

GBPPR 'Zine



Issue #50 / The Monthly Journal of the American Hacker / June 2008

"No, I can't fix public education. The problem isn't the teachers unions or a lack of funding for salaries, vouchers or more computer equipment. The problem is your kids!"

--- May 4, 2008 quote from a P.J. O'Rourke commencement speech.

Table of Contents

- ◆ **Page 2 / Alcatel 1603/12 SONET Multiplexer – Craft Interface Operation**
 - ◆ Local and remote interfacing techniques for the Alcatel 1603/12 OC-3 SONET multiplexer.
- ◆ **Page 8 / Alcatel 1603/12 SONET Multiplexer – Security/User Authorization**
 - ◆ Overview of input message restrictions for the Alcatel 1603/12 OC-3 SONET multiplexer.
- ◆ **Page 26 / Gasoline From Coal?**
 - ◆ Scan of an interesting article from the September 1978 issue of *Mechanix Illustrated*.
- ◆ **Page 29 / Nortel DMS-100 Automatic Number Identification Attributes Table (ANIATTRS)**
 - ◆ Table which lists directory numbers which don't pass ANI information.
- ◆ **Page 31 / Portable Antenna Mast System**
 - ◆ Utilize simple plumbing hardware to make a nice portable antenna mast.
- ◆ **Page 39 / Bonus**
 - ◆ Change
- ◆ **Page 40 / The End**
 - ◆ Editorial and rants.

Alcatel 1603/12 SONET Multiplexer

Craft Interface Operation

LOCAL ACCESS

The basic means for locally interfacing with the 1603/12 SM system is provided by the COA30X or COA40X Craft, Orderwire, and Alarm plug-in unit (COA). On the front panel of the COA is a 9-pin subminiature D connector (marked "USI") which serves as the CRAFT1 (RS-232) access port. Figure 1, Page 2, illustrates the pin configuration of the connector. If desired, a 9-pin to 25-pin translation cable (601229-540-072) can be ordered. For a more permanent connection, a second craft port with wire-wrap pins is available on the shelf backplane (see Remote Access below).

To initially access the COA, a Visual Display Terminal (VDT) (ASCII monitor and keyboard) is required. A Personal Computer (PC) with a terminal emulator program may be used instead. The terminal must be capable of satisfying the following default communications parameters:

Baud rate:	9600
Number of bits:	8
Parity:	None
Stop bits:	1
Line width (characters):	80

When the user has accessed the COA, it is possible to change the baud rate to one of the following: 300, 1200, 2400, 4800, 9600, AUTO_BAUD. However, a baud rate change does not take effect until **after** the user logs off and logs back onto the NE. To regain access, the VDT must be reset to the new parameters.

REMOTE ACCESS

There are two methods for remotely logging onto an NE. One method is via a modem connected to the RS-232 wire-wrap pins on the shelf backplane. This port is called the CRAFT2 port and requires the COA301 or COA401 plug-in unit to be used. As far as the NE is concerned, this is a second local craft port. The CRAFT2 port could be wired to a VDT instead of a modem for a permanent local craft interface.

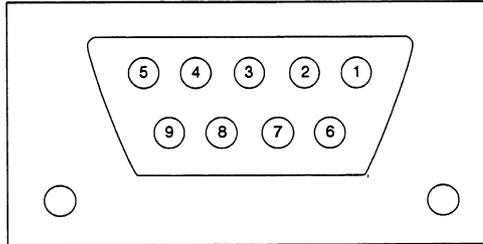
The second method of remotely logging onto an NE allows a user to be connected to one NE (the local NE) and request a login session on another NE (the remote NE). The user specifies the Terminal Identifier (tid) of the remote NE when logging in, and the session is established over the SONET embedded communication channel between the local and remote NEs.

CRAFT INTERFACE OPERATION

ISSUE 2	OCT 1994
ALCL 363-203-502	TNG
PAGE 1 of 6	503

Alcatel 1603/12 SONET Multiplexer

Craft Interface Operation



PIN NUMBER	DESCRIPTION
1	DCD
2	RXD
3	TXD
4	DTR
5	SGND
6	DSR
7	RTS
8	CTS
9	OPTIONAL

FRONT VIEW

A5627

Figure 1. COA30X or COA40X USI RS-232 Connector, Front View

E2A INTERFACE

The COA302 or COA402 has only one craft interface, but it does provide a second interface for serial E2A. Like the COA301 or COA401, this port is accessed via the wire-wrap pins on the shelf backplane. The interface is a differential RS-422 type (TBOS protocol).

ISSUE 2	OCT 1994
ALCL 363-203-502	TNG
PAGE 2 of 6	503

CRAFT INTERFACE OPERATION

Alcatel 1603/12 SONET Multiplexer

Craft Interface Operation

LOGGING ON

A user-ID (login name) and password are required to log onto the NE. Use either the system default login/password or the login/password assigned by the System Administrator (see TNG-510). To gain access to the system, the following sequence must be performed:

1. Connect the VDT or PC to the COA craftport by using an RS-232 cable.
2. Turn on the VDT or run the Terminal Emulation program if using a PC.
3. Log onto the local or remote NE by one of the two methods that follow:

Log Directly onto NE

Enter the following command to log directly onto the NE:

ACT-USER:[tid]:uid:[ctag]::pid;

where:

tid = Name of NE you wish to log onto (defaults to local NE if not entered)
uid = User-ID (login or logname)
ctag = Correlation tag (not required)
pid = Password

Log onto NE by Using Prompt Mode

- Press the ENTER or carriage return <cr> key several times until the <tid> prompt appears.
 - If you are logging onto the local NE, press <cr> key to get next prompt. If you wish to log onto a remote NE, enter the NE's Terminal Identification (TID) code followed by a <cr>.
 - At the USERNAME prompt, enter the User-ID code followed by a <cr>.
 - At the PASSWORD prompt, enter the password assigned to the User-ID.
4. The system prompt (<) will appear if a successful login session is established.

CRAFT INTERFACE OPERATION

ISSUE 2	OCT 1994
ALCL 363-203-502	TNG
PAGE 3 of 6	503

Alcatel 1603/12 SONET Multiplexer

Craft Interface Operation

COMMAND ENTRY

Once the username and password have been entered, the following display with a HELP MENU appears on the screen and/or printer:

```
1603SM 70-01-01 00:00:03
M 0 Cmpld
/* ACT-USER */
/*
/*
/*          NOTICE: This is a private computer system
/*          Unauthorized access or use may lead to prosecution
/*
/* 1 User(s) Logged On */
;
<
/*          HELP MENU

HELP          or   ?   Type HELP or ? for this menu.
MENU          or   ?   Type MENU or menu mode.
<UP ARROW>   or   ^B   Recall previous commands.
<DOWN ARROW> or   ^N   Recall successive commands.
<LEFT ARROW> or   ^D   Move cursor left one space.
<RIGHT ARROW> or  ^F   Move cursor right one space.
<CAN>        or   ^X   Reset command input processing.
<BS>         or   ^H   Delete previous input character.
<DEL>        or   ^H   Restart current line input. */
```

Other useful control codes not listed are:

- '^A' go to the beginning of the line
- '^E' go to the end of the line

Once logged on, the user can operate in any one of three dialog modes: command, prompt, and menu. The command mode is intended for the experienced user who enters the entire command before pressing the ENTER (<cr>) key. However, the command processor reverts to the prompt mode if the entry is incomplete. The prompt mode steps the user through a series of question prompts and provides option listings for parameter entry. The command processor builds the command as the prompts are answered. The prompt mode is intended for the average or semi-experienced user. The menu mode is for least experienced user and provides the highest level of user assistance. In this mode, menus are provided for the user to select from. To enter the menu mode, type "menu" (without the quotations) at the system prompt.

ISSUE 2	OCT 1994
ALCL 363-203-502	TNG
PAGE 4 of 6	503

CRAFT INTERFACE OPERATION

Alcatel 1603/12 SONET Multiplexer

Craft Interface Operation

CONVENTIONS USED IN THIS MANUAL FOR ENTERING COMMANDS

To distinguish commands from normal text, the commands are printed in bold type as shown below:

RTRV-OC3:[tid]:LG1-HIFA:[ctag];

In the example command, the square brackets [] are not actually entered but are used to indicate that the enclosed parameter is optional. Generally, optional parameters enclosed in brackets have default values that are used by the command processor if you choose not to enter the parameter. If you are using the prompt or menu modes to enter the command, the default value is typically shown in brackets also.

As a general convention throughout this manual, command entries are shown with a mixture of uppercase and lowercase character strings. The uppercase character string signifies that the string is entered exactly as shown. The lowercase character string identifies that the input is not entered as shown, but relates to a value determined by the context of the command; i.e., the lowercase character string is substituted by a value that depends on the intent of the user. As an example, in the command shown below, INIT-LOG is entered as shown, but the parameters *tid*, *ctag*, and *logms* are replaced by entries to provide the command processor with information needed to properly execute the command:

INIT-LOG:[tid]::[ctag]::logms;

(example command structure as shown in manual)

INIT-LOG:1603_MAINOFFICE::1::EERLOG;

(example of how command might actually be entered)

_____||_____|||_____||

Command tid ctag logms
Code

The example below shows where both uppercase and lowercase character strings are used in one parameter (dgx-DMI-path):

RTRV-T1:[tid]:dgx-DMI-path:[ctag];

(example command structure as shown in manual)

RTRV-T1:1603_MAINOFFICE:DG1-DMI-1;;

(example of how command might actually be entered)

_____||_____|||_____|||_____||| ctag

Command tid dgx path (null)
Code

Alcatel 1603/12 SONET Multiplexer

Craft Interface Operation

In the preceding example, DG1 represents Drop Group No. 1 and 1 represents path number 1. In this example, the *ctag* parameter was omitted, which tells the command processor to use the default value. In both examples, the optional *tid* parameter was entered as 1603_MAINOFFICE which is the (optional) Terminal Identifier (or network name) of the example NE. All output responses and messages for this NE will include this identifier whether or not the *tid* is included in the command input.

The parameters *tid* and *ctag* are available for every command in the 1603/12 SM command language. These two common parameters are optional and typically are not used, unless the user is sending and receiving commands/messages to one NE while logged onto another. Because of this, and for brevity, these parameters are not defined along with the other command parameters in the Detailed Level Procedures (DLPs) of this manual. For a definition of these parameters, see TNG-501 (Command Structure).

LOGGING OFF

To terminate the craft session, enter either of the following commands:

LOGOFF (non TL-1 command also used on earlier SONET products)

-or-

CANC-USER:[tid]:[uid]:[ctag];

where:

tid = Name of NE to log onto (defaults to local NE if not entered)

uid = User-ID (login or logname)

ctag = Correlation tag (not required)

ISSUE 2	OCT 1994
ALCL 363-203-502	TNG
PAGE 6 of 6	503

CRAFT INTERFACE OPERATION

Alcatel 1603/12 SONET Multiplexer

Security/User Authorization

GENERAL

This document provides a summary of the security mechanism provided by the 1603/12 SM Network Element (NE) to restrict either the intentional or inadvertent unauthorized use of input commands. Other security issues, such as physical security and the security mechanisms provided by the Operation Systems (OS) interfacing with the 1603/12 SM, are not covered here, but are assumed to be provided per local telephone practices.

The main purpose of command entry security is to restrict the access to the NE data base which stores the vital information concerning the operations and configuration of the NE. Inadvertent alterations to this data base can disrupt the traffic-carrying and communications ability of the NE and, ultimately, interrupt service. Restricting access to and action on the information stored in the NE data base to those who need this access privilege for the performance of their tasks is an effective security strategy to preserve the integrity of the NE data base. This strategy is called the policy of least user privilege or, sometimes, the need-to-know policy, as it grants all users the smallest set of privileges necessary to perform their tasks.

The general security features provided by the 1603/12 SM are categorized as follows:

- **Identification:** Identification is the process of recognizing a session requester's unique and (audible) identity, such as the user ID. The user ID is not confidential; it is the name by which a valid user is recognized by the NE. A user ID aging mechanism is available to disable a user ID after some extended period of non-use time.
- **Authentication:** Authentication is the process of verifying the claimed identity of the session requester. For a user login, this is done by the use of a password which must be entered after the user ID when logging in to the NE. This password is known only by the NE and the user. A password aging mechanism is available which requires periodic changing of a user's password. In the case of OS network access channels that use the three-layer protocol such as X.25, a network-level security (i.e., not end-to-end connection security) is provided by verifying the calling address that is delivered to the NE via the "call-set-up packet."
- **System Access Control:** System access control authorizes establishment of a login session and continuation of a session until logoff. System access (except for a limited set of commands) is allowed only to those users who are identified and authenticated. A session privilege level is established that is determined by the combination of the user and the channel (port) privilege levels.
- **Command Access Control:** Command access control provides the capability of denying access to certain commands depending on the comparison of the session privilege level and the command privilege level. This subject is explained in greater detail in the remainder of this section.

SECURITY/USER AUTHORIZATION

ISSUE 2	JULY 1994
ALCL 363-203-502	TNG
PAGE 1 of 18	510

Alcatel 1603/12 SONET Multiplexer

Security/User Authorization

GENERAL (cont)

- **Data and System Integrity:** Data integrity and system integrity deal with the consistency and reliability issues associated with the NE system and its data and software resources.
- **Security Log (Audit):** Security log provides tools to establish an audit trail. If a security breach is suspected, an audit trail may be used to investigate the breach.
- **Security Administration:** Security administration consists of proper activation, maintenance, and usage of the security features of the NE, conducted by the system administrator. It includes, among other things, overriding Alcatel-supplied defaults and managing the security data base (i.e., keeping up-to-date user logins, privilege codes for users, commands and calling channels/ports).

CALLING CHANNEL IDENTIFIER (CID)

The Calling Channel Identifier (CID) describes what port or OS channel is used to access the NE. Two general classes of CIDs are available: user login and OS.

Local and remote user login access points are available. Local access consists of craft ports physically located at the NE. Remote login capability is provided over the SONET overhead channels to allow login capability at one NE while physically being located at another.

Operations performed on an NE can be tendered from centralized operations centers (OCs), often via Operations Systems (OSs). An OC may have a number of work groups that provide technical expertise and clearly defined assignment of responsibilities in a central location for the best use of human resources. To accommodate the different work groups, OS-channel recognition is provided by the NE. The OS channels provided by the 1603/12 SM are for maintenance (MAINT-OS), testing (TEST-OC), and memory administration (MEMADM-OS).

Certain security parameters are defined for each of the CIDs. A privilege code (described in more detail later) is assigned to each CID which is used for restricting access to commands that are outside of the CID's domain of responsibility. Also, certain monitoring parameters can be set for each CID such as: maximum number of invalid login attempts (MXINV), minimum time interval required between consecutive session setup attempts (MINT), inactivity time-out interval (TMOUT), and time interval over which the CID can be disabled due to an intrusion alert (DURAL).

ISSUE 2	JULY 1994
ALCL 363-203-502	TNG
PAGE 2 of 18	510

SECURITY/USER AUTHORIZATION

Alcatel 1603/12 SONET Multiplexer

Security/User Authorization

PRIVILEGE CODES

The determination of whether a command can be executed is based on privilege codes. A privilege code can be associated with a command, a user, a port, or a (login) session. The Command Privilege Code (COPC) specifies the minimum privilege requirements for all who will be able to execute a given command. Each command has an associated COPC which is set up by a system default and maintained by the system administrator. The User Privilege Code (UPC) provides the user with a set of privileges which will eventually help determine which commands he can execute and where he stands in the system user hierarchy. Each user has an associated UPC which is assigned when he is entered into the system, and maintained by the system administrator. The Calling Address Identifier (CID, also known as port) Privilege Code (CAPC) is assigned to each network access point to provide a means of regulating the types of commands which can be executed through a given port. Each network access point to the NE has an associated CAPC assigned to it. The CAPC is initially set up by a system default and is maintained by the system administrator. Finally, the Session Privilege Code (SPC) is defined by a combination of the UPC and CAPC, just as the user session itself is defined by both the user who is logged in and the port with which he is accessing the NE.

Once all of these privilege codes have been established, the question of command execution versus denial is answered by a comparison of the command privilege code (COPC) and the session privilege code (SPC). In general, if the SPC is "greater-than" or "equal-to" the COPC, the command will be executed. If not, the command will be denied. Before more details of the comparison can be made, a more detailed look at the privilege code is in order.

PRIVILEGE CATEGORIES

Each privilege code is made up of four categories, and each category contains a one-digit privilege level. The categories are defined as Maintenance (M), Provisioning (P), Security (S), and Test (T). These categories reflect the four basic categories of system TL-1 commands. The privilege levels for the four categories are concatenated into a single Privilege Code (PC):

PC = (M, P, S, T)

where: M, P, S, and T are the privilege levels for the respective categories.

SECURITY/USER AUTHORIZATION

ISSUE 2	JULY 1994
ALCL 363-203-502	TNG
PAGE 3 of 18	510

Alcatel 1603/12 SONET Multiplexer

Security/User Authorization

PRIVILEGE LEVELS

Each privilege category (M, P, S, and T) is assigned a privilege level that ranges from 0 to 7. Privilege levels from 0 to 7 can be assigned by the system administrator to user privilege codes (UPC), CID privilege codes (CAPC) and command privilege codes (COPC). The privilege levels (0 - 7) are defined as follows:

- **Level 7:** Level 7 is reserved for the system administrator and commands which can alter the integrity of the system.
- **Levels 3 - 6:** These levels are open and can be used by the system administrator to organize the user hierarchy as required by the application (e.g., supervisor, clerk).
- **Level 2:** Level 2 is the base level of a user who is considered logged into the system. This level includes basic commands which for security purposes should be executable by anyone who is allowed to login (includes most of the RTRV commands).
- **Level 1:** The Level 1 privilege is the lowest level and it is applied to all users who are "connected" to the system, but have not yet logged in. This level allows the user to execute the most basic commands such as RTRV-HDR (to retrieve the system header), ACT-USER (to activate a user), and LOGOFF.
- **Level 0:** This level is assigned to a privilege category when it is not to be considered during the process of deciding whether to allow a user to execute a command.

COMMAND EXECUTION

When a user enters a command, the NE's command processor must first decide whether the user has the proper privilege levels before allowing or denying the execution of the command. This is done by comparing each privilege category (M, P, S, and T) of the Session Privilege Code (SPC) and Command Privilege Code (COPC). When an SPC and a COPC are being compared, only the common categories are considered. A common category is one in which the both the SPC and COPC have a non-zero privilege level. In this way, a zero privilege level disables or disqualifies a category from the comparison. A zero value in the category for either the SPC or COPC causes the comparison process to skip to the next category with no immediate effect on the outcome. If a common category is found and the SPC's privilege level is greater-than or equal-to the COPC's privilege level, the comparison is considered successful and the next category is compared. The comparison is done for each privilege category until a comparison fails or all categories have been compared. In the case of a comparison failure, the comparison process is halted and the command's execution is denied.

ISSUE 2	JULY 1994
ALCL 363-203-502	TNG
PAGE 4 of 18	510

SECURITY/USER AUTHORIZATION

Alcatel 1603/12 SONET Multiplexer

Security/User Authorization

COMMAND EXECUTION (cont)

At least one successful comparison must be found before the command can be executed. It is possible that a command could be denied execution even though none of the comparisons failed. This is possible if no common categories are found. For example, if a session user with an SPC = 5500 tries to execute a command with a COPC = 0003, the command would be denied, since the two privilege codes contain no common categories to be compared. Likewise, if a session user with an SPC = 5500 tries to execute a command with a COPC = 7003, the command would also be denied, since in its only common category, MAINT, the COPC (7) is greater than the SPC (5). On the other hand, if a session user with an SPC = 0500 tries to execute a command with a COPC = 6406, the command would be executed, since in the only common category, PROV, the SPC (5) is greater than the COPC (4).

Commands and users can be grouped by category. In the case of the COPC, the privilege level associated with each category determines to which categories the command belongs (e.g., COPC = 0005 would indicate this command is strictly a T command and the session user trying to execute it must have a minimum T privilege of 5). In the case of an SPC, the privilege level associated with each category determines which types of commands the session user can execute (e.g., SPC = 0070 implies that this session will be able to execute S commands of privilege levels up to 7). Table A, Page 9, lists the 1603/12 SM system TL-1 commands, their functional category and their default COPC levels.

THE SUPERUSER AND A SUPERUSER

The "Superuser" is the system administrator who has a security privilege level of 7. No user in the system is able to delete the superuser. The superuser can create another user, with privilege levels equal to his own, who may also be considered a superuser. To distinguish between the two, they are referenced as The superuser (system administrator) and A superuser (created superuser). The difference is that The superuser can modify and delete A superuser, but A superuser cannot modify The superuser or any other created superuser (there can be more than one created). The superuser's user ID and password are provided by Alcatel and are programmed into the NE's factory-default software. The superuser's password can be changed but not its user ID. A superuser is simply a user ID with a user privilege code set to 7777.

SECURITY/USER AUTHORIZATION

ISSUE 2	JULY 1994
ALCL 363-203-502	TNG
PAGE 5 of 18	510

Alcatel 1603/12 SONET Multiplexer

Security/User Authorization

SECURITY TL-1 COMMANDS

Described in this section are the TL-1 commands associated with security administration. Only the commands available in Release 3 of the 1603/12 SM product are described. Other security related commands available in later releases will be added as applicable.

- **ACT-USER** This is the command for logging on to the NE. It should have a fairly low security privilege code since it must be executed by users who, prior to login, are provided only a default low level (connected) privilege. The recommended security code is 1111.
- **CANC-USER** This is the command executed by the user to logoff the NE. This command can also be used by A superuser or The superuser to log another user off the NE. Since this command must be executed by all users, its recommended security code is 1111.
- **DLT-SECU-USER** This command deletes a user from the system and can only be executed by The superuser or A superuser. The superuser can delete A superuser. The superuser cannot be deleted. This command allows deletion of one or a combination (by grouping) of users at the same time. Even if this command's security level is lowered, it can only be executed by successfully by A/The superuser. The recommended security code is 0070.
- **ED-SECU-CID** This command is used to edit or change the privilege code (CAPC) associated with a single or combination (grouping) of CIDs. Also, certain monitoring parameters can be set for each CID such as: maximum number of invalid login attempts (MXINV), minimum time interval required between consecutive session setup attempts (MINT), inactivity time-out interval (TMOUT), and time interval over which the CID can be disabled due to an intrusion alert (DURAL). This command should have a high security privilege code which would only allow A/The superuser to execute it. If the command privilege level is lowered, an internal mechanism prohibits a user from modifying the CID if his security privilege is lower than that of the CID. The recommended security code is 7777.
- **ED-SECU-CMD** This command is used to edit the privilege code (COPC) associated with a single or combination of commands. This command should have a high security privilege code which would only allow The/A superuser to execute it. But, if the command privilege level is lowered, an internal mechanism will prohibit a user from modifying the command if his security privilege is lower than that of the command. The recommended security code is 0070.

ISSUE 2	JULY 1994
ALCL 363-203-502	TNG
PAGE 6 of 18	510

SECURITY/USER AUTHORIZATION

Alcatel 1603/12 SONET Multiplexer

Security/User Authorization

SECURITY TL-1 COMMANDS (cont)

- **ED-SECU-PID** This command is used by a user to edit his own password (private identifier). The user must enter his old password before he can change it. The recommended security code is 2222.
- **ED-SECU-USER** This command is used to edit the security parameters associated with a single or combination of users. This command permits changing a user's privilege code (UPC), user ID, and password. Parameters also can be set for password aging as well as user ID aging. This command should have a high security privilege code which would only allow The/A superuser to execute it. If the command privilege level is lowered, an internal mechanism will prohibit a user from modifying another user of equal or greater privilege. The superuser can modify A superuser, but The superuser cannot be modified by any other user. The recommended security code is 0070.
- **ENT-SECU-USER** This command is used to enter a new user and all associated parameters listed for the ED-SECU-USER command. This command should have a high security privilege code which would only allow The/A superuser to execute it. If the command privilege level is lowered, an internal mechanism will not allow a user to create another user with higher privileges than his own. The recommended security code is 0070.
- **RTRV-SECU-CID** This command is used to retrieve the security parameters associated with a single or combination of CIDs. This command should have a low security privilege code which would allow all users to execute it. Although a user may have sufficient privilege to execute the command, he may not have sufficient privilege to view all the requested data base information. An internal mechanism will not allow a user with a lower security privilege than that of the CID to actually retrieve it. For example, a user with a security privilege sufficient to execute this command, yet lower than all the CIDs, would get the "completed" message (verifying his execution privilege), but he would still not be able to see any CID data in output. The recommended security code is 2222.
- **RTRV-SECU-CMD** This command is used to retrieve the privilege code associated with a single or combination of commands. This command should have a low security privilege code which would allow all users to execute it. An internal mechanism will not allow a user to retrieve information for a command which has a higher security privilege level than his own. In this case, provided a user has sufficient command privilege, he could execute the command, but would only see data pertaining to those commands which he is sufficiently privileged to see. The recommended security code is 2222.

SECURITY/USER AUTHORIZATION

ISSUE 2	JULY 1994
ALCL 363-203-502	TNG
PAGE 7 of 18	510

Alcatel 1603/12 SONET Multiplexer

Security/User Authorization

SECURITY TL-1 COMMANDS (cont)

- **RTRV-SECU-UPC** This command is executed by a user to retrieve his own User Privilege Code (UPC). The recommended security code is 2222.
- **RTRV-SECU-USER** This command is used to retrieve the security parameters associated with a single or combination of users. This command should have a low security privilege code which would allow all users to execute it. An internal mechanism will not allow a user to retrieve data base information on users who have a higher security privilege than his own. For example, a user with a security privilege sufficient to execute this command, yet lower than some of the other users, would get the "completed" message (verifying his execution privilege), but he would still not be able to see any information on users with a security privilege higher than his own; he would only see information for users of equal or lower security privilege. The recommended security code is 2222.
- **LOGOFF** This is another command for logging off the NE. The recommended security code is 1111.

ISSUE 2	JULY 1994
ALCL 363-203-502	TNG
PAGE 8 of 18	510

SECURITY/USER AUTHORIZATION

Alcatel 1603/12 SONET Multiplexer

Security/User Authorization

Table A. 1603/12 SM Commands and Default Command Privilege Codes (COPC)

COMMAND	FUNCTIONAL CATEGORY	COPC (MPST)
ACT-USER	MPST	1111
ALW-AUTORST	M---	2000
ALW-DGN-EQPT	M---	2000
ALW-LPBK-T1	M---	2000
ALW-MSG-ALL	M---	2000
ALW-PMREPT-ALL	M---	2000
ALW-PMREPT-EC1	M---	2000
ALW-PMREPT-EQPT	M---	2000
ALW-PMREPT-OC3	M---	2000
ALW-PMREPT-STS1	M---	2000
ALW-PMREPT-SYNCN	M---	2000
ALW-PMREPT-T1	M---	2000
ALW-PMREPT-T3	M---	2000
ALW-PMREPT-VT1	M---	2000
ALW-SWDX-EQPT	M---	2000
ALW-SWTOPTN-EQPT	M---	2000
ALW-SWTOWKG-EQPT	M---	2000
CANC-USER	MPST	1111
CLR-E2ADISP	-P--	0200
CONFIG-SYS	-P--	0700
CPY-MEM	M---	7000
DGN-EQPT	---T	2002
DLT-BITS	-P--	0200
DLT-CRS-STS1	-P--	0200
DLT-CRS-VT1	-P--	0200
DLT-DLMAP	-P--	0200
DLT-E2AMAP	-P--	0200
DLT-EC1	-P--	0200
DLT-EQPT	-P--	0200
DLT-OC3	-P--	0200
DLT-PORT	MP--	2200

NOTE: For Functional Category and Default COPC columns: M = Maintenance, P = Provisioning, S = Security, and T = Testing.

SECURITY/USER AUTHORIZATION

ISSUE 2	JULY 1994
ALCL 363-203-502	TNG
PAGE 9 of 18	510

Alcatel 1603/12 SONET Multiplexer

Security/User Authorization

Table A. 1603/12 SM Commands and Default Command Privilege Codes (COPC) (cont)

COMMAND	FUNCTIONAL CATEGORY	COPC (MPST)
DLT-SDCC	-P--	0200
DLT-SECU-USER	--S-	0070
DLT-SML	-P--	0200
DLT-T1	-P--	0200
DLT-T3	-P--	0200
ED-BITS	-P--	0200
ED-CRS-STS1	-P--	0200
ED-CRS-VT1	-P--	0200
ED-DLMAP	-P--	0200
ED-EC1	-P--	0200
ED-EQPT	-P--	0200
ED-FFP-OC3	-P--	0200
ED-FFP-STS1	-P--	0200
ED-FFP-VT1	-P--	0200
ED-OC3	-P--	0200
ED-PORT	MP--	2200
ED-SDCC	-P--	0200
ED-SECU-CID	--S-	7777
ED-SECU-CMD	--S-	0070
ED-SECU-PID	--S-	2222
ED-SECU-USER	--S-	0070
ED-SML	-P--	0200
ED-STS1	-P--	0200
ED-SYNCN	-P--	0200
ED-T1	-P--	0200
ED-T3	-P--	0200
ED-VT1	-P--	0200
ED-X25	-P--	0200
ENT-BITS	-P--	0200
ENT-CRS-STS1	-P--	0200
ENT-CRS-VT1	-P--	0200

NOTE: For Functional Category and Default COPC columns: M = Maintenance, P = Provisioning, S = Security, and T = Testing.

ISSUE 2	JULY 1994
ALCL 363-203-502	TNG
PAGE 10 of 18	510

SECURITY/USER AUTHORIZATION

Alcatel 1603/12 SONET Multiplexer

Security/User Authorization

Table A. 1603/12 SM Commands and Default Command Privilege Codes (COPC) (cont)

COMMAND	FUNCTIONAL CATEGORY	COPC (MPST)
ENT-DLMAP	-P--	0200
ENT-E2AMAP	-P--	0200
ENT-EC1	-P--	0200
ENT-EQPT	-P--	0200
ENT-OC3	-P--	0200
ENT-PORT	MP--	2200
ENT-SDCC	-P--	0200
ENT-SECU-USER	--S-	0070
ENT-SML	-P--	0200
ENT-T1	-P--	0200
ENT-T3	-P--	0200
INH-AUTORST	M---	2000
INH-DGN-EQPT	M---	2000
INH-LPBK-T1	M---	2000
INH-MSG-ALL	M---	2000
INH-PMREPT-ALL	M---	2000
INH-PMREPT-EC1	M---	2000
INH-PMREPT-EQPT	M---	2000
INH-PMREPT-OC3	M---	2000
INH-PMREPT-STS1	M---	2000
INH-PMREPT-SYNCN	M---	2000
INH-PMREPT-T1	M---	2000
INH-PMREPT-T3	M---	2000
INH-PMREPT-VT1	M---	2000
INH-SWDX-EQPT	M---	2000
INH-SWTOPTN-EQPT	M---	2000
INH-SWTOWKG-EQPT	M---	2000
INIT-LOG	M-S-	7070
INIT-REG-EC1	M---	2000
INIT-REG-EQPT	M---	2000
INIT-REG-OC3	M---	2000

NOTE: For Functional Category and Default COPC columns: M = Maintenance, P = Provisioning, S = Security, and T = Testing.

SECURITY/USER AUTHORIZATION

ISSUE 2	JULY 1994
ALCL 363-203-502	TNG
PAGE 11 of 18	510

Alcatel 1603/12 SONET Multiplexer

Security/User Authorization

Table A. 1603/12 SM Commands and Default Command Privilege Codes (COPC) (cont)

COMMAND	FUNCTIONAL CATEGORY	COPC (MPST)
INIT-REG-ST51	M---	2000
INIT-REG-SYCN	M---	2000
INIT-REG-T1	M---	2000
INIT-REG-T3	M---	2000
INIT-REG-VT1	M---	2000
INIT-SYS	M---	7000
LOGOFF	MPST	1111
OPR-ACO-COM	M---	2000
OPR-EXT-CONT	M---	2000
OPR-LPBK-EC1	---T	2002
OPR-LPBK-OC3	---T	2002
OPR-LPBK-T1	---T	2002
OPR-LPBK-T3	---T	2002
OPR-LSR	M---	2000
OPR-PROTNSW-OC3	M---	2000
OPR-PROTNSW-ST51	M---	2000
OPR-PROTNSW-VT1	M---	2000
OPR-SYCNNSW	M---	2000
RD-MEM-ADRS	M---	2000
RD-SYCN	M---	2000
RLS-EXT-CONT	M---	2000
RLS-LPBK-EC1	---T	2002
RLS-LPBK-OC3	---T	2002
RLS-LPBK-T1	---T	2002
RLS-LPBK-T3	---T	2002
RLS-PROTNSW-OC3	M---	2000
RLS-PROTNSW-ST51	M---	2000
RLS-PROTNSW-VT1	M---	2000
RLS-SYCNNSW	M---	2000
RMV-BITS	M---	2000
RMV-EC1	M---	2000

NOTE: For Functional Category and Default COPC columns: M = Maintenance, P = Provisioning, S = Security, and T = Testing.

ISSUE 2	JULY 1994
ALCL 363-203-502	TNG
PAGE 12 of 18	510

SECURITY/USER AUTHORIZATION

Alcatel 1603/12 SONET Multiplexer

Security/User Authorization

Table A. 1603/12 SM Commands and Default Command Privilege Codes (COPC) (cont)

COMMAND	FUNCTIONAL CATEGORY	COPC (MPST)
RMV-EQPT	M---	2000
RMV-OC3	M---	2000
RMV-SML	M---	2000
RMV-T1	M---	2000
RMV-T3	M---	2000
RST-BITS	M---	2000
RST-EC1	M---	2000
RST-EQPT	M---	2000
RST-OC3	M---	2000
RST-SML	M---	2000
RST-T1	M---	2000
RST-T3	M---	2000
RTRV-ALM-ALL	M---	1111
RTRV-ALM-BITS	M---	1111
RTRV-ALM-COM	M---	1111
RTRV-ALM-DLMAP	M---	1111
RTRV-ALM-EC1	M---	1111
RTRV-ALM-ENV	M---	1111
RTRV-ALM-EQPT	M---	1111
RTRV-ALM-OC3	M---	1111
RTRV-ALM-PORT	M---	1111
RTRV-ALM-RMT	M---	1111
RTRV-ALM-SDCC	M---	1111
RTRV-ALM-SML	M---	1111
RTRV-ALM-STS1	M---	1111
RTRV-ALM-SYCN	M---	1111
RTRV-ALM-T1	M---	1111
RTRV-ALM-T3	M---	1111
RTRV-ALM-VT1	M---	1111
RTRV-ALM-X25	M---	1111
RTRV-ATTR-BITS	M---	2000

NOTE: For Functional Category and Default COPC columns: M = Maintenance, P = Provisioning, S = Security, and T = Testing.

SECURITY/USER AUTHORIZATION

ISSUE 2	JULY 1994
ALCL 363-203-502	TNG
PAGE 13 of 18	510

Alcatel 1603/12 SONET Multiplexer

Security/User Authorization

Table A. 1603/12 SM Commands and Default Command Privilege Codes (COPC) (cont)

COMMAND	FUNCTIONAL CATEGORY	COPC (MPST)
RTRV-ATTR-COM	M---	2000
RTRV-ATTR-CONT	M---	2000
RTRV-ATTR-DLMAP	M---	2000
RTRV-ATTR-EC1	M---	2000
RTRV-ATTR-ENV	M---	2000
RTRV-ATTR-EQPT	M---	2000
RTRV-ATTR-OC3	M---	2000
RTRV-ATTR-PORT	M---	2000
RTRV-ATTR-RMT	M---	2000
RTRV-ATTR-SDCC	M---	2000
RTRV-ATTR-SML	M---	2000
RTRV-ATTR-STS1	M---	2000
RTRV-ATTR-SYCN	M---	2000
RTRV-ATTR-T1	M---	2000
RTRV-ATTR-T3	M---	2000
RTRV-ATTR-VT1	M---	2000
RTRV-ATTR-X25	M---	2000
RTRV-BITS	-P-	0200
RTRV-CMD-STAT	MPST	1111
RTRV-CNFGRN	M---	2000
RTRV-COND-BITS	M---	2000
RTRV-COND-COM	M---	2000
RTRV-COND-DLMAP	M---	2000
RTRV-COND-EC1	M---	2000
RTRV-COND-ENV	M---	2000
RTRV-COND-EQPT	M---	2000
RTRV-COND-OC3	M---	2000
RTRV-COND-PORT	M---	2000
RTRV-COND-RMT	M---	2000
RTRV-COND-SDCC	M---	2000
RTRV-COND-SML	M---	2000

NOTE: For Functional Category and Default COPC columns: M = Maintenance, P = Provisioning, S = Security, and T = Testing.

ISSUE 2	JULY 1994
ALCL 363-203-502	TNG
PAGE 14 of 18	510

SECURITY/USER AUTHORIZATION

Alcatel 1603/12 SONET Multiplexer

Security/User Authorization

Table A. 1603/12 SM Commands and Default Command Privilege Codes (COPC) (cont)

COMMAND	FUNCTIONAL CATEGORY	COPC (MPST)
RTRV-COND-STS1	M---	2000
RTRV-COND-SYCN	M---	2000
RTRV-COND-T1	M---	2000
RTRV-COND-T3	M---	2000
RTRV-COND-VT1	M---	2000
RTRV-COND-X25	M---	2000
RTRV-CRS-STS1	-P-	0200
RTRV-CRS-VT1	-P-	0200
RTRV-DLMAP	-P-	0200
RTRV-E2AMAP	-P-	0200
RTRV-EC1	-P-	0200
RTRV-EXT-CONT	M---	2000
RTRV-EQPT	-P-	0200
RTRV-FFP-OC3	MP-	2200
RTRV-FFP-STS1	MP-	2200
RTRV-FFP-VT1	MP-	2200
RTRV-HDR	MPST	1111
RTRV-INV-EQPT	MP-	2200
RTRV-LED	M---	2000
RTRV-LOG	M---	2000
RTRV-NE-ALL	M---	2000
RTRV-OC3	-P-	0200
RTRV-PM-EC1	M---	2000
RTRV-PM-EQPT	M---	2000
RTRV-PM-OC3	M---	2000
RTRV-PM-STS1	M---	2000
RTRV-PM-SYCN	M---	2000
RTRV-PM-T1	M---	2000
RTRV-PM-T3	M---	2000
RTRV-PM-VT1	M---	2000
RTRV-PMODE-EC1	M---	2000

NOTE: For Functional Category and Default COPC columns: *M* = Maintenance, *P* = Provisioning, *S* = Security, and *T* = Testing.

SECURITY/USER AUTHORIZATION

ISSUE 2	JULY 1994
ALCL 363-203-502	TNG
PAGE 15 of 18	510

Alcatel 1603/12 SONET Multiplexer

Security/User Authorization

Table A. 1603/12 SM Commands and Default Command Privilege Codes (COPC) (cont)

COMMAND	FUNCTIONAL CATEGORY	COPC (MPST)
RTRV-PMODE-EQPT	M---	2000
RTRV-PMODE-OC3	M---	2000
RTRV-PMODE-SYCN	M---	2000
RTRV-PMODE-T1	M---	2000
RTRV-PMODE-T3	M---	2000
RTRV-PORT	MP-	2200
RTRV-PTHTRC-STS1	M---	2000
RTRV-SDCC	-P-	0200
RTRV-SECU-CID	--S-	2222
RTRV-SECU-CMD	--S-	2222
RTRV-SECU-UPC	--S-	2222
RTRV-SECU-USER	--S-	2222
RTRV-SML	-P-	0200
RTRV-STATUS	MPST	2222
RTRV-STS1	-P-	0200
RTRV-SWVER-EQPT	M---	2000
RTRV-SYCN	M---	2000
RTRV-T1	-P-	0200
RTRV-T3	-P-	0200
RTRV-TH-EC1	M---	2000
RTRV-TH-OC3	M---	2000
RTRV-TH-STS1	M---	2000
RTRV-TH-T1	M---	2000
RTRV-TH-T3	M---	2000
RTRV-TH-VT1	M---	2000
RTRV-VT1	-P-	0200
RTRV-X25	-P-	0200
SET-ACO-COM	M---	2000
SET-ATTR-BITS	M---	2000
SET-ATTR-COM	M---	2000
SET-ATTR-CONT	M---	2000

NOTE: For Functional Category and Default COPC columns: M = Maintenance, P = Provisioning, S = Security, and T = Testing.

ISSUE 2	JULY 1994
ALCL 363-203-502	TNG
PAGE 16 of 18	510

SECURITY/USER AUTHORIZATION

Alcatel 1603/12 SONET Multiplexer

Security/User Authorization

Table A. 1603/12 SM Commands and Default Command Privilege Codes (COPC) (cont)

COMMAND	FUNCTIONAL CATEGORY	COPC (MPST)
SET-ATTR-DLMAP	M---	2000
SET-ATTR-EC1	M---	2000
SET-ATTR-ENV	M---	2000
SET-ATTR-EQPT	M---	2000
SET-ATTR-OC3	M---	2000
SET-ATTR-PORT	M---	2000
SET-ATTR-RMT	M---	2000
SET-ATTR-SDCC	M---	2000
SET-ATTR-SML	M---	2000
SET-ATTR-STS1	M---	2000
SET-ATTR-SYNCN	M---	2000
SET-ATTR-T1	M---	2000
SET-ATTR-T3	M---	2000
SET-ATTR-VT1	M---	2000
SET-ATTR-X25	M---	2000
SET-DAT	-P-	7777
SET-E2ADISP	M---	2000
SET-NE-ALL	M---	2000
SET-PMMODE-EC1	M---	2000
SET-PMMODE-EQPT	M---	2000
SET-PMMODE-OC3	M---	2000
SET-PMMODE-SYNCN	M---	2000
SET-PMMODE-T1	M---	2000
SET-PMMODE-T3	M---	2000
SET-PTHTRC-NE	M---	2000
SET-SYNCN	M---	2000
SET-TH-EC1	M---	2000
SET-TH-OC3	M---	2000
SET-TH-STS1	M---	2000
SET-TH-T1	M---	2000
SET-TH-T3	M---	2000

NOTE: For Functional Category and Default COPC columns: *M* = Maintenance, *P* = Provisioning, *S* = Security, and *T* = Testing.

SECURITY/USER AUTHORIZATION

ISSUE 2	JULY 1994
ALCL 363-203-502	TNG
PAGE 17 of 18	510

Alcatel 1603/12 SONET Multiplexer

Security/User Authorization

Table A. 1603/12 SM Commands and Default Command Privilege Codes (COPC) (cont)

COMMAND	FUNCTIONAL CATEGORY	COPC (MPST)
SET-TH-VT1	M---	2000
SW-DX-EQPT	M---	2000
SW-TOPROTN-EQPT	M---	2000
SW-TOWKG-EQPT	M---	2000

NOTE: For Functional Category and Default COPC columns: *M* = Maintenance, *P* = Provisioning, *S* = Security, and *T* = Testing.

ISSUE 2	JULY 1994
ALCL 363-203-502	TNG
PAGE 18 of 18	510

SECURITY/USER AUTHORIZATION

Gasoline From Coal?

ASK ANY bright first-grader what we're getting short of and he'll tell you it's gasoline. But what do we have a lot of? Coal. Why, the United States is to coal what the Middle East is to oil.

Since coal and petroleum are related chemically, both being fossil fuels coming from the remains of animals and plants alive when the world was knee-high to a dinosaur, why can't we simply convert coal to gasoline and have enough to run our cars and trucks until the next ice age?

The answer could be a surprise to many worried motorists. Truth is, we can convert coal to gasoline. We can do it and we have done it. And right now we're coming mighty close to the day when what you get out of a pump at Mobil or Shell or Exxon or the rest will, at least in part, not be gasoline but gasoal—fuel made from coal that looks like, smells like and propels your car just like the real stuff.

The experts say gasoal (or gascoal, coaline or coalene, if you prefer) is not now commercially feasible in the States. They're right, of course—but barely. The substance shown in the photograph on our cover is gasoal. And not a laboratory sample, either.

We bought that gasoal at a service station in Johannesburg, South Africa, and had it flown to New York. The pump it came from was just like our gas pumps in the States. Fuel like it flows every day from this pump into the gas tanks of cars, trucks and motorcycles.

Now South Africa may seem a long way away, and even the first-grader we were talking to a while ago might be able to tell you that, though you find a lot of diamonds over there, they got the short end of the stick when crude oil was passed out. Besides diamonds, however, South Africa has important coal deposits. So gasoal makes sense over there.

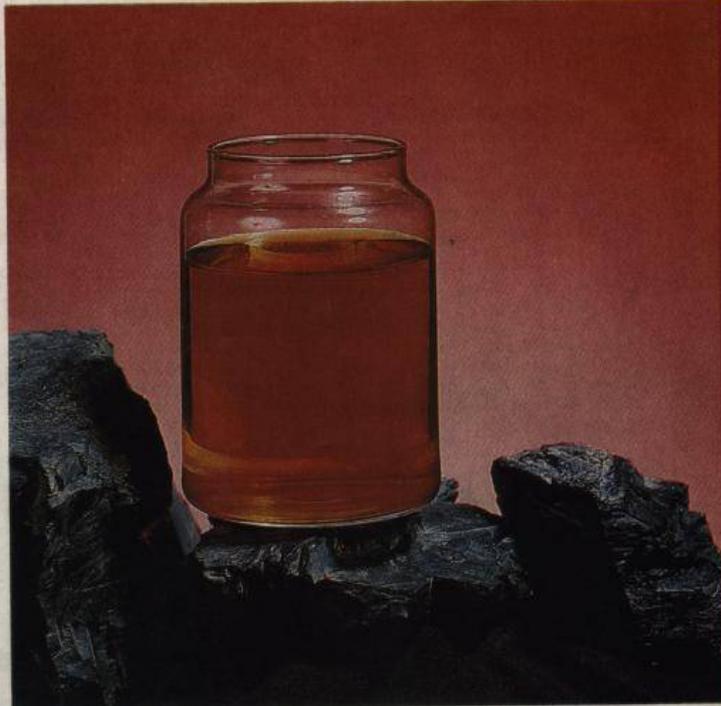
Five years ago we felt complacent about gasoline. It might be expensive and even scarce in En-

gland or Japan or Nepal but that would never happen here. Well, it has. And now is the time to get used to the idea that what South Africa is doing today, we'll probably be doing tomorrow.

It's a fact that a major movement toward gasoal and away from petroleum-derived gasoline right now would solve our energy problems almost immediately and for years to come. Of course, our coal reserves also have an end. So one day the specter of fuel shortages could haunt us again. Except by that time, we should have a new solution, which we'll discuss later.

The big oil companies—among them Mobil and Exxon—are busily engaged these days in further gasoal research. They obviously see the day of gasoline made from coal in filling-station pumps as being fairly close at hand. Otherwise, they wouldn't be investing money.

We've known how to make fuel from coal since back in the last century. Kerosene is also known as coal oil for obvious reasons. It's made from coal and came along when America was still working on its first century to replace whale oil in the lamps of the world. Kerosene is a less-volatile cousin of



GASOLINE from coal, or gasoal, is sold commercially in South Africa, where we bought our sample (being poured on our cover). That's coal in this photo, of course.

Gasoline From Coal?



COAL is plentiful in the U.S., petroleum much less so. This mountain of coal is being converted to electricity. It could as well be turned into gasoal to run cars.

Gasoline from Coal?

gasoline, both being hydrocarbons.

About three decades ago the federal government set up an experimental gasoal plant at Louisiana, Mo., a town on the Mississippi in an area where Tom and Huck used to hang out. The object was to prove that large-scale production of gasoal was feasible. And it succeeded. For every 500 lbs. of coal that went into the machinery, 13 gals. of gasoal came out.

There was a problem, of course. The stuff was costing about 19 cents a gallon to produce. If you added on normal oil-industry mark-up, the selling price would have been about 29 cents a gallon—at a time when you could buy low cut-rate gas for 17.9 cents.

Today even cut-rate runs about 56 cents. In that light, 29-cent gasoal looks great. Except its cost

and prospective price haven't stood still for 30 years. If you could draw gasoal out of a pump right now, the price would have to be about 90 cents a gallon.

Gasoline and gasoal are starting to move toward each other, however. The petroleum stuff is going higher and higher. Meanwhile, when the research being done on mass-production of gasoal is complete, we'll have the knowledge necessary for turning out millions of barrels a day, which is likely to bring the price down.

Someplace around the 75-cent area, gasoline and gasoal should meet one of these days soon. Alcohol may also saunter into the scene as we predicted in a report last January (Alcohol for Cars). What seems likely to happen is a fuel blend instead of a situation in which cars and trucks are running on all gasoline, gasoal or alcohol.

Gasoal normally has a lower octane rating than does its petroleum equivalent so a 50/50 blending with gasoline not only makes a better fuel but also achieves the desired goal of stretching our petroleum reserves. If you throw in the idea of alcohol as a similar stretcher-outer, the energy picture for the future looks much brighter. Alcohol, as we said in our January report, can be produced from the fermentation of any vegetable matter, which makes for an endless possible supply. Though, as we said, our coal reserves do have a limit—they aren't making that stuff anymore—the facts are pleasing.

In this country alone we have as much as a trillion tons of coal, enough to last hundreds of years if we keep using it at the current rate. Most of it is located out West or deep underground in eastern states.

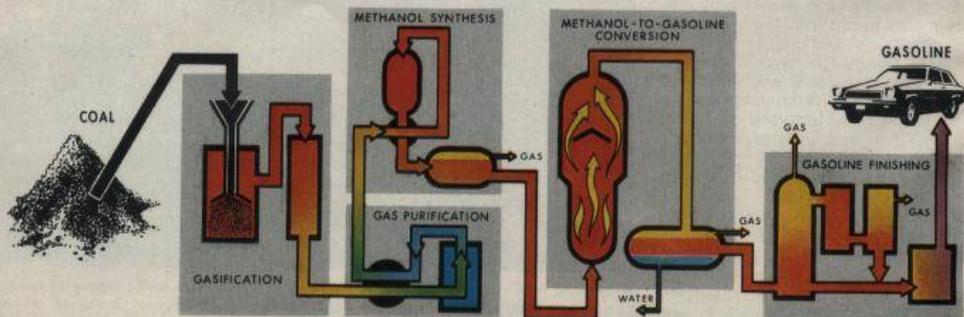
The reason coal can be converted to gasoal is that, like the crude from which gasoline is refined, coal is a hydrocarbon. So is natural gas.

Basically, the difference between coal, natural gas and petroleum is the amount of hydrogen and carbon they contain. Coal has less hydrogen than either oil or natural gas.

The trick to converting coal is to increase its hydrogen content. This can be done by putting it into a device resembling a pressure cooker, turning up the heat, then stirring in hydrogen and oxygen. Out comes synthetic gas or oil, depending on how much hydrogen you add and how long you let it simmer.

There are a bunch of coal-conversion processes aimed at making gasoal. Most involve lique-

CONVERTING coal to gasoline via the Mobil method (below). Coal is first gasified.



Gasoline From Coal?

faction, an intermediate step to produce crude oil that is then refined into gasoil, much as natural crude oil is refined into gasoline. But some gasoil processes include a gasification step—which means turning the material into a vapor somewhere along the line.

The main paths to gasoil currently being pursued take the scenic route—through crude oil via liquefaction. The problem is not a lack of technology to produce automobile fuel from oil but a shortage of oil. That's where coal comes in. Instead of a natural crude-to-gasoline chain, we're talking about adding one link and changing the others, making the chain coal-to-synthetic crude-to-gasoil.

The three processes aimed at producing the synthetic crude from which eventually comes gasoil are known as the Solvent Refined Coal (SRC), H-Coal and Exxon Donor Solvent (EDS) methods. Each follows its own variation of the coal-cooking recipe. Again, the output is oil, not gasoil.

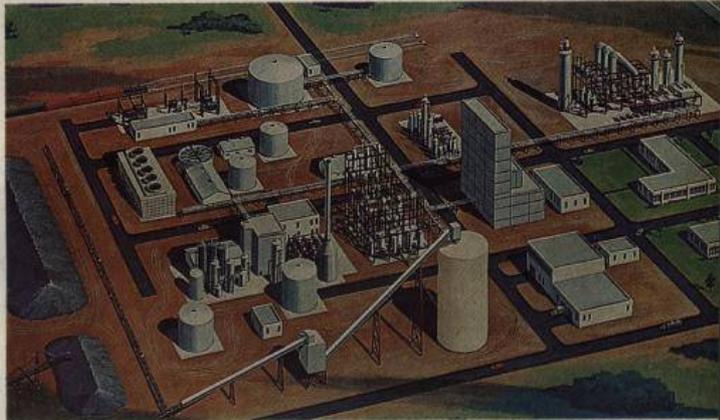
Two SRC pilot plants are operating, one in Tacoma, Wash., and another at Wilsonville, Ala. Originally, the SRC process was designed to clean up coal but the idea is being developed to make coal into a liquid.

Exxon Research and Engineering Co. has a small EDS test bed in operation, making about three barrels of oil a day from 1 ton of coal. A much larger 250-ton-a-day pilot plant is under construction in Baytown, Tex., near Houston.

An H-Coal pilot plant that will chew up 600 tons of coal a day and spit out some 2,200 barrels of liquid crude is shooting up at Catlettsburg, Ky. This project is a joint venture of Ashland Oil in Kentucky and Hydrocarbon Research, Inc., in Virginia.

While these methods look promising, they have their problems. One is cleaning up the liquids produced. When you open the spigot at the end of any of these processes, you don't get nice, clean oil, which is refinable into gasoil. What comes out is a nightmarish conglomeration of liquids, ash, unburned coal, some gas and other undesirables. And it's highly corrosive. This is not the road to gasoil. It's like the old joke: You can't get there from here.

So, instead of making liquid crude oil from coal, some other processes first turn it into gas, which is easier to clean. Then the



ARTIST'S concept of a plant to turn coal into gasoline. The economics of coal liquefaction are a bit out of step these days, but rising oil prices may change that.



TECHNICIAN at Mobil lab taps gasoline from methanol, which can be coal-derived.

clean gas is converted through a series of steps into liquid. This liquid is gasoil. The South Africans do it. So does Mobil Oil Corp., at its Paulsboro, N.J., research facility.

Researchers at Mobil had been working to develop catalysts (substances that promote chemical changes) for conventional refining of oil when they stumbled onto a material that promotes the conversion of wood alcohol (methanol) into gasoline.

Since methanol derives from

coal and the process is a proven one, the Mobil method completes the coal-to-gasoil chain. Mobil is considering a test plant to convert 4,200 gals. of methanol a day into gasoil.

A commercial-size liquefaction plant could create plenty of environmental and health problems. One reason would be sheer size, not to mention the amount of coal needed.

To be practical, a commercial operation would need at least 16,000 tons of coal per day—equal to the output of several large underground mines—and thousands of gallons of water. The plant would have to be built near coal and water to keep transportation costs down.

Of course, the practical route to gasoline from coal has to balance all the advantages and disadvantages. The cost of selling gasoil would become competitive if the price of getting conventional gasoline to the pump keeps rising.

Coal, gasoil, gasoline, alcohol—how's it all going to end? In the long view, the best bet would seem to be using both gasoil and alcohol to blend with and piece out our dwindling oil reserves. Long before the end is near for all fossil fuels, our grandchildren or great-grandchildren should be driving cars propelled by something we can only imagine now—atomic batteries, hydrogen briquets, supercondensed nitrogen or something we don't even know about in 1978. ●

Nortel DMS-100 Automatic Number Identification Attributes Table (ANIATTRS)

Table Name

Automatic Number Identification Attributes Table

Functional Description of Table ANIATTRS

Table ANIATTRS is a screening table that contains the Directory Numbers (DN) of subscribers whose calling line information will not be displayed to the terminating subscriber.

All Automatic Number Identification (ANI) digits datafilled in this table will have the Initial Address Message (IAM) calling party number parameter flagged as "presentation restricted."

Note: A Traffic Operator Position System (TOPS) toll office can provide operator services for Operator Assisted (OA) calls routed from non-TOPS toll offices. These calls arrive at the TOPS toll office over TOPS-type trunk groups. To provide screening at the TOPS toll office for these types of OA calls, the table ANIATTRS datafill in the originating non-TOPS toll office must be duplicated in the TOPS toll office. The duplicated datafill is only required in the TOPS toll office when office parameter SUPPRESS_ANI_TO_CLID_DISPLAY is set to "N" (no). If this parameter is set to "Y" (yes), all calls in the TOPS toll office will be flagged as "presentation restricted," regardless of the datafill in table ANIATTRS.

Datafill Sequence / Meaning & Table Size

There is no requirement to datafill other tables prior to table ANIATTRS. The minimum size of this table is 0 tuples. There is no restriction on the maximum size of this table.

Datafill

The following table lists datafill for table ANIATTRS.

Table ANIATTRS Field Descriptions

Field	Subfield	Entry	Explanation and Action
ANIKEY		See Subfields	<i>Automatic Number Identification Key</i> This field consists of subfields NPA, NXX, MS_XX, and LS_XX, which comprises the ten-digit ANI sequences of those subscribers that choose to have their DNs suppressed from display.
	NPA	200 to 999	<i>Numbering Plan Area</i> Enter the numbering plan area.
	NXX	200 to 999	<i>NXX</i> Enter the office code.
	MS_XX	00 to 99	<i>MS_XX</i> Enter a two-digit number.
	LS_XX	00 to 99	<i>LS_XX</i> Enter a two-digit number.

-End-

Datafill Example

The following example shows sample datafill for table ANIATTRS.

ANIKEY			
919	843	26	00
919	843	26	50
618	848	17	54

Portable Antenna Mast System

Overview

This is a simple antenna mast project which is designed to be both portable and rugged. Most other portable antenna mast designs are based around common PVC pipe, which severely limits the overall antenna height and size (wind load) they can handle.

The antenna mast design shown here will be based around common 3/4-inch and 1/2-inch diameter galvanized plumbing pipe and connectors. Using three sections of 4-foot long, 3/4-inch diameter galvanized pipe for the main mast will result in a very solid, 12-foot high antenna mast. The 3/4-inch diameter pipe will be a little too small for most stock antenna mounting brackets, so you may have to drill new antenna mounting holes or build your own bracket mounting system. Using larger diameter pipe for the bottom mast section and then tapering off with smaller diameter sections will also let you increase the overall antenna height. Non-metallic guy lines should be added if you want to go any higher, or if the antenna has a large wind load. The antenna stands leg's can also be stabilized to the ground using standard tent stakes, should you need to deploy on a grass or dirt surface.

Construction Notes & Pictures



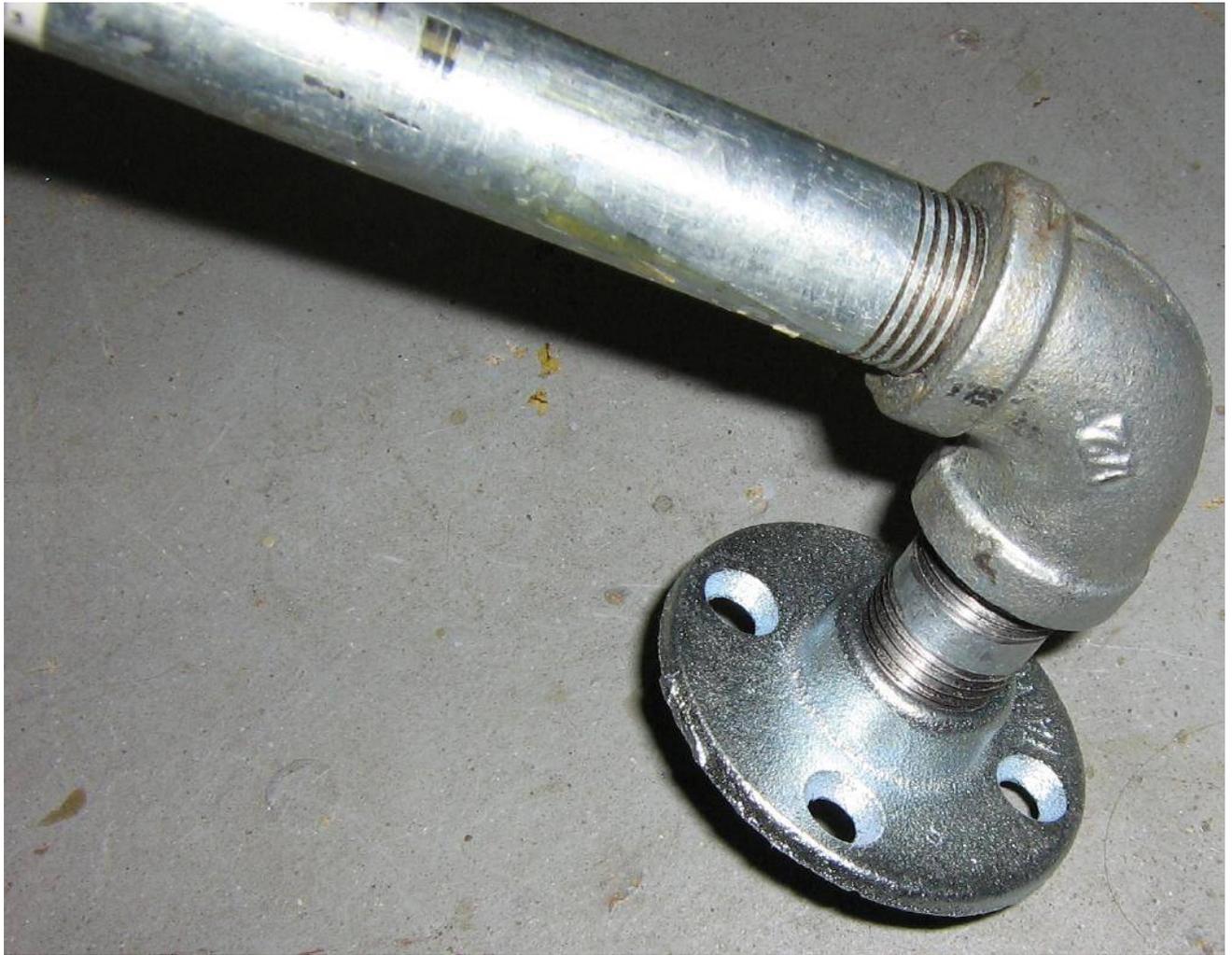
Antenna mast parts overview.

On the top-left are three, 4-foot long pieces of 3/4-inch diameter galvanized pipe, an optional top cap, and two 3/4-inch couplers, and a 3/4-inch threaded floor stand. These will be for the making the mast antenna mounts to.

Off to the far-right are four, 1-foot long pieces of 1/2-inch diameter galvanized pipe. These will be used to make the mast's base legs.

In the middle are four each of 1/2-inch diameter nipples, 90° elbows, and threaded floor stands.

You also need some assorted 1/4-inch stainless steel hardware. Wing nuts will be handy for quick assembly, and using stainless steel hardware will prevent rusting.

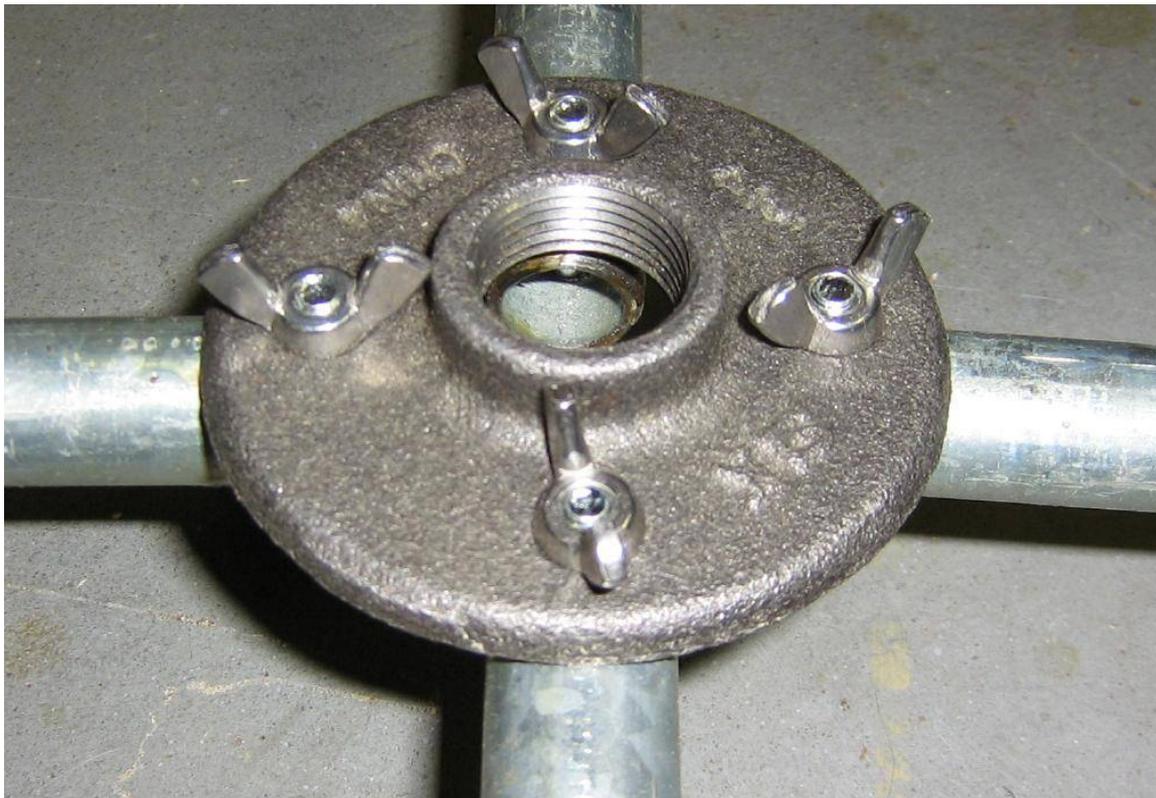


One leg of the mast's stand.

Take one of the foot long pieces of 1/2-inch diameter pipe, a 90° elbow, a short nipple, and a 1/2-inch threaded floor stand and put them together as shown. You may wish to add some Teflon tape to the threads to help secure the connections.



After you've made the four legs for the mast stand, drill a 1/4-inch hole through one end of the 1/2-inch diameter pipe, as shown above. This is how the legs will attach to the 3/4-inch floor stand which supports the main mast itself. Secure the legs using the 1/4-inch hardware.



Temporarily attach the legs to the center floor stand to check everything out. You can use whatever hardware is most convenient, but wing nuts are handy for quick assembly and disassembly.

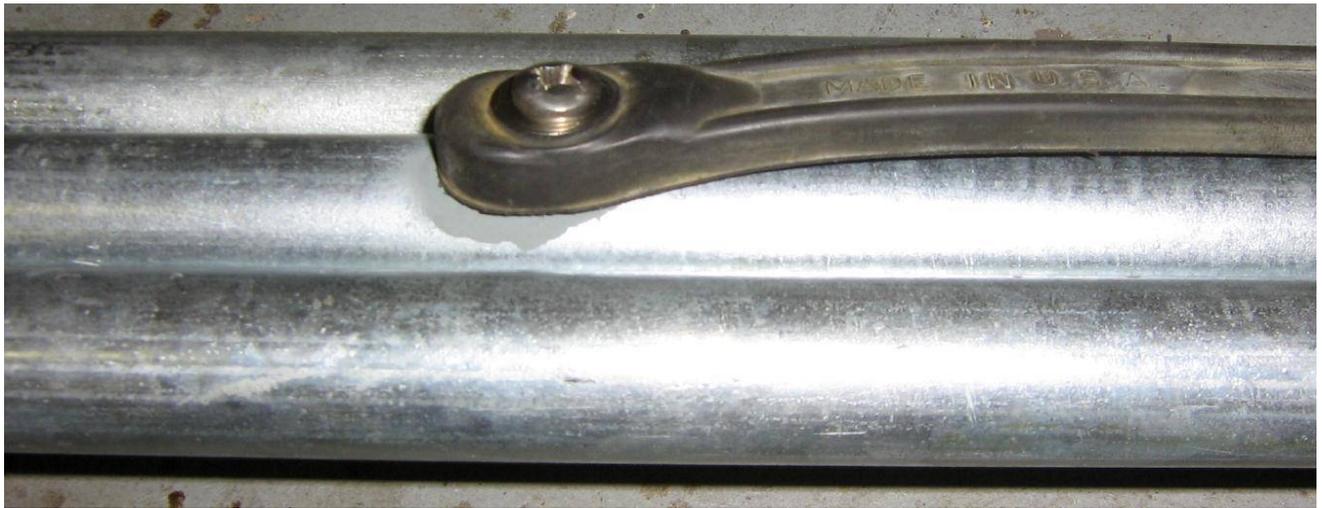


Overview of the finished antenna mast stand.

Double-check that each of the legs are level. Twist the legs slightly if they don't match up.



To store the mast sections during transport, drill holes through each of the 3/4-inch pipes near each end. Place a large 1/4-inch threaded bolt through them and secure with wing nuts.



Add an optional bungee cord handle to the center mast section to make the mast bundle easier to carry.



Completed portable antenna mast system.

You may wish to store the mast stand legs, couplers, securing hardware, antenna hardware, and a wrench in an old ammo box or duffel bag attached to the main mast sections.

You may also wish to add a small tool kit in case you need to add or fix any RF connectors or cables.

The antenna's coaxial cable should be secured to the mast sections with zip ties or reusable velcro straps.

You may also wish to mark the mast sections with some tape to help with mast section identification during disassembly and transportation.



Another 3/4-inch floor stand can be attached to the top mast piece to make a platform for a magnetic mount antenna.



Completed antenna stand in operation.

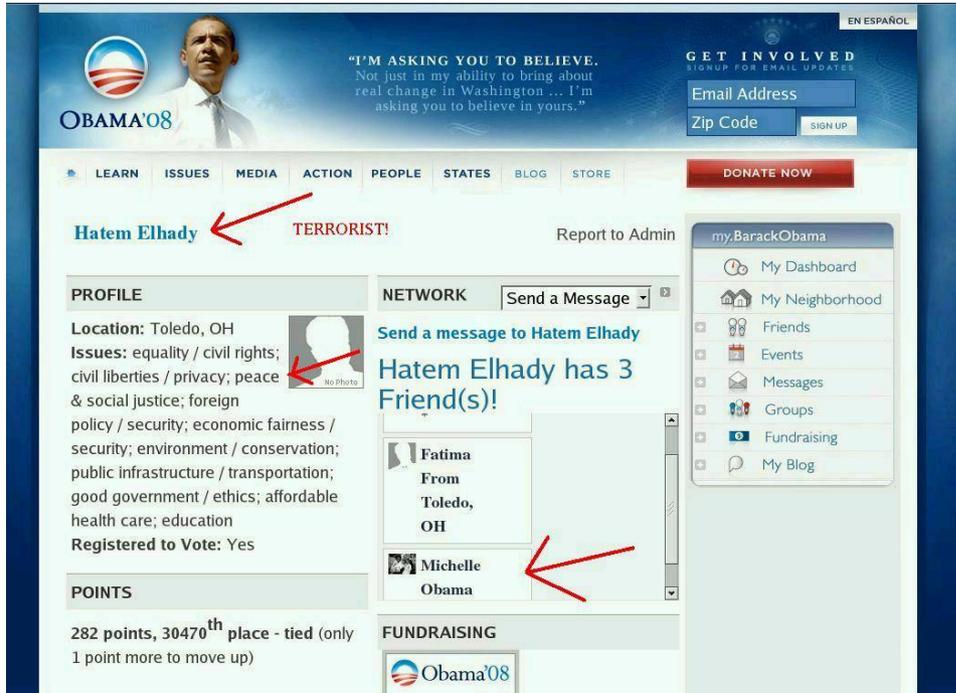


Looking up the mast.

Antennas with a large wind load should only use two sections of pipe (8-foot overall height) unless you add some mast support guy lines.

Zinc-chromate paint was sprayed around any holes in the pipe to prevent rusting.

Bonus



From: <http://my.barackobama.com/page/dashboard/public/gGN9pM>

Michelle Obama's name was removed from Hatem El-Hady's web page profile listing at the official Barak Hussein Obama '08 website.

Hatem El-Hady was the former chairman of the Toledo-based Hamas charity, Kindhearts. This was closed down in 2006 by the U.S. government for actively supporting terrorist fundraising.

More at Little Green Footballs: <http://littlegreenfootballs.com/article/29729>

The website's censors, err... "editors" eventually deleted the entire profile.



Change.

End of Issue #50



Any Questions?

Editorial and Rants

At the end of every sentence in this article, say the word "niggers."

Report Warns of Black–White Gap in Madison

April 29, 2008 – From: www.madison.com

By Chris Rickert

Known nationally as a liberal enclave and regularly named one of the most livable cities in the United States, Madison still struggles with wide disparities between blacks and other racial groups when it comes to educational attainment, economic well-being and other factors, a report has found.

"The State of Black Madison 2008: Before the Tipping Point," released Tuesday by the Urban League of Greater Madison and representatives from five other local groups, draws on existing data to illustrate gaps between blacks and the community at large in six areas: experience in the criminal justice system, economics, education, health care, housing and political influence.

"It's certainly not the south side of Chicago yet," said Urban League president and CEO Scott Gray, speaking of the potential for an enduring underclass in Madison. "But it could grow into a problem. For the black community, it's starting to tip that way."

That blacks in Dane County are 13 times more likely to be newly incarcerated than the rest of the population or that blacks are about 20 percent less likely to have a high school diploma are evidence of these gaps, which most Madisonians are "absolutely not" aware of, said Kenneth Black, president of 100 Black Men of Madison.

"It's a great town for them and not so great for the African-American community," he said. "There are some shortcomings."

In some areas, the differences were starker in Madison than nationally, although blacks also tended to do better as a group on some measures than blacks nationwide, according to the report. It's also clear that Madison as a whole ranks better on measures such as educational attainment and employment rate, which exacerbates disparities with the black population.

"This is a town where you have to have more than even a college degree to get a job," said Gray.

Mayor Dave Cieslewicz said the report "identifies some very important issues in the community" and pointed to the city's efforts to help support the creation of the Urban League's new work force development center at the Villager Mall and black and Latino business organizations.

He agreed many residents will likely be surprised at how wide some of the gaps are, and said, "We can't think of ourselves as a successful community unless everyone has an opportunity to share in that success."

Gray said the groups' next steps are to reach out to political, educational and business leaders and to convene a summit of black community leaders to discuss the problems and come up with strategies for solving them.

He was hopeful the city will respond.

"Madison is a relatively ... small city and you can get your arms around these issues," he said.

Highlights of the Report

From "The State of Black Madison 2008: Before the Tipping Point," based on data reported in recent years:

CRIME: Blacks in Dane County were 13 times more likely to be newly incarcerated than the population as a whole in 2002.

ECONOMICS: A larger percentage of Dane County's black population lived in poverty in 2000 than did the nation's black population.

EDUCATION: Almost a third of black students in the Madison School District were in special education programs.

HEALTH CARE: Blacks in Dane County are 10 times as likely to rely on government-provided health insurance than the population at large.

HOUSING: There was less racial disparity in Dane County than in the nation as a whole in 2000 when it comes to home values.

POLITICAL INFLUENCE: A little less than 60 percent of black Madison voters cast ballots in the 2004 presidential election. Almost 75 percent of the community as a whole did.



Health | Most Popular

World Video Middle East Europe Latin America Africa Asia Canada Australia/Antarctica
Kevin Sites

Search: All News

Vietnam to try American for terrorism 

WORLD VIDEO **Healing the world through film** CNN
 **Myanmar speaks at U.N.** CNN
 » All news video

Thu May 8, 7:49 AM ET

HANOI, Vietnam - A Vietnamese-American and two Vietnamese nationals will be put on trial on charges of terrorism for allegedly planning to distribute anti-government pamphlets in Vietnam, an official said Thursday.

Nguyen Quoc Quan, of Sacramento, and Vietnamese nationals Nguyen Hai and Nguyen The Vu face jail terms of up to

ADVERTISEMENT
 Privoxy blocked
http://ad.yieldmanager.com/st?ad_type=iframe&
 See why or go there anyway.

From: http://news.yahoo.com/s/ap/20080508/ap_on_re_as/vietnam_dissident_trial_1

Reminder: There is no liberal bias in the media!

At the end of every sentence in this article, say the word "spics."

Local 10-Year-Old Gives Birth to Baby Girl

May 7, 2008 – From: www.kidk.com

By Nate Eaton

It's an unbelievable story that has an entire community in shock. Several sources confirm a 10-year-old girl from St. Anthony gave birth to a little girl on Saturday at Madison Memorial Hospital in Rexburg.

The girl was allegedly raped by 37-year-old Guadalupe Gutierrez-Juarez. Gutierrez-Juaraz is an illegal immigrant who is in the Fremont County Jail on rape charges.

Gutierrez-Juarez was arrested April 29th after medical personnel alerted police that a pregnant child had come in for treatment. That child is now one of the youngest mothers in Idaho.

Counselor Matt Christensen has worked with sexually abused kids for over 10 years. Although he has nothing to do with this specific case, he's seen pregnancies affect other teenagers.

Matt Christensen, Counselor: "Children go through development stages and when something seriously traumatic hits, they tend to stop the development phases at that point."

It's unclear who will take custody of the newborn, what will happen to the ten year old, and if Gutierrez-Juarez will face charges. The St. Anthony police department is still conducting an investigation against Gutierrez-Juaraz so officers did not want to comment on the case. They say more details may be released later.

Gutierrez-Juarez is being held on 250 thousand dollars bond. Even if he did post the required amount, he would not be released because he is an illegal immigrant.

Another spic shitting out a low-I.Q. subhuman.

Note how it says the phone was disconnected. She's probably an illegal and poor, but can somehow "afford" to have a kid while only 17 years old.

No, wait... Bend over tax payers!

Local 10-Year-Old Gives Birth to Baby Girl

May 3, 2008 – From: ap.google.com

LONG BEACH, Calif. (AP) -- A 17-year-old girl gave birth secretly at home, then walked four blocks to a hospital with the baby still attached by its umbilical cord.

"I was just a little nervous" when the labor began, Xochitl Parra said Friday from St. Mary Medical Center as she cradled her 8-pound, 3-ounce son, Alejandro.

The boy was normal and "eating like a champ," said Dr. Jose Perez, director of the Neonatal Intensive Care Unit.

The teenager said she was alone and taking a shower around 5:30 a.m. Wednesday to get ready for school. Then the contractions took over.

"I felt his head coming, so I sit down and pushed so he could come out," she said.

Parra did not call 911 because the home phone was disconnected, and she did not want to wake the neighbors because it was so early. Instead, she wrapped the baby, got dressed and went to the hospital on foot.

"I started walking and jogging to the hospital," she said.

The teen came into the hospital lobby and asked for help, Perez said.

"She still had the placenta and the baby was still attached, so of course everyone said, 'Don't move!'" he said.

Perez praised the girl for taking quick action.

"They could have bled to death; thank God that didn't happen," the doctor said. "She was very clever. She knew what to do. She wrapped the baby up and walked over here."

Parra, a sophomore at Long Beach Poly High, said she had kept her pregnancy a secret because she was afraid her mother would "kick me out of the house." Her mother has now accepted the situation and is going to help the teen care for the baby so she can continue attending school, Parra said.

Perez called the outcome "heartwarming."

"We hear so much negative with teenagers throwing their babies in the Dumpsters," he said. "This baby is fine, and hopefully there will be a happy ending with the extended family."

The CIA "Psychic" Comedy

This is from a 1996 posting to *The Randi Hotline*, a mailing list run by well known skeptic James Randi of the James Randi Educational Foundation, <http://www.randi.org>.

From: James Randi --- Wizard (randi-hotline@ssr.com)
Date: Sun, 28 Jan 1996 01:57:27 -0500

NOW WE KNOW....

When we all learned that Ed May, the scientist, was in charge of spending 20 million dollars of our money to direct a team of "psychics" (I've always preferred the collective noun "giggle" to designate a group of these) for defense purposes, we felt a certain further failing of our confidence in the common sense of our government. What I'll tell you here with do nothing to restore it.

May figured that the psychics were about 15% correct in their guesses. It might be fairly said that that's not anything to take to the racetrack, but how was that figure arrived at? The success rate of a rambling discourse about "I feel that maybe..." and "Perhaps it might be that..." would seem difficult to arrive at. But when asked about this, Dr. May illustrated his method, and also the difficulties that it entailed.

There was always a general of some sort looking over his shoulder, waiting to be alerted to any disaster that might come via crystal ball, Tarot cards, fortune cookies, or whatever. Then one of the highly talented psychics that we were paying to sit around and guess, declared that she'd had a strong vision that a gang of Lebanese terrorists were going to take over a United Airlines jumbo jet at Washington's National Airport, load it with high explosives, and steer it into the Congress while Ronald Reagan was delivering his State of the Nation speech a few days from then. And, said the psychic, she felt there was also a lady in a red dress here, somewhere. (Perhaps she'd been mis-tuned in on the Dillinger capture by the Feds, back in 1934. That happens a lot in psychic circles, y'know.) Much alarmed, May informed his general of this prophecy.

"Are you telling me this officially, or unofficially?" demanded the officer. "If it's officially, I'll have to call out the militia, close down the airport, reroute all commercial aircraft, and spend millions to do it. If it's unofficial, I'll just ignore it." Well, Dr. Strangelove -- uh, I mean, Dr. May -- was in a dither, but bravely decided to fly in the face of this Cassandra by making his report officially unofficial.

Reagan lived through the day (probably guided by his astrologer!) the Congress did not go boom, and no Lebanese villains showed up. But, Dr. May pointed out, all validation was not lost by the psychic, for -- hold your breath -- Margaret Thatcher showed up in a red dress! Wow!

The mind boggles....

James Randi



Tell-ah Amnesty-ia Internationllia to-ah fuck-ah off-ah!

Italy Condemned for 'Racism Wave'

May 28, 2008 – From: news.bbc.co.uk

Human rights group Amnesty International has said it is extremely alarmed by what it calls a "climate of discrimination" in Italy.

The Italian section of the rights body said recent tough new immigration measures were a worrying trend.

It added that politicians from both sides of the spectrum were legitimising the use of racist language.

Last week, Italy's new centre-right government introduced a series of measures aimed at improving security.

Illegal immigration will become punishable by up to four years in prison, it will be easier to expel illegal immigrants and there will be a three-year prison sentence for using minors to beg for money.

But the head of Amnesty International in Italy, Daniela Carboni, said the moves represented "heavy restrictions and new crimes that will target, above all, immigrants".

She said the organisation was particularly worried by the measure that would mean attempted illegal immigrants could be held for up to 18 months in a detention centre.

"Amnesty International is extremely alarmed both by the contents and haste of these measures... and by the climate of discrimination which preceded them," Ms Carboni said in the report.

There is deep suspicion throughout the country of the Roma community, whom many Italians blame for a disproportionate amount of crime.

In mid-May Italian police were forced to intervene to protect Roma Gypsies who came under attack from local residents in Naples, who set their camps alight.

Ms Carboni urged the Italian government to investigate fully the torching of the two Roma slum communities.

In April's national elections the centre-right coalition led by Silvio Berlusconi – which includes the anti-immigration Northern League and the post-Fascist Alleanza Nazionale – swept to victory, pledging to tackle illegal immigration.

In Rome, Gianni Alemanno, also of the Alleanza Nazionale, was elected mayor on a pledge to expel 20,000 people.

I want to be a sophisticated European too!!!

Serbian civilians killed, and internal organs stolen, by Croatians, or Albanians, or whatever the fuck they call themselves today...

