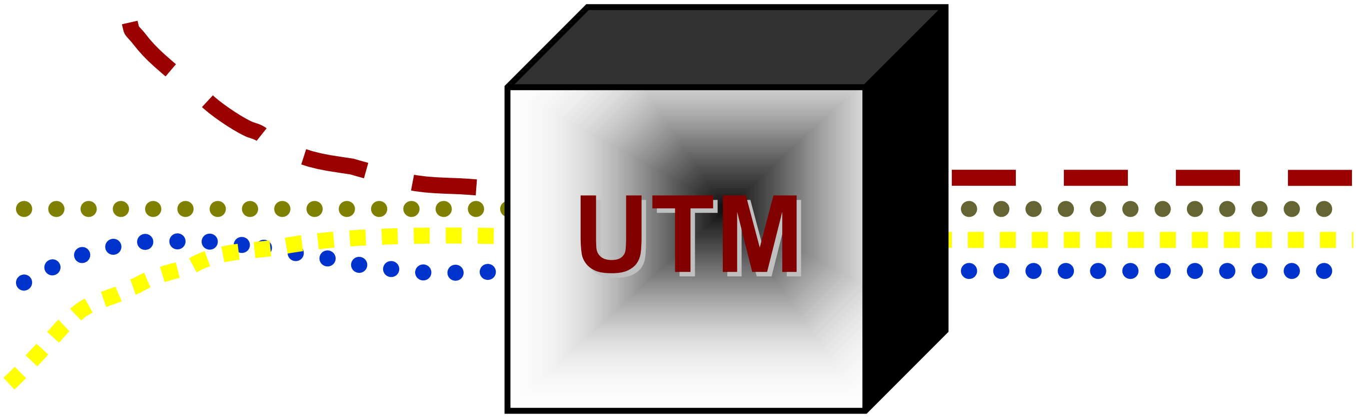
U T M

UNIVERSAL TRUNK MODULE

USER'S MANUAL



RELEASE 17.X

Manufacture & Distribution:

102 SW Orange Blossom
Lake City, Florida
32025-1613
phone: 386-754-5700
email: sales@trdcusa.com
http://www.trdcusa.com

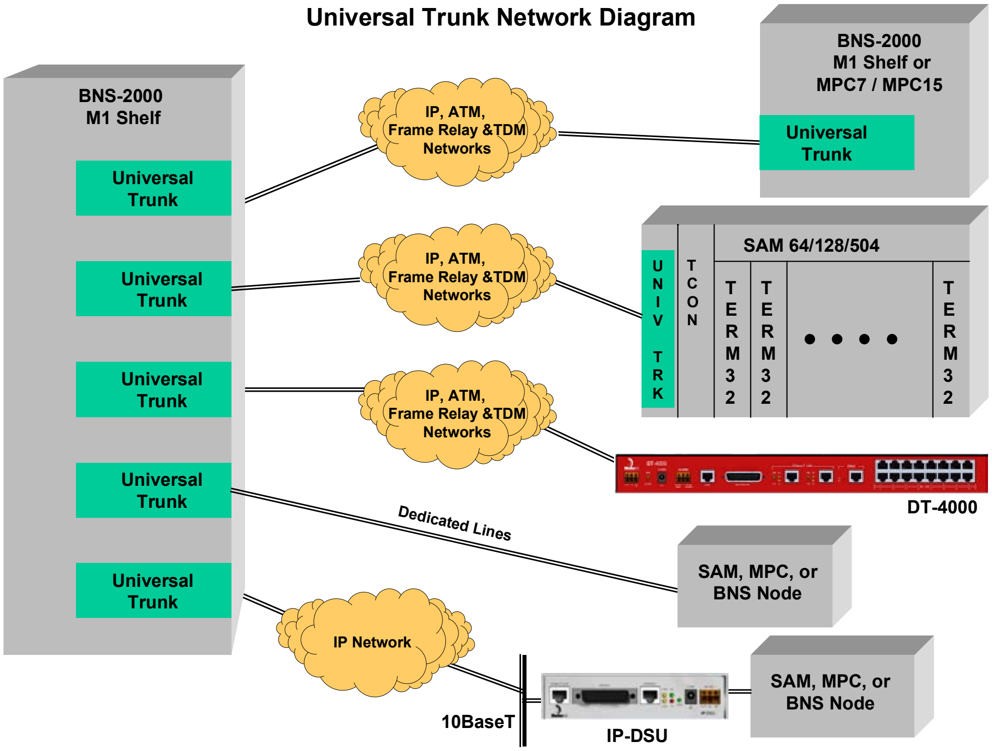
http://www.datatekcorp.com

Table of Contents

1 INTRODUCTION

The Universal Trunk *(UTM)* is a BNS module that allows the customer to employ more cost-effective interconnection facilities between Nodes and other BNS product family components *(Remote Shelves and SAM devices)*. Facilities such as IP, ATM or Frame Relay can be used rather than traditional leased line services thus permitting the movement of the BNS products toward the network edge.

Universal Trunk Network Diagram



The UTM supports an IP infrastructure, which is compatible with an IP-DSU[1]. It also supports a base protocol layer of HDLC, Frame Relay and AAL5 ATM all at rates up to E1. The transport layer is implemented using the BNS DDS, SWT, or PQ trunk protocols. UTM trunk interfaces can be duplexed for higher reliability as well.

Basic IP operations are supported even when the 10BaseT interface is not being used for transport. These IP applications include ICMP *(ping)*, the Telnet Console, and SNMP.

The Universal Trunk is a companion product to the DT-4000[2] and supports the same trunk interfaces. Being a *firmware* based trunk module the UTM may be installed in a SAM64, SAM128,

[1] The IP-DSU allows router (IP) networks to carry both its original traffic and its new BNS-2000/BNS-2000 VCS trunk traffic simultaneously. The IP-DSU replaces an existing, conventional DSU on each end of the circuit and eliminates the interconnecting dedicated facility.

[2] The DT-4000 is a product existing in BNS and IP networks simultaneously. It appears to the BNS as a SAM16, but also supports IP interfaces and significantly higher port speeds. The DT-4000 communicates via Frame Relay, ATM or IP across the backbone network and becomes a standalone edge device in non-BNS networks

SAM504 or Multi-Purpose Concentrator *(MPC)* to upgrade the device’s trunk options and capabilities.

In order to support older controller releases, the UTM reports identifies itself to the BNS Control Computer as either a TRK-T1, SAMSL, TRK64 , CPM-HS, or as an SWT module. Therefore, a BNS generic software update is **not** required for the UTM.

The UTM can field upgraded. Upgrades are accomplished through two different I/O interfaces accessed via its I/O board: Telnet or RS-232C.

The UTM houses an SNMP Version 1 agent and supports a large array of MIB variables. **Trap**, **Set** and **Get** operations are available as well.

The **UTM** supports up to two TACACS+ RADIUS servers for login authentication. These are a primary, and a secondary, although each is individually enabled. The TACACS+ support is for either encrypted, or clear authorization. Encryption keys may contain spaces.

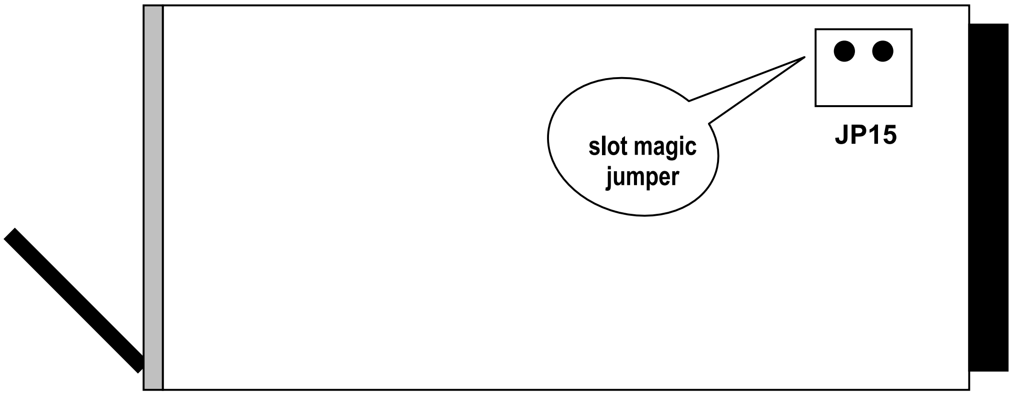
2 PHYSICAL DESCRIPTION

2.1 MODULE

The UTM is shipped from the factory with the slot “magic” jumper disabled. The “magic” jumper is only used when the UTM is installed in a remote shelf, or when connectivity to a remote shelf is a network.

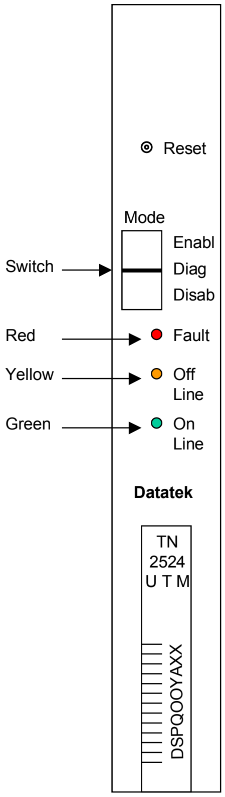
<u>Configurations requiring the jumper to be **enabled** are:</u>

- ❑ UTM in Node directly connects to a Remote Shelf (MPC) – **set jumper**
- ❑ UTM in MPC directly connects to a node – **set jumper**
- ❑ UTM in Node and connecting to IP, ATM or FRM networks – **set jumper**



2.2 2.2 Faceplate

2.2.1 Light Emitting Diodes (LED)



The lights on the module faceplate are **green**, **amber**, and **red**. They indicate on-line, off-line, and fault states respectively. When the module circuitry detects an on-board fault, the red LED *(fault)* is lit.

2.2.2 Mode Switch

The Mode Switch supports three positions: **Enabl**, **Diag** and **Disab**. The Mode switch must be in the **Enabl** position for the UTM to function properly.

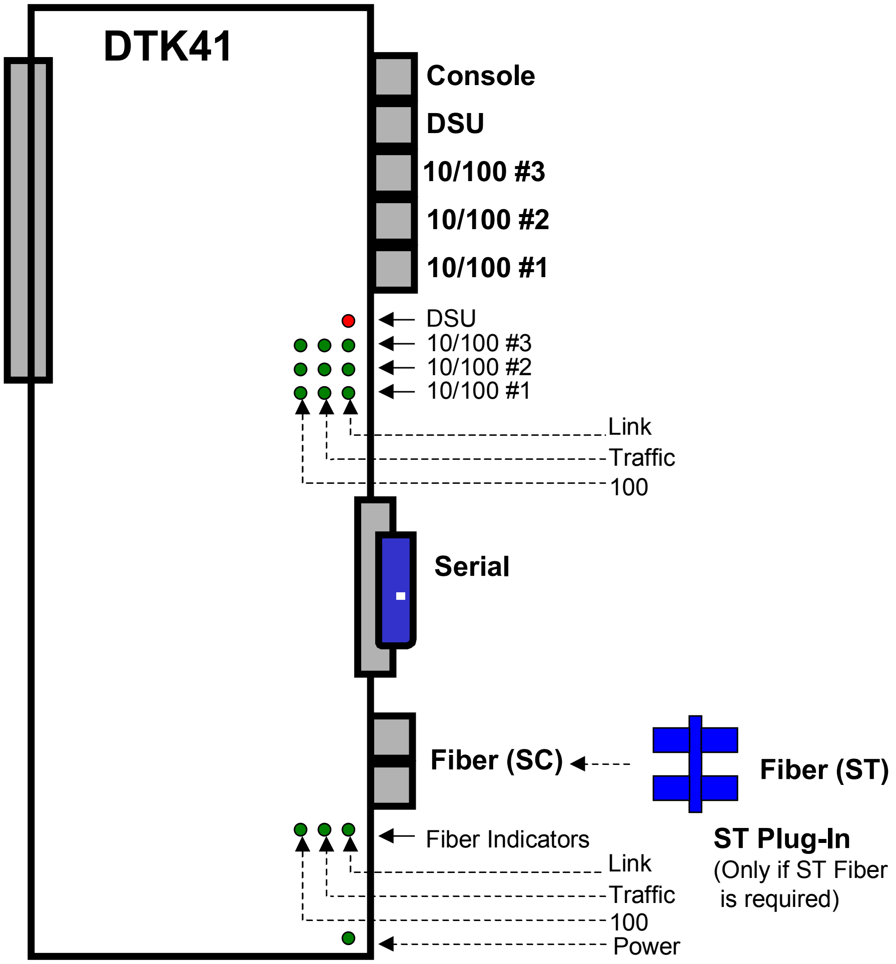
2.2.3 Reset Button

When the Reset button is pressed, the module buffers and registers are cleared, and the module application program is restarted. The module is taken out of service, and all connections are terminated.

2.3 High Performance I/O Board

The UTM[3] mates with the DTK41 High Performance I/O (HPIO) board in support of the UTM connectivity options. The DTK41 I/O board contains all the necessary connectors the UTM requires for currently available Console and LAN connections.

Note: Cables and adapters are available



2.3.1 Serial

The UTM Serial interface is software configurable. Options are as an RS-232C DTE for serial rates up to 64Kbps, or as a V.35 DTE for serial rates up to E1.

[3] A Series 1:2 UTM is required for the DTK-41 (or any other I/O board which requires power) since the original UTM did not provide any power whatsoever to the I/O module, and the original UTM did not provide a management interface.

2.3.2 CONSOLE

The UTM Console interface may be used for console activities and the initial configuration. It assumes the connected device is configured as 9600 baud, 8 bits and no parity.

2.3.3 10/100 BASET AND FIBER LAN

The DTK41 LAN and Fiber ports are used for IP network connectivity. The UTM simultaneously supports IP-DSU style BNS trunks and Internet peer level protocols *(e.g. IP, TCP, UDP, ICMP and SNMP)*. All of the 10/100 ports are fully switched, not bridged. The capacity of the switch is over 1Gbps. The 10/100 and Fiber ports are managed from the UTM console. Each 10/100 port and the Fiber port may be enabled or disabled individually. Alarms are generated if a link is established, or if a link is lost.

An advanced feature DTK41 is that no crossover cable is ever required on the 10/100 ports. The 10/100 ports will automatically correct for the cabling mismatch.

The 10/100 ports will self-configure to match the speed of the link (10 Mbps or 100 Mbps), and the Duplex (Full or Half). No configuration is required.

The Fiber interface connects to the industry standard SC cabling. If ST cabling is used, the DTK41 ST plug-in module is used. No adapter cables are required.

2.3.4 DSU

The UTM DSU *(4-wire)* interface is software configurable for T1 or E1 rates. A value of T1 is used for domestic 1.544 MHz interfaces with 193 Bit Superframes. A value of E1 is used for European 2.048 MHz interfaces with 256 Bit Superframes. The DSU functionality is built in. This interface may be used for connectivity to TDM Trunks, Frame Relay and ATM networks.

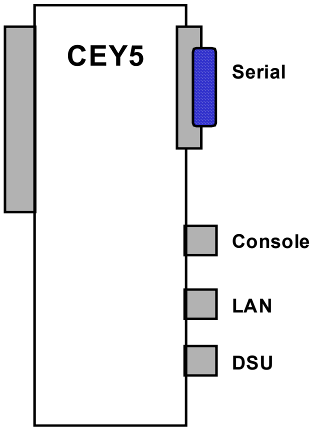
2.3.5 VARIANTS

The **DTK41** high performance I/O board is available with two different mounting brackets. The **DTK41N** incorporates a mounting bracket specifically designed to be installed in a BNS node, a Datakit VCS node, or an MPC. The **DTK41S** has a mounting bracket specifically designed to be placed in a SAM504, SAM64, or SAM128.

2.4 STANDARD PERFORMANCE I/O BOARD

The UTM mates with the CEY5 (or CEY6) I/O board in support of the UTM connectivity options. The CEY5 (or CEY6) I/O board contains all the necessary connectors the UTM requires for currently available Console and 10BaseT LAN connections.

Note: Cables and adapters are available



2.4.1 SERIAL

The UTM Serial interface is software configurable. Options are as an RS-232C DTE for serial rates up to 64Kbps or as a V.35 DTE for serial rates up to E1.

2.4.2 CONSOLE

The UTM Console interface may be used for console activities and the initial configuration. It assumes the connected device is configured as 9600 baud, 8 bits and no parity.

2.4.3 LAN

The UTM LAN interface is used for IP network connectivity. It simultaneously supports IP-DSU style BNS trunks and Internet peer level protocols *(e.g. IP, TCP, UDP, ICMP and SNMP)*. The LAN interface supports 10BaseT.

2.4.4 DSU

The UTM DSU *(4-wire)* interface is software configurable for T1 or E1 rates. A value of T1 is used for domestic 1.544 MHz interfaces with 193 Bit Superframes. A value of E1 is used for European 2.048 MHz interfaces with 256 Bit Superframes. The DSU functionality is built in. This interface may be used for connectivity to TDM Trunks, Frame Relay and ATM networks.

2.4.5 VARIANTS

The **CEY5** I/O board is available with two different mounting brackets. The **CEY5** incorporates a mounting bracket specifically designed to be installed in a BNS node, a Datakit VCS node, or an MPC. The **CEY6** has a mounting bracket specifically designed to be placed in a SAM504, SAM64, or SAM128.

3 INSTALLATION

UTM installation consists of:

- ❑ inserting the DTK41 or CEY5 I/O distribution board into the backplane slot
- ❑ inserting the module in the corresponding shelf slot
- ❑ cabling console and data ports

Note: To avoid damage to electronic components from ESD (Electro Static Discharge) always wear an ESD wrist strap. To prevent damage to module circuitry, always insert the I/O board before inserting its corresponding module. Never remove the I/O board before removing the module.

3.1 INSERTING THE I/O BOARD

The I/O board plugs into the backplane at the rear of the shelf. It is held in place by shrouds on the backplane pinfield and secured with two screws. Insert the I/O board before inserting its corresponding UTM.

- ❑ Align the I/O board backplane connector with the backplane pinfield and align the screw slots with the screw holes.
- ❑ Slip the backplane connector onto the pins. The board should seat easily. If seating is difficult, the board may be canted or some pins may be bent.
- ❑ Insert the screws, and tighten them securely.

Removing the I/O Board

Remove the I/O board only for relocation, replacement, or board type confirmation.

Note: The Module in the slot corresponding to the I/O board must be removed first.

- ❑ Disconnect all cabling to I/O board ports, labeling the cable ends if appropriate.
- ❑ Remove the screws holding the I/O board in place.
- ❑ Carefully rock the board as you pull it out.

Inserting the UTM

Note: The I/O board for the module must be installed in its corresponding slot on the backplane at the rear of the shelf first.

- ❑ Set the mode switch on the module faceplate to **Disab**.
- ❑ With the module latch extended, carefully push the module all the way into the slot. The backplane pins slip into the module receptacle.
- ❑ Close the latch to lock the module into position.
- ❑ Move the mode switch on the module faceplate to **Enabl**.

Removing the UTM

Note: You can remove and replace a UTM in an operating node without damaging the module itself, or without disrupting calls on other modules. Only the calls on the UTM being removed are disrupted. Remember that the I/O board for the module must still be in its corresponding slot on the backplane at the rear of the shelf.

- ❑ If the mode switch is in the **Enabl** position, move it to **Disab**.
- ❑ Open the latch on the module faceplate.
- ❑ Pull the module straight out of the slot.

3.2 CABLING

This section provides information on how to cable the UTM console and data ports with the DTK41 I/O board, or the CEY5 I/O board.

Consult the following table for ordering information regarding all of the cabling options shown in this section.

Depending upon access availability, the following cables will be needed to setup a UTM console connection.

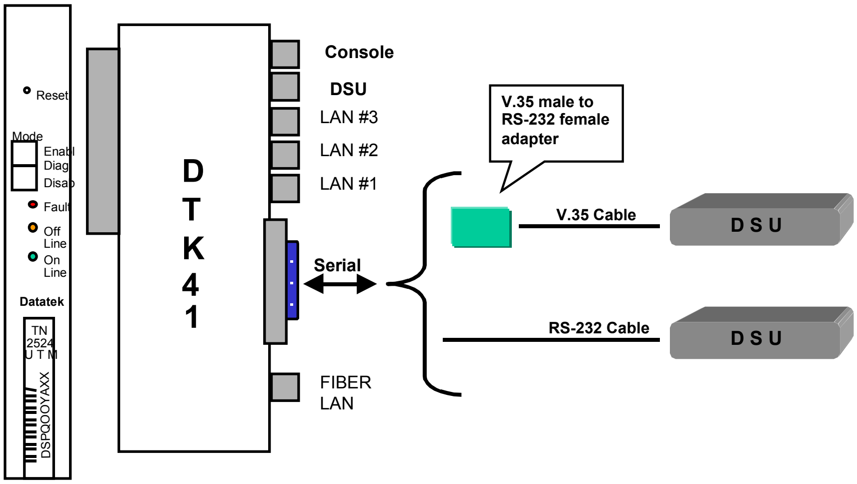
Cable / Adapter	Description
258B adapter	50-pin M to 6 8-pin mod
CS25AS-MOD	50-pin 180-M to 34-pin V.35
V.35 to RS-232C adapter	Male 34 pin V.35 to Female DB25
V.35 to RS-232C adapter	Female 34 pin V.35 to Male DB25
T1 crossover modular cable	8-pin mod to 8-pin mod
Mod DB15 adapter	8-pin mod to DB15 M
D8AH-M adapter	25-pin M to mod socket
D8AH-F adapter	25-pin F to mod socket
D8AG-M adapter	25-pin M to mod socket
D8AG-F adapter	25-pin F to mod socket
Console Cable (special wiring)	8-pin mod to 8-pin mod
Straight modular cable	8-pin mod to 8-pin mod
CAT5 modular cable	8-pin mod to 8-pin mod (shielded)

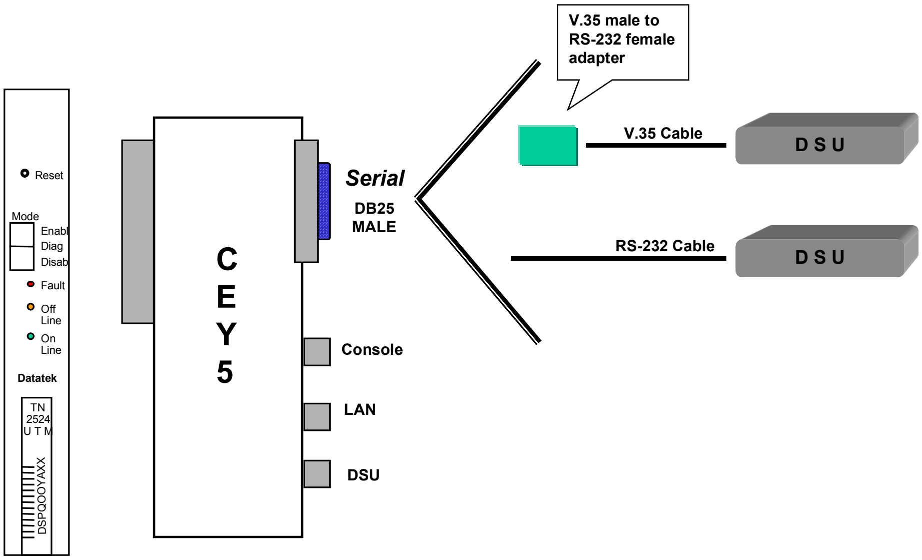
Notes:

- ❑ *Use an AG adapter to talk to a terminal and an AH adapter to talk to a modem.*
- ❑ *The AH adapter will be used to terminate the cable and will be attached to the appropriate device. The attached device will determine the gender of the AH adapter.*

3.3 CABLING THE I/O MODULE SERIAL PORT

When cabling the Serial port, a UTM circuit pack and an I/O board is required. The cabling is identical for a DTK41 or a CEY5 I/O board. The cable will terminate into either a DSU or DSU/CSU.

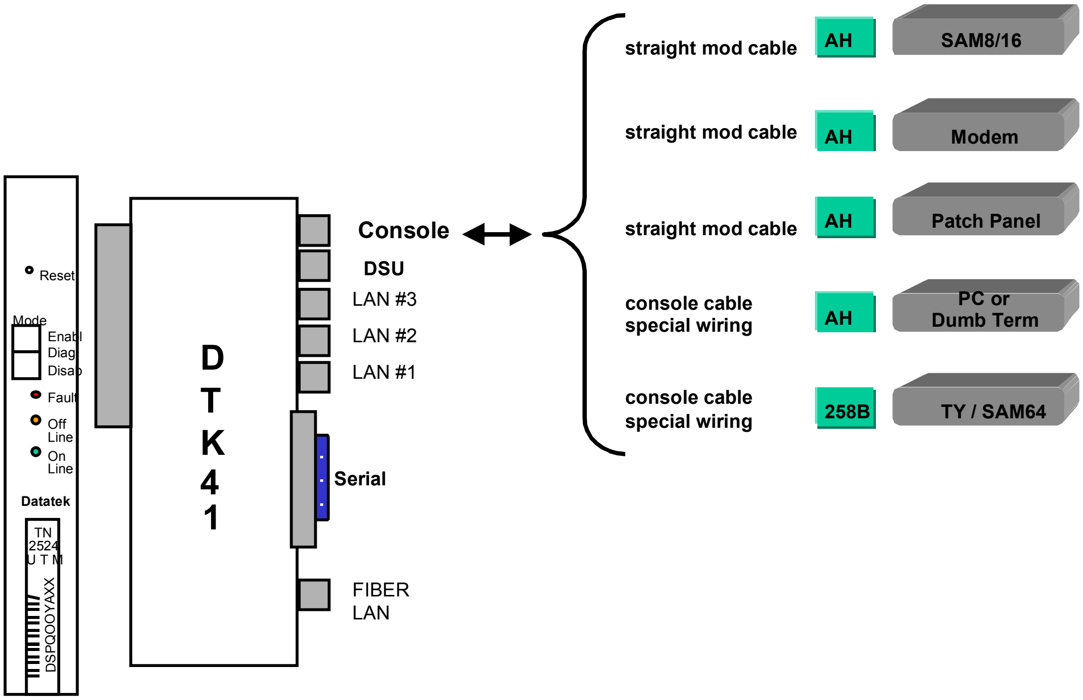


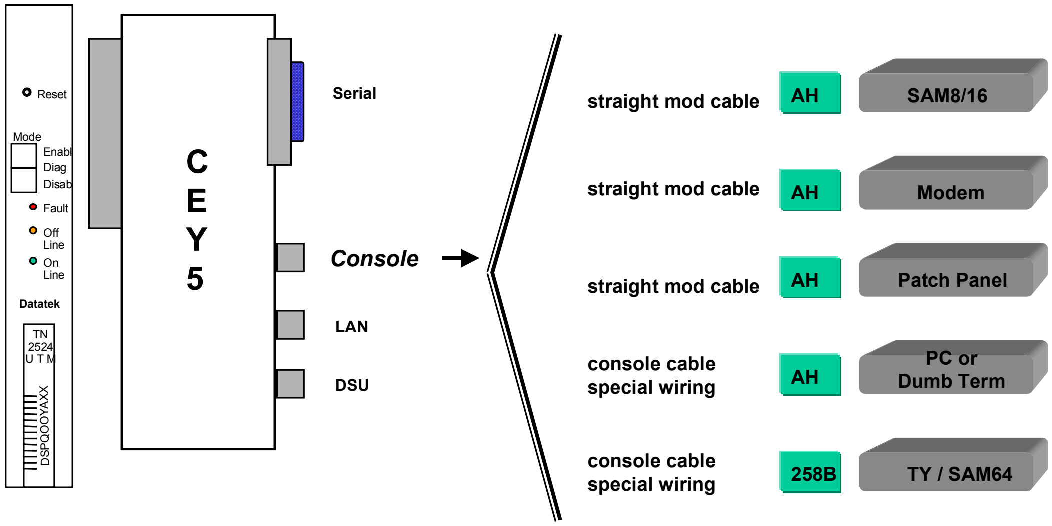


3.4 CABLING THE I/O CONSOLE PORT

Depending upon access availability, the following will be needed to setup a UTM console connection.

- A UTM circuit pack and an I/O Board. The console cabling is identical on both the DTK41, and the CEY5 I/O boards.
- Either a straight modular or console cable *(special wiring)* will be used to connect from the console port into either an AH adapter or into a 258B adapter
- The AH adapter will be used to terminate the cable and will be attached to the appropriate device. The attached device will determine the gender of the AH adapter.

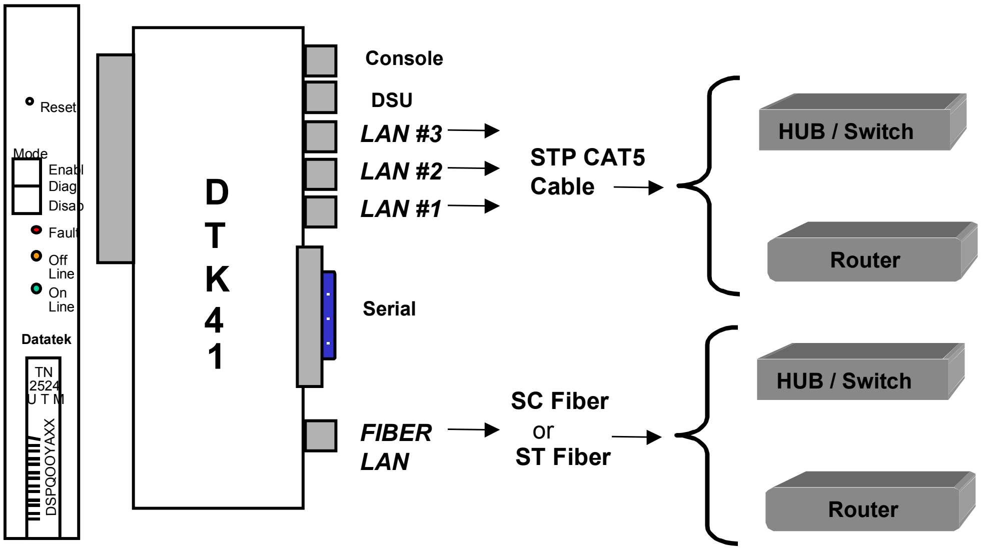


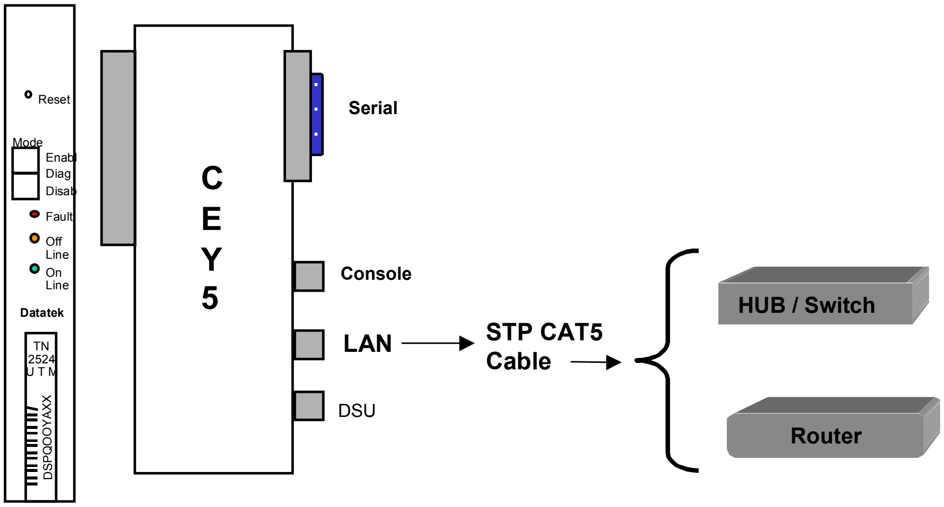

Reset
Mode
Enabl
Diag
Disab
Fault
Off Line
On Line
Datatek
TN 2524 U T M
DSPQOOYAXX
C E Y 5
Serial
Console
LAN
DSU
straight mod cable
AH
SAM8/16
straight mod cable
AH
Modem
straight mod cable
AH
Patch Panel
console cable special wiring
AH
PC or Dumb Term
console cable special wiring
258B
TY / SAM64

3.5 Cabling a LAN Port

When the **type** option of the **trunk** command *(see module command set)* is selected as **IPDSU** the LAN port will provide data transport and a UTM circuit pack with either the DTK41 or the CEY5 I/O Board.

A Shielded Twisted Pair CAT5 cable is attached to the LAN port of the I/O board and will allow for cabling either into a hub or router. The DTK41 I/O board may use a 10BaseT or 100BaseT hub or router. The CEY5 I/O board uses a 10BaseT hub or router.

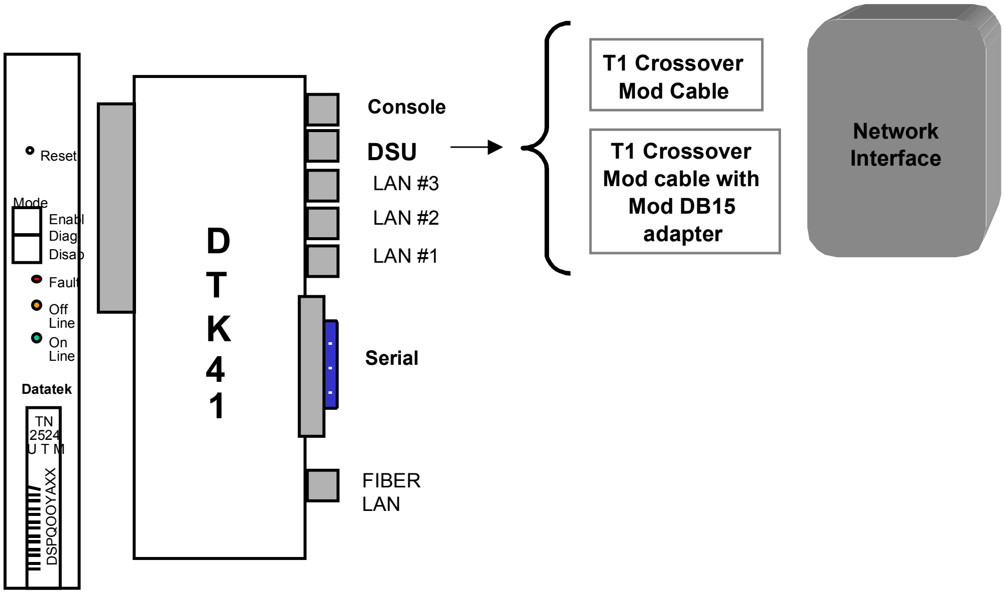


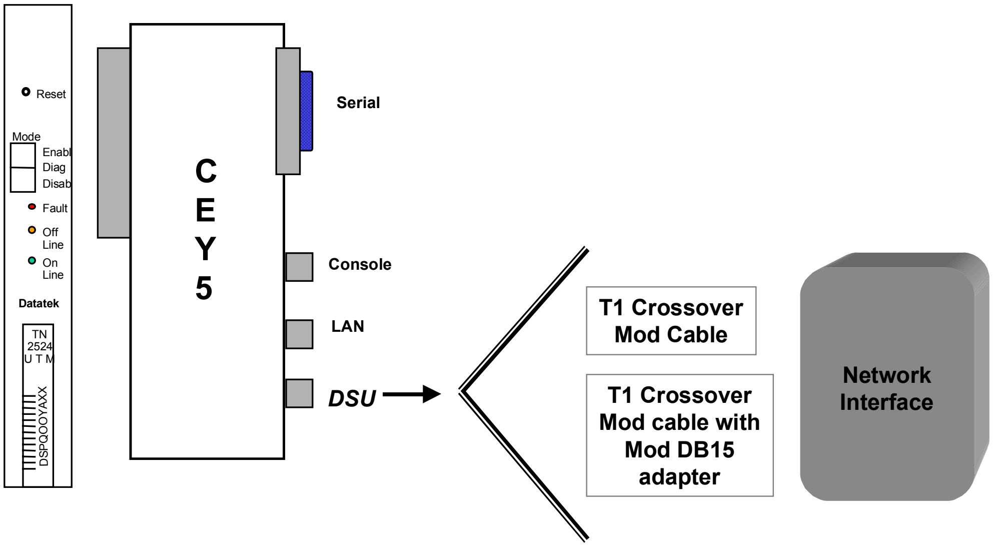

Reset
Mode
Enabl
Diag
Disab
Fault
Off Line
On Line
Datatek
TN 2524 U T M
DSPQOOYAXX
C E Y 5
Serial
Console
LAN
STP CAT5 Cable
DSU
HUB / Switch
Router

3.6 Cabling the I/O DSU Port

When the **phy** option *(see module command set)* of the **trunk** command is selected as **DSU**, the following will be needed:

- ❑ A UTM circuit pack and either a DTK41 IO Board, or a CEY5 I/O Board
- ❑ A T1 crossover modular cable or T1 crossover cable with adapter can be connected to the DSU port's modular 8-pin modular interface
  - ❑ **Option 1**: Use the T1 crossover mod cable with a modular 8-pin connector on one end and an 8-pin modular connector on the other.
  - ❑ **Option 2**: Use the T1 crossover mod cable with a modular 8-pin connector on one end and an 8-pin modular connector on the other and add a Mod/DB15 adapter.




Reset
Mode
Enabl
Diag
Disab
Fault
Off Line
On Line
Datatek
TN 2524 U T M
DSPQOOYAXX
C E Y 5
Serial
Console
LAN
DSU
T1 Crossover Mod Cable
T1 Crossover Mod cable with Mod DB15 adapter
Network Interface

3.7 FIELD UPGRADE AND SOFTWARE REGISTRATION

The **UTM,** when initially delivered, will need one or more software keys to activate the software. Software keys are also required when an optional individual feature packages are added to the device. Finally, when the **UTM** is upgraded with revised software, one or more software keys are required to register the installed software and any feature packages registered for the device.

When performing an upgrade, the revised software is initially downloaded by **upgrade** into a staging area and is not active. The software then is activated by a ***reboot***. The new software will execute normally prior to registration. However, no backup, reloads, or upgrades can be performed. Module level parameters, such as the device IP address, may be changed and activated. Interface specific parameters cannot be changed.

The procedure for performing a software registration has been mechanized. Manual procedures are error prone and not recommended. They are no longer covered in this user manual.

The mechanized Software Upgrade Registration procedure allows simplified administration of one or more devices. When a quantity of devices are upgraded, manual software registration of each device has the potential of becoming increasingly tedious. The mechanized software upgrade registration process was designed to alleviate the problems associated with multiple device upgrades. It is also preferred for single device upgrades as it eliminates any potential for error.

The new software is downloaded to the **UTM** via the **upgrade** command. This may be performed for one or more devices. The “-r” option to the dtupgrade command will restart the device on the new software after the download completes successfully. It is highly recommended. In the alternative, the device may be downloaded without a restart and restarted at a later time during a scheduled maintenance window. Restarting the device on the new software prior to registration is required. After the restart, the devices will continue to operate normally on the new software without registration. Some operations interface functions are inhibited pending software registration. Below is an example of a typical **upgrade** invocation. Note the use of the “-r” option as it is recommended.

```
upgrade –v –d –r –i –mUNIV 192.168.0.231 univ_pp.17.1
```

Mechanized registration is performed in three steps. Each of which does not require user intervention.

The steps are as follows:

1. The **getinfo** utility is invoked on a file containing a list of devices to be administered. This file is called the master device list file and is typically named “dt_device.master”. The master device list file may have any name and it is provided as an argument to

the **getinfo** utility. The master device list may also contain devices that do not require registration. The **getinfo** utility makes inquiry of each device in the master device list and creates a device information file named “dt_device.info” in the current directory.

2. The “dt_device.info” file is then sent via email to keys@trdcusa.com for registration processing.
3. A file name “dt_device.register” file is returned via email to be used as input in the next step. A file named “dt_device.msgs” is a text file that may be displayed or printed showing the results of the registration function.
4. The **setreg** utility is invoked and uses the “dt_device.register” file provided as an argument. If no argument is provided, the file is assumed to be in the current directory. The **setreg** utility contacts each device that requires registration and have been assigned keys. One or more keys are installed during the dialogue.
5. The “dt_device.info” file and the “dt_device.register” file are deleted as they are transient and have no further value. Neither can be reused for the purpose of registration. However, the dt_device.info file may be used for inventory reports..

The source for the registration procedure is the inventory master device list file that is created, and maintained, by the administrator using their favorite text editor.

The master device list file contains one IP address per line, with an optional TCP port, and an optional password override, to access the device. The IP address is the console *connection address*, and not necessarily the actual device IP address. Registration via the serial console is explicitly supported. Comments are allowed between addresses, and after addresses. A password override is only required if the default password of “initial” has been changed.

The master device file line format is as follows:

```
<IP ADDRESS> [<TCP PORT>] [-P<Password>] # Comment
```

An example “dt_device.master” file follows:

```
# This is a Sample master device list file “dt_device.master”.
# Note that there is one device ( Connect IP Address ) per line.
# TCP Port Override is allowed. Registration may use the serial console.
# Password Override is allowed.
# It is OK to have devices that do not need registration listed for inventory.
# Comments in this file are preceded with a pound symbol.
# Blank Lines are treated as comments.
# Basic Line Format is as follows:
```

```
10.0.1.80 # Device at Location 'A'
192.168.7.82 # Device at Location 'B'
192.168.7.155 50001 # Example of TCP port Override.
192.168.7.156 50001 –pcustom1 # Example of Password Override.
```

Once the "dt_device.master" file is prepared, it is used as an input to the **getinfo** utility.

```
getinfo dt_device.master
```

This **getinfo** utility will collect information on each device in the master file. The **getinfo** utility will also make a determination if a registration is actually required. Consequently, the **getinfo** utility is also useful in performing inventory functions outside of the device registration. The output of the **getinfo** utility is a file named "dt_device.info" that is always created in the current directory.

The file "dt_device.info" is attached to an email and sent to the address keys@trdcusa.com.The registration procedure is performed and a file named "dt_device.register" is attached to return email to the original sender. A messages file named "dt_device.msgs" is also attached and may be printed as a report of the key generation function.

After receiving the "dt_device.register" file, the **setreg** utility is invoked with the relative path of the "dt_device.register" file as it's sole argument. The **setreg** utility will only contact the devices that actually need registration, and for which one or more keys were successfully generated. All of the appropriate keys, including a device key and multiple per port feature package keys, are installed by the **setreg** utility. The device is not restarted and this operation may occur during normal transport operation.

A report utility **devrep** is available. The **devrep** utility uses the "dt_device.info" file to display the inventory information. The usage is as follows:

```
devrep [-v] dt_device.info
```

If the file is not specified, the dtdevrep utility attempts to use the "dt_device.info" file resident in the current directory.

4 CONFIGURATION

The Universal Trunk requires BNS Control Computer administration as well as module administration. Control Computer administration consists of the typical commands required for configuring trunk modules in the BNS Control Computer Node database. Module administration defines the type of trunk the UTM will mimic and insures proper connectivity to other BNS network components.

Control Computer administration is typically accomplished through StarKeeper® II NMS or a Node’s local console interface. Information for the type of trunk the UTM will mimic is added to the Node database and then manipulated and checked, using the enter, change, delete, and verify trunk commands.

Control Computer configuration of the UTM is always the same as that of the trunk module it is required to mimic. Since the UTM appears to the BNS Control Computer as whatever trunk it is defined, no BNS Controller changes are necessary.

Module administration is available through the LAN or Console interface on the UTM DTK41 or CEY5 I/O board. Information is added to the UTM firmware database and then manipulated and checked using the verify command that is part of the module's command set.

4.1 THE UTM AS A TRUNK REPLACMENT

When the UTM is used to replace one side of an existing BNS trunk pair, follow the steps below. *(Examples for all configuration options in back)*

1. Remove Trunk and I/O board to be replaced.

2. Physically insert the DTK41 or CEY5 I/O Board *(Installation Section).*

3. Physically insert and activate the UTM *(set faceplate rocker switch to Enabl).*

4. From the UTM console *(NOT the Controller Console)* configure the UTM *(Module Command Section)*.

Sample Command lines to specify the trunk the UTM will mimic:

Replacing a Trunk-PQ	`Trunk type=HDLC phy=V35 modtype=TRKT1`
Replacing a SWT	`Trunk type=HDLC phy=V35 modtype=SWT`
Replacing a SAMSL	`Trunk type=HDLC phy=232 modtype=SAMSL`
Replacing a TRK64	`Trunk type=HDLC phy=V35 modtype=TRK64`

5. Restore the UTM board to service from the module and node consoles.

4.2 How to Install a New Pair of Universal Trunks

When installing a pair of UTM circuit packs follow the configuration steps below. Note that the examples given are for BNS-2000 VCS nodes.

```
From CC type: enter trunk ↵

TRUNK MODULE TYPE [64, dds, hs, pq, sft, swt, t1]:
```

Enter the trunk type you want to mimic. Refer to the trunk command in the module command section. In this section, notes on the modtype parameter of the trunk command will help you make your decision.

```
MODULE ADDRESS: 78 ↵

SESSION MAINTENANCE TRUNK [yes, no: +(no)]: no ↵

COMMENT [up to 60 chars double quoted]:

"Sample Universal Trunk configuration" ↵

GROUP [up to 8 chars]: utm1 ↵

NUMBER OF USER CHANNELS [1-2042: +(26)]: 200 ↵
```

The number of user channels should match for both UTMs

```
LINE SPEED [56k, 64k, 128k, 192k, 256k, 320k, 384k, 448k, 512k, 576k,
640k, 704k, 768k, 832k, 896k, 960k, 1.024M, 1.088M, 1.152M, 1.216M,
1.280M, 1.344M, 1.408M, 1.472M, 1.536M, 1.544M, 1.984M, 2.048M:
+(1.536M’)]: 1.536M ↵

NUMBER OF SECONDS BETWEEN TRUNK ACTIVE TESTS [5-256: +(180)]:↵

MAXIMUM CONSECUTIVE TRUNK ACTIVE FAILURES [2-10: +(3)]: ↵

ENABLE TRUNK MEASUREMENTS FOR THIS TRUNK [yes, no: +(no)]: yes ↵

CALL SCREENING PROFILE ID [up to 8 chars, none: +(none)]: ↵
```

- ❑ Physically insert the UTM (DTK41 or CEY5) I/O Board *(Installation Section)*.
- ❑ Physically insert and activate the UTM *(set faceplate rocker switch to Enabl)*.
- ❑ Via the Module command set, configure the UTM *(Module Command Section)*.
- ❑ Restore the UTM board to service from the Module console.
- ❑ Restore the UTM board to service from the Node console.
- ❑ Note that modules can be pre-configured prior to installation *(as this example depicts)*. All configuration data is non-volatile.

5 COMMANDS

5.1 NODE COMMANDS

Refer to the BNS-2000 Trunk Guide to configure the UTM into the node configuration database.

5.2 MODULE COMMANDS

The Module commands are used to configure UTM connectivity to other components in the BNS network. Support is provided for direct serial URP trunks, as well as IP-DSU trunks. The use of Frame Relay and ATM infrastructures is supported between a pair of Universal Trunk Modules. In general, module commands are “set and forget”, that is, they are executed once when the module is installed and are not changed.

5.2.1 DSU

```
Syntax: DSU  [type=<E1|T1>]
             [prof=<T1 WaveForm>]
             [timing=<INT|NET>]
             [tsrate=<56|64>]
             [addslot=<ALL|slot_no>]
             [delslot=<ALL|slot_no>]
```

The **DSU** command configures the RJ48C interface with built in DSU functionality. It does not associate a protocol with the interface, nor does it make the interface active. The DSU must be configured before it is made active by assigning the *phy (defines the physical trunk type)* to the DSU in the *trunk* command.

The **type** parameter indicates what basic framing is to be used. A value of T1 is used for domestic 1.544 Mhz interfaces with 193 Bit Superframes. A value of E1 is used for European interfaces at 2.048 Mhz with 256 Bit Superframes.

The **prof** parameter indicates the Transmission Waveform to be used with T1 transport. There is only one E1 transport profile, which is automatically set.

The following table indicates the available waveforms used with T1 transport.

Option	Description
0DB	T1 Long Haul w/ 0 DB Attenuation.
7DB	T1 Long Haul w/ 7.5 DB Attenuation.
15DB	T1 Long Haul w/ 15 DB Attenuation.
22DB	T1 Long Haul w/ 22 DB Attenuation.
S0	T1 Short Haul @ 0-110 Feet.
S110	T1 Short Haul @ 110-220 Feet.
S220	T1 Short Haul @ 220-330 Feet.
S330	T1 Short Haul @ 330-440 Feet.
S440	T1 Short Haul @ 440-550 Feet.

S550	T1 Short Haul @ 550-660 Feet.
T0	TR62411 T1 Long Haul w/ 0 DB Attenuation.
TS0	TR62411 T1 Short Haul @ 0-110 Feet.
TS110	TR62411 T1 Short Haul @ 110-220 Feet.
TS220	TR62411 T1 Short Haul @ 220-330 Feet.
TS330	TR62411 T1 Short Haul @ 330-440 Feet.
TS440	TR62411 T1 Short Haul @ 440-550 Feet.
TS550	TR62411 T1 Short Haul @ 550-660 Feet.

The **timing** parameter indicates the timing signal to be used for transmission. A value of INT *(for internal)* indicates that the Universal Trunk should generate the transmit clock internally from its precision oscillator. A value of NET *(for network)* indicates that the Universal Trunk should recover the transmit clock from the receive data stream and use it for transmission.

It should be noted that there may only be one master clock in the DSU interface between components, and there must be one master clock in that interface.

The **tsrate** parameter indicates the type of timeslot to be used. This is used for DDS and Frame Relay protocols, which may be connected to a remote channel bank at 56K instead of 64K. Please note that the ATM protocol *must* have 64K timeslots.

The **addslot** parameter allows the user to map a timeslot in the usage map. This allows fractional T1/E1 from one timeslot to all of them *(24 in T1 and 30 in E1)*.

Note: With E1 framing, the first timeslot, and the 16th (17th counting from one) is not usable per the ITU standard (G.704, G.706, G.703).

The **addslot** parameter allows the addition of a single time slot, or all of them defined for the DSU type. The numeric range is one through 24 for a T1 DSU, and one through 32 for an E1 DSU where one, and seventeen are not configurable.

The **delslot** parameter allows the user to remove a timeslot from the usage map. All of the timeslots may be removed with the all option.

5.2.2 TRUNK

```
Syntax: trunk [type=<IPDSU|HDLC|FR|ATM >]
              [phy=<V35|232|DSU >]
              [dest=<ipaddr>]
              [encrypt=<ON|OFF>]
              [loop=<ON|OFF>]
              [dlci=<dlci_num>]
              [cir=< OPEN|16K|32K|64K|128K|256K|512K|768K]
              [vpi=<vpi_num>]
              [vci=<vci_num>]
              [modtype=<TRKT1|SWT|SAMSL|TRK64|CPM>]
              [duplex=<ON|OFF>]
```

The **trunk** command configures the protocol to be used between components, and associates the physical interface to the protocol.

The **type** parameter indicates the base protocol set to be used between interfaces.

> A value of **IPDSU** indicates that the trunk is to communicate to a remote entity using the IP-DSU base protocol.
>
> A value of **HDLC** indicates that the protocol set uses HDLC bit encoding.
>
> A value of **FR** indicates that the Frame Relay base protocol stacks is to be used.
>
> A value of **ATM** indicates that the ATM AAL5 protocol stacks is to be used.

The **phy** parameter defines the physical interface.

> A value of **V35** for the **phy** parameter selects the Serial **phy** using the V.35 physical layer. This configuration may be used at speeds up to E1.
>
> A value of **232** for the **phy** parameter selects the serial **phy** using the RS-232 physical layer. This configuration may be used at speeds up to 64K.
>
> A value of **DSU** for the **phy** parameter selects the DSU interface, which was configured using the DSU command.

*Note: The selection **type=IPDSU** automatically uses the LAN interface.*

The **dest** specifies the address of the remote destination. If the UTM connects to an IP-DSU compatible device on an IP infrastructure, the **dest** parameter is set to the IP address of the remote IP-DSU or Universal Trunk.

The **encrypt** option enables or disables the IP-DSU encryption algorithm. This requires the same setting on both ends of the connection.

The **loop** option is only valid with an IP-DSU type trunk. When set to *ON*, it will echo back all data received on a trunk back to its origin *(the default is set to OFF)*. This only applies to the IP-DSU trunk and not any other protocol traffic on the LAN.

The **dlci** parameter allows the selection of the DLCI to be used for frame relay transport. It is only valid when the selected **type** is **FR**. It should be noted that DLCI values 0-15, and those above 1008 are reserved for LMI and not available.

The **cir** parameter allows the selection of the administered committed data rate on the facility. It is only valid when the selected **type** is **FR**. The **cir** value administered is used as the maximum data rate at which the UTM will send data when the facility has indicated congestion with the **BECN** flag on a frame received by the UTM. Every frame received from the facility will update the congestion status that is used to make the determination as to whether or not the **cir** parameter is applicable. The valid values are **open** which is the default, and indicates that no restriction should be made; **16k** for 16kbps, **32k** for 32Kbps, **64K** for 64Kbps, **128K** for 128Kbps, **256K** for 256Kbps, **512K** for 512Kbps, **768K** for 768Kbps, and **1024K** for 1Mbps.

The **vpi** parameter and its associated **vpi** and **vci** options allow the selection of the VCC to be used for ATM AAL5 transport. They are only valid when the selected **type** is **ATM**. It should be noted that VCI values of 0-31 are reserved for specific functions under UNI 3.1 and UNI 4.0. Consequently, they are not available for use.

The **modtype** parameter allows for the selection of a module type as seen by the BNS-2000/ BNS-2000 VCS Control Computer. This is necessary since not all trunk types will fit all functions. For example, for connectivity to an MPC, it is necessary to configure the **modtype** as an **SWT**. In order to connect to a SAM8, or SAM16, it is necessary to set the **modtype** as a **SAMSL**. To use the universal trunk as a CPM connection, a **modtype** of **CPM** is used. In the CPM case, all the transport mechanisms are supported, but the IP-CommKit host software uses only the IP-DSU mechanism. Under normal circumstances, the **modtype** will be set as a **TRKT1**. By selecting the appropriate **modtype**, the Universal Trunk may be used in any existing installation without a control computer upgrade.

The transport protocol automatically follows the selection made by the **modtype** option. Selecting a value of **TRKT1** will select the PQ transport protocol. A value of **SWT** or **CPM** will select the SWT/TIM transport protocol. Finally, a value of **SAMSL** or **TRK64** will select the DDS transport protocol.

When the Universal Trunk is a replacement trunk for one end of a trunk pair the “trunk modtype” must match the type of trunk on the other end of the circuit. Except when the far end trunk is a Trunk-PQ. Here, “trunk modtype” must be set to **TRKT1**

When the Universal trunk is not a replacement trunk, there is flexibility in the choice of the “trunk modtype” to be used.

The **duplex** option selects the type of operation of the trunk. When **duplex** is **off**, the trunk operates in *simplex* mode. That is, there is a single logical connection between trunk pair ends. The connection can exist via an IP, FR, ATM, or TDM infrastructure as noted earlier. When the **duplex** is **on**, there are two connections between the trunk pair. The first is (and must be) an IP-DSU connection as noted in this section. The second is a non IP connection via either the serial port (V.35 or RS-232) or the internal DSU. Any network type, including Frame Relay and ATM, is allowed for the second connection. In the duplex mode, a failure of either facility is alarmed, and the data is automatically switched over to the alternate facility. When the serial port is used, the carrier signal (DCD) is used to indicate a carrier failure from the external modem. When the internal DSU is used, a *loss of signal* is used to determine the carrier failure. Since the master clock end provides its own signal, the *loss of signal* is only noted on the recovered clock end of the DSU connection. Alarms are placed on the console port to be monitored by StarKeeper II NMS.

5.2.3 LOGIN

Syntax #1: login passwd=<password> **(default password is: initial)**
Syntax #2: login

This command is a security command required for accessing the bulk of the command set. It is only available when the user is logged off. The command has two forms, and three modes of operation.

The first syntax example provides legacy compatibility for operations systems that use that form. The password must contain between one and seven alphanumeric characters. The typed password is case sensitive.

In the second example, the password is not provided on the command line. The login command will then prompt for a password. A password given at the prompt will not be echoed. There is a timeout of approximately 30 seconds on the password prompt.

If one or more **TACACS+** RADIUS Servers are defined, the *second* form is used to log into the device. When used, a connection is made to the first available server. Prompts for “Username” and “Password” are requested. These Usernames and Passwords are administered on the **TACACS+** RADIUS server; and not on the device.

5.2.4 LOGOUT

Syntax: logout

The **logout** command returns the Universal Trunk to its logged out mode thus preventing unauthorized access.

5.2.5 CHANGE PASSWORD

Syntax: chgpass old=<password> new=<password> confirm=<password>

The **chgpass** command allows the user to change a previously configured password. The old password is the one currently in effect. The new and confirm passwords should be identical. The password must contain between one and seven alphanumeric characters and is case insensitive where special characters are not allowed. All arguments are required to complete the command.

5.2.6 LOCAL

```
Syntax: local [ ipaddr=<IP address>  ]
              [ submask=<submask> ]
              [ tcpunreach=< ICMP | RESET > ]
```

The **local** or **lo** command sets the IP address of the Universal Trunk to facilitate IP communication.

The **ipaddr** is the IP address of this unit. The **submask** is the subnet mask of this unit with a default value of 8 bits (255.255.255.0). The IP address and subnet mask are used by the unit to determine whether an IP address is on the same LAN segment, or if a gateway hop is required. This is performed during address resolution.

The operation of the unit**,** when it is called to an invalid TCP port, is specified with the **tcpreach=<ICMP | RESET>]** parameter. When set to **ICMP**, the caller is sent an “ICMP Port Unreachable” message. When set to **RESET**, the TCP connection is sent a TCP reset to the initiator.

5.2.7 GATEWAY

Syntax: gateway ipaddr=<IP address>

The **gateway** or **ga** command identifies the IP address of the local gateway router, if any. If the remote device resides on a different LAN, the gateway is the first hop the data travels through to reach the remote device.

The **ipaddr** is the IP address of the gateway router to be used if an IP address is on a different LAN segment.

5.2.8 TACACS+ RADIUS SERVERS

```
Syntax: tac < PRI | SEC >  [ ipaddr=<IP Address> ]
                           [ port=<TCP Port> ]
                           [ key="Encryption Key" | NONE ]
                           [ ENABLE ]
                           [ DISABLE ]
```

The **tacplus** command is only visible when the unit is logged in. The tac command allows the configuration of up to two **TACACS+** RADIUS servers for the device. the servers are used as a primary server and a secondary server, although they may be individually disabled.

The **< PRI | SEC >** syntax specifies which server is to be configured. A server may not be configured while enabled

The **[ipaddr=<IP Address>]** specifies the IP address of the configured server.

The **[port=<TCP Port>]** specifies the TCP port to use when communicating with the server. The TACACS+ service defaults to TCP port 49, but any port may be specified.

The **[key="Encryption Key" | NONE]** specifies an encryption key to use. The Encryption key must be enclosed in double quotes, and the double quotes are not part of the key. If no encryption is desired, the value of **NONE** is used to designate unencrypted service.

The **ENABLE** command allows this server to be used for service, and prevents further configuration.

The **DISABLE** command prevents this server from being used for service, and subsequently allows configuration.

5.2.9 HELP

Syntax: help

The **help** or **?** command without arguments displays the entire Universal Trunk, command set and command syntax for the mode (logged out or logged in) the unit is currently in. Individual command syntax is available when the help command is followed by the command name.

5.2.10 VERSION

Syntax: ver

The **version** or **ver** command displays the current software and database revisions of the unit and is only visible when the user is logged in. The command has no arguments.

5.2.11 REBOOT

Syntax: reboot

The **reboot** command resets the unit, which allows physical attributes to be set, and the command has no arguments. It is only visible when the unit is logged in. After reboot, the OA&M interface returns to the logged-out mode.

The **reboot** command will always prompt for a password for validation purposes even if the administrator is logged at the appropriate level or higher.

5.2.12 REMOVE

Syntax: remove

The remove or rm command takes the unit out of service. This command must be performed before any module level configuration changes can occur. It is only visible when the unit is logged in. The command has no arguments.

The **remove** command will always prompt for a password for validation purposes even if the administrator is logged at the appropriate level or higher.

5.2.13 RESTORE

Syntax: restore

The **restore** or **rs** command returns the Universal Trunk to service, and it has no arguments. If any physical attribute was changed on the unit, including the MAC address, the unit will be automatically rebooted by this command.

5.2.14 PING

Syntax: ping <IP Address> [Interval Seconds]

The **ping** command is only visible when the unit is logged in. The command has a single required argument, the IP address that is to be pinged.

The **ping** command formats an ICMP echo request packet that is then sent to the IP Address specified. The device with that address will issue an ICMP echo reply to the request. This is required of all IP implementations by RFC 791. If a reply is received, an informational alarm is issued on the UMI console. If no reply is received, there is a timeout message that will appear for that ICMP echo request.

The ping command issues a single ICMP echo request packet and awaits a response. The response is printed, and another ICMP echo request is issued. The operation continues until the user presses *any* character. The **[Interval Seconds]** argument specifies the amount of time to wait in seconds between the individual ICMP echo requests.

It should be noted that some host Internet Protocol implementations issue duplicate responses to a single ICMP request. The ping command will suppress duplicate replies.

5.2.15 CLEAR

Syntax: clear

The **clear** or **clr** command is only visible when the unit is *logged in*. The command has no additional arguments. It sets all the measurement and error counters to zero.

5.2.16 MODULE DISPLAY MEASUREMENTS

Syntax: dm

The **dm** command displays the current measurements of the unit and is only visible when the user is logged in. The command has no arguments.

This measurement command is different from the module measurement command available through the Node console or StarKeeper. The following distinguishes between the two types of Universal Trunk measurements.

The measurement report for the node level DMEAS command reports measurement counters for From Bus Packets, To Bus Packets and Percent Utilization.

The measurement report for the module level (**dm**) command reports measurement counters for Packet, Frame, Error and Ethernet Counters plus specific per protocol counters.

The table below itemizes the measurements available using the **dm** command. The base measurements are always displayed, and the error and exception counters are only displayed if nonzero.

Interface	Type	Protocol	Description
10, 10/100, Fiber	Base	All	Number of 10BaseT Packets Received
10, 10/100, Fiber	Base	All	Number of 10BaseT Packets Transmitted.
10, 10/100, Fiber	Except	All	Number of ICMP Echo Requests Received.
V.35, RS232, DSU	Except	HDLC, FR	Number of Serial Trunk Frames Received.
RS232, V.35, DSU	Except	HDLC, FR	Number of Serial Trunk Frames Transmitted.
DSU	Except	ATM	Number of ATM AAL5 Trunk Frames Received.
DSU	Except	ATM	Number of ATM AAL5 Trunk Frames Transmitted.
10, 10/100, Fiber	Error	All	Number of Ethernet Discards (Resource).
10, 10/100, Fiber	Error	All	Number of Late Collisions (TX).
10, 10/100, Fiber	Error	All	Number of Under-run. (TX).
10, 10/100, Fiber	Error	All	Number of packets which exceeded the Retry Limit (TX).
10, 10/100, Fiber	Error	All	Number of Carrier Sense Lost (TX).
10, 10/100, Fiber	Error	All	Number of Frame Collisions (RX).
10, 10/100, Fiber	Error	All	Number of Receiver Overruns (RX).
10, 10/100, Fiber	Error	All	Number of Receive CRC Errors. (RX).
10, 10/100, Fiber	Error	All	Number of Short Frame Errors. (RX).

10, 10/100, Fiber	Error	All	Number of Non-Aligned Frame Error. (RX).
10, 10/100, Fiber	Error	All	Number of Frame Length Violations. (RX).
10, 10/100, Fiber	Error	All	Number of Unsupported Protocol Frames. (RX).
10, 10/100, Fiber	Error	All	Number of Invalid UDP frames. (RX).
10, 10/100, Fiber	Error	All	Number of Rx Frames w/IP Header Checksum Errors. (RX).
10, 10/100, Fiber	Error	All	Number of Rx Frames w/ICMP Checksum Errors. (RX).
10, 10/100, Fiber	Error	All	Number of ICMP Unreachable Destination Messages (RX).
10, 10/100, Fiber	Error	IP-DSU	Number of Rx Frames from Non-Peer Entity.
10, 10/100, Fiber	Error	All	Number of Unknown ICMP Messages. (RX).
10, 10/100, Fiber	Error	IP-DSU	Number of Packets lost from TTL Network Error. (RX).
10, 10/100, Fiber	Error	All	Number of Packets with wrong IP Destination Address (RX).
10, 10/100, Fiber	Error	All	Number of Rx Packets with Unknown ARP Operations. (RX).
10, 10/100, Fiber	Error	All	Number of Bad ARP Reply Packets Received.
10, 10/100, Fiber	Error	All	Number of RFC894 Packets with an Unknown protocol type field. (RX).
10, 10/100, Fiber	Error	All	Number of 802.3 Frames with an Unknown protocol type field. (RX).
RS232, V.35, DSU	Error	HDLC, FR	Number of Frames aborted by CTS lost (TX).
RS232, V.35, DSU	Error	HDLC, FR	Number of Frames Under-Run. (TX).
RS232, V.35, DSU	Error	HDLC, FR	Number of Rx Frames Over-Run.
RS232, V.35, DSU	Error	HDLC, FR	Number of Rx Frames with CRC Errors.
RS232, V.35, DSU	Error	HDLC, FR	Number of Non-Aligned Frame Errors (RX).
RS232, V.35, DSU	Error	HDLC, FR	Number of Frame Length Violations. (RX).
DSU	Error	ATM	Number of ATM AAL5 Frames discarded due to buffer congestion.
DK	Except	All	Number of Trunk Data Chunks ingress. (TDK).
DK	Except	All	Number of Trunk Data Chunks egress. (FDK).
DK	Except	All	Number of DK Packets ingress. (TDK).
DK	Except	All	Number of DK Packets egress. (FDK).
DK	Except	All	Number of DK Parity Errors (FDK).
DK	Except	All	Frames discarded due to TDK FIFO Overflow.
RS232, V.35, DSU	Except	FR	Number of Frame Relay Frames received with the discard eligible (DE) bit set.
RS232, V.35, DSU	Except	FR	Number of Frame Relay Frames received with the Forward Explicit Congestion Notification (FECN) bit set.
RS232, V.35, DSU	Except	FR	Number of Frame Relay Frames received with the Backward Explicit Congestion Notification (BECN) bit set.

5.2.17 Verify Module Configuration

Syntax: vfy mod

The **vfy mod** command is only visible when the unit is *logged in*. The command displays the module configuration in a formatted report on the console.

5.2.18 SNMP

```
Syntax: snmp [ ipaddr= < trap mgr addr > ]
             [ port= < trap mgr port > ]
             [ CUG=<<+|-> CUG Number> ]
             [ PUBLIC=< YES | NO > ]
             [ COMM="Double Quoted String" | NONE ]
             [ SYSCONTACT="Double Quoted String" | NONE ]
             [ SYSNAME="Double Quoted String" | NONE ]
             [ SYSLOC="Double Quoted String" | NONE ]
```

This command is used to configure the IP address of the SNMP trap manager. Since traps are unsolicited alarms, an agent can take the initiative to inform the manager of the occurrence of a predefined condition. Typical conditions include the cold-start or warm-start of equipment and a link-down or link-up condition.

A single and multiple SNMP managers can access the **UTM**. However, only one SNMP manager can be defined as the trap manager. As a result of this command, all traps will be directed to the chosen trap manager.

The **ipaddr** field defines the IP address of the SNMP manager to which the traps are to be sent.

The **port** field indicates the UDP port on that SNMP manager and defaults to the standard value of 162.

Any combination of closed user group membership may be assigned to the SNMP interface using the parameter of **cug=[+|-]<CUG Number>**. The closed user group membership is displayed on the "verify module" output. Packets which have failed the SNMP Closed User Group Test are discarded. An alarm is not presented, but the failure is counted. The number may be displayed with the "dmeas mod" command.

The **UTM** allows setting of an SNMP community in addition to the *public* community. The *public* community is recognized when the **[PUBLIC=YES]** option is selected. Recognition of the public community is the default operation. When **[PUBLIC=NO]** is selected, the *public* community is not recognized.

The **UTM** allows setting of an SNMP community in addition to the *public* community. When configured, the UTM will respond to SNMP manager requests in that community. The UTM will always respond to a request in the *public* community. The settable SNMP community is configured with the **[COMM="Double Quoted String" | NONE]** option. The community may be in any case. The double quote encapsulation is not part of the community string. The settable community may be cleared by setting it to the keyword **NONE**.

The MIB-II variables sysName, sysContact, and sysLocation may be initialized from the **UTM** non-volatile database using the **SNMP** command. These variables are volatile in that they may be over-written by an SNMP manager. However, any change made by the SNMP manager will not impact the **UTM** non-volatile database. Setting the value to **NONE** will clear the entries in the **UTM** non-volatile database. Each field may be of 31 characters or less. The double quote encapsulation is not part of the respective variable. Any of the variables may be cleared by setting it to the keyword **NONE**.

5.2.19 INSTALL (SOFTWARE REGISTRATION)

Syntax: install [key=<software key>]
[fpkey=<software key>]

The **UTM** has a unique device software key, and multiple per interface feature package keys. This section is included in the user manual for completeness. Under normal circumstances, only the mechanized utilities utilize this command. It may be executed manually under an emergency situation. Depending on the device, the keys may or may not be installed by the factory. The per port feature package keys my be added at any time, and do not affect the operation of the unit. The registration procedure does not require a restart to take effect on a device running the registered software.

When executed without arguments, the **install** command will display the significant information needed to manufacture the device software key. The device IP address may also be required. No additional information is needed to create the feature package keys.

The **key=<software key>** argument allows the entry of an eight-character alphanumeric software registration that is unique to this **UTM** device. If an invalid key is entered, a MINOR alarm is generated to that effect. The passwords are not altered. The **rstpass** command has been created to reset the passwords should that become necessary.

The **fpkey=<software key>** argument allows the entry of an eight-character alphanumeric software registration that is unique to an interface, and software feature package, on this **UTM** device for the current software build. The specific feature package referenced by the software key becomes immediately available on the port without subsequent download. The <software key> has effect on only one interface. Other interfaces on the device are not affected. If the same software feature package is needed on multiple interfaces, then multiple feature package keys are applied.

The **install** command is always available.

5.2.20 RSTPASS

Syntax: rstpass [key=<Software Key>]

The **rstpass** command is always available regardless of whether the console is logged in or not. When invoked without any arguments, it will display unique identification about this particular device. The user may then contact the manufacturer with that information to obtain the <Software Key>. The <Software Key> is an eight character alphanumeric which is unique to this module. When the **rstpass** command is entered with the **key**=<Software Key> option, the user password is reset to the original value of “initial”. If an invalid key is entered, a MINOR alarm is generated to that effect.

5.2.21 TIMEOUT

Syntax: timeout [OFF | <Number of Minutes>]

For those users that wish the console to automatically log off after a period of inactivity, there is the console timer. The console timer defaults to the disabled condition and may be activated by the timeout command.

The command is only visible when the console is logged in. The <Number of Minutes> must be between 1 and 255 inclusive. When the module determines a period of inactivity of the specified time, it shall automatically log off the console. An INFO level alarm is issued at that time.

5.2.22 LABEL

Syntax: label [“Double Quoted String” | none]

The **label** command is used to give the command console a unique prompt. The command is visible only when logged into the **UTM** administrative console. If the **label** command is invoked without arguments, the current configuration of the label is displayed. If the argument to the **label** command is the word ‘none’, any current label is set to a null value. If the argument to the **label** command is a double quoted string, the contents of the string becomes the application console prompt label. A console label may be up to 31 characters in length.

5.2.23 HPIO

```
Syntax: HPIO RESET
             ENABLE < ALL | FIBER | <10/100 PHY RANGE> >
             DISABLE < ALL | FIBER | <10/100 PHY RANGE> >
             AUTO < ALL | <10/100 PHY RANGE>
             10HDX < ALL | <10/100 PHY RANGE>
             10FDX < ALL | <10/100 PHY RANGE>
             100HDX < ALL | <10/100 PHY RANGE>
             100FDX < ALL | <10/100 PHY RANGE>
```

The **HPIO** command is used to enable or disable the physical LAN connections on the DTK41 high performance I/O module. The DTK41 operates defaults to all ports being active. Therefore, no configuration is required unless security of the unused ports becomes an issue.

The **RESET** command option is used to perform a restart on the DTK41 module. Under normal circumstances, it should never be required to use this command. No arguments are required. The **'Link Active'** alarms for all connected links will be issued after a reset.

The **ENABLE** command enables the physical interfaces that have been previously disabled. The DTK41 defaults to all interfaces being enabled. The **ENABLE** accepts a target to specify those ports to be affected. A target value of **ALL** specifies that all three 10/100 BaseT ports, and the Fiber port is to be affected. A target value of **FIBER** specifies that only the fiber port is to be affected. A numeric value or range specifies the 10/100 BaseT ports. The numeric value may be a single number (e.g. '2') or a range (e.g. 1-2).

The **DISABLE** command disables physical interfaces. When disabled, the interface is not capable of communications. The **DISABLE** accepts a target to specify those ports to be affected. These are in the same form as the ENABLE command.

The DTK41 10/100 PHY ports default to automatic negotiation. This can also be set with the **AUTO** command option. The 10/100 ports can be set to a *static* configuration. When set to a *static* configuration, the automatic negotiation advertisement of the DTK41 10/100 PHY is limited to the selected option. The four *static* configurations are: **10HDX** for 10Mbps half duplex, **10FDX** for 10Mbps full duplex, **100HDX** for 100Mbps half duplex, and **100FDX** for 100Mbps full duplex.

It is **strongly recommended** that the default configuration of automatic negotiation (**AUTO**) is used. Any forced mismatch between the DTK41 10/100 port and the attached hub, switch or router will almost certainly result in unpredictable data error or loss.

5.2.24 ADMINISTER SECURITY BANNER

Syntax: banner [clear] [L#="Line # Message"]

The banner command is only visible when the unit is logged. It is used to administer the security banner. The default is a NULL banner. If a security banner is configured, it is displayed at each user login. The **clear** option is a shortcut to erase the entire message.

5.2.25 DATA-BASE RESET

Syntax: dbreset passwd=<password>

This command returns the ***DT-4000*** to the default configuration set up by the factory. The password will return to the factory default of ***initial***.

5.2.26 CLOSED USER GROUP (CUG) ADMINISTRATION

**Syntax: cug < cug num > [ipaddr=< ip address >]
[submask=< ip submask >]**

The **cug** command is only visible when the unit is logged in. The **<CUG_num>** parameter is the closed user group identifier used to assign the CUG to a user port (with the **port** command), or the console (with the **console** command). The **<CUG_num>** may be a value between 1 and 16, inclusive.

A single IP address and subnet mask pair specifies each CUG. The **ipaddr** parameter is an address of an endpoint (or base address of a group of endpoints) to be allowed into the group. The **ipaddr** value *ANDed* with the **submask** value must agree with the caller's or destination's IP address *ANDed* with the same **submask** for a call to be allowed to or from a user port to which the CUG is assigned. Depending on the **submask** value, this allows an individual (submask=255.255.255.255), intermediate, or network-wide level of authorization.

Setting the **ipaddr** value to 0.0.0.0 deletes any prior configuration for the **<CUG_num>**. A **<CUG_num>** may not be deleted if it is currently assigned to any user port.

A list of all configured CUGs is reported via the **vfy cug** command. The list of closed user groups associated with a given user port is presented in response to the **vfy port** command.

5.2.27 VERIFY CUG

Syntax: vfy cug

This command is only visible when the unit is logged in. It displays the configuration of all Closed User Groups.

5.2.28 ASSIGNING A CUG TO THE CONSOLE

Syntax: console cug=<+|->< cug num >

The **console** command is only visible when the unit is logged in. The **<CUG_num>** parameter is the closed user group identifier as defined with the **cug** command. A prefix of **+** will add the **<CUG_num>** to the list associated with the telnet console. A prefix of **–** will delete the **<CUG_num>** from the list associated with the telnet console.

If the telnet console is connected at the time a closed user group is defined, the connection must be allowed in the closed user group. If the connection is not allowed, an error message is displayed and the association will not take place.

If it is desirable to disable the telnet console entirely, a closed user group consisting only of the **UTM** address may be assigned to the console. The net effect is to disallow any and all connections via the telnet console.

6 UTM SNMP AGENT

The Universal Trunk SNMP V1 agent supports a multitude of SNMP MIB variables, SNMP trap operations, set operations and gets.

The SNMP agent may be queried by one or more SNMP managers.

6.1 SNMP VERSION 1 COMMANDS

Command	Operational Result
Get	Requests the values of one or more Management Information Base (MIB) variables.
GetNext	Enables MIB variables to be read sequentially, one variable at a time.
Set	Permits one or more MIB values to be updated.
GetResponse	Used to respond to a Get, GetNext, or Set.
Trap	Indicates the occurrence of a predefined condition.

Universal Trunk SNMP MIB Variable Database

RO = Read Only Variable

R/W = Read Variable / Write Variable

SIV = Storage is Volatile

MIB Variable Number	Name	MIB	Console Equivalent	Access	Notes
1.3.6.1.2.1.1.1.0	SysDescr	MIB-II	Banner Message	RO	
1.3.6.1.2.1.1.2.0	SysObjectID	MIB-II	None	RO	
1.3.6.1.2.1.1.3.0	SysUpTime	MIB-II	None	RO	
1.3.6.1.2.1.1.4.0	SysContact	MIB-II	None	R/W	SIV
1.3.6.1.2.1.1.5.0	SysName	MIB-II	None	R/W	SIV
1.3.6.1.2.1.1.6.0	SysLocation	MIB-II	None	R/W	SIV
1.3.6.1.2.1.1.7.0	SysServices	MIB-II	None	RO	
1.3.6.1.2.1.4.1.0	IpForwarding	MIB-II	None	RO	
1.3.6.1.2.1.4.2.0	IpDefaultTTL	MIB-II	None	RO	
1.3.6.1.2.1.4.3.0	IpInReceives	MIB-II	Number of Ethernet Pkts Rcvd	RO	
1.3.6.1.2.1.4.4.0	IpInHdrErrors	MIB-II	Nbr of Packets w/Header Errs	RO	
1.3.6.1.2.1.4.5.0	IpInAddrErrors	MIB-II	Nbr Rx Packets w/Wrong Addr	RO	
1.3.6.1.2.1.4.6.0	IpForwDatagrams	MIB-II	None	RO	
1.3.6.1.2.1.4.7.0	IpInUnknownProtos	MIB-II	Nbr of Packets w/Unk Protocol	RO	
1.3.6.1.2.1.4.8.0	IpInDiscards	MIB-II	Nbr of Packets Disc due to Resource	RO	

1.3.6.1.2.1.4.9.0	IpInDelivers	MIB-II	Inferred from DMEAS counters	RO	
1.3.6.1.2.1.4.10.0	IpOutRequests	MIB-II	Number of Device Frames Transmitted	RO	
1.3.6.1.2.1.4.11.0	IpOutDiscards	MIB-II	Nbr of Port frames Disc due to Resource	RO	
1.3.6.1.2.1.4.12.0	IpOutNoRoutes	MIB-II	None	RO	
1.3.6.1.2.1.4.13.0	IpReasmTimeout	MIB-II	None	RO	
1.3.6.1.2.1.4.14.0	IpReasmReqds	MIB-II	None	RO	
1.3.6.1.2.1.4.15.0	IpReasmOKs	MIB-II	None	RO	
1.3.6.1.2.1.4.16.0	IpReasmFails	MIB-II	None	RO	
1.3.6.1.2.1.4.17.0	IpFragOKs	MIB-II	None	RO	
1.3.6.1.2.1.4.18.0	IpFragFails	MIB-II	None	RO	
1.3.6.1.2.1.4.19.0	IpFragCreates	MIB-II	None	RO	
1.3.6.1.2.1.4.21.0	IpRoutingDiscards	MIB-II	None	RO	
1.3.6.1.2.1.5.1.0	IcmpInMsgs	MIB-II	None	RO	
1.3.6.1.2.1.5.2.0	IcmpInErrors	MIB-II	ICMP Errors	RO	
1.3.6.1.2.1.5.3.0	IcmpInDestUnreach	MIB-II	None	RO	
1.3.6.1.2.1.5.8.0	IcmpInEchos	MIB-II	Nbr of Pings	RO	
1.3.6.1.2.1.5.9.0	IcmpInEchoReps	MIB-II	None	RO	
1.3.6.1.2.1.6.1.0	TcpRtoAlgorithm	MIB-II	None	RO	
1.3.6.1.2.1.6.2.0	TcpRtoMin	MIB-II	None	RO	
1.3.6.1.2.1.6.3.0	TcpRtoMax	MIB-II	None	RO	
1.3.6.1.2.1.6.4.0	TcpMaxConn	MIB-II	None	RO	
1.3.6.1.2.1.6.5.0	TcpActiveOpens	MIB-II	None	RO	
1.3.6.1.2.1.6.6.0	TcpPassiveOpens	MIB-II	None	RO	
1.3.6.1.2.1.6.7.0	TcpAttemptFails	MIB-II	None	RO	
1.3.6.1.2.1.6.8.0	TcpEstabResets	MIB-II	None	RO	
1.3.6.1.2.1.6.9.0	TcpCurrEstab	MIB-II	None	RO	
1.3.6.1.2.1.6.10.0	TcpInSegs	MIB-II	None	RO	
1.3.6.1.2.1.6.11.0	TcpOutSegs	MIB-II	None	RO	
1.3.6.1.2.1.6.12.0	TcpRetransSegs	MIB-II	None	RO	
1.3.6.1.2.1.6.13.X	TcpConnTable Entries	MIB-II	None	RO	
1.3.6.1.2.1.6.14.0	TcpInErrs	MIB-II	None	RO	
1.3.6.1.2.1.6.15.0	TcpOutRsts	MIB-II	None	RO	
1.3.6.1.2.1.7.1.0	UdpInDatagrams	MIB-II	Derived from other Counts.	RO	
1.3.6.1.2.1.7.2.0	UdpNoPorts	MIB-II	Non-Peer and Spurious UDP errors	RO	
1.3.6.1.2.1.7.3.0	UdpInErrors	MIB-II	Frame Errors	RO	

1.3.6.1.2.1.7.4.0	UdpOutDatagrams	MIB-II	Frames Sent, Keep Alive Messages sent, etc.	RO	
1.3.6.1.2.1.7.5.X	udpEntry Table	MIB-II	None	RO	
1.3.6.1.2.1.11.1.0	SnmpInPkts	MIB-II	None	RO	
1.3.6.1.2.1.11.3.0	SnmpInBadVersions	MIB-II	None	RO	
1.3.6.1.2.1.11.4.0	SnmpInBadCommunityNames	MIB-II	None	RO	
1.3.6.1.2.1.11.5.0	SnmpInBadCommunityUses	MIB-II	None	RO	
1.3.6.1.2.1.11.6.0	SnmpInASNParseErrs	MIB-II	None	RO	
1.3.6.1.2.1.11.30.0	SnmpEnableAuthenTraps	MIB-II	None	R/W	SIV
1.3.6.1.2.1.11.31.0	SnmpSilentDrops	MIB-II	None	RO	
1.3.6.1.2.1.11.32.0	SnmpProxyDrops	MIB-II	None	RO	

6.2 Supported Traps

Alarm Text	Severity	Trap Type	Notes
None	N/A	ColdStart	Generated when the unit starts up
Lost Connectivity to Peer IP-DSU	Minor	LinkDown	Generated when Peer Connectivity is lost; DCD & CTS is dropped
Peer Connectivity Established	Info	LinkUp	Generated when Peer Connectivity is established; DCD & CTS is asserted
None	N/A	AuthFail	SNMP Authorization Failure

7 ALARMS

Below is an enumeration of the module level alarms presented on the Universal Trunk Console along with their severity.

Alarm	Severity
Remote CC Requested Backplane Reset	INFO
Remote CC Requested Reboot in Progress	INFO
DKGA EEPROM Failure.	MAJOR
Tx Error on 10BaseT. Check Physical Connection.	MAJOR
Insufficient Buffers for FRAME RELAY LMI Status Report.	MAJOR
Lost Connectivity to Peer IP-DSU.	MINOR
Peer Connectivity Established.	INFO
User Requested Reboot in Progress	INFO
Invalid Login Attempt.	MINOR
Invalid Password Change Attempt.	MINOR
Gateway Connectivity Established.	INFO
SNMP Trap Manager not reachable (ICMP).	INFO
ICMP Destination Unreachable Msg Received.	MINOR
Tx Error on Serial Trunk	MAJOR
Over-Temperature Condition Detected.	MAJOR
Over-Temperature Condition Cleared.	INFO
High Temperature Condition Detected.	MINOR
High Temperature Condition Cleared.	INFO
DB contains an Invalid Datakit Trunk Configuration.	MAJOR
DTK41 10/100 BaseT PHY #N 'Link Active'.	MINOR
DTK41 10/100 BaseT PHY #N 'Link InActive'.	MINOR
DTK41 Fiber 'Link Active'.	MINOR
DTK41 Fiber 'Link InActive'.	MINOR

7.1 MAJOR ALARMS

A major alarm indicates a serious, service-degrading condition.

7.2 MINOR ALARMS

A minor alarm indicates a secondary or transient error that is not likely to affect overall service unless multiple minor alarms are issued. In this case, a serious condition exists that may affect overall system performance

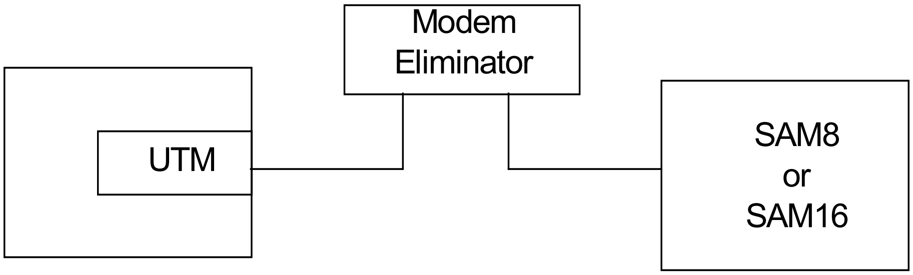
Info alarms

An information alarm is a message that does not necessarily require attention. It typically is important for network administration, but does not adversely affect service.

8 Sample Configurations

8.1.1 Configuration #1

This sample configuration is a direct replacement of a SAMSL with a Universal Trunk.



The commands used to configure the Universal Trunk Module are as follows:

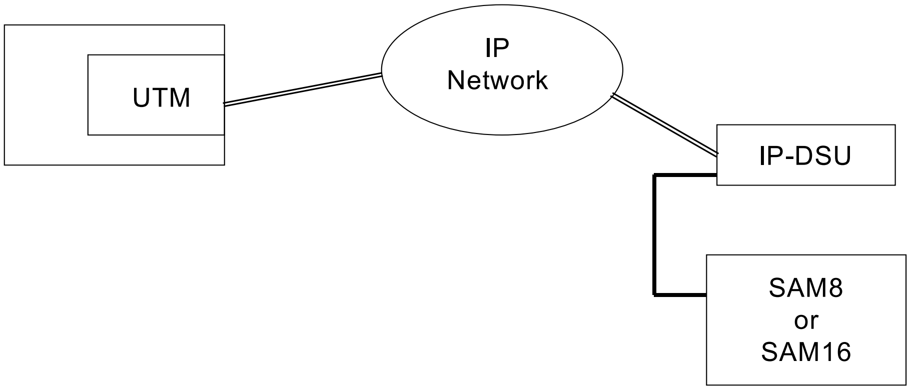
```
trunk type=hdlc phy=v35 modtype=samsl
```

All other commands are optional.

A SAM8 will not function properly above a 56Kbps clock rate. A SAM16 will function up to 128Kbps clock rate. A DT-4000 as a SAM16 replacement in this configuration will function up to a clock rate of E1.

Configuration #2

This configuration replaces the direct facility between components with an IP infrastructure.



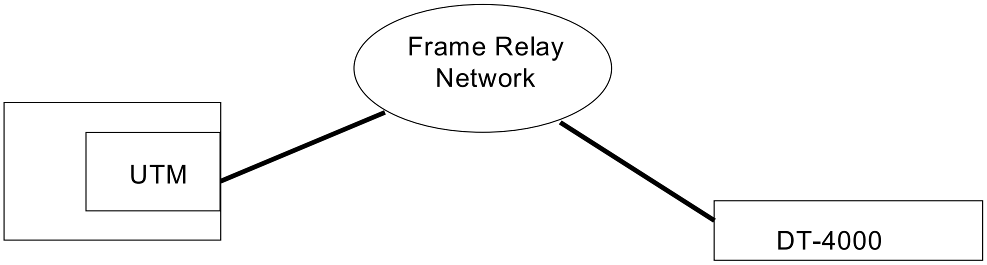
The commands used to configure the Universal Trunk Module are as follows:

```
trunk type=ipdsu modtype=samsl dest=<ipaddr>
local ipaddr=<ipaddr> submask=<mask>
gateway ipaddr=<ipaddr>
restore
```

Please note that it is assumed that the MAC address has been pre-configured in the unit.
A DT-4000 may be used to replace both the SAM16 and the IP-DSU in the depiction above.

Configuration #3

In this example, the Serial interface is used to communicate with a Frame Relay network to a DT-4000.



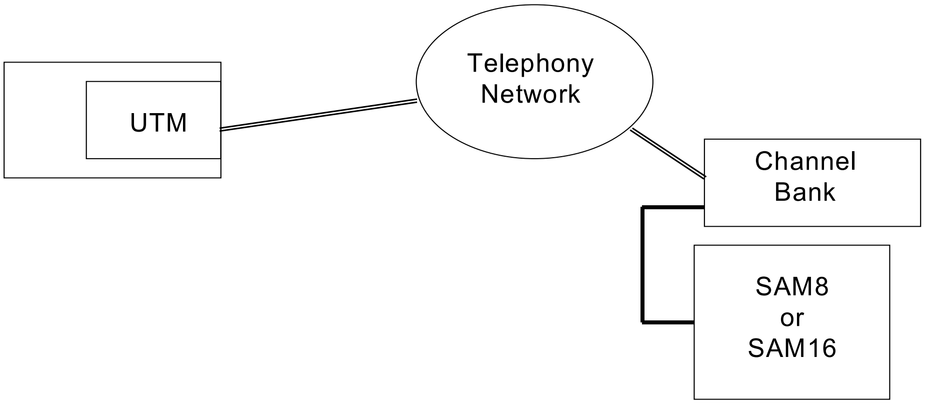
The commands used to configure the Universal Trunk Module are as follows:

```
trunk type=fr phy=v35 modtype=samsl dlci=16
```

Please note that the Frame Relay network would need to be configured to transport the circuit on DLCI 16 on the UTM side. The DLCI may be different on the DT-4000 side.

Configuration #4

In this configuration, we explore using the Universal Trunk for interfacing to an existing entity minus the local DSU.



The commands used to configure the Universal Trunk Module are as follows:

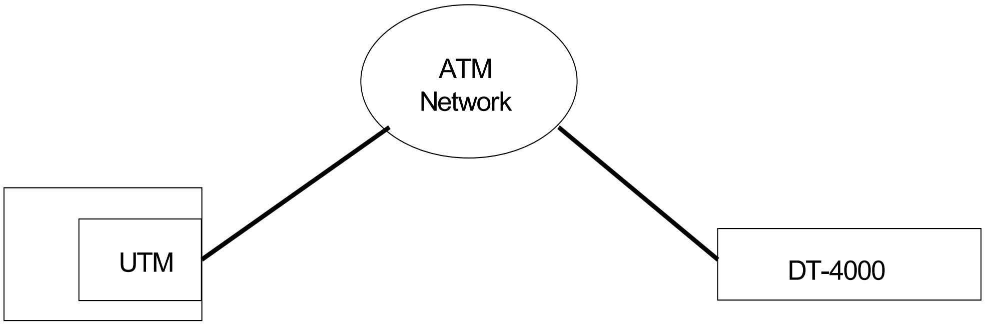
```
dsu type=t1 prof=s0 timing=net tsrate=56 delslot=all addslot=1
trunk type=hdlc phy=dsu modtype=samsl
restore
```

The above will transport one 56Kbps timeslot to the channel bank via a T1 carrier. This is “fractional T1” because only a fraction is being used. The Channel Bank then presents a serial data stream to the SAM8/16.

If a DT-4000 were used in the picture above, the channel bank would not be required.

Configuration #5

This is a sample ATM configuration. The entire T1 is used for ATM since the transport protocol for ATM convergence requires it as such.



The commands used to configure the Universal Trunk Module are as follows:

```
dsu type=t1 prof=s0 timing=net tsrate=64 addslot=all
trunk type=atm phy=dsu modtype=samsl vpi=0 vci=32
restore
```

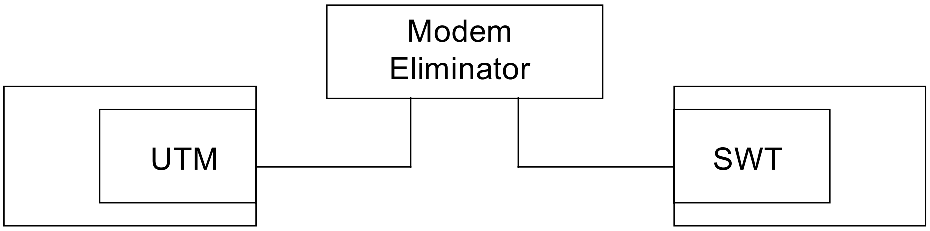
The ATM network endpoint connected to the UTM must be configured to provide a circuit at the administered VCC (VPI/VCI combination). This may be a different number than that presented to the DT-4000 since it has only local significance.

9 UTM INTERWORKING

9.1 INTERWORKING WITH THE SWT

The Universal Trunk can be made to inter-work with an existing SWT. This allows the UTM to be a direct spare for existing installations. It should be noted that when inter-working with an SWT, the UTM-> SWT direction will enjoy the benefits of the UTM's per VCC priority queueing while the SWT->UTM direction will keep the SWT's two queue model for all VCCs.

Consider the following diagram:



The configuration is as follows:

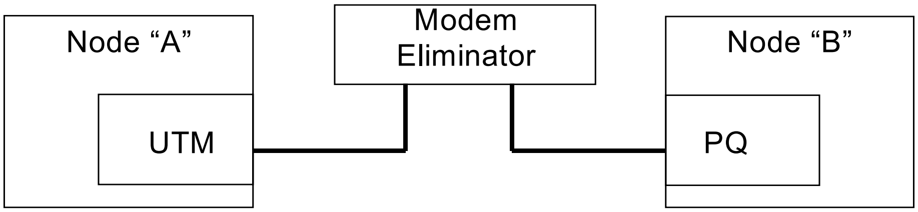
```
trunk type=hdlc phy=v35 modtype=swt
```

The SWT should be configured in NRZ (I/O board switch) operation.

9.2 INTERWORKING WITH THE TRK-PQ

The Universal Trunk can be made to inter-work with an existing PQ trunk module. This allows the UTM to be a direct spare for existing installations.

Consider the following diagram:



The configuration is as follows:

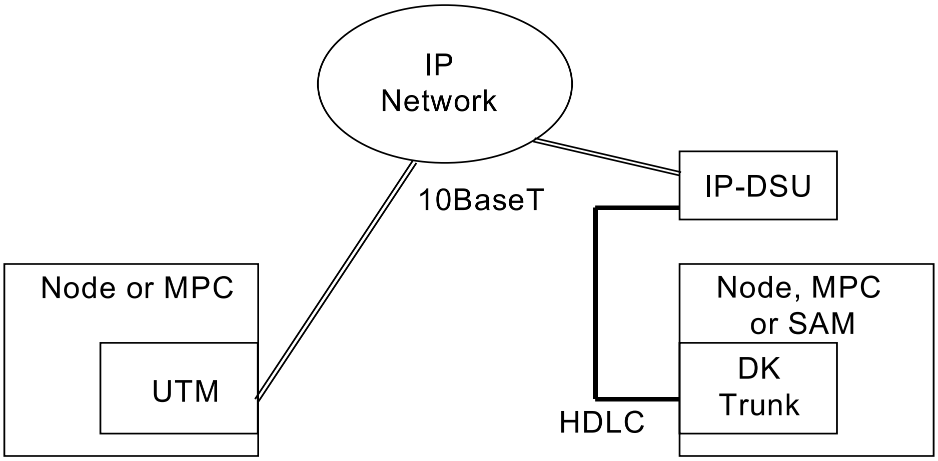
```
trunk type=hdlc phy=v35 modtype=trkt1
```

The TRK-PQ in Node "B" will have the same number of user channels as the TRK-T1 configured in the CC of "Node A" for the UTM. However, the user channel offsets will differ. The range for the TRK-T1 begins at channel 6, and the range for the TRK-PQ begins at channel 10. This adjustment is made automatically by the UTM and no further configuration is required.

9.3 INTERWORKING WITH AN IP-DSU AND SWT/TRK-PQ/TRK-64/SAM

The Universal Trunk will also inter-work with an existing Datakit trunk module via an IP-DSU. This allows the UTM to be used with a remote partner that is connected via an IP-DSU to an IP infrastructure.

Consider the following diagram:



Configuration of the UTM is as follows:

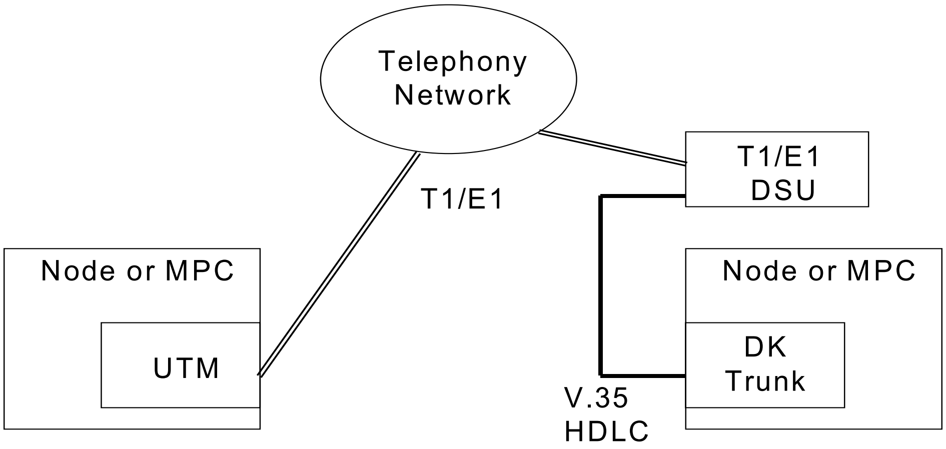
```
trunk type=ipdsu modtype=<SWT | TRKT1 | TRK64>  dest=<ipaddr>
local ipaddr=<ipaddr> submask=<mask>
gateway ipaddr=<ipaddr>
restore
```

Please note that it is assumed that the MAC address has been pre-configured in the unit.

9.4 INTERWORKING WITH A DSU AND SWT/TRK-PQ

The Universal Trunk will also inter-work with an existing Datakit trunk module via a T1 or E1 IP-DSU. This allows the UTM to be connected directly to a T1/E1 facility and use a remote trunk that would require an external DSU.

Consider the following diagram:



Configuration of the UTM is as follows:

```
dsu type=t1 prof=s0 timing=net tsrate=64 addslot=all
trunk type=hdlc phy=dsu modtype=<SWT | TRKT1 | TRK64>
restore
```

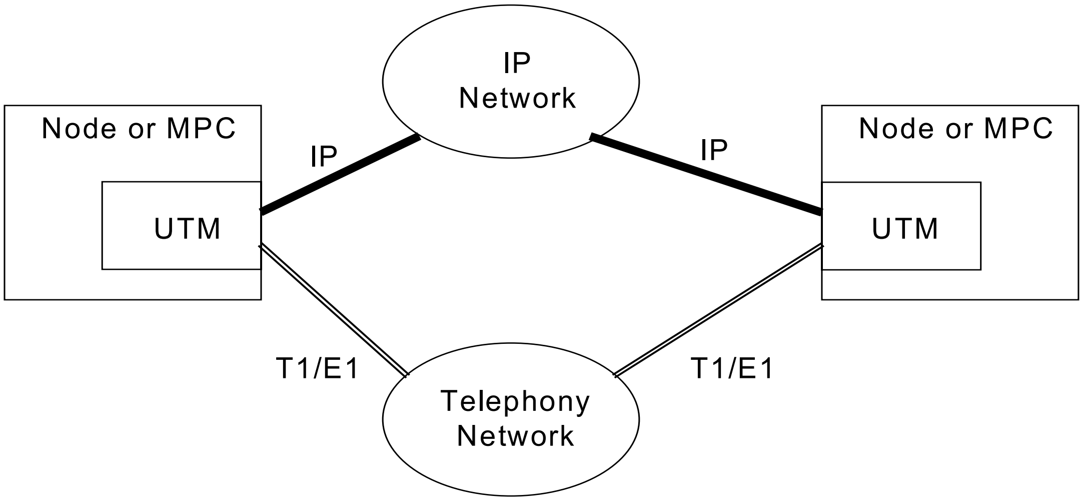
Please note that the above sample configuration is for a T1 line, assigns all 24 timeslots, and has a relatively short line equalization value. These would all be adjusted accordingly in an actual installation. The modtype selects the protocol used and needs to be consistent with the remote module.

10 DUPLEX TRUNKS

The Universal Trunk will provide fault tolerant trunking with the **duplex** feature. When a trunk is duplex, it has two different networks in which the data may traverse. The first is an IP network using the IP-DSU protocol. The second may be a direct facility, a Frame Relay network, or an ATM network. The internal DSU or the serial port may be used as the interface to the second network.

Consider the following diagram:

Fault Tolerant Duplex Trunk Example



Configuration of the UTM is as follows:

```
local ipaddr=<local_ip_address> submask=<subnet_mask>
gateway ipaddr=<gateway_ip_address>
dsu type=t1 prof=s0 timing=net tsrate=64 addslot=all
trunk type=hdlc phy=dsu modtype=<SWT | TRKT1 | TRK64>
trunk duplex=on dest=<other UTM IP address>
restore
```

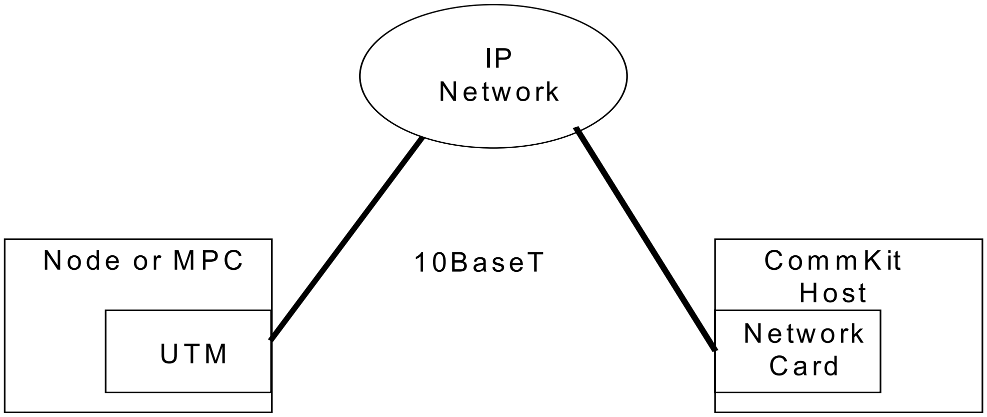
Please note that the above sample configuration is for a T1 line, assigns all 24 timeslots, and has a relatively short line equalization value. These would all be adjusted accordingly in an actual installation. The **modtype** selects the protocol used and needs to be consistent with the remote module. The **duplex** option enables fault tolerant trunking and the **dest** specifies the remote UTM IP address.

11 Using the UTM as a CPM

The IP-CommKit software allows a UTM to be used as a CPM. This method of attaching CommKit hosts does not require the host to be co-located. The UTM supports all of its transport mechanisms for the connection, however the IP-CommKit has only implemented the IP-DSU protocol.

Consider the following diagram:

The UTM as an IP-CommKit Interface



Configuration of the UTM is as follows:

```
local ipaddr=<local_ip_address> submask=<subnet_mask>
gateway ipaddr=<gateway_ip_address>
trunk type=ipdsu  modtype=CPM  dest=<COMMKIT Host IP Address>
restore
```

In the example above, the IP network may be simply a cross-over cable, or span many routers.

12 HARDWARE WARRANTY

The warranty period for the Universal Trunk Module hardware shall be ninety (90) days from the date of shipment from TeleComp R&D or a designated manufacturer. Replacements and repairs are guaranteed for the longer of the remaining original warranty period or 30 days whichever is longer.

13 SOFTWARE END-USER LICENSE AGREEMENT

This License Agreement ("License") is a legal contract between you and the manufacturer ("Manufacturer") of the system ("HARDWARE") with which you acquired software product(s) identified above ("SOFTWARE"). The SOFTWARE may include printed materials that accompany the SOFTWARE. Any software provided along with the SOFTWARE that is associated with a separate end-user license agreement is licensed to you under the terms of that license agreement. By installing, copying, downloading, accessing or otherwise using the SOFTWARE, you agree to be bound by the terms of this LICENSE. If you do not agree to the terms of this LICENSE, Manufacturer is unwilling to license the SOFTWARE to you. In such event, you may not use or copy the SOFTWARE, and you should promptly contact Manufacturer for instructions on return of the unused product(s) for a refund.

13.1 SOFTWARE LICENSE

You may only install and use one copy of the SOFTWARE on the HARDWARE (unless otherwise licensed by Manufacturer). The SOFTWARE may not be installed, accessed, displayed, run, shared or used concurrently on or from different computers, including a workstation, terminal or other digital electronic device (“Devices”). Notwithstanding the foregoing and except as otherwise provided below, any number of Devices may access or otherwise utilize the services of the SOFTWARE. You may not reverse engineer, decompile, or disassemble the SOFTWARE, except and only to the extent that such activity is expressly permitted by applicable law notwithstanding this limitation. The SOFTWARE is licensed as a single product. Its component parts may not be separated for use on more than one HARDWARE. The SOFTWARE is licensed with the HARDWARE as a single integrated product. The SOFTWARE may only be used with the HARDWARE as set forth in this LICENSE. You may not rent, lease or lend the SOFTWARE in any manner. You may permanently transfer all of your rights under this LICENSE only as part of a permanent sale or transfer of the HARDWARE, provided you retain no copies, you transfer all of the SOFTWARE (including all component parts, the media and printed materials, any upgrades, this LICENSE and, if applicable, the Certificate(s) of Authenticity), and the recipient agrees to the terms of this LICENSE. If the SOFTWARE is an upgrade, any transfer must also include all prior versions of the SOFTWARE. Without prejudice to any other rights, Manufacturer may terminate this LICENSE if you fail to comply with the terms and conditions of this LICENSE. In such event, you must destroy all copies of the SOFTWARE and all of its component parts.

13.2 INTELLECTUAL PROPERTY RIGHTS

The SOFTWARE is licensed, not sold to you. The SOFTWARE is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. You may not copy the printed materials accompanying the SOFTWARE. All title and intellectual property rights in and to the content which may be accessed through use of the SOFTWARE is the property of the respective content owner and may be protected by applicable copyright or other intellectual property laws and treaties. This LICENSE grants you no rights to use such content. All rights not expressly granted under this LICENSE are reserved Manufacturer and its licensors (if any).

13.3 SOFTWARE SUPPORT

SOFTWARE support is not provided by Manufacturer, or its affiliates or subsidiaries separate from the HARDWARE. For SOFTWARE support, please contact your supplier of the HARDWARE. Should you have any questions concerning this LICENSE, or if you desire to contact Manufacturer for any other reason, please refer to the address provided in the documentation for the HARDWARE.

13.4 EXPORT RESTRICTIONS

You agree that you will not export or re-export the SOFTWARE to any country, person, or entity subject to U.S. export restrictions. You specifically agree not to export or re-export the SOFTWARE: (i) to any country to which the U.S. has embargoed or restricted the export of goods or services, which as of March 1998 include, but are not necessarily limited to Cuba, Iran, Iraq, Libya, North Korea, Sudan and Syria, or to any national of any such country, wherever located, who intends to transmit or transport the products back to such country; (ii) to any person or entity who you know or have reason to know will utilize the SOFTWARE or portion thereof in the design, development or production of nuclear, chemical or biological weapons; or (iii) to any person or entity who has been prohibited from participating in U.S. export transactions by any federal agency of the U.S. government.

13.5 LIMITED WARRANTY

Manufacturer warrants that (a) the SOFTWARE will perform substantially in accordance with the accompanying written materials for a period of ninety (90) days from the date of shipment from TeleComp R&D or a designated manufacturer. Software support is limited to the hours of 9AM to 5PM ET Monday through Friday excluding TeleComp R&D observed holidays. An extended warranty may be purchased at additional cost. Any implied warranties on the SOFTWARE are limited to ninety (90) days. Some states/jurisdictions do not allow limitations on duration of an implied warranty, so the above limitation may not apply to you.

Manufacturer's and its suppliers' entire liability and your exclusive remedy shall be, at Manufacturer's option, either (a) return of the price paid, or (b) repair or replacement of the SOFTWARE that does not meet this Limited Warranty and which is returned to Manufacturer with a copy of your receipt. This Limited Warranty is void if failure of the SOFTWARE has resulted from accident, abuse, or misapplication. Any replacement SOFTWARE will be warranted for the remainder of the original warranty period or thirty (30) days, whichever is longer.

13.6 NO OTHER WARRANTIES

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, MANUFACTURER AND ITS SUPPLIERS DISCLAIM ALL OTHER WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT, WITH REGARD TO THE SOFTWARE AND THE ACCOMPANYING WRITTEN MATERIALS. THIS LIMITED WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHERS, WHICH VARY FROM STATE/JURISDICTION TO STATE/JURISDICTION.

13.7 LIMITATION OF LIABILITY

To the maximum extent permitted by applicable law, in no event shall Manufacturer or its suppliers be liable for any damages whatsoever (including without limitation, special, incidental, consequential, or indirect damages for personal injury, loss of business profits, business interruption, loss of business information, or any other pecuniary loss) arising out of the use of or inability to use this product, even if Manufacturer has been advised of the possibility of such damages. In any case, Manufacturer's and its suppliers' entire liability under any provision of this License shall be limited to the amount actually paid by you for the SOFTWARE and/or the HARDWARE. Because some states/jurisdictions do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation may not apply to you.

13.8 SPECIAL PROVISIONS

The SOFTWARE and documentation are provided with RESTRICTED RIGHTS. Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and HARDWARE Software clause at DFARS 252.227-7013 or subparagraphs (c)(1) and (2) of the Commercial HARDWARE Software-Restricted Rights at 48 CFR 52.227-19, as applicable. Manufacturer is TeleComp R&D or it’s designee manufacturer., 102 SW Orange Blossom, Lake City, Florida, 32025-1613.

If you acquired the SOFTWARE in the United States of America, this Software License are governed by the laws of the State of Florida, excluding its choice of laws provisions. If you acquired the SOFTWARE outside the United States of America, local law may apply. This LICENSE constitutes the entire understanding and agreement between you and the Manufacturer in relation to the SOFTWARE and supercedes any and all prior or other communications, statements, documents, agreements or other information between the parties with respect to the subject matter hereof.

14 SALES & DISTRIBUTION

CBM of America, Inc.
Mr. Mike Stephens
1455 West Newport Center Drive
Deerfield Beach, Florida
33442

800-881-8202
954-698-9104 Fax: 954-360-0682

www.cbmusa.com

DATATEK APPLICATIONS, INC.
Mr. Dan Conklin
379 Campus Drive, Suite 100
Somerset, New Jersey
08873

732-667-1080 Fax: 732-667-1091

www.datatekcorp.com

15 AUTHOR

Comments and Questions regarding this document or the products covered within this document should be addressed to the author Angel Gomez via email at angel@trdcusa.com or via telephone at 386-754-5700.