PROGRAM OF INSTRUCTION

FOR THE DIGITAL TRAINING FACILITY MANAGER (DTFM)

Prepared For:
The Program Management Office TADLP
Rock Landing V
11846 Rock Landing Dr.
Newport News, VA 23606

Prepared By:
ACS Systems & Engineering, Inc.
5301 Cleveland St.
Virginia Beach, VA 23462

14 NOVEMBER 2001

Version 2.0

Disclaimer

The use of trade names in this document does no constitute an official endorsement or approval of the use of such commercial hardware or software. Do not cite this document for the purpose of advertisement

Changes

Refer requests for all changes that affect this document to:

Army Distance Learning Program Office

Attn: Bob Williamson (DTFM-PM)

Bldg. 1522, 11th Street

Fort Eustis, VA 23604-5168

OFFICIAL BUSINESS #41

Disposition Instructions

Destroy this document when no longer needed. Do not return it to the organization. Safeguard and destroy this document with consideration given to its classifications or distribution statement requirements.

LESSONS INCLUDED

① Block 1 Sites ② Block 2 Sites

Lesson I: Non-Networked Courses ① 20

Task: In-processing students for IMI.

Condition: DTFMs will follow the procedures for registering students, in-processing them into the DTF, and assisting them as required.

Standard: DTFMs will submit the required information to register student(s), and act as the classroom facilitator. DTFMs will also monitor the classroom equipment and correct problems in a timely manner per the guidelines for daily operation of the DTF.

Duration: 15-20 minutes **Method of Instruction:** VTT/Self-paced study in DTF

Lesson II: Setting Up and Using Outlook② 22

Task: Using Microsoft Outlook (managers' workstation only)

Condition: DTFM will follow the procedures for setting up an Outlook account, using messaging, *(email system on TADLP DOMAIN)* and the calendar system for scheduling classes, and for checking and resolving scheduling conflicts.

Standard: DTFM will verify that classes are scheduled and that there are no conflicts, DTFM will also use the messaging system to contact the TAC Help Desk, Security, and other DTFMs.

Duration: 30 - 45 minutes **Method of Instruction:** VTT/Self-paced study in DTF

Lesson III: Using ARWeb② 28

Task: Using ARWeb

Condition: DTFMs will learn the procedures for logging onto the ARWeb web-site, registering students, submitting utilization reports and opening trouble tickets.

Standard: DTFMs will log on to the ARWeb site, submit the required information for registering students, and report classroom utilization. They will also submit trouble tickets in a timely manner.

Duration: 25-30 minutes **Method of Instruction:** VTT/Self-paced study in DTF

Lesson IV: Networked Courses② 30

Task: Check students in for Networked Courses.

Condition: DTFMs will follow the procedures for registering students, in-processing them into the DTF, and assisting them when required.

Standard: DTFMs will submit the required information to register student(s), and act as the classroom facilitator. DTFMs will also monitor the classroom equipment and correct problems in a timely manner per the guidelines for daily operation of the DTF.

Duration: 15-20 minutes **Method of Instruction:** VTT/Self-paced study in DTF

Lesson V: TADLP Workstation Usage[1][2] 32

Task:	Usage of the workstation by a DTFM, student/users, and courseware developers.		
Condition:	DTFM will instruct the student how to log on using the UserID and password, assist the student in the proper procedures for changing the password, and the loading of software on the computer used for his/her training. The DTFM will also walk the student through the steps for locking the workstation during breaks and or lunch. In addition, managers will instruct the student in the proper procedures for shutting down and restarting the computer at the end of the day.		
Standard:	DTFM will perform the items covered in this training per the guidelines for daily operation of the DTF.		
Duration:	20-30 minutes	Method of Instruction:	VTT/Self-paced study in DTF

Lesson VI: Data Storage[1][2] 34

Task:	Saving items to the "SHARED" Drive		
Condition:	DTFM will follow the procedures as outlined in the following training and assist the student in saving the items or documents he or she is using.		
Standard:	DTFM will perform the items covered in the training per the guidelines for daily operation of the DTF.		
Duration:	15-20 minutes	Method of Instruction:	VTT/Self-paced study in DTF

Lesson VII: Procedures for Imaging Computers[1][2] 36

Task:	Normal student workstation imaging.		
Condition:	DTFM/students will image the workstations by following the instructions on the desktop listed as step 2 for restarting the computer or by using the Pullman utility.		
Standard:	The DTFM will monitor re-imaging of all the workstations at the end of the workday.		
Duration:	20-25 minutes	Method of Instruction:	VTT/Self-paced study in DTF

Lesson VIII: TAC Help Desk[1][2] 38

Task:	Understand TAC Help Desk Structure		
Condition:	The DTFM will become familiar with the responsibilities and processes of the Training Access Center Help Desk.		
Standard:	DTFMs will acquire total understanding of help desk structure, responsibilities, and functions.		
Duration:	10-15 minutes	Method of Instruction:	VTT/Self-paced study in DTF

Lesson IX:Computer Component Replacement[1][2] 42

Task:	Replacing Computer Components.		
Condition:	DTFMs will be able to follow the procedures for replacing computer components.		
Standard:	DTFMs will be able to replace computer components and return workstations to normal operation.		
Duration:	1-2 hours	Method of Instruction:	VTT/Self-paced study in DTF

POSITION OVERVIEW

Contact Information

The DTFMs are under the operational control of the distance learning point of contact (POC) at each site, and under the administrative and managerial control of the DTFM Project Manager (PM) for ACS Systems & Engineering located in Fort Eustis, VA. The following Training Access Center information is provided for coordination purposes:

Address	Army Distance Learning Program Office	Phone:	COM	(757) 878-0442	DSN	927-0442
	Attn: Bob Williamson (DTFM-PM)	Fax:	COM	(757) 878-0440	DSN	927-0440
	Bldg. 1522, 11th Street					
	Ft. Eustis, VA 23604-5168					
	OFFICIAL BUSINESS #41					

Distance Learning Training:

The Total Army Distance Learning Program (TADLP) is designed to support training for Active Duty Soldiers, the Reserve Component, DOD Civilians and others as approved by the local commander. Access to the DTFs must be provided based on the hours established by the installations/commands for normal operations prior to obtaining full operational capability. The operating hours will not exceed those set by the TADLP PM office. Any training beyond the standard hours will require the local installation/command to either provide trained individuals or to coordinate with the TADLP PM office for DTFM support to accommodate the schedule.

Video Teletraining (VTT) describes the system providing real time two-way communication via video and audio that can be transmitted simultaneously to multiple Distance Learning sites. Sometimes, this results in several time zones receiving training concurrently. Upon approval, the VCR supplied with the VTT equipment can be used to record the transmission.

In other cases, a flexible schedule may be more appropriate. A training battalion in a remote area may adjust site operating hours for asynchronous training to suit student availability. Synchronous (concurrent) training requirements must also be met. For periods after normal duty hours, installation and local POCs or commanders may adjust DTF operating hours to meet local conditions.

Other Training:

A DTF may be used for other instruction when it is not scheduled for distance learning training. This other training is required to meet all security requirements and must not change, modify or cause the system configuration to change beyond the capability of restoring the systems from the server. All personnel receiving non-distance learning training must meet security requirements for use of DOD computer systems.

General:

The DTFM is responsible for daily DTF operation under the direction of the installation POC. The following chart outlines the various responsibilities of the DTFM with relation to each site.

The DTFM will:

Operate the DTF in accordance with the schedule and availability restrictions established by the local POC.
Implement procedures to identify, account for, and secure all assigned equipment.
Ensure sufficient classroom seats are available for both incoming students and students currently in training. In addition, a student ID and password must be requested by completing a "Student Account Request Form" and submitting it to TAC Help Desk.
Perform preventative maintenance as indicated in PM procedures. Perform limited repairs on TPW computer systems (i.e., replace hard drive, power supply, switches, fans, 3.5 drive and PC cards).

Organizational Responsibilities:

Digital Training Facilities provide training to Active Duty soldiers, the Reserve Component, Department of the Army Civilian (DAC) personnel and other authorized students within a fifty-mile radius of your location. Please see the section entitled "First Time Classroom Set-up" for more information regarding these specific components.

Security:

You will need to become familiar with the TADLP Information Systems Security briefing, the INFOSEC Security CD-ROM, Security Features Users Guide (SFUG), and the Trusted Facility Manual (TFM).

World Wide Web sites - Access to Web sites are authorized only when posted to the Internet using official Army Service providers. Commercial Internet service providers will not be used to provide Web sites for TADLP. The installation commander will assign Information System Security Office (ISSO) responsibility for the DTF.

Briefings:

Each DTFM is required to present two briefings to each student or class utilizing the DTF.

ORIENTATION BRIEF:

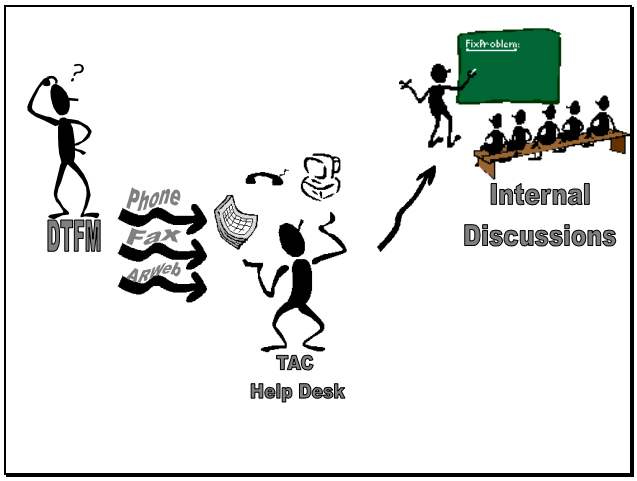
An orientation briefing is required to give the student the required information about the operating hours of the DTF, location of the necessary facilities within the building, and to notify the students that there will be no eating, drinking, or tobacco product use allowed in the DTF. This briefing is completed each time a student or class utilizes the DTF.

INFOSEC BRIEF:

The second briefing is the INFOSEC briefing presented via Microsoft Power Point on the VTT monitor, or via student handout. Upon completion, each student must read and sign the "TADLP INFOSEC Student and User Agreement". This briefing is given to each student and is valid for one year.

Training Access Center (TAC):

One important function of the Training Access Center (TAC) is to provide Help Desk services to TADLP students, Digital Training Facility Managers, and instructors.



POINTS OF ENTRY FOR SERVICE CALLS COMING INTO THE HELP DESK.

TAC Help Desk Site Information:

Mailing/Shipping Address:	TAC Building 1522, TAC PO Box "O" 11th Street Fort Eustis, VA 23604	**Help Desk Phone**	Toll Free COM DSN	(877) 251-0730 (757) 878-4745 927-4745
		Help Desk Fax	COM DSN	(757) 878-0440 927-0440

The TAC Help Desk is responsible for supporting the DTFM in DTF operations. The DTFM may call the TAC Help Desk for immediate assistance and to report any problems affecting DTF operation 24 hours a day seven days a week.

Each DTFM is responsible to report problems and issues within the DTF for the equipment listed below:

Workstations

- Monitors
- CPUs
- Mouse
- Keyboards
- Power strips
- Network Interface Cards (NICs)
- Printers/fax machines

VTT System

- Monitors
- VTEL 5000
- Gate Mixer
- Student camera
- Push-to-talk microphones
- Video cabinets
- Manager microphones
- ELMO
- Keyboards
- RF receivers
- IR receivers

NOTE

Problems with the VTT systems must first be reported to the Network Control Center (NCC) at (757) 878-4815 for resolution. The NCC is responsible for connection and repair of the VTEL system. If encounter a problem with the VTT system when attempting to make a connection for scheduled training, immediately contact the NCC to resolve the problem and then follow up by opening a trouble ticket with the Help Desk.

Additionally, the DTFM will submit a trouble ticket to the TAC Help Desk if there is a problem that is beyond the DTFM responsibility. Examples are listed below:

- Electrical - Power outages (note when power goes out and when it is restored).
- Mechanical - Inoperative heating ventilation and air conditioning (HVAC) systems or degraded HVAC systems that may cause disruption to the training environment.
- Furniture - Desk lamination (top or bottom), or any items affecting the capability to support the computer systems. This includes problems with student/user chairs.
- Telephone System - Phone system outages or missing instruments.

Trouble Shooting:

The DTFM will troubleshoot problems with system computers, network components and printers and will perform repairs as necessary. The DTFM should not leave the DTF for the day unless all trouble tickets are resolved or released by TAC Help Desk due to lack of replacement components.

Component replacement is authorized after communication with the TAC Help Desk and the needed required new parts are received from TPW. Components authorized for replacement are hard drives, power supplies, sound cards, video cards, NIC cards, CD-ROMs, and 3.5 floppy drives.

Problem Reporting:

It is the responsibility of the DTFM to insure that updates to the problem reports are furnished to the TAC Help Desk on all trouble tickets. When the problem is resolved, the DTFM will contact the TAC Help Desk to close out the ticket. Tracking of all trouble tickets will be done using the trouble ticket number generated by the TAC Help Desk.

The DTFM is responsible to maintain copies of the closed trouble tickets for the current year in an active file. Please use the file entitled CM-102 Trouble Ticket Log, which can be found on either the new DTFM-CD or on the FTP site in the folder named **Forms**, subfolder **Classroom Forms**. At the end of the current year the file will be maintained as an inactive file for a period of one year and then destroyed. These files are subject to inspection and review by the Office of the Program Manager.

CM-102 Trouble Ticket Log

It is vital that the DTFM promptly report all problems to activate the repair sequence allowing the PM to track the time elapsed in system repair and problem resolution. To ensure vendors meet their contracted repair times, the DTFM is the key individual in setting the repair procedure in motion.

When problems arise with the VTT system, the DTFM will first report the problem to the NCC and subsequently report the problem to the TAC Help Desk and provide feedback as the NCC works to resolve the issue.

Network Control Center (NCC):

The Network Control Center is responsible for operating and supporting all the components required for VTT connectivity to all DTFs and other VTT sites. The NCC is located at Fort Eustis, VA. Please refer to the section entitled "General VTT Information" for more detail.

Tools used by the DTFM to operate the DTF:

THERE ARE SEVERAL TOOLS AVAILABLE FOR THE DTFMS USE ARE LISTED BELOW:

- ✓ Microsoft Exchange (Outlook) for E-mail and Calendar functions to enter scheduled training under the "public folders" section. Each networked DTFM has the capability to see what other DTFMs have scheduled in their classrooms by viewing the calendar for that site under the public folders.
- ✓ Army Knowledge Online (AKO) for Messaging outside of the closed DL Network and using Internet Explorer.
- ✓ ARWeb can be accessed via Internet Explorer and is used to submit facility usage reports, TAC Help Desk service requests, TADLP student registration, and DTF asset inventory updates.

NOTE

Tickets requiring immediate attention should **NEVER** be entered through ARWeb

Administrative Duties

Courseware:

Only approved courseware is authorized for use in the DTF. The student will load all CD-ROM based courseware onto the workstation. Networked DTFs will have the capability to load courseware to the "D" partition of the hard drive only. A master list of approved and tested courseware can be found at www.tadlp.army.mil. To access the list, select "Enter", "Links", and click on "Courseware CDs" for software customarily available at every DTF or on "TADLP Tested Courseware" for approved software available for order by the student.

The DTFM will maintain a copy in each DTF of all legacy courseware provided by the TADLP PM that may be used in the DTF. Instructors and students may use these copies; however, they are not to be removed from the classroom.

It is also the responsibility of the DTFM to coordinate with installation or TASS (The Army School System) battalion commander regarding emergency enrollments (e.g., deployment requirements) that exceed facility capabilities.

SmartForce courseware is web-based courseware and instructions for utilization of this courseware can be found in the DTFM SOP (Standard Operating Procedure) Manual.

Utilization Reports

DTF sites that are networked will submit usage reports via ARWeb. More information on ARWeb can be found in the DTFM SOP and DTFM Program of Instruction (POI), Lesson VII.

DTF sites that are not networked will submit reports using the TADLP web site, www.tadlp.army.mil under "Utilization."

Student Assistance:

The DTFM will monitor student needs during training and advise students that the senior service member will be in charge of maintaining discipline in the DTF. At the beginning of every session, the DTFM will identify who that individual is. Traditionally in the military, the senior service member is always responsible for good order and discipline. If the senior service member is unable to maintain discipline in the DTF, the DTFM will advise the installation/site POC of the situation.

In addition, the DTFM will show students how to install IMI Courseware and will monitor its use. Your responsibility is to maintain functionality, not content, and provide assistance as necessary.

Contact the TAC Help Desk with all courseware problems and they will direct you to the ATSC Help Desk.

FIRST TIME CLASSROOM SET-UP

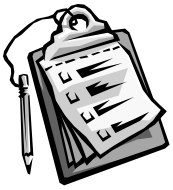
Types of Installations

Digital Training Facilities provide training to Active Duty soldiers, the Reserve Component and Department of the Army Civilian (DAC) personnel and other authorized students within a fifty-mile radius.

Active Component Installations:

Installation commanders or POCs will have operational control for TADLP facilities and DTFMs at active component installations. This responsibility includes property accountability. It is the responsibility of the POC to ensure that the equipment located inside the DTF is entered into the property book for that site.

Each DTF at an active component site will consist of 16 student workstations (One per station: CPU, monitor, keyboard, mouse, and headphones), 1 manager workstation (One of each: CPU, monitor, keyboard, mouse, and headphones), 1 office jet multifunction machine (allowing printing, faxing, copying and scanning of documents), and a HP Laser printer. Each DTF will also have a VTT system installed and configured to allow two-way training with other sites. Each site will have the necessary networking equipment installed to allow for network connections to the NIPRnet (Internet) to provide access for web-based training. Enterprise management from the TAC located at Fort Eustis, VA, will monitor the network and provide necessary patches, Norton Anti-Virus (NAV) updates and other upgrades as required by the program manager.



Components: The following components are parts of the networking solutions for the active component locations

- EED: Encapsulation encryption device
- Switch: Cisco 2900 series switches
- UPS: Uninterrupted Power Supply
- Servers: Three IBM servers at located at each site.
- Monitor: One monitor
- Keyboard: One keyboard
- Mouse: One mouse
- KVM Switch: Allows the manger to view the three servers using only one monitor, keyboard, and mouse.

Reserve Component Installations:

TASS training battalion commanders, in coordination with the brigade commander and the Regional Coordinating Element (RCE), provide command and control for DTFMs at reserve component DTFs. This responsibility includes property accountability and designating an ISSO. These facilities support the local reserve component and reserve component student populations within their regions. Each DTF at a reserve component site will consist of 12 student workstations (One per station: CPU, monitor, keyboard, mouse, and headphones), 1 manager workstation (One of each: CPU, monitor, keyboard, mouse, and headphones), 1 office jet multifunction machine (allowing printing, faxing, copying and scanning of documents), and a HP Laser printer. Similar to the Active Component facilities, each DTF will also have a VTT system installed and configured to allow two-way training with other sites. Each site will have the necessary networking equipment installed to allow for network connections to the

NIPRnet to provide access for web-based training. Enterprise management from the TAC located at Fort Eustis, VA will monitor the network and provide necessary patches, Norton Anti-Virus (NAV) updates and other upgrades as required by the Program Manager.

Components: The following components are part of the networking solutions for the reserve component locations

- EED: Encapsulation encryption device
- Switch: Cisco 2900 series switches
- UPS: Uninterrupted Power Supply
- Servers: Three IBM servers at located at each site.
- Monitor: One monitor
- Keyboard: One keyboard
- Mouse: One mouse
- KVM Switch: Allows the manger to view the three servers using only one monitor, keyboard, and mouse.
- Router: One each
- IDS: Intrusion Detection System

Supplies and Set-up

Classroom Set-up Folder (DTFM CD)

FOR NEW DTFS NOT NETWORKED, THE FOLLOWING SUPPORT IS AVAILABLE:

- ✓ Each new DTFM will contact the TADLP Project Manager's Office at 757 878-6491 to provide the necessary information to the PM representative to obtain a TSACS for e-mail capability within the DTF.
- ✓ Each new DTFM will contact the TAC Help Desk manager to provide the necessary information to ensure that the correct site and DTFM information is entered in the proper databases.
- ✓ Each new DTFM is hired two weeks prior to the completion of the DTF and during this time period the DTFM will do the following:

1) Perform equipment setup and check out procedures to ensure that all classroom equipment is operable.
2) Perform inventory in soft copy (templates will be provided) and send to DTFM PM.
3) Submit the Initial Equipment Inventory Reports for newly established TADLP classrooms. These reports, (the Video Teletraining (VTT) Inventory Report and the Computer Equipment Inventory Report) are submitted once and updated through the TAC Help Desk. The reports are used to populate the Configuration Management Baseline. The Baseline must be maintained to ensure the TADLP system retains the capability to meet the training load.
4) Work with the construction team and become knowledgeable about the wiring of the classroom and the equipment installed.
5) The networking portion of the DTF will be installed and set up to provide internal networking of the DTF to allow functions such as imaging and tape back up but with no outside connectivity to the TAC or RTAC. Installers and software engineers will provide basic training on necessary functions.

6) Make contact with the DL POC to insure that there is a proper understanding of the DTF position and work hours are established. Unless instructed differently, the operating hours for the new DTF are 40 hours per week. If weekend work is required, hours worked will be compensated during the week (e.g., If work is done on Saturday, time off will be taken during that pay period.)

Items Provided to DTFM:

Each site will be provided a "push package", which consists of the following items to support the DTF and DTFM:

• 3.5 " Diskettes	• scotch tape with dispenser
• Disk and CD cleaning kits	• 3 hole punch
• paper towels	• binders
• cleaning Solution	• Laser print cartridge
• compressed air	• Office jet cartridge (color and black)
• printer paper	• post it's
• VCR head cleaner	• white-out
• VHS tapes	• batteries
• rubber bands	• computer tool kit
• pens/ pencils	• pencil sharpener
• paper clips	• key cabinet
• writing pads	• trash can
• stapler with staples	• file folders

Each DTF has one workstation per student, one manager workstation, one filing cabinet, a storage cabinet, a bookcase and a coat-rack.

AF-101 Order Form

Replenishment of items in the push package will be accomplished by submitting a request form to the ACS supply room. If you require an item not on the replenishment list, approval must be obtained prior to making any purchase.

Each push package contains four CD-ROMs. Two of the CDs contain training for the VTT system; one CD is the "MS Office 2000 standard" package to be installed **only** on the VTT system. The last CD, titled "DTFM," contains all the required documents and forms needed for the DTFM to support the program and submit the proper documents to ACS for required functions. Updates to these forms will be provided using the ACS FTP site. Information on how to access this site is provided in this document.

DTF File Process:

To ensure all DL sites have the required documents, forms, and file set up; the filing system outlined below will be used.

SECURE FILE CABINET SETUP:

The secure file cabinet will be utilized to maintain all instructions and forms used to support DTF operations. Files contained in the secure file cabinet will be maintained for two years. The current 12-month files will be maintained in the active file drawer while the previous 12-month files will be maintained in an inactive file drawer.

The standard file system used by the DTFM will be as follows:

DRAWER 1	**Active files** (Month 1-12) **Manuals**– DTFM SOP, Computer Operations Manual and Student SOP, Security Instructions and DTFM POI. **Class folders** - consisting of all information obtained for each student (i.e. copies of orders, account registration forms and the class DTF sign in/out log). **Walk-in DTF sign in/out log**. **Preventive Maintenance Logs** **Visitor Logs** **Trouble Ticket Log** **Copy of INFOSEC Brief** **SF 701 Activity Security Checklist**
DRAWER 2	**Continuation of the active file drawer** (if required) **Any local site required documents**
DRAWER 3	**Blank Forms & Miscellaneous**
DRAWER 4	**Inactive file drawer** **Inactive Files** (Month 13 to 24)

NOTE:

In the event that a folder is maintained in another location a reference document will be placed in the appropriate file folder indicating where the file is located/maintained.

SECURITY RESPONSIBILITIES

Some of the most important duties of the DTFM revolve around security issues, specifically: maintaining the integrity of the room and equipment, ensuring that only properly authorized personnel are admitted, and preserving the functionality of software and hardware. Each section will be explained in detail below.

Physical Facility Security

The physical security of the TADLP facility includes structural integrity, key control, lighting, lock application, inventory, and accountability. Physical and environmental security standards must be established to prevent unauthorized access, damage, or adverse interference to TADLP premises, IT services, and other assets. TADLP facilities supporting critical or "Sensitive But Unclassified" (SBU) activities must also be physically protected from security threats and environmental hazards. In addition, TADLP facilities will only be used for authorized business purposes. Guidelines to fulfill these goals follow:

- The classroom access door must be locked during all unattended hours.
- All forms, software, student records, and other documentation should be securely filed away following TADLP guidelines.
- All lighting should be maintained in working order with bulbs and fixtures replaced as necessary.
- An inventory of all equipment and software should always be current.
- Portable computing equipment (laptop or palmtop computers) or data transfer devices (CD-R drives, Zip drives, etc.) may not be connected to the DTF network at any time.

NOTE:

Any suspected intruder activity or theft of equipment/information should be reported to the Information Systems Security Officer (ISSO) in writing and to the TAC Help Desk immediately.

Access to the Facility

TADLP provides for training available only to certain sections of the DOD population. All other users must receive permission from the local POC with Program Management approval. In order to comply with this standard, the DTFM should perform the following checks:

- Verify the user's identity, need-to-know status, and access authorizations by checking students for the appropriate DD Form 2 or Form 1602, or memorandum signed by a CG installation CO or school commandant.
- Ensure that all appropriate paperwork to obtain user identifications and passwords is completed and submitted in a timely fashion.

Information Security

The subject of information security covers a variety of subjects including security briefings, virus prevention, software standards, data backup and recovery, User Identification (UserID) and password control, and the retention and storage of student records, and user and courseware documentation.

Security Briefings

The DTFM will present the INFOSEC security briefing for every user of the facility either via PowerPoint presentation on the VTT or handout. After the briefing, the DTFM will obtain from the user a signed copy of the "TADLP INFOSEC Student and User Agreement". This briefing is given to each student and is valid for one year.

Virus Prevention Policies and Procedures

The "Virus Protection Strategy" is the plan for implementing the necessary processes to keep the TADLP network virus free. Viruses (also known as "malicious logic") are programs that can cause a computer or network to malfunction or fail completely. The objective for the Virus Protection Strategy is to anticipate and minimize the impact of viruses on the TADLP. Our strategy involves the following components:

- Awareness of viruses
- Incident management
- Reporting and analysis of incidents

In order to implement this strategy, the TADLP will provide Norton Anti-Virus software on all Windows NT Servers/Workstations within the network and procedures to update the virus definition files every two weeks.

To minimize the potential impact of virus infection of the TADLP network and workstations, only authorized TADLP software may be introduced to the DTF per the guidance of TADLP Project Manager's Office Courseware section. Students and users may not bring in or load any software on any TADLP Workstation. Authorized software is provided officially through government channels.

Suspected Virus Infection

In the event the DTFM suspects either a virus infects the network or workstations, he or she will do the following **immediately:**

1) Report the incident to TADLP TAC Help Desk Operator. TADLP TAC Management will inform the appropriate Army officials IAW IA-25 and AR 380-5.
2) Conduct an investigation into all computer security violations to determine the extent of the compromise.
3) Inform the Information Systems Security Officer (ISSO) of the potential security compromise in writing.

Software Standards

It is imperative that the integrity of the basic setup for every workstation be strictly maintained. The tool used by the DTFM to implement this policy is known as "disk imaging." A copy (known as an "image") of the basic software and hardware configuration for every computer is saved in a central location on the servers and each computer has its own unique disk image. In order to reset a computer to its ready state, the image must be loaded from the server onto the individual workstation. Any changes to disk images must either originate from TADLP or the TAC Help Desk.

NOTE:

Every student workstation should have the basic image loaded back onto the machine at the end of every day.

Only TADLP approved software and courseware may be loaded onto any workstation in the DTF. No software may be loaded onto network servers without prior approval.

In addition, both original and backup copies of CD-ROM courseware stored in the classroom should be securely stored in the cabinet. The proponent schools, including courseware developers and instructors, have the responsibility to protect and maintain master copies of course materials.

Backup and Recovery

The objective the TADLP Backup and Recovery Strategy is to anticipate and minimize the impact of failures on the network. Managing the backup and recovery processes involves predefined documented procedures and software/hardware recovery capability. The objective is to ensure that the TADLP organization achieves its defined availability service levels.

The DTFM is responsible for diligence in labeling backup tapes and replacing them in the servers on a rotating schedule.

User Identification (UserID) and Password control

Every student and user of the DTF is assigned a unique UserID (or login) and password. The DTFM must remind all users that this information is secret and should not be written down, shared, or otherwise stored.

Retention and Storage of Student Records

The following shall be maintained for each user in the locked cabinet:

1) Copies of student orders
2) Registration Form
3) Signed INFOSEC acknowledgment statement

These records will be saved in an active file for a period of one year. After one year has elapsed, these records should be moved to an inactive file. Following the expiration of the second year, these records shall be destroyed.

User and Courseware Documentation

The DTFM will give documents printed per user/student request an appropriate cover sheet identifying the document as FOUO or Privacy Act Information. Users should use due diligence to prevent unauthorized disclosure of these records.

REPORTING AND RESOLUTION OF INFORMATION SECURITY VIOLATIONS

All suspected and potential compromises of information security guidelines will be reported in writing to the ISSO including supporting evidence and documentation.

TADLP COOP/Contingency Responsibilities:

The DTFM will prepare a list of possible installation-specific situations that may impact security concerns. The SOP will be modified to deal with any site-unique contingencies. The DTFM is also responsible for periodic testing of COOP/Contingency Plan components and ensuring that required updates to the COOP/Contingency Plan made alongside all changes to the system.

CONTINGENCIES:

- The basic element of TADLP architecture is the DTF. The following contingencies should be considered, and plans developed to address each of these and any other installation-specific circumstances identified.
- Loss of functionality of individual software including operating system and courseware, or processors (e.g., DTFM workstation, student workstation, etc.).
- Temporary or permanent loss of individual pieces of equipment within the DTFM or student workstation (e.g., hardware loss).
- Temporary or permanent loss of any aspect of training applications such as lost videotape, missing CD-ROM, etc.
- Training material that has become corrupt or unusable.
- Loss of TADLP system data such as user identification (UserID) or password at any installation
- Temporary or permanent loss of individual pieces of equipment within TADLP information system architecture.
- Loss of communications lines: Video Tele Training (VTT), voice, or both.
- Temporary or permanent loss of an entire DTF. All installation instructors, DTFMs, and users/students must be prepared to respond to these contingencies and take the necessary action to restore the system to an operational state according to the local COOP/Contingency Plan or DTFM SOP.

Availability Requirements and Solutions:

Requirements and system design solutions to restore DTF operations within one hour following a failure or loss.

- Restoration of the TNET VTT will be accomplished using the existing maintenance contract for all problems that exceed the capabilities of the DTFM.
- In the event of a complete DTF failure, the DTFM will attempt to coordinate a move to an open TADLP DTF at the same site if possible.
- Communications must be restored within 24 hours. Voice and video communications (e.g., telephones, TNET signal lines, etc.) are quickly repairable via maintenance contracts. Failed equipment no longer under individual maintenance contracts may be replaced through replacement of components available at the installation or through vendor support.
- Restoration of leased circuits will be pursuant to the leasing agreement. Data integrity will be maintained.

LESSON I: NON-NETWORKED COURSES

Resident, IMI and VTT Courses

TASK: In-processing students for IMI.

CONDITION: DTFMs will follow the procedures for registering students, in-processing them into the DTF, and assisting them as required.

STANDARD: DTFMs will submit the required information to register student(s), and act as the classroom facilitator. DTFMs will also monitor the classroom equipment and correct problems in a timely manner per the guidelines for daily operation of the DTF.

CT-100 Class Log OR CT-103 Walk-in Log
One copy each: All Contents of Block 1 Security Folder (DTFM-CD)
SF-100 Security Statement
SF-101 Student Registration Form

1) Verify Student eligibility:

- Request the students military or Department of the Army Civilian (DAC) Identification Card.
- Request the student's orders, if available.
- Ensure the courseware the student will be utilizing is TADLP approved.

2) Register Students:

- Copy the student's orders if available.
- Seat the student at a workstation.
- Ask students to complete a Student Registration form (SF-101), if not previously submitted. Please attempt to have account requests completed at least 24 hours prior to the commencement of class. Submit the completed account request via ARWeb or by faxing forms to the TAC Help Desk. Perform this step only if computers will be used during the training session.
- Have the student complete a class attendance form. (CT-100 OR CT-101 OR CT-103)

3) Brief Students:

- Welcome students to the TADLP classroom and advise them regarding your responsibilities.
- Inform students of building facilities and classroom procedures.
- Brief the users on the INFOSEC Brief/Army Privacy Act program.
- Have students complete the TADLP INFOSEC Security Statement (SF-100)

4) Student Log on:

- Give the student his or her UserID and generic password as generated by the TAC Help Desk.
- Inform the student that the new password must be at least 8 characters in length and that at least one character must be either upper case or a numeral.
- Instruct the student in the procedure for locking the workstation during breaks. This is done by pressing the "Ctrl-Alt-Delete" keys simultaneously, then pressing the "W" key or clicking the "lock workstation" button once.
- Next, explain the proper shutdown procedure: Pressing "Ctrl-Alt-Delete", moving the cursor over the "shut down" button and left-clicking once on "Shut Down". The student should then place the cursor over "Shutdown and Restart" and left-click in the circle for "Shutdown and Restart." Finally, the user should move the cursor over the "OK" button and left-click once. This will be done when the student leaves for the day unless previous arrangements for multi-day usage have already been made. For instructions on how to make arrangements for multi-day usage, please consult the *Multi-Day Course Procedure* section of Lesson VII.

5) Assist Student:

Resident Courses:

- Inform students that the computers are to remain on with the monitors turned off if workstations are not required for their training session. If they suspect that something may be wrong with the computer they should notify the DTFM and not take any action to correct the problem.
- The push-to-talk microphones on the desks are used for VTT sessions only and should not be used during the training session unless required.
- Act as a facilitator to assist the students and instructor as required. Operate the VTT equipment on behalf of the instructor.

Options

IMI Courses:

- Refer to section 4.3 of the Computer Operation Manual.
- Follow courseware load instructions provided with the CD.

VTT Courses:

- Notify students about the start and completion times of the training session.
- Brief students on use of push-to-talk microphones and related camera functions.
- Assist students as needed. (e.g. faxing information, recording VTT sessions, providing required course material to students, etc.)
- Monitor VTEL equipment for proper operation during the VTT. Call NCC to correct operational problems as required. If you encounter transmission difficulties, NCC will join in to the conference, monitor the system, and attempt to correct the problem.

6) After Training:

- Check that the student workstation is operational, that all components are present and that the area is neat and orderly.
- Ensure that all materials to be retained in the DTF are returned.
- Perform any preventative maintenance to prepare the system for the next student.
- Ensure that the student logs off the computer properly. At this time you may inform the students that they may leave.
- Determine if the machine has a clean image. If not, manually re-image the computer.
- Report any damaged or missing items to the student's commander, the TAC Help Desk, and the PMO RMD.
- If this is the last class in the DTF for the day, secure the DTF and initial the Standard Form 701.

LESSON II: SETTING UP AND USING OUTLOOK

TASK: Using Microsoft Outlook (managers' workstation only)

CONDITION: DTFM will follow the procedures for setting up an Outlook account, using messaging, *(email system on TADLP DOMAIN)* and the calendar system for scheduling classes and for checking and resolving scheduling conflicts.

STANDARD: DTFM will verify that classes are scheduled and that there are no conflicts, DTFM will also use the messaging system to contact the TAC Help Desk, Security, and other DTFMs.

Purpose for Using Microsoft Outlook

Outlook is a messaging system connecting TADLP personnel. This system allows the DTFM to send messages to TAC Help Desk, Security, or any individuals in the TADLP system.

In addition, the system allows the TAC Help Desk to inform the DTFM regarding classroom schedules and student enrollment as provided by ATRRS.

A calendar system to allow the DTFM to update the classroom schedules under their control. Others within TADLP will be allowed to view the schedules.

A calendar system to allow the DTFM to recognize and resolve classroom schedule conflicts.

NOTE

DTF must be a Block Two site (since Block One sites have no network). Each DTFM at the site will need to accomplish these procedures under their own Windows NT Network Login. This training manual and the TAC Help Desk will provide instructions and assistance with Outlook account set up.

Setting Up Outlook

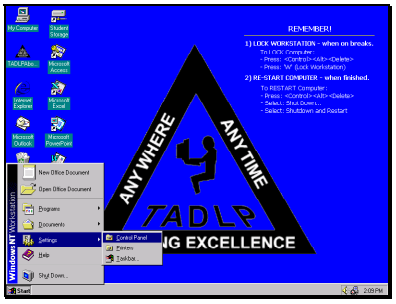


FIGURE II.1

1) Position the cursor on the start button in the bottom left corner of the desktop and left-click mouse button one time. *(see figure II.1)* Select settings on the start menu. Then select "Control Panel" and left-click once.

FIGURE II.2

2) Position the cursor over the “Mail Icon” in the control panel window and double-click the left mouse button. *(see figure II.2)*

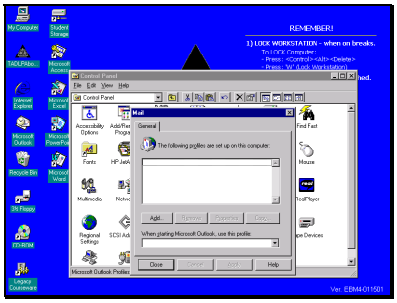


FIGURE II.3

3) When the “Mail Window” opens it should be blank. *(see figure II.3)* Position the cursor over the “Add” button and left click the mouse button one time

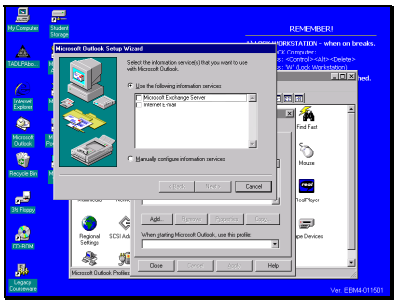


FIGURE II.4

4) The Microsoft outlook setup wizard window will open. *(see figure II.4)*

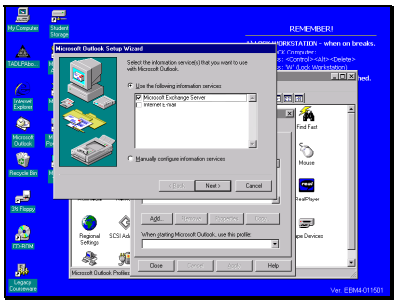


FIGURE II.5

5) Place the cursor over block in front of “Microsoft Exchange Server” and left-click the mouse button once to put a check mark in the block. *(see figure II.5)* “Microsoft Mail and Internet Mail” should remain unchecked. Position cursor over the next button and left-click the mouse button once.

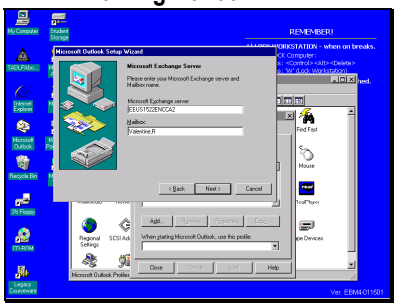


FIGURE II.6

6) The next setup window will appear; you will be entering the server name and your name. *(see figure II.6)* The server name to be used is EEUS1522ENCCA2

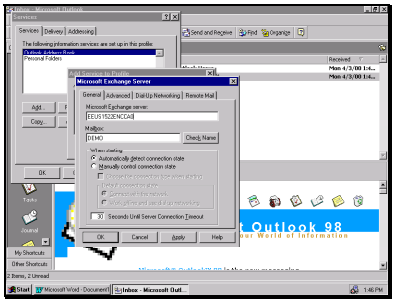


FIGURE II.7

7) You may get a screen like the one depicted in *figure II.7*. If you do, just click on the "check name" box and wait for the system to underline your name, then click on the "apply" button and then the "OK" button.

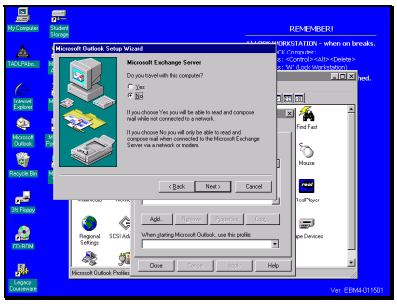


FIGURE II.8

8) The next setup window asks, "Do you travel with this computer". *(see figure II.8)* Select "No" and press "next" to continue.

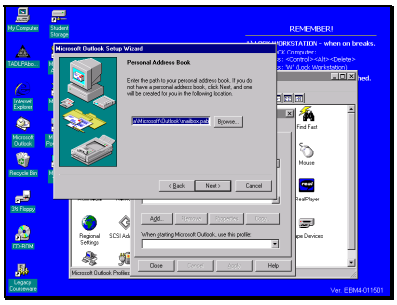


FIGURE II.9

9) Use the default unless you have a shared network drive you may wish to keep your address book on. If so, then browse to the location. *(see figure II.9*) When done press "Next" to continue.

FIGURE II.10

10) *(This next step may change at a later date)* Accept the default of not auto-starting Outlook when you login. *(see figure II.10)* Select next to continue.

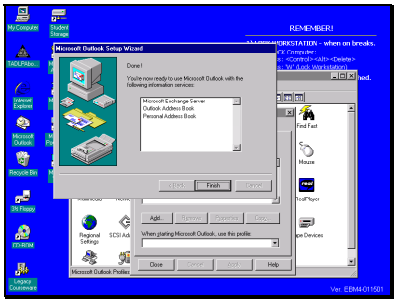


FIGURE II.11

11) The last profile creation screen will open letting you know you are ready to start using Outlook; press the finish button to continue. *(see figure II.11)*

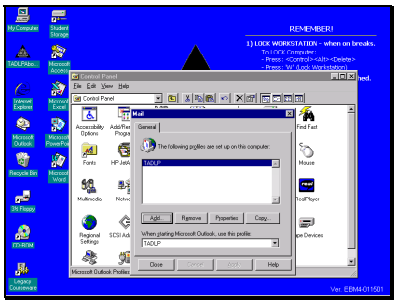


FIGURE II.12

12) Press the close button to exit the "Mail" window and go to the control panel. *(see figure II.12)*

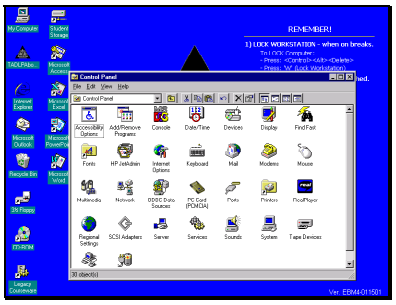


FIGURE II.13

13) Press the "X" in the upper right corner of this window to exit the "control panel" and close the window. *(see figure II.13)*

14) Once you have setup Outlook, you must run "Legacy" from the icon and logoff then login as a DTFMGR and run "Legacy" again and "Push the Image" up to the server so your profile will be on the workstation when the image is copied over that night.

Using Outlook

Once your Outlook account is setup you can start using the “email” system.

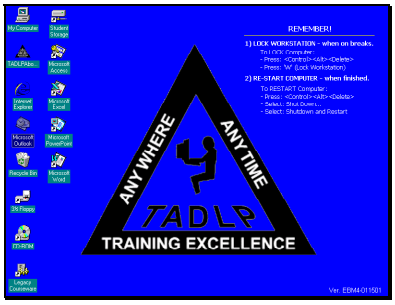


FIGURE II.14

1) From the desktop, double-click the “Microsoft Outlook Icon” *(see figure II.14)* or go to “Start, Programs and Microsoft Outlook.” *(see figure II.15)* and click once

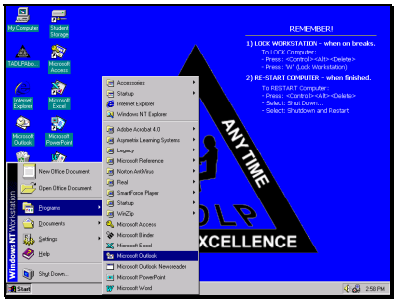


FIGURE II.15

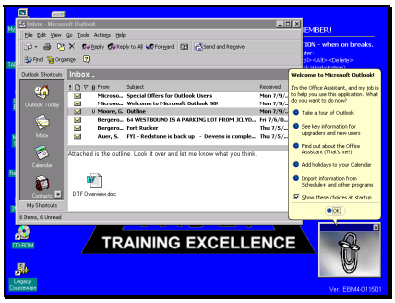


FIGURE II.16

2) After the program automatically creates shortcuts for your folders, it should open up to your “inbox” you may have two messages from outlook you can read them or delete them. If you are unsure how to use the outlook program, “take the tour of outlook.” To keep the screen above the “office assistant” from reappearing every time you login uncheck the “show these choices at startup” box and click on “OK”. *(see figure II.16)*

MESSAGING

1) Once you have pushed the image up you should end up with a screen similar to the screen above. *(see figure II.16)* This is your messaging screen. Use standard email processes for sending and receiving messages**. You cannot send or receive messages from outside TADLP from this system.**

2) To view your messages, just left click once on the message to view it in the lower half of the screen. To view the entire message, double-click on the message in your upper screen.

3) Once you have viewed the message, you can reply, reply to all recipients, forward the message, or delete it by using the icons on the tool bar at the top of the screen.

4) To send a message, left-click the icon under the "File" Button in the upper left corner of the screen, the icon is a letter and envelope. You will get a new window to use for your message. To select the recipient of the message left-click the "To" button. Then select the name or group to whom you wish to send the message (from the global address list). Use HELPDESK for any TAC Help Desk related issues and SECURITY for any security issues.

5) Key in your message and then left-click on the send button to send it.

SCHEDULING USING OUTLOOK CALENDAR

1) Click on the "Inbox" button at the top left of the email window to open the tree that lists all the items mapped in Outlook.

2) Click on the "+" in front of public folders.

3) Click on the "+" in front of all public folders.

4) Then pick the folder you want.

5) If you want to view the calendar of one of the other DTF sites go down to "+" symbol in front of the folder click on it and then click on the classroom.

LESSON III: USING ARWEB

TASK: Using ARWeb

CONDITION: DTFMs will follow the procedures for logging onto the ARWeb web-site, registering students, submitting the utilization reports and opening trouble tickets.

STANDARD: DTFMs will log on to the ARWeb site, submit the required information for registering students, and report classroom utilization. They will also submit trouble tickets in a timely manner.

NOTE:

Utilization reports are required daily even if there are no classes scheduled.

Logging into ARWeb

Only Block 2 sites have the capability to access ARWeb.

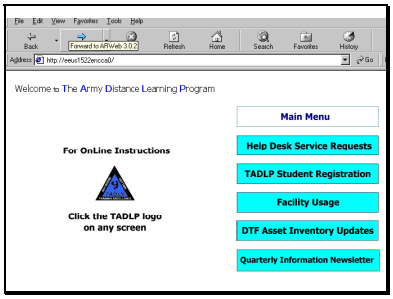


FIGURE III.1

1) The site address is http://EEUS1522ENCCA0
   - **NOTE**: WWW is not required. .
2) The Main Menu screen is displayed. *(see figure III.1)*

   Options:
   - Help Desk Service Request
   - TADLP Student Registration
   - Facility Usage
   - DTF Asset Inventory Updates
   - Quarterly Information Newsletter
3) Click on the option you wish to select.
4) The login screen is displayed on all options except for the Newsletter. *(see figure III.2)* You must put the cursor in the "user" block of the login screen. Enter your user ID (I.G.: JRAC1234), in upper case and a password only if you were assigned one by the TAC Help Desk. Click on the login button.

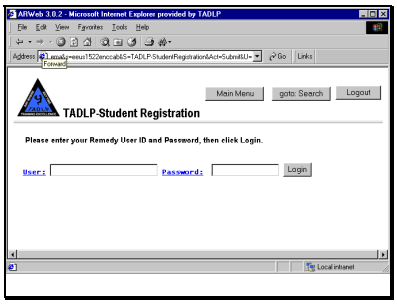


FIGURE III.2

NOTE:

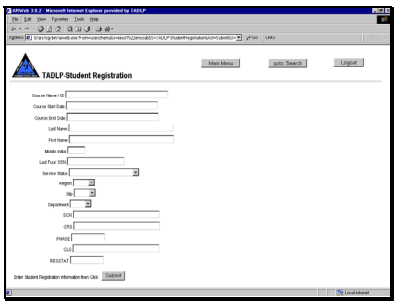
Only use a password if you were assigned one by the TAC Help Desk.

Help Desk Service Request

Refer to Lesson VIII *(page 38)* for more information and instructions on this option.

TADLP Student Registration

Fill in student registration information from the SF-101 form on this screen, using the items below. *(see figure III.3)*



1) Course Name/ID
2) Start and Ending Date (**required**)
3) Name (last, first, MI)
4) Last four digits of the SSN (**only the last four**)
5) Service status. (I.E. Mil. DA Civ., Contractor.)
6) Region (1,2,3, or 4)
7) Site
8) Department (DL1, DL2 or DL3)
9) Click on "Submit" when finished

FIGURE III.3

Utilization Reports

Click on the Facility Usage button. *(see figure III.4)* Fill in all available information on this screen.

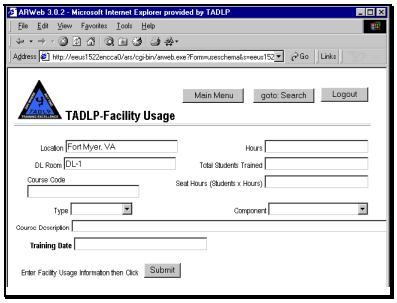


FIGURE III.4

1) Location
2) DL room
3) Course code, if applicable
4) Type (I.E. VTT, IMI, CBT)
5) Hours
6) Total students trained
7) Seat hours (# of students x total hours trained)
8) Component (Army Reserve, Active Army, Navy, etc.)
9) Course description
10) Training date
11) Click on "Submit" when finished

NOTE:

Entries can be modified in the event of a mistake or a double submission by clicking on the "goto: Search" button and specifying search criteria.

DTF Asset Inventory Updates

If you receive replacement equipment or parts, use this function to update your site's inventory of serial and part numbers.

Quarterly Information Newsletter

The most recent edition of the DTFM Newsletter can be found at this location.

LESSON IV: NETWORKED COURSES

Resident, IMI, SmartForce and VTT

TASK: Check students in for Networked Courses.

CONDITION: DTFMs will follow the procedures for registering students, in-processing them into the DTF, and assisting them when required.

STANDARD: DTFMs will submit the required information to register student(s), and act as the classroom facilitator. DTFMs will also monitor the classroom equipment and correct problems in a timely manner per the guidelines for daily operation of the DTF.

CT-100 Class Log OR CT-102 SmartForce Log OR CT-103 Walk-in Log
One copy each: All Contents of Block 2 Security Folder (DTFM-CD)SF-100 Security Statement
SF-101 Student Registration Form

1) Verify Student eligibility:

- Request the students military or Department of the Army Civilian (DAC) Identification Card.
- Request the student's orders, if available.
- Ensure the courseware the student will be utilizing is TADLP approved.

2) Register Students:

- Copy the student's orders if available.
- Seat the student at a workstation.
- Ask students to complete a Student Registration form (SF-101), if not previously submitted. Please attempt to have account requests completed at least 24 hours prior to the commencement of class. Submit the completed account request via ARWeb or by faxing forms to the TAC Help Desk. Perform this step only if computers will be used during the training session.
- Have the student complete a class attendance form. (CT-100 OR CT-101 OR CT-103)

3) Brief Students:

- Welcome students to the TADLP classroom and advise them regarding your responsibilities.
- Inform students of building facilities and classroom procedures.
- Brief the users on the INFOSEC Brief/Army Privacy Act program.
- Have students complete the TADLP INFOSEC Security Statement (SF-100)

4) Student Log on:

- Give the student his or her UserID and generic password as generated by the TAC Help Desk.
- Inform the student that the new password must be at least 8 characters in length and that at least one character must be either upper case or a numeral.
- Instruct the student in the procedure for locking the workstation during breaks. This is done by pressing the "Ctrl-Alt-Delete" keys simultaneously, then pressing the "W" key or clicking the "lock workstation" button once.
- Next, explain the proper shutdown procedure: Pressing "Ctrl-Alt-Delete", moving the cursor over the "shut down" button and left-clicking once on "Shut Down". The student should then place the cursor over "Shutdown and Restart" and left-click in the circle for "Shutdown and Restart." Finally, the user should move the cursor over the "OK" button and left-click once. This will be done when the student leaves for the day unless previous arrangements for multi-day usage have already been made. For instructions on how to make arrangements for multi-day usage, please consult the *Multi-Day Course Procedure* section of Lesson VII.

5) Assist Student:

Resident Courses:

- Inform students that the computers are to remain on with the monitors turned off if workstations are not required for their training session. If they suspect that something may be wrong with the computer they should notify the DTFM and not take any action to correct the problem.
- The push-to-talk microphones on the desks are used for VTT sessions only and should not be used during the training session unless required.
- Act as a facilitator to assist the students and instructor as required. Operate the VTT equipment on behalf of the instructor.

Options

IMI Courses:

- Refer to section 4.3 of the Computer Operation Manual.
- Follow courseware load instructions provided with the CD.

SmartForce Courseware

- At the Desktop, the student should double-click with the left mouse button on the Internet Explorer icon.
- On the address line of the "Welcome to the Army Portal " browser window the user should type www.armycbt.army.mil and depress the Enter key.
- Next, the student should click on "New Registration" or "Registered Students" (as applicable) and follow the on-screen login and access procedures for utilizing SmartForce courseware.

VTT Courses:

- Notify students about the start and completion times of the training session.
- Brief students on use of push-to-talk microphones and related camera functions.
- Assist students as needed. (e.g. faxing information, recording VTT sessions, providing required course material to students, etc.)
- Monitor VTEL equipment for proper operation during the VTT. Call NCC to correct operational problems as required. If you encounter transmission difficulties, NCC will join in to the conference, monitor the system, and attempt to correct the problem.

6) After Training:

- Check that the student workstation is operational, that all components are present and that the area is neat and orderly.
- Ensure that all materials and documents to be retained in the DTF are returned.
- Perform any preventative maintenance to prepare the system for the next student.
- Ensure that the student logs off the computer properly. At this time you may inform the students that they may leave.
- Determine if the machine has a clean image. If not, manually re-image the computer.
- Report any damaged or missing items to the student's commander, the TAC Help Desk, and the PMO RMD.
- If this is the last class in the DTF for the day, secure the DTF and initial the Standard Form 701.

NOTE:

INFOSEC Brief is **ONLY** required if computers are used for the course.

LESSON V: TADLP WORKSTATION USAGE

TASK: Usage of the workstation by a DTFM and student/user.

CONDITION: DTFM will instruct the student how to log on using the UserID and password, assist the student in the proper procedures for changing the password, and the loading of software on the computer used for his/her training. The DTFM will also walk the student through the steps for locking the workstation during breaks and or lunch. In addition, managers will instruct the student in the proper procedures for shutting down and restarting the computer at the end of the day.

STANDARD: DTFM will perform the items covered in this training per the guidelines for daily operation of the DTF.

1) Requesting UserID & Password:

- Submitted through the use of ARWeb or by faxing the student registration form to the TAC Help Desk.

2) Logging on to the Computer:

- Instruct the student to turn on the monitor.
- The user should press the “CTRL, ALT, DELETE” keys simultaneously.
- Have student read DOD acceptance script and select “OK”.
- Once the log on screen appears ask student to type in his or her “UserID.” This is not case sensitive; upper or lower case letters/numbers may be used.
- The user should then press the “Tab” key to move the cursor to the password field.
- The password received from the TAC Help Desk is the “UserID” in reverse; it must be typed using only capitals.
- Once the password is entered, the student should press “Tab” again to advance to the “Domain” field and check that the correct domain name appears.
- The student can then press the “Enter” key or move the cursor over the “OK” button and left-click the mouse button one time.
- The window to change the password will open.
- Passwords should be eight (8) characters minimum, and no longer than fourteen (14) characters. At least one character must be a capital letter and/or a numeral.
- Once the window to change the password opens, instruct the student to place the cursor in the field labeled “New Password”.
- Have the user type in his or her new password; making sure it meets the requirements stated above.
- Press the tab key to move the cursor to the “Confirm New Password” field and ask the student to reenter the new password again. This will ensure that the password has been changed successfully.
- A window informing the user the password has been changed will open if all the information was entered correctly. The system will then log the student onto the network.

3) Loading of courseware on computers:

- The DTFM will ensure that the courseware is authorized by checking the list of approved courseware for TADLP use in the DTF. The DTFM can contact the courseware-testing center with questions regarding acceptable software.
- The DTFM will also assist the student with loading the courseware if the student requires help. Courseware will be loaded to the "D" drive only.

4) Locking the Workstation

- If a student needs to leave his or her workstation unattended for any reason the workstation must be left in the "locked" state.
- In order to lock the workstation, the student should save his or her work, and then press the "Ctrl, Alt, Delete" keys simultaneously. The "Windows NT Security" dialog box will open.
- The user should press the "W" key on the keyboard or position the pointer over the button for "Lock Workstation," and left-click the mouse button once.

5) Unlocking the Workstation

- When the student returns after his or her break the workstation can be unlocked by pressing the "Ctrl, Alt, Delete" keys simultaneously, typing in the password and pressing the "Enter" key or moving the cursor over the "OK" button and left-clicking the mouse button one time.

NOTE:

Student Registration is covered in the *Lesson III: Using ARWeb*

Courseware developers for TADLP are permitted to test courseware in any DTF. Developers are issued Student IDs and passwords. However, they are not permitted to make any configuration changes to the image. Courseware cannot be used by students until approved by the TADLP Testing Branch.

LESSON VI: DATA STORAGE

TASK: Saving items to the "SHARED" Drive

CONDITION: DTFM will follow the procedures as outlined in the following training and assist the student in saving the items or documents he or she is using.

STANDARD: DTFM will perform the items covered in the training per the guidelines for daily operation of the DTF.

Saving to the Shared Drive:

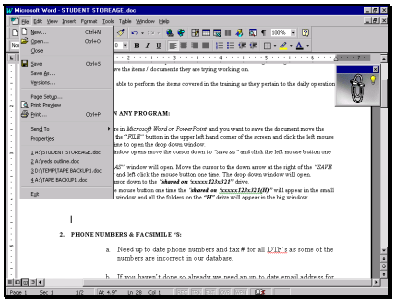


FIGURE VI.1

1) When the student wishes to save his or her progress, he or she should move the cursor up to the "FILE" button *(see figure VI.1)* in the upper left hand corner of the screen and left-click to open the drop down menu.
2) When the window opens, the user should move the cursor down to "Save As" *(see figure VI.2)* and left-click once.
3) The "Save As" dialog box will open. *(see figure VI.3)*

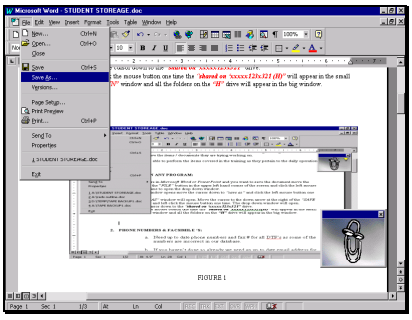


FIGURE VI.2

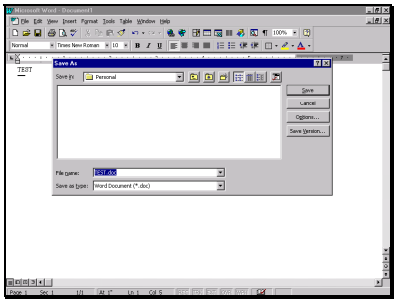


FIGURE VI.3

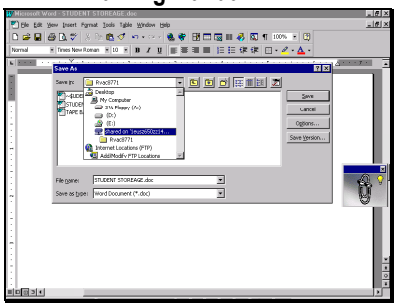


FIGURE VI.4

4) The student will move the cursor to the down arrow at the right of the "Save in:" window *(see figure VI.4)* and left-click the mouse button one time. The drop down menu will open.

5) Instruct the user to move the cursor down to the "Shared on 'xxxxx123x321" drive.

6) Next, the student should left-click the mouse button once. The entry "shared on 'xxxxx123x321 (H)" will appear in the small "Save in:" field and all the folders on the "H" drive will appear in the large open section of the dialog box. *(See figure VI.5.)*

Locating your Student Folder

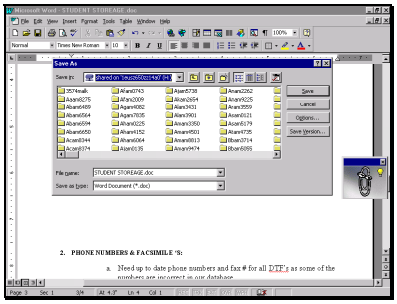


FIGURE VI.5

7) Once all of the folders appear in the window of the "Save as:" dialog box, the student should move the cursor to the slide bar at the bottom of the window and then left-click on the right arrow to locate the appropriate folder. The student folder name is the same as the UserID. *(see figure VI.5)*

Opening your Folder

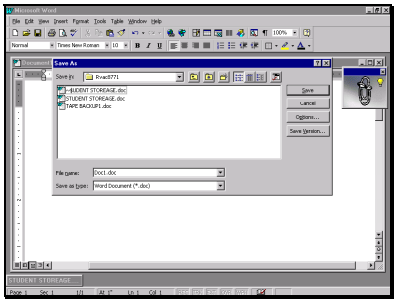


FIGURE VI.6

8) The user should find his or her folder in the list, move the cursor over the icon, and double-click the left mouse button.

9) The folder name will appear in the small "Save in:" window. *(see figure VI.6)*

10) Instruct the student to move the cursor to the "Save" button and left-click once.

11) Once the system is finished saving the document it will appear in the large window in the "Save in:" window.

NOTE:

When the TAC Help Desk creates a student UserID and password, a temporary storage folder is also created. This folder will be deleted 2 weeks after the student completes the current course.

LESSON VII: PROCEDURES FOR IMAGING COMPUTERS

TASK: Normal student workstation imaging.

CONDITION: DTFM/students will image the workstations by following the instructions on the desktop listed as step 2 for restarting the computer.

STANDARD: The DTFM will watch the all the workstations re-image at the end of the workday.

Normal Imaging of Workstations

Imaging the workstations will be done at the end of the day by the DTFM.

The student will perform the re-image function at the end of the class following the instructions in the upper right hand corner of the desktop.

Problems Imaging Workstations

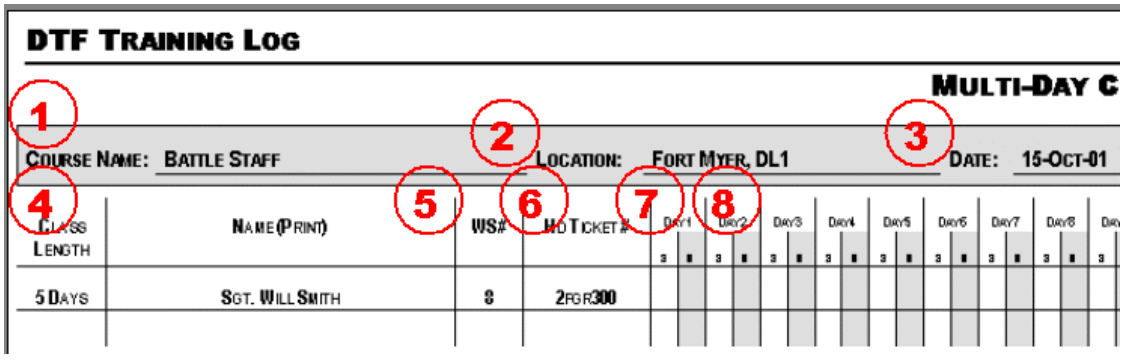
The DTFM will contact the TAC Help Desk to open a trouble ticket if any workstation fails to re-image normally.

Corrupt Workstation Images

In the event a student workstation image becomes corrupt, the DTFM should not attempt to load a new image without Help Desk assistance. This includes loading from any disk or CD, loading any archived image, or any image from another workstation.

Multi-Day Course Procedure

According to the newest release of the SOP, DTFMs have the option to skip re-imaging student workstations each day when training includes a multi-day course in which the student will be using the same programs. Please read the *Business Case for Relief of Object Reuse (re-image) Requirement*, released by the PEO STAMUS for a full understanding of the policies regarding this process. According to this document, the DTFM is required to keep an additional log (*CF-104 Multi-Class Log.doc*) on file for this specific situation. This instruction guide is intended to facilitate the gathering and maintenance of pertinent information.



NOTE

DTFM is to complete ALL gray areas of form.

① **Course Name**	Be sure to include the name of the course on the top of the form. Every student registered for this course, starting on that date should be included on this. If more than one page is needed for one class or if the class runs longer than 10 days, please staple all logs together.
② **Location**	Please include not only the site location but also the DL classroom (i.e. DL1, DL2, DL3)
③ **Date**	This should be the **START** date of the computer usage
④ **Class Length**	According to the directive, one computer cannot be in use without being re-imaged for longer than 10 days. This space allows the DTFM to indicate how long the student will be occupying the workstation. If the student will be there for longer than 10 days, only place a "10" in the space. After the 10th day, the workstation **must** be re-imaged, and a new log will start.
⑤ **WS# (Workstation #)**	The student will **ONLY** use the workstation indicated. This information is important to give to the Help Desk when opening the ticket, and will allow the systems administrators to track the viral update signatures.
⑥ **HD (Help Desk) Ticket #**	Once a workstation has been assigned, the DTFM must call the Help Desk and open a trouble ticket. Identify each workstation and the length of time it will be occupied (up to 10 days). Record the Help Desk Trouble Ticket number in this space. If the class is longer than 10 days, once the machine has been re-imaged and the new line in the log started, you must close one ticket and open another
⑦ **S**	In this space please have the student **INITIAL EACH MORNING** when he/she arrives at the appropriate workstation to indicate that nothing has been changed since the evening before.
⑧ **M**	In this space, DTFMs **MUST** initial at the **END OF EACH DAY**, once they have done a visual inspection to ensure that the computer has been **LOCKED** for the evening, **NOT** logged out.

NOTE

All workstations have to be re-imaged everyday before leaving. **DO NOT** push a student image up to the server without prior consent from the TAC Help Desk.

Using the Pullman Utility

To simplify mandatory daily re-imaging of student workstations, the DTFM may log into the manager's workstation using the administrator user name and password and employ the Pullman Utility. This program allows the DTFM to pull images from the server for the entire site, individual classrooms, or for a specific workstation.

To use this utility, double click the "Pullman" icon. A MS-DOS window will appear offering four options: (A) Entire Site; (B) Entire Classroom; (C) Individual Workstation; or (D) Quit. Currently, the only working option is (C) Individual Workstation. Type "C" and at the prompt enter the host name of the machine (e.g. 1MYRZ404ZZZ1W4) you wish to re-image. When it asks if the name is correct, choose Y(es) or N(o). If your response is Y(es), a clean image will be pulled from the server.

LESSON VIII: TAC HELP DESK

TASK: Understand TAC Help Desk Structure

CONDITION: The DTFM will become familiar with the responsibilities and processes of the Training Access Center Help Desk.

STANDARD: DTFMs will acquire total understanding of help desk structure and function.

Purpose:

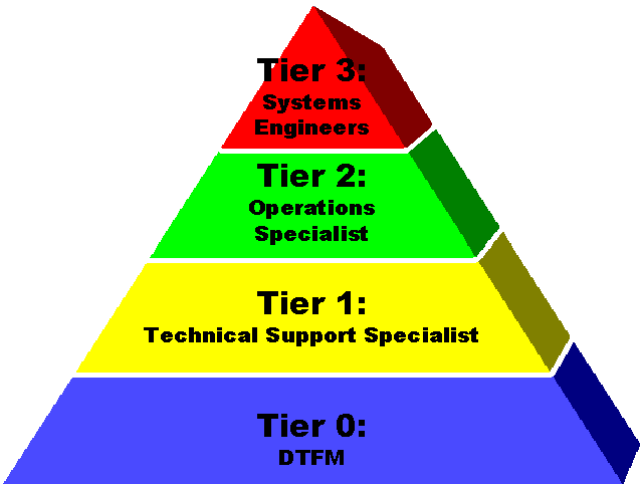
The TAC Help Desk is the central contact point for information technology support at the Training Access Center. It is also the portal through which the DTFMs submit problem reports, and request student access to the network (UserIDs and passwords). DTFMs submit trouble reports to the TAC Help Desk at either the Tier 1 or Tier 2 level. The Tier 1 Help Desk Specialist will evaluate the problem and provide a solution or escalate the problem to a Tier 2 Specialist or vendor for resolution. The Tier 2 Specialist can, in turn, escalate issues to the Tier 3 level for resolution. DTFMs are only authorized to call the TAC Help Desk and speak with Tier 1 or 2 Specialists. The only exception to this directive would be to return the call of a Tier 3 engineer as requested.

TAC Help Desk Site Information:

Mailing/Shipping	TAC	Help Desk Phone	Toll Free	(877) 251-0730
Address:	Building 1522, TAC		COM	(757) 878-4745
	PO Box "O"		DSN	927-4745
	11th Street	Help Desk Fax	COM	(757) 878-0440
	Fort Eustis, VA 23604		DSN	927-0440

Organizational Structure:

The TAC Help Desk is structured in Tier levels.



1. **Tier 0: DTFM** — The DTFM is the first point of contact and is responsible for basic troubleshooting of hardware and software problems. The DTFM must report problems to the TAC Help Desk Support Specialist if he or she is unable to resolve a problem within a reasonable timeframe.
2. **Tier 1: Technical Support Specialist** — TAC Help Desk Support Specialists handle initial calls and assist in troubleshooting problems, student registrations, and Tivoli tickets. The Tier 1 Support Specialist escalates issues or problems that require a greater level of expertise for resolution. Tier 1 can also pass problem tickets on to external vendors, e.g. TPW, EVEREX, and NCC.
3. **Tier 2: Operations Specialist** — Operations Specialists are lead level technicians assist the Tier 0 or Tier1 personnel with troubleshooting and problem solving. They also handle high-level network management and monitoring. These individuals are the gateway to Tier 3 because only Tier 2 Operations Specialists can forward a problem to Tier 3 for resolution.
4. **Tier 3: System Engineers** — Individuals rated as Tier 3 work for the System Engineering group. They handle all high-level infrastructure issues and are charged with making sure the system meets current design criteria. Due to the nature of the System Engineer's responsibilities and project requirements, direct calls to these engineers are prohibited unless the DTFM is instructed to do so.

Reporting Problems/Opening Tickets:

The preferred method of reporting problems to the TAC Help Desk is via phone or facsimile. This will allow the TAC Help Desk Specialist to obtain all the necessary information for the trouble ticket.

If facsimile is used, a phone number for the DTF must be included and the DTFM at the site must be available to receive phone calls to provide further information not included in the fax transmission.

ARWeb is capable of accepting trouble tickets created by the DTFM. This method should only be utilized for problems that do not affect a student or class and that do not require an immediate response.

All VTT problem tickets must be reported to the Network Control Center (NCC). The TAC Help Desk is not authorized to provide support for VTT equipment or software. However, the TAC Help Desk should be kept informed of all changes to the status of a NCC trouble ticket.

All trouble tickets reported to the TAC Help Desk will also be recorded on the trouble ticket log maintained for each DTF.

Help Desk Service Request via ARWeb

NOTE:

ARWeb should never be used to submit Service Requests unless the DTF phone lines are unavailable or unless the request's importance is considered "non-priority"(does not affect students or classes).

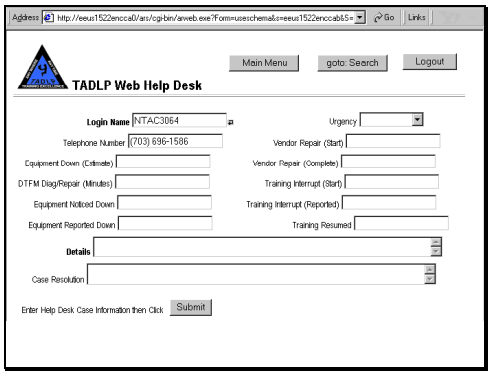


FIGURE VIII.1

1. **Login Name** — The Enterprise BDC maintains a READ ONLY copy of the security database for the purpose of validating user accounts and login account control for that location. This field is auto generated by the system. The login name for the DTFM will be displayed. *(see figure III.5)*
2. **Telephone Number** — Type the contact telephone number. This field will default to the phone number listed in Remedy for your site; however, if you wish to get a call back at a different phone number, update this field.
3. **Equipment Down (Estimate)** — Type the estimated date and time that the equipment (i.e. workstation, VTT, server, switch) went down or problem occurred. The format is DD-Month-YR HR:MN AM./PM, example 29-March-00 7:00 AM.
4. **DTFM Diagnosis/Repair Minutes** — Type the amount of time the DTFM spent working on the problem. The format of this field is in total minutes
5. **Equipment Notice Down** — Type the date and time the equipment was down. This field should not be equal to the Equipment Down (Estimate) field. This field is the exact time the down condition was noted. The format is DD-Month-YR HR:MN AM./PM, example 29-March-00 7:00 AM
6. **Equipment Report Down** — Type the date and time the equipment was reported down. This is the time that an individual reported the equipment was down. The format is DD-Month-YR HR:MN AM./PM, example 29-March-00 7:00 AM.
7. **Urgency** — Select the appropriate urgency level for the ticket. Urgency is defined in the Help Desk Operation Guide as:
   URGENT – Multiple Classrooms down or affected.
   EMERGENCY – Single Classroom down or affected.
   ROUTINE – Single user down or affected.
   ENHANCEMENT – Requesting a change to a system, process, or equipment.
   LOW – as required
   INFORMATIONAL – as required.
8. **Vendor Repair (start)** — Type the date and time the vendor (e.g. VTEL, SPRINT, TPW, and GTSI) started the repair. The format is DD-Month-YR HR:MN AM./PM, example 29-March-00 7:00 AM.

9. Vendor Repair (complete)	Type the date and time the vendor (e.g. VTEL, SPRINT, TPW, and GTSI) completed the repair. The format is DD-Month-YR HR:MN AM./PM, example 29-March-00 7:00 AM.
10. Training Interrupt (start)	Type the date and time training was interrupted. Only enter this field if training was interrupted. The format is DD-Month-YR HR:MN AM./PM, example 29-March-00 7:00 AM.
11. Training Interrupt (reported)	Type the date and time training was reported as "interrupted." This is the time at which a student or other non-DTFM personnel reported the training as interrupted. The format is DD-Month-YR HR:MN AM./PM, example 29-March-00 7:00 AM.
12. Training Resumed	Type the date and time the training in the classroom resumed. The format is DD-Month-YR HR:MN AM./PM, example 29-March-00 7:00 AM.
13. Details	Type all available information about this ticket. Relevant information should include the hardware affected (workstation #12), the component affected (i.e., hard drive, monitor, camera, microphone), the serial numbers or model numbers, the location (DL1, DL2, DL3), and the course, class, or group.
14. Case Resolution	This field should only be updated when the problem is resolved by the DTFM. The DTFM should report the action taken to resolve the problem.

LESSON IX: COMPUTER COMPONENT REPLACEMENT

TASK: Replacing Computer Components.

CONDITION: DTFMs will be able to follow the procedures for replacing computer components.

STANDARD: DTFMs will be able to complete the replacing of computer component and return the computer to normal operation.

NOTE:

When replacing any components for workstations, servers, or VTT equipment, you must notify Bob Williamson and the Help Desk of both the new and old serial and/or part numbers.

Also, some replacement components will require you to load updated drivers for the hardware. Contact the help Desk for guidance. If they agree to allow you to load the new drivers, install the software, run legacy, restart the workstation, and test the new hardware. Notify the Help Desk of the results and they will assist you with pushing the updated image onto the server.

Accessing Internal Components in your Workstations

✓ Phillips Screwdriver

1) Before shutting down any **TPW (computers)** Workstations, call the TAC Help Desk and tell them you are shutting down Workstation XXX. For the sites who have Everex computers, please follow your designated protocol.

2) To open the chassis to service or replace components, you will need to SHUTDOWN the computer. When the computer says ready to restart you can power off the workstation by pressing the power button just once.

3) Remove all cables and connectors at the rear of the computer:

- ① To remove the Power Cable, keyboard, mouse, video, network cable pull them straight out. If the headphones are installed, remove them as well.
- ② Slide the chassis out of the cubbyhole and stand it up on the desktop, do not lay it down on its side. Be sure that the front 2 to 3 inches of the computer hang over the edge of the desk.

4) Removing the face of the computer:

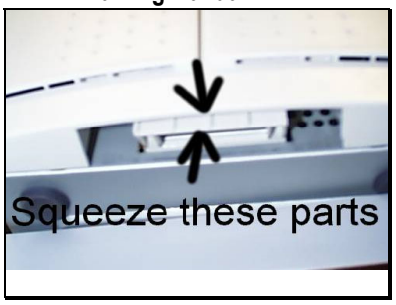


FIGURE IX.1

5) At the bottom of the face of the computer (plastic front cover) there is a hole large enough to grasp with two fingers.

6) Squeeze the plastic piece inside and the outside face of the plastic front cover and this will release the catch inside *(see Figure IX.1)*. Pull the cover outward and then up about 3 to 4 inch's. The face is hinged at the top, and as it swings out you will need to push the top down about a quarter of an inch, so you do not snap the plastic hinges. Once off, set the front cover off to one side, inside face up, and use it to hold all screws and parts that you remove from the computer.

Removing the LEFT SIDE PANEL:

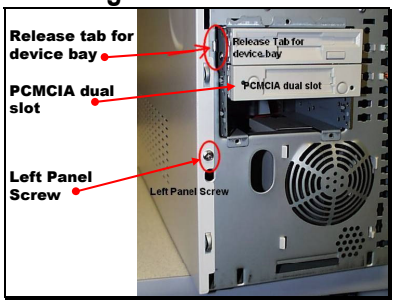


FIGURE IX.2

1) Facing the computer, on the left side about 4 inches up you will see a Phillips screw. *(see Figure IX.2)*

2) Remove it and place it in the front cover. Now grasp the side panel at the indentation and slide it forward about ½ inch or so and tilt the top away from body and lift it straight up. Set the cover off to the side, so as not to scratch or damage it.

Removing/Installing the CD-ROM Device:

- ✓ Phillips screwdriver
- ✓ Tweezers
- ✓ Colored Dry Erase Markers
- ✓ Anti-static bag

Familiarization:

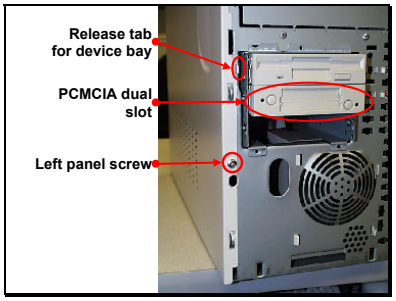


FIGURE IX.3

- **Power cable** to the CD-ROM drive has 4 wires that connect into a white plastic connector that is about 1 inch wide with tabs on either side.
- **Data Cable**, CD-ROM cable is a 2 inch wide flat ribbon cable (40 wire) with a stripe down one side of the cable. You should notice that the colored stripe on the ribbon cable is always closest to the power cable. The ribbon cable goes to the motherboard using a white connector similar to the power cable connector. **(DO NOT REMOVE ANY OF THE CABLES FROM THE ADAPTER CARDS OR FROM THE MOTHERBOARD).**
- **Sound Cable**; there is a 3-wire cable that connects the CD-ROM reader directly to the sound card. It is located when looking in the open side of the computer all the way to the far side of the CD-ROM. It goes in only one way (it has a small click lock tab on top, similar to one that you would find on a phone jack in your home).

1) First you will need to remove the Data Cable (ribbon cable) from the back of the CD-ROM not the motherboard. To remove the data cable grab the white connector and using a gentle side to side rocking motion pull straight out. You can damage the cable by pulling only on the cable.

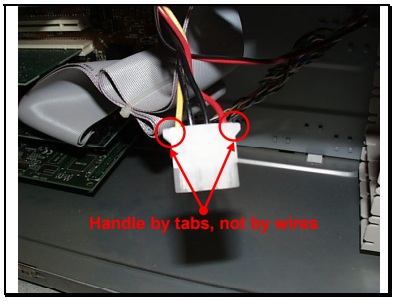


FIGURE IX.4

2) To remove the power cable grab the white connector and using a gentle side to side rocking motion pull straight out. Remember the power cables for the CD-ROM device has angles cut in 2 corners and can only go in one way when replacing it. It is usually very hard to remove. (**DO NOT PULL ON THE WIRES**). *(see Figure IX.4)*

3) Remove the sound cable by squeezing the tab at the top of the sound cable and pulling straight out.

Removing the CD-ROM Device:

4) When all the cables are removed from the back of the device, go to the front of the computer. On the sides of the CD-ROM there are 2 tabs sticking out. Squeeze them towards each other at the same time and slide the device out towards you.

5) When it is completely out of the chassis you will notice that attached to each side of the CD-ROM is a guide rail. Rails must go back in the same way they were removed. Installing the wrong screws in a device can cause damage to the device's electronic circuits and or cause a fire. Use your dry erase markers to mark the rails where the screw goes and mark the screws so that you put them on the new CD-ROM exactly the same way. (see figure IX.5)

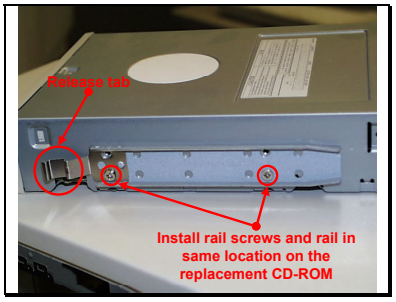


FIGURE IX.5

6) On the back of the CD-ROM Device there is a jumper, this is a small piece of black plastic that is covering two or more of the pins on the back of the device. The location of this jumper whether it is MASTER, SLAVE, or CSL is very important and must be noted. Putting the new CD-ROM in with the jumper set to the wrong setting (master, slave or csl) will cause the CD-ROM reader to be inoperable. To make sure that you get the jumper in the correct location, take a dry erase marker and mark the pins on the new device where the jumper should go and. Using your tweezers, remove the jumper from the old CD-ROM and place it in the correct location on the new unit. Now that the rails and the jumper have been transferred to the new device, put it in a Static Free bag (the bag the new drive came in).

NOTE:

Wait for the new device to come in and then take the rails off the old unit and install them on the new one. This way you will have a guide to its specific location. If you install the rails incorrectly, the front face (plastic cover) may not fit properly or the device will protrude out further than normal and could cause it to be damaged. Make sure that when you reinstall the front face, that the CD-ROM is flush with it.

Installing the CD-ROM Device:

7) Line up the rails in the top slot and push the new device back in until it clicks into place.

Reinstalling all the cables:

8) The best way to reinstall the cables to the new CD- ROM is in this order:

- Sound cable
- Data cable, remember that the colored stripe should be next to the power cable
- Power connector

Removing/Installing the Hard Drive, 3.5” Floppy Drive or PCMCIA dual card holder

- ✓ Phillips screwdriver
- ✓ Anti Static Bag
- ✓ Dry Erase Markers
- ✓ Plastic Re-Sealable bags

When you are required to remove the hard drive, the 3.5 floppy drive, or the PCMCIA dual cardholder, please follow steps one through four below. After you have completed those steps, refer to the section for each specific part for further instructions. Once the replacement component has been installed, the final steps for reassembly are identical and are listed at the end of this section.

Familiarization:

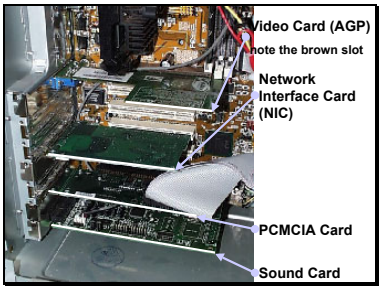


FIGURE IX.6

- The Hard Drive is in a removable bay that holds 3 pieces of equipment, the floppy drive or A drive, which is the top most device; the PCMCIA dual card holder or the middle device; and the Hard Drive which is the bottom most device.

- **Power cables** to the Hard Drive and PCMCIA dual card holder are the same type. They are bother 4 wires with a white plastic connector about 1 inch wide with grab tabs on the side. Note that they both have angles cut in 2 corners and can only be installed one way. You may also mark each one on the top with a dry erase marker. The Floppy drive has a smaller mini power connector it is about ½ inch wide, review the way it is installed and you will notice that the red cable on this connector is closest to the outside of the computer. You will need to mark the top of this connector to make sure that you reinstall it correctly. *(see Figure IX.7)*

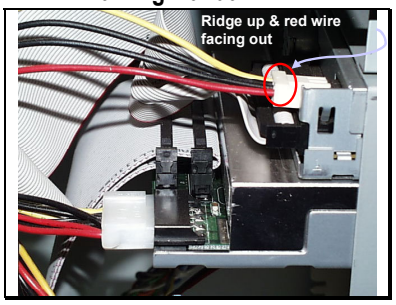


FIGURE IX.7

- ***Data Cable***s Hard Drive cable is a 2 inch wide flat ribbon cable (40 wire) with a stripe down one side of the cable this ribbon cable goes to the motherboard. **(DO NOT REMOVE ANY OF THE CABLES FROM THE ADAPTER CARDS OR FROM THE MOTHERBOARD).** You should notice that the colored stripe on the ribbon cable is always closest to the power cable.

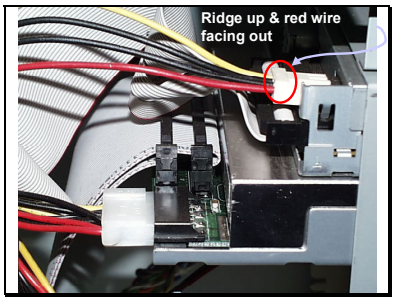


FIGURE IX.8

- There are also TWO, 3-inch ribbon (50 wire) cables attached to the PCMCIA dual card holder (middle device). One of these has a stripe down one side and the stripe will be closest to the power connector as well. Use your dry erase markers to mark on the cable front or back, so that you know which cable goes where.
- There is a 1.5 inch ribbon cable that goes to the **Floppy Drive** and it also has a stripe on one side of the cable, ***this stripe goes to the inside of the device only***. The ***photo of the floppy power connector*** shows the ribbon cable just below the white power connector. As you can see that edge of the ribbon cable does not have a colored edge to it like the previous photo.

Initial Steps for removing the Hard Drive, 3.5" Floppy Drive or the PCMCIA Card

1) First, you will need to remove the Data Cables (ribbon cables) from all of the devices in the bay (Floppy drive, PCMCIA and Hard Drive). Removing Data Cables, is best done by grabbing the hard plastic end closest to the device itself and pulling it straight out while gently rocking side to side. ***You can damage the cable by pulling on only the cable***.

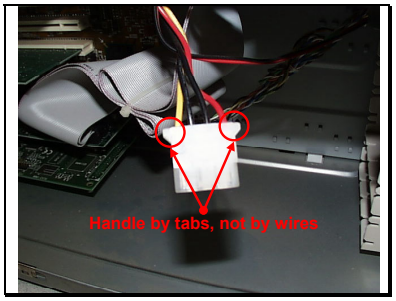


FIGURE IX.9

2) Next remove the Power cables from the PCMCIA device and the Hard Drive. This is best done the same way that you removed the power cable from the CD-ROM Drive, by rocking it side to side as you pull straight out. *It is usually very hard to remove*. There are plastic tabs on each side that make it easier to grab **(DO NOT PULL ON THE WIRES)**. *See Figure IX.9*

3) The Floppy drive power cable is a mini type connector and is removed by lifting just a little (lift about 1/8th of an inch or so) and pulling straight out**. DO NOT ROCK from side to side**. It should come out fairly easy.

4) Now that all the wires are removed from all the devices in the bay, you can remove the bay by going to the front of the computer and you will see to the right and left of the floppy drive (device bay) a small metal tongue sticking outward. Squeeze these tongues flush with the sides of the bay/floppy and then pull the entire bay forward.

Removing the Hard Drive:

1) At this point you will see that there are 4 screws (2 located on each side) that hold the Hard Drive to the bay chassis. Remove these 4 screws and place them in a re-sealable plastic bag marked as Hard Drive screws as **installing the wrong screws in a device can cause damage to the device's electronic circuits and or cause a fire**.
2) Before sliding the Hard Drive out of the bay, you will need to touch some part of the chassis of the computer body so as to discharge any static electricity that your body is holding**, DO THIS NOW**.
3) Slide the Hard Drive out the back of the bay, taking care not to touch any of the circuit board. Best to hold the Hard Drive only by its sides.
4) At the back of the Hard Drive, there is a jumper, the location of this jumper, you must note or mark the location of the jumper on the new Hard Drive. Putting the new Hard drive in with the jumper set to the wrong setting (master, slave or csl) will cause the hard drive to be inoperable. Take the new device out of its static free bag and immediately put the old Hard Drive in it.

Removing the PCMCIA dual card holder:

1) Like the Hard Drive, Remove these 4 screws and place them in a re-sealable plastic bag marked as PCMCIA Card Holder screws as **installing the wrong screws in a device can cause damage to the device's electronic circuits and or cause a fire**.
2) Discharge yourself by touching the chassis and then slide the device out towards the front.
3) Take the new device out of its static free bag and put the device you removed in the same bag. When installing the new device be sure that the face of the device is flush in the front with the Floppy Drive face (top device).

Removing the Floppy Drive:

1) The Floppy device has 4 screws holding it in place (two on each side). Be sure mark the location of the screws so that you can reinstall them correctly on the new device as **installing the wrong screws in a device can cause damage to the device's electronic circuits and or cause a fire**.
2) Discharge yourself by touching the chassis and then slide the floppy drive out towards the front.
3) Take the new device out of its static free bag and put the device you removed in the same bag. When installing the new device, be sure that the face of the device is flush in the front with the PCMCIA face (middle device).

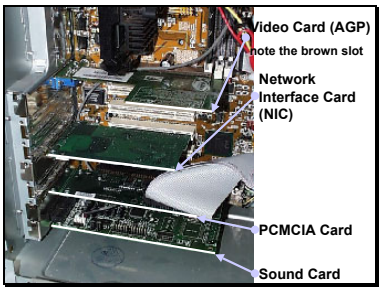
Reinstalling all the Cables:

1) It is best if you install all of your ribbon cables first, then install your power cables. Keep in mind where the colored stripes of the ribbon cables go. The hard drive and PCMCIA power cables have your marker and angles cut and fit in one way only. On the floppy power cable when attached look for your top mark or for the red cable to be closest to the outside of the computer.

Removing/Installing a Power Supply

✓ Phillips screwdriver

Familiarization

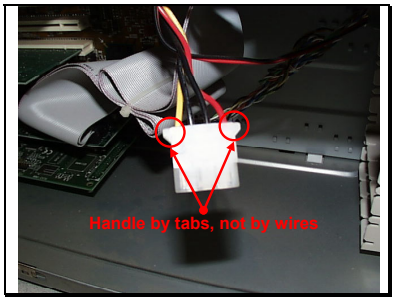


The locations of all power leads to their respective devices (CD-ROM, Hard Drive, 3.5" Floppy, and PCMCIA and the primary ATX connector on the motherboard).

FIGURE IX.10

Removing a Power Supply

Remove all of the power connectors



1) If need be label them with some scotch tape so you put them back were they belong, since many of them have been tie wrapped (you will need to put a power supply back into its original computer when you use it to see if another is bad).

FIGURE IX.11

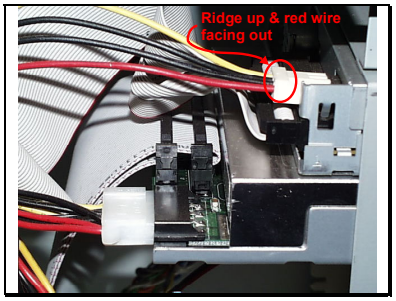


FIGURE IX.12

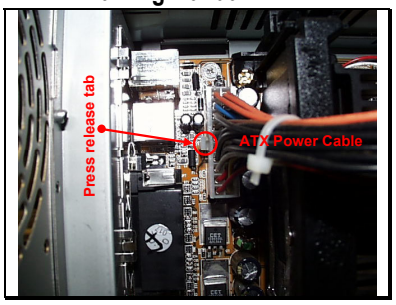


FIGURE IX.13

2) The ATX Power connector looks like an egg crate with lots of wires going into it on the mother board. It can be removed by squeezing the tab on it towards the wires and lifting straight up. If it is difficult to lift up then you have not squeezed the tab enough to release the catch that is holding the connector onto the motherboard.

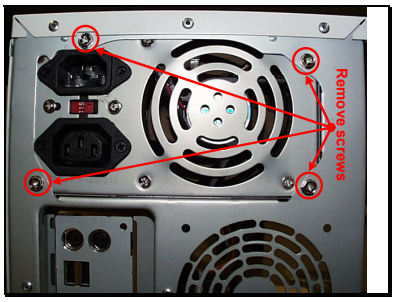


FIGURE IX.14

3) Looking at the back of the computer chassis you will see that there are 4 Phillips screws that hold the power supply to the chassis. One of the screws is just above the connector where your power cable goes into and the other 3 are at each of the outside corners.

4) Before you remove these 4 screws lay the computer down so that the open side is facing up. Remove the 4 screws and place in a plastic re-sealable bag labeled Power supply screws.

5) From the back push the power supply forward (towards the front) about 2 inch's. This will clear the support tabs inside the chassis that support the power supply. Tilt the power supply towards the motherboard till it clears the lip area and remove it.

Installing a Power Supply:

1) Put the power supply in its location.

2) Install all 4 screws.

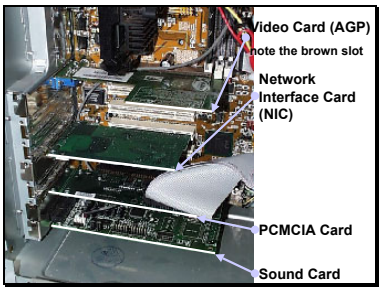
3) When replacing a power supply, be sure to attach all the cables to your devices and tie wrap them accordingly, you do not want any loose wires to come in contact with moving parts or parts that become hot. If you are not sure how to do this look at another machine and copy how they tie wrapped their wires.

4) Install the ATX connector last, it is designed to go in one way only. The Tab should be facing the back of the computer.

Removing/Installing a Network Interface Card (NIC)

- ✓ Phillips screwdriver
- ✓ Anti Static Bag

Familiarization



Before you remove the NIC card, note its location or slot.

FIGURE IX.15

Removing the NIC

1) Remove the Phillips Screw from the Tongue of the NIC card on the inside.
2) Discharge any static build-up you may have, by touching an unpainted surface of the chassis or a screw that is installed somewhere on the chassis.
3) Grasp the board by the tongue and the farthest edge from the tongue. Rock the board first toward the front of the computer and then toward the back just a little (just want to loosen it), rock it one more time towards the front then pull straight out towards you. Once the board is out, handle it by the tongue only, and put it into the Anti-Static bag.

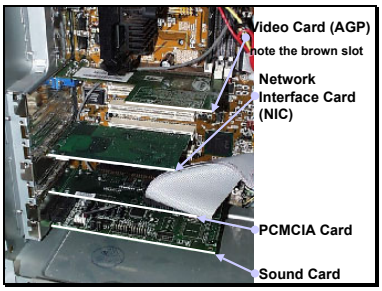
Installing the NIC

4) When installing the Network Interface Card, insert the tongue between the Motherboard and the chassis first, and be sure that the gold colored contacts are aligned over the slot that it fits in. Push the whole board in evenly and all the way down.
5) One way to verify that the board is properly seated is to check the tongue (is it flush were the screw goes).
6) Second, check to make sure that if you push at the end furthest from the tongue, does the board go down a little more, if it does push evenly again in the middle. One final check to make sure that it is completely seated and not tilted in some fashion.
7) Install the Screw on the tongue. Insure that it is tight.

Removing/Installing the Sound Card

- ✓ Phillips screwdriver
- ✓ Anti Static Bag

Familiarization

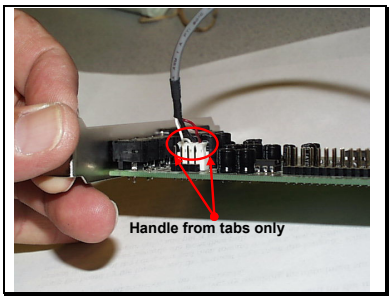


Before you remove the sound card, note its location or slot. The sound card should be the bottom most card in the computer.

FIGURE IX.16

Removing the Sound Card

1) Remove the CD-ROM audio cable (do not pull by the wires), grasp the top of the white connectors and gently pull up while rocking from side to side.



2) Once removed note the 2 raised lips on the cable side of the connector and the seat on the motherboard has a groove that both of those lips fit into.

FIGURE IX.17

3) Remove the Phillips Screw from the Tongue of the SOUND card on the inside.

4) Discharge any static build-up you may have, by touching an unpainted surface of the chassis or a screw that is installed somewhere on the chassis.

5) Grasp the board by the tongue and the farthest edge from the tongue. Rock the board first toward the front of the computer and then toward the back just a little (just want to loosen it), rock it one more time towards the front then pull straight out towards you. Once the board is out, handle it by the tongue only, and put it into the Anti-Static bag.

Installing the Sound Card:

6) When installing the Sound Card, insert the tongue between the Motherboard and the chassis first, and be sure that the gold colored contacts are aligned over the slot that it fits in. Push the whole board in evenly and all the way down. One way to verify that the board is properly seated is to check the tongue (is it flush were the screw goes). Second is to check to make sure that if you push at the end furthest from the tongue, does the board go down a little more (if it does push evenly again in the middle. One final check to make sure that it is completely seated and not tilted in some fashion.

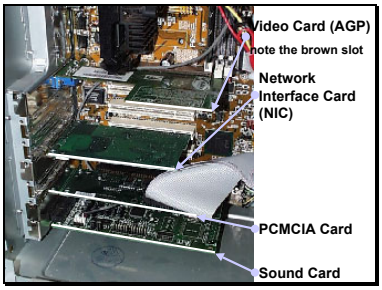
7) Install the Screw on the tongue. Insure that it is tight.

8) Install the CD-ROM audio cable back in its seat.

Removing/Installing the Video Card

- ✓ Phillips screwdriver
- ✓ Anti Static Bag

Familiarization



Before you remove the board, check to see what slot it is in PCI (white) or AGP (brown) and where it is located.

FIGURE IX.18

Removing the Video Card

1) Remove the Phillips Screw from the Tongue of the video card on the inside.

2) Discharge any static build-up you may have, by touching an unpainted surface of the chassis or a screw that is installed somewhere on the chassis.

3) Grasp the board by the tongue and the farthest edge from the tongue. Rock the board first toward the front of the computer and then toward the back just a little (just want to loosen it), rock it one more time towards the front then pull straight out towards you. Once the board is out, handle it by the tongue only, and put it into the Anti-Static bag.

Installing the Video Card:

4) When installing the Video card, insert the tongue between the Motherboard and the chassis first, and be sure that the gold colored contacts are aligned over the slot that it fits in. Push the whole board in evenly and all the way down. One way to verify that the board is properly seated is to check the tongue (is it flush were the screw goes). Second is to check to make sure that if you push at the end furthest from the tongue, does the board go down a little more (if it does push evenly again in the middle. One final check to make sure that it is completely seated and not tilted in some fashion

5) Install the Screw on the tongue. Insure that it is tight.

LESSON X: NETWORK EQUIPMENT

TASK: The DTFM will identify the equipment in the cabinets using the naming structure the Army has assigned, and do basic trouble shooting of the system with the assistance of the TAC Help Desk.

CONDITION: DTFM should understand the basic operation and trouble shooting techniques to be used in the DTFs with the assistance of the TAC Help Desk

STANDARD: DTFMs will follow the instructions provided by the TAC Help Desk to enable the networking systems to function properly.

Host Naming Structure

The Hosting Name Structure for the DTF system uses the following format:

GENERAL		EXAMPLE	
RSSSBBBBCCCCDD		**1EUSZ650ZZZ1WB**	
R	Region Identifier	1	Region 1
S	Site, Installation or Campus	EUS	Fort Eustis
B	Building Number	Z650	Building Number (with a space holder in “z”)
C	Classroom or Room Number	ZZZ1	DTF#1 in Building 650
D	Device Identifier	WB	Workstation B (or 11)

In those cases where an entity identifier has fewer characters than the field requires, that identifier shall be padded with enough leading “Z” characters to fill the field.

The following codes are used for each portion of the Hosting Naming Structure format:

Encapsulated Encryption Device (EED)

1. Operation Workstations send and receive data on the EED’s ‘private’ connection. Data is encrypted and forwarded on the EED’s ‘public’ connection. During Normal operation, the Green - Power and the Amber - Self-test light will be on steady. The Amber - Keys light will be blinking.

2. Troubleshooting During potential troubleshooting operations, it is essential that the system not be powered off unless directed to do so. The TAC loses all ability to access devices on the private side of the EED when powered down. If a problem is suspected, the help desk should be contacted immediately.

3. Self Destruct Key The round self-destruct key is required for FIPS140 compliance. Inserting this key destroys all data in the EED. This would require replacement of the EED to return to an operational status. Only on direction or if a site is compromised, should this key be utilized to destroy the EED. This key should not be locked in the server cabinet.

Switch

1. **Operation** — All active ports (ones with devices plugged in) should have green lights. They should blink occasionally. If a device is powered off, the associated port light will lose illumination.

Normally two Cisco 2900 series switches are used to provide network connectivity in the classroom.

One switch provides connections for the ATM or Cat 5 10/100 lines and public connection for the EED.

The second switch provides connection ports for the workstations, printer, server and the private connection for the EED

Patch Panel

The patch panel is a non-intelligent device utilized to physically connect devices with flexibility.

Firewall – Security Stack

This equipment prevents unauthorized access to the TADLP network.

IDS – Intrusion Detection System

The IDS alerts the network administration to any breach of network security.

Servers

In the TADLP network, servers play different roles. These classifications include Enterprise Backup Domain Controllers (BDC), Regional Backup Domain Controllers (BDC), and Member Servers.

1. **Enterprise BDC** — The Enterprise BDC maintains a READ ONLY copy of the security database for the purpose of validating user accounts and login account control for that location.
2. **Regional BDC** — Regional BDC are servers also located in or near the classrooms and control network domain security and computer accounts.
3. **Member Servers** — Member Servers are part of the domain and are IBM 5500 servers located in or near the classrooms. They provide storage for shared files and images.

LESSON XI: TAPE BACKUP PROCEDURES

TASK: Tape backup procedures.

CONDITION: DTFM will follow the procedures for removing, loading, and labeling tapes used for backup. They will also verify the status of all backups.

STANDARD: DTFM will verify that the tapes are labeled properly and that the server has performed the appropriate backup.

Logging into the Server

1) Turn on the monitor.

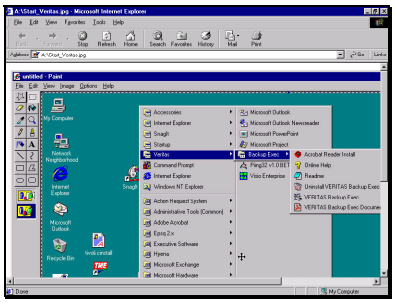
2) **For DTFMs with servers in two cabinets, side-by-side:** Look in the upper left-hand corner of the screen; you should see a small green box with a number in it. Press the print screen key and a window should open with "ports and names." **Depending on your site, you may have Ports 1-4, however, you will only be using 1-3**, which correspond to the servers in your cabinet. Use the up and down arrow keys to move through the numbers in this box, starting with number one (1). Press Enter, and the window will close.

3) **For all users:** Log on to the server using your UserID and password, (e.g., DLAC#### / Letmein1) and TADLP0 as the Domain. If you can not log on to the server, notify the TAC Help Desk.

Opening/Verifying Backup Program

NOTE:

Backups will be checked daily (Mon-Fri) and on weekends when open)



1) From the desktop double click on the "Veritas Backup Exec" icon, or use Start, Programs, Veritas, Backup Exec and Veritas Backup Exec and left-click once. *(see figure XI.1)*

FIGURE XI.1

2) Once the program opens go to the "Job Monitor" tab, at the bottom of the window and left click. This will open the window: Scheduled, Active, and Completed Jobs. The job status (successful/failed) is listed on this screen: Look for the job name, job status, percent completed (i.e. 100%), and start time. Also whether the job ran the previous night, or failed.

3) Verify "Scheduled" job in Job Status column (MONDAY / TWTFSS). Monday is a full backup and TWTFSS are incremental backups.

4) Report to the TAC Help Desk, any jobs with the following errors: "failed loading," "pending," "on hold," or "failed more than one hour".

Changing Media

1) Press and release the "Blue" Unload button on face of the tape drive. Observe the lights on the face of the drive, and wait for the lights to change from amber to green "Operate Handle" light. NEVER OPERATE THE HANDLE UNLESS THE GREEN "OPERATE HANDLE" LIGHT IS ILLUMINATED
2) Lift the handle, remove the tape, and replace it with the next tape in series.
3) Allow time for media to reset (all amber lights).

Labeling

The tape case will be labeled according to the following protocol:

1. **Server Name:** e.g. EEUS1522ENCCA2 (name of your server)
2. **Tape Number:** Week
   - Label First Tape with Weeks, 1,5,9,13,17,21,25,29,33,37,41,45,49.
   - Label Second Tapes with Weeks, 2,6,10,14,18,22,26,30,34,38,42,46,50.
   - Label Third Tape with Weeks, 3,7,11,15,19,23,27,31,35,39,43,47,51.
   - Label Fourth Tape with Weeks, 4,8,12,16,20,24,28,32,36,40,44,48,52.
3. **Tape Date:** The date will include the start date of the tape and ending date of the tape: e.g. 05/05/01 – 05/11/01

Hard Code Labeling of the Media (Tape)

NOTE:

Do **NOT** continue labeling media until all "failed," "on hold," etc. jobs have been aborted.

The media used in the Veritas program will be labeled as follows:

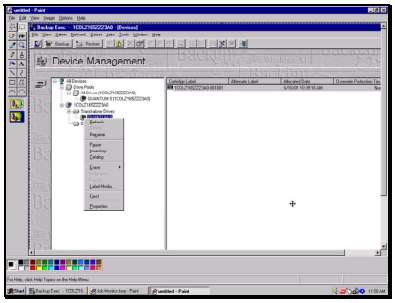
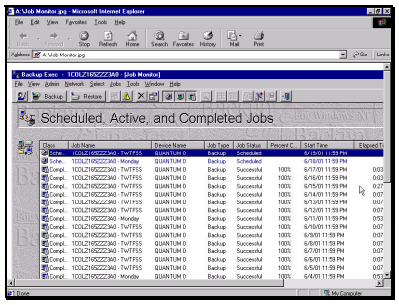


FIGURE XI.2

1) From the Backup Exec screen, select the "Devices" tab from the lower screen menu bar. Right-click on "QUANTUM-1or 0" under "Stand-alone Drives", (*see figure XI.2*) in the tree on the left-hand side of the screen. Select "Label Media" and left-click once.
2) A warning message window about media erasure will open; click "OK".
3) The "New Cartridge Label" window should open. If it has the server name and date in the block, change just the date. If this information does not appear, enter the server name and date.
4) DEVICE NAME will be entered as follows.
   ✓ EXAMPLE: EEUS1522ENCCA2-MMDDYY.

5) After labeling the tape, click on "OK". The "Backup Exec Warning" window will display with all the tape information, click on the "Respond Ok" button in the upper right hand side of the window.



6) Select the "Job Monitor" tab and observe Labeled Media is "Running" in "Job Status" column. Once tape has completed "Running", the "Job Status" column will default to "Scheduled" for that assigned date. *(see figure XI.3)* Close all open windows; return to desktop and log off server.

FIGURE XI.3

Care of Media

Store tapes flat (in the same position as if they were in the tape drive)

Storage location should be no warmer than 75 degrees.

Tape storage location will be in accordance with the TADLP COOP (Appendix A of DTFM SOP Ver 2.2 dated MMDDYY).

Cleaning Tape

If the "Use Cleaning Tape" light comes on, follow the same procedures used above to remove media from the drive. Insert the cleaning (yellow) tape. When the tape cycle is done, the "Operate Handle" light will come on. If the "Operate Handle" light does not illuminate, press and release the blue button and wait for the "Operate Handle" light.

Media Rotation

NOTE

It is mandatory that all managers complete a daily check of each server to insure that a complete/good backup was completed the night before. If problems are encountered the TAC Help Desk must be contacted.

Tapes are to be changed on all of the servers on Monday morning. If Monday is a federal holiday, the tapes will be changed the Friday before the holiday, or if there is training over the weekend before the holiday the tape will be changed after the training is completed. When you check for a proper back up on Tuesday after the holiday it will be normal to see errors for Friday, Saturday, and Sunday because the scheduled full back up is not done until Monday night.

Each server should have four dedicated tapes.

Tapes are rotated on a four-week schedule (week 1 – 4).

LESSON XII: GENERAL VTT INFORMATION

TASK: This lesson will provide the DTFM with the information required for the operation of the VTT system, guidance in the proper procedures when preparing, conducting VTT sessions, and reporting problems with the VTT system.

CONDITION:

STANDARD: The DTFM upon completion of this lesson will have the working knowledge to operate the VTT system, prepare, conduct VTT sessions, and report VTT operational problems.

NOTE

Two CD-ROMs included in the "push package" provide training to the DTFM on the operation and trouble shooting of the VTT system. Please be sure to review these CDs. This document is **ONLY** a follow-up reference document.

The Operating System

Peripherals

CPU	Intel Pentium 233Mhz microprocessor running Windows 95. The CPU contains a 3.5" High Density diskette drive and a 24 speed CD-ROM
CODEC	A coder/decoder that digitizes and compresses video and audio for sending and expands and converts incoming video and audio for receiving
Cordless Keyboard	Used in conjunction with the infrared located at the front of the classroom. This device allows the Classroom Manager to move around the classroom while operating the keyboard. *Remember that this keyboard must have line-of-sight with the sensor in order to function.*
Standard Keyboard	Backup for the cordless keyboard
Trackman Live receiver	Operates with the air mouse and the VTEL Cordless mouse. It plugs into the mouse extension located under the Classroom Manager's desk
Trackball air mouse	Works in conjunction with the Trackman Live receiver. Operating distance can not exceed 7 feet from the receiver. *This is another option for operating the system moving about the classroom.*
VTEL Cordless Mouse	Works with the Trackman Live receiver and again, the operating distance can not exceed 7 feet. *It must be used on a flat surface.*
Monitors (2)	The left monitor views the distant site and the right monitor displays the local classroom and graphics
Cabinets (2)	Houses the VTT system components and supports the monitors
Student Microphones	Located on student workstations throughout the classroom. *Each microphone is shared by two workstations.*

NOTE

All keyboards must be kept locked in the cabinet unless a VTT session is in progress and the DTFM is present in the classroom.

Audio Components

Eight Channel Automatic Gate	Detects which microphone has an incoming audio signal and sets the priority.
Eight Channel Microphone Mixer	Mixes the microphone signals and allows volume adjustments
Manager (OMNI) Microphone	A "hot" (always on) omni-directional microphone.
Student Microphones	Set for "push-to-talk" and to focus on the student
Acoustic Stereo Speakers (2)	Allows participants to hear the audio from other participants in remote locations
Audio Amplifier	Transmits incoming audio to the speakers

NOTE

While in a VTT session, please remember to disconnect the Manager Microphone. It will pick up all sounds in the vicinity and will divert attention from the current speaker.

Video Components

Programmable Response Module (PRM)	Controls automated camera control of the student camera. Through the use of "push-to-talk" microphones, the camera can be automatically positioned to focus and zoom on an individual student when that student wishes to speak. When a student presses and holds the "My Turn" button, the camera will move to that station. That microphone will be live while the button is held and the red light on the microphone is lit.
CameraMan Pan/Tilt Camera	Functions include zoom and image management that can be controlled using the ParkerVisions's Remote Control Keypad
CameraMan Remote Control Keypad	Sets and stores the camera workstation positions

ELMO (Visual Presenter & Document Camera)

The ELMO is a Visual Presenter and Document camera that can be used to display paper documents, 3 dimensional objects, slides and transparencies on the VTT monitors.

The VCR

Operation of the VCR is covered in the individual instructions for your VCR. You must ensure that the VCR is set to receive local programming and not to receive from cable or an antenna. Instructions should come with the VCR. To tape a session from the CPU, local camera or distant end, the user must select the appropriate menu function in the VTEL toolbar.

CAUTION

Care must be taken to ensure that the local camera selection under tool bar one does not have the "Send VCR" option activated when recording a training session.

System Operation

The VTT system must be left in the following ready state depending on where the DTF is located:

- Systems in Continental United States (CONUS) must be left in a call at all times with the monitors turned off.
- Systems located in Germany must be left on at all times with the monitors turned off.

Leaving the VTT systems in this state will allow for system checks or troubleshooting by the NCC without the manager being present. The NCC at Fort Eustis, VA, will initiate all calls and "bridging" (connecting sites between networks) according to scheduled VTT requests.

Setting up a VTT session

WITHIN THE TADLP NETWORK

Each manager is responsible for setting up a VTT session with other DTF sites. When a student requests a VTT session with another distance learning site, the host site performs the following tasks.

1) Check to see the availability of the sites to be included in the broadcast
2) If the sites to be broadcast are available, the host DTFM will schedule the VTT with the NCC.
3) The host DTFM will utilize NCC web site http://155.217.20.36/armyrequest1.html to schedule the VTT session. Once the form is submitted it is sent to the NCC for scheduling, you will receive an email confirmation of your request.

OUTSIDE THE TADLP NETWORK

1) The VTT session will be scheduled as stated above except that the request must be submitted to the NCC 5 working days prior to the start of the session
2) VTT sessions outside the TADLP network require the approval of the TADLP PM office after the request is submitted to the NCC.

Problem Reporting

The procedures listed below are to be followed by the DTFMs at all sites when problems are discovered with the VTEL VTT system.

1) The DTF manager must immediately call the NCC (757 878-4815; DSN 927-4815) or email (TNET@atsc.army.mil) at Fort. Eustis, VA or email to report the problem and receive guidance on repair
2) After reporting the problem to the NCC, the DTFM will then call the TAC Help Desk to report the problem and obtain a trouble ticket number.
3) The NCC personnel are the only authorized individuals to provide resolution to VTT system problems.
4) DTFMs will provide updated status reports to the Help Desk daily for problems not resolved within 24 hours.
5) Once the system is repaired, the DTFM will make contact with the Help Desk to close the problem ticket.

Trouble Shooting

Managers are permitted to trouble shoot the VTT equipment only for:

- Loose cables - tighten cables and/or swap cables under the specific guidance of the technician.
- Observe that all the proper system lights indicate proper operation or indicate faults.
- Perform system troubleshooting under the specific guidance of the technician.
- Any other trouble shooting procedure will only take place under the guidelines of the VTEL technician.

NOTE

The Help Desk will only track the repair of the VTT system and will not provide technical guidance on repairing the VTT components or any part of the communications hardware or circuits.

LESSON XIII: THE VTT TOOLBAR

TASK: Learn VTT toolbar

CONDITION: This lesson will give the DTFM a working knowledge of Video Teletraining toolbars.

STANDARD: The DTFM will be able to operate the Video Teletraining toolbars.

Turning on the VTT system

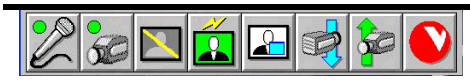
1) The master power switch for the VTT system is located either on the front or back of the power panel. The VTT System master power switch should remain on at all times, except in times of power outages.
2) Ensure the cable connection, T1 RJ45, and proper green system indicator lights are visible on the CPU, Pair Gain and the Ascend Unit. These network interface control components are used to connect with the Network Control Center (NCC).
3) The power switch for the monitors is located on the front of each unit. Monitors should be powered down when not in use.
4) Should you loose power to your classroom, immediately turn off the master power switch. When power is restored, turn on the master power switch. The system will boot-up automatically.

Running AppsView Software

1) When the VTT System is turned on, Windows 95 and AppsView Software will start up automatically. The VTEL red ball and local classroom volume control will appear in the lower right corner of the right monitor.
2) The AppsView Software is the package utilized in a Windows 95 environment to perform Video Teleconferencing.
3) The VTEL Ball activates and controls three toolbars. When not used the ball will disappear in approximately one minute. However, when the cursor is placed on either the VTEL ball or a toolbar, they will remain displayed indefinitely.
4) Each toolbar has been customized for Distance Learning Functionality.

Using AppsView toolbars

This section explains how to display and select the toolbars. Remember the toolbars operate from RIGHT to LEFT, starting with the red VTEL ball. If the VTEL ball is not visible, moving the cursor will make it reappear.

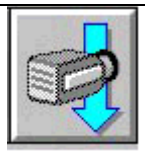


FUNCTIONS OF TOOLBAR ONE

To display toolbar one, click the VTEL ball once.

When you select the first button, Local Video Source, the local video source toolbar will be displayed. Five options used for distance learning are:

- Camera 1 - Send Video Source One. This controls the Local Camera.
- Camera 2 - Send Video Source 2. This controls the ELMO.
- Camera 3 is not currently used in distance learning classrooms, as there is only one local camera.
- Camera 4 - Send Video Source VCR plays the VCR.
- Camera 5 - Send Video Source PC displays selected images from the PC. For example, a PowerPoint slide show.



When you select the second button on toolbar one, Remote Video Source, the remote video toolbar is displayed. This toolbar gives the user the option to control the distant end cameras when in a point-to-point conference. This function is not available during a multi-cast. To perform this function, select a camera from the toolbar. Move your cursor to the left until it is visible on the left monitor. At this time you can control the remote camera by holding the left mouse button. The camera will move in the direction of the cursor arrow.

The third button on toolbar one, is PIP tools. This is for displaying the Picture in Picture, or PIP Toolbar. Four options of PIP are:

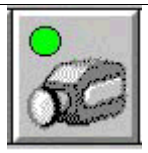
- Option 1 - Show/Hide PIP Window. This turns the PIP on and off.
- Option 2 - Select next PIP Size. There are only 2 sizes, small or large.
- Option 3 - PIP Swap. This changes the PIP from the distant classroom to the local classroom.
- Option 4 - Reposition PIP. The PIP can be repositioned to any corner of the screen by clicking on the reposition PIP button. Each click will move the PIP to a new position.

The fourth button on toolbar one, Show connection interface, is used to place a VTT call. When activated the Connection Interface dialogue box appears showing the Speed Dialer, Hand Dialer, Telephone, Address Book, and Hide functions.

- The Speed Dialer option is for normal operations and is conducted in the direct connect mode.
- The Hand Dialer and Telephone options are rarely used in Distance Learning Classrooms.
- The Address Book option is used to set up the Speed Dialer. This is done during the initial installation process.
- The Hide option is used to hide the Connection Interface dialogue box.
- There are three ways to place a call. With the desired connection number highlighted, press the “Dial” button. Or, you can double click the desired connection number. The third method is to select and click a connection button on the right side.
- After you place a call, the Site Dialed screen will be displayed and the Port status will change from Yellow to Green.

To disconnect a call, select the fifth button on toolbar 1, Disconnect Video Call. This action will disconnect the current call. The system will display the Site Dialed dialogue box and the Port A status block will change from Green to Yellow to Black.

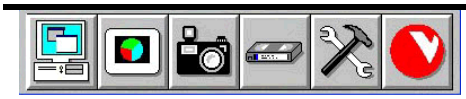
- The system will then display the Call Status dialogue box indicating the call was disconnected by the local site.



The sixth button on toolbar one, Set Video Privacy, controls what the distant site sees and hears.

- When Video Privacy is set, Audio Privacy is also turned "ON". The distant end will see a display of a camera with a lined out symbol and two smaller icons indicating to them that video and audio privacy are activated.
- To turn off video privacy, click the Set Video Privacy button again on toolbar one.

The seventh button on toolbar one, Set Audio Privacy, controls audio privacy from the local site. When Audio Privacy is set "ON" audio is off at all Student workstations and the Classroom Manager workstation.



FUNCTIONS OF TOOLBAR TWO

To display toolbar two, click the VTEL ball twice.

The first button is the Show Tools Toolbar, which is used to setup and modify system settings.

- The first option shows Controls Interface displaying the "Control Panel" and is used for Audio, Video, and Communications adjustments.
- The Audio view controls the adjustment of the system speaker volume, and provides a graduated scale control of the volume.
- The VCR Play Volume controls the VCR output sound levels.
- The VCR Record Volume controls the VCR recording sound levels.
- The Video view controls the adjustment of the color balance and chroma-key color. These controls are set during the initial installation process and should not be adjusted.
- The Communications view has three settings, the only one used in the Distance Learning application is "Internal Loop back".
- Internal Loop back allows you to view what is being sent to the distant end. For local testing, the distant end is the left monitor. It also allows for the testing of the microphone system. You will notice a slight delay when using Internal loop back. As a troubleshooting tool it will test approximately 98% of the systems capabilities.
- To disconnect from loop back, go to toolbar 1 and place the cursor on the "Disconnect Video Call" and then press enter or click the mouse button.
- The second option on the Show Tools Toolbar is set configuration. There are four options: appearance, launch, file locations and document camera.
- Appearance and Document Camera are the only options that Distance Learning uses, all other options should be avoided.
- When viewing the Appearance dialog box the items to be checked are; "Display Preset Toolbar and Configurable Toolbar. Toolbar timeout should be set at 5 seconds.
- When viewing the Document Camera dialog box, the camera being used for documents should be checked. This will identify which camera is used in support of the ELMO. Camera two was preset during installation for the ELMO and should not be adjusted.

- ***NEVER*** click the "Launch Advanced Configuration Program" button unless advised to do so by the NCC.
- The third option on the Show Tools Toolbar is Show Call Status Window, which displays the status of the call. The following colors indicate the status of the call:
  Black = the call is disconnected
  Yellow = attempting connection
  Green = the call is connected
- The fourth option on the Show Tools Toolbar is Show System Monitor, which displays the VTEL System Monitor. ***Do not*** enter this area or make adjustments unless advised to do so by the NCC.

The second button on Toolbar two, is Select VCR Recording Source. This brings up the VCR record toolbar with three options.

- Option one, record local PC, enables the Classroom Manager to record from the local classroom computer. For example, PowerPoint Presentations.
- Option two, record local video, enables the Classroom Manager to record Local Video from the local classroom camera.
- Option three, record remote video, enables the Classroom Manger to record Remote Video from the distant end.

The third button on Toolbar two, when selected shows the Snapshot toolbar with three options.

- Option one, snapshot from remote, enables the Classroom Manager to take a snapshot from the remote camera.
- Option two, snapshot from local camera, enables the Classroom Manager to take a snapshot from the local camera.
- Option three, snapshot from PC, enables the Classroom Manager to take a snapshot from the local CPU.

When a snapshot is taken, the snapshot toolbar appear on the left side of the local monitor. As with the previously discussed toolbars, each button is explained by the system when highlighted. Each button gives you an option to apply an action to a snapshot.

- **The Snapshot One Toolbar has five options and they are:**
  - Hide toolbar
  - Line Drawing Mode, lets you draw lines on your snapshot
  - Text insertion mode allows text to be added to the snapshot.
  - Eraser mode allows the use of single point erasing.
  - The color selection allows you to select the color you want to use for drawing.
- **The Snapshot Two Toolbar also has five options and they are:**
  - Hide toolbar
  - Font Size lets you change the font size. Three sizes are available. Each click of the button changes the font size.
  - Line thickness allows you to change the drawing line thickness. Two sizes are available. Click the button to change the line size. Then click and drag on the snapshot.
  - White board clears the screen by bringing up a white board.
  - Clear Annotation will remove any drawing or text changes made to the current snapshot.
- **The Snapshot Three Toolbar has five options and they are:**
  - Slide Tray allows you to add a slide or a snapshot to a tray for later viewing
  - Save Slide gives you the option to save a slide or snapshot so it can be saved to the slide tray.
  - Send Slide sends the current slide or snapshot to the distant end.
  - Next Slide shows the next slide on the local monitor.
  - Previous Slide shows the previous slide on the local monitor.

The third button on Toolbar two displays View PenPal for Windows. This provides the user quick access to the Snapshot Toolbars when working with slides from the slide tray.

The fourth button on Toolbar two displays View PC Screen. This displays the Windows 95 screens and functions. This option controls local viewing only and should not be confused with Toolbar one, button one, option five that sends the image from the PC to the distant site.

FUNCTIONS OF TOOLBAR THREE

To display toolbar two, click the VTEL ball three times. Toolbar three is used to Preset Camera Positions and move the camera to these positions.

To set a camera position, click on the store button. You should see a green light on the button. Next, move your camera using the cursor on the local monitor. The camera will move in the direction of the cursor arrow when you hold down the left mouse button. You can also zoom, by moving the cursor to the center of the monitor. When a plus or Minus symbol appears, hold the left mouse button. The camera will zoom in during plus mode, and zoom out during minus mode. When the camera is in the desired position, click on a local button A through F. This will preset the position

When the Remote button is displayed, there are six Local Function buttons, A through F, available for use. Each allows you move the local camera to a different preset position.

When the Local button is displayed, there are six Remote Function buttons, A through F, available for use. Each allows you to move the remote camera to a different preset position. This function is only available in a point-to-point conference.

Setting the Camera Workstation Positions

The Cameraman Remote Control keypad is used for setting and storing the camera workstation positions.

1) The Camera power must be on in order to operate the Camera Remote Control keypad. Distance learning uses a single camera application. Currently, only camera one is functional.
2) The Image settings adjust the picture brightness in the video frame. The Manual Settings will override the Auto Image mode and put the camera in manual mode. The Automatic Settings will automatically adjust the Image (light and dark) for each camera view.
3) The manual four position Pan/Tilt keys allow the user to adjust the pan or tilt of the Camera in the desired direction. The zoom feature allows the user to zoom in for a tighter view and zoom out for a wider view.
4) Location Preset positions can be stored and recalled using the Camera Control Keypad. Each Location Preset memorizes and stores up to four camera control functions: Pan, Tilt, Zoom, and Image.
5) To recall a location preset, select the camera of choice. Next, input the location preset number (1 through 99) then press and release the enter button. The Cameraman will move to the preset location and recall the stored information.

LESSON XIV: VTT ANTI-VIRUS

TASK: Installation, set-up and configuration, and installation updates of the anti-virus software.

CONDITION: DTFM will follow the procedures for installation, set-up and configuration, and updates of the anti-virus software. Acknowledge and confirm the updates every two weeks

STANDARD: DTFM will verify that updates have been installed on the system.

Anti-Virus Protection and Upgrade:

Symantec Norton Anti-virus (NAV) 5.2 is a Windows application that is used to safeguard the VTT computer from virus infection. The system will be protected from viruses that spread from hard drives, floppy disks. DTF Manager's will download these files from TADLP ISSO, ACERT, CERT and/or local DOIM web site when updating VTT systems throughout TADLP.

NOTE:

All TADLP DTFMs (Blocks 1& 2) will acknowledge and confirm the updates every two weeks via e-mail or fax depending on the network capabilities on site.

NOTIFICATION:

DTFMs will send a one-line message to the following when they have completed the updates every two weeks. Only one office needs to be notified:

1. **TADLP DTFM-PM:** 757 878-0442
2. **TADLP Help Desk Phone Number:** toll free 1-877-251-0730.
3. **TADLP DTFM-PM and Help Desk Fax Number:** commercial 757-878-0440

   or DSN 927-0440.

CONFIGURE NORTON ANTI-VIRUS:

Follow the steps below to setup and configure the VTT system for protection. This configuration is mandatory, as are the biweekly updates.

This outline provides directions on the installation, set-up and configuration, and updates of the anti-virus software. As a rule all files and folders should be set to scan for the protection of the system. Norton Anti-virus is preset to provide complete protection against viruses.

1) On the main screen, choose “Start”, “Programs”, “Norton Anti-virus”, and “Norton Anti-virus” at the pop up menus.
2) Click on “Options” button
3) Click on the “scan” tab. Click on the “Auto Protect” tab. In the field “What to scan” select “All files.” In the field “How to respond” select “repair automatically.”
4) Click on the “Auto Protect” tab. In the field “What to scan” select “All files” In the field “What to scan” select “All files.” In the field “How to respond” select “repair automatically.” Deselected “Auto protect can be disabled”
5) In the “Options” window click on OK button

NORTON ANTI-VIRUS UPDATE:

Download these files from TADLP ISSO, ACERT, CERT and/or local DOIM web site when updating VTT systems.

The updates on the VTT systems have to be the same as on the workstations.

Follow the instructions listed below on how to update the anti-virus definitions**.**

1) The DTFM is responsible for downloading (at least) every two weeks from either the TADLP ISSO and/or TAC Help Desk e-mail. Any of these Army approved web-sites: (http://www.acert.belvoir.army.mil, http://www.cert.mil, and/or the local DOIM web-site)
2) Insert “disk 1” in the VTT workstation 3.5 inch drive, go the start icon, then Run. Type A:\xxxi321.exe, then press OK.
3) The system will prompt you to load all three disks.
4) Click on OK button, when prompted.

LESSON XV: TADLP INSTRUCTOR PACKAGE

TASK: To obtain an understanding of the VTEL VTT Instructor Package.

CONDITION: Student must have a complete working knowledge of the VTEL LC5000 ESA system. DTF must have the instructor package installed.

STANDARD: Proficiency in the operation of the instructor package.

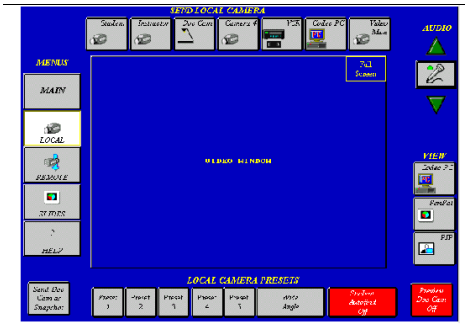
NOTE

This lesson is designed to guide the DTFM in using the APX touch screen that controls all functionality/operation of the VTEL VTT instructor package. This lesson is not to be used unless the instructor package is installed in the DTF.

Logo Page

The logo page is displayed when the system is powered down. Pressing anywhere on the screen powers up the system and brings you to the Local Camera Page.

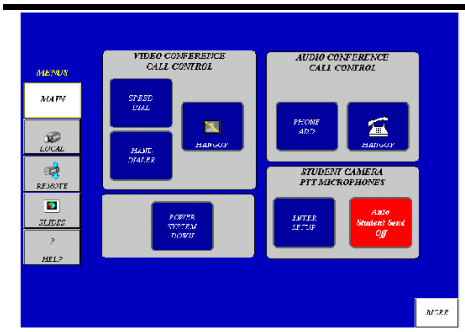
Main Connect Page



This page is used to access the pages for placing video / audio calls, setting the "Auto Find" presets for the student camera, and powering the system down. Additionally the operator may call any of the other menus available through the menu select buttons on the left side of the page.

MENU SELECTIONS (LEFT SIDE OF SCREEN)

MAIN menu button	This button will cause the touch panel to display the Main Connect Page where the operator can access the pages for placing video and audio calls
LOCAL menu button	This button will cause the touch panel to display the Local Camera Control Page. The Local Camera Control Page provides the operator with access to system camera selection, and the control associated with those cameras.
REMOTE menu button	This button will cause the touch panel to display the Remote Camera Control Page provides the operator with access to far end camera selection and the controls associated with those cameras.



SLIDES menu button — This button will cause the touch panel to display the Slide Control Page. Slide Control Page provides the operator with access to the controls for using the VTEL CODEC slide capabilities. Capabilities include sending, saving, and previewing still images.

HELP menu button — This button will cause the touch panel to display the Main Connect Help Page. This page will provide the operator with a brief explanation of many of the functions available on the current page

MORE button — This button will cause the touch panel to display the Advance Connect Page. The Advanced Connect Page provides access to system's software version, as well as the setup options for the touch panel. The advance configuration is password protected and to be used only by an administrator

NOTE

For training purposes we will bypass the Local Camera Page and proceed directly to the Main Connect Page

VIDEO CONFERENCE CALL CONTROL

SPEED DIAL button — This button will cause the touch panel to display the Speed Dial page. This page allows the operator to select video conferencing numbers from the speed dial entries stored in the VTEL CODEC. Our options are direct dial, H.221 or auto.

HAND DIALER button — This button will cause the touch panel to display the Manual Dial page. This page allows the operator to manually input video conferencing numbers. TADLP currently does not use this function.

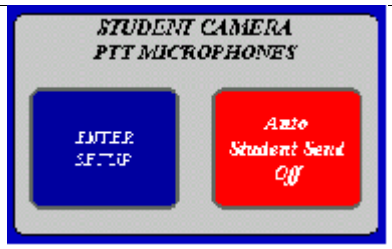
HANG UP button — This button is used to disconnect any active video conference calls

AUDIO CONFERENCE CALL CONTROL

PHONE ADD button — This button will cause the touch panel to display the Phone Add page. This page allows the operator to manually input audio conferencing numbers.

HANG UP button — This button is used to disconnect any active audio conference calls

STUDENT CAMERA PTT MICROPHONES



ENTER SETUP button — This button will cause the touch panel to display the PTT preset page. The PTT Preset page allows the operator to modify the student camera presets associated with the push-to-talk microphones

AUTO STUDENT SEND on/off — This button allows the system to automatically switch from the instructor camera to a student camera when a push-to-talk microphone is activated by a student and return to the instructor camera when the push-to-talk microphone is released. (this feature work in conjunction with the Student Auto Find function located on the local camera page)

POWER DOWN SYSTEM BUTTON

This button is used to power the system down. Prior to shutdown, the Shutdown Confirmation Page is displayed where the operator is required to verify the function.

Local Camera Page

VIDEO WINDOW AREA

This area of screen is used to display the video being transmitted from the room or the graphics from the codec if selected. The video is the same as that seen on the right hand system monitor.

FULL SCREEN BUTTON

Pressing this button causes the touch panel to display the video window full screen (Video Window Page). The appropriate controls for the selected video source will be overlaid on the displayed video.

SEND LOCAL CAMERA SELECTIONS

STUDENT CAMERA button — Pressing this button selects the student camera to be transmitted, It also overlays the camera controls on the touch panel video window.

INSTRUCTOR CAMERA button — Selects the auto track presenter camera to be transmitted. It also overlays the camera controls on the touch panel video window.

DOCUMENT CAMERA button — This button selects the document camera (ELMO) to be transmitted. Setup of the ELMO is performed on the ELMO control panel.

CODEC PC button — This button selects the Codec PC function to be transmitted

VIDEO MUTE button — Pressing this button will mute both the audio and video being transmitted.

AUDIO CONTROLS

MICROPHONE MUTE button	Pressing this button mutes the audio being transmitted.
VOLUME UP/DOWN (arrow) buttons	This feature allows the operator to raise or lower the volume of the Codec audio.

VIEW CONROLS

VIEW CODEC PC button	This button causes the Codec PC video to be displayed on the monitor allowing the instructor to preview functions from the Codec PC prior to being transmitted
VIEW PENPAL button	This button caused the CODEC PenPal video to be displayed on the monitor
PICTURE IN PICTURE button (PIP)	Button displays the PIP Control Page which allows the following, turn PIP off/on, change the size of the PIP, move the PIP to different corners of the screen and to swap the PIP with the distant end view

CAMERA FUNCTIONS

CAMERA CONTROL	The camera controls are overlaid on the screen for both the student camera and the instructor camera.
STUDENT CAMERA	The operator has the capability to control the following functions of the student camera, focus, adjust the iris, zoom the picture and move the camera up/down or side to side.
INSTRUCTOR CAMERA	The controls for the instructor camera are the same as the student camera plus there is an added feature to turn the camera autotrack on and off.
AUTOTRACK button	Used to turn the Auto Track feature of the instructor presenter camera on or off. When on the camera will cause the camera to track the instructor. Activating any of the camera pan/tilt functions will turn off the Auto Track function.
PRESET 1 through 5, WIDE-ANGLE button	These buttons are used to store and recall the presets for the selected camera. The overlaid camera controls are used to adjust the camera to the desired preset location. Pressing and releasing one of the buttons causes the selected camera to recall the corresponding preset. Pressing and holding the button for approximately 4 seconds will store the present camera position as the preset, and the touch panel will “beep” to indicate it has been stored.

STUDENT AUTO FIND button	This button is used to turn the feature on or off. With the feature on it allows the student camera to respond to the student push to talk microphones. It allows the student camera to focus on the student who actives the push to talk microphone and when deactivated the camera will return to a wide shot of the facility or the instructor (it will return to the instructor if the Auto Student Send feature is activated on the Main Connect Page)
PREVIEW DOC CAM button	This button allows the instructor to view any document placed on the ELMO without sending it to the distance end. It allows the instructor to toggle between previewing the ELMO and the Remote Video.
SEND DOC CAM AS SNAPSHOT button	Pressing this button will take a snapshot of the object on the ELMO and send it as a graphic to the distance end while continuing to send the current live image.

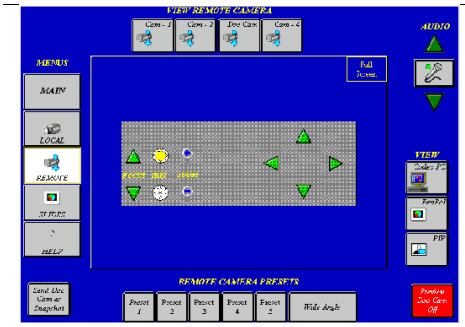
NOTE

Selecting this button also activates the SLIDE button on the opposite side of the screen allowing the instructor to select previous, next, send or save slides to folders that have been opened for use.

Prior to selecting the PenPal option the instructor must us the on screen icons and the mouse to select the folder that is to be presented.

There may be a brief interruption of live camera transmission while the snapshot is captured.

Remote Camera Page



REMOTE CAMERA SELECTED	Page is displayed via the REMOTE menu selection on the left side of the touch panel. This page allows camera selection and camera control of the remote system. These capabilities are subject to compatibility with the remote codec. The camera controls and many of the other buttons on this page are the same as those used for Local Camera Control pages and have been discussed previously. Only the buttons unique to this page will be discussed at this time.
DOC CAM BUTTON	This feature must be off when using remote camera control
VIEW REMOTE CAMERA	The system currently allows the user to control up to 4 different cameras at the distant end. When CAM – 1, 2, or 4 is selected the camera controls will be overlaid on the displayed screen. If DOC CAM or VCR is selected, no controls will be displayed. Control of the distant end camera has to be compatible with both the transmitting.

PRESET 1-5, WIDE-ANGLE BUTTON	These buttons are used to store and recall the presets for the selected remote camera. The overlaid camera controls are used to adjust the camera to the desired preset location. Pressing and releasing one of the buttons causes the selected camera to recall the corresponding preset. Pressing and holding the button for approximately 4 seconds will store the present camera position as the preset, and the touch panel will "beep" to indicate it has been stored
HELP MENU BUTTON	Activating this button will cause the touch panel to display the Remote Camera Help Page.

CODEC Slide Page

This page is used to access the graphic capabilities of the VTEL codec. Prior to using the buttons at the bottom of the page the instructor has to select the folder that is to be used during training by employing the APPSVIEW software. Once the folder is open the operator can use the buttons at the select a previous slide, move to the next slide, send a slide to the distant end or save a slide to a folder.

PREVIOUS / NEXT buttons	Allow the operator to step forward or back through the slides in the selected folder.
SEND button	Causes the codec to capture the currently transmitted video source and send it to the remote codec as a still image.
SAVE button	Causes the codec to capture the currently transmitted video source and send it to the remote codec as a still image. The operator then has the ability to save the slide using the codec keyboard / mouse
HELP button	Pressing this button will provide help screens to the instructor / operator for the different system functions.

COMMON DEFINITIONS & ABBREVIATIONS

AC	Active Component
ADLS	Army Distance Learning System
ADTDL	Army Doctrine and Training Digital System
ATRRS	Army Training Requirements And Resources System
ATSC	Army Training Support Center
BDC	Backup domain controller - maintains a backup of the security database for the purpose of validating user accounts. As well, directory replication services import updates in login scripts and Systems Management Server binaries.
BLAN	Building Local Area Network (Inside a Building)
Cache	A separate memory space for recently performed operations
CAN	Campus Area Network
CD-ROM	Compact Disk-Read Only Memory
CMP	Configuration Management Plan
COOP	Continuity Of Operation Plan
CPU	Central Processing Unit
CUITN	Common User Installation Transport Network
Daisy Chain	All units are plugged into 1; if you physically break one connection, the others after it are also broken
DCO	Dial Central Office
DISN	Defense Information Systems Network
DL	Distance Learning
DLL	A *.dll (Dynamic Link Library) is an application extension file. It is referenced by the .exe when certain menu actions are performed and contains the objects, windows, and code for that function
Domains	A logical grouping of machines running the MS Win NT operating system
DRAM	Dynamic RAM
DTAC	Digitized Training Access Center
DTF	Digital Training Facility
DTFM	Digital Training Facility Manager
ESA	Enterprise Series Architecture
Firewall	Software and hardware designed to keep outside users from penetrating a company's computer network
Floppy Disk	A removable disk
GPF *does not apply in Window NT version	General Protection Fault - signifies that something unexpected has happened within the Windows environment, typically an improper memory access. For example, an application or a Windows component might read or write to a memory location that has not been allocated to it (memory that it does not "own"), potentially overwriting and corrupting other program code in that area of memory.
GUI	Graphical User Interface

Hard Disk	Permanent Date storage
IDE	Integrated Device Electronic; a of hard drive
ILSP	Integrated Logistics Support Plan
Install Shield	Wizard-based software installation procedures
ISSO	Information Systems Security Officer
NCC	Network Control Center
NuBus/PCI	Expansion Slot
ODBC.ini	Open Database Communications - allows you to communicate from desktop to database. Microsoft's effort to provide a single API for database (called data source) access. Data sources with ODBC interfaces include: Xbase (*.DBF) files; SQL databases; Microsoft Access and Excel; Paradox; Novell Btrieve files; IBM DB2). Since it is a general-purpose (not tailored to a specific database), it provides only a subset of most database vendors' capabilities.
OISS	Operational Information Systems Security
Oracle	A type of database
PBD	A PBD is a non-compiled version of a .DLL file.
PCMCIA	Personal Computer Memory Card International Association
PDC	The Primary Domain Controller, or PDC, is responsible for maintaining the primary copy of the security database on the network. The PDC itself is also responsible for maintaining a list of the computers on the local network for browser requests and authenticating security requests for other NT Domains that are "trusted" by our network.
Ports	Socket or jack on a hub or switch.
PRAM	Parameter RAM
RAM	Random Access Memory -. A computer chip (hardware) that is plugged into the computer's motherboard. These chips are called SIMMs or Single Inline Memory Modules or DIMMs, Dual Inline Memory Modules. Measured (quantity) in Megabytes (MB) and in speed. Memory access time is measured in nanoseconds. You must have the right speed for your computer or you will have major problems. RAM must have electricity flowing through it to work. If the power is interrupted or the computer crashes, all information stored in RAM is lost. How much RAM do you need on your computer? As much as you can afford and then some. Starting the computer (booting up) consists of a self-test including testing the RAM, and then loading the necessary operating instructions into RAM. Similarly, starting an application consists of loading the basics of the program into RAM. For desktop publishing, a good rule of thumb is to base your RAM configuration on your use of. To be efficient and productive, take 5 times your average PhotoShop file size. If you run other applications with PhotoShop, add those in as well plus another 8 MB for the system.
RC	Reserve Component
Remedy	The call tracking database used by the TAC Helpdesk
Rollback	A good SQL implementation will automatically roll back an uncompleted transaction (a less-good implementation may require the application program to check a transaction log at start-up and reverse the first steps of uncompleted transactions).

ROM	Read Only Memory - information about how the computer operates also called ROM routines are burned into chips during manufacture. There are two types of ROM routines or manages: 1) The programming tools, called the "Toolbox," that developers use to create menus, windows, dialog boxes, and the other ways we interact with the computer and its applications. 2) The hardware managers that manage RAM allocation, port usage, printing and other hardware-based functions. "Non volatile memory" - permanent, does not need power to retain its data
SATS	Standard Army Training System
SBU	Sensitive But Unclassified
SCC	STAMIS Computer Contract
SCSI ("Scuzzy")	Small Computer Systems Interface
SFUG	Security Features User's Guide
SIPRNET	Secure Internet Protocol Router Network
SME	Subject Matter Expert
SQL	Structured Query Language - a standardized language that is used to define and manipulate data in a database server. The format of the requests is standardized, but the APIs that are used to generate the queries are not part of the SQL standard. Also most database vendors provide desirable nonstandard SQL extensions (making SQL implementation less portable). SQL database suppliers usually provide an API that provides application programmers with the interface they need to submit these queries to a database (which is usually elsewhere on a LAN or WAN). For example, two of the industry-leading SQL database software suppliers are Oracle Corporation and Sybase, Inc., which have Pro*C and OpenClient, respectively. SQL Server is a database product, which supports the operation of SMS.
SSN	Social Security Account Number
STAMIS	Standard Army Management Information Systems
SVGA	Super Video Graphics Adapter
Switch	Similar to a hub, it provides a non-shared connection to each device.
TADLP	The Army Distance Learning Program
TASS	The Army School System
TATS	The Army Training System
TCP/IP	A type of protocol for communication. TCP/IP is a routable protocol, which means that TCP/IP supports wide-area networking (WAN).
Test Database	A test environment for internal software applications, such as Banner.
TFM	Trusted Facility Manual
TNET	Telecommunication Network
TRADOC	U.S. Army Training and Doctrine Command
USAISEC	U.S. Army Information System Engineering Command
USAR	United States Army Reserve

Virtual Memory	"Fake memory" that pretends that part of the hard disk is RAM memory. You will need a fair amount of contiguous free space on your hard drive to use Virtual Memory. If a program loads into Virtual Memory rather than real memory, it will run much slower as hard drives are much slower than real RAM. Generally, the slowing of the applications in Virtual Memory outweighs any productivity gains and Virtual Memory is best left off.
VRAM	Video RAM - dedicated ram used strictly for enhancing display settings
VTT	Video Tele Training
WAN	Wide Area Network
Win 95 v. Win NT	NT has greater security. There is virtually no security on Windows 95
WWW	World Wide Web