wrench. This helps to simulate the turning pressure you would normally use on the tension wrench. This method will only work on simple pin tumbler locks *without* any security pins. (To pick "security" locks, you need to feel the security pins with your tension wrench hand).

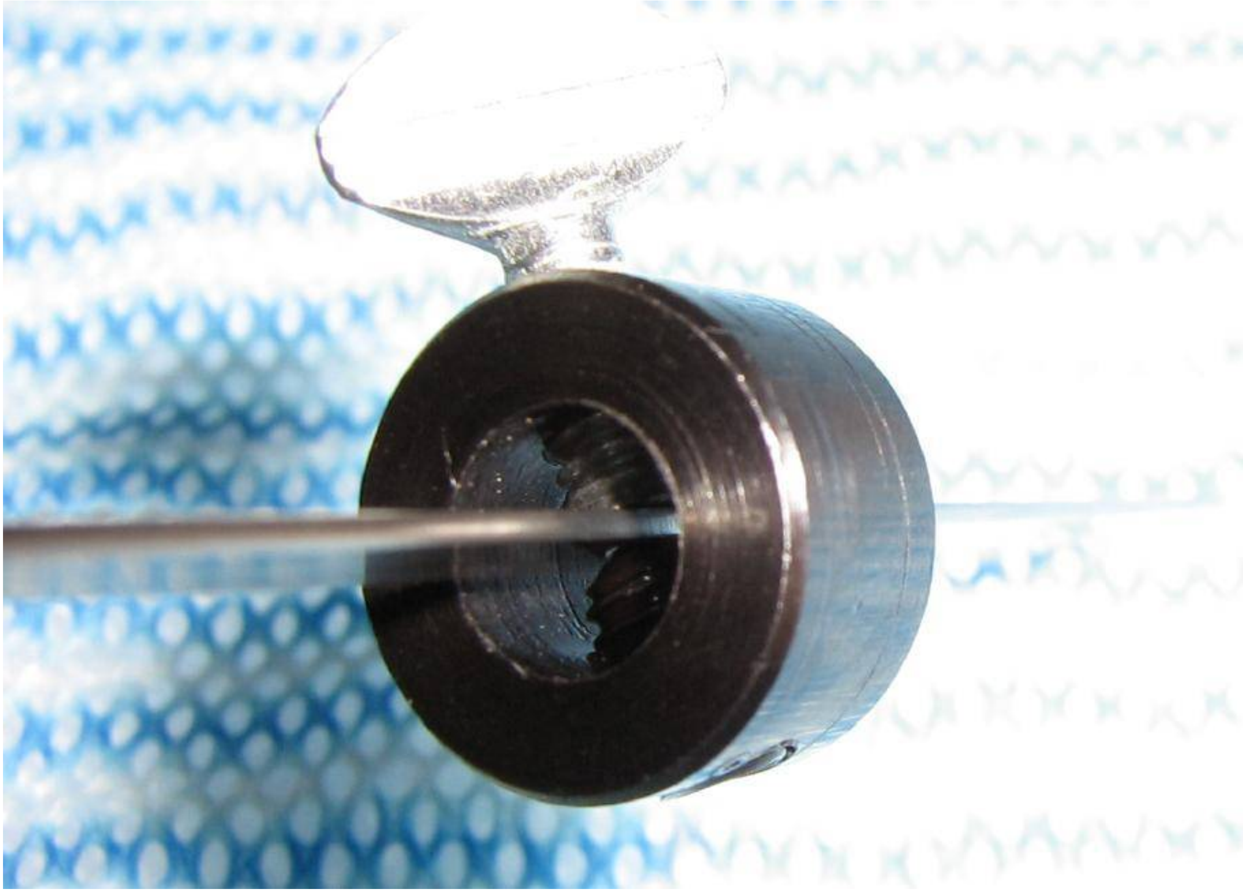
For this project, a 1/4−inch diameter drill stop will be drilled and tapped to hold a #6 size thumbscrew, in addition to the stock set screw. The drill stop can then act as an adjustable "weight" when clamped onto the tension wrench. The set screw on the drill stop does not need to be adjusted and will be held in place with some Loctite.



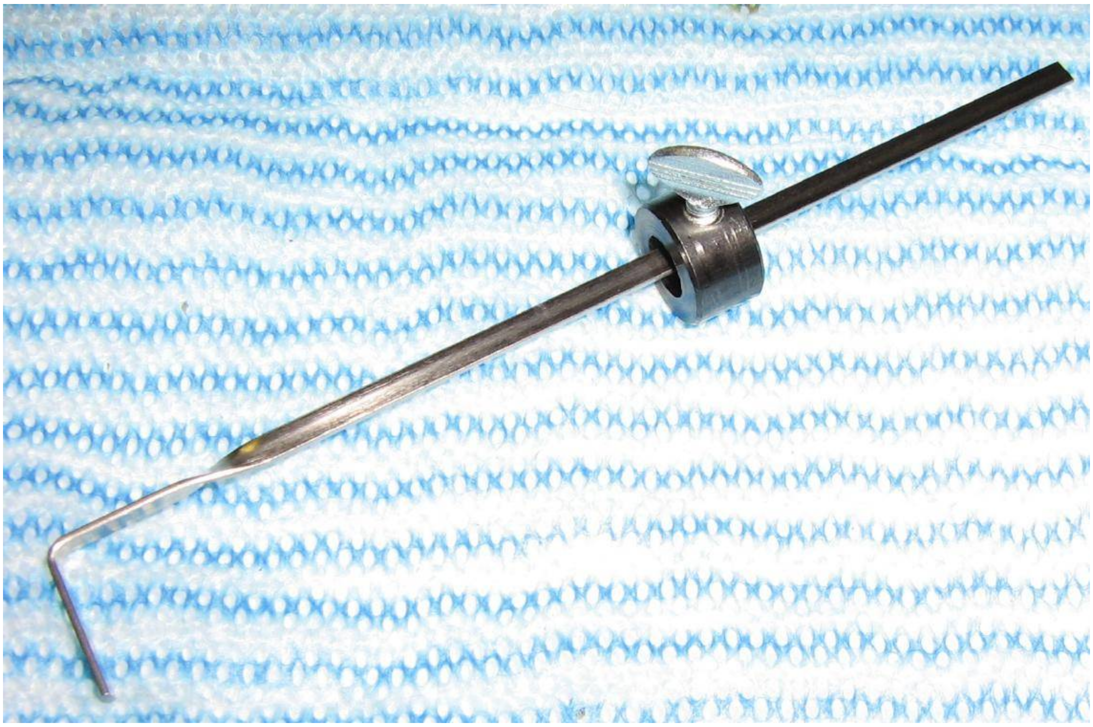
Tools needed. You'll need a #6–32 tap and #36 drill bit for the thumbscrew. Drill and tap on the opposite side of the stock set screw.



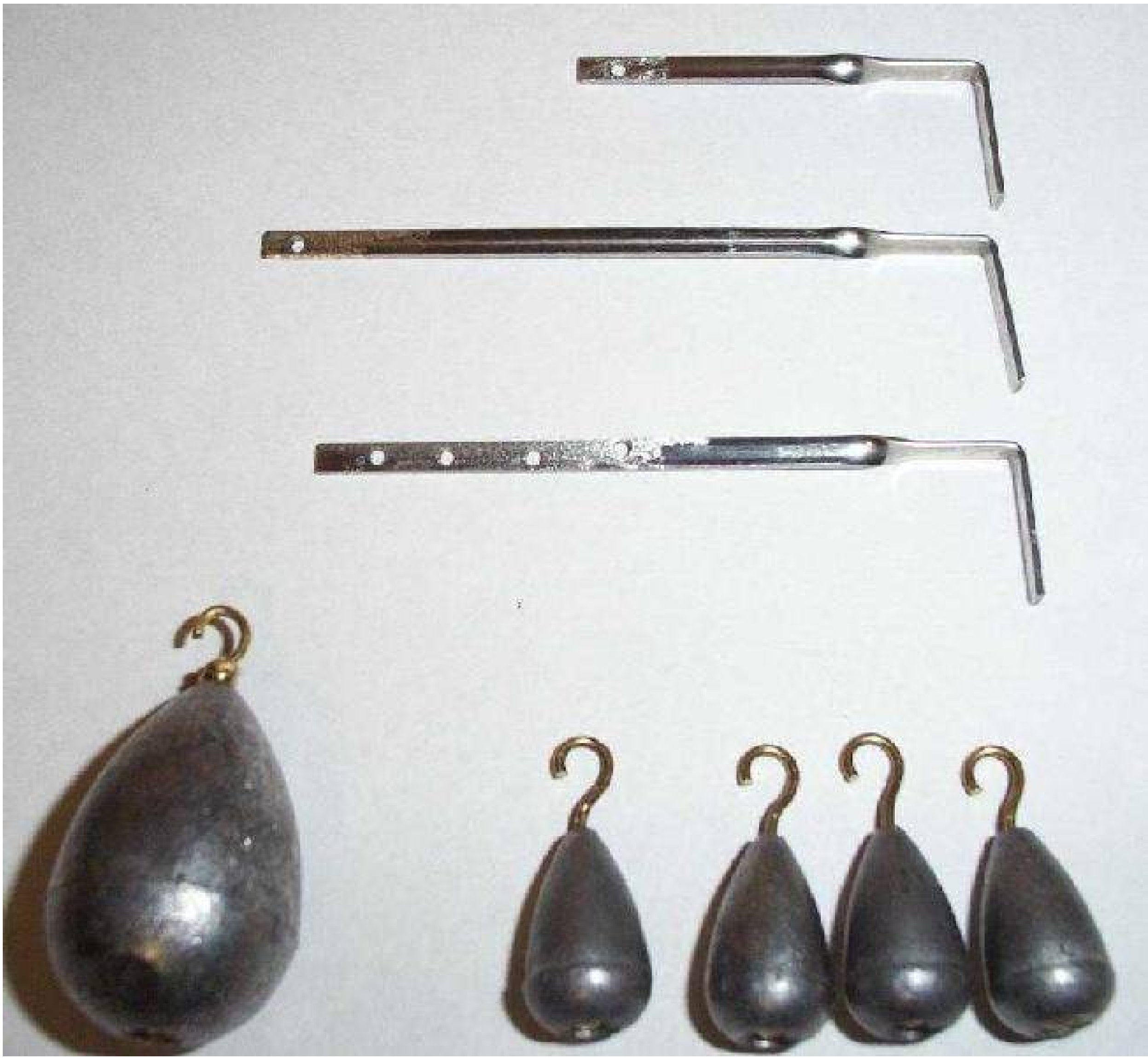
Completed adjustable tension wrench weight. That's all there is!



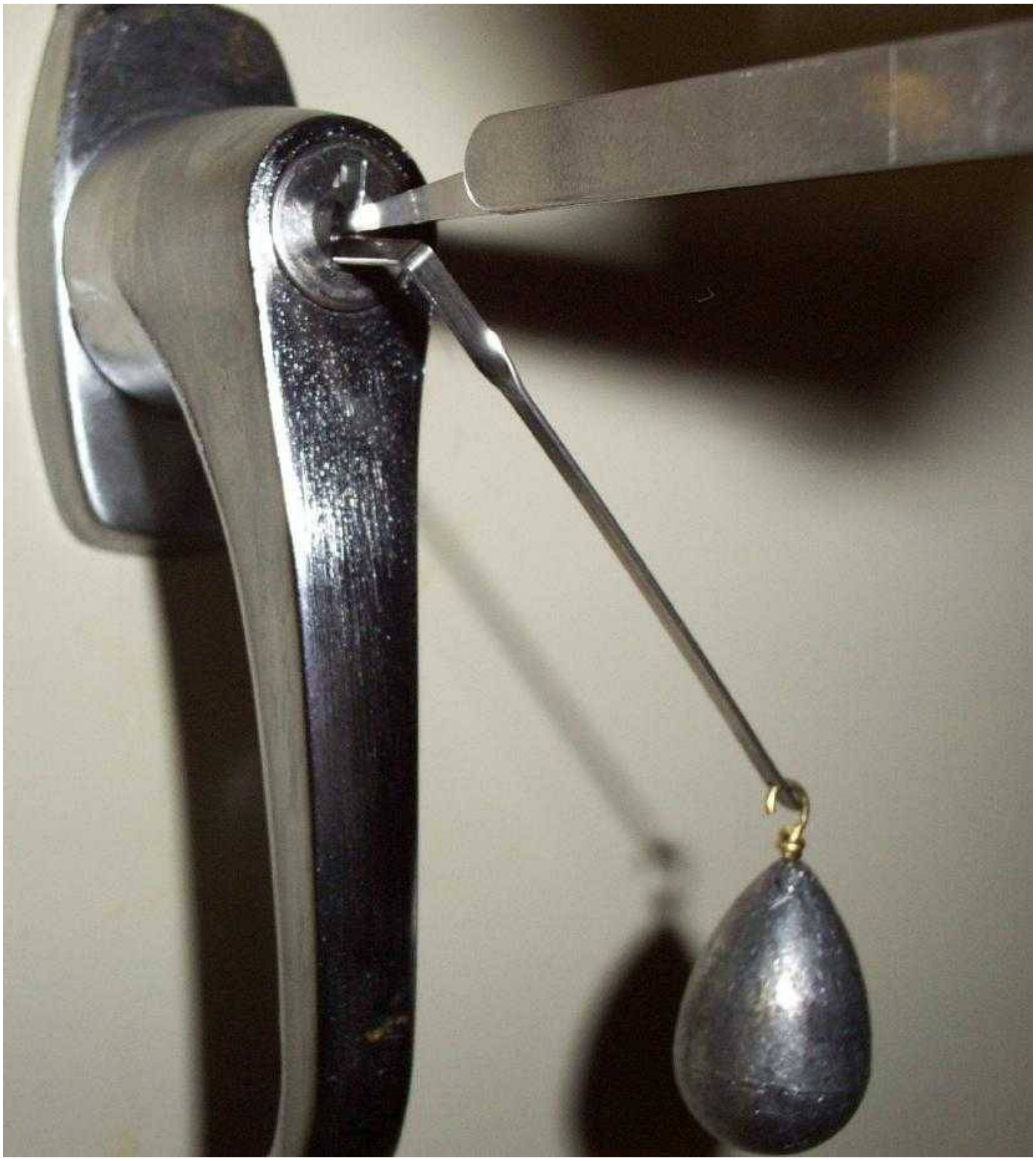
Close up.



In operation. Slide the weight up or down the wrench for the proper turning pressure. Add more weights if you need more pressure.



You can also do the same thing by drilling holes into the tension wrench and adding slightly modified lead fishing sinkers. Trim the eye hooks so they are removable. Experiment with different size sinkers and tension wrench hole positions.



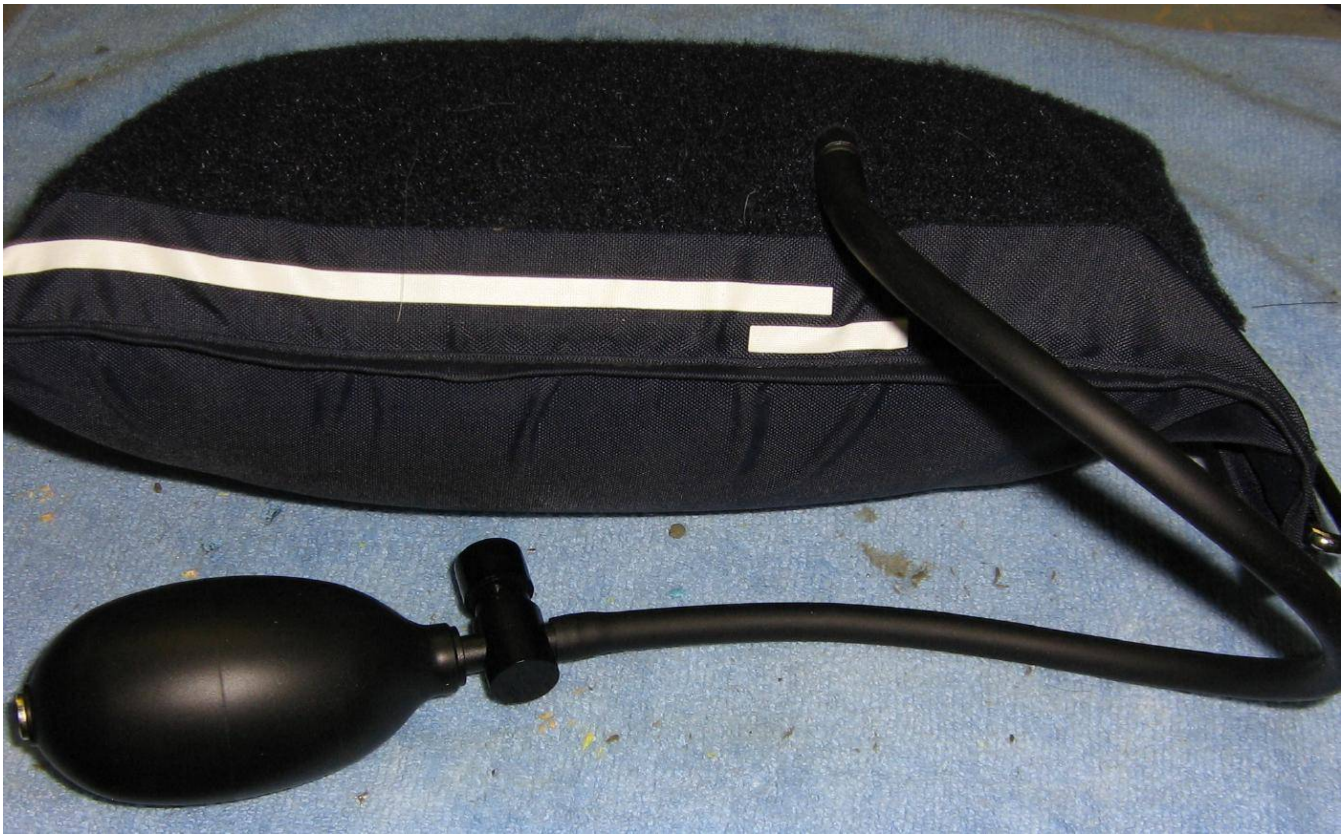
In operation.

Inflatable Blatter

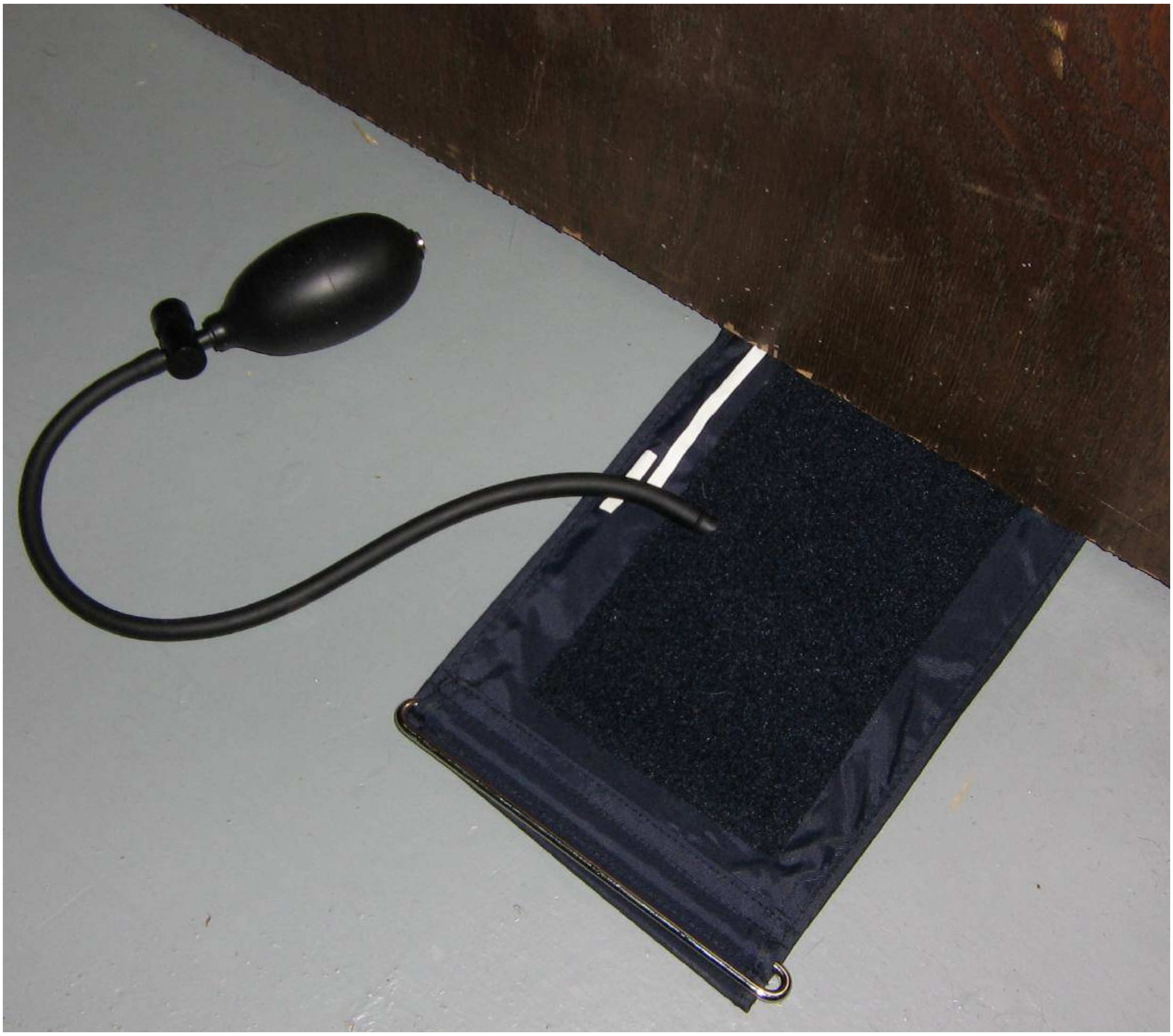
An old inflatable blood pressure monitoring arm cuff can be used as a simple tool to slightly raise closed doors. This is useful if you ever need to slip something underneath a door, and there just isn't enough room. A good example is if you ever need to fill a dorm room with knock–out gas so you can insert a hidden radio receiver inside someone's braces.

This particular blood pressure monitoring cuff has the words "TYPE: ACMNP−1" written on it. The manufacturer is unknown.

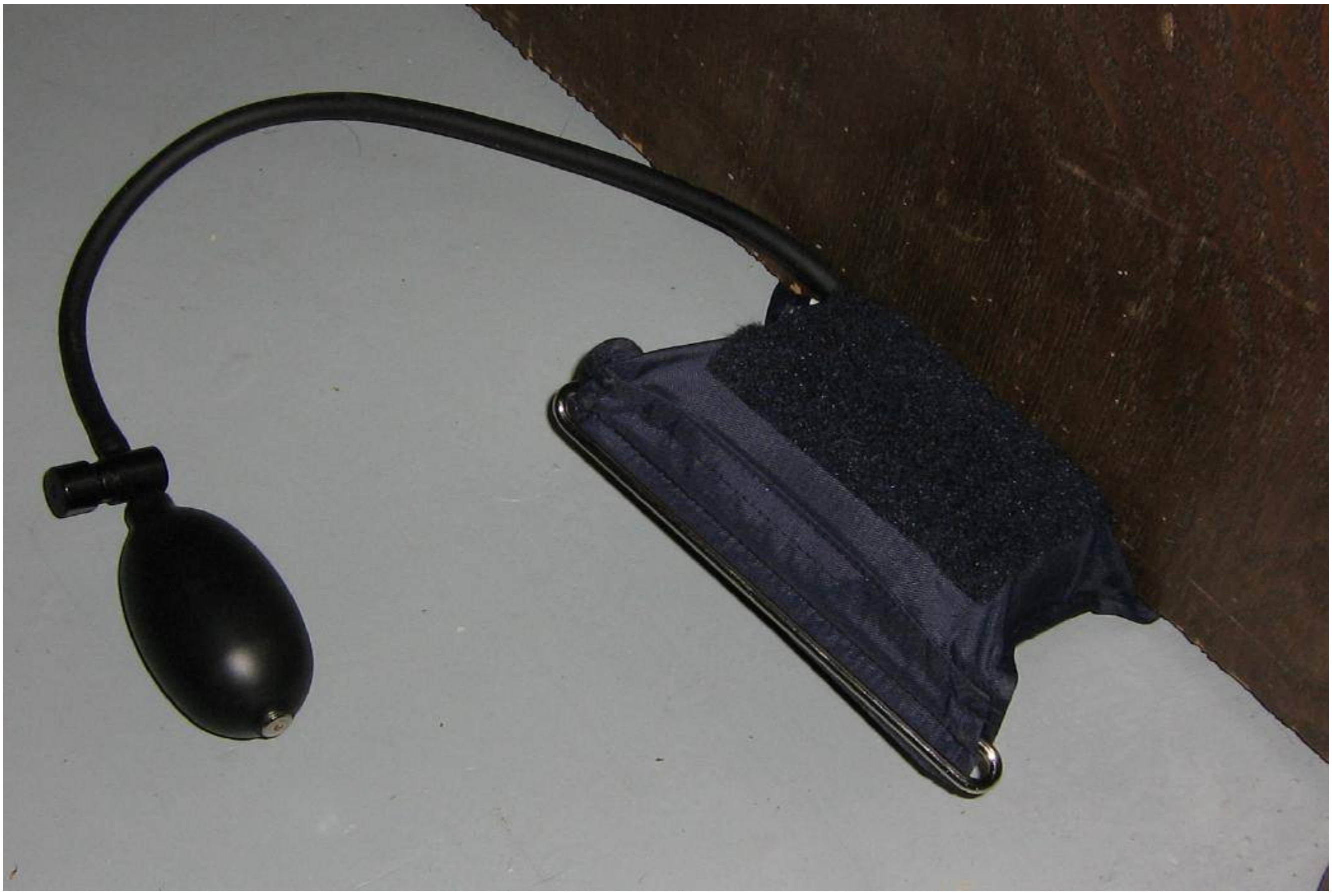
The only real modification, besides removing the electronics and shortening the inflator tube, is to remove the little rubber end piece on the arm cuff. This will allow it to slide more easily underneath doors with a narrow gap.



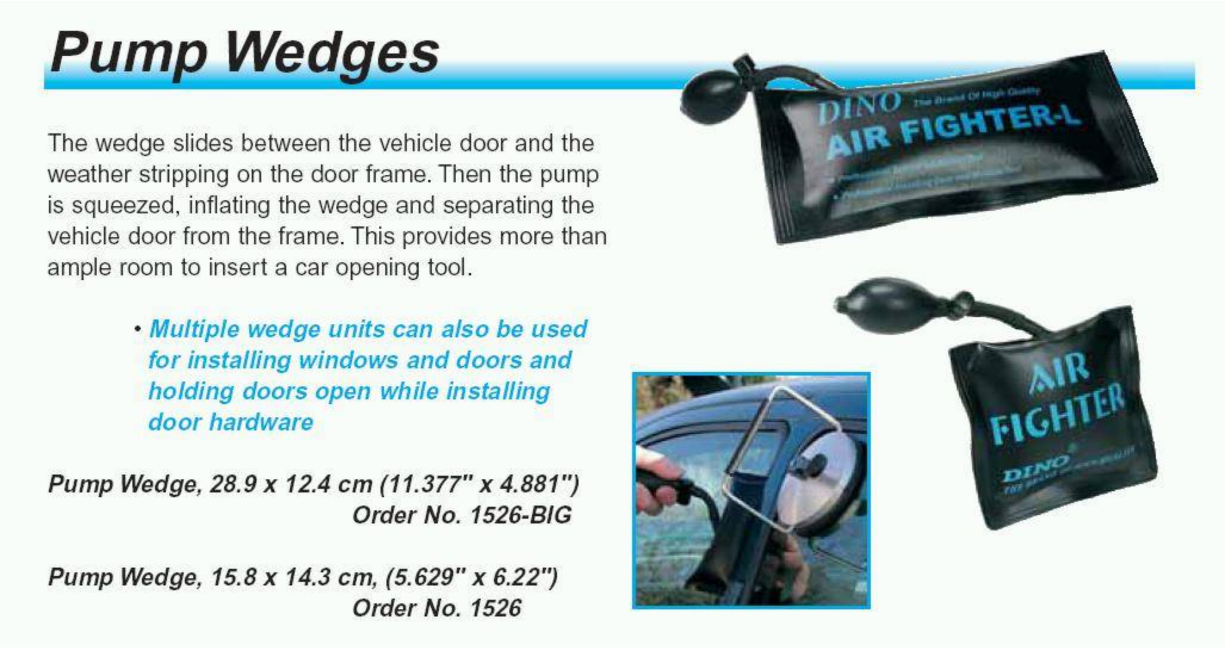
This is what it looks like when inflated. I have no idea what the maxiumum pressure is.



To use it, slide it underneath the door to be lifted. It should be located *away* from the hinge side for maximum "upwards" pressure on the door.



Then start pumping! It does work, but it only raises the door a fraction of an inch.



Pump Wedges

The wedge slides between the vehicle door and the weather stripping on the door frame. Then the pump is squeezed, inflating the wedge and separating the vehicle door from the frame. This provides more than ample room to insert a car opening tool.

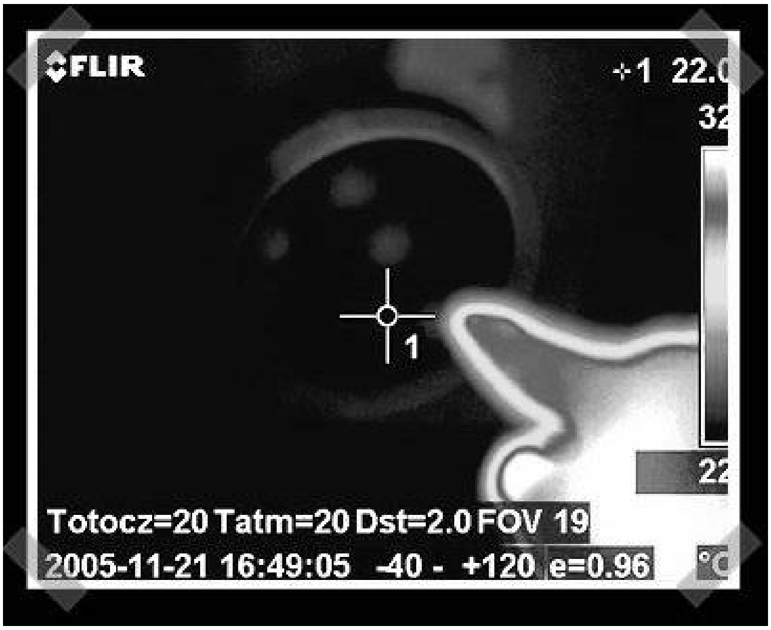
- *Multiple wedge units can also be used for installing windows and doors and holding doors open while installing door hardware*

Pump Wedge, 28.9 x 12.4 cm (11.377" x 4.881")
Order No. 1526-BIG

Pump Wedge, 15.8 x 14.3 cm, (5.629" x 6.22")
Order No. 1526

This is a commercial version of an inflatable blatter.

Thermal Button Pressed Checker Thing


FLIR
1 22.0
32
1
22
Totocz=20 Tatm=20 Dst=2.0 FOV 19
2005-11-21 16:49:05 -40 - +120 e=0.96
°C

About a year ago (November 2005), there was a posting on LED–a–Day about a "Thermal Keypad Combo Snooping" project:

http://www.hackaday.com/2005/11/23/thermal–keypad–combo–snooping/

The project involved using a thermal imaging camera to measure the residual heat signature left on an alarm or safe keypad after a person entered the unlocking code. This is a very clever idea, but thermal imaging cameras are still horribly expensive.

You can experiment a bit with a *much cheaper* alternative. The idea is to use a Cen−Tech Non−Contact Infrared Thermometer (Harbor Freight Tools #93983) to measure the ambient keypad's temperature, then quickly remeasure the key's temperature after it has been pressed. This overall idea still needs a little tweaking, but it does appear to work.

Testing. The Non−Contact Infrared Thermometer is held against a key to measure its ambient temperature, 69.9° F in this case.

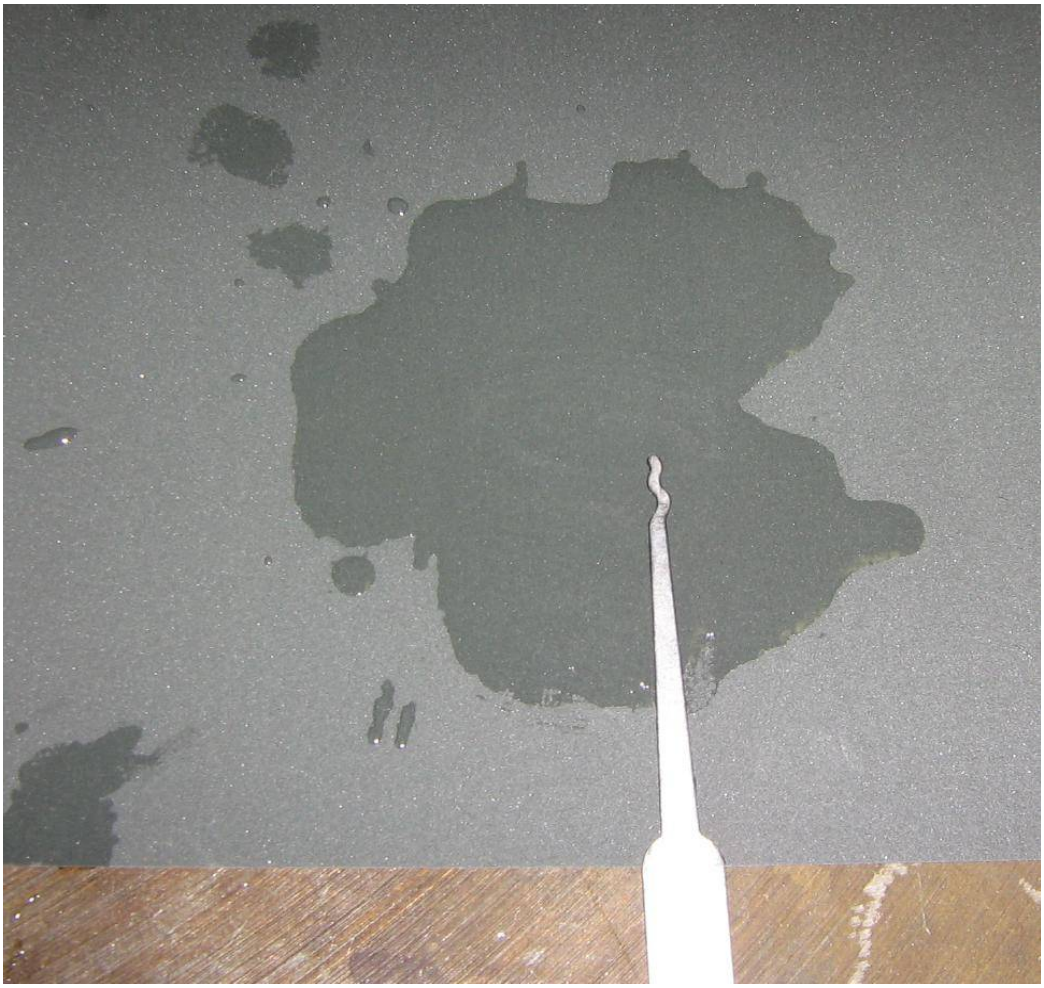
The key was pressed, and the key's temperature is remeasured. It has now risen to approximately 71.7°F. This has to be done very quickly as the key will drop back to room temperature, or to within the thermometer's error margin range, in under two seconds.

Polished Lock Picks

Commercial, mass−produced lock picks are often stamped out of sheet metal. This means they'll have sharp edges which, if not properly sanded down, will catch inside the lock or even, in some cases, leave tell−tale forensic markings inside the lock. For better pick performance and "pick feel" it is a good idea to polish your picks − or at least that has been my experience. Your milage may vary on this one. It may be a good idea to start out practicing on some "cheap" lock picks before destroying your set of Falle−Safe picks.

All you'll need for this one is some 1000 grit wet/dry sandpaper and a Dremel tool with some polishing compound (Dremel Tools #421) and a buffing wheel attachment.

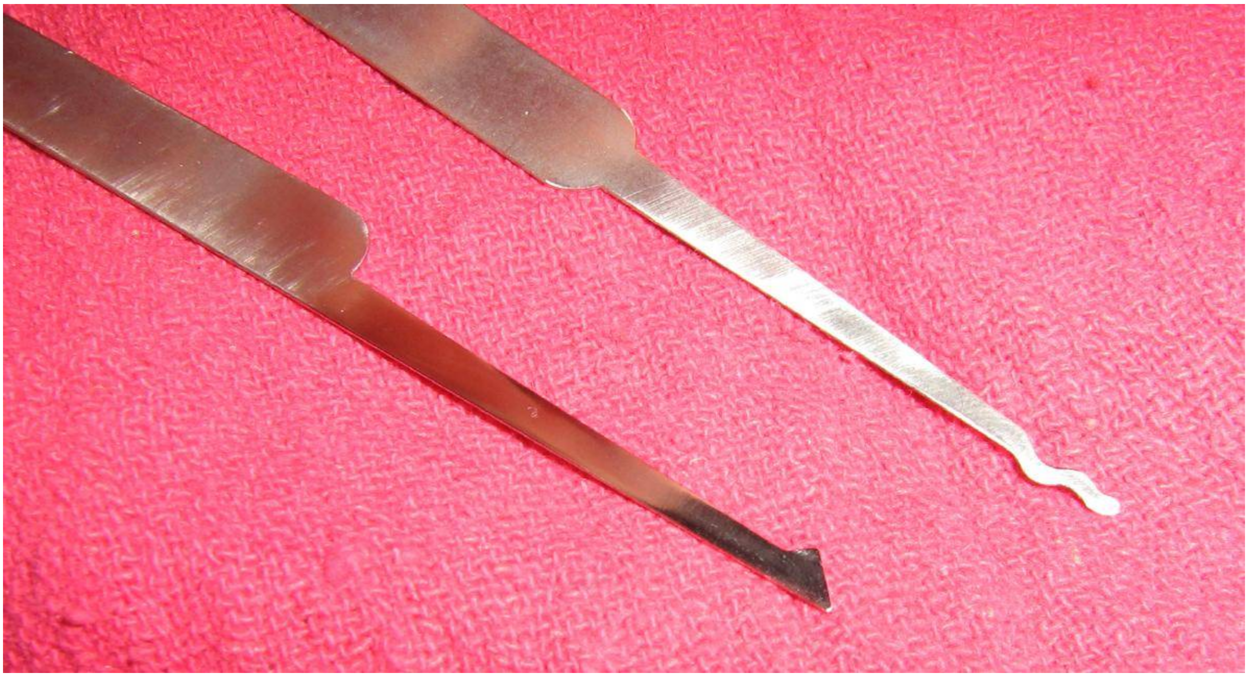
Overview of some stock Southern Ordnance lock picks. Note the fairly sharp edges.



Lightly sprinkle some water onto the 1000 grit sandpaper. Work the lock pick over the sandpaper in a figure−eight pattern being sure to rotate the pick from time−to−time to get both sides. The idea is to remove any "high" spots on the pick's sides while smoothing down the edges.

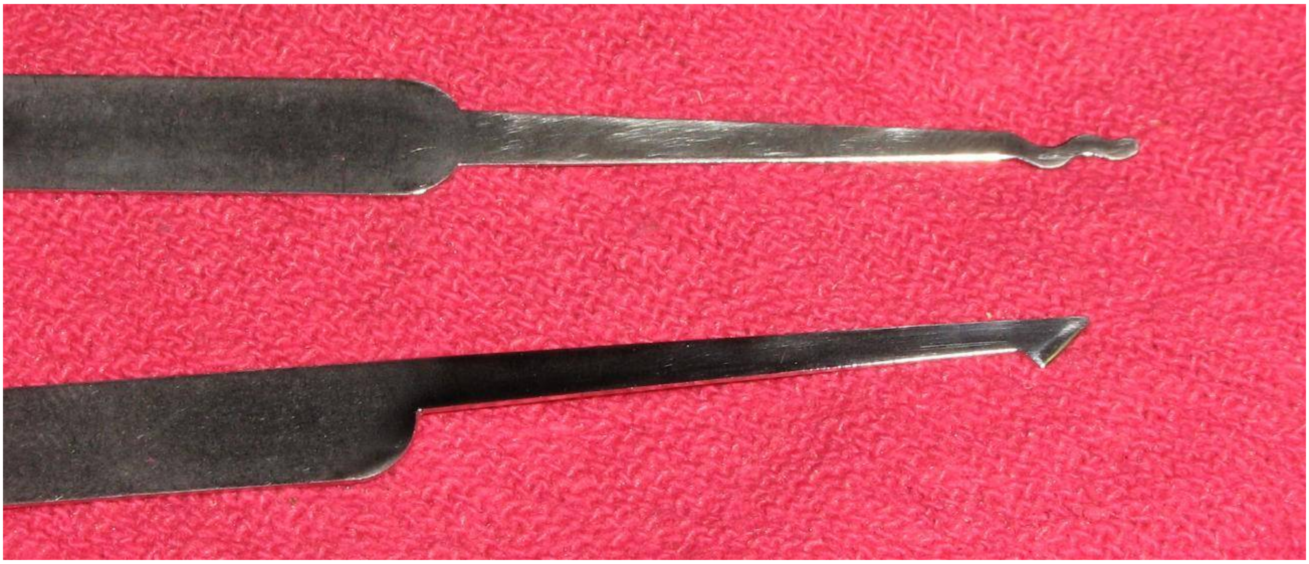
Be sure to do this on a very flat and sturdy surface.

Picture showing some of the high spots being removed from the lock pick. Note the sanded areas near the tip of the lock pick.



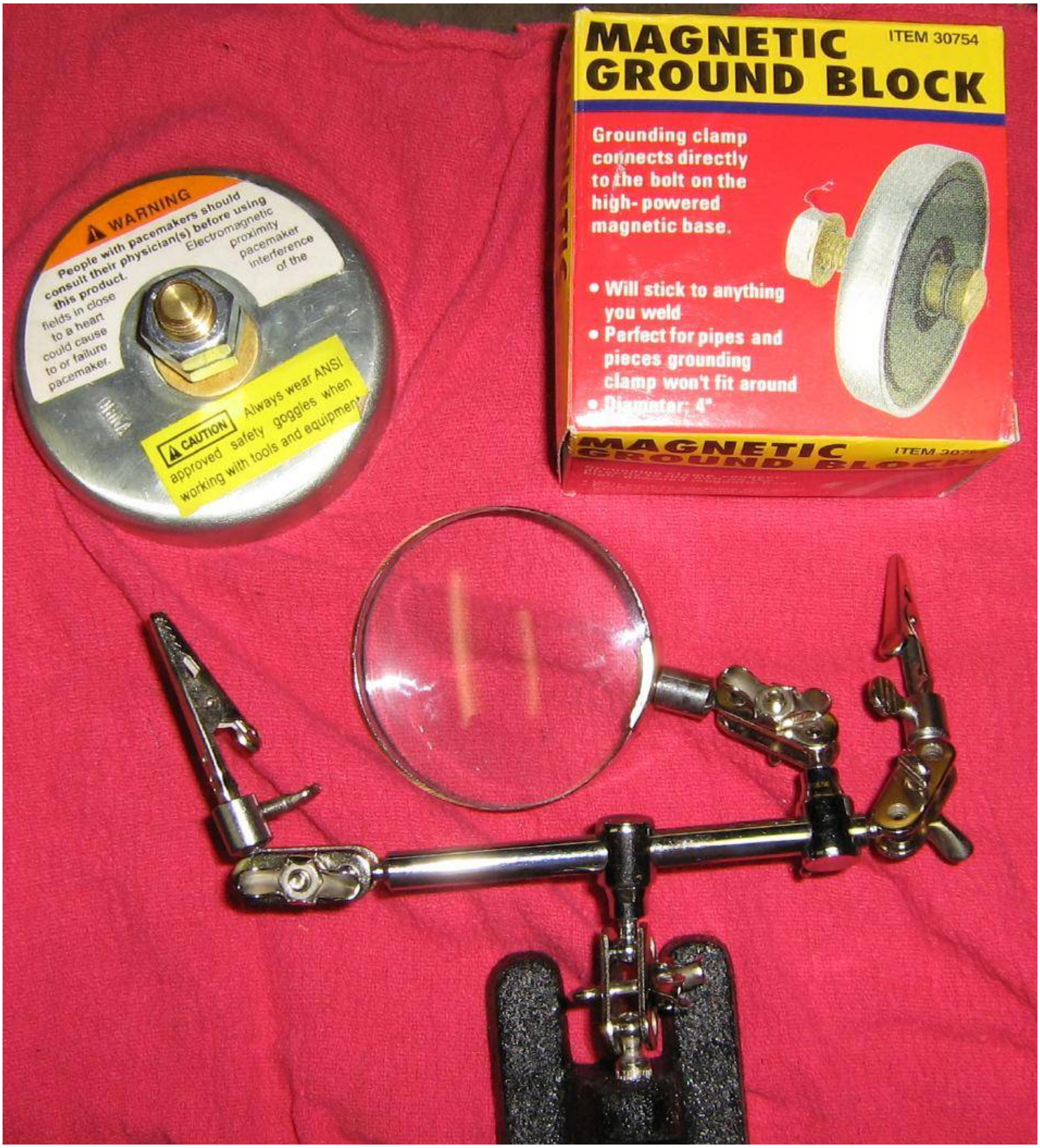
After the pick has been sanded, you can then perform the final step of polishing the pick to a mirror–like finish. Apply some polishing compound to the buffing wheel in the Dremel tool and lightly work both sides of the lock pick.

The top pick in this above picture is a stock pick, the one below it has been polished to nearly a mirror finish.



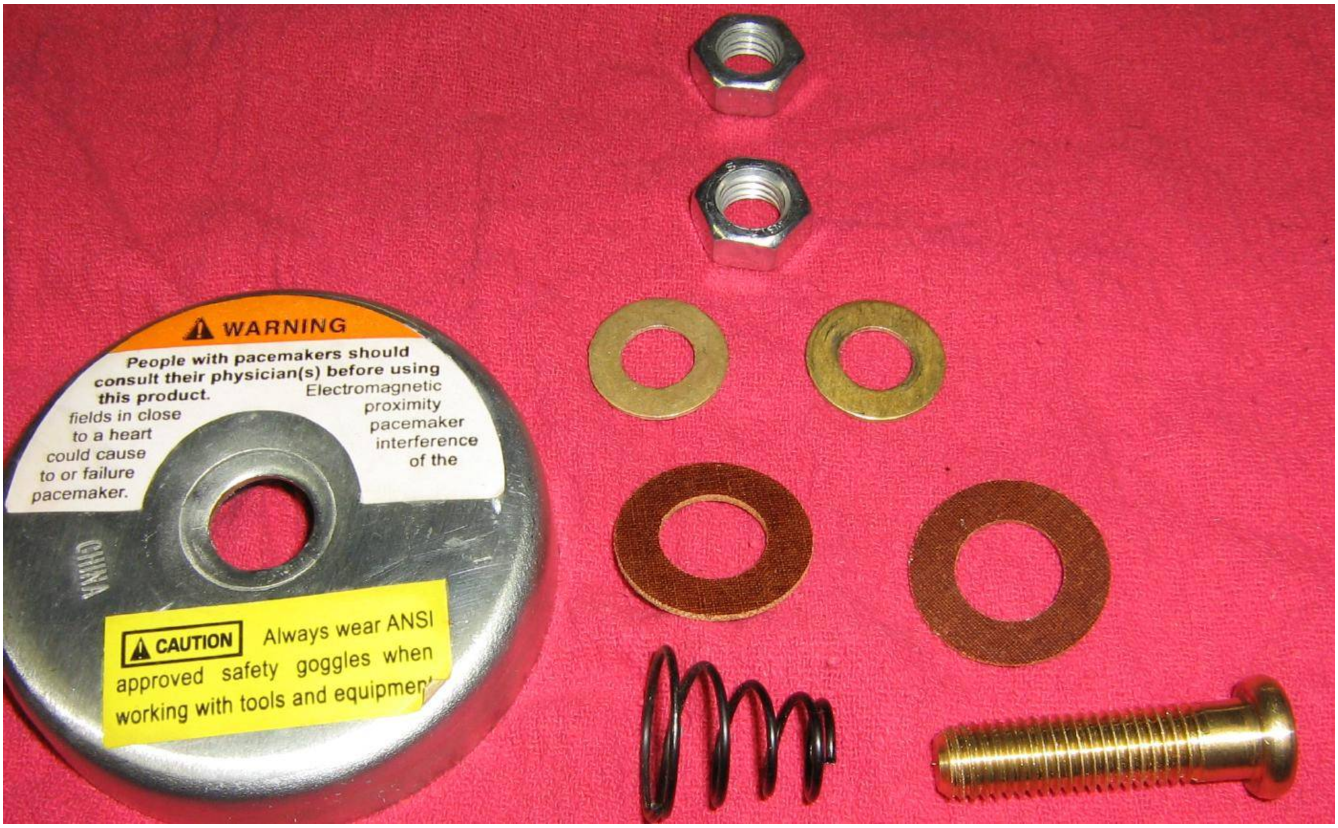
Alternate view. Stock lock pick on top.

Safe Dial Magnifier

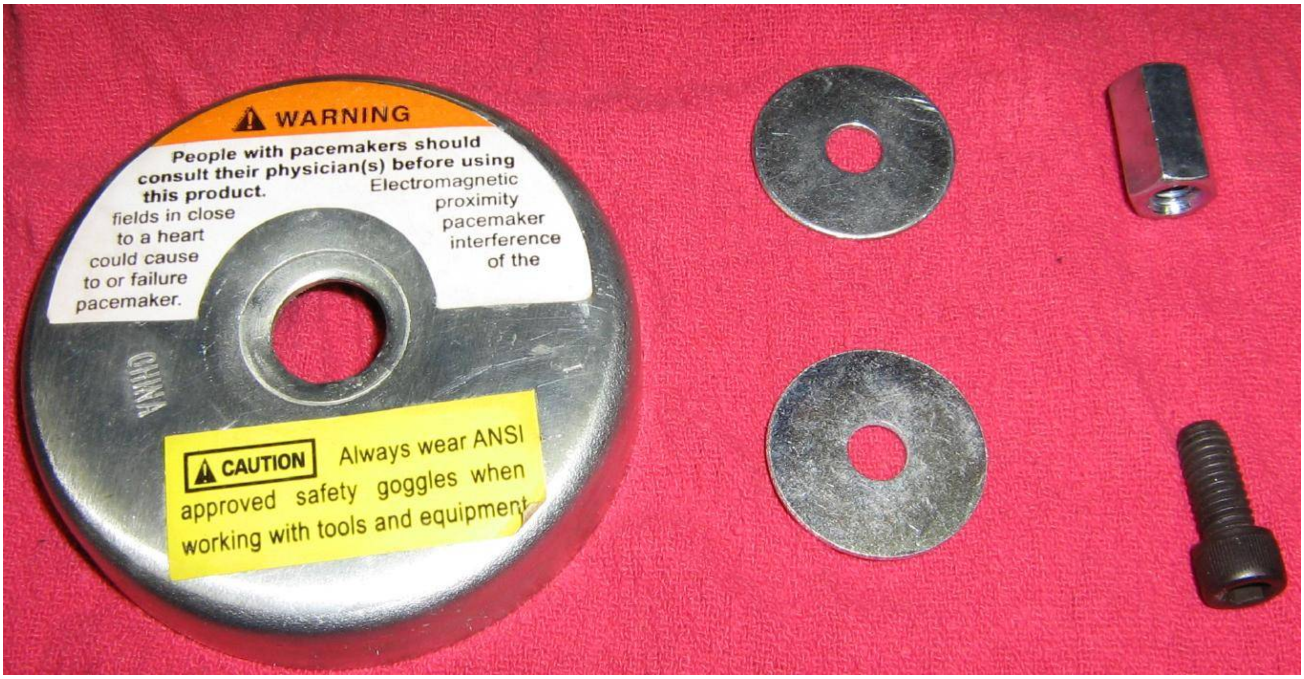

MAGNETIC GROUND BLOCK
ITEM 30754
Grounding clamp connects directly to the bolt on the high-powered magnetic base.
• Will stick to anything you weld
• Perfect for pipes and pieces grounding clamp won't fit around
• Diameter: 4"
WARNING
People with pacemakers should consult their physician(s) before using this product. Electromagnetic fields in close proximity to a heart pacemaker could cause interference to or failure of the pacemaker.
CAUTION Always wear ANSI approved safety goggles when working with tools and equipment
CHINA

A useful tool when cracking "analog" safes is a simple magnetic−mount magnifying glass. This is then placed over the safe's dial to aid in manipulation.

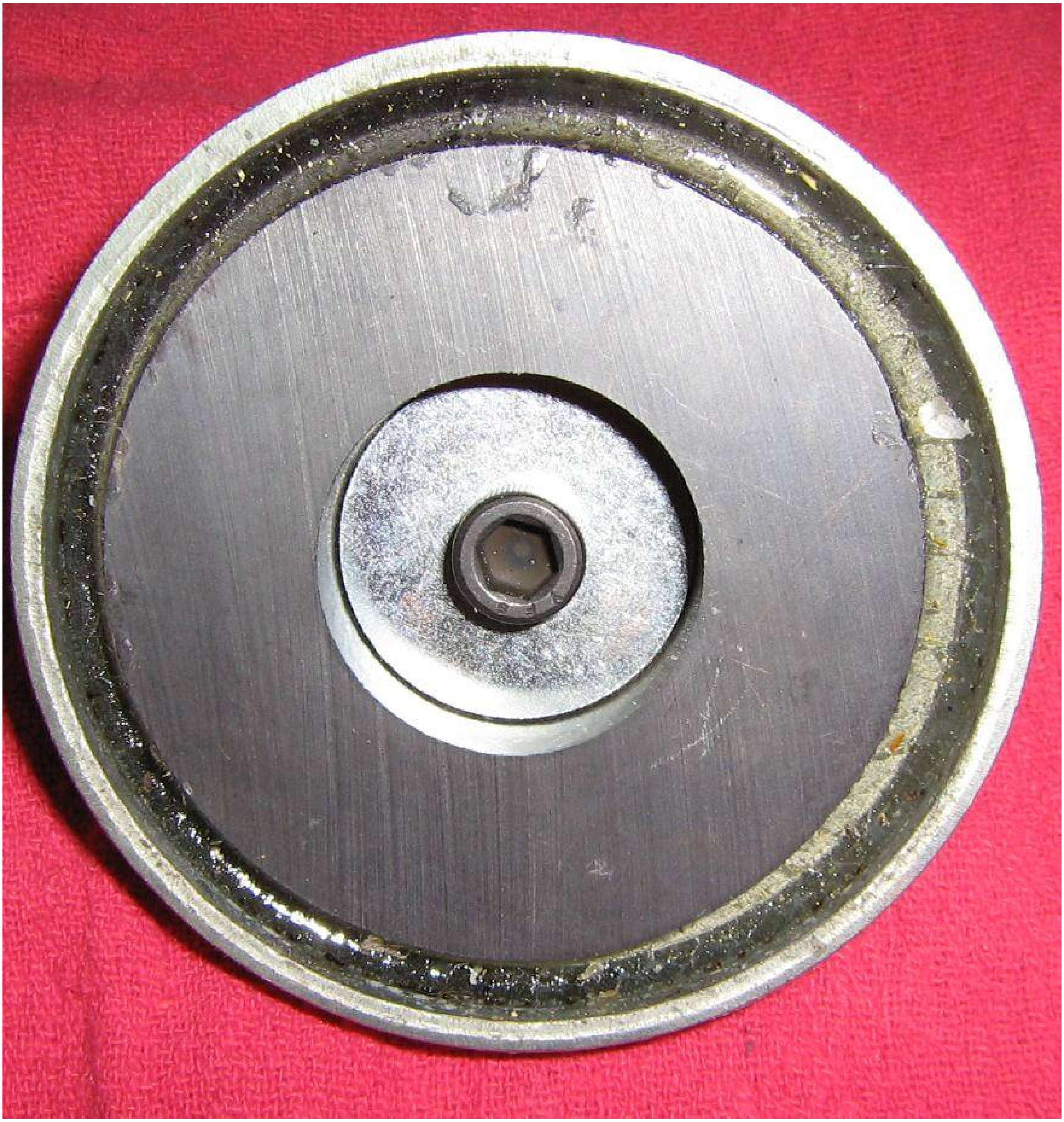
Commercial magnetic−mount magnifiers exist, but the magnetic mount is often not very powerful. This version will use a *very powerful* welding Magnetic Ground Block, which is also available from Harbor Freight Tools (#30754). The magnetic base is 3.5−inches in diameter and can probably handle ten pounds of weight with no problems. You will also need one of those "Helping Hands" tools with the magnifying glass attachment (Harbor Freight Tools #319).



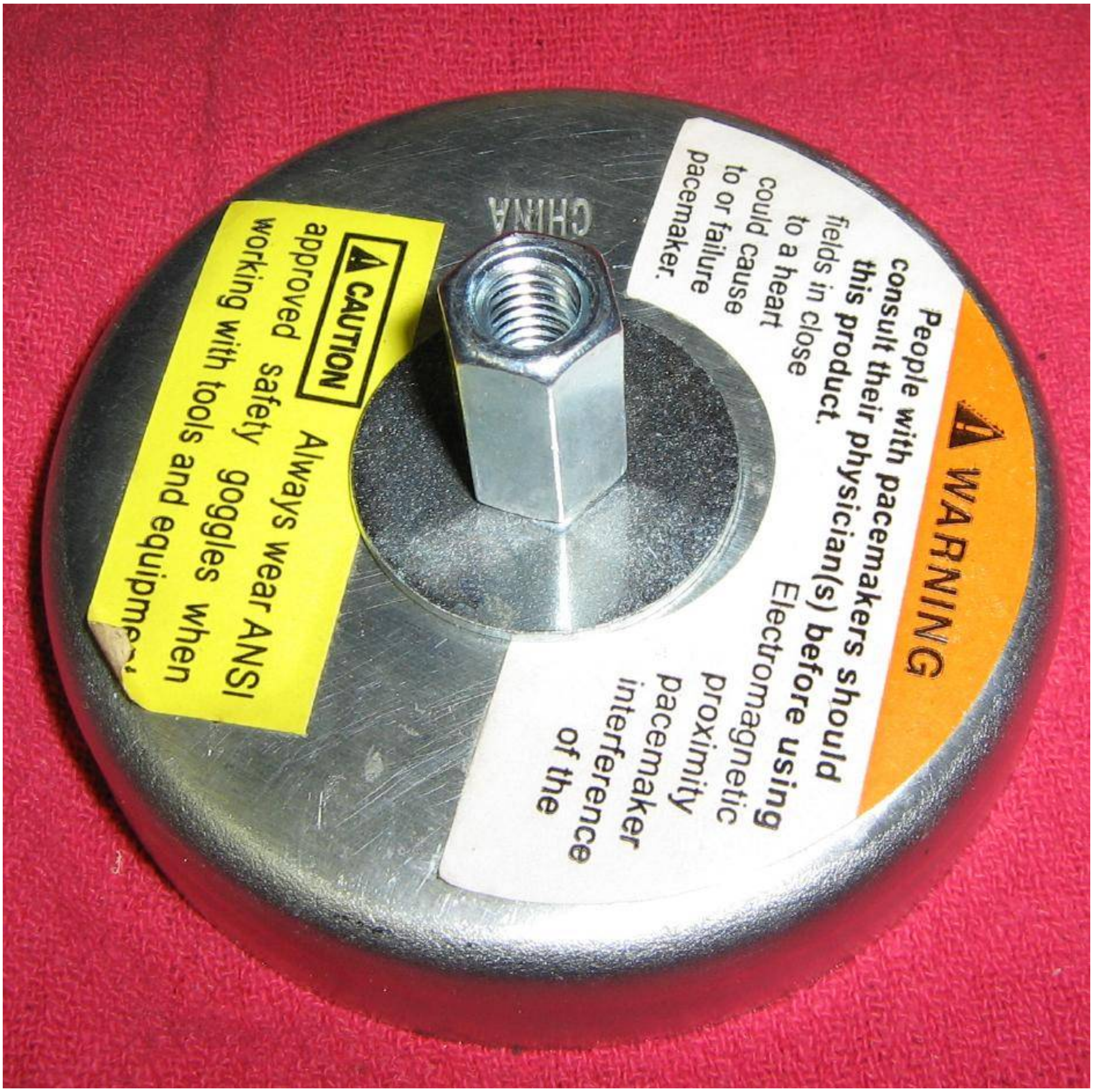
Start by taking the Magnetic Ground Block apart. You'll just need the magnetic base for this project. You may wish to remove all the stupid stickers to make it look pretty.



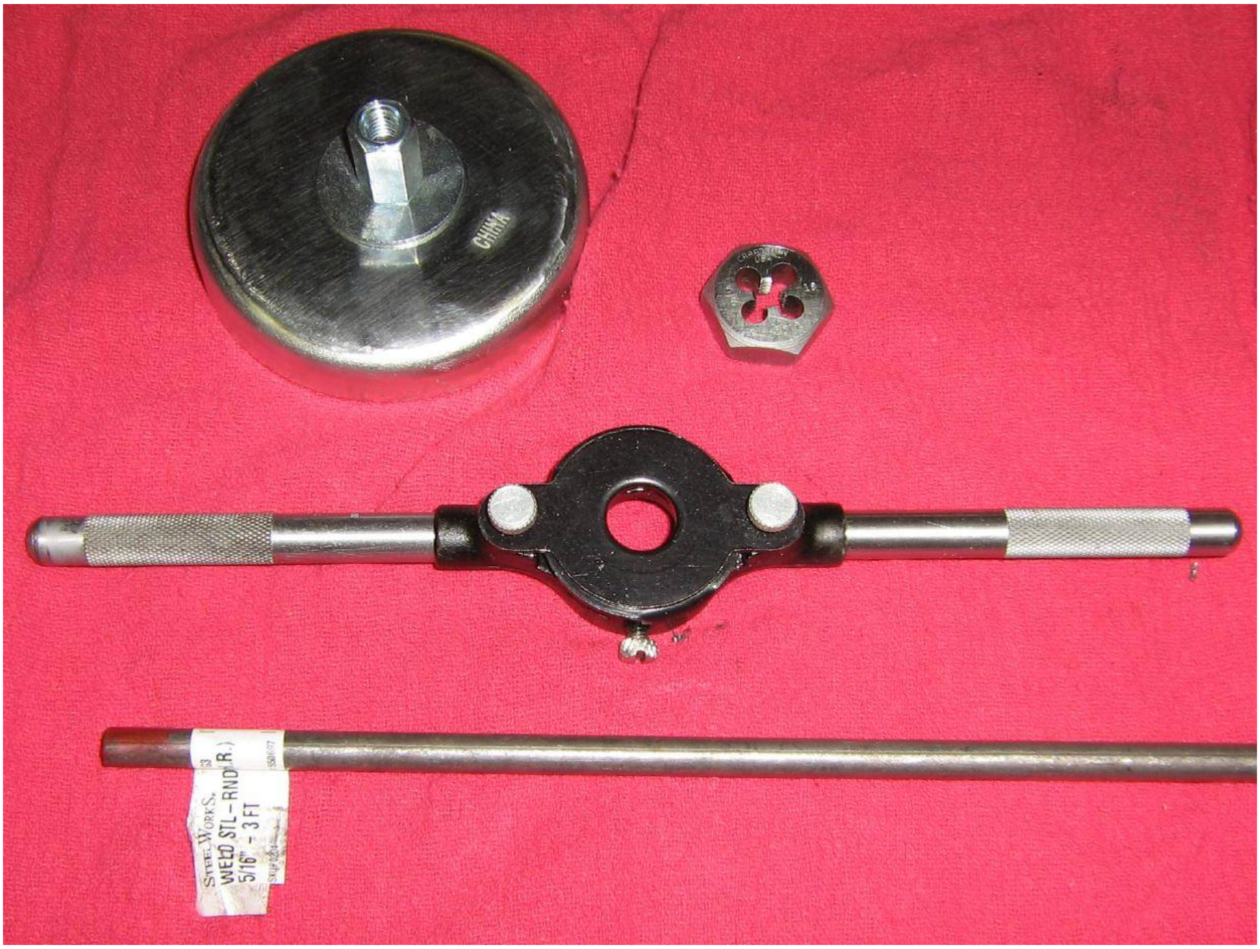
Then get two 1.25–inch outside diameter (5/16–inch inside diameter) fender washers, a 5/16–inch coupling nut, and an inch long 5/16 bolt.



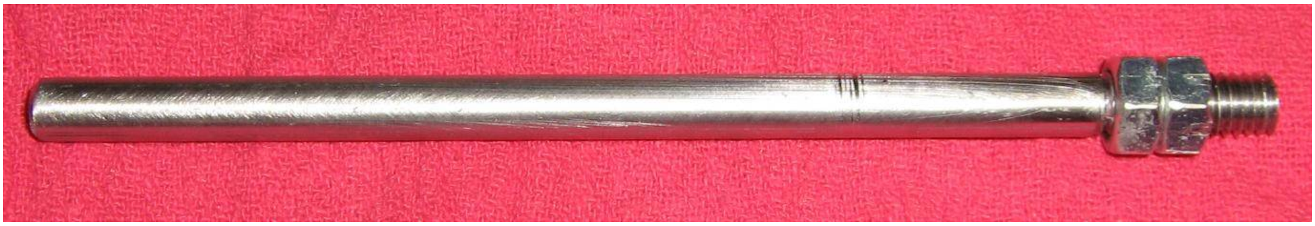
Bottom view. Put it together like this with one fender washer on top and one on the bottom with the coupling nut and bolt holding everything together. Secure everything very tightly.


CHINA
WARNING
People with pacemakers should
consult their physician(s) before using
this product. Electromagnetic
fields in close proximity
to a heart pacemaker
could cause interference
to or failure of the
pacemaker.
CAUTION Always wear ANSI
approved safety goggles when
working with tools and equipme

Top view.

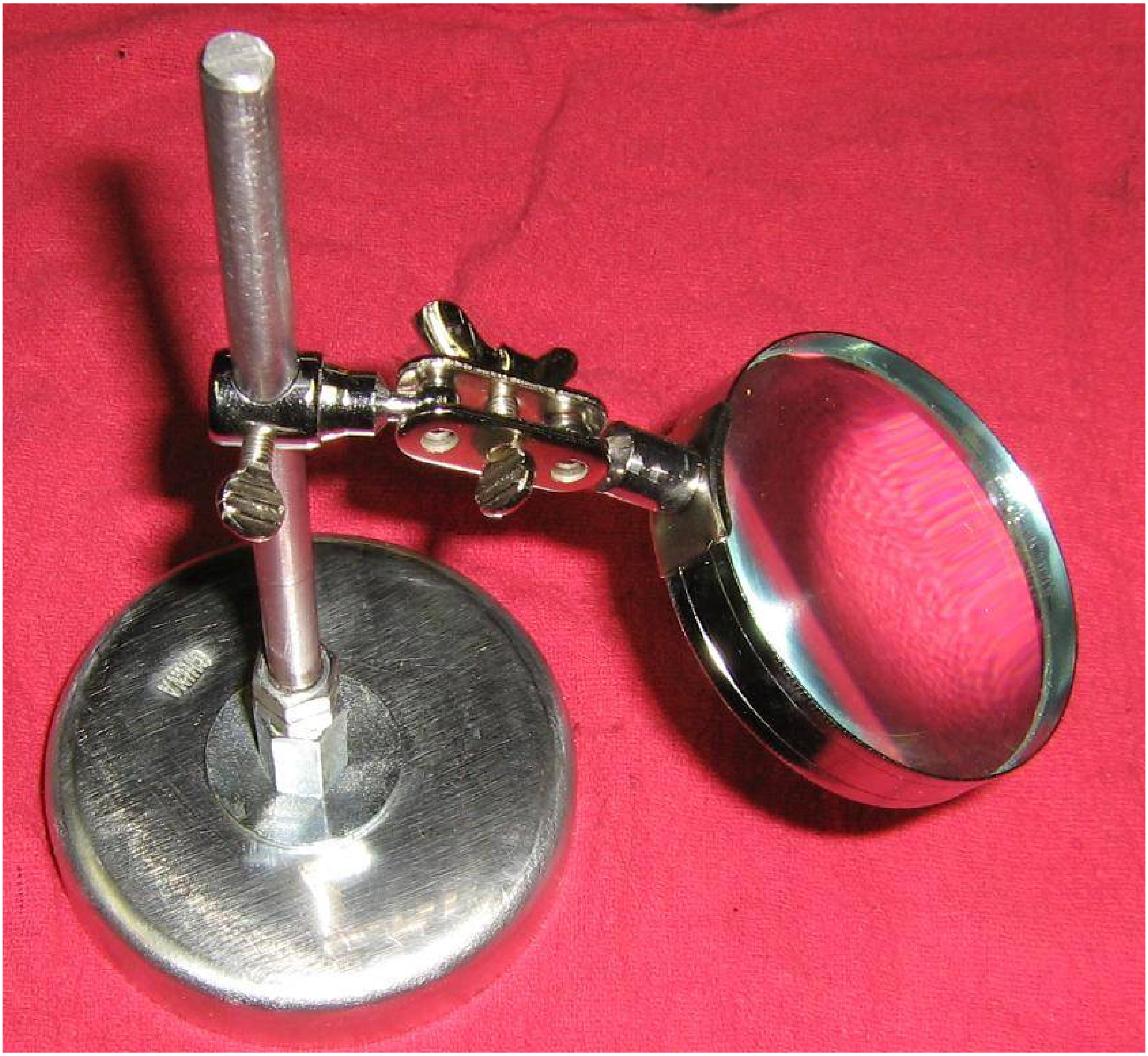


Next, get a six inch long piece of 5/16–inch diameter steel rod and a 5/16–18 thread die. You'll need to thread one end of the steel rod to screw inside the coupling nut.



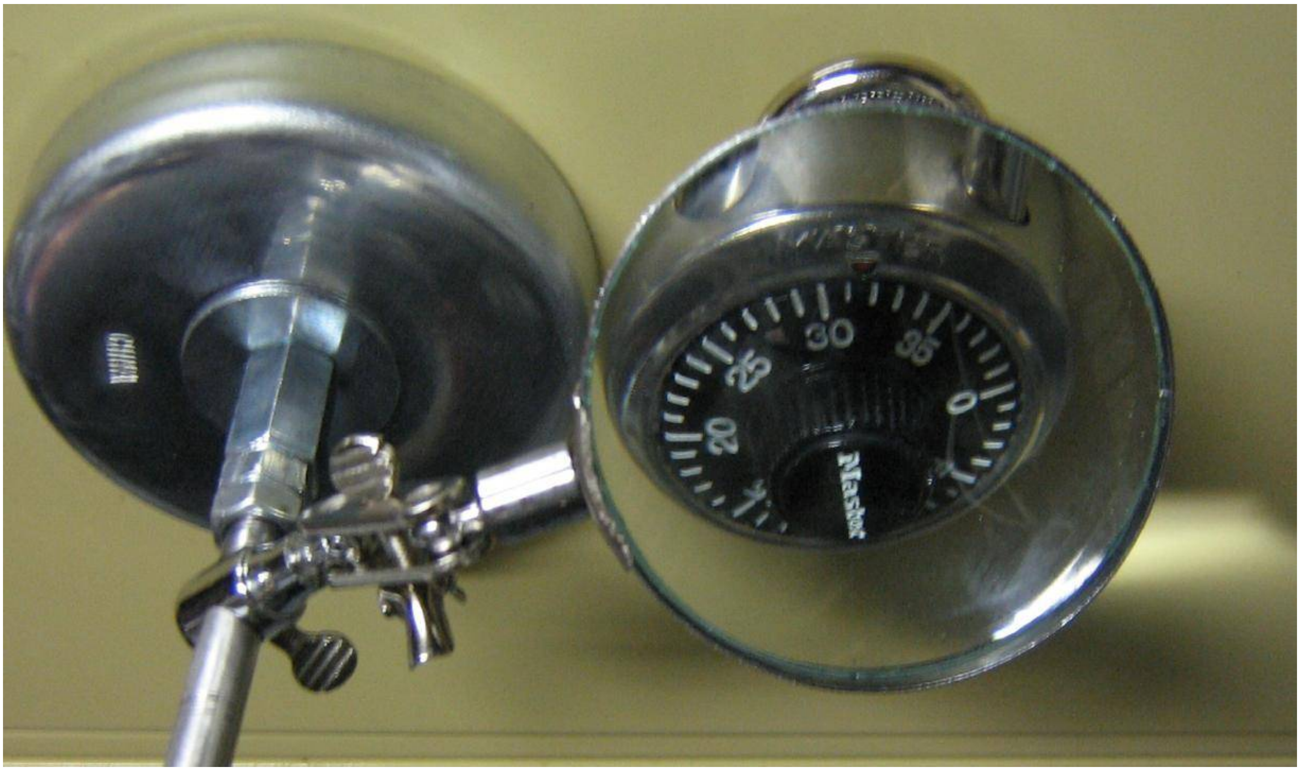
It should look something like this when finished. Use two "jam" nuts on the threaded end to secure the rod into the coupling nut. You will also want to polish the steel rod with some fine sandpaper or steel wool.

Remove the magnifying glass attachment from the Helping Hands tool. You may wish to replace the magnifying glass with one of much higher glass quality or magnification.



Screw the steel rod into the magnetic base and slide the magnifying glass attachment onto the rod. Lock it into place with the thumbscrew.

You can use the other parts from the Helping Hands tool if you need an extenstion.



Don't have a safe on hand, but I can glue a Master lock to a filing cabinet.

Bonus

End of Issue #32

Any Questions?

Editorial and Rants

More proof "multinational" forces don't work.

Kill all Eurosavages.

Confronted by the Islamist Threat on all Sides, Europe Pathetically Caves In

September 22, 2006 – *From:* *www.timesonline.co.uk*

By Gerard Baker

LATE LAST YEAR, at the invitation of Nato, and in the company of a small band of globetrotting pundits, I travelled to Afghanistan to witness first–hand the allied operation to reconstruct the benighted country.

After a day of briefings in Kabul, our friendly Nato hosts flew us by military transport to Herat, on the western border with Iran. We were due to spend a day touring a Nato post in the city and then fly back that evening to the capital. But the Danish plane that had taken us developed propeller problems and was grounded. As we cooled our heels outside the airfield , we waited for word of the aircraft that was supposed to come for us: a German C–130.

It soon became clear that the replacement plane was not coming. The reason, it turned out, was that the Germans would not fly in the dark. German aircraft are not permitted by their national rules to undertake night flights.

Now to those who survived the Blitz and Barbarossa, the news that today's Luftwaffe will not fly at night in potentially hostile environments might be regarded as a welcome historical development. But when you are trying to fight a war against a ruthless band of terrorists who operate 24/7, never pausing to consider the dangers of venturing out in the dark, limiting yourself to daytime operations is a little constraining.

The Germans are not alone. Many of the European nations with forces in Afghanistan are operating under similarly ludicrous restrictions. Though their soldiers and airmen are highly capable and indeed eager to take the fight to the Taleban, their governments are desperately fearful of the public reaction should their soldiers suffer significant casualties. They don't think that their voters will stomach it. And the tragedy is, they are probably right.

I was reminded of my unscheduled night in Herat, and what it said about Europe's dwindling commitment to its own survival, by a series of disheartening developments in the past week on the political and diplomatic front.

Last week we had the tragicomic spectacle of European Nato countries lining up to decline politely the request to beef up their forces in Afghanistan, many of whom are now fighting in perilously under−resourced conditions against a resurgent enemy.

Then on Monday Jacques Chirac went to New York to upend the long, delicate diplomacy designed to deny Iran nuclear weapons. He said France no longer thought the UN should impose sanctions if Iran did not end its uranium enrichment programme.

Various explanations were offered by commentators for this volte−face −− from the thought that France might be fearful of the economic consequences of sanctions, to the possibility that M Chirac was trying to curry favour with sanctions−opposing Russia and China, to the suggestion that Paris worries that its new peacekeeping force in Lebanon might come under fire from Hezbollah if France acted tough with its Iranian sponsors.

Whatever the proximate cause of this latest French surrender, the basic reality is that Europeans have been extremely reluctant to press Iran with sanctions all along −− the same noises are coming out of Berlin now −− and are content instead to acquiesce in the nightmare of a nuclear−armed Tehran.

Then, of course, we have had the predictable European outrage following the latest apparent provocation of Islamic extremists by free speech in the West −− Pope Benedict XVI's remarks last week on Islam.

I actually heard a senior member of the British Government chide the Pope this week for what he described as his unhelpful comments. This minister went on to say that the Pope should keep quiet about Islamic violence because of the Crusades.

It was a jaw−dropping observation. If it was meant seriously its import is that, because of violence perpetrated in the name of Christ 900 years ago, today's Church, and presumably today's European governments (who, after all, were eager participants in the Crusades) should forever hold their peace on the subject of religious fanaticism. In this view the Church's repeated apologies for the sins committed in its name apparently are not enough. The Pope has no right, even in a lengthy disquisition on the complexities of faith and reason, to say anything about the religious role in Islamic terrorism.

It is apt that Pope Benedict should have received such European opprobrium for his remarks. His election last year looked like a final attempt by the Church to revive the European spirit in the face of accelerating secularisation and cultural morbidity.

But the scale of Europe's moral crisis is larger than ever. Opposing the war in Iraq was one thing, defensible in the light of events. But opting out of a serious fight against the Taleban, sabotaging efforts to get Iran off its path towards nuclear status, pre–emptively cringing to Muslim intolerance of free speech and criticism, all suggest something quite different.

They imply a slow but insistent collapse of the European will, the steady attrition of the self–preservation instinct. Its effects can be seen not only in the political field, but in other ways –– the startling decline of birth rates across the continent that represent a sort of self–inflicted genocide; the refusal to confront the harsh realities of a global economy.

It may well be that history will judge that Europe's decline came at the very moment of its apparent triumph. The traumas of the first half of the 20th century have combined with the economic successes of the second half to induce a collective loss of will. Great civilisations die not in the end because of external force majeure but because internally the will to thrive is sapped.

The symptoms of this moral collapse may be far away from the affluent and still largely peaceful cities and towns of the old continent –– in the mountains of Afghanistan, the diplomatic reception halls of Tehran and the angry Pope–effigy–burning streets of the Middle East. But there should be no doubt that it is closer to home where the disease has taken hold.

You didn't see this on CNN!

Kill all Eurosavages.

Iraqi Report Could Prove Damaging to Germany

December 17, 2002 – *From:* www.dw–world.de

Just as the heated debates within the German government over the role of German troops and equipment in a possible war against Iraq seem to be cooling down, another potential bombshell threatens to reignite the fires.

On Tuesday, the Berlin–based left–wing paper, Tageszeitung reported that aspects of the 12,000–page Iraqi report on Iraq's weapons programs, submitted to the U.N. last week, could prove highly embarrassing for Germany.

The newspaper – believed to be the first to have access to the top–secret dossier – has written that the Iraqi declaration contains the names of 80 German firms, research laboratories and people, who are said to have helped Iraq develop its weapons program.

Germany, Iraq's number one arms supplier?

The most contentious piece of news for Germany is that the report names it as the number one supplier of weapons supplies to Iraq. German firms are supposed to easily outnumber the firms from other countries who have been exporting to Iraq.

They have delivered technical know–how, components, basic substances and even entire technical facilities for the development of atomic, chemical and biological weapons of mass destruction to Iraq right since 1975.

In some cases, conventional military and technical dealings between Germany and Iraq are said to date till 2001, ten years after the second Gulf war and a time when international sanctions against

Saddam Hussein are still in place.

The paper reports that the dossier contains several indications of cases, where German authorities right up to the Finance Ministry tolerated the illegal arms cooperation and also promoted to it to an extent.

Wait and watch says German Finance Ministry

The German Finance Ministry has said that it will react to the report only once it has studied the Iraqi declaration.

"We'll first wait till the report is in our hands," a spokesman from the ministry said on Tuesday.

The spokesman however said that the German government of the time in 1990 had informed the parliament about such German supplies to Iraq.

Ever since Iraq invaded Kuwait in 1990, there has been a strict embargo against the country. The spokesman said that there have been a few cases of violation of the embargo and the government has initiated investigations.

German military exports to Iraq nothing new

Explosive as the newspaper report may appear, it's not the first of its kind.

For months rumors have been circulating in the German media of murky deals between German arms companies and businessmen with Iraq despite the rigid embargoes in place.

In October this year, a magazine of the German radio channel, Sudwestrundfunk reported that electronics giant Siemens had delivered specialized technical equipment to Iraq for the treatment of kidney stones, but which could also under certain circumstances be used as a detonator for atom bombs.

Siemens insisted that the device could not be misused because it had commissioned an Iraqi company to regularly monitor the equipment. In fact the delivery was even sanctioned by the sanctions council of the U.N. and the Federal Office of Economics and Export Control (BAFA).

The latest newspaper report also touches upon the gray zone between medicine and armaments and writes of so−called dual−use goods that can be used for developing weapons as well as for civilian purposes.

The German government was apparently informed in 1999 of the delivery of such dual−use goods to Iraq, but is said to have turned a blind eye.

German defense firms conduct roaring trade with Baghdad

German arms companies in the meantime have been conducting booming business with Iraq in recent years. According to the German Federal Statistics Office, German military exports to Iraq have been steadily rising from year to year.

From annual exports amounting to 21,7 million euro in 1997, the volume of exports for the following year shot to some 76,4 million euro. The trend continued in 2001 with exports to Iraq bringing German firms profits in the range of 336,5 million euro.

German goods worth 226,2 million euro have already been shipped to Iraq in the first half of this year. Some of the official heavyweights in the export scene are the German electronics firm Siemens with medical equipment and energy distribution systems and carmaker DaimlerChrysler. Both are reported to rake in revenues worth double digit figures in the millions.

Chancellor Schroeder in precarious situation

Though the German government has not officially reacted to the Iraqi declaration detailing its role in supplying Iraq with arms, there is little doubt that the issue is bound to stoke passions.

Ever since Chancellor Gerhard Schroeder refused to be part of any military action in Iraq before the German general elections in September, Berlin's relation to Washington has been a strained one.

With Schroeder sticking to his pacifist line, but dithering over the level of cooperation with the U.S. in the case of a war against Iraq, the latest report is guaranteed to provide ammunition to the opposition who have strongly criticized Schroeder's policy towards America.

Another real fear is that Schroeder's image as a staunch pacifist might now be sullied if it emerges that Germany has all along been helping the very leader who it has been unwilling to topple, to stockpile his weapons.

The report could also provide the U.S. with an excuse to step up the pressure on Germany to give in to American military demands for deployment of German troops and use of German military equipment in the case of a military attack on Iraq.

> *Norway has several oil drilling operations in northern Iraq. Funny, they can protect that...*
>
> *Kill all Eurosavages.*

No to NATO

September 13, 2006 – *From:* *www.aftenposten.no*

The Norwegian soldiers, many of them fresh from basic training, were in danger earlier this month of being sent from the relatively calm north to escalating conflicts with the Taliban in the south.

NATO wants to shift more force to fight the Taliban in the area and sketched out a draft order that would move Norway's Quick Reaction Force from the north to Kandahar in the troubled south. There it would relieve an allied watch force which in turn would join the fight against the Taliban.

Defense Department spokesman Kjetil Eide in Oslo said that NATO had sent an 'inquiry' and not an 'order'. Norway's vice–admiral Jan Reksten decided to exercise the right of members to veto ISAF (International Security Assistance Force) orders.

"This was an assignment not in keeping with the what the Norwegian soldiers were sent to Afghanistan to do," brigadier Gunnar Gustavsen, chief of staff at the Joint Defense operative headquarters, told Aftenposten.

According to Aftenposten's sources, the NATO plan would not have meant using Norwegian soldiers in combat operations.

Norway has made it clear that its forces in Afghanistan are not sufficiently trained to take part in combat and not properly equipped to do so either.

Wow! A Eurosavage country helping Al–Qaeda. There's a real shocker!

Kill all Eurosavages.

__**Weekly Claims Wartime Bosnian President Linked to Al–Qaeda**__

September 8, 2006 – *From:* www.adnki.com

Bosnia's wartime president, the late Alija Izetbegovic received money from a Saudi businessman, Yassin al–Kadi – who has been designated by the United States, the United Nations, and the European Union as a financier of al–Qaeda – Sarajevo weekly Slobodna Bosna (Free Bosnia) has reported, quoting local and foreign sources.

Izetbegovic, a Muslim, who died in 2003, received 195,000 dollars in 1996 from al–Kadi, Slobodna Bosna alleges. Al–Kadi's bank accounts were frozen in 2001 by the United States authorities for money laundering and financing al–Qaeda.

The weekly said that Bosnian authorities obtained the information on this transaction from a British bank in the process of investigation of activities of al–Kadi's humanitarian organisation, Mufavak, which was outlawed four years ago and which began operating in Bosnia under the name 'Blessed relief'.

Under the guise of humanitarian aid, Mufavak channelled 15–20 million dollars to various organisations, which at least three million dollars went straight into the bank accounts of al–Qaeda leader Osama bin Laden, Slobodna Bosna said, quoting unnamed Saudi sources.

Izetbegovic led Bosnia to independence from the former Yugoslavia, and thousands of foreign fighters or 'mujahadeen' from Islamic countries came to Bosnia to fight on the side of local Muslims in bloody 1992–1995 civil war. The war effort was partly financed under the cover of 'humanitarian' organisations from Islamic countries, according to intelligence sources.

Many mujahadeen remained in Bosnia after the war, and some have been operating terrorist training camps and indoctrinating local youths with radical Islam, intelligence reports have claimed. The Bosnian authorities are currently reviewing the citizenship Izetbegovic's government granted to 1,500 individuals from Islamic countries. So far, 50 people have been stripped of their Bosnian citenship as a result.

Wow! The Germans are helping terrorists. There's a real shocker!

Kill all Eurosavages.

__**Terrorist Ali Hamadi Rejoins Hezbollah Following Release From Prison**__

September 12, 2006 – *From:* www.foxnews.com

By James Rosen

WASHINGTON –– One of the most infamous terrorists of the 1980s has rejoined Hezbollah following his release from a German prison and deportation to his native Lebanon in December

2005, a senior Bush administration official told FOX News.

Mohammed Ali Hamadi was released despite strong U.S. objections, FOX News learned. Those objections were raised in phone calls to German authorities by Attorney General Alberto Gonzales and FBI Director Robert Mueller, as well as by top−level State Department and administration counter−terrorism officials.

"[The Germans] ignored us and didn't give us enough time to pursue it through legal action," an official told FOX News on the condition of anonymity. "They gave us very short notice."

U.S. officials said they "can't rule out" the possibility that Germany deported Hamadi, after he had served 19 years of a life sentence, in exchange for the release of Susanne Osthoff, a German archeologist taken hostage in Iraq and freed four days after Hamadi's deportation. German authorities have denied any such deal was made.

In June 1985, Hamadi was one of four Islamic militants who commandeered TWA Flight 847 −− en route from Athens to Rome −− and hijacked it to Beirut. The ensuing hostage ordeal lasted 17 days, with the plane shuttling among various Mediterranean airports.

On the second day of the hijacking, Hamadi and his accomplices learned that U.S. Navy diver Robert Dean Stethem was on board. Hamadi and his co−conspirators beat Stethem unconscious, then shot him to death and dumped his body on the tarmac of the Beirut airport. The hijackers later escaped.

In 1987, Hamadi was arrested in Frankfurt, Germany, for carrying explosives in his bag at the airport. He was convicted both on that charge and of Stethem's murder and sentenced to life in prison. Late last year he was paroled by the German authorities and deported to Lebanon.

On Dec. 21, 2005, shortly after Hamadi's return to Lebanon, State Department spokesman Sean McCormack told reporters: "I think what I can assure anybody who's listening, including Mr. Hamadi, is that we will track him down, we will find him and we will bring him to justice in the United States for what he's done.

"We will make every effort, working with the Lebanese authorities or whomever else, to see that he faces trial for the murder of Mr. Stethem."

At a press briefing Tuesday, State Department spokesperson Tom Casey confirmed that contact had been made with the Lebanese government regarding Hamadi, and that the case remains active.

"The United States still believes that he and anyone else who is responsible for such heinous acts should face justice," Casey said. "And we do continue to wish to see him be brought to the United States to face trial here."

Hamadi's alleged accomplices −− Hassan Izz−Al−Din, Ali Atwa and Imad Mughniyeh −− were never captured.

Mughniyeh is also believed to be responsible for the 1983 barracks bombing that killed 241 U.S. Marines in Lebanon and for the 1984 torture and murder of William Buckley, the CIA Station Chief in Beirut.

Mughniyeh, who is believed to have undergone extensive plastic surgery to make himself unrecognizable, has been described in the media as "probably the world's most wanted outlaw."

Upon hearing news of Hamadi's release in 2005, Stethem's family members said they would keep pressuring the U.S. government to seek extradition from Lebanon.

"We'll be after him," Stethem's mother, Patricia, said of Hamadi. "We won't let it rest."

> *And you wonder why Eurosavages don't support sanctions. They are in bed with the ragheads!*
>
> *Kill all Eurosavages.*

<u>Iran's Commercial Ties With Italy Growing</u>

August 28, 2006 – *From: www.iranmania.com*

LONDON, August 28 (IranMania) – Secretary of Iran–Italy Chambers of Commerce said that investing in Iranian projects implies concurrent investment in all regional countries given that Iran is the pivotal country in the Persian Gulf and Central Asia–Caucasus regions.

Speaking to ILNA, Jamshid Haqgou added that the volume of trade between Iran and Italy in 2006 has increased. This is while in 2005 bilateral trade amounted to over five billion dollars, he said noting, "The figure is rapidly increasing and we predict that by the end of this year it will exceed $5.5 billion."

He added, "Iranian investments in Italy are very meager and limited to small companies only. However, there are more opportunities for Italian businessmen to invest in Iran than the other way around."

Haqgou recalled that investing in Iranian undertakings can be very attractive for Italians and Europeans.

"However, suitable conditions do not exist for investments due to tensions in the Middle East. The most important barriers are regiona conditions and local banking regulations. This is while Iran needs foreign investments to ensure its advancement based on its 20–Year Vision," he noted.

> *Eurosavages care about "human rights" only when it can bash America.*
>
> *Kill all Eurosavages.*

<u>Europe's 'Moral Outrage'</u>

December 4, 2005 – *From: www.opinionjournal.com*

Europe is enthralled by another American "torture scandal." Governments demand the truth behind allegations, first made by the Washington Post last month, that the CIA has operated covert prisons in Europe and secretly transported terrorist suspects through European airports. Human Rights Watch claims to have located the prisons in "New Europe"––Poland and Romania.

The outrage on the Continent is deafening. Franco Frattini, the normally level–headed European Commissioner for Justice, threatened "serious consequences," including the unprecedented "suspension of voting rights" in the European Union for the Poles and Romanians if the allegations prove true. After all, "European values" would have been violated.

It is difficult to comment on the substance of the allegations because there isn't much substance at the moment. Both the Romanian and Polish governments have denied the reports, while Washington promised to look into the case. So for the time being, there are only allegations and a lot of moral outrage. That moral posturing, though, deserves a closer look.

We'd be the first to applaud Europeans for finally concerning themselves with moral principles instead of commercial interests. Many of the Middle East's problems, including terrorism, would be easier solved if Europe were seriously concerned about morality. Europe would no longer be Iran's No. 1 trading partner, and its companies wouldn't be able to attend trade fairs in Sudan anymore.

Unlike American companies−−recently defamed in Germany as "(blood) suckers" and "locusts" by the former government−−European firms are quite busy in Sudan. The chamber of commerce and industry in Stuttgart has enthused over what great opportunities Sudan's oil resources offer to German companies.

Lest people think they are doing something morally reprehensible, the salesmen from Stuttgart prefer to describe the massacres of black Africans in Darfur as "political disturbances." The German economics ministry, which sponsored the German pavilion at last February's trade fair in Sudan, will also support next February's event, the chamber of commerce assures its members.

Where is the outrage? How does that jibe with supposed European values?

Or who in Europe has heard of Soghra, an Iranian woman sentenced in October to death by stoning for adultery? Or Mokhtar N. and Ali A., hanged last month in a public square in Iran for homosexuality?

In much of Europe's public debate, the true meaning of human rights has degenerated into a tool that gives anti−Americanism an aura of legitimacy. The real, horrendous human−rights violations in the Middle East, North Korea, China, Cuba, etc., are largely ignored or relegated to news blurs on the back pages. For front−page coverage, you need an American angle.

It is often said that this has nothing to do with anti−Americanism but with the fact that democracies, such as the U.S., must be held to higher standards. Really? Let's look at some recent European violations of human rights.

In October, the European Council's Commissioner for Human Rights inspected what the French call a detention center for foreigners. Alvaro Gil−Robles believes it is more properly called a dungeon. "With the exception of maybe Moldavia, I have not seen a worse center," he said about the facilities underneath the Palais de Justice in Paris, located not more than a few hundred yards from Notre Dame.

And what was Europe's reaction to these astonishing accusations? A yawn, a few wire reports and press pickups; that's it. After all, those prisoners, locked up under horrendous sanitary conditions, without natural sunlight and ventilation, some of whom, according to one prison guard, have in desperation mutilated themselves and smeared their blood on the walls, were only simple illegal immigrants. No need to suspend French voting privileges on their account, that's for sure.

Let's imagine for a moment the media coverage, the moral outcries and the calls for inquiries if those unfortunates had not been harmless migrants held in the City of Lights but jihadi terrorists held by Yankee soldiers?

Or take the double standard about allegations that CIA planes have used European airports to bring terror suspects to third countries where they might be tortured. The fact that Europe routinely sends back thousands of asylum seekers to countries where they could be tortured does not make the front pages, though. As recently as October, Amnesty International accused the Spanish government of violating the European Human Rights Convention for the mass expulsion of African migrants from the Spanish enclaves in Morocco. "Torture and bad treatment is endemic in Morocco," Esteban Beltran, the director of the Spanish Amnesty International section said.

If he could have proved that some of those poor souls trying to reach Europe to start a better life were in fact terrorists, and if he could have also somehow implicated the U.S. in their expulsion, he might have been able to get an audience for his complaints.

Anti−Americanism is so prevalent in Europe that it has permeated almost all areas of public discourse−−from arts to politics to economies. "American conditions" is a popular German slur against alleged social coldness in the U.S.−−one that former Chancellor Gerhard Schroeder has "successfully" used to reject necessary economic reforms. And just as it has poisoned the economic debate in Europe, anti−Americanism also poisons the debate about how to deal with terrorism. Any measure that involves the U.S. is almost immediately tainted as being beyond the pale.

That's particularly true because in the public debate in Europe, as all too often in the U.S. as well, terrorism is still seen as a conventional threat. That it is decidedly not, one doesn't need to trust the Bush Administration alone. Here is what Europe's antiterror czar, the Dutch Gijs de Vries, told us recently: "Bin Laden has called the acquisition of nuclear weapons by terrorists a religious duty. There is every reason to believe that here, as elsewhere, he is deadly serious about this."

Those decrying secret prisons and tougher interrogation methods (assuming the allegations have some validity) have yet to spell out what kind of "humane" treatment they would give to bombers whose mission it is to destroy Western civilization. If they can't, their complaints are hypocritical and intellectually shallow. How many bombing murders on European soil does it take for this realization to sink in?

> *Were they wearing a "Free Mumia" T−shirt?*
>
> *Kill all Eurosavages.*

Outrage After Two Police Ambushed in Suburb

September 20, 2006 − *From:* www.expatica.com

EVRY, France, Sept 20, 2006 (AFP) − Police unions reacted with outrage Wednesday after two members of a CRS anti−riot unit were badly hurt in an ambush by youths in the southern Paris suburb of Corbeil−Essonnes.

The men were patrolling Tuesday night in an unmarked car in the Les Tartarets housing project when the vehicle was attacked with stones, a police spokesman said.

When one of the officers left the vehicle, he was set upon by about 20 youths who had been hiding in the undergrowth.

"The driver rushed to help. The two were then covered in blows to the face and other parts of the body as they lay on the ground," the spokesman said. The gang dispersed when reinforcements arrived.

Both officers suffered injuries to the face and head, as well as bruising to the body. One was hospitalised.

The Synergie−Officier police union said it was "revolted by this savage attack .... These explosions of violence against the police are a kind of guerrilla warfare aimed at getting the forces of law and order to leave certain areas in order to immerse them in a logic of sedition and terror."

The UNSA union said the officers were "victims of a genuine ambush by individuals whose sole aim was to attack the forces of law and order."

Opposition parties said the attack was a sign that the security policies of Interior Minister Nicolas Sarkozy, a likely presidential candidate in next year's election, have failed.

It followed a stark warning about the risk of a new outbreak of suburban rioting in a letter published Tuesday from the prefect or state−appointed governor of the Seine−Saint−Denis department, centre of last year's disturbances.

Jean−Francois Cordet told Sarkozy in a letter sent in June that tensions were continuing to rise in the northern Paris suburbs −− with rising crime, a court system that was failing to punish, and the active incitement of Islamic radicals.

In a statement Wednesday the Socialist party (PS) said that the attack on the two policemen "showed that the alarming comments made by the prefect of Seine−Saint−Denis apply to many other suburbs as well."

Prime Minister Dominique de Villepin said that the government will "draw lessons from what has happened in order to devise appropriate responses ... to the risks to which part of our forces of law and order are exposed."

Is that part of that infamous "cultural superiority?"

Kill all Eurosavages.

Nazis Set to Claim German Seats

September 14, 2006 − *From:* www.theage.com.au

By Allan Hall

NEO−NAZIS are set to gain important seats in German Chancellor Angela Merkel's home state on Sunday in an election that will show a dark past continues to haunt the country.

As many as 12 MPs are forecast to be elected in the state near Berlin, which US President George Bush visited in July. They will join other neo−Nazis elected in Saxony two years ago as legislators in a state government.

Despite attacks against black people in the run−up to the World Cup −− itself themed against racism −− and warnings of no−go zones in the former communist east because of right−wing violence, the lure of extremist politics remains strong in the region.

Mecklenburg−Vorpommern, near Berlin, will vote on Sunday for a new legislature that will control vital areas such as police, education and health. A bloc of NPD (National Democratic Party) politicians would be embarrassing and controversial, influencing policy in the region.

The strength of the far−right highlights the continuing agony of east Germany 15 years after the Berlin Wall fell. Unemployment remains above 20 per cent in most places, more than a million people have gone west and little investment has been forthcoming for those left behind.

In the past decade−and−a−half, Berlin has hurled about $A2.5 trillion at the 17 million citizens who once lived behind the Iron Curtain.

East Germany loses 80 people a day. Since reunification, 1.4 million of its best and brightest young people have left.

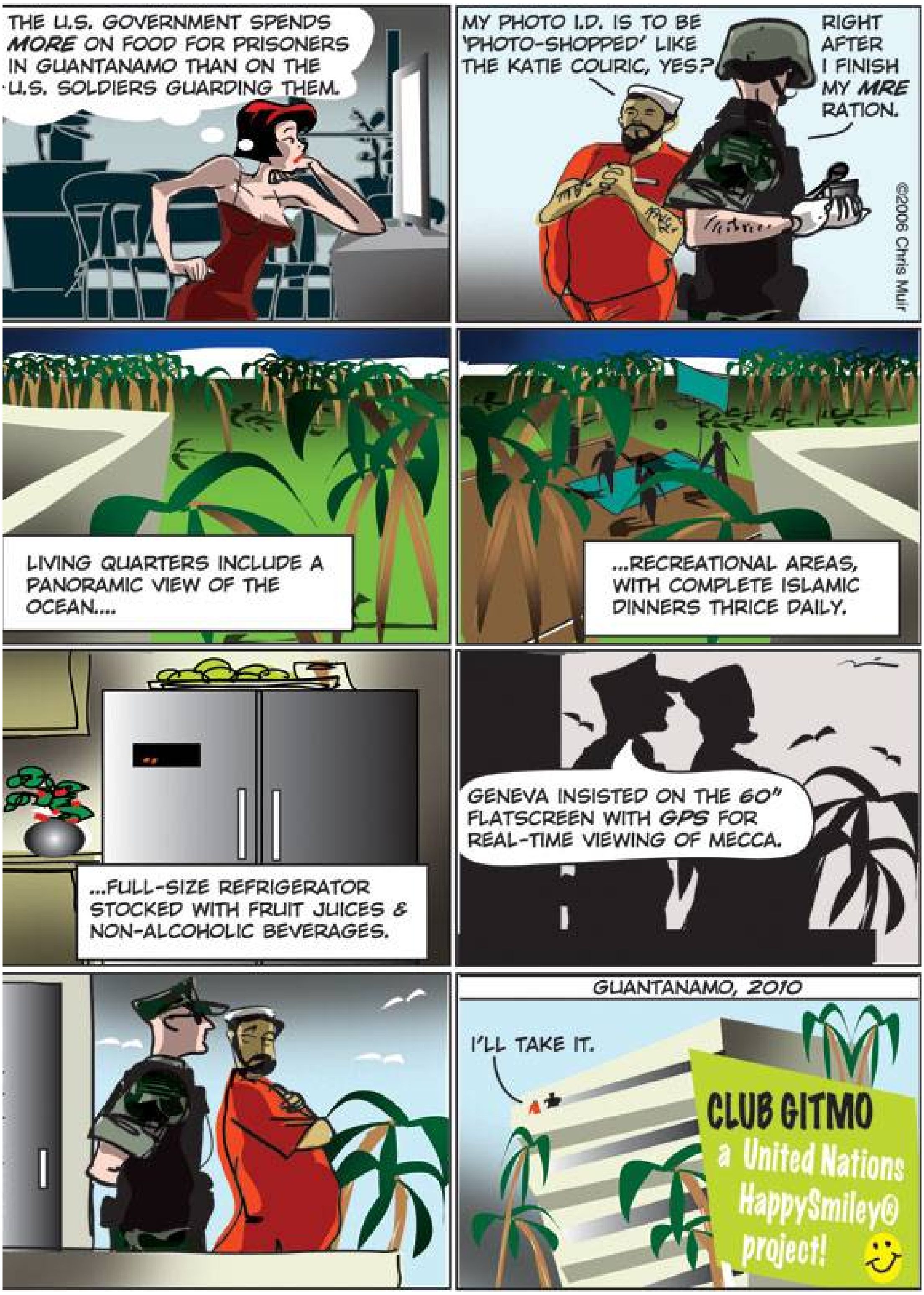
In Meck−Pomm, as locals call it, that has left behind the hardened skinheads and others who have turned to the dubious glories of the Nazi period. In some towns unemployment is as high as 25 per cent.

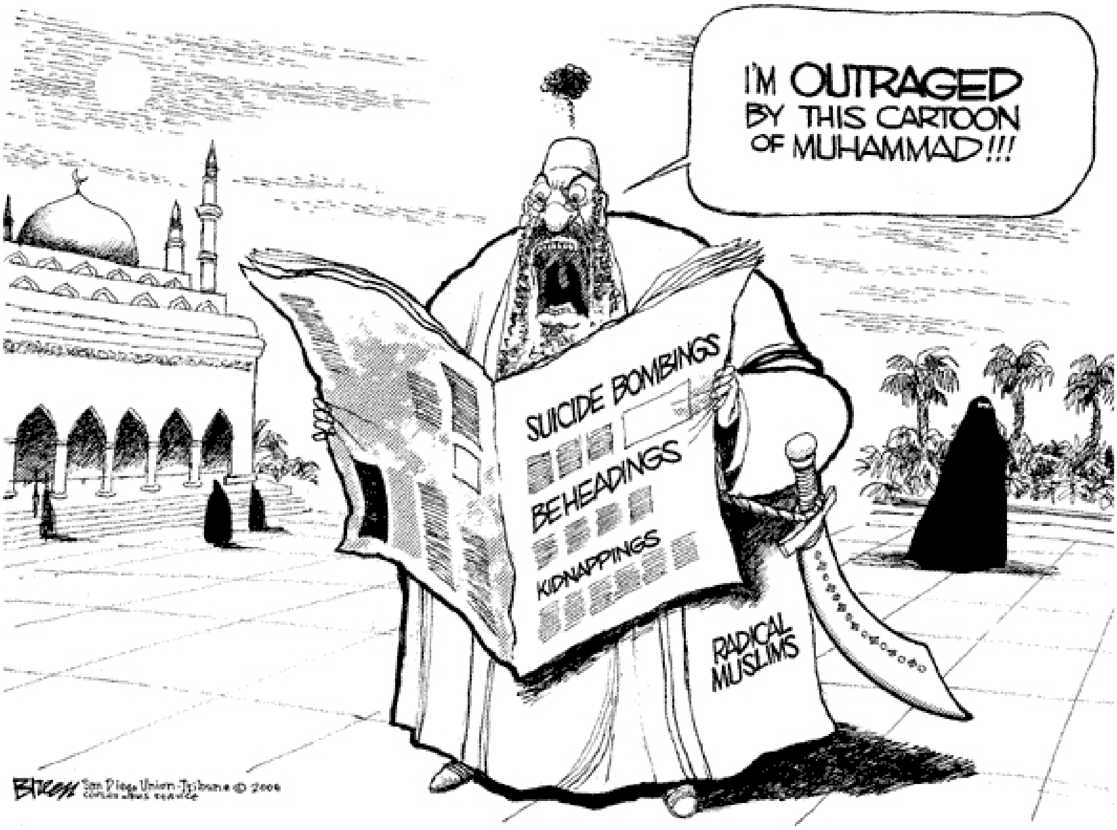
The NPD is Germany's oldest neo−Nazi party and is set to win about 6 per cent of the vote in the September 17 election. Far−right parties would then be represented in three of the six state parliaments in eastern Germany.

Its xenophobia, anti−semitism and fondness for the Third Reich are couched behind populist rants against globalisation and the European Union.

RAMIREZ
SIR, IF YOU DONT MIND... WHEN YOU FEEL UP TO IT, WOULD YOU MIND GIVING US SOME INFORMATION ON THE PEOPLE TRYING TO KILL US?
DEATH TO AMERICA

THE NEW IRAQI PRISONER INTERROGATION TECHNIQUE

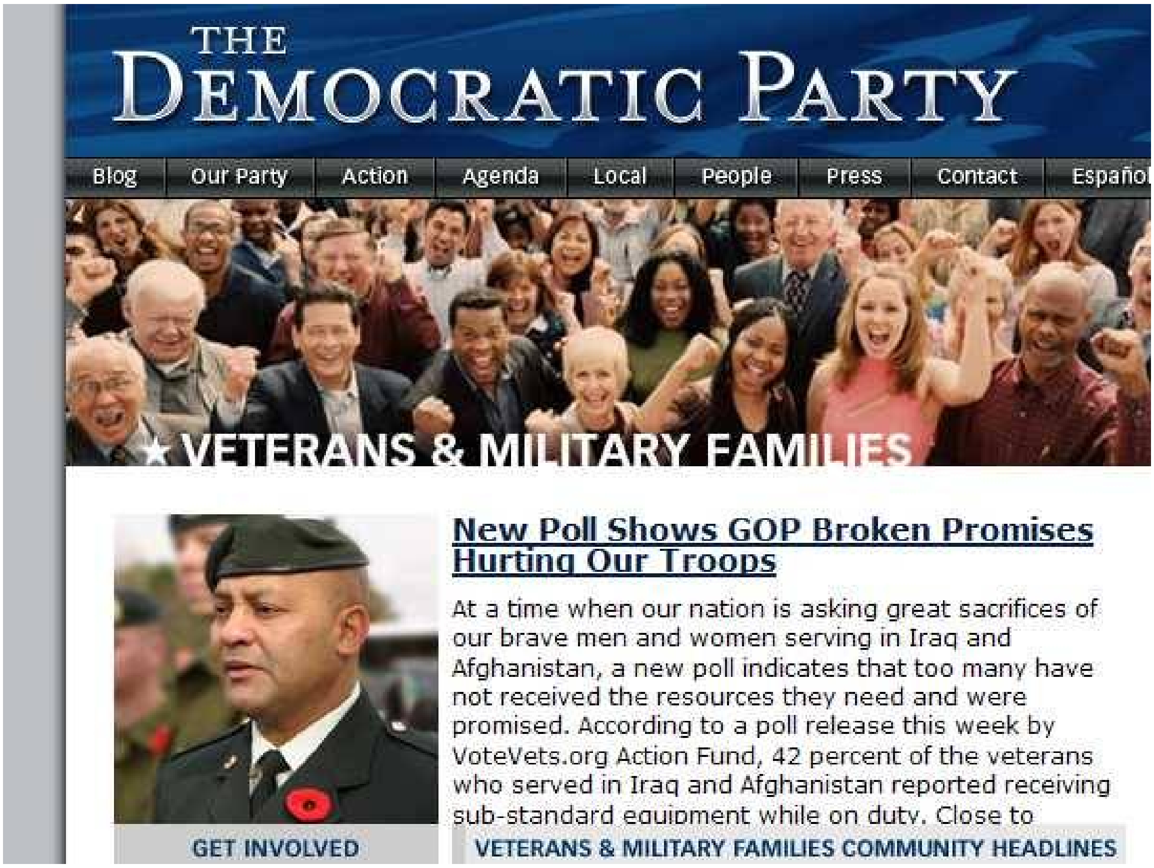

THE U.S. GOVERNMENT SPENDS *MORE* ON FOOD FOR PRISONERS IN GUANTANAMO THAN ON THE U.S. SOLDIERS GUARDING THEM.
MY PHOTO I.D. IS TO BE 'PHOTO-SHOPPED' LIKE THE KATIE COURIC, YES?
RIGHT AFTER I FINISH MY *MRE* RATION.
©2006 Chris Muir
LIVING QUARTERS INCLUDE A PANORAMIC VIEW OF THE OCEAN....
...RECREATIONAL AREAS, WITH COMPLETE ISLAMIC DINNERS THRICE DAILY.
...FULL-SIZE REFRIGERATOR STOCKED WITH FRUIT JUICES & NON-ALCOHOLIC BEVERAGES.
GENEVA INSISTED ON THE 60" FLATSCREEN WITH *GPS* FOR REAL-TIME VIEWING OF MECCA.
GUANTANAMO, 2010
I'LL TAKE IT.
CLUB GITMO
a United Nations HappySmiley® project!



San Diego Union-Tribune © 2006
Copley News Service

How to tell if there is a terrorist at the airport...

"Vote Democrat!"



New Poll Shows GOP Broken Promises Hurting Our Troops

At a time when our nation is asking great sacrifices of our brave men and women serving in Iraq and Afghanistan, a new poll indicates that too many have not received the resources they need and were promised. According to a poll release this week by VoteVets.org Action Fund, 42 percent of the veterans who served in Iraq and Afghanistan reported receiving sub-standard equipment while on duty. Close to

That's a Canadian soldier!