# CDC 1C853A

# Radar, Airfield & Weather Systems Journeyman

## Volume 1. Introduction to the 1C8X3 Career Field & Computer Fundamentals

**Air Force Career Development Academy**

**Air University**

**Air Education and Training Command**

**1C853A 01 1903, Edit Code 01**

**AFSC 1C8X3**

**Author:** MSgt Michael P. Webb & MSgt Troy A. Partin
334th Training Squadron
Radar, Airfield & Weather Systems School (AETC)
334 TRS/ULCA
610 Hangar Road, Building 4214
Keesler Air Force Base, Mississippi, 39534-2030
DSN: 597-3118
E-mail address: 334TRS.ULCA.1C8CDCWriter@us.af.mil

**Instructional Systems Specialist:** Linda Matthews

**Editor:** Elizabeth Melton

Air Force Career Development Academy (AFCDA)
Air University (AETC)
Maxwell AFB-Gunter Annex, Alabama

Material in this volume is reviewed annually for technical accuracy, adequacy, and currency. For Weighted Airman Promotion System (WAPS) Specialty Knowledge Test (SKT) purposes, the examinee should check the *Enlisted Promotions References and Requirements Catalog* to determine the correct references to study.

THIS IS A FOUR volume A set career development course (CDC) which covers the fundamental career knowledge you need to satisfy the CDC requirements for the award of the 5-skill level in the 1C8X3 Air Force specialty code (AFSC).

This volume is divided into three units that introduce you to the Radar, Airfield & Weather Systems (RAWS) career field and computer fundamentals.

Unit 1 covers Radar, Airfield & Weather Systems (RAWS) career field structure and is divided into three sections. The first section covers the RAWS career field including AFSC structure, progression, and duties within the AFSC. The second section covers management of processes, inspections, evaluating equipment and personnel, and documenting results. The last section covers the organizational structure of the AFSC and different types of squadrons that require RAWS support.

Unit 2 covers work center fundamentals and is divided into three sections. Section one discusses safety and risk management with a strong emphasis on AFSC hazards and tower climbing safety. The second section covers publications and directives that are used in daily operations to include Department of Defense (DOD), Air Force, and technical order (TO) directives. The last section discusses security in relation to physical security of RAWS assets and other facility security procedures.

Unit 3 digs into computer and network fundamentals and is divided into six sections. It starts with describing basic computer components in section one and moves to a description of software, operating systems, and malicious influences in section two. Section three covers the UNIX operating system and section four delves into communications and network protocols. Section five relates the several different types of networks before finishing with a description of several often used network devices in the final section.

A glossary is included for your use.

Code numbers on figures are for preparing agency identification only.

The use of a name of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the Air Force.

To get a response to your questions concerning subject matter in this course, or to point out technical errors in the text, unit review exercises, or course examination, call or write the author using the contact information provided in this volume.

**NOTE:** Do not use Air Force Instruction (AFI) 38-402, *Airmen Powered by Innovation and Suggestion Program,* to submit corrections for printing or typographical errors. For Air National Guard (ANG) members, do not use Air National Guard Instruction (ANGI) 38-401, *Suggestion Program.*

If you have questions that your supervisor, training manager, or education/training office cannot answer regarding course enrollment, course material, or administrative issues, please contact Air University Educational Support Services at http://www.aueducationsupport.com. Be sure your request includes your name, the last four digits of your social security number, address, and course/volume number.

For Guard and Reserve personnel, this volume is valued at 16 hours and 4 points.

**NOTE:**

In this volume, the subject matter is divided into self-contained units. A unit menu begins each unit, identifying the lesson headings and numbers. After reading the unit menu page and unit introduction, study the section, answer the self-test questions, and compare your answers with those given at the end of the unit. Then complete the unit review exercises.

*Page*

**Unit 1. Radar, Airfield & Weather Systems Structure ..... 1-1**
1–1. Radar, Airfield & Weather Systems Career Field ..... 1-1
1–2. Management of Processes ..... 1-14
1–3. Organizational Structure ..... 1-22
**Unit 2. Work Center Fundamentals ..... 2-1**
2–1. Safety and Risk Management ..... 2-1
2–2. Publications and Directives ..... 2-18
2–3. Security ..... 2-30
**Unit 3. Computer and Network Fundamentals ..... 3-1**
3–1. Basic Components ..... 3-1
3–2. Software ..... 3-7
3–3. Unix Operating System ..... 3-10
3–4. Communications and Network Protocols ..... 3-16
3–5. Network Types ..... 3-29
3–6. Network Devices ..... 3-37

*Glossary ..... G–1*

# Unit 1. Radar, Airfield & Weather Systems Structure

**1–1. Radar, Airfield & Weather Systems Career Field ..... 1–1**
001. Air Force specialty structure ..... 1–1
002. Progression within the Air Force specialty 1C8X3 ..... 1–5
003. 1C8X3 Air Force specialty code ..... 1–9
**1–2. Management of Processes ..... 1–14**
004. Automated information systems ..... 1–14
005. Perform self-inspections ..... 1–16
006. Evaluations ..... 1–17
007. Document results ..... 1–19
**1–3. Organizational Structure ..... 1–22**
008. Operations support squadron ..... 1–23
009. Air Force Flight Standards Agency ..... 1–24
010. 557th Weather Wing ..... 1–28
011. Deployable squadrons ..... 1–30

CONGRATULATIONS! You have achieved your 3-skill level by graduating from your Air Force specialty (AFS) basic course. Enrollment in this career development course (CDC) started your upgrade training and began the path towards a 5-skill level within your Air Force specialty code (AFSC). Achieving your 5-skill level is the next milestone on the career progression journey as an operations support journeyman. One of the requirements for award of the 5-skill level is to complete the various task requirements stated in the corresponding 1C8X3 Career Field Education and Training Plan (CFETP). The CFETP and career progression are covered later in this unit. The lessons in this unit are designed to give you an overview of the operations support career field. The first section will begin by talking about the AFS structure, followed by career progression, and finally discussing the duties in the 1C8X3 AFS.

## 1–1. Radar, Airfield & Weather Systems Career Field

The United States Armed Forces depend on Radar, Airfield & Weather Systems (RAWS) in defending our way of life and in employing the instruments of national military power. Potential adversaries recognize America's reliance on advanced sensors as a critical component of military capability. These adversaries are actively seeking to discover and exploit any weaknesses in technology. Therefore, efforts to advance the development of Air Force command and control (C2) capabilities are strategic imperatives for protecting and preserving capabilities to respond to potential challenges to the sovereignty of the United States.

### 001. Air Force specialty structure

The changing environments in which the command, control, communications, computer, and intelligence (C4I) and air and space expeditionary forces (AEF) operate require vision, preparation, and attention. Coordination is necessary, in order to have people with the right skills and tools, to deliver the C4I capabilities and support required by the war fighter in meeting today's Air Force mission and prepare for the future.

Declining resources, expanding mission diversity, and ever-changing technologies are impacting the military's most valuable resource—its people. These challenging factors will continue in the future, making it critical that the work force is trained effectively and efficiently to perform duties required of each skill level within an AFS. The Air Force relies on a core-training document that outlines the basic skills, responsibilities, and training required for the 1C8X3 AFSC—the Career Field Education and Training Plan, generally called the CFETP for short.

## Career Field Education and Training Plan

The CFETP is the core document specifying the required training for enlisted personnel in an AFSC. The CFETP provides the information necessary for Air Force career field managers (AFCFM), major command (MAJCOM) functional managers (MFM), commanders, training managers, supervisors, and trainers to plan, develop, manage, and conduct an effective career field-training program.

The CFETP outlines the initial skills, upgrade, qualification, advanced, and proficiency-training requirements for individuals in specific AFSCs in order to develop skills and promote career progress. The 1C800 AFCFM maintain the 1C8X3 CFETP. The following table introduces you to a few common terms used in the CFETP.

| CFETP Terminology | |
|---|---|
| **Term** | **Description** |
| **Duty Position Tasks** | The tasks assigned to an individual for the duty position currently held. These include, at a minimum, all core tasks that correspond to the duty position, and tasks assigned by the supervisor according to Air Force Instruction (AFI) 36–2101, *Classifying Military Personnel (Officer and Enlisted).* |
| **Core Competencies** | Core competencies are defined as an integrated bundle of expert knowledge and organizational skills inherent to a particular career field(s), which makes a disproportionate contribution to the success of providing the right skills needed for military operations, anywhere, anytime. It cannot be duplicated by any other organization, and is critical for the future. |
| **Core Tasks** | AFCFM identify core tasks as a minimum qualification requirement for everyone within an AFSC, regardless of duty position. A core task may be specified for a particular skill level or in general across the AFSC. You can find guidance for using core tasks in the applicable CFETP narrative. |

## Managers in the 1C8X3 career field

1C8X3 career field managers oversee their career fields and ensure radar and airfield systems operate and support mission goals. This lesson discusses the responsibilities of three very important positions in the career field: the AFCFM, MFM, and the wing- or base-level functional manager.

### *Air Force career field manager*

The AFCFM is the advisor for all matters affecting the RAWS career field. The AFCFM communicates directly with MFM and Air Education and Training Command (AETC) training managers to disseminate all Air Force and career field policies and program requirements. As required, they also make sure your CFETP is developed, implemented, and maintained. The AFCFM also serves as the chairperson for the Specialty Training Requirements Team (STRT) and Utilization and Training Workshops (U&TW). The AFCFM uses the STRT/U&TW as a forum to determine and manage career field education and training requirements as they apply to mission needs. The AFCFM is the final decision authority for waiver requests for CFETP requirements, including CDCs. AFCFMs assist AETC training managers and course supervisors with planning, developing, implementing, and maintaining all AFSC-specific training courses. The AFCFMs also assist in developing AFSC-related manpower standards.

### *Major command functional manager*

The MFM advises MAJCOM commanders and their staff on manpower utilization and training issues. The MFM serves as the MAJCOM voting representative during career field U&TWs. The MFM's duties include assisting with gathering inputs and data to complete enlisted grade allocation for career progression group reviews and to provide guidance to subordinate units on manpower personnel issues. The MFM will assist with the dissemination of information regarding Air Force and career field policies, plans, programs, and procedures to subordinate units. The MFM also assists in identifying qualified SMEs to help with the development of specialty knowledge tests (SKT) and

CDCs. The MFM also acts as the primary MAJCOM reviewer on CDC training and classification waiver request packages. Finally, the MFM coordinates on all MAJCOM staffing and manpower issues.

### *Base functional manager*

Base functional manager (BFM) duties are normally assigned to the ranking 1C8X3 superintendent or chief enlisted manager (CEM) on-station. The BFM manages system analysis and design, programming, systems operation, maintenance, resource management and security management.

The BFM also establishes training requirements and training programs to meet local knowledge and certification requirements. The BFM manages plans, implementations, development functions, and helps functional users define requirements. The BFM supervises functional user requirements translation into automated systems capabilities. The BFM organizes teams that use methodologies to meet mission requirements and supervises test and evaluation efforts to determine performance. The BFM also organizes and participates in mission implementation and conversion and ensures continued interface between functional users and programming and operations personnel.

## Other career field activities

Several other activities and groups fulfill important functions related to career field training and CFETP development. These include workshops, including the U&TW, STRT, and Training Advisory Groups (TAG). This lesson also covers the very important area of occupational surveys and their purpose.

### *Workshops*

Workshops contribute greatly towards sustaining the Air Force mission. They allow the Air Force to match training with the skills that are required to meet the various missions. You need to be familiar with the different workshops because, ultimately, you provide the information the teams use to make decisions.

#### *Specialty Training Requirements Team*

The STRT is a meeting that includes the AFCFM, MFMs, CDC writers, Qualification Training Flight (Q-flight), and subject matter experts (SME). This meeting is a forum where the CFETP is written and updated, to include what will be trained at the technical training school house and what topics are covered within the CDCs. It is important that local work centers provide inputs of need changes and recommendations when requested by the MFM.

These activities go hand-in-hand in terms of reviewing training and identifying changes that affect overall training requirements for a career field. The AFCFM may call for a STRT of senior MAJCOM representatives to review the current training documents and develop a draft specialty training standard (STS), also called a “strawman”, in preparation for a U&TW.

#### *Utilization and Training Workshop*

A U&TW brings together a group of individuals in an effort to determine the most effective and efficient way to ensure training standards and skill level requirements for a career field are accurate and meet the needs of the Air Force. The following is a list of personnel that commonly attend a U&TW:

- Career field functional manager.
- MAJCOM functional managers.
- Subject matter experts from across the Air Force.
- Instructors from 3-skill-level courses.
- 5-level CDC writers.
- 7-level instructors or CDC writers.

- Test development specialists from the Airman Advancement Division (AAD).

The main goal of the U&TW is to establish a viable CFETP. Typically, the Air Force AFCFM initiates a workshop every other year, but it can occur at almost any time to deal with changes, deficiencies, or other impacts on training. This workshop addresses every aspect of career field training including CDCs, CFETP, job qualification standard (JQS), supplemental requirements, and specific technical training school processes.

During the U&TW, the team uses the data from occupational surveys to determine what will be in the CFETP. The information gathered from the surveys are the driving force behind what is taught in the 3-level school, and it also determines the information designated for both the 5- and 7-level CDCs. The occupational analysis report contains over 140 duty descriptions, each with numerous tasks meticulously broken out to cover the entire career field. Basically, this is a snapshot of the different tasks that AFSC personnel perform on the job at the time of the survey. This data is used to make decisions about what is taught in the different career field training courses as well as what you will need to study for promotion testing. The test development specialist at ADD uses the occupational survey results to build promotion tests and ensure the tests are valid and relevant using several inputs including task importance, knowledge of the job structure, and performance by pay-grade specific tasks. These surveys are very critical to ensuring that training is designed to meet the Air Force's requirements. It is important that you complete these surveys when you receive them. They provide you an opportunity to help determine the way the career field progresses. It is what your career field is all about!

### *Training Advisory Groups*

The career field's TAG convenes annually and provides a cohesive approach to address training management issues affecting AFSCs. These groups review training concerns and successes and coordinate training initiatives. In addition, they also do the following things:

- Set training goals and priorities.
- Review training programs affecting the communications and information community, including ancillary training, and recommend changes to formal and informal supplemental courses.
- Evaluate emerging training, training tracking, and technologies.

### *Lead Command Advisory Group*

The Lead Command Advisory Group is a forum chartered by the Air Force Flight Standards Agency (AFFSA) Headquarters Commander to facilitate the implementation of lead command processes. It meets annually to promote commonality and interaction across commands, addresses and resolves multi-command issues, and ensures the successful implementation and sustainment of multi-command systems and equipment. The advisory group's key areas of concentration include:

- MAJCOM requirements for new common and command-unique equipment for the National Airspace System (NAS) and deployable systems to support current and future combat operations.
- System modernization and sustainment efforts.
- Acquisition strategies and command perspectives.
- The lead command memorandum of agreement (MOA) between the MAJCOMs and AFFSA.
- Lead command and system affiliate responsibilities.
- Career field related Joint Services and Interagency Agreements.
- Goals and objectives of the Air Force air traffic management (ATM) strategic plan.

### *Weapons System Review*

The Weapon Systems Review (WSR) is a meeting headed up by AFFSA for RAWS and includes a complete review of the systems program to include modifications, funding, safety concerns, supply issues, and so forth. They will also discuss changes and recommendations that local work centers have provided to the MFM.

### *Occupational surveys*

Have you ever received an e-mail asking you to log onto a site and take a job survey? While some of those surveys have other purposes, one is of critical importance. It's called the *Occupational Survey* and it will ask you to select the duties you perform, indicate how long it takes to complete that duty, and what percent of your duty time goes into doing those duties and certain other tasks. The survey is designed to cover all aspects of the career field and the tasks that different skill levels are performing on the job.

Occupational surveys are constructed by the AETC Occupational Analysis Division (OAD), which compiles the data and generates the occupational survey data that is used during various training review activities including STRTs and U&TWs. So, how is the information generated by the survey and analysis used? Once the survey data has been compiled, analyzed, and consolidated in a comprehensive report, the results are used in formal training reviews. AFCFMs, STRTs, and U&TWs, along with those responsible for resident and non-resident training, use the report to revise training and proficiency codes at all levels when making changes to the applicable sections of the CFETP. The data drives changes for the 3-level technical school, 5-level CDCs, and resident or non-resident 7-level training. The same data is also used in developing the career field specific areas of the SKT used in promotion testing. The test development specialists at AAD use the occupational survey results to build promotion tests and ensure the tests are valid and relevant using several inputs including task importance, knowledge of the job structure, and performance by pay-grade specific tasks. From this short paragraph, you can see just how vital these surveys are. You *should not* take them lightly—they have an important impact on your career!

The survey results are also used for other purposes as well. Occupational analysis information is used to make classification decisions and verify the proper boundaries between occupations, identify changes needed for classification documents, remove tasks that personnel no longer perform, and identify new responsibilities. Those making training decisions use occupational analysis as part of the instructional systems development process for revising existing training course or developing new ones based on survey data. In the broadest sense, surveys provide a basis for updating training at all levels.

## 002. Progression within the Air Force specialty 1C8X3

Adequate training and timely progression from the apprentice to superintendent skill levels play an important role in the Air Force's ability to accomplish its mission. It is essential that everyone involved in training do his or her part to plan, manage, and conduct an effective training program. The guidance provided in this lesson will ensure individuals receive viable training at appropriate points in their careers. See figure 1–1, for an outline of training required to advance in the career field.

| 1C8X3 RAWS Career Field Path | | | | | | | |
|---|---|---|---|---|---|---|---|
| | Apprentice | Journeyman | Craftsman | | Superintendent | | Chief Enlisted Manager |
| Rank | | | | | | | |
| High Year of Tenure | N/A | 8 Years | 15 Years | 20 Years | 24 Years | 26 Years | 30 Years |
| Earliest sew-on time (TIS) | 6 Months<br>16 Months | 30 Months | 3 Years | 5 Years | 8 Years | 11 Years | 14 Years |
| 1C8X3 Average Note (1) | | **2.6 Years** | **4.5 Years** | **8.5 Years** | **14.5 Years** | **17.71 Years** | **23.56 Years** |
| Badges | <br>Basic RAWS Badge | | <br>Sernior RAWS Badge | | <br>Master RAWS Badge | | |
| EPME | Distance Learning Course (DLC)<br>Preservice Training<br>BMT Airmanship 100<br>Tech Training Airmanship 200<br>FTAC Airmanship 300 | ALS | Joint PME Opportunities<br>NCO DLC | NCOA | SNCO DLC | SNCOA | Required Resident Course<br>CLC |
| Upgrade Training | **3-Level**<br>**PAFSC 1C833**<br>- Awarded upon graduation from Initial Skills Course | **5-Level**<br>**PAFSC 1C853**<br>- 12 months UGT, (retrainee 9 months)<br>- Complete CDC's<br>- Complete 5-level core tasks | **7-Level**<br>**PAFSC 1C873**<br>- Min rank of SSgt<br>- 12 Months UGT (retainee 6 months)<br>- Complete CDC's<br>- Complete 7-level core tasks | | | **9-Level**<br>**PAFSC 1C893**<br>- Min rank SMSgt | **CEM**<br>**PAFSC 1C800**<br>- Min rank CMSgt |
| Professional Development | - Basic Military Training<br>- FTAC | - Train the trainer<br>- Can become supervisor after ALS | - CCAF<br>- NCO Professional Enhancement Course<br>- Basic Instructor Course | - SNCO Professional Enhancement Course<br>- SEJPME I | - CCAF<br>- Professional Mgr's Cert.<br>- SEJPME II | - SEJPME II | - MAJCOM CMSgt Orientation Course |
| Job/ Opportunities | | - Trainer<br>- CONUS RMC Tech<br>- Supervisor | - RMC Technician (Any)<br>- Instructor Duty<br>- Team Chief<br>- Supervisor<br>- Technician | - NCOIC<br>- RMC (Any)<br>- Team Chief<br>- Curriculum Developer | - Flight Chief<br>- Section Chief<br>- Instructor Supervisor<br>- CDC Writer<br>- MFM | - MFM<br>- RMC Superintendent<br>- Flight Superintendent | - CFM<br>- MFM<br>- Group Superintendent<br>- CCM |

**Figure 1–1. 1C8X3 career field path.**

## Enlisted Professional Enhancement programs

The Enlisted Professional Enhancement (EPE) programs are commonly grouped with professional development. They are designed to complement the leadership and professional development Airmen receive from Basic Military Training School (BMTS) and Professional Military Education (PME), as

well as augment lessons learned from supervisory and leadership experiences in an effort to prepare Airmen for greater supervisory and leadership roles as they progress through their AF careers.

### *First-Term Airman Center*

As a newly graduated 3-level, arriving at your first base, one of the first things you will be required to do is to attend training at the First-Term Airman Center (FTAC). The FTAC provides a structured program to transition Airmen from a training mindset to a mission-oriented environment. The FTAC provides orientation type information and reinforces lessons learned in BMTS and technical training to aid in successful transition. This unique opportunity creates an environment for Airmen to further develop their warrior ethos and continued expeditionary mindset. All first-term Airmen (FTA) must attend FTAC and are not required to attend Right Start. Supervisor support and involvement with individuals attending FTAC are critical to the future success of Airmen. See below for a description of a basic FTAC course.

- All Air Force bases will be required to establish an FTAC unless an exception is requested from the wing commander through the MAJCOM and Air Force Personnel Center (AFPC) to USAF Headquarters. Where more than one wing-level command structure exists, the host wing is responsible for the implementation and operation of FTAC.
- The FTAC will be a minimum of 28 hours, but no more than 10 duty days in length. All mandatory course objectives and minimum hours must be met regardless of course length.
- MAJCOMs and wings are encouraged to tailor the FTAC to meet local objectives in addition to the mandatory standardized requirements as outlined. However, expanded programs must be limited to additional in-processing requirements and/or training. Extending programs for activities not related to training/in-processing (i.e., self-help projects, leisure activities, community involvement, details, etc.) is not authorized.
- FTAC attendees may be required to participate in physical training (PT), unless restricted by medical waiver. When a PT program incorporates into the agenda, the program must comply with minimum standards for unit PT as established by AFI 36–2905, *Fitness Program*.
- FTAC is a consolidated training/in-processing environment, and is not considered a formal education course or PME. Therefore, completing FTAC does not necessarily warrant a formal graduation ceremony and/or banquet.

### *Noncommissioned Officer Professional Enhancement course*

This course is intended to augment and reinforce (not replace) information taught in basic military training, technical training, ancillary training, PME, and job experience.

- The Noncommissioned Officer Professional Enhancement (NCOPE) course is designed to target noncommissioned officers (NCO) who completed Airman Leadership School (ALS) at least three years before and/or who have not yet attended the NCO Academy (NCOA).
- NCOPE courses must be at least three, but no more than five duty days in length. Based on the size of the eligible populace, this course must be offered enough times to ensure all have the opportunity to attend.
- Instructors will conduct their briefings according to Air Force Standardized Lesson Plans. Career assistance advisors (CAA), as course managers, will ensure the lesson plans are used in teaching the NCOPE block/course. All approved EPE lesson plan material is maintained at the CAA/FTAC/EPE Community of Practice at the following Web site: https://afkm.wpafb.af.mil/ASPs/CoP/ClosedCoP.asp?Filter=OO-DP-AF–08.

### *Senior Noncommissioned Officer Professional Enhancement Course*

This course is intended to augment and reinforce (not replace) information taught in Basic Military Training, technical training, ancillary training, PME, or job experience.

- The Senior Noncommissioned Officer Professional Enhancement (SNCOPE) course is designed to provide newly selected master sergeants with an in-depth view of their increased supervisory, leadership, and managerial responsibilities. It also provides assistance in making the transition to senior noncommissioned officer (SNCO) status more effective.
- All SNCOPE courses will be a minimum of three and no more than five duty days in length. The target population for SNCOPE is all newly selected master sergeants. In an effort to assure 100 percent of those eligible have the opportunity to attend, each installation conducts a minimum of two SNCOPE courses annually.
- Instructors conduct their briefings according to Air Force Standardized Lesson Plans. CAAs, as course managers, will make sure the lesson plans are used in teaching the SNCO PE block/course. All approved EPE lesson plan material is maintained at the CAA/FTAC/EPE Community of Practice at the following Web site: https://afkm.wpafb.af.mil/ASPs/CoP/ClosedCoP.asp?Filter=OO-DP-AF–08.

## Enlisted Professional Military Education

Enlisted Professional Military Education (EPME) introduces Airmen to appropriate skills at specific milestones throughout their career. This allows Airmen to develop the needed skills at the correct time in their career to move to the next level. Without accomplishing the required EPME, you will not be eligible to move on to the next rank.

### *Airman Leadership School*

Airman Leadership School is an Air Force education program held at base level to prepare senior Airmen (SrA) for positions of greater responsibility. The course teaches leadership skills required of supervisors and reporting officials throughout the Air Force. Airman Leadership School enhances the development of Airmen by strengthening their ability to lead, follow, and manage while they gain a broader understanding of the military profession. The principal instructional method is guided discussion, in which students share ideas, experiences, and work together to achieve various educational objectives.

Formative evaluations are an integral part of the ALS curriculum and serve as feedback tools for the student and instructor. Summative objective and performance evaluations are used to determine whether the educational requirements outlined in the course are met. Students must satisfactorily accomplish all lesson objectives, including those pertaining to fit-to-fight, drill, and ceremonies using the criteria outlined in the course curriculum.

### *Noncommissioned Officer Academy*

The Noncommissioned Officer Academy (NCOA) is designed to develop adaptable NCOs for current and future leadership and management challenges and to operate (think/act) critically in complex and ambiguous environments. Unlike other courses which evaluate one's knowledge and comprehension using end-of-course examinations, this course integrates written and experiential projects designed to assess one's cognitive abilities through the use of nine varying modules.

NCOA is the second level of EPME and prepares technical sergeants to be professional, war-fighting Airmen who can manage and lead Air Force units in the employment of airpower. Currently, there are 10 NCOAs worldwide, see the chart below.

| NCOA Locations | |
|---|---|
| **Continental United States (CONUS)** | **Outside the continental United States (OCONUS)** |
| Airey NCOA (Tyndall AFB, FL) | Binnicker PME Center (Joint Base Pearl Harbor-Hickam, HI) |
| Gaylor NCOA (Lackland AFB, TX) | Elmendorf PME Center (Joint Base Elmendorf-Richardson, AK) |
| Mathies NCOA (Keesler AFB, MS) | Erwin PME Center (Kadena AB, Japan) |

| NCOA Locations | |
|---|---|
| **Continental United States (CONUS)** | **Outside the continental United States (OCONUS)** |
| McGhee-Tyson NCOA (McGhee-Tyson ANGB, TN) | Kisling NCOA (USAFE PME Center, Kapaun AS, Germany) |
| Sheppard NCOA (Sheppard AFB, TX) | |
| Vosler NCOA (Peterson AFB, CO) | |

The NCOA program is a substantial investment of resources, personnel, and facilities, all dedicated to providing you with the tools you need to lead people and manage resources. The Air Force's SNCO leadership strongly supports this investment because of the importance they place on strengthening enlisted leadership. The goals of the NCOA program are to provide the best academic program possible and to maintain the service's high military standards (MIL-STD). This academy is not a college campus, nor is it an extension of basic military training. It is a professional school designed to educate and advance the high ideals necessary for leadership, teamwork, good order, and discipline in the Air Force. Active duty Airman are required to complete the NCOA in-residence course, while Guard and Reserve Airman can complete through distance learning (DL) or in-residence.

### *Senior Noncommissioned Officer Academy*

The Air Force Senior Noncommissioned Officer Academy (AFSNCOA) is the third level of enlisted EPME. AFSNCOA prepares SNCOs to lead the enlisted force in the employment of airpower in support of United States national security objectives. AFSNCOA is a single in-resident course located at Maxwell AFB–Gunter Annex, along with a DL option, which is available for Guard and Reserve Airmen only.

The AFSNCOA Advanced Leadership Experience (ALE) is a resident Community College of the Air Force (CCAF)-affiliated program that consists of 200 classroom hours. The ALE prepares SNCOs for increased leadership responsibilities in the joint, combined, and interagency operating/strategic environment. Specifically, the AFSNCOA ALE educates SNCOs to help them become adaptable, critically thinking, and strategically relevant leaders in their operating environment. Just like in NCOA, active duty Airmen must complete AFSNCOA by attending the single in-resident course. Air National Guard and Air Force Reserve Airmen will have the option to complete their EPME through DL or in-residence attendance.

### *United States Air Force Chief Master Sergeant Leadership Course*

The United States Air Force (USAF) Chief Master Sergeant Leadership Course (CLC), located on Maxwell-Gunter AFB, AL, consists of 165 hours of facilitated resident learning. The USAF CLC mission is to provide chief master sergeants (CMSgt) the education to bridge operational-to-strategic perspectives of the Air Force. As a result of this executive-level experience (ELE), strategic-level leaders will be equipped to inspire, effectively lead, manage, and mentor our present day and tomorrow's Airmen.

The CLC is the capstone and pinnacle level of EPME. To further expand on the CLC's vision and mission, the strategic-level leadership competencies provided during this ELE will provide our new CMSgts the impenetrable foundation that is instrumental as we fly, fight, and win in the employment of air, space and cyberspace capabilities!

## 003. 1C8X3 Air Force specialty code

So far, you've learned about the AFSC structure and how to progress in the career field. In this lesson, you'll learn about your actual job in the 1C8X3 career field. You'll learn about the duties and responsibilities for your AFSC as a whole. As a new technician, you will be responsible for some of the duties in this section. Other duties and responsibilities in this section you will perform as you grow in rank and technical ability.

## Specialty summary

1C8X3 personnel deploy, install, maintain, and repair fixed or mobile RAWS equipment. RAWS equipment includes: air traffic control (ATC), weather, ground aircraft control and warning radar systems, related radar operator training devices, aircraft identification equipment, remoting systems, video mappers, computerized processors, meteorological, navigation, and ATC ground-to-air radio systems. RAWS technicians operate and relocate related support and communications equipment, uses test equipment, analyzes performance trends, and supervises maintenance activities. You may be required to maintain entire facilities, subsystems, or individual services or equipment that assist in the safe and expedient movement of air traffic throughout the NAS as well as providing support to the National Weather Service (NWS).

## Duties and responsibilities

The members of the 1C8X3 AFSC have a lot of responsibility. RAWS technicians provide critical maintenance and repair to navigational aids, instrument landing systems, and many other pieces of equipment that ensure the safety of air crews when accomplishing their missions. Because of the high level of responsibility, you must perform many duties. The following paragraphs discuss the duties and responsibilities that apply to all levels of the 1C8X3 AFSC.

### *Performs Radar, Airfield & Weather Systems functions*

Many different functions are required of RAWS personnel. These functions are key to running and managing a work center. Your noncommissioned officer in charge (NCOIC) will probably be responsible for most of these functions; however, some may be delegated to personnel in the work center. Some of these functions include the following:

- Plans, organizes, and schedules work assignments, workloads, and maintenance procedures for RAWS.
- Establishes production controls and standards.
- Prepares reports on maintaining, installing, repairing, removing, and siting all types of air traffic control systems.
- Ensures operations and maintenance economies by improving work methods and procedures.
- Designs and develops organizational structures, including manning, duty assignments, and workloads. Inspects and evaluates RAWS activities. Performs or directs all maintenance inspections organized to evaluate base or command maintenance programs. Completes all associated communication electronic research and development projects to modernize, upgrade, or replace RAWS.

### *Installs, removes, and relocates radar, airfield and weather systems*

Technology is constantly advancing; this forces the Air Force to change as well. New technology is developed, new bases are opened, old bases close; there is change going on all the time. In order to keep up RAWS will have to change as well. Your duties may include the following (and more):

- Assembles, connects, modifies, and adjusts electronic subassemblies such as antennas, transmitters, receivers, processors, indicator groups, and ancillary systems.
- Studies system characteristics, local terrain, and planned base facilities and requirements.
- Conducts tests of installed equipment for proper component assembly and compliance with TOs.
- Determines equipment position based on plans, diagrams, and specifications.
- Checks and inventories equipment and project materials for serviceability.
- Performs operational tests.
- Completes flight inspections.

### *Oversees work*

Part of having a successful work center is ensuring the work is done correctly. Several programs in the Air Force evaluate work center performance. However, the most effective method is for the work center to monitor itself. While most of these duties are for experienced/higher level technicians, remember that it is everyone's responsibility to ensure that all work is being done correctly.

- Establishes requirements for maintenance and support equipment, tools, and spare parts.
- Requisitions, accounts for, and turns in supplies and material.
- Diagnoses and recommends equipment repair, replacement, or depot overhaul.
- Certifies RAWS facilities after repair actions or periodic flight inspections.
- Interprets inspection findings and determines publications and procedures.
- Develops and enforces safety standards.
- Evaluates and resolves problems encountered during siting, installing, repairing, and overhauling equipment.
- Interprets maintenance and installation policy and procedures.

### *Repairs, overhauls, and modifies radar, airfield and weather systems*

Regardless of how well equipment is maintained, it will eventually need service. It falls to 1C8X3 personnel of all levels to repair the equipment so it can be put back into operation. This is the largest part of the RAWS technician's job, and the most demanding. Aircraft in the sky depend on RAWS equipment to travel and land safely so when it fails, it must be fixed quickly. You will become very familiar with the duties listed below:

- Isolates malfunctions by prescribed systems checking procedures, visual inspections, voltage checks, and other tests using electronic test equipment.
- Repairs RAWS subassemblies, including antennas, transmitters, receivers, operator training devices, radar beacon systems, remoting systems, video mappers, display systems, and associated communications systems and related equipment.
- Conducts performance tests of repaired subassemblies, using bench mockups, and applicable test equipment.
- Accomplishes organizational and intermediate level equipment modifications according to time compliance technical orders (TCTO) or field directives.
- Assembles, installs, and repairs antenna systems, transmission lines and waveguides.
- Performs corrosion control.

### *Develops methods for improving maintenance*

New equipment is constantly being developed. When new equipment is fielded, the manufacturer estimates maintenance procedures and intervals. RAWS technicians develop recommendations for actual maintenance intervals through maintenance data collection and repair intervals. These recommendations help ensure a reliable maintenance program and result in less equipment downtime.

- Interprets inspection findings, and determines adequacy of corrective actions.
- Ensures maintenance data collection forms, inspection records, and maintenance records are accurately completed.
- Recommends changes to improve equipment performance, maintenance practices, or system interoperability.
- Evaluates justification and practicality of recommended improvements to equipment performance and maintenance procedures.
- Develops and enforces safety standards and practices for RAWS maintenance activities.

- Coordinates with appropriate agencies to ensure systems support requirements.

### *Establish requirements*

Every RAWS work center will have unique requirements based on the equipment it maintains. It's important that the work center have all the tools/supplies necessary based on its requirements. The following actions will help ensure that the work center is equipped appropriately.

- Ensures adequate tools, test/support equipment, personnel, supplies, and technical documents are available.
- Develops work standards, methods, and controls for functions such as periodic inspections, operational testing, and equipment repair.
- Identifies maintenance problem areas and initiates corrective action.
- Maintains inspection and maintenance records.
- Records and reviews meter readings, test results, and historical data in equipment records.
- Completes and reviews maintenance data collection and equipment status reporting (ESR) database.

### *Deploy*

The Air Force may be required to deploy equipment to a variety of locations. The deployment may be in support of a warfighting mission or in response to a natural disaster. In either case, you could be required to deploy at a moment's notice. The job functions listed below will ensure the work center is prepared to deploy when needed:

- Deploys, surveys, sets-up, and activates tactical/mobile RAWS and associated equipment.
- Completes all required maintenance to sustain system operations according to higher headquarters (HHQ) requirements.
- Coordinates with Federal Aviation Administration (FAA) as well as other agencies as needed.
- Reconstitutes and redeploys systems.

For more detail concerning the specific responsibilities for your AFSC, consult Section B, *Career Field Progression and Information*, of your AFSC-specific CFETP.

## Self-Test Questions

**After you complete these questions, you may check your answers at the end of the unit.**

### 001. Air Force specialty structure

1. What is the CFETP and what does it include?

2. Match the term in column B with the correct description in column A. Column B items may be used more than once or not at all.

| *Column A* | *Column B* |
|---|---|
| ____ (1) Integrated bundle of expert knowledge and organizational skills inherent to a particular career field, which makes a disproportionate contribution to the success of providing the right skills needed for military operations, anywhere, anytime. | a. Core task. |
| ____ (2) The tasks assigned to an individual for the duty position currently held. | b. CFETP. |
| ____ (3) The minimum qualification requirement for everyone within an AFSC, regardless of duty position. | c. Core competencies. |
| | d. Duty position tasks. |

3. Who is the final decision authority for CDC waiver requests?

4. What are functions of the TAG?

5. Psychologists at the AAD use what item to build promotion tests and ensure the tests are valid and relevant to the career field?

### 002. Progression within the Air Force Specialty 1C8X3

1. What is the high year of tenure, the maximum amount of time you can stay in the Air Force, as a technical sergeant?

2. How many SNCOPE courses will be conducted annually, at each installation, in an effort to assure 100 percent of eligible have the opportunity to attend?

3. What EPME teaches leadership skills required of supervisors and reporting officials throughout the Air Force?

### 003. 1C8X3 Air Force specialty code

1. What specific AFSC maintains equipment that assists in the safe and expedient movement of air traffic throughout the National Air Space as well as provides support to the National Weather?

2. Why must RAWS equipment be quickly repaired and restored to normal operation?

3. Why would a RAWS technician recommend changes to equipment or procedures?

4. 1C8X3 personnel will complete all required maintenance to sustain deployable systems according to whose requirements?

5. Where can you find details concerning the specific responsibilities for your AFSC?

## 1–2. Management of Processes

Management of a work center requires the use of many different processes. You will need to access multiple information systems and perform several types of evaluations. These processes will not only be needed for the equipment you maintain but also for the personnel in the work center. In this section, you will learn about some of the major processes that are used to keep your work center running effectively and efficiently.

### 004. Automated information systems

Multiple automated information systems (AIS) are used for up-channeling equipment status as well as tracking and documenting repair, troubleshooting actions on- and off-equipment, and documenting training actions of technicians at various levels in their career. The help managers identify equipment trends and determine when items are reaching the end of their effectiveness. It is hard to get through a single day without dealing with at least one of these systems as a technician.

#### Training Business Area

The Training Business Area (TBA) is probably the first AIS you will get to know. It is a net-centric, Web-based application providing Air Force warfighters with global, real-time visibility into the technical qualifications, certifications and training status of logistics, communications and information professionals Air Force-wide. TBA supports base, wing, and work center level training management activities by automating training management business processes. The primary users of TBA will be any personnel directly involved in base level training management and certification activities.

To put it simply, TBA is where all your training documentation takes place. Your supervisor and training manager will assign training tasks to you in TBA. The tasks can be knowledge tasks, or equipment tasks. Once you have completed these tasks, either through reading or through on-equipment training, then you will be signed off in TBA. TBA will then show that your training on that task has been completed.

### Integrated Maintenance Data System

Integrated Maintenance Data System (IMDS) is the standard Air Force base level automated Maintenance Information Management System for managing weapon systems worldwide. The system will support aircraft, communications-electronics, and support equipment maintenance activities at worldwide operating bases, Air National Guard/AF Reserve sites, and selected North Atlantic Treaty Organization (NATO) locations. IMDS provides on-line remote terminals connected to the Standard Base-Level Computer (SBLC) system throughout the maintenance complexes. Integrated Maintenance Data Systems automates aircraft history, aircraft scheduling, aircrew debriefing processes, and provides a common interface for entering base-level maintenance data into other logistics management systems. IMDS is a mission critical system. IMDS current capabilities are automated debriefing, training/personnel, IMDS/supply interface, automated scheduling, Comprehensive Engine Management System (CEMS), inspection/time change, job data documentation (JDD), status and inventory reporting, specialist dispatch, and operational events.

In the late 1980s, IMDS originally started as the Core Automated Maintenance System (CAMS) used by aircraft units to track its maintenance. By the early 1990s, communications squadrons adapted CAMS for tracking their equipment outages, which is why you use IMDS today. The recent development of the graphical user interface (GUI) transformed the remarkably painful CAMS "green screen" experience into a slightly frustrating one. The biggest improvement was the inclusion of look-up wizards that allow you to choose various data codes (e.g., work unit code [WUC], action taken [AT], when discovered [WD], etc.) and enter them into an applicable field.

For a 5-level technician, IMDS will be used mainly for JDD. You will use IMDS on a daily basis. All the equipment systems you work on should be loaded into IMDS. Each system will have a variety of preventative maintenance inspections (PMI) assigned it. PMIs are used to assess the systems health and ensure it is operating properly. Once you have completed a PMI you will update IMDS that the work has been completed. You will also document any on- or off-equipment maintenance in IMDS. As a technician on the equipment it will be your job to make sure any work done on the equipment is correctly documented in IMDS. At any time, you should be able to look up all the systems assigned to your work center and see the current operating status of each system along with jobs that are open for that system.

You can find manuals at the following link: https://ceds.gunter.af.mil/AISHome.aspx?AIS=35

### Global Cyber Support Systems-Dashboard

Global Cyber Support Systems-Dashboard (GCSS-D) provides the ability for users to have an enterprise visibility of ESR, performance metrics, inventory, TCTO reporting, and maintenance documentation within one integrated application.

The purpose of the GCSS-D application is to use the transparent data reporting and analytical capabilities provided by Logistics Installations and Mission Support-Enterprise View (LIMS-EV) for communication-electronic equipment data. It also provides the capability to view/display equipment status and drill-down capability to serial number information from all levels.

GCSS-D retrieves database inputs from various information systems. IMDS takes information entered by the work center and makes it available to the GCSS-D. The GCSS-D is used to display data primarily for external reporting. It provides a standardized view of the communication electronics equipment metrics, which provide a performance and capability measurement. Management metrics are a crucial form of information used by communication leaders to improve the performance of organizations, equipment, and people when compared with established goals and standards. The following lists of some of the information available through the GCSS-D:

- Research a specific type of equipment (i.e., GPN–22 Precision Approach Radar [PAR]) and find out at which bases it is located and how many that each location owns.
- Research where a specific asset is located by searching its serial number.

- Status of the equipment can be displayed (green, amber, or red).
- Current maintenance on the asset can be seen.
- Performance of an asset can be viewed (operational availability, operational dependability, operational readiness, and use rates).
- Inventory of a specific location can be displayed to show all the radar equipment available at a specific base.

The GCSS-D is a valuable tool that offers a lot of functionality. The database is completely customizable to display available information in a number of different ways. The user can save specific "views" so that information can be retrieved easily in the future.

Although the name of the GCSS-D remains the same, the location has changed. It is now part of the LIMS-EV platform. To access the GCSS-D you must select the Air Force Portal Applications A-Z Index and navigate through the index until you locate the LIMS-EV application listing. Access information is provided in the application description.

## 005. Perform self-inspections

Commanders are responsible for unit self-assessment, not the inspector general (IG). Self-assessment provides commanders with a means for internal assessment of a wing's overall health and complements external assessments. At a minimum, commanders must use applicable self-assessment communicators (SAC) in the Management Internal Control Toolset (MICT). However, because SACs only communicate the highest risk areas, commanders are encouraged to include additional measures as directed by superior commanders, functional directives, or proven lessons and experience.

Each program manager will use MICT to record self-assessments and identify individual assessors for each SAC based on the types of questions asked in the SAC. Program managers will not delegate wing-level questions to individual assessors.

Unit inspections are commonly referred to as vertical inspections since they typically stay within command lanes. Vertical inspections are usually conducted at the squadron or group level.

### Management Internal Control Toolset

MICT is the Air Force program of record to communicate a unit's current status of self-assessment communicator (SAC), Headquarters Air Force self-assessment communicator fragmentary order (HAF SAC FRAGO) and special interest item (SII) compliance. In addition, MICT provides supervisors and the command chain, from squadron commander to the Secretary of the AF, tiered visibility into user-selected compliance reports and program status, as well as indications of program health across functional and command channels. Additionally, MICT can assist IGs by informing the risk based sampling strategy and formulating specific inspection methodology and IG team composition for the 'Commander's Inspection Program (CCIP) and unit effectiveness inspection (UEI) Capstone Event. MICT also helps facilitate the SII and HAF SAC FRAGO programs by gathering time-sensitive data in an expeditious manner.

### Self-assessment communicator

A self-assessment communicator is a two-way communication tool designed to improve compliance with published guidance and communicate risk and program health up and down the chain of command in near real-time. Compliance with a SAC does not relieve individual Airmen from complying with all statutory and regulatory requirements in AFIs and directives at the local, state or federal level.

As a self-assessment tool, SACs ask commanders, supervisors, and Airmen at all levels of operations to self-report compliance and non-compliance. While the responses are assumed truthful and timely, SACs are frequently verified for accuracy and currency by wing IGs and MAJCOM IGs.

## 006. Evaluations

The Air Force spends a lot of time and money training personnel to do their jobs. Unfortunately that does not mean people are doing their jobs correctly. Evaluations are used to measure how efficiently something is performing. They allow you to measure how well equipment operates, or how well personnel perform their jobs. In the following lesson, you will learn about several types of evaluations and the purpose for completing them.

### Perform personnel evaluations

The personnel evaluation (PE) program assesses the effectiveness of a work center's training program, technician competence, and technical and procedural data adequacy. These evaluations ensure equipment or systems are maintained in an effective and efficient manner to meet mission requirements. The evaluation can be done on a system, piece of equipment, or on a service-oriented function the technician is qualified to perform (i.e., align radar system, repair navigation system, follow a written process, etc.). Evaluators observe how well processes are performed to determine if the technician demonstrates sufficient skill to accomplish tasks. There are four types of PEs: individual evaluations, unit type code (UTC) evaluations, special evaluations, and equipment evaluations (EE).

#### *Individual personnel evaluation*

Individual PE is completed on all 1C8X3 enlisted personnel within one year of the initial assignment to an organization and upon return to the production work center after an absence of one year or longer. This does not apply to MSgts through CMSgts unless they are task qualified to maintain equipment. Air Force Reserve (AFR) and ANG personnel conduct this evaluation within two years of assignment. For short tour overseas assignments of 18 months or less, individual personnel evaluations (IPE) will be accomplished no later than nine months' time on station.

#### *Unit type code personnel evaluation*

Unit type code personnel evaluations (UTCPE) assess readiness against the UTCPE mission capability (MISCAP) and personnel ensure mission reliability. UTCPEs are completed on all 1C8X3 personnel assigned to UTC-based organizations whose primary mission is to deploy. These evaluations will be completed within 90 days (180 days for ANG/AFR) after an individual is reported as Resource Readiness/Air and Space Expeditionary Force Reporting Tool (ART) qualified by their supervisor. These evaluations can be done during field training exercises and other internal training opportunities. Team UTC PEs is encouraged. These evaluations do not apply to UTCs that do not have an equipment or technical component. This evaluation can be accomplished in conjunction with the initial PE and/or replace the initial PE. If an individual is permanently reassigned to another UTC or the primarily assigned UTC has major changes (e.g., equipment replacement, new tasks identified) another UTC PE is required.

#### *Special personnel evaluation*

Special PEs (SPE) are conducted on an as-needed basis. Commonly these evaluations are conducted after major modifications of equipment and systems, or reevaluation of an individual who received a not in compliance result from a previous evaluation, or who has had his/her qualification status revoked for any reason other than supervisor decertification. SPEs are required on a sampling of personnel within 60 days of new equipment or system acceptance (120 days for Air Reserve Component [ARC]).

#### *Equipment personnel evaluation*

Equipment personnel evaluations are conducted to make sure technicians meet proficiency requirements. The evaluation must assess the technician's ability to determine when equipment should be taken out of service and under what conditions the equipment or facility can be returned to service. Evaluations should measure the technician's capability to perform standard maintenance

practices and troubleshooting processes. Evaluations should be done during UEI Capstone events at the inspector's discretion, unless prescribed by a formal agreement.

### Evaluate equipment

Equipment evaluations give an overall view of the quality of RAWS maintenance. EEs ensure adequate actions are taken to meet expected standards of quality. They also provide useful data for identifying training deficiencies and potential problem areas. EEs are performed in enough depth to ensure equipment and systems are maintained and managed according to applicable technical data and standards. The evaluation of systems maintained by the work center will be conducted as part of the Air Force Inspection System (AFIS) by completing the applicable portions of the self-inspection checklist in the MICT database. During the UEI Capstone event, the respective IG team will validate and verify the results of the unit's self-inspections.

AFI 13–204, Volume 4, *Management of Ground Radar and Airfield Systems*, Attachment 4, *Sampling Plan*, can be used for EEs consisting of multiple like items. Special equipment evaluations (SEE) on RAWS equipment can be achieved through using Airfield Operations Compliance Inspection (AOCI) checklists or through submitting a request for maintenance assistance to the servicing regional maintenance center (RMC). For Deployment Air Traffic Control and Landing Systems (DATCALS), there is no requirement for a separate equipment evaluation, only UTC evaluations.

In the 1C8X3 career field, EEs are usually divided into 4 types: core equipment, other/ancillary equipment, UTC, and special. EEs are conducted using Air Force maintenance quality control checklist (AFMQCC)/MICT. Use as many checklists as applicable to the equipment being evaluated. Commanders may authorize the substitution of pre/post deployment inspections to satisfy the requirements for an equipment evaluation. Such substitutions must be approved in writing and the pre/post deployment inspection must be observed by quality assurance (QA) and QA representative (QAR) personnel.

Scheduling for subsequent EEs will be adjusted from the pre/post deployment inspection date. Equipment evaluation reporting still applies.

#### *Core equipment evaluations*

A core EE is accomplished on equipment, systems, and infrastructure devices/items or processes that have grave effect(s) on base/key organization's mission and day-to-day operations if not fully mission capable. Generally, these items are listed in the base restoral plan, mission essential listing, and/or are one-of-a-kind items. These systems could prevent mission success (e.g., main satellite communications terminal) and/or prevent the base from meeting its operational capability. Personal voice, video, and data devices are excluded from this requirement (e.g., radios, cell phones, pagers, laptops, desktop computers, and other personal electronic devices).

Every 18 months, QA or a QAR will evaluate all core base voice, video, data transport, and transmission systems (e.g., voice switch, distribution nodes, AF-owned technical control systems, etc.). Each item is reviewed for technical parameters; grounding, bonding, power, corrosion, standard installation procedures, and operations according to applicable AFMQCCs/MICT.

#### *Other/ancillary equipment evaluations*

Other/ancillary EEs are accomplished on systems and equipment not meeting the definition of core equipment that are maintained or supported by 1C8X3. Examples include communications closets, command post radios, and so forth.

Every 24 months, a sample of other/ancillary base voice, video, data transport, and transmission systems (e.g., transmitters, receivers, comm. closets, etc.) will be evaluated by QA according to AFI 13–204, Attachment 4, *Sampling Plan*. The inspected systems are reviewed for technical parameters, grounding, bonding, power, corrosion, standard installation procedures, and operations, according to applicable AFMQCCs/MICT. Personal voice/video/data devices are excluded from this requirement

(e.g., land mobile radio (LMR), secure mobile environment-personal electronic devices (SME-PED), cell phones, pagers, laptops, desktop computers, etc.).

#### *Unit type code equipment evaluations*

A unit type code equipment evaluation (UEE) is accomplished on equipment and systems that are critical and/or one-of-a-kind that, if degraded, disrupt key operations. Equipment/systems within UTC-based organizations are equipment/systems that would prevent mission success (e.g., main satellite communications terminal, Promina, large voice) and/or prevent the UTC from meeting its MA. The unit's senior cyber official associated will approve and document the potential items for evaluations per assigned UTC unless otherwise identified by a higher authority. Personal voice, video, and data devices are excluded from this requirement (e.g., LMR, SME-PEDs, cell phones, pagers, laptops, desktop computers, etc.).

Every 18 months, QA or QAR will evaluate a sample per AFI 13–204, Volume 4, attachment 4, of voice, video, data transport, and transmission systems (e.g., voice switch, distribution nodes, Promina, crypto module, etc.) and/or equipment assigned per UTC within the organization. For example, a combat communications squadron has 15 UTCs. Each UTC has 25 pieces of voice, video, data transport and transmission systems. Of the 25 pieces, the senior cyber officer identified 11 pieces for evaluation. Based on the sampling plan in AFI 13–204 Volume 4, QA or the QAR would only evaluate four pieces during the first 18-month period. Each item is reviewed for technical parameters, grounding, bonding, power, corrosion, standard installation procedures, and operations according to applicable AFMQCCs/MICT. Evaluators select equipment not previously evaluated during the last UEE period. Units are encouraged to perform these evaluations during training exercises, pre-deployment inspections, or recurring PMIs to minimize packing and unpacking equipment.

#### *Special equipment evaluation*

Special equipment evaluations are evaluations on any type of applicable equipment or when determined to be required by unit leadership or QA. Any equipment/system outgoing or incoming, including in-process inspections to an organization, or deemed by unit leadership is required to have a SEE excluding personal voice/video/data devices (e.g., LMR, PEDs, cell phones, pagers, laptops, desk top computers, etc.). If the equipment/system is new to the Air Force and used by more than one MAJCOM, an AFMQCC is required. MAJCOMs will develop MAJCOM Local Quality Control Checklists (LCQCC) for MAJCOM-unique systems. The MFM will notify A3CF/A6CF if the new equipment/system is used by more than one MAJCOM. Unit commanders determine other SEEs. RAWS special-acceptance inspections will be conducted by AFFSA/A3M; normally, it's the personnel assigned to a RMC conducting the inspections: specialized communications team (SCT) and Air Force Engineering and Technical Services (AFETS). QA personnel or a QAR will complete these evaluations whenever determined by unit leadership and/or within 60 days after the equipment arrives or up to 60 days of equipment being transferred between units.

## 007. Document results

Once the evaluation is completed, it must be documented. Documenting the results is extremely important. These results are used to track problems, diagnose cause, and make sure improvements are made. Without proper documentation, the evaluation is useless.

### Report writing

To determine overall results, evaluators will review notes and captured examples, then validate references. Results are based on overall process performance. The following is what evaluators must do:

- Document all evaluation task deficiencies including corrected-during-evaluation (CDE) corrections.
- Track all deficiencies for trend analysis using standardized codes to include CDEs. The decision to document a deficiency must be based on published standard practices and

procedures, technical data, and other policy guidance.

- Make sure all validated deficiencies include a deficiency code and a category rating of either critical (CAT I), major (Cat II), or minor (Cat III) based on AFI 13–204, Volume 4, table A2.1.
- Rate each task included in the overall evaluation. All deficiencies are then totaled and assigned an overall task result according to AFI 13–204, Volume 4, table A2.2, *Personnel Evaluation Task Result Matrix*. Results are based on the following three-grade system: in-compliance ($C^2$), complies-with-comments (CWC), or not in compliance (NIC), per AFI 13–204, Volume 4, table A2.2. Technicians will be decertified on tasks rated NIC.
- Personnel evaluations that contain no (zero) NIC tasks are rated as "Satisfactory." Evaluations that contain one or more NIC tasks are rated as "Unsatisfactory."
- Brief the evaluatee and the work center supervisor upon determining the evaluation resulted in one or more NIC task ratings.

  **NOTE:** An evaluation that resulted in one or more NIC-rated tasks requires an investigation to determine the root cause of the identified deficiencies for each NIC task, and initiation of the decertification process on those respective tasks. See AFI 36–2651, *Air Force Training Program*, for more details.
- Develop an executive summary of what was evaluated, the overall result (satisfactory or unsatisfactory), a comment about the technician's performance, strengths and weaknesses, and a deficiency trend analysis to include root causes and recommended management actions to prevent recurrence.

### Report submission

Document PEs on AFMQCC 100–1, *Personnel Evaluation Report*, or an automated substitute according to AFI 13–204, Volume 4, attachment 2. Comments and recommendations are made on the evaluation report to eliminate the need for separate correspondence. The report also provides a source for analyzing the effectiveness of the overall training program. The following are things that need to be done when documenting personnel evaluations:

- Identify task deficiency codes and results, provide additional comments and references to each deficiency code, provide recommendations, and explain rescheduling actions, if required. Explain management, system or equipment deficiencies not directly reflecting on job performance in a separate special equipment report.
- The unit commander's review of all evaluation reports with an overall result of unsatisfactory. All other reports are reviewed at commander's discretion.
- If an individual's UTC evaluation result is unsatisfactory, the unit commander determines whether the individual's Status of Resources and Training System (SORTS)/ART status is changed.
- PE reports will be routed only once through the routing chain. At a minimum, include the evaluated individual, individual's supervisor, work center supervisor, and unit training manager (UTM). For reports with an overall result of unsatisfactory, also include the unit commander and flight commander/superintendent. Reports will be closed within 30 calendar days from the date of evaluation as indicated on the AFMQCC 100–1. The closing authority for "Satisfactory" evaluations is the evaluator that performed the evaluation. The closing authority for "Unsatisfactory" evaluations is the unit commander or their designated representative.

The work center supervisor or the UTM will annotate the PE date completion in IMDS. Supervisors will annotate the PE completion date as a journal entry in TBA.

## Self-Test Questions

**After you complete these questions, you may check your answers at the end of the unit.**

### 004. Automated information systems

1. What information system supports base, wing, and work center level training management activities?

2. What two AISs can be used to view the status of the equipment assigned to a work center?

3. What information system uses inputs from various sources and provides the capability to view equipment status and drill down capability to serial number information from all levels?

### 005. Perform self-inspections

1. Who is responsible for unit self-assessments?

2. What provides supervisors and the command chain, from squadron commander to SAF, tiered visibility into user-selected compliance reports and program status, as well as indications of program health across functional and command channels?

3. What is used as a two-way communication tool designed to improve compliance with published guidance and communicate risk and program health up and down the chain of command in near-real-time?

### 006. Evaluations

1. What program assesses the effectiveness of a work center's training program, technician competence, and technical and procedural data adequacy?

2. Which evaluation does not apply to MSgt-CMSgt unless they are task qualified to maintain equipment?

3. How often are SPE conducted?

4. What do equipment personnel evaluations measure?

5. What is the purpose of an EE?

6. What type of evaluation is accomplished on equipment, systems, and infrastructure devices/items or processes that have grave effects on base/key organizations mission and day-to-day operations if not fully mission capable?

7. How often are ancillary EEs performed?

8. Who will conduct special acceptance inspections for RAWS equipment?

### 007. Document results

1. Which category rating indicates a critical evaluation deficiency?

2. What evaluation report is used to document a PE?

3. Within how many days will a PE report be closed?

## 1–3. Organizational Structure

The Air Force uses standard levels described in AFI 38–101, *Air Force Organization*, chapter 2, to design organizations. Organizations are established at the lowest level required to successfully accomplish the primary mission. Factors such as scope of responsibility, span of control, and functional grouping of related missions/activities are the predominant factors that determine organizational type. In this section, you will learn some of the basic organization types that you will deal with during your career. See figure 1–2 to find out how you fit into the overall AF organizational structure.

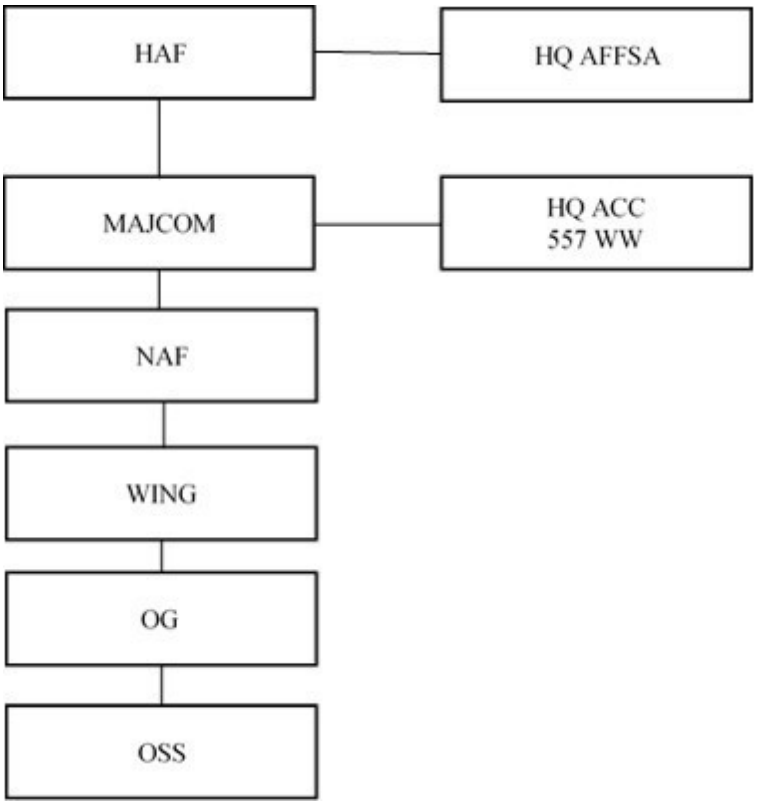


**Figure 1–2. Organizational structure.**

## 008. Operations support squadron

The operations support squadron (OSS) is centered on the flying mission of the United States (US) Air Force. Its role is to provide support to operations squadrons in designated areas. These designated areas are discussed below.

### Weapons and tactics flight

The weapons and tactics flight (OSK) develops procedures and unit tactics for planning and employing operational mission and wing assets. It advises wing staff on operational capabilities, limitations and status of resources.

### Airfield operations flight

The airfield operations flight (OSA) provides airfield management and air traffic operations services to the base flying wing transient and civil users. These services can include control tower, radar operations and base operations functions.

### Current operations flight

Responsible for all wing-flying operations, the current operations flight (OSO) monitors and directs flying, scheduling and training. It manages the flying hour program, flight simulator systems and provides centralized flight records support. The OSO coordinates wing combat mission planning and sortie allocation. It also provides inspection support and coordinates deployment requirements for the operations group.

### Aircrew flight equipment flight

The aircrew flight equipment flight (AFE) performs functions that enhance aircrew performance and preserve human lives. It does this by ensuring proper integration of the weapon system equipment and the personnel. It issues, fits, repairs, and maintains critical mission performance and lifesaving equipment such as: parachutes, helmets, nuclear flash/thermal protection devices, oxygen equipment,

anti-gravity garments, anti-exposure suits, aircrew ocular devices, survival kits, life preservers, rafts, electronic communications, helmet mounted weapons integration devices, and aircrew chemical, biological, radiological, nuclear (CBRN) equipment. The AFE flight also instructs aircrew on the proper use and care of equipment under normal, contingency, and CBRN operations. In order to mitigate aircrew contamination; it maintains and sets up aircrew contamination control areas, and processes aircrew through them.

### Weather flight

The weather flight (OSW) provides weather services for all operations on base as well as all activities supported by the base and reserve component activities as directed. It prepares and disseminates weather information for base resource protection from severe weather and other environmental effects. OSW provides weather inputs into the Department of Defense (DOD) databases to support DOD operations worldwide providing tailored weather inputs to satisfy specific combat operations and weapon system requirements.

### Intelligence flight

The intelligence flight (IN) provides support for the wing during all phases of conflict and decision making. It trains aircrew/operators and prepares the wing for contingency and wartime missions. The flight is tailored to the wing's operational mission and base support activities. This allows it to provide full-spectrum threat assessments and mission planning in support of deployments, contingencies, and combat operations.

### Radar, Airfield & Weather Systems

RAWS provides maintenance support of wing, transient and civil air operations. These services include maintenance of legacy radar, navigational aids, weather, and air traffic control radio systems. Flight personnel also provide limited support for systems maintained by RMCs.

## 009. Air Force Flight Standards Agency

The Air Force Flight Standards Agency (AFFSA) maximizes the effectiveness of Air Force global air operations by ensuring access to worldwide airspace in all weather conditions. AFFSA does this by providing accurate, relevant, and timely flight information and support services to DOD, national, and coalition aviators. It also acts as lead command for the creation and application of criteria, procedures, and precision equipment for worldwide instrument flight operations, ATC, airfield management, and ATC and landing systems for the Air Force. AFFSA evaluates and capitalizes on emerging technologies to ensure unrestricted access to domestic and international airspace. It is located at Will Rogers International Airport along with the Federal Aviation Administration. AFFSA partners with the FAA, sister services, MAJCOMs, coalition partners, and host nations to maintain the consistency and accuracy of more than 81 airfields, 1,092 navigation systems, and 8,214 instrument approach procedures worldwide. It performs combat flight inspections, oversees the Air Force airfield operations standardization program and instructs the Air Force Advanced Instrument School.

### System management

Lead command system managers (LCSM) provide an AF focal point for maintenance and sustainment support for common communications equipment/systems. LCSMs ensure common systems are reliable, maintainable, and available to meet mission needs by providing all levels of support. They are in direct communication with the field units, program management offices (PMO), RAWS system program office (SPO), logistics and acquisition communities, depots, lead commands cyber systems integrators, AFETS, Engineering and Installation (E&I) community, the MAJCOM SME, and AFCFM. Basic system management duties and responsibilities include, but are not limited to, the following items.

- Work with MAJCOM SME to ensure equipment/systems are available to meet mission requirements.
- Understand the reason for, and role of, designated lead commands (LC) and develop/maintain close working relationships with them for their designated systems.
- Develop and maintain a point of contact (POC) list for all Item/Program Managers, MAJCOM Staff, and all maintenance work centers within each MAJCOM. Use of an organizational inbox is the preferred contact method for initial e-mail correspondence to and from the LCSM.
- Stay abreast of related technological changes in order to manage effectively the equipment/systems for which they are responsible.
- Address HHQ inquiries and act as SME to support system development, sustainment, and logistical support.
- Research, develop courses of action, and provide recommendations on life cycle management of fielded systems.
- Provide logistical SME support by conducting reviews of the Air Force Equipment Management System (AFEMS), Allowance Source Code (ASC), and other supply approved information systems. Provide change/improvement recommendation to MAJCOMs or individual organizations.
- Interpret policy and procedures for requesting organizations.
- Assist with development of AFMQCC, Air Force maintenance special instructions (AFMSI), other inspection checklists, and policy. See AFI 13–204, Volume 4, attachments 5 and 6, for a list of AFMQCCs and AFMSIs.
- Participate in maintenance and logistics community working groups, conferences, and seminars (e.g., Product Improvement Working Groups [PIWG], WSR, supply summits, allowance source code review, etc.).
- Conduct data calls for LCs, HHQ, MAJCOMs, and lateral agencies. Draft requests, validate responses, consolidate information, conduct data/root cause analysis, and provide detailed report.
- Assist in revision of system policy, training, and guidance documents (i.e., technical order (TO), Air Force Job Qualification Standard (AFJQS), Air Force Qualification Training Package (AFQTP), AFIs, CFETP, CDCs, STS, as well as other documents impacting fielded systems.
- Review system/equipment documentation for policy and procedural implications and coordinate legal review.
- Coordinate and resolve ESR and JDD issues with applicable organizations.
- As requested, augment MAJCOM IG.
- Coordinate operational issues that affect mission degradation with lateral agencies (e.g., LC, SPO, PMOs, primary contracting officer, FOAs, 38th Cyberspace Engineering Installation Group [CEIG], AFETS, and associated system depot offices).
- Assist with new system requirements from LC, MAJCOM or unit. LCSM coordinates requirements with appropriate agencies, provides comprehensive recommendation, and forwards validated requirement to appropriate office.
- Coordinate and process system modification request per TO 00–5–1, *AF Technical Order System*, and AFI 63–101/20–101, *Integrated Life Cycle Management*.
- Provide SME support on system/equipment life cycle management plans.

- Provide technical input, requirements, and assessment on system/equipment contracts. LCSMs may also provide source selection recommendation/technical assessment.
- Review system/equipment architecture and technical information from equipment manufacturer/lateral agency to ensure fielded systems are reliable, available to meet mission needs, and logistically supportable.
- Assist in health of fleet reporting.
- Validate discrepancy notices and recommend potential solutions.

### Regional maintenance center

The RMC ensures safe, reliable RAWS performance for non-remote and remotely maintained systems. The RAWS support includes the three fixed-base RMCs in the European, Pacific, and continental United States (CONUS) theaters. HQ AFFSA/XMR manages all three RMCs in support of the using commands and local base units.

The CONUS RMC (HQ AFFSA/XMRC) is located at Oklahoma City, OK, and services the continental US as well as Greenland, and South and Central America. The European RMC (HQ AFFSA/XMRE) is located at Kapaun AB, Germany and service sites in Europe and Africa. The Pacific RMC (HQ AFFSA XMRP) is located at Yokota AB, Japan, and service sites in the Pacific, including Alaska and Hawaii.

The appropriate RMC will provide maintenance support/monitoring for remote maintenance systems. All RMCs maintain equipment within their respective region, but can be called upon to support other regions. The RMCs will provide all traditional AFETS, specialized maintenance team (SMT), and RAWS radar evaluation support for all units. Duties and responsibilities of key positions in the RMC can be found below; this does not include all positions of the RMC.

#### *Team chief*

The team chief will lead maintenance actions during RAWS site visits, equipment restorations, and installations. He or she is responsible for selecting an appropriate team based on skills and number of technicians requires. The following are key duties of the RMC team chief:

- Schedule all annual site visits, restorals, installations, and site surveys.
- Review and interpret all facility reference and site data before any site visit and equipment maintenance.
- Notify and coordinate all equipment downtime and notice to Airmen (NOTAM) schedules with site agencies responsible for system status.
- Notify and coordinate with local work centers for all assistance with remote or on-site maintenance on all affected systems.
- Schedule and confirm any flight checks necessary for any equipment restorations or installations before trip departure date.
- Conduct in-brief/out-briefs with respective operations agencies for all site visits.
- Ship all tools and test equipment before departure. Make sure all shipping documentation has been accomplished for departure and return shipments.
- Collect and document all data on appropriate equipment forms after any maintenance is performed.
- Make sure all changes to facility reference data is verified, documented, and input into approved databases. (Verify by ground checks or necessary flight check).
- Confirm equipment configuration files are up to date and saved to any predesignated file share locations.

### *Technician*

The RMC technician will maintain RAWS equipment and perform all assigned RMC tasks as directed by RMC team chiefs/supervisors. They are responsible for assisting with site visits, conducting alignments and repairs, as well as modifications of RAWS equipment. The technician is the one doing most of the work when you call for equipment restoral assistance. The duties of the technician include the following:

- Use specialized test equipment and software-controlled diagnostics to tune, align, and adjust RMC equipment
- Install, maintain, and modify RMC equipment according to the applicable TO procedures.
- Conduct flight inspections, performance tests and evaluate results to ensure proper system operation.
- Perform preventive maintenance on RAWS equipment and initiate action to correct unsatisfactory equipment performance trends.
- Record and maintain inspection and maintenance records.

### *Air Force Engineering and Technical Services/specialized maintenance team*

The Air Force Engineering and Technical Services/specialized maintenance team provides technical assistance, training, and emergency on-site assistance for all non-remote systems. Initial response to an on-site assistance request from the unit will be as soon as possible after request is received by HQ AFFSA by MAJCOM. Restoral priorities for non-remote systems will be handled on a first-in, first-out basis and according to MAJCOM MOA. The corresponding MAJCOM will be notified when an AFETS/SMT technician will respond to an on-site emergency assistance request for non-remote systems. Some of the AFETS/SMT duties include:

- Respond to and prioritize requests for on-site support.
- Provide telephone support to field technicians during normal duty hours.
- Provide on-site outage response when outages exceed field technicians' abilities.
- Provide training support on-site as requested
- Provide SME for analysis of complex problems, flight check failures and engineering requests.

### *Radar, Airfield & Weather Systems evaluations work center*

The RAWS evaluations work center provides technical assistance, training, and emergency on-site assistance for terminal ATC radar systems. The initial response to an on-site assistance request from the unit will be as soon as possible after the request is received by HQ AFFSA from the requesting MAJCOM. Radar evaluations will also assist units with commissioning activities for new/relocated radar facilities. Some of the work centers additional duties are as follows:

- Provide first-call response to system outages in conjunction with RAWS AFETS/SMT. Coordinate restoral efforts if second-level assistance is required (e.g., FAA second-level engineering, Standard Terminal Automation Replacement System [STARS] Operational Support Facility).
- Provide technical expertise to PMO or LCSM for technical instruction changes, system modifications, procedure development, operational requirements development, and operational testing.
- Re-optimize/certify radar systems following changes to the system, radar environment, or mission (e.g., new construction, changes to assigned airspace).
- Provide pre-construction analysis of potential radar impacts related to construction of new buildings, solar farms, and wind turbines according to AFI 13–201, *Airspace Management*. Assist units with post-construction mitigation to reduce or eliminate impacts.

- Monitor the FAA Obstruction Evaluation/Airport Airspace Analysis (OE/AAA) system for wind turbine projects near CONUS terminal radars.
- Provides representative to Air Staff Encroachment Management Working Group/Mitigation Response Team (EMWG/MRT) according to AFI 90–2001, *Encroachment Management.*

## 010. 557th Weather Wing

On March 27, 2015, the Air Force Weather Agency was officially re-designated as the 557th Weather Wing (WW). As such, the 557 WW stands alone as the Air Force's premier WW, providing world-class weather support and decision superiority to commanders and warfighters to "win today's and tomorrow's fight." This change came about because of an Air Force organization management headquarters review announced in 2014. The 557 WW reports directly to the 12th Air Force under Air Combat Command.

The mission of the 557 WW is to maximize America's power through the exploitation of timely, accurate, and relevant weather information: anytime and everywhere. Headquartered at Offutt Air Force Base, Nebraska, the 557 WW is comprised of nearly 1,500 personnel: the 1st Weather Group (WXG) as well as the 2 WXG, 11 squadrons, five detachments, and five operating locations. The 557 WW strategic vision is world-class Airmen, the DOD's provider of choice for innovative, actionable and authoritative terrestrial and space weather information to win the fight—today and tomorrow.

### 1st Weather Group

The 1 WXG is comprised of six operational weather squadrons (WS) providing timely, accurate, and relevant weather operations around the clock in support of joint warfighters worldwide. Each squadron produces decision-quality forecasts and weather threat assessments for aviation and ground forces tasked to fulfill specific geographic combatant command, service component, and international partner operations. The 1 WXG also includes Operating Location Kilo (OLK), which is responsible for managing the DOD's portion of the next-generation weather radar program. OLK works alongside NWS and FAA professionals to engineer, maintain and sustain over 160 Doppler radars worldwide as part of a tri-agency agreement with the Department of Commerce and Department of Transportation.

Around the world, operational WSs provide weather support covering a specified region of the world. Professional meteorologists and weather technicians operate the squadrons around the clock ensuring continuous monitoring of any terrestrial and space weather activity. They are responsible for producing and disseminating mission planning and execution weather analyses, forecasts, and briefings for Air Force, Army, Guard, and Reserve forces operating around the world proving installation commanders advanced warning of severe weather to protect personnel, weapon systems and infrastructure. The following table is a list of the 1 WXG locations and their area of responsibility.

| 1st Weather Group | |
|---|---|
| **Squadron** | **Area of Responsibility** |
| 15th Operational Weather Squadron | 120 installations/sites in a 22 state region of the northeastern United States. |
| 17th Operational Weather Squadron | 95 million square miles of the Pacific region including Australia, Korea, and Japan. |
| 21st Operational Weather Squadron | Europe, Greenland, and most of Africa. |
| 25th Operational Weather Squadron | 68 installations/sites in an 11 state region of the western United States. |
| 26th Operational Weather Squadron | 70 installations/sites in a 7 state region of the southeastern United States. |

| 1st Weather Group | |
|---|---|
| **Squadron** | **Area of Responsibility** |
| 28th Operational Weather Squadron | Sites throughout Central Command including southwest Asia and the Horn of Africa. |
| Operating Location Kilo - Radar Operations Center | Currently consists of 6 active duty military members and 8 Air Force civilian employees working with the other agencies in the Radar Operations Center. |

## 2d Weather Group

The 2 WXG delivers timely, relevant, and specialized terrestrial, space, and climatological environmental intelligence to joint forces, defense agencies, DOD decision-makers and allied and coalition partners worldwide to plan and execute missions across the range of military operations. The group operates, sustains, maintains, and monitors the wing's $303M strategic high-performance computing complex, production network and applications and provides DOD's only space weather operations center, climate monitoring and prediction capability and environmental data for Live, Virtual and Constructive modeling and simulation. The WXG exploits leading-edge weather forecasting models and provides fielded weather systems experts for operational testing, deployment training, and deployed maintenance on tactical weather systems.

The 2d WXG is comprised of 6 primary subordinate units: 2d Weather Squadron, 2d Systems Operations Squadron, 16th Weather Squadron and Detachment 1, 2d WXG are located at Offutt Air Force Base, Nebraska. 2d Combat Weather Systems Squadron is located at Hurlburt Field, Florida, and 14th Weather Squadron in Asheville, North Carolina. In addition, four solar observatories fall under 2 WXG at Learmonth, Australia; Sagamore Hill, Massachusetts; Holloman AFB, New Mexico; and Kaena Point, Hawaii. The following table is a list of the 2 WXG units and a description of each.

| 2d Weather Group | |
|---|---|
| **Squadron** | **Mission** |
| 2d Weather Squadron | Continuously supports Joint warfighters and DOD decision-makers, including the intelligence community and space operators with accurate, relevant, timely and specialized global terrestrial and space observations, analyses, forecasts and alerts.<br>• 2 WS, American Forces Network (AFN) Weather Center<br>• 2 WS, Radio Solar Telescope Network<br>• 2 WS, Solar Observing Optical Network |
| 2d Systems Operations Squadron | Delivers reliable and timely global environmental intelligence products and services for the defense of the United States of America and its global interests; and operates and sustains the Air Force's $303M strategic weather high performance computing center to deliver authoritative environmental intelligence to decision makers across the spectrum of global operations. |
| 2d Combat Weather Systems Squadron | Performs operational test and evaluation of Air Force fixed-based and tactical weather systems, train weather and communications Airmen for deployed operations, and provide combat weather system maintainers to enable worldwide military operations. |
| 2d Weather Support Squadron | Performs operational test and evaluation of Air Force fixed-based and tactical weather systems, train weather and communications Airmen for deployed operations, and provide combat weather system maintainers to enable worldwide military operations. |
| 14th Weather Squadron | Aligned under the 2d Weather Support Squadron. The Air Force's only climate operations unit that collects, protects, and exploits authoritative climate data to optimize military and intelligence operations and planning in order to maximize the combat effectiveness of DOD personnel and weapons systems. |

| 2d Weather Group | |
|---|---|
| **Squadron** | **Mission** |
| 16th Weather Squadron | The center of excellence for developing, implementing, and visualizing terrestrial, atmospheric and space weather models; displaying observational and model data, and identifying environmental impacts on future weapons systems. |

## 011. Deployable squadrons

Most squadrons in the Air Force are fixed squadrons; they are assigned to a base within the CONUS or OCONUS and that is where they perform their primary duties. Occasionally the Air Force needs to send a specialized unit to a forward location to support a conflict, or restore capabilities after a natural disaster. That is where ATC squadrons and air control squadrons (ACS) are required. They are specially trained units that can pick up, transport their unit, and set up their equipment anywhere in the world in a very short time.

### Air traffic control squadron

The air traffic control squadron (ATCS) mission is to provide the United States Air Force with trained personnel ready to deploy and provide air traffic services for worldwide contingencies. There are ten squadrons, which are components of the ANG and operate out of the following locations:

| Air National Guard, Air Traffic Control Squadron Locations | | |
|---|---|---|
| 235 ATCS New London, NC | 248 ATCS Meridian, MS | 270 ATCS Klamath Falls, OR |
| 241 ATCS St Joseph, MO | 258 ATCS Johnstown, PA | 297 ATCS Kapolei, HI |
| 243 ATCS Cheyenne, WY | 259 ATCS Alexandria, LA | |
| 245 ATCS McEntire ANGB, SC | 260 ATCS Portsmouth, NH | |

These units maintain, operate, and deploy RAWS equipment systems in support of their state and also worldwide in support of operational forces at host nations or bare base locations. They provide basic airfield services and combat airspace support to the Theater Air Operations Center. Certain capabilities that are provided are the ability to identify, sequence, separate aircraft, and provide final approach guidance and control instructions to aircraft in all types of weather. These units are activated as required by operations tempo.

The 53 ATCS, based in Robins AFB, Georgia, is the only active duty ATCS in the Air Force. They provide the same level of service as the Air National Guard bases listed above, but do so utilizing active duty Air Force members. 53 ATCS provides Deployable Air Traffic Control and Landing Systems (DATCALS) when a Combatant Commander needs to establish a new airfield, project airpower into contested areas or supplement existing air traffic control systems. 53 ATCS also has the capability to support Humanitarian Assistance/Disaster Relief efforts (HA/DR). Equipment and personnel can deploy within 72 hours of a “prepare to deploy” order.

### Air control squadron

An air control squadron provides a mobile, combat-ready, senior radar element of the Theater Air Control System for worldwide contingencies. Additionally, it provides combat and control of joint air operations by conducting surveillance identification, weapons control, theater missile defense, battle management, and theater communications data links. These squadrons provide the theater Air Force commander a rapid reaction mobile air control system and control/ reporting center during worldwide contingencies.

## Self-Test Questions

**After you complete these questions, you may check your answers at the end of the unit.**

### 008. Operations support squadron

1. Which operational support flight advises wing staff on operational capabilities, limitations and status of resources?

2. Maintenance of radar, navigational aids, weather, and ATC radio systems is performed by which operational support flight?

### 009. Air Force Flight Standards Agency

1. What agency acts as the lead command for the creation and application of criteria, procedures, and precision equipment for worldwide instrument flight operations, ATC, airfield management, and ATC and landing systems for the Air Force?

2. Where is the AFFSA located?

3. What support does the RMC provide to all units?

4. For what is the RMC technician responsible?

5. What function does AFETS/SMT provide?

6. How are restoral priorities determined for non-remote systems?

7. Who provides first-call response to system outages in conjunction with radar AFETS/SMT?

### 010. 557th Weather Wing

1. What is the mission of the 557 WW?

2. How many operational weather squadrons does the 1 WG contain?

3. What information does the 2 WG deliver?

### 011. Deployable squadrons

1. Deployable squadrons are specially trained to perform what task?

2. What is the mission of an ATCS?

3. An ATCS provides what service?

## Answers to Self-Test Questions

### 001

1. The CFETP is the core document specifying the required training for enlisted personnel in an AFSC.

   The CFETP outlines the initial skills, upgrade, qualification, advanced, and proficiency requirements for individuals in specific AFSCs in order to develop skills and promote career progress.
2. (1) C.

   (2) D.

   (3) A.
3. Air Force career field manager.
4. (1) Set training goals and priorities.

   (2) Review training programs impacting the communications and information community.

   (3) Evaluate emerging training, training tracking, and technologies.
5. Occupational Survey.

### 002

1. 20 years.
2. Minimum of two.
3. ALS.

### 003

1. 1C8X3.
2. Aircraft in the sky depend on RAWS equipment to travel and land safely.
3. To improve equipment performance, maintenance practices, or system interoperability.
4. Higher headquarters.
5. CFETP for your AFSC.

### 004

1. Training Business Area.
2. Integrated Maintenance Data System and Global Cyber Support Systems Dashboard.
3. Global Cyber Support Systems Dashboard.

### 005

1. Commanders.
2. Management Internal Control Toolset.
3. SAC.

### 006

1. Personnel evaluation program.
2. Individual personnel evaluation.
3. On an as-needed basis.
4. The technician’s capability to perform standard maintenance practices and troubleshooting processes.
5. To give an overall view of the quality of RAWS maintenance.
6. Core equipment evaluation.
7. Every 24 months.
8. AFFSA/A3M.

### 007

1. CAT I.
2. AFMQCC 100–1.

3. 30 calendar days.

**008**

1. Weapons and tactics flight.
2. Radar, Airfield and Weather Systems.

**009**

1. Air Force Flight Standards Agency.
2. Will Rogers International Airport.
3. Traditional AFETS, SMT, and RAWS radar evaluation.
4. Assisting with site visits, conducting alignments and repairs, and modifications of RAWS equipment.
5. Technical assistance, training, and emergency on-site assistance for all non-remote systems.
6. First-in, first-out basis and according to MAJCOM MOA.
7. RAWS evaluations work center.

**010**

1. To maximize America's power through the exploitation of timely, accurate, and relevant weather information; anytime, everywhere.
2. Six.
3. Timely, relevant and specialized terrestrial, space and climatological environmental intelligence to joint forces, defense agencies, DOD decision-makers and allied/coalition partners worldwide for planning and execution of missions across the range of military operations.

**011**

1. To pick up, transport their unit, and set up their equipment anywhere in the world in a very short time.
2. To provide the United States Air Force with trained personnel ready to deploy and provide air traffic services for worldwide contingencies.
3. It provides a mobile, combat-ready, senior radar element of the Theater Air Control System for worldwide contingencies.

**Complete the unit review exercises before going to the next unit**.

## Unit Review Exercises

**Note to Student:** Consider all choices carefully, select the *best* answer to each question, and *circle* the corresponding letter. When you have completed all unit review exercises, transfer your answers to the Field-Scoring Answer Sheet.

**Do not return your answer sheet to the Air Force Career Development Academy (AFCDA).**

1. (001) What is the *main* goal of the Utilization and Training Workshop (U&TW)?
   a. Establish a viable job qualification standard (JQS).
   b. Establish a viable specialty training standard (STS).
   c. Plan upcoming Specialty Training Requirement Team (STRT).
   d. Establish a viable Career Field Education and Training Plan (CFETP).

2. (002) Where is a newly graduated 3-level required to attend training after arriving at his or her new base?
   a. Professional Development Center.
   b. Airman Leadership School (ALS).
   c. First-Term Airman Center (FTAC).
   d. Airman Family and Readiness Center (A&FRC).

3. (002) Which course is designed to target NCOs who completed Airman Leadership School (ALS) at least three years before and/or who have *not* yet attended the NCO academy?
   a. Airman Leadership School (ALS).
   b. Enlisted Professional Military Education (EPME).
   c. Noncommissioned Officer Professional Enhancement course (NCOPE).
   d. Senior Noncommissioned Officer Professional Enhancement course (SNCOPE).

4. (003) What specific Air Force specialty code (AFSC) maintains equipment that assists in the safe and expedient movement of air traffic throughout the National Airspace System (NAS) as well as provides support to the National Weather Service (NWS)?
   a. 1C8X1.
   b. 1C8X2.
   c. 1C8X3.
   d. 1C8X4.

5. (003) Who provides critical maintenance and repair to navigational aids, instrument landing systems, and many other pieces of equipment that ensure the safety of aircrews accomplishing their missions?
   a. Aircraft maintenance.
   b. Aircrew safety management.
   c. Computer systems technicians.
   d. Radar, Airfield & Weather Systems (RAWS) technicians.

6. (003) Where are details concerning specific responsibilities for your Air Force specialty code (AFSC) found?
   a. Your AFSC-specific Career Field Education and Training Plan (CFETP).
   b. Enlisted Professional Military Education (EPME).
   c. Your base functional manager (BFM).
   d. Job qualification standard (JQS).

7. (004) What information system supports base, wing, and work center level training management activities?
   a. Training Business Area (TBA).
   b. Integrated Maintenance Data System (IMDS).
   c. Management Internal Control Toolset (MICT).
   d. Global Cyber Support Systems-Dashboard (GCSS-D).

8. (004) What information system uses inputs from various sources, provides the capability to view equipment status, and drill down capability to serial number information from all levels?
   a. Training Business Area (TBA).
   b. Integrated Maintenance Data System (IMDS).
   c. Management Internal Control Toolset (MICT).
   d. Global Cyber Support Systems-Dashboard (GCSS-D).

9. (005) Who is responsible for unit self-assessments?
   a. Commanders.
   b. Unit training manager.
   c. Wing inspector general (IG).
   d. Base training manager (BTM).

10. (006) What program assesses the effectiveness of a work center's training program, technician competence, and technical and procedural data adequacy?
    a. Self-inspection.
    b. Personnel evaluation.
    c. Equipment evaluation.
    d. Unit type code equipment evaluation.

11. (006) Which evaluation assesses unit type code (UTC) personnel readiness against the UTC mission capability (MISCAP) and ensures mission reliability?
    a. Special personnel evaluation.
    b. Equipment personnel evaluation.
    c. UTC personnel evaluation.
    d. Individual personnel evaluation.

12. (006) Who can authorize the substitution of pre/post deployment inspections to satisfy the requirements for an equipment evaluation?
    a. Commander.
    b. Unit training manager (UTM).
    c. Wing inspector general (IG).
    d. Base training manager.

13. (006) How often will quality assurance (QA) evaluate *all* core base voice/video/data transport and transmission systems?
    a. Every 6 months.
    b. Every 12 months.
    c. Every 18 months.
    d. Every 24 months.

14. (006) Where can you find the sampling plan for unit type code (UTC) equipment evaluations?
    a. Career Field Education and Training Plan (CFETP).
    b. Air Force Instruction (AFI) 36–2651, *Air Force Training Program.*
    c. AFI 13–204, Volume 4, *Management of Ground Radar and Airfield Systems*, Attachment 4, *Sampling Plan.*
    d. AFI 63–101/20–10, *Integrated Life Cycle Management.*

15. (007) Technicians will be decertified if they receive which rating on a personnel evaluation?
    a. Satisfactory (Sat).
    b. Unsatisfactory (Unsat).
    c. Not in compliance (NIC).
    d. Complies-with comments (CWC).

16. (007) Who is the closing authority for unsatisfactory evaluations?
    a. Unit commander.
    b. Unit training manager (UTM).
    c. Wing inspector general (IG).
    d. Base training manager (BTM).

17. (008) Which operational support flight provides airfield management and air traffic operations services to the base flying wing transient and civil users?
    a. Aircrew flight equipment flight.
    b. Current operations flight (OSO).
    c. Airfield operations flight (OSA).
    d. Radar, Airfield & Weather Systems (RAWS) flight.

18. (008) Which operational support flight performs maintenance on radar, navigational aids, weather, and air traffic control (ATC) radio systems?
    a. Aircrew flight equipment flight.
    b. Current operations flight (OSO).
    c. Airfield operations flight (OSA).
    d. Radar, Airfield & Weather Systems (RAWS) flight.

19. (009) What agency acts as the lead command for the creation and application of criteria, procedures, and precision equipment for worldwide instrument flight operations, air traffic control, airfield management, and air traffic control and landing systems for the Air Force?
    a. Air traffic control (ATC).
    b. Federal Aviation Administration (FAA).
    c. Air Force Flight Standards Agency (AFFSA).
    d. Air Education and Training Command (AETC).

20. (010) Where is the headquarters of the 557th Weather Wing located?
    a. Davis-Monthan AFB, Arizona.
    b. Mountain Home AFB, Idaho.
    c. Keesler AFB, Mississippi.
    d. Offutt AFB, Nebraska.

21. (010) What program is Operating Location Kilo responsible for managing?
    a. Environmental climatology program.
    b. Combat weather systems development.
    c. American Forces Network Weather Center.
    d. Department of Defense’s portion of the next-generation weather radar program.

22. (011) What dictates when air traffic control squadrons are activated for deployment?
    a. Operations tempo.
    b. Time from last deployment.
    c. Air National Guard training schedule.
    d. Ten-year deployment plan developed by congress.

23. (011) Who provides the theater Air Force commander a rapid reaction mobile air control system and control/reporting center during worldwide contingencies?
    a. Intelligence squadron.
    b. Air control squadron.
    c. Operations support squadron.
    d. Air traffic control squadron.

**Please read the unit menu for unit 2 and continue ➔**

# Unit 2. Work Center Fundamentals

**2–1. Safety and Risk Management ..... 2–1**
012. Air Force consolidated occupational safety ..... 2–1
013. Career field hazards ..... 2–2
014. Safety precautions and work center programs ..... 2–4
015. Tower climbing and safety requirements ..... 2–8
**2–2. Publications and Directives ..... 2–18**
016. Department of Defense publications and directives ..... 2–18
017. Air Force publications ..... 2–19
018. Technical orders ..... 2–22
019. Industry and military standards ..... 2–27
**2–3. Security ..... 2–30**
020. Physical security ..... 2–30
021. Facility security ..... 2–32

IF YOU HAVE NOT realized by now, safety is a priority for task accomplishment in the Air Force. You have heard the term "safety first," and as a RAWS technician, you now must not only ensure your own safety, but also the safety of those around you. Operational risk management should be the first step when you or your co-workers are performing any action or task.

This unit covers safety, hazards of the AFSC, precautions you can take, and tower climbing information to help you analyze and draw conclusions on how to work safely in climbing situations. It will also cover publications, directives, TO, and physical security. These topics will give you a proper foundation for day-to-day operations in support of your mission, no matter where you are.

## 2–1. Safety and Risk Management

Safety never takes a holiday. RAWS technicians need to make sure safety and risk management are a part of any planning process and used on a daily basis. This section delves into certain aspects of safety; some are broad and overreaching, while some are very precise and catered to the daily procedures of every RAWS member. This information may save you or your co-worker's life one day.

### 012. Air Force consolidated occupational safety

Occupational Safety and Health Administration (OSHA) safety guidance published in the Department of Labor (DOL) 29 series Code of Federal Regulations (CFR) provides workers a safe and healthy workplace. OSHA dictates what must be accomplished in the workplace, but not necessarily how it will be accomplished, or by whom.

Commanders are responsible for the safety of their facilities and personnel, including the correction of all hazards and deficiencies in their workplaces. Safety guidance assigns responsibilities to individuals or functions to help commanders manage their safety and health programs, ensuring they comply with OSHA and Air Force guidance. AFMANs provide guidance for a uniform program, which MAJCOM/wing/installation commanders may supplement, as necessary, to ensure a safe and healthy work place.

Air Force Manual (AFMAN) 91–203, *Air Force Occupational Safety, Fire, and Health Standards*, references to other Air Force publications, OSHA standards, and national safety consensus standards are provided as appropriate. This instruction is intended for use by installation occupational safety officials, commanders, functional managers, supervisors, and workers at all levels, including

Air Force civilians. The information in AFMAN 91–203 is derived from many sources and includes non-Air Force and Air Force directives in a single document to protect workers and comply with Federal law.

All Air Force units must comply with applicable safety guidance during Air Force operations. MAJCOMs, direct reporting units (DRU) and field operating agencies (FOA) may supplement AFOSH guidance when additional or safety that is more stringent, fire prevention and health criteria are required. When there is conflicting guidance, use the guidance that provides the most protection. Always follow AFOSH guidance at all times. It implements parts of 29 CFR, and includes additional requirements not addressed by the OSHA standards. In addition, follow safety, fire prevention and occupational health requirements in equipment TOs at all times. Area-specific instructions and technical data include other safety criteria. When AFOSH guidance or safety criteria does not cover a situation, then use non-Air Force standards to include, but not limited to, national consensus standards, professional safety and health standards, and other Federal agency standards. Air Force activities must comply with OSHA requirements at all times, unless the military-unique exemption exception applies according to DODI 6055.01, *DOD Safety and Occupational Health (SOH) Program*.

Air Force safety officials cannot grant exemptions to OSHA standards, only the DOL has the authority to grant exemptions to OSHA standards. Refer to AFI 91–202, *The US Air Force Mishap Prevention Program*, for additional information. The Air Force Safety Center, HHQs and installation safety offices may establish more stringent requirements than those established by OSHA.

**NOTE:** OSHA references in this standard list the CFR number, part number and part title, as applicable (i.e., 29 CFR 1910.120, *Hazardous Waste Operations and Emergency Response).*

## 013. Career field hazards

Work in any career can be hazardous. The key to preventing injuries is to understand what the hazards are, and how to deal with them. In this lesson, you are going to learn what hazards are common in the RAWS career field and the problems they can cause.

### Electrical hazards

Today, just about everything runs off electricity and the equipment used in the military is no different. Electricity can be very convenient, but it can also be very dangerous. There are many hazards associated with electricity. In the next few paragraphs, you will learn about a few of the most common hazards that you may encounter as a RAWS technician.

#### *Shock*

The severity of electric shock is determined by the amount of current flowing through the body, the time of exposure, and the body's physical condition. Normally, any voltage capable of producing a current flow of 50 milliamperes or more through the body can cause a shock that may cause cardiac arrest. Any individual receiving an electric shock will seek immediate medical attention. Some effects of electrical exposure to the body are:

- Contraction of the chest muscles, which may interfere with breathing to such an extent that death, will result from asphyxiation with prolonged exposure.
- Temporary paralysis of the nerve center, which may result in failure of respiration, a condition that often continues long after the victim is freed from the circuit.
- Ventricular fibrillation, an irregular and erratic heartbeat, which may result in cardiac arrest.
- Serious internal injuries to nerve and bone can occur with the passage of electrical current through limbs. Externally, apparent damage does not always appear severe. If pain, loss of sensation, or function occurs, seek medical attention immediately.

### *Arcing*

When a metal object, such as a tool, contacts an electric current, it will become a conductor. The electric current may result in an arc, which may cause serious burns to the body and temporary or permanent blindness. Arcing is extremely dangerous because you do not actually have to contact the source of electricity. If two conductors get close enough, the electric current can jump from one conductor to another. A natural reaction after making contact with an electric current or seeing an arc is to push oneself away from the source. This can result in falls or abrupt contact with fixed objects causing serious or fatal injuries.

## Climbing hazards

The primary hazards associated with climbing are falls and contact with electrical systems. Examples of climbing hazards include the following:

- Pole attachments such as conduits, molding, cable and ground wire, strain plates, signboards, nails and metal pole numbers.
- Tower conditions such as cracks, rust, corrosion, loose/missing hardware, ice on climbing surfaces, bent/broken steps, improper grounding, dirt and excessive grease and oil.
- Improper clothing such as badly worn shoes (e.g., loose heels, thin soles), low-cut shoes, and jackets too loose or too long. Proper climbing boots with a designated heel and steel supportive shank are highly advised. Steel toe boots are required per OSHA regulations.
- Equipment items that do not fit properly, such as loose climber straps too tight, too loose, too long or broken; or the wrong sized harness.
- Failure to follow approved methods for climbing and working on poles and tower structures.
- Failure to maintain good physical condition.

These are just a few hazards to consider. Climbing safety will be covered more in depth later in this unit.

## Radiation hazards

Radiation is a significant hazard in the RAWS career field. There are two types of radiation, non-ionizing and ionizing, but they come from many different sources. In the following paragraphs, you will learn about the two types of radiation that you may come in contact with during your daily duties.

### *Non-ionizing radiation*

Non-ionizing radiation produces heat in body tissues. Absorption by the body is both frequency and body-shape dependent. Thus, it is possible for a person to absorb damaging amounts of non-ionizing radiation in deep tissue and organs with little or no sensation of skin heating. Refer to AFI 48–109, *Electromagnetic Field Radiation (EMFR) Occupational and Environmental Health Program*, and 29 CFR 1910.97, *Nonionizing Radiation*, for additional guidance on management of hazards associated with non-ionizing radiation.

### *Ionizing radiation*

Radioactive material contained in electron tubes present no significant hazard as long as the tube is intact. The level of radiation from a small number of electron tubes at maintenance shops does not approach a dangerous level; however, at major supply points, the storage of large quantities of radioactive tubes, in a relatively small area, may create a hazard. Further, a broken radioactive tube is potentially hazardous since the radioactive material may be inhaled or ingested. Radio frequency generators such as certain klystrons, thyratrons, magnetrons, transmit-receive tubes and similar high voltage devices emit ionizing radiation. Refer to 29 CFR 1910.1096, *Ionizing Radiation*, for additional guidance.

## 014. Safety precautions and work center programs

Now that you know some of the hazards associated with your job, you need to know how to prevent serious injury while performing maintenance. The following precautions will greatly decrease your chance of injury while work center safety practices will bolster your safety mindset. Refer to AFMAN 91–203 for further information.

### Energized equipment

To prevent serious injury while working on electrical circuits follow these precautions:

- Workers near exposed electrical circuits or maintenance and installation activities, regardless of location, shall not wear rings, watches or other conductive objects that may increase the shock risk or be the source of potentially severe burns when energized.
- Do not use, or carry in your pockets, metallic measuring rules, tools, or metal-cased objects. Metal-framed eyeglasses may be worn if secured with a nonmetallic cord to prevent them from falling into an energized circuit.
- *At a minimum*, two qualified technicians, or one qualified technician and one safety observer, will work together when exposed to high voltage of 600 volts, nominal or more, or current flow of 50 milliamperes or more. All necessary personal protective equipment (PPE) and special tools shall be available and used. Personnel, to include safety observers, whose normal daily job exposes them to energized electric circuits, will be certified in cardiopulmonary resuscitation (CPR) and self-aid/buddy care. Identified personnel will recertify annually and provide written documentation of recertification. CPR training is emergency training and is *not* a substitute for safe electrical work practices.
- Electrical circuits should always be de-energized, locked, and tagged out before attempting any work, unless the nature of the work requires the circuits remain energized. Do not rely on safety devices such as interlocks, high-voltage disconnect relays, or automatic circuit grounds. Each of these is subject to failure.
- All workers, including safety observers, will know the location and on-off operation of the power distribution panels, power control switches and stations, and electrical danger areas in their work area. This knowledge is essential to de-energize equipment in the event of a fire or accidental electrical contact. Quick reference signage or labeling on equipment racks for the applicable circuit breaker is highly advisable, when physically possible. In addition, emphasis shall be placed on the need to maintain clear, unrestricted access to these controls at all times. Workers will open and close all equipment switches quickly and positively. The doors to high voltage racks shall be closed at all times except for authorized maintenance and repairs.
- Interlocks shall not be permanently disconnected or bypassed. Interlocks can be disconnected during maintenance or adjustments only when prescribed by applicable TOs. During these periods, Air Force Visual Aid (AFVA) 91–305, *DANGER—INTERLOCKS DISABLED*, or a sign, either locally manufactured or the nearest commercially available equivalent, shall be placed on the equipment or nearest available equipment. If the equipment has a defective interlock, all workers shall be made aware of the hazardous condition, and a warning sign or tag shall be posted on the equipment.
- Grounded railings, barriers or enclosures shall be used to protect workers from shock resulting from contact with conductors, bus bars, switches, control panels, and so forth. All contacts, terminals, and devices having voltages between 50 and 599 volts root mean square (RMS) or direct current (DC) with respect to ground will have barriers or guards to prevent accidental contact by personnel. Holes in the barrier may be provided for maintenance testing. Assemblies operating at potentials in excess of 600 volts RMS or DC shall be completely enclosed from the remainder of the assembly. The barrier, guard, or enclosure shall be marked to indicate the approximate highest normal voltage (nearest round number) which may be encountered upon its removal.

- When possible, technicians should perform energized electrical work following the “One Hand Rule.” This requires the technician to place one hand in a pocket, or behind your back, to prevent contact with grounded work surfaces while performing energized electrical work and to prevent electrical current from flowing through both arms and the heart.

### High voltage

AFMAN 91–203 defines high voltage as any RMS voltage of 600 volts, nominal, or greater. However, much lower voltage can be lethal. The design and development of all military electronic equipment shall provide fail-safe features for safety of workers during the installation, operation, maintenance or interchanging of a complete equipment assembly or component part. Operators and technicians shall not attempt to adjust any electronic equipment when there is a possibility of injury from unprotected high voltage.

Adjustments on operating high voltage equipment, other than those specified by the TO or manufacturer’s manuals, shall only be authorized by the unit commander. The unit commander shall consider all operational requirements, TOs, manufacturer’s guidance, safety precautions and emergency procedures before authorizing work to proceed. Workers using high voltage to troubleshoot and/or test cables shall be instructed in the precautions necessary for their safety and the safety of others. Workers are warned to stay clear while voltage is applied.

- Only qualified personnel shall perform work near energized overhead power lines**.**
- While working on high-voltage there will be a minimum of two workers present. The second worker will not be working on the equipment but acting solely as a safety observer.
- Warning signs or AFVA 91–306, *DANGER—HIGH VOLTAGE*, shall be prominently posted in all areas housing high voltage equipment; the highest expected voltage shall also be posted.
- Insulating matting will be used near electrical apparatus or circuits in high voltage maintenance areas as an additional safety measure to protect workers.

### Radio frequency hazards

Many types of RAWS equipment are sources of non-ionizing radiation. Personnel shall be instructed in the hazards of non-ionizing radiation and shall not be exposed to non-ionizing radiation levels above the permissible exposure limits outlined in AFI 48–109*.* Evaluations and control measures are good practices to help mitigate these hazards.

#### *Electromagnetic field hazard evaluations*

All electromagnetic field (EMF) transmitters owned and operated by avionics workplaces, communications facilities, industrial processes, and medical facilities will be identified during the regularly scheduled, on-site bioenvironmental engineering (BE) health-risk assessment activities to these areas. At a minimum, EMF emitters will be inventoried biennially (every other year) to identify new emitters, and evaluations shall be conducted if operations change or new systems are added to the inventory. Consultation with the installation frequency manager shall be conducted to verify all emitters have been identified from these workplaces and potential additional work centers.

Inventories will be maintained for the EMF transmitters identified. BE should coordinate with the weapons safety manager and installation spectrum manager to ensure a complete base inventory. At a minimum, the inventories will include the following categories: work center, POC, POC phone number, emitter nomenclature (i.e., AN/GRT–21), emitter description (i.e., Tactical Air Navigation System (TACAN), quantity, frequency range, upper tier and lower tier maximum permissible exposure (MPE), and hazard distances.

The operational and maintenance environments, operational parameters, and exposure potential shall be evaluated against the applicable MPEs by BE to determine if exposures may be in excess of the standard. Records of surveys, reports, calculations, and control measures imposed should be

maintained for each fielded EMF emitter which is capable of exceeding the lower tier MPEs listed in AFI 48–109, table A2.2.

### *Electromagnetic field hazards control*

Control measures may be recommended by BE following thorough evaluation of the hazard potential, to include survey measurements. Following the hierarchy of controls according to AFMAN 48–146, *Occupational & Environmental Health Program Management*, engineering controls are followed by administrative controls.

Engineering controls, such as interlocks, are either inherent in the system or used in conjunction with its maintenance or operation to prevent potential overexposure or injury to the worker. Administrative and physical controls are used primarily as exclusions to the EMF operational area by barrier or administrative procedures such as access restriction (e.g., elevation or fencing) and signage. These control measures should be used when engineering controls or other methods are not adequate. Areas where the potential exists for EMF exposures to exceed exposure limits shall be clearly marked with appropriate signs. The signs are posted when engineering controls or other methods are not adequate. Signs may be used as a complement to other administrative controls. Signs will be multilingual when in locations where English is not the primary language and compliant with the requirements of the host nation.

## Hazardous materials

In the RAWS career field you will be working with or around several hazardous materials. The materials range from simple batteries to potentially explosive gasses. In this area, you will learn about some of the most common hazardous materials in RAWS. Learning the characteristics of these materials gives you the knowledge to work both smarter and safer.

### *Flammables and combustibles*

A flammable liquid has a closed cup flashpoint below 100° Fahrenheit (F) and a vapor pressure not exceeding 40 pounds per square inch, gauge (psig) at 100° F. Flammable liquids are categorized as Class I liquids. A combustible liquid has a closed cup flashpoint at or above 100° F; combustible liquids are categorized as Class II or Class III liquids.

### *Batteries*

Appropriate PPE, approved and certified in BE's occupational and environmental health (OEH) risk assessment, shall be worn whenever charging, maintaining, removing and/or replacing batteries. PPE required when working with batteries is documented according to AFI 91–202, *The US Air Force Mishap Prevention Program*. PPE is required when:

- Cleaning batteries, battery connection points and/or cables, servicing fluid level, connecting or disconnecting a battery charger at the battery, jump-starting a battery installed in a vehicle or piece of equipment, or any other type of service activity, requires American National Standard Institute (ANSI/ International Safety Equipment Association (ISEA) Z87.1 approved eye protection with side shields. When handling electrolyte, always wear a face shield, splash resistant chemical goggles, and chemical resistant gloves and apron.
- Handling vented lead acid vehicle or support equipment batteries (removing or installing in vehicles or equipment or transporting them) or when working in the battery room or maintenance area, requires personnel to wear acid resistant gloves, arm gauntlets, aprons, face protection and ANSI/ISEA Z87.1 approved eye protection with side shields. Acid-resistant safety shoes or acid-resistant rubber knee length safety-toed boots are always worn.

### *Composite materials*

Composite materials (e.g., fiberglass, carbon fiber, Kevlar, etc.) are widely used in Air Force operations. These materials can present potentially serious health and safety hazards to personnel unless specific precautions are taken. Environmental, Safety, and Occupational Health personnel must

evaluate operations involving fabrication, repair and handling of composite materials to assure adequate precautions are taken to prevent injury or illness to personnel and/or damage to equipment.

Composite materials require careful handling at all times. Many of the chemicals and materials used in composite fabrication and repairs pose serious health or fire hazards and must be used and handled with care. Air Force personnel must be made aware of the potential hazards associated with composite materials through appropriate training. Workers shall refer to the safety data sheets before starting any work when hazardous materials or chemicals are involved or needed for the process. As a minimum, job safety training shall include: need for and use of approved PPE; maintenance and care of PPE; safe chemical handling procedures; and emergency treatment practices in case of exposure, ingestion or inhalation of liquids, vapors or dusts from composite operations.

### *Compressed gases*

Inspect all cylinders for damage, that is, dents, gouges, evidence of leakage or cracks before use. Tag damaged cylinders "Out of Service," and returned to the manufacturer or distributor. Workers must know a cylinder's contents. Do not use a cylinder if you cannot quickly determine its contents by wording on the cylinder or a tag securely attached to the cylinder. If the tag has become detached or the label defaced, do not use the cylinder. Do not rely on color-coding the cylinder. Different manufacturers use different color codes.

Handle all cylinders carefully. Careless handling may damage cylinders and valves. Install valve and dust covers when cylinders are not in use. Use cylinders for no purpose other than containing compressed gases; handle them with the same care whether full or empty. Secure all cylinders, whether in use or in storage, full or empty, by using a chain or other fastening device to a solid fixture (wall, stanchion, etc.) to prevent cylinders from falling over. Non-metallic or synthetic straps may be used to secure non-flammable gases, except oxygen.

Move cylinders safely. Appropriate dollies or hand trucks are used to move cylinders weighing more than 50 pounds. Secure the cylinder to the hand-truck before and during movement. Movement by spinning, sliding, rolling, and so forth, is prohibited. Cylinders less than 50 pounds may be moved without using a dolly or hand-truck. However, personnel need to be aware of the potential for injury if improper lifting techniques are used when lifting cylinders.

## Work center safety program

As a junior member of your work center, your role in administering a safety program will be minimal but all members of the work center play an important part in safety. In fact, the individuals in the work center have the most important role of all. The individuals doing the work must recognize a dangerous situation and know what actions to take to maintain a safe work environment.

### *Responsibilities*

The safety requirements of work center members are listed below:

- Comply with all safety instructions, TOs, job guides and operating procedures. Demonstrate knowledge of their roles and responsibilities with relation to risk management and mishap prevention.
- Consider personal safety and the safety of co-workers while performing assigned tasks as well as off-duty activities. Identify and report hazardous conditions that place Airmen or property at risk. Use the AF Form 457, USAF Hazard Report, when necessary.
- Report personal injury, property damage and any suspected exposure to biological, chemical or nuclear hazardous materials to their supervisor as soon as possible.
- Immediately report to their supervisor if they believe that they have a physical or mental condition that they feel may impact safe job performance.
- Use and maintain recommended and appropriate PPE for job tasks. Inspect and maintain PPE according to the TO, manufacturer's instructions, or BE guidance.

- Apply risk management principles in both on-duty and off-duty activities to enhance the safety and well-being of themselves and other personnel.
- Military members will immediately notify their primary care managers of a known pregnancy and make an appointment with public health to initiate a workplace evaluation for exposures that may be hazardous to the fetus and determination of work restrictions. Government civilian employees are encouraged to notify their supervisor and make an appointment with public health for a workplace evaluation, but are not required to do so. Any worker with questions regarding how their worksite exposures can affect immediate family members (e.g., spouse, children) should contact public health.
- Have the opportunity to participate in safety and health programs, report hazards, near misses and work-related injuries/illnesses without fear of coercion, discrimination or reprisal.
- Use official on-duty time to take part in safety activities.

Hand-carry or electronically transfer safety training documentation provided by previous supervisor, as specified in AFI 91–202, *The US Air Force Mishap Prevention Program*, paragraph 1.8.22.5, to the new supervisor when deploying or transferring to another Air Force position/location.

#### *General housekeeping*

It's important to maintain a clean, neat environment in your work center and maintenance areas. Messy areas can lead to accidents that can not only injure people but also have a detrimental effect on the work center. The following points are some general good practices to ensure good housekeeping:

- Keep floors and walking surfaces free of debris and tripping hazards.
- Dispose of combustible waste according to approved hazardous waste procedures.
- Make sure proper lighting in all work areas.
- Remove excess garbage regularly and store equipment and shop items appropriately.
- Keep all surfaces free of excessive soils, liquids, and dust.

This is not an all-inclusive list. Where appropriate, MAJCOMs, FOAs, DRUs, local safety statutes may determine location or shop-unique requirements.

## 015. Tower climbing and safety requirements

The beginning of this unit described overarching guidance for the Air Force with reference to AFMAN 91–203. This lesson will focus on specific guidance within these references with a targeted look at climbing safety, fall protection, and proper equipment use and storage.

### Consolidated Occupational Safety Instructions/OSHA climbing standards

AFMAN 91–203 will be your go-to reference when researching safety, climbing, and fall protection standards. Described below, are some of the most important climbing safety areas.

#### *Types of fall protection*

There are two types of fall protection: passive and active. Passive fall protection such as guardrails, work stands and platforms, nets, ladder cages, and other devices can prevent a worker from falling, but are not directly connected to the worker. Nets do not prevent a worker from falling, but does prevent a worker from hitting the next level. If passive fall protection is not feasible, active fall protection is the preferred option.

Active fall protection, such as positioning and restraint systems, ladder climbing devices and the personal fall arrest systems (PFAS), require the worker to wear a harness and attach himself/herself to an anchorage or lifeline. Positioning and restraint systems prevent a worker from falling while a PFAS permits a worker to fall, but limits arresting loads to generally safe levels.

### *Training*

Unit commanders designate, in writing, all personnel required to maintain climbing proficiency. Commanders shall restrict climbing authorizations to structures that must be climbed to accomplish mission requirements. Documentation needs to be updated regularly to ensure incoming and outgoing personnel are properly added and removed.

### *Certification procedures*

Upon assignment to a unit, each individual whose future duties will require climbing poles and towers where they may be subject to a fall of four (4) feet or more in height shall be trained and certified, as applicable. The requirements ensure workers who must climb use proper PPE, are fully qualified and physically capable of climbing and working aloft. Personnel who have not climbed within the last 12 months as a part of their normal job require refresher training under the supervision of a qualified instructor. The climbing instructor determines the amount of training required.

Authorized workers will be trained and evaluated before using any PFAS. Training includes methods of use, application, inspection and storage, and any manufacturer's recommendations; application limits; proper anchoring and tie-off techniques; estimation of free fall; deceleration and total fall distance to prevent striking a lower level; and applicable fall protection, fall prevention, rescue, and evacuation plans. Recurring training is conducted annually, when work conditions change or new fall arrest systems are used, and documented according to AFI 91–202.

## Climbing safety principles

As a climber, you have many responsibilities to ensure your climbing experience is safe. When climbing a tower there are six things you can do to make your climb easier. If you are climbing and you get tired quickly, you may not be climbing properly. The next few points talk about things you can do to assist in climbing safety.

- Climb with your legs not your arms. Your leg muscles are stronger than your arms and won't tire as easily. While you are climbing, you should try to keep your arms straight. When you bend your arms and you use them to climb with, your arms will tire quicker than if you climb with your legs.
- Climb on the high side of the tower. This makes climbing easier. It is almost impossible to climb the low side of a tower. The main factor you will deal with is gravity. This also mainly deals with towers that are tilted or leaning.
- Legs lead on the climb, arms lead on the descent. While climbing you step first with your legs then move your arms. On the descent, reach down with your arms first then move your legs. This will help to prevent fatigue.

  **WARNING:** You must have three points of contact while climbing *at all times*. Either one hand and two feet or two hands and one foot must be in contact with the tower or ladder *at all times*.
- Rest often and use the rest platforms when they are available. Platforms are installed for resting. While climbing you will burn lots of energy, this could cause your muscles to cramp up. When you get to a platform or any other safe place, stop and take a break. While resting, make sure to drink plenty of fluids to prevent dehydration.
- Keep your body swing at a minimum. The more body swing you have the harder your climb will be. You are not just carrying your weight but also the weight of your safety equipment.
- Be well rested, confident and medication free. You should never climb a tower while under the influence of medications that may affect your performance. If you know you will be climbing the next day, you need to get a good night's rest. Lack of sleep, being under the influence of medications, and a lack of confidence will prevent you from concentrating and the results could be fatal for you and/or a co-worker.

As stated earlier, steel-toe boots are *required* per OSHA regulations when climbing. Hard hats are also *required* per OSHA for all personnel while working at a climbing location, even if you are not climbing. The chinstrap *must* be worn when climbing but can removed while on the ground.

When performing aerial work, safety observers *must* be qualified to operate the equipment in use and should have a current climbing certification, be proficient in CPR and administering emergency first aid treatment that involves control of bleeding, shock, open wounds and burns, and procedures for obtaining medical assistance. Observers should also be knowledgeable of rescue operations.

### *Rescue plan*

Rescue plans will be developed for all fall protection activities. Never allow PFAS use if a means to rescue a fallen worker is *not* available. Self-rescue by a fallen worker may be possible, depending on location and work conditions. However, the supervisor should make sure a rescue plan is in place to rescue workers should they be injured or unable to self-rescue.

Workers suspended in a full body harness often lose consciousness after a fall. This happens because the harness restricts blood flow to the extremities. The rescue plan must ensure a rescue can be implemented very quickly to prevent or minimize permanent injury or death. When potential for serious injury exists due to a fall and no threat requires immediate movement of the fallen worker, the worker should remain in place and encouraged to remain still while emergency services personnel are called to assist.

### *Tower rescue*

While not every situation will be the same in a rescue scenario, the following steps are a general guideline for proper preparation and rescue of an individual on a tower. Remember, all tower workers shall be qualified in first aid, buddy care, and CPR. Use the following steps for descending/suspension method of rescue:

- Climb the tower using the “Y” lanyard and attach a snatch block to the tower.
- Install a rope through the snatch block. This shall be used to raise the other equipment that’s used for rescue.
- Attach the canvas bucket to the rope and raise it to the anchor position.
- Attach the anchors; one for the victim’s rope grab, and another for the rescuer’s rope grab. The third anchor for the descender, which is attached in the middle, with the victim to the right and the rescuer to the left.
- Rig the three termination plates and attach them to the anchor straps.
- The rescuer shall attach to the rope grab, rig the descender, and prepare to rescue the victim.
- The rescuer shall not disconnect from the rope grab until on the ground.
- Once in position, the rescuer shall descend to the victim and permanently lock-off the descender.
- After permanent lock-off has been accomplished, the rescuer shall attach to the victim using a carabiner.
- After connecting to the victim, the rescuer shall cut the mule tape which will cause the victim to fall about two (2) inches. The descender shall take on the weight of the victim, and the rescuer will not feel the effect of the victim’s weight.
- Once attached to the victim, the rescuer shall position the victim on his/her right hip.
- After getting the victim positioned properly, the rescuer shall place the descender in the descend position and lower him or herself and the victim to the ground.
- The rescuer shall apply first aid, buddy care or CPR, if needed, while awaiting the arrival of emergency services.

### *Climbing hazards*

The basis for all safety is identifying hazards before they cause serious injury or even death. There are many different types of hazards for climbing. Here we describe the three main hazards: environmental hazards, live hazards and structural hazards. Once a hazard has been identified, it becomes the task of safe practices to determine how to eliminate the hazard, control the hazard, or avoid the hazard.

#### *Environmental hazards*

One of the main environmental hazards is the weather. In some areas, the weather changes constantly so you will need a method of getting weather updates in case you need to get off the tower. This can be accomplished using radios and more commonly by the use of cell phones. The wind can exert force on the structure, materials and the climber. Many times a tower is taller than the surrounding structures so the effect of the wind is even greater on the tower than the effects while on the ground. Extra care must be taken to avoid the dangers of the wind. The Air Force policy states that if the winds are in excess of 25 miles per hour (mph), you must get off the tower.

Another condition that affects your climbing abilities would be during snow/icing conditions. With the snow, you must be careful to prevent slipping and frost bite. With icing conditions, you have three main factors to deal with while climbing or working on towers. First, ice can be very slippery while moving on or around the tower making tasks even more hazardous than normal. Second, ice is heavy and causes additional weight on the tower structures. This could result in your anchor points not being as strong as expected. Third, ice can break off and fall on you or your equipment. If possible, you should never climb when there is ice buildup on the structure or conditions suggest that ice will form while you are working.

Moisture can be just as slippery as ice; however, it can be harder to detect. Rain or dew can cause a steel tower to become very hazardous and you must be very careful while climbing. When climbing on a wet tower, be careful as if you were climbing on an icy surface.

Lightning can be one of a climber’s worst nightmares. During storms a tower can become a lightning rod; you must ensure the tower is properly grounded. Air force policy states that if there is lightning within five miles you must get off the tower immediately.

The sun can be one of the most dangerous of the environmental hazards. The sun’s rays can cause severe sunburns. Sunscreen with a minimum sun-protection-factor (SPF) rating of 15 is recommended. There will be times when you will have to work in the sun for extended hours. For these situations, wear long sleeved shirts. Most importantly, the sun can also cause you to become dehydrated. Make sure you and all your co-workers drink plenty of fluids or your muscles may start cramping and it will be hard to descend the tower. If this happens, there is a good chance your co-workers will have to rescue you.

#### *Live hazards*

Insects can ruin a good day climbing. Climbers need to be aware of insects such as bees, wasps, spiders and other stinging insects. If a co-worker is stung by a wasp or bitten by a spider, you need to find the insect and identify the type of bite or sting. If the insect is unknown, try to catch it and give it to the emergency personnel. The emergency personnel will need this information to treat the victim properly. Know your co-workers; if you work with someone that has an allergic reaction to a bite or a sting, you need to know how to treat the person. This could be the difference between life and death.

Birds can also become a nuisance while working on towers. Since birds are territorial, they may become very protective of their nest and babies. When climbing a tower, you need to be aware of nests and droppings, because they can be slick and carry diseases.

#### *Structural hazards*

There are varieties of structural hazards you need to look for while climbing and working on towers. You need to make sure the tower anchors are not corroded and they are not creeping. The anchors

need to be inspected at the point of daylight. This is the area where the anchor first comes out of the ground and where the anchor will first start to corrode. If the tower you are working on is a guyed tower then you need to inspect the condition of the guy wires also to ensure they are not corroded, frayed, or loose. Corrosion and rust will eat away at the steel tower sections and first shows up as a white or gray powder. Remove signs of corrosion with a wire brush and then sprayed with a coat of primer paint or any other rust prevention paint.

Cracks in tower section will indicate stress on the structure and must be fixed before climbing. The cracks may be the results of stress on the tower caused by high winds or improper installation of guy wires and tower sections.

When you walk around the base of a tower and find nuts and/or bolts lying on the ground you need to find out where they came from. The bolts and/or nuts may be missing from the tower bracing where your safety equipment is supposed to be anchored. Install bolts with the head up and out. This means that all bolt heads will be on the underside of the tower bracing or from the inside out.

## Proper care, use and storage of climbing equipment

When climbing or working on towers your safety is only as good as your equipment. Here we will discuss care of fall restraint devices and various other climbing equipment. With the proper care and use of this equipment, you will be able to climb easier and with more confidence.

### *Harness inspection*

Beginning in February of 1995, OSHA required that employers provide fall protection for any employee whose work requires them to be six feet or more above a lower level or off the ground. You will be using a full body climbing harness at your location. Making sure your harness fits and is in good condition is critical to your personal safety.

#### *Ensuring the correct harness fit*

When climbing, you need to make sure the harness is the correct size and that you adjust the straps to fit your body properly. In other words, you should not use an extra-large harness if you normally use a small. If you were to use the wrong size, you could slide out of the harness during a fall. Fit the harness across your shoulders so the D-ring on the back of the harness lies flat against the upper middle of your back. Buckle the straps securely around your waist then secure the ends through the belt keepers. Buckle the chest straps then secure the ends through the belt keepers. Buckle the leg straps then secure the ends through the belt keepers. These leg straps need to be as tight as you can get them and still be comfortable. During a fall, your safety harness will be attached to a safety lanyard that will jerk your body to a stop. Your leg straps will ride up and cause some major discomfort if not tightened securely. Use the friction slide adjuster so that the strap fits snugly.

You may be lucky enough to have your own climbing harness issued to you at your location. Most will not, so taking care of them will be the responsibility of every climber. According to AFMAN 91–203, workers shall ensure a competent person inspects all PFAS equipment before each day's use to determine if it is in safe working condition. An old expression that fits here is, "the life you save may be your own." AFMAN 91–203 also states that supervisors will make sure all PFAS components receive a thorough inspection *at least* quarterly. Document and maintain this inspection for *at least* one year. The appropriate procedures for the inspection, care, and maintenance of this equipment are detailed below.

#### *What to inspect*

The general areas to inspect are the stitching and webbing, buckles and buckle holes, straps and strap ends, and D-rings. Inspect stitching and webbing for broken, burned, cut, or pulled stitches. Broken strands appear as tufts on the surface. To inspect, hold the webbing with your hands six to eight inches apart. Bend the webbing in an inverted "U" to cause surface tension, exposing problem areas.

Inspect all web areas. Damage from cuts, abrasion, corrosives, heat, or chemicals should be apparent. Figure 2–1 illustrates the proper technique.

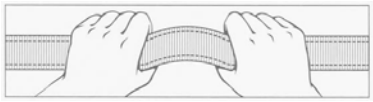

**Figure 2–1. Inspect stitching and webbing.**

Inspect the buckle, buckle holes, and ends of all straps. These areas can wear from repeated opening and closing. Enlarged or distorted holes may indicate excessive wear or damage through impact loading. Harnesses with unusually enlarged or distorted holes should fail inspection. Figure 2–2 depicts this inspection. You NEVER punch additional holes in or alter a harness. If you alter it in any way, the harness is unserviceable.

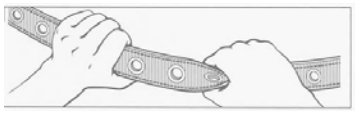

**Figure 2–2. Inspect buckle holes and strap ends.**

Inspect all D-rings for distortion. Check D-ring attachment points for unusual wear or damaged fibers. Badly pitted D-rings indicate chemical corrosion and they should fail inspection. Figure 2–3 illustrates the inspection of D-rings.

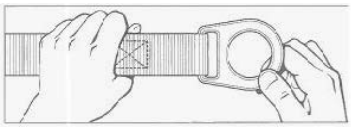

**Figure 2–3. Inspect D-rings for damage and/or wear.**

Inspect stitching or rivets at hardware attachment points. For stitched attachment points, check that stitching is not broken, burned, cut, or pulled. Check all riveted attachment points for tightness. Badly pitted rivets indicate chemical corrosion, and should fail inspection.

Inspect all tongue buckles for distortion, sharp edges, and cracks. The tongue should move freely and overlap the frame. Rollers should not be distorted and should roll freely. Figure 2–4 illustrates this inspection.

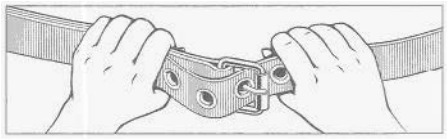

**Figure 2–4. Inspect tongue buckles.**

Inspect friction slide adjusters and buckles for distortion, sharp edges, and cracks. Make sure outer bars and center bars are straight. Also, check corners and attachment points for wear. Figure 2–5 depicts a typical friction slide adjustor/buckle.

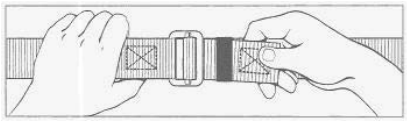

**Figure 2–5. Inspect friction slide adjustor/buckle.**

Inspect easy-connect buckles for distortion, sharp edges, and cracks. For stitched attachment points, check that stitching is not broken, burned, cut, or pulled. Figure 2–6 depicts typical easy connect buckles.

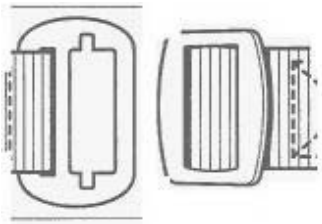

**Figure 2–6. Inspect easy connect buckles (male and female).**

Inspect friction-style buckles for sharp edges, cracks, and distortion. Make sure that outer bars and center bar are straight. Also, check corners and attachment points for wear. Figure 2–7 shows a typical friction-style buckle.

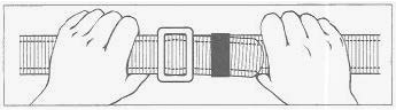

**Figure 2–7. Inspect friction-style buckles.**

Destroy or replace worn or damaged harnesses if evidence indicates excessive wear, deterioration, or mechanical malfunction. Destroy the harness by cutting across webbing or straps. Attach a DD Form 1577–2, Unserviceable (Reparable) Tag-Materiel, and turn in to your supervisor. Never work with worn or damaged equipment as it can cause serious injury or death. Check all equipment thoroughly and follow all safety procedures and guidelines. Do not take any shortcuts.

### *Lanyard inspection*

A lanyard is nothing more than a safety strap used for climbing and working on towers. When inspecting the lanyards you look for the same things you looked for while inspecting the harness. Inspect stitching and webbing for broken, burned, cut, or pulled stitches. Broken strands appear as tufts on the surface. To inspect, hold the webbing with your hands six to eight inches apart. Bend the webbing in an inverted “U” to cause surface tension, exposing problem areas. Inspect all web areas. Inspect the snaps and hooks for signs of corrosion. If you find any damage from cuts, abrasion, corrosives, heat, or chemicals discard the lanyard.

Make sure you check the lanyard for knots. One knot in the lanyard can reduce the strength of the lanyard by 50 percent. Also, know the weight a lanyard can safely handle. Lanyards *must* be removed from service after an impact load occurs or any signs of shock absorber activation.

### *Rope inspection*

There are many different kinds, types, and sizes of ropes. The two most commonly used by RAWS technicians are kernmantle and fiber rope.

#### *Kernmantle rope*

There are mainly two different types of kernmantle rope: static and dynamic. The static rope is used in situations where little stretching is required, mainly for hauling items, rappelling, and other applications where you would not want the rope to stretch. Dynamic rope, on the other hand, is used to secure climbers, and is designed to stretch under heavy loads to absorb the shock of a fallen climber. Dynamic ropes are only rated to handle a certain number of falls so, discard them once signs of stress appear. These signs show up as a tapered appearance in the rope.

Kernmantle rope should be inspected after each use, for any signs of damage. Damage to the kern will show up as “boogers” which indicates internal damage. Boogers will appear as tufts of white thread poking out through the mantle. Ropes that have been shock loaded (stressed) will have tapered sections to the rope, where you can see and feel the damage. Rope that has been cut should be examined carefully and discarded if unsafe. Never step on kernmantle rope! Getting fine rock and

dust particles in the sheath (mantle) will happen with everyday work; however, stepping on the rope will grind these particles into the inner core (kern) and cause damage to the rope internally, making the rope unsafe.

### *Fiber rope*

Inspect a fiber ropes internal condition at least once a month and inspect the surface condition every three months. Some signs of surface deterioration would be abrasions, broken fibers, cuts, stress which shows up as soft rope indicating the rope is badly wore or overloaded, and burns or decay caused by chemicals.

In order to inspect for internal deterioration, separate the strands at 3-foot intervals by twisting the rope and observe the inner part of the rope for broken fibers, embedded powders and particles, for mildew or mold caused by poor storage or improper drying. A change in fiber color will also indicate deterioration and is easily identified because the color of fiber rope is light and the deterioration will show up as a darker color.

## ***Other equipment***

Not all sites will have the same equipment but they should have the following basic climbing items. These will need to be inspected along with harnesses, lanyards, and rope. They are just as important to your safety as your ropes and harness.

### *Anchor straps*

Anchor straps are used as anchor points for climbing. At a minimum, these anchor straps must be rated at 5,000 pounds (lb.) when used for climbing. These anchor straps will be used to anchor the ropes and other climbing equipment. Inspect them by making sure there are no tears in the main strap. Some anchor straps come with a protective cover that is placed against the tower bracing to help prevent tearing of the anchor strap.

### *Carabiners*

Carabiners are nothing more than clips or hooks. However, when used for climbing you need to look for three things. First, they have to have a spring loaded gate (keeper), second, that the gate is self-locking and third, that the carabiner is rated to handle 5,000 lb. Carabiners are normally used to attach ropes, self-retracting lanyards and other climbing equipment together. There is a difference between a hook and a carabiner. Carabiners are weight tested on all side of the carabiner including the gate, while hooks are only weight tested at the vertical ends. Once you have determined the carabiner can handle the weight, inspect for proper operation of the gate and locking mechanisms, look for cracks, corrosion and pitting. If any exist, or the gate will not lock closed, do not use it.

### *Rope grabs*

A rope grab is a mechanical device. To inspect a rope grab you look for any signs of corrosion or cracks. If any are found, do not use it. You also want to test the rope grab for proper operation. Make sure the rope grab is installed with the arrow pointed in the up position and properly locked down onto the rope. Slide the rope grab up and down the rope ensuring that it slides freely. When a sharp downward pull is applied, the braking mechanism should activate preventing the rope grab from moving downward. An important thing to realize is that rope grabs come in different sizes for different sized ropes. If you have a 5/8” rope then you need a 5/8” rope grab. If you have a 1/4” rope and a 5/8” rope grab, the brake will not activate and this could be fatal.

### *Descenders*

Climbing and rescue descenders may vary from location to location but there are generally two types used today: the Fisk descender and mechanical descenders. The Fisk descender is a solid piece of metal but check for cracks, corrosion, and pitting. Also, look to see if it has been bent from overloading. If any of these conditions exist, do not use it. Mechanical descenders are a more popular

piece of equipment used today. As with a rope grab, make sure all braking mechanisms work properly and rope flows freely when expected. Finally, check for cracks, corrosion, and pitting. If any of these conditions exist or it is mechanically unsound, do not use it.

### *Storage*

Climbing equipment should be kept in a temperature-controlled facility. In order to minimize tangling, knots, and other damages, hang harnesses and lanyards. Do not throw them in a box. Keep these items away from sharp objects to reduce damage. Keep ropes in a sealed container or hung away from other items to minimize damage. You should never put ropes where they can be stepped on.

## Self-Test Questions

**After you complete these questions, you may check your answers at the end of the unit.**

### 012. Air Force consolidated occupational safety

1. Who is responsible for the safety of their facilities and personnel, including the correction of all hazards and deficiencies in their workplaces?

2. Who has the authority to grant exemptions to OSHA standards?

### 013. Career field hazards

1. What three factors determine the severity of electric shock?

2. What amount of current flow (or more) through the body can cause a shock that may result in cardiac arrest?

3. What are the two *primary* hazards associated with climbing?

4. Name the two types of radiation that you may encounter in your duties as a RAWS radio guide technician.

### 014. Safety precautions and work center programs

1. While working on energized equipment, personnel should never wear what items as they may increase the shock risk or be the source of potentially severe burns when energized?

2. Unless the nature of the work requires the circuits to remain energized, what should you do *before* attempting any work?

3. Define the term “high voltage.”

4. How often should EMF emitters be inventoried to identify new emitters and evaluations conducted if operations change or new systems are added to the inventory?

5. How should hazardous EMF exposure areas be marked when English is not the primary language?

6. What type of liquids are categorized as Class I liquids, Type II, and III liquids?

7. What should you wear whenever charging, maintaining, removing and/or replacing batteries?

8. Why should you never rely on the color-coding of a compressed gas cylinder?

9. Why should pregnant personnel immediately notify their primary care managers and public health?

### 015. Tower climbing and safety requirements

1. Who designates personnel required to maintain climbing proficiency?

2. After initial climbing training, when should recurring training be conducted?

3. When climbing, what three points of contact should you have at all times?

4. Other than a harness and lanyard, what two PPE items are required by OSHA while climbing?

5. What *must* a rescue plan ensure in order to prevent or minimize permanent injury or death?

6. In a rescue situation, on what three things should all tower workers be qualified?

7. What are the three types of climbing hazards?

8. At what wind speed are you *required* to get off the tower?

9. What are two of the biggest effects the sun can have on you when climbing?

10. If you see corrosion on a steel tower, how would you treat it?

11. What two things indicate cracks in a tower section is causing stress on the structure?

12. Per AFMAN 91–203, how often shall supervisors ensure all PFAS components receive a thorough inspection?

13. By how much can a knot reduce the strength of a lanyard?

14. Name the two most commonly used types of rope RAWS technicians will use while climbing?

15. How often should you inspect a kernmantle rope?

16. When used for climbing, carabiners should be inspected for what three things?

## 2–2. Publications and Directives

Communications technology has significantly changed how the Air Force conducts day-to-day business. Today's fast-paced telecommunications environment gives you access to an abundance of information. Records, forms, and publications are at your fingertips and nearly all official government forms and publications are available from official governmental websites. Having access to these publications is critical for completing the Air Force mission. In order to be successful, you must have a basic understanding of the different publications that are available to you.

### 016. Department of Defense publications and directives

Since Operation Desert Storm, there is arguably no other topic within the DOD that has received more attention, or generated more controversy, than information operations (IO). In 1995, both the Joint Staff and armed services consolidated their ideas as the first drafts of joint and armed services

doctrine circulated around the DOD. These early efforts illustrated that there was no clearly settled consensus on IOs.

The DOD sets policies and publishes them through publications and directives. These can be accessed through the following websites:

- The official website is http://www.defense.gov.
- DOD publications are located at http://www.dtic.mil/whs/directives/corres/pub1.html.
- DOD directives are located at http://www.dtic.mil/whs/directives/corres/dir.html.

### Joint publications

Joint publications (JP) are prepared under the direction of the chairman of the Joint Chiefs of Staff (CJCS). They set forth joint doctrine governing the activities and performance of the armed forces of the United States. Joint publications focus on armed forces activities in joint operations. JPs provide the doctrinal basis for interagency coordination and for US military involvement in multinational operations. JPs provide military guidance for the exercise of authority by combatant commanders and other joint force commanders and prescribes joint doctrine for operations and training. JPs also provide guidance for the military services to use in preparing appropriate joint operations plans.

Joint doctrines provide common governance for joint warfighting. One important publication is Joint Publication 3–13, *Information Operations*, which provides a doctrine for information operations (IO) planning, preparation, execution, and assessment in support of joint operations. Joint doctrines set forth a means to govern the activities and performance of the armed forces of the US in joint operations. The different JPs provide guidance for the armed forces in preparing strategic plans.

### Allied communication publications

Allied communication publications (ACP) standardize communication procedures for allied forces. One such example is ACP 133, *Common Directory Services and Procedures*. This ACP defines the directory services, architecture, protocols, theory, policies, and procedures to support allied communications, including Military Message Handling System services based on ACP 123, *Common Message Strategy and Procedures*, in both the strategic and tactical environments.

Another example is ACP 117, *Allied Routing Indicator Book*. This publication provides information for routing message traffic within and/or between communications systems and for transferring message traffic between national communications systems. This ACP contains a list of the routing indicators and routing information to be used on the common-user data networks of the United States and selected allies.

## 017. Air Force publications

Determining policy is an important function for Air Force leadership. Policy provides both a focus for Air Force action and a guide for the behavior of an organization and its members. Title 10 United States Code, Section 8013, states that the secretary of the Air Force (SAF) is responsible for “the formulation of policies and programs by the Department of the Air Force that are fully consistent with national security objectives and policies established by the President or the Secretary of Defense.” In addition, Section 8013 states that the secretary is responsible for “the effective and timely implementation of policy, program, and budget decisions and instruction of the President or the Secretary of Defense.”

The SAF as the head of a DOD component, or his/her designated official(s) reviews and coordinates on proposed DOD Issuances that are relevant to the Air Force mission. The SAF ensures Office of the Secretary of Defense (OSD) policy is carried out by issuing AF publications, as required, and according to Headquarters Operating Instruction (HOI) 90–1, *Headquarters Air Force Mission Directives and Department of Defense Issuances Program*, and AFI 33–360, *Publications and Forms Management*.

## Types of Air Force publications

The Air Force Departmental Publishing Office (AFDPO) manages Air Force publications. The AFDPO, under the director, Headquarters Air Force Information Management (HAF/IM), implements Air Force publications, and forms management guidance and serves as the headquarters' publications and forms manager. AFDPO maintains and manages the E-Publishing website, assists the office of primary responsibility (OPR) with creating and developing publications and forms, provides customer service support, procures special printing jobs for senior leadership, and issues unique departmental publications and forms. The AFDPO mission is to provide publishing products and services for administrative publications and forms to Air Force customers worldwide.

Air Force publications and forms are developed, distributed, and used by Air Force personnel to provide official policy and guidance. The Air Force E-Publishing website provides a wealth of official Air Force forms and publications. The official website for Air Force E-Publishing is http://www.e-publishing.af.mil. The following table discusses the different type of publications that are available through the AF E-Publishing system.

| **Official Air Force Publications** | |
|---|---|
| **Type** | **Description** |
| Air Force doctrine documents (AFDD) | AFDDs explain the Air Force's perspective on information superiority, and the relationship between IOs and its two pillars, information warfare and information-in-warfare. One is AFDD 2–5, *Information Operations*, which focuses its discussion primarily on information warfare. The "gain" and "exploit" aspects of IOs are explained in:<br>• AFDD 2–5.1, *Electronic Warfare.*<br>• AFDD 2–9, *Intelligence Surveillance and Reconnaissance*. |
| Air Force instructions (AFI) | AFIs are directive publications that provide essential procedural guidance on implementing Air Force policies. For example, you know there are specific requirements for dress and appearance. AFI 36–2903, *Dress and Personal Appearance of Air Force Personnel*, helps to guide you in your dress and appearance and it provides specific requirements for everything from hair length to proper wear of the uniform. |
| Air Force policy directives (AFPD) | AFPDs are drafted at the Air Force level and provide guidance for AFIs. AFIs are drafted at the MAJCOM and FOA level. AFPDs are orders of the Secretary of the Air Force and contain directive policy statements of Office of the SAF and HQ USAF to initiate, govern, or regulate actions of conduct, within their specified areas of responsibility. |
| Air Force manuals (AFMAN) | AFMANs are guidance documents for procedures that contain examples for performing standard tasks, or supporting education and training programs. One example is AFMAN 33–326, *Preparing Official Communications*, which provides procedural guidance on how to write official Air Force correspondence. |
| Air Force pamphlets (AFPAM) | AFPAMs are informational publications which are "*how to*" documents. AFPAMs are *not* directive in nature. One example is an AFPAM, which provides guidance on how to properly fill out a form, but has no authority to enforce you to do so. AFPAMs have an informal writing style designated to maintain the reader's interest. An example is AFPAM 34–1202, *Guide to Protocol*. |
| Operating instructions (OI) | OIs assign directive actions, responsibilities, and prescribe procedures. OIs differ from AFIs in that they are written at a much lower organizational level, such as a squadron or flight level. OIs are likely to be much more detailed and specific in contrast to AFMANs or AFIs. Superintendents or flight chiefs commonly write OIs. Many OIs can contain systematic procedures for local tasks or operations. |

## Other types of publications

A few publications you will use as a RAWS technician are commercial vendor and FAA publications. Commercial publications will not override AFIs but will sometimes help fill a gap in information about a product or system. The next paragraphs will briefly explain both publications.

### *Commercial vendor publications*

The Air Force contracts with many commercial vendors in day-to-day operations, thus requiring the DOD to accept vendor publications. These organizations have publications of their own, which must be used by Air Force personnel. Commercial off-the-shelf (COTS) manuals are generally developed at contractor expense and are sellable as a commodity item. The Air Force must deal with issues, that is, proprietary data rights, copyright restrictions, and a myriad of different formats for this type of data. The Technical Order Management Agency (TOMA) cannot assume that just because the Air Force purchased a COTS item, that the government owns the rights to the technical data. Each contractor can set their own restrictions on the sale, printing, distribution, and storage of COTS technical data.

### *Commercial off-the-shelf versus new development*

Existing commercial operating instructions (COI), parts breakdown handbooks, and repair manuals are acquired instead of developing new TOs if no degradation in system operation, safety, support or reliability will result according to AFI 63–101/20–101, *Integrated Life Cycle Management*. Using existing data will save money and time for the TO program. COTS manuals are reviewed and evaluated by the TOMA, MAJCOM, and assigned equipment specialists according to MIL-PRF–32216, *Evaluation of Commercial Off-the-Shelf (COTS) Manuals and Preparation of Supplemental Data*.

Approved manuals will be adopted for Air Force use, assigned a TO number and managed in the TO system unless a waiver is approved. Approved manuals will be developed to identify pertinent information associated with COTS manuals. An identifying technical publication sheet (ITPS) is posted as a cover page immediately on top of the COTS manual title page or safety summary and provide all necessary information about the manual to include definition of the AF limits of releasability and/or data rights.

### *Federal Aviation Administration publications*

Simply put, FAA publications and manuals are those used by the FAA to regulate air transportation procedures. The intent of such regulations are to advance the growth and safety of air travel, military and civilian, while simultaneously satisfying national defense needs. They are located on the aeronautical data exchange (ADX). You can access publications at the following link: https://www.adx.faa.gov/portal/.

According to the FAA, “The ADX is a portal-based ‘data-mart’ tailored to distribute aeronautical related data to FAA employees, contractors, DOD Personnel, and the aviation community.” The ADX site provides up-to-date manuals for the digital air surveillance radar (DASR) and the STARS and provides services to field level technicians. These services were developed using an open source enterprise portal framework from Liferay and include document and asset repository, collaboration, and subscription/notification capabilities. ADX allows access to locally archived data and customized reports, as well as providing the capability for brokered access to data not stored on ADX. Providing this one-stop-shop service, ADX has been employed supporting the FAA mission for over 15 years.

The ADX is the primary storehouse that maintains all the TOs and updated adaptation files. The ADX site also provides the following data and collaboration services:

- Data products.
- Adaptation information.
- Aeronautical information.

- Product change information.
- Custom queries and filters.
- System wide information management (SWIM)-compliant Web services.
- Communities of interest.
- Document and asset repository.
- RSS services.
- Subscriptions.

## 018. Technical orders

The Air Force Standard TO Management System is used for the configuration management, storage, and distribution of TO management and content data. The scope of the Air Force Standard TO Management System includes activities from the creation and publication of TOs to their eventual decommissioning. The system includes hardware and software, personnel and facilities, and all manuals developed or acquired for organic operation, maintenance, inspection, modification, or management of centrally acquired and managed Air Force military programs and end items. These TOs are developed according to technical manual specifications and standards, non-embedded personal computer software which automates the function directed by a TO, contractor-developed manuals adopted for Air Force use, and approved COTS manuals.

### Enhanced Technical Information Management System

The principal automated TO management applications is the Enhanced Technical Information Management System (ETIMS). This application is employed to establish and manage information about Air Force TOs, disseminate current information on available TOs, manage technical order distribution office (TODO) accounts for the ordering of TOs and the maintenance of TO records, and enable the viewing of electronic technical orders (eTO) online in the ETIMS connected mode and on eTools in the ETIMS disconnected mode.

ETIMS is the AF system of record, a secure web, Global Combat Support System-Air Force (GCSS-AF) application accessible by the AF portal with the TO catalog, ordering and the TODO account management functions. ETIMS system functions to acquire, improve, publish, catalog, manage, store, distribute, and display official TOs needed for safe and effective operation of AF weapon systems and equipment. ETIMS connects TO users and TO managers in the operational environment. ETIMS users are assigned “roles” that include a set of system privileges using a specific role to provide capability to perform various functions.

ETIMS features an active eTO content repository, an eTO publisher/transformer, and an eTO viewer with online (connected) and portable (disconnected) modes. Primary users are TOMAs, TODO personnel, TO distribution account personnel, TO library custodians, eTool administrators, and TO users.

### Technical order identification

The basic task of TO numbering specialists is to group similar TO data into categories, systems, equipment series and equipment sub-series by means of an identifying numeric or alphanumeric TO number. There are 41 categories that a TO can be numerically grouped into. TOs are grouped numerically by type of equipment covered by the TO category. The listing of TO categories can be found in TO 00–5–18, *AF Technical Order Numbering System*.

#### *Breaking down the numbers*

Each category of TO data has its own TO numbering pattern. Sufficient flexibility exists within the total numbering system to allow for expansion or contraction within numbering parameters, yet maintain standard application of numbering patterns within each category.

TO numbers are composed of groups separated by dashes, and each group is further divided into parts. The number of parts within any group varies according to the TO data being numbered in a specific category. Each part of a group consists of one or more numeric characters or one or more alpha characters.

Seven groups may be used in the TO numbering pattern. TO data is identified, in most categories, by using only the first three or four basic groups. The remaining groups are primarily used to extend the TO number to identify specific sections of sectionalized TOs, supplemental manuals, and supplement checklist and work-card sequence numbers.

The five major elements of information considered most essential in assigning TO numbers are federal supply class (FSC), descriptive nomenclature, functional system, part number, and the Joint Electronics Type Designation System (JETDS) nomenclature. These are explained further in the next paragraphs.

### *Federal supply class*

An FSC is assigned to Air Force stock listed equipment by cataloging specialists. A system or equipment item that has not been assigned an FSC is non-stock listed, and a TO number will not be assigned to the related technical data. The FSC identifies a system, sub-system, and equipment series that can be related to a TO category and equipment series. The FSC is the first four digits of the National Stock Number. **EXAMPLE:** FSC 5825 identifies ground radio navigation equipment and relates to TO numbering as you see in the following table.

| **31R4 Breakdown** | |
|---|---|
| 31 | Ground Electronic Equipment (Category 31) |
| R | Radio System |
| 4 | Navigation Equipment Series |

### *Descriptive nomenclature*

The nomenclature provided on the ETIMS screens or Air Force Technical Order (AFTO) 203, Technical Order Numbering, Indexing, and Control Record, supplements the FSC by further defining the system or equipment series. A combination of only the FSC and the descriptive nomenclature in many instances can provide the numbering specialist with a complete TO number. For example, if FSC 5826, airborne radio navigation equipment, is provided in conjunction with an equipment nomenclature reading Maintenance Manual—Radio Set, Type AN/ARN–24, the following TO number may be assigned.

| **12R5–2ARN24–2 Breakdown** | |
|---|---|
| 12 | Airborne Electronic Equipment (Category 12) |
| R | Radio system |
| 5 | Navigation Equipment Series |
| 2 | Numeric 2 indicates the Equipment has a JETDS nomenclature |
| ARN | JETDS Nomenclature that indicates: A - Airborne; R - Radio; N - Navigation |
| 24 | Radio Model 24 |
| 2 | Maintenance Manual |

### *Functional system*

The functional system furnished on the ETIMS screens or AFTO Form 203 is the next higher echelon of equipment or system for the equipment covered by the subject TO. The functional system identifies an equipment series if the TO being numbered covers an equipment sub-equipment series. The functional system identifies a system if the TO being numbered covers an equipment series.

### *Part number*

A TO number will not normally be assigned to equipment without a part number, model number, or other identifier. All part numbers, model numbers or any other identifiers will be included in the TO title. If the equipment is not already listed in ETIMS then the equipment specialists or item manager must enter it using the ETIMS maintain equipment screen. Data to be entered includes the weapon system application, the equipment part number, and the manufacturer/vendor Commercial and Government Entity (CAGE) code. This data is then extracted from ETIMS for the TO-Equipment number Cross-Reference section of the TO catalog.

### *Joint Electronics Type Designation System nomenclature*

JETDS is a method developed by the US War Department during World War II for assigning an unclassified designator to electronic *equipment*. If the JETDS (formerly ‘‘AN’’) nomenclature appears in the title lines of a TO, it must be reflected in the TO number. Below is a table showing what the first letter relates to in terms of the general equipment group or installation.

| First letter | Installation |
|---|---|
| A | Piloted aircraft |
| B | Underwater mobile (submarine) |
| C | Cryptographic equipment National Security Agency (NSA) use only |
| D | Pilotless carrier (drone, unmanned aerial vehicle [UAV]) |
| F | Fixed ground |
| G | General ground use |
| K | Amphibious |
| M | Ground mobile |
| P | Human portable |
| S | Water (surface ship) |
| T | Transportable (ground) |
| U | General utility (multi use) |
| V | Vehicle (ground) |
| W | Water surface and underwater combined |
| Z | Piloted/pilotless airborne vehicles combined |

The next table shows the second letter in the designation and a more specific type of equipment.

| Second letter | Type of equipment |
|---|---|
| A | Invisible light, heat radiation (infrared) |
| B | Communications security (COMSEC) (NSA use only) |
| C | Carrier (electronic wave or signal) |
| D | Radioactivity detection, identification, and computation |
| E | Laser |
| F | Fiber optics |
| G | Telegraph or teletype |
| I | Interphone and public address |
| J | Electromechanical or inertial wire covered |
| K | Telemetering |
| L | Countermeasures |
| M | Meteorological |
| N | Sound in air |
| P | Radar |

| Second letter | Type of equipment |
|---|---|
| Q | Sonar and underwater sound |
| R | Radio |
| S | Special or combination |
| T | Telephone (wire) |
| V | Visual, visible light |
| W | Armament (not otherwise covered) |
| X | Fax or television |
| Y | Data processing |
| Z | Communications (NSA use only) |

The third letter describes the purpose associated with the equipment. These are explained below.

| Third letter | Purpose |
|---|---|
| A | Auxiliary assembly |
| B | Bombing |
| C | Communications (two way) |
| D | Direction finding, reconnaissance and surveillance |
| E | Ejection and/or release |
| G | Fire control or searchlight directing |
| H | Recording and/or reproducing |
| K | Computing |
| M | Maintenance or test |
| N | Navigation aid |
| Q | Special or combination |
| R | Receiving or passive detecting |
| S | Detecting, range and rearing, search |
| T | Transmitting |
| W | Automatic flight or remote control |
| X | Identification or recognition |
| Y | Surveillance and control |
| Z | Secure (NSA use only) |

Following the three-letter designation, after a dash, is a number that uniquely identifies the equipment. For example, a GRC–171 Transceiver nomenclature can be broken down like this: the first letter “G” is for general ground use, the second letter “R” is for radio, and the third is “C” which correlates to two-way communications. The “171” is a unique identifier for that equipment. When it is all put together, it is a ground radio transmitter/receiver (transceiver).

### *Numbering related technical orders*

The following table provides brief definitions of dedicated numbers used in most TO categories, except categories 1, 21, and 22. (Additional numbers are required in categories 1, 21, and 22 to identify distinct types of TO data.) The TOs are often referred to as “dashes”, for example, the OIs are in the “dash one” TO.

| TO Dedicated Numbers | |
|---|---|
| –01 | List of applicable publications (LOAP) |
| –06 | Work unit code (WUC) manuals |
| –1 | Operating instructions |

| TO Dedicated Numbers | |
|---|---|
| –2 | Organizational, Intermediate, field maintenance, or service manuals, troubleshooting and repair manual |
| –3 | Depot maintenance, overhaul, schematic, or wiring diagram manuals |
| –4 | Parts list, parts breakdown or illustrated parts breakdown manuals |
| –6 | Inspection requirement manuals |
| –7 | Installation and installation test procedure manuals |
| –8 | Test procedures, user manuals, reference manuals, programmed test manuals, or software-related instruction manuals, configuration guide |
| –9 | Alignment instruction manuals |

**NOTE:** The number –5 is used to identify a wide variety of types of TOs, depending on the applicable TO category. The number –8 includes subsequent sequence numbers indicated as 8–1, 8–2, 8–x, and so forth. This sequence number is used in all categories.

### Time compliance technical orders

Time compliance technical orders (TCTO) provide instructions to modify military systems or commodities within specified time limits, initiate special “one time” inspections to impose temporary restrictions and track support system and equipment configuration on systems or equipment. TCTO priority levels (PL) are categorized as Immediate Action, Urgent Action, Routine Action, Routine Safety Action and Record. The category determines the compliance period. These levels are extensively explained in TO 00–5–15, *Air Force Time Compliance Technical Order Process*.

TCTOs for fielded systems and equipment are planned, prepared, and issued by the responsible equipment specialist/technical content manager (ES/TCM) (or modification manager) under the authority of the affected system, equipment program manager, and/or supply chain manager. The TO manager is responsible for assisting an ES/TCM or modification manager with the development and publication of TCTOs and related TO updates.

The TCTO implementation process follows a systematic regimen involving QA, program management office, work centers, plans scheduling and documentation, supply, and item managers. When a TCTO is needed at your site, you may receive parts or equipment, if necessary, by mail or through the supply system. Detailed instructions will guide technicians on every step of completing the TCTO. Coordination with other agencies, such as the Communications Squadron, may be needed to assist with installation. When TCTO actions are completed by the performing work center, all pertinent information will be loaded into the IMDS as a matter of record and disposition of any removed equipment can begin, if applicable.

### Standard installation practices technical orders

Standard installation practices technical orders (SIPTO) are basic manuals for standard installation practices, identifying tools and equipment, detailing safety procedures, and general services allied to installation and maintenance of many types of Air Force equipment and systems.

The contents of a SIPTO are intended to acquaint and inform installation personnel with basic standard practices associated with equipment, facilities and systems. They serve as a manual of instruction in the development of installation and maintenance proficiency with a minimum of formal training time. SIPTOs also provide a reference, which will facilitate the proper installation of equipment, systems, and supporting items inside and outside facilities in support of the Air Force mission.

SIPTOs are go-to references for Engineering and Installation (E&I) squadrons and for RAWS work centers looking for general and specific information to assist with tasks such as grounding, terminating and soldering, cabling, anchoring, and many other installation practices.

## 019. Industry and military standards

As you are aware, TOs and commercial manuals provide standards for maintaining or OSs that are approved for use in the Air Force. There are also industry standards that manufacturers use to develop products, as well as military standards (MIL-STD), which approve or disapprove systems for use within the DOD. This lesson will provide information for some enterprise and telecommunications standards as well as detail MIL-STDs.

### Enterprise and telecommunications standards

Commercial companies must follow many industry standards for communications equipment. These standards define how systems interconnect and interface with similar systems of various manufacturers. Additionally, there are standard connections that many companies use to cut down on the development of proprietary connections and components. Below is a description of some of the leading industry standards utilized with communications equipment.

#### *American National Standard Institute*

The ANSI oversees the creation, publication, and use of norms and guidance that directly influence nearly every sector of business. ANSI is responsible for the civilian accreditation of the many industry standards used to develop the cyberspace support equipment the Air Force operates and maintains. The most common industry standards used in communications are Electronic Components Industry Association (ECIA) and Telecommunications Industry Association (TIA).

#### *Telecommunications Industry Association*

TIA is the leading trade association representing the global information and communications technology (ICT) industries through standards development, government affairs, business opportunities, market intelligence, certification, and worldwide environmental regulatory compliance. TIA is accredited by ANSI and develops industry standards for a variety of ICT segments. It operates in the 12 engineering communities, which develop guidelines for various communications equipment commonly used or maintained by RAWS support technicians.

TIA produces various standard publications for ICT products as well as the glossary of telecommunication terms. The Electronic Industries Alliance (EIA)/TIA glossary of telecommunication terms provides definitions and explanations for more than 5,800 engineering words and phrases in the ICT industry. The TIA commercial standards are available for purchase on their website at www.tiaonline.org.

#### *Electronic Components Industry Association*

Formerly known as EIA, ECIA is responsible for developing standards for interconnect, passive and electro-mechanical electronic components under the ANSI-designation of EIA standards. Nearly all equipment used within the DOD meets these standards for interconnection with other equipment using EIA/ANSI approved connectors such as RS–232 and RS–422 serial interfaces.

### Military standard

A United States defense standard, often called a military standard (MIL-STD) or military specification (MIL-SPEC) is used to help achieve standardization objectives by the DOD. Standardization is beneficial in achieving interoperability ensuring products meet certain requirements, commonality, reliability, total cost of ownership, compatibility with logistics systems, and similar defense-related objectives. Defense standards are also used by other non-defense government organizations, technical organizations, and industry.

Although the official definitions differentiate between several types of documents, all of these documents are commonly referred to as “military standards”, including defense specifications, handbooks, and standards. Strictly speaking, these documents serve different purposes. According to the Government Accountability Office, MIL-SPEC describe the physical and/or operational characteristics of a product, while MSs detail the processes and materials to be used to make the

product. Military handbooks, on the other hand, are primarily sources of compiled information and/or guidance. See the following table for additional information.

| Military Standards | |
|---|---|
| Military Standard (MIL-STD) | Establishes uniform engineering and technical requirements for military-unique or substantially modified commercial processes, procedures, practices, and methods. There are five types of defense standards: interface standards, design criteria standards, manufacturing process standards, standard practices, and test method standards. MIL-STD–962, *Defense Standards Format and Content,* covers the content and format for defense standards. |
| Military Handbook (MIL-HDBK) | A guidance document containing standard procedural, technical, engineering, or design information about the material, processes, practices, and methods covered by the Defense Standardization Program (DSP). |
| Military Specification (MIL-SPEC) | Describes the essential technical requirements for purchased material that is military unique or substantially modified commercial items. MIL-STD–961, *Defense and Program-unique Specifications Format and Content,* covers the content and format for defense specifications. |
| Military Performance (MIL-PRF) | A performance specification that states requirements in terms of the required results with criteria for verifying compliance, but without stating the methods for achieving the required results. A performance specification defines the functional requirements for the item, the environment in which it must operate, and interface and interchangeability characteristics. |
| Military Detail (MIL-DTL) | A specification that specifies design requirements, such as materials to be used, how a requirement is to be achieved, or how an item is to be fabricated or constructed. A specification that contains both performance and detail requirements is still considered a detail specification. |

MIL-STDs are published and approved through the DSP and are posted on the Acquisition Streamlining Standardization Information System (ASSIST) website (https://assist.dla.mil). It is important to note that while these standards are located in numerous places throughout the Internet, ASSIST is the only official source for DSP publications.

## Self-Test Questions

**After you complete these questions, you may check your answers at the end of the unit.**

### 016. Department of Defense publications and directives

1. The DOD sets policies and publishes them through what means?

2. JPs provide the doctrinal basis for what?

3. What do ACPs provide?

### 017. Air Force publications

1. What are developed, distributed, and used by Air Force personnel to provide official policy and guidance?

2. Directive publications that provide essential procedural guidance on implementing Air Force policies are called what?

3. Which type of Air Force publications assign directive actions, responsibilities, and prescribe procedures but are written at a much lower organizational level such as a squadron or flight level?

4. Where will an identifying technical publication sheet be posted in a COTS manual and what information does it provide?

5. What are FAA manuals used for?

### 018. Technical orders

1. In what system can you view eTOs with or without Internet access?

2. How are TOs systematically grouped together?

3. What are the five major elements of information considered most essential in assigning TO numbers?

4. Using the equipment nomenclature tables, what does TRN–48 stand for?

5. In what type of dedicated TO number would an illustrated parts breakdown be listed?

6. Which TOs provide detailed instructions for the modification of military equipment?

7. If your work center was ensuring that the grounding system of a facility was installed within Air Force tolerances, what type of TO would you use to find guidance?

### 019. Industry and military standards

1. Which organization is accredited by the ANSI and develops industry standards for a variety of ICT segments?

2. Which association is responsible for developing standards for IP&E electronic components under the ANSI-designation of EIA standards?

3. Match the definitions in Column B to the appropriate military standard term in Column A. Items in Column B will only be used once.

| *Column A* | *Column B* |
|---|---|
| ____ (1) MIL–STD. | a. Defines the functional requirements for the item, the environment in which it must operate, and interface and interchangeability. |
| ____ (2) MIL–HDBK. | b. Establishes uniform engineering and technical requirements for military-unique or substantially modified commercial processes, procedures, practices, and methods. |
| ____ (3) MIL–SPEC. | c. Specifies design requirements, such as materials to be used, how a requirement is to be achieved, or how an item is to be fabricated or constructed. |
| ____ (4) MIL–PRF. | d. Describes the essential technical requirements for purchased material that is military unique or substantially modified commercial items. |
| ____ (5) MIL–DTL. | e. A guidance document containing standard procedural, technical, engineering, or design information about the material, processes, practices, and methods covered by the Defense Standardization Program. |

## 2–3. Security

Air, space, and cyberspace power projection assets are critical enablers to the national security of the United States and contribute to the achievement of national strategy objectives**.** A central and fundamental component of the Air Force capability is power projection platform operations and installations, along with the most important critical enabler, professional Airmen. Both require a deliberate and focused security strategy for protecting and defending air, space, and cyberspace power, one that considers mission accomplishment, threats, vulnerabilities, and the inherent risks associated with operation of a military installation. Within the Air Force, that strategy is Integrated Defense. This section will describe the physical security aspect of Integrated Defense in relation to secure areas and facility security requirements.

### 020. Physical security

You must safeguard Air Force war-fighting resources from theft, damage, or destruction in both peace and wartime. Physical security works with other security programs to protect classified, sensitive, and high-value information, equipment, and facilities. Conducting security operations that present hostile persons or groups with unacceptable risks and penalties if they attempt to breach the security system achieves deterrence.

#### Defining physical security

Physical security is the part of COMSEC that results from using all physical measures necessary to safeguard COMSEC material from access by unauthorized personnel. Physical security measures include applying control procedures and physical barriers. Apply physical security to comply with national policy requiring the US government to safeguard and control COMSEC materials.

The physical security program provides guidance to deter, detect, and defeat hostile acts against

Air Force priority resources and helps leaders make sound resource allocation decisions to achieve these goals. The objective of the program is to achieve a reasonable degree of security relative to the importance and value of priority resources.

Physical security also assures the continued integrity, prevents access by unauthorized persons, and controls the spread of COMSEC techniques and technology when it is not in the best interest of the US and its allies. Common physical security measures include verifying the need to know and clearance of personnel granted access, following proper storage and handling procedures, accurately accounting for all materials, transporting materials using authorized means, and immediately reporting the loss or possible compromise of materials. For additional information, refer to AFPD 31–1, *Integrated Defense*.

### Resource designations

Security plans will consider both peacetime and advanced threat environments. Ensure security provisions at home station and deployed locations are at an appropriate level. Security arrangements are regularly exercised, reviewed, and evaluated. Headquarters US Air Force assigns security priorities and approves security standards based on the importance of each system to the mission. The four common resource PL designations, “PL1,” “PL2,” “PL3,” and “PL4” are described in the table below.

| **Resource Designation Security** | |
|---|---|
| **Priority** | **Description** |
| PL1 | PL1 is assigned to those resources for which the loss, theft, destruction, misuse, or compromise would result in great harm to the strategic capability of the United States.<br>Examples of PL1 resources are nuclear weapons in storage, mated to a delivery system, or in transit; designated command, control, and communications (C3) facilities; and aircraft designated to transport the president of the United States.<br>PL1 security must result in the greatest possible deterrence against hostile acts. This level of security will provide maximum means to achieve detection, interception, and defeat of a hostile force before it is able to seize, damage, or destroy resources. |
| PL2 | PL2 is assigned to resources for which the loss, theft, destruction, misuse, or compromise would cause significant harm to the war-fighting capability of the United States.<br>Examples of PL2 resources are nonnuclear alert forces; designated space and launch systems; expensive, few in number, or one-of-a-kind systems or facilities; and intelligence gathering systems.<br>PL2 security must result in significant deterrence against hostile acts. This level of security will ensure a significant probability of detecting, intercepting, and defeating a hostile force before it is able to seize, damage, or destroy resources. |
| PL3 | PL3 is assigned to resources for which the loss, theft, destruction, misuse, or compromise would damage United States war-fighting capability.<br>Examples of PL3 resources are non-alert resources that can be generated to alert status, such as F–16 fighters; selected C3 facilities, systems, and equipment; and non-launch-critical or non-unique space launch systems.<br>PL3 security must result in a reasonable degree of deterrence against hostile acts. This level of security ensures the capability to impede a hostile force and limit damage to resources. |
| PL4 | PL4 is assigned to resources that do not meet the definitions of PL1, PL2, or PL3 resources, but for which the loss, theft, destruction, misuse, or compromise would adversely affect the operational capability of the Air Force.<br>Examples of PL4 resources are facilities storing Category I, II, or III sensitive conventional arms, ammunition, and explosives; fuels and liquid oxygen storage areas; and Air Force accounting and finance vault areas.<br>PL4 resources are secured by containing them in controlled areas. Unit commanders are responsible to provide physical protection for PL4 resources. Security forces conduct preventive patrols in areas and provide armed response. |

Trained and equipped security forces detect possible hostile acts, discriminate between hostile and non-hostile occurrences, initiate an alarm, and deny hostile forces the ability to damage or destroy priority resources. Electronic security systems that increase security levels should be used to improve security and reduce risk in addition to, or in place of, security force manpower.

## 021. Facility security

Secured facility vulnerabilities are weaknesses that make a facility subject to attack or damage. A secured facility is vulnerable when it is not protected according to standards, or when it does not have the protection required to counter a known or perceived threat. This lesson will outline certain requirements that you need to know in order to eliminate vulnerabilities at your current location and all assignments throughout your career.

### Identifying and reporting vulnerabilities

Secured facilities receive extensive inspections during resource protection program reviews. These inspections identify most vulnerabilities and the survey report records deficiencies that require further investigation.

How easy can you fix the problem? How much will it cost? What is the nature of the threat? How much risk can the installation accept for that particular facility? These are just a few things to consider.

Any deviations from prescribed security standards require correction or waivers. If it is a slight problem (within 10 percent of the standard) and fixed within 60 days, no deviation request is required. Otherwise, the activity that is responsible for the facility must submit a deviation request.

There are three types of secured facility deviations—temporary, permanent, and technical.

- Temporary deviations (*waivers*) which are granted for one year.
- Permanent deviations (*exceptions*) which are granted for two years.
- Technical deviations (*variances*) which are granted indefinitely.

If an organization submits a waiver request, it must also include some measures to compensate for the problem until it is repaired. Compensatory measures include extra security patrols, new procedures, barricades, or additional locks.

### Secured facility security requirements

Secured facilities and the areas surrounding them require controlled access. There are two basic criteria you must meet in order to enter a controlled area—qualification and authorization.

| Security Requirements for Secured Facilities | |
|---|---|
| Controlled area qualification | The installation commander determines the basic entry qualifications, which can range from local file checks to in-depth special investigations. |
| Controlled area authorization | The installation commander also grants authority for people to enter controlled areas. You may find that on your installation your unit commander delegates this authority. |

The unit's controlled area monitor trains personnel working in secured areas. They must receive training before they gain access to the facility and must receive training annually thereafter. Training and awareness are the most important aspects of the controlled area program. A flawless administrative program is of no value if people working in and around the controlled area are not trained and vigilant. Most loss, damage, and theft of military resources are the result of a lack of care, concern, or awareness. Seldom does loss, damage, or theft of resources result from insufficient physical safeguards.

## Facility security requirements

There are numerous types of facilities used to support the Air Force mission. Critical communications facilities, such as the DISN, include facilities located on and off military installations. Physical security requirements vary significantly based on the type of business conducted and information processed within the facility. Because of differences in location, the physical layout of equipment, and security you must assess security considerations for each facility.

To help understand facility security requirements, you need to know about secure areas and the control measures used for facilities.

### *Secured areas*

Secured areas include restricted areas, controlled areas, and limited access areas. These areas are briefly described below. There will be many different types of secured areas in the Air Force but they will fall into these general areas.

| Secured Areas | |
|---|---|
| **Type** | **Description** |
| Controlled areas | A controlled area is any building, area, or structure containing Air Force resources that are a lucrative target for theft, compromise, or destruction.<br>More protection is provided by limiting entry into these areas.<br>Make sure, only authorized personnel have access to controlled areas. |
| Restricted areas | Entry to a restricted area is subject to special restrictions or control for security reasons or to safeguard property or material.<br>Only authorized personnel have access to restricted areas.<br>Personnel requiring access to a restricted area must possess a valid restricted area badge. |
| Limited access areas | These are similar to restricted areas.<br>Only authorized personnel can enter these areas.<br>These individuals require by name identification on an access control list. |

### *Control measures*

Entry into a facility may need control measures because of sensitive data or expensive equipment. Access control measures provide a mechanism to achieve this. A control measure may be as simple as having to show a valid military identification card or as elaborate as voice pattern recognition and verification systems. The level of control present will be in direct proportion to the anticipated severity of damage caused by unauthorized access. In a secure area, there are two types of authorized access: unescorted and escorted. The table below describes control measures associated with escorted and unescorted access.

| Control Measures | |
|---|---|
| Unescorted access | If a work center is a controlled or restricted access area, an access control list will identify all personnel by name and Social Security number who are authorized access to these areas.<br>If your name is on the list, you have unescorted access to the area. |
| Escorted access | Authorized individuals on the access control list have permission to escort personnel who are not on the access list.<br>For example, if a facility is experiencing problems with the air conditioning system, maintenance personnel from the base civil engineering squadron may need to gain access to the facility to perform maintenance. In this case, they have escorted access to the facility.<br>An authorized individual permitted to escort visitors will accompany the escorted personnel and remain with them during their entire visit. |

### *Determining cleared personnel*

How do you know if someone has the necessary security clearance to enter a facility? If the individual is assigned to the unit, the unit security manager can tell you. If the individual is a visitor or inspector from another base, you can verify their clearance by checking their orders or contacting their home unit. If you are still unsure, check with your unit security manager before granting access.

Once you have determined an individual has an appropriate security clearance, how do you establish they have a valid need to know? With few exceptions, personnel who are conducting official business such as your flight commander, flight chief, unit commander, COMSEC manager, unit security manager, have a valid need to know. Personnel not identified by name on the access control list who have the proper security clearance and valid need to know must be signed in and out of the secure area on AF Form 1109, Visitor Register Log. Once signed in, these individuals require an escort and observation during their *entire* visit.

### *Unclassified areas*

Control measures as stringent as those above may not be required if you work in a typical office environment. There are reasons to control access to your area from visiting personnel who should not view documents containing Privacy Act information. Almost every office may handle some type of sensitive or personal data protected by the Privacy Act of 1974. This material must also be protected against theft or unauthorized viewing. Stay alert to possible threats and follow these general practices to protect sensitive material and prevent vulnerabilities:

- Do not arouse unnecessary interest in critical facilities.
- Place equipment where it cannot be seen or reached from window and door openings.
- Keep critical information systems separate from general use systems.
- Place general-use workstations in open, visible spaces to prevent clandestine (sneaky) use, unless they routinely display sensitive information.
- Maintain up-to-date logs of all equipment, with serial numbers, in a secure location.
- Mark equipment in a permanent and easily identifiable way. Also, label the inside of equipment with the organization’s name to serve as evidence of ownership.
- Limit and monitor access to equipment areas. Keep an up-to-date list of personnel authorized to access sensitive areas. Never allow equipment to be moved or serviced unless the task is preauthorized and service personnel can produce an authentic work order and verify who they are. Make picture and other forms of identification a requirement, if necessary, and maintain logs of all service and repair activity.
- Keep photocopiers, fax machines, and optical scanners in public view. Monitor their use since they disseminate information.
- Assign shared printers to users with similar security clearances.
- Label printed information appropriately.
- Destroy sensitive waste.

This concludes this unit on safety, publications and security programs. For additional information, always refer to Air Force and DOD instructions. This unit does not cover all aspects of safety, publications, security, and security measures. Be aware that the AFIs and procedures covering data and personal protection have constant revisions for accuracy. Always make sure that you are consulting and following the most recent publication version and procedures.

## Self-Test Questions

**After you complete these questions, you may check your answers at the end of the unit.**

### 020. Physical security

1. What is the objective of the Air Force physical security program?

2. What PL designation would the president's plane, Air Force One, be considered?

3. What PL designation would be given to a facility that holds ammunition and explosives?

### 021. Facility security

1. What are the two basic criteria you must meet in order to enter a controlled area?

2. Name the three types of secured areas.

3. When entering a secured area, personnel not identified by name on the access control list, who have the proper security clearance and valid need to know, must do what two things?

## Answers to Self-Test Questions

### 012

1. Commanders.
2. Department of Labor.

### 013

1. (1) Amount of current flowing through the body.
   (2) Time of exposure.
   (3) Body's physical condition.
2. 50 milliamperes or more.
3. Falls and contact with electrical systems.
4. Non-ionizing and ionizing radiation.

### 014

1. Rings, watches, or other conductive objects.
2. Make sure circuits are de-energized, locked, and tagged out.
3. Any RMS voltage of 600 volts, nominal, or greater.
4. Biennially.
5. Signs will be multilingual and compliant with the requirements of the host nation.
6. Flammable. Combustible.

7. Appropriate personal protective equipment, approved and certified in bioenvironmental's occupational and environmental health risk assessment.
8. Different manufacturers use different color codes.
9. To initiate a workplace evaluation for exposures that may be hazardous to the fetus and determination of work restrictions.

**015**

1. Unit commanders.
2. Annually, when work conditions change or new fall arrest systems are used.
3. Either one hand and two feet or two hands and one foot must be in contact with the tower or ladder *at all times*.
4. Steel-toed boots and a hard hat.
5. Ensure a rescue can be implemented very quickly.
6. (1) First aid.
   (2) Buddy care.
   (3) CPR.
7. (1) Environmental.
   (2) Live.
   (3) Structural.
8. 25 MPH.
9. Sunburns and dehydration.
10. Signs of corrosion should be removed with a wire brush and then sprayed with a coat of primer paint or any other rust prevention paint.
11. High winds or improper installation of guy wires and tower sections.
12. At least quarterly.
13. By 50 percent.
14. Kernmantle and fiber.
15. After each use.
16. (1) It has a spring loaded gate (keeper).
    (2) The gate is self-locking.
    (3) The carabiner is rated to handle 5,000 lb.

**016**

1. Publications and directives.
2. Interagency coordination and for US military involvement in multinational operations.
3. Standardized communication procedures for allied forces.

**017**

1. Air Force publications and forms.
2. AFIs.
3. OIs.
4. Posted as a cover page immediately on top of the COTS manual title page or safety summary and shall provide all necessary information about the manual to include definition of the AF limits of releasability and/or data rights.
5. To regulate air transportation procedures.

**018**

1. ETIMS.
2. Numerically by type of equipment covered by the TO category.
3. (1) Federal supply class.

(2) Descriptive nomenclature.
(3) Functional system.
(4) Part number.
(5) JETDS nomenclature.

4. Transportable radio navigational aid with “48” as its unique designator.
5. –4 or commonly referred to as “dash 4.”
6. TCTO.
7. SIPTO.

**019**

1. TIA.
2. ECIA.
3. (1) b.
   (2) e.
   (3) d.
   (4) a.
   (5) c.

**020**

1. Achieve a reasonable degree of security relative to the importance and value of priority resources.
2. PL1.
3. PL4.

**021**

1. Qualification and authorization.
2. (1) Controlled.
   (2) Restricted.
   (3) Limited access.
3. Must be signed in/out of the secure area on AF Form 1109 and are required to have an escort with observation during the *entire* visit.

**Complete the unit review exercises before going to the next unit**.

## Unit Review Exercises

**Note to Student:** Consider all choices carefully, select the *best* answer to each question, and *circle* the corresponding letter.

24. (012) Who is the only entity that can grant exemptions to Occupational Safety and Health Administration (OSHA) standards?
    a. Department of Labor.
    b. Air Force Chief of Safety.
    c. Major command (MAJCOM) commanders.
    d. Bioenvironmental Occupational and Environmental Working Group (BOEWG).

25. (013) Which action is *not* a determining factor for the severity of an electric shock?
    a. Amount of time exposed.
    b. Body's physical condition.
    c. Amount of current flowing through the body.
    d. Conductance ratio of voltage versus time exposed.

26. (013) What amount of current flow through the human body can cause shock that may cause you to go into cardiac arrest?
    a. 50 milliamperes or more.
    b. 40 milliamperes or less.
    c. 50 volts or more.
    d. 40 volts or less.

27. (013) Which statement is true regarding electrical arcing?
    a. Objects *must* contact the electricity source to create an arc.
    b. Objects do not have to contact the electricity source to create an arc.
    c. Arcing is not dangerous since it only exerts a small amount of the originating voltage.
    d. Arcing cannot occur when power is removed from the equipment you are working on.

28. (013) What does non-ionizing radiation cause?
    a. A cooling effect in the body.
    b. Radioactive poisoning of the blood.
    c. Damage of deep body tissues and organs.
    d. Radioactive poisoning of the cells in deep body tissues.

29. (014) When working on energized equipment, what is a good practice to perform?
    a. Make sure the equipment is tagged with Air Force Visual Aid 91–306, *DANGER—HIGH VOLTAGE*.
    b. Keep one hand in your pocket or behind your back.
    c. Have a safety observer, only if available.
    d. Permanently bypass all interlocks.

30. (015) What are the two types of fall protection?
    a. Rescue and tower.
    b. Passive and active.
    c. Positioning and restraint.
    d. Environmental and structural.

31. (015) Why do workers suspended in a full body harness often lose consciousness after a fall?
    a. Dehydration.
    b. Head trauma from the fall.
    c. Neck whipping motion due to the fall.
    d. Restrictions in blood flow to extremities caused by the harness.

32. (015) Which hazard is *not* an example of an environmental climbing hazard?
    a. Corrosion.
    b. Moisture.
    c. Ice/snow.
    d. The sun.

33. (015) What does a knot in a lanyard do to its overall strength?
    a. Increases strength by 25 percent.
    b. Increases strength by 50 percent.
    c. Reduces strength by 50 percent.
    d. Has no effect.

34. (015) Carabiners used in climbing should be rated to handle how many pounds?
    a. 500.
    b. 1,000.
    c. 5,000.
    d. 10,000.

35. (016) Joint publications provide guidance for military services to use while preparing
    a. appropriate joint operations plans.
    b. doctrinal guidance for a host nation in time of war.
    c. United States military involvement in domestic emergencies.
    d. secretary of the Air Force guidance for Air Force forces in remote locations.

36. (016) What do allied communication publications do?
    a. Provide procedural guidance on Air Force policies.
    b. Standardize communication procedures for allied forces.
    c. Provide routing information for allied nations to route appointment letters.
    d. Establish a common directory of policies in English and French for allied and United States leadership.

37. (017) Who manages Air Force publications?
    a. Air Force Publications and Forms Management Office.
    b. Air Force Departmental Publishing Office.
    c. Air Force E-Publishing Website.
    d. Air Force Doctrine Department.

38. (017) What publications are usually written at a lower organizational level, such as the squadron and flight level?
    a. Operating instructions (OI).
    b. Air Force manuals (AFMAN).
    c. Air Force policy directives (AFPD).
    d. Air Force doctrine documents (AFDD).

39. (017) Where are Federal Aviation Administration (FAA) publications located?
    a. Standard Terminal Automation Replacement System (STARS) online.
    b. Aviation Data Exchange Portal (ADXP) online.
    c. Aeronautical Data Exchange (ADX) online.
    d. FAA Exchange (FAAX) online.

40. (018) What online system functions to acquire, improve, publish, catalog, manage, store, distribute and display official technical orders?
    a. Electronic technical operations (eTO).
    b. Technical order distribution office (TODO).
    c. Air Force Technical Ordering System (ATOS).
    d. Enhanced Technical Information Management System (ETIMS).

41. (018) Using the Joint Electronics Type Designation System, what does “GRR” represent?
    a. Ground Radar Receiver.
    b. Ground Radio Receiver.
    c. General Radar Receiver.
    d. General Radio Receiver.

42. (018) What technical order provides instructions on how to modify military systems or equipment?
    a. Work unit code (WUC) manuals.
    b. Time compliance technical order (TCTO).
    c. Standard installation practices technical order (SIPTO).
    d. Depot maintenance modification technical order (DMMTO).

43. (018) With a *minimum* of formal training time, what technical order serves as a manual of instruction in developing installation and maintenance proficiency?
    a. Operating instructions.
    b. Work unit code (WUC) manuals.
    c. Time compliance technical order (TCTO).
    d. Standard installation practices technical order (SIPTO).

44. (019) Who is responsible for the civilian accreditation of the many industry standards used to develop the cyberspace support equipment the Air Force operates and maintains?
    a. American National Standard Institute (ANSI).
    b. Telecommunications Industry Association (TIA).
    c. Electronic Industry Components Association (EICA).
    d. Acquisition Streamlining Standardization Information System (ASSIST).

45. (019) Why is military standardization beneficial to the Air Force?
    a. Ensures products meet certain requirements set forth by the United Nations.
    b. Ensures Air Force communication systems cannot be used by other countries.
    c. Ensures Air Force equipment has broad engineering and technical requirements.
    d. Achieves Department of Defense interoperability, commonality, reliability, and compatibility with logistics systems.

46. (019) What *describes* the essential technical requirements for purchased material that is military unique or substantially modified commercial items?
    a. Military detail (MIL-DTL).
    b. Military performance (MIL-PRF).
    c. Military specification (MIL-SPEC).
    d. Military workbook (MIL-WRKBK).

47. (020) What resource priority level (PL) is assigned to resources for which the loss, theft, destruction, misuse, or compromise would cause *significant* harm to the war-fighting capability of the United States?
    a. PL1.
    b. PL2.
    c. PL3.
    d. PL4.

48. (021) When an organization submits a security standard waiver request, what compensatory measures should be taken until fix actions occur?
    a. Extra security patrols, reduced work hours, or additional locks.
    b. Reduced work hours, extra security patrols, or new procedures.
    c. Reduced work hours, new procedures, barricades, or additional locks.
    d. Extra security patrols, new procedures, barricades, or additional locks.

49. (021) Which is *not* a type of facility secured area?
    a. Limited access.
    b. Controlled.
    c. Restricted.
    d. Critical.

**Please read the unit menu for unit 3 and continue ➔**

# Student Notes

# Unit 3. Computer and Network Fundamentals

**3–1. Basic Components ..... 3–1**
022. Computer components ..... 3–2
023. Input/output devices ..... 3–3
024. Peripheral and storage devices ..... 3–4
**3–2. Software ..... 3–7**
025. Operating systems ..... 3–7
026. Infectious and malicious software ..... 3–8
**3–3. Unix Operating System ..... 3–10**
027. Unix characteristics ..... 3–10
028. Using Unix ..... 3–13
**3–4. Communications and Network Protocols ..... 3–16**
029. International Organization for Standardization and the Open Systems Interconnection reference model ..... 3–16
030. Department of Defense standards ..... 3–17
031. Transport protocols ..... 3–18
032. Transmission Control Protocol/Internet Protocol ..... 3–20
033. Internet Protocol ports ..... 3–27
**3–5. Network Types ..... 3–29**
034. Network architecture ..... 3–29
035. Types of networks ..... 3–30
036. Network topologies ..... 3–31
**3–6. Network Devices ..... 3–37**
037. Modems ..... 3–37
038. Switches and bridges ..... 3–38
039. Routers, multiplexers, and converters ..... 3–39
040. Encryption devices ..... 3–41
041. Communication mediums ..... 3–42

IN THIS UNIT, computer and network fundamentals are discussed. This unit begins by covering computer components, moving to software and a few commonly used operating systems (OS), then wrapping up with the fundamentals of networking. Computers have proven their worth over the years and have automated many tasks. To improve efficiency, computers are networked together. Network devices assist in the transfer of data from one computer to the next. As more and more computer systems network together in the Global Information Grid, understanding how these systems work is vital in maintaining RAWS equipment.

## 3–1. Basic Components

Frequently, computer systems are under warranty or contract maintenance. However, you will be working with computers at some level in your daily tasks. As experts in this field, you need to be prepared and knowledgeable in all aspects of computer technology. This section describes the function and characteristics of computer hardware and peripheral devices.

Before a personal computer (PC) turns on, it is a mere collection of sheet metal, plastic, metallic tracings, and tiny flakes of silicon. When you push the ON switch, one burst of electricity starts a string of events that brings to life what otherwise would remain an oversized paperweight.

What makes a PC such a miraculous device is that each time you turn it on, it starts from a blank state to one capable of doing anything it is programmed to do.

## 022. Computer components

This lesson should be a review as you have most likely learned what a computer and its components do throughout your lifetime. The lesson lists some of the major components you will find in a normal computer: central processing unit (CPU), memory, motherboard, and power supply.

### Central processing unit

The computing part of the computer is the CPU. Also called the microprocessor, it consists of two main components: a control unit and the arithmetic logic unit. The CPU functions can be a single chip (microprocessor), on circuit board, or spread over several boards (mini and mainframe computers).

### Memory

Memory is volatile if the data contents are lost when removing power from a system; whereas, memory that retains data after removing power is non-volatile memory. Non-volatile memory devices have another characteristic associated with them; they can be erasable or non-erasable. Non-erasable memory means once programmed, it is unchangeable. A non-volatile reprogrammable device is an erasable device. System programs for computer start-up are stored in non-volatile memory and software programs use volatile memory while running for temporary storage of data.

For the CPU to function at its designed speed, there must be the ability to supply it with data and instructions as fast as it is ready for them. To accomplish this, memory devices must be able to supply data in periods measured in nanoseconds. The time it takes the CPU to obtain data from a memory device is “access time.”

#### *Random access memory*

In common usage, this type of memory is read-write memory. This type of memory can have data read from it, and written into each memory location. The term “random access” refers to the method of addressing memory. With random access, the CPU can address any memory location directly and read the data contained at that memory location.

Random access memory (RAM) chips are manufactured using large-scale integration and very large scale integration techniques. These chips contain tens of thousands of transistors in a single integrated circuit package. With recent advances in technology, RAM chips became more densely packed. This translates into more storage in a single chip with less cost. The use of these volatile RAM chips is to store data and running programs temporarily. RAM will retain its data as long as stable power is applied.

#### *Read-only memory*

The data stored in read-only memory (ROM) is always there, whether there is power or no power. You can remove ROM from the PC, stored it for an indefinite period, then replace it, and the data it contains will still be available. For this reason, it is non-volatile storage. A hard disk is also non-volatile, for the same reason, but regular RAM is not. It is more difficult to modify ROM as opposed to RAM, which provides a measure of security against accidental or malicious changes to its contents. Another characteristic of ROM, compared to RAM, is that it is much slower, typically having twice the access time of RAM. This is one reason why the code in the basic input/output system (BIOS) ROM is often shadowed into RAM to improve performance.

#### *Basic input/output system*

The BIOS controls how your PC works and saves data to non-volatile memory so that it is preserved even when the machine is off. A special type of memory used to store this information, called complementary metal oxide semiconductor memory, uses a very small battery to trickle a small charge to the BIOS ensuring that the data is preserved. These memories are very small, typically 64

bytes, and the batteries typically last for years. This so-called “non-volatile” memory is non-volatile RAM.

### *Cache*

Cache (pronounced “cash”) is a speed enhancement. It is a small amount of memory placed inside the CPU or between the CPU and the main memory. Its main purpose is to reduce CPU access time. In modern PCs, there are several layers of cache. Each layer is closer to the processor and faster than the layer below it.

In general, the following is how cache works. The processor requests a piece of information. The first place it looks is in the level 1 cache, since it is the fastest. If the information is there, the system uses it with no performance delay. If not, it is a miss then the processor searches the level 2 cache. If it finds it there (level 2 “hit”), it is able to carry on with relatively little delay. Otherwise, it must issue a request to read it from the system RAM. The system RAM may in turn either have the information available or have to get it from the still slower hard disk or compact disc—read only memory (CD-ROM). It is important to realize the difference in speed with some of these devices compared to the processor. Even the fastest hard disks have an access time measuring around 10 milliseconds. If it has to wait 10 milliseconds, a 200 MHz processor will waste 2 million clock cycles. CD-ROMs are generally at least 10 times slower than hard drives. This is why using caches to avoid accesses to these slow devices is so crucial.

### Motherboard

A motherboard is an architectural design that houses the CPU directly onto the system board. A motherboard will contain all the circuits necessary to process data and many times will contain associated video, memory and BIOS circuits.

### Power supply

A power supply is an electrical system that converts the wall outlet’s AC into DC to provide power to all internal circuitry in a computer. Linear and switching are the two basic power supplies, with switching being the most common on computers.

## 023. Input/output devices

This lesson will discuss various interfaces/ports used to connect hardware devices, both internally and externally. There are too many ways to connect to the main components to discuss all of them within this lesson objective. However, the more popular standards discussed within this lesson provide enough information to draw upon some relationships between interfaces, ports and devices. The term input/output (I/O) describes any program, operation or device communicating to and from a computer.

### Integrated Drive Electronics controller

Integrated Drive Electronics (IDE) and Advanced Technology Attachment (ATA) are the same thing—a disk-drive scheme designed to integrate the controller onto the drive itself, instead of relying on a stand-alone controller board. This approach reduces interface costs and makes drive firmware implementations easier. IDE proved to be a low-cost, easily configured system—so much so that it created a boom in the disk-drive industry. Although IDE and ATA are sometimes interchangeable, ATA is the formal standard that defines the drive and how it operates, but IDE is really the “trade name” that refers to the 40-pin interface and drive-controller architecture designed to implement the ATA standard.

### Advanced Technology Attachment Packet Interface

One of the major disadvantages of ATA is that it was designed for hard drives only. With the broad introduction of CD-ROM drives, designers needed a means of attaching CD-ROMs (and other devices, such as tape drives) to the existing ATA IDE interface, rather than using a stand-alone

controller card. The ATA Packet Interface (ATAPI) is a standard based on the ATA IDE interface designed to allow non-hard drive devices to plug into an ordinary ATA IDE port. Hard drives use ATA IDE support through BIOS, but ATAPI devices require a device driver to support them. Since ATA–1, a newer version of the ATA interface (ATA–2, 3, 4, 5, 6, 7 and Serial Advanced Technology Attachment [SATA]–8) support larger and faster drives. Each newer version is backward compatible with the previous versions. ATA–7 includes both parallel and serial ATA but SATA–8 is serial only.

### Serial Advanced Technology Attachment

SATA is an improvement of the parallel ATA physical storage interface. Serial ATA is a serial link using a single cable with a minimum of four wires that creates a point-to-point connection between devices. Transfer rates for serial ATA begin at 150 megabits per second (Mbps). One of the main design advantages of serial ATA is that the thinner serial cables maximize space and facilitate more airflow inside the computer's chassis. In contrast, IDE cables used in parallel ATA systems are bulkier than serial ATA cables and can only extend to 16 inches long, while serial ATA cables can extend up to 3 feet. Serial ATA supports all ATA and ATAPI devices.

### Peripheral Component Interconnect bus

Peripheral Component Interconnect (PCI) is a popular local I/O bus developed by Intel and introduced in 1993. Geared specifically to Pentium systems, the PCI bus moves from a slower parallel interface to a faster serial interface, by using full duplex lanes at a transfer rate that varies based on number of lanes used (i.e., x1, x4, x8, x16). The highest number of lanes is usually reserved for video cards (x16).

### Accelerated Graphics Port

Traffic on the PCI bus can be heavy on high-end PCs, with video, hard disk, and peripheral data all competing for the same I/O bandwidth. To combat the signal and data traffic saturation of the PCI bus, Intel developed the Accelerated Graphics Port (AGP) interface. They designed AGP to support the video subsystem in response to greater performance requirements for video. The AGP slot looks similar to a PCI slot, except that it offsets further from the back edge of the motherboard.

### Universal Serial Bus

Universal Serial Bus (USB) is an I/O bus that transfers data at up to 12 megabits per second (Mbps) for USB 1.1 and at 480 Mbps for USB 2.0. USB 3.0 is the newest version that adds the new transfer rate referred to as SuperSpeed USB that can transfer data up to 5 Gbps (billions of bits per second). Manufacturers are urged to distinguish USB 3.0 connectors from other versions by blue color coding receptacles and plugs. USB can handle up to 127 peripherals at once. This standard has plug and play capability allowing users the convenience of automatically configuring the computer to communicate with a newly attached device with little intervention. Additionally, USB allows users to add or remove devices such as a mouse, keyboard or printer with the computer powered on, otherwise known as "hot swapping" or "hot plugging."

### FireWire

Originally created by Apple and standardized in 1995 as the specification Institute of Electrical Electronics Engineers (IEEE) 1394 High Performance Serial Bus, FireWire is very similar to USB. FireWire is a method of transferring information between digital devices, especially audio and video equipment because of its guaranteed rate of data delivery. FireWire 400 (IEEE 1394a) supports a data transfer rate up to 400Mbps. FireWire 800 (IEEE 1394b) supports a data transfer rate up to 800 Mbps. Up to 63 devices can connect to a FireWire bus.

## 024. Peripheral and storage devices

A peripheral device is not a main component of a computer and can be either internal or external. Internal devices often use serial ATA to connect with the motherboard and communicate with the CPU processor. Some of the more common internal devices integrate into the motherboard freeing

interface slots for more devices and functionality. External devices may connect through a port connection on the computer case by USB, FireWire, and so forth.

### Hard disk

Hard disk drives are rigid platters storage devices that spin at a high rate of speed with a magnetic coating and a mechanism that can precisely position a magnetic read/write head over a particular track and sector on the disk surface. Because disk drives are subject to mechanical failure that may render stored data unreadable, it is essential to periodically backup critical information, or copy it onto other media. Hard drives interface with IDE or small computer system interface (SCSI) for internal drives, but there are many external drives today that can interface by USB or FireWire.

### Compact disc/digital versatile disc-read only memory drive

CD-ROM drives are necessary for most application programs installation or copying. Since both tasks are rare on a computer, speed has not been as big of an issue as in the past. A single CD-ROM can store up to 700 MB of data. CD-R is a write once, read many times, optical drive format that maintains a high level of compatibility with CD-ROMs. Compact disc-rewriteable (CD-RW) usually have the same disc capacity as CD-Rs, but with less compatibility with CD-ROM drives. As the name implies, CD-RWs are rewriteable to roughly 1,000 times.

Digital versatile disc-read only memory (DVD-ROM) drives operate much in the same way as CD-ROM drives. Single-sided single layer DVD-ROM discs can store up to 4.7 GB, more than six times the size of a regular CD-ROM. There are some special DVDs capable of storing more data such as: single-sided double-layer (up to 8.7 GB), double sided single-layer (9.4 GB) and double-sided double layer (17.08 GB). There are numerous recordable DVD formats. Some are similar to the CDs, but high-definition can yield up to 60 GB or Blu-ray discs can store as much as 50 GB using dual layers.

These drives also interface with IDE/SCSI for internal drives and there are some external drives that can interface via parallel, USB or FireWire.

### Graphics/video card

The video card performs the function of displaying the screen you see on the monitor. Inside the video card is a special kind of memory called video memory, where information is stored that represents what you see on the screen. If you look closely at the screen, you can see that it consists of many dots, or pixels. Each pixel’s color and brightness is stored in the video memory. When the computer wants to display something, it calculates how it needs to change the color and brightness of the different pixels, and changes the values in the video memory. The video card then presents the new pixels to you on the monitor. In modern computers, this calculating job occurs with the processor and the video card sharing the load. The video card is specialized to do graphics processing calculations. While the video card is processing graphics, the CPU is free to perform other tasks. Many of today’s motherboards contain video card circuitry.

### Monitors

Without a monitor, the computer would be useless. Monitors provide feedback to the user, and display all video content from a computer. They have come a long ways since the ages of the Cathode Ray Tube. Today’s monitors are capable of vividly producing a much wider array of colors than their tube predecessors produce. There are two types of monitors commonly in use today. The liquid crystal display (LCD) and the light-emitting diode (LED) monitor. Both types have subtle benefits and drawbacks, but offer outstanding video resolution. LED monitors have more improved sharpness and lower power consumption than LCD monitors, but are more costly.

### Image scanner

An image scanner, often referred to as just a scanner, is a device that optically scans images, printed text, or an object, and converts it to a digital image. Common examples found in offices are variations of the office desktop scanners also known as flatbed scanners. Hand-held scanners are devices that

use scanning wands held in the hand of the user. The user motions the wand across the scanning item or document.

### Keyboard

A keyboard's function is to input data to the computer. The keyboard is in a typewriter or calculator format using the QWERTY key setup. The keyboard is a series of single-pole single-throw switches mounted on a circuit board. Pressing a key closes the mechanical contacts. The switch closure uses American Standardized Code for Information Interchange (ASCII) or extended ASCII character encoding.

### Mouse

A mouse is an alternate means of cursor control. The mouse is a small box with two, three or more buttons on top and a ball poking out of the bottom. Moving the mouse on a table moves the cursor in the same direction on the screen. Optical mice use a transmitting LED and a sensor that detects movement by seeing the surface move under the mouse.

### Printer

Generally, a printer is a device that provides hard copies of text or graphics with whatever processing power is required. Most printers for home use connect to the computer through a parallel or USB cable. These low-volume printers frequently rely on the computer to process the graphics required to print fonts and illustrations. However, most high-volume printers can connect to a network directly and perform as a server to process print jobs. This frees the sending computer's processor to be available for other functions.

## Self-Test Questions

**After you complete these questions, you may check your answers at the end of the unit.**

### 022. Computer components

1. Also called the microprocessor, what computer component is considered the computing part of the computer?

2. What characteristic makes memory volatile?

3. How is BIOS memory preserved?

4. What is the main purpose of the cache?

### 023. Input/output devices

1. What is a major disadvantage for ATA?

2. What serial interface was created to increase throughput by utilizing full duplex lanes of communication?

3. Which interface allows users to add or remove external devices with the computer powered on, otherwise known as *hot swapping*?

### 024. Peripheral and storage devices

1. What periodic actions are suggested to prevent loss of data on a hard disk?

2. Name the peripheral device that processes graphics and displays them on the monitor.

## 3–2. Software

This section describes software characteristics and the functions of a few commonly used OSs. It also identifies the basic architecture of the OS and its relationship with application programs. Some examples of those OSs include Microsoft Windows, Unix, and Linux. Not only will this section cover the characteristics of these OSs, but it will also describe the relationship between the OS and application software.

Software is a generic term that refers to an OS, application, or utility programs that manage computer resources. Software generally divides into three categories: systems software, OSs software, and applications software. Applications software comprises of programs designed for an end user, such as word processors, database systems, and spreadsheet programs. Systems software includes compilers, loaders, linkers, and debugger programs used to write applications or operating system software. Unfortunately, software can be corrupted by infectious and malicious sources. This section will briefly explain facts relating to these vulnerabilities.

### 025. Operating systems

The OS defines your computing experience, and the software enables all the programs you use, allowing the computer to operate. The OS organizes and controls the hardware and software on your computer.

#### Operating systems overview

At the simplest level, an OS does two things:

1. It manages the hardware and software resources of the computer system. These resources include such things as the processor, memory, disk drives, sound card, and so forth.
2. It provides a stable, consistent way for applications to deal with the hardware without having to know all the details of the hardware.

The first task, managing the hardware and software resources, is very important, as various programs and input methods compete for the attention of the CPU and demand memory, storage and I/O bandwidth for their own purposes. In this capacity, the OS plays the role of the good parent, making sure that each application gets the necessary resources while playing nicely with all the other applications, as well as apportioning the limited capacity of the system to the greatest good of all the users and applications.

The second task, providing a consistent application interface, is especially important if there is to be more than one of a particular type of computer using the OS, or if the hardware making up the computer is ever open to change. A consistent application program interface allows a software developer to write an application on one computer and have a high level of confidence that it will run on another computer of the same type, even if the amount of memory or the quantity of storage is

different on the two machines. Even if a particular computer is unique, an OS can ensure that applications continue to run when hardware upgrades and updates occur.

### Types of operating systems

There are many different commercial OSs on the market today. The next few paragraphs describe Windows, Unix, and Linux. They are a few of the most popular OSs in use today.

#### *Microsoft Windows*

Microsoft Windows is a GUI based OS that was introduced in 1985 and has been released in many versions since. The primary design goal during the development of these OSs was to provide the user with a graphical rich environment user interface that is consistent, intuitive and user friendly.

There have been many versions of Windows since its inception back in 1985. The newest release of Windows is the Windows 10 line of client/desktop OS. Windows 10 expands on the framework of Windows 8 and Windows 7, and supersedes the line of Windows Vista. The different editions of Windows support various hardware platforms and are available in versions that support different processor platforms and embedded systems.

#### *Unix*

Unix is the first disk OS developed to operate on a wide range of computer systems.
It is possible to compile the code for just about any available platform. It is capable of running on mainframes, single user PCs, networked PCs or high-speed servers. Bell Labs developed the Unix OS in the early 1970s and licensed Unix inexpensively to anyone who wanted it. Universities and scholars adopted Unix and began to make modifications and additions to the system. As a result, different flavors of Unix have developed. Unix will be covered more in-depth later in this unit.

#### *Linux*

Linux is a freely distributable version of Unix, originally developed by Linus Torvalds, who began work on Linux in 1991 as a student at the University of Helsinki in Finland. Linus released the initial version of Linux free on the Internet, inadvertently spawning one of the largest software-development phenomena of all time. Today, Linux is authored and maintained by a group of several thousand (if not more) developers loosely collaborating across the Internet. Companies have sprung up to provide Linux support, to package it into easy-to-install distributions, and to sell workstations pre-installed with the Linux software. Ultimately, Linux is a complete Unix clone. Almost all major free software packages have been ported to Linux, and commercial software is becoming available. In fact, many developers start by writing applications for Linux, and port them to other Unix systems later.

## 026. Infectious and malicious software

Along with the free flow of information in the world today, there comes a potential threat that someone, somewhere wants to access that information or corrupt it. Threats may come from adversaries or random criminals looking to gain in some way from your data. Below are a few vulnerabilities from malicious software (malware) inherent to computers and network systems.

### Viruses

One of the most common computer security threats is software viruses. Software viruses are software programs that destroy data on computers that contract them. They also can spread from computer system to computer system. Damages from viruses can result in reformatting a hard disk; erasing programs and files; adding unrecognizable characters to files; or destroying disk directories and file allocation tables preventing the computer from using the tables or directories to locate files. Base communications squadron personnel should maintain antivirus remedies for the systems at your locations.

### Spyware

Another huge threat comes from spyware. Spyware is computer software designed to collect personal information about users without their informed consent. Personal information is secretly recorded with a variety of techniques, including: collecting cookies, logging keystrokes, recording Internet Web browsing history, and scanning documents on the computer's hard disk.

Spyware can be designed to retrieve passwords and financial details or to record Internet search history for targeted advertising. Spyware attempts to collect different types of information. Some variants attempt to track the websites a user visits and then sends this information to an advertising agency. More malicious spyware variants attempt to intercept passwords or credit card numbers as a user enters them into a web form or on-line applications.

The spread of spyware has led to the development of an entire anti-spyware industry. These products are designed to remove or disable existing spyware on the computers they are installed on and prevent its installation. To protect against viruses and spyware, use a good antivirus software product as well as these practical tips listed:

1. Take precautions when you share disks. Viruses can spread through infected disks; do not share disks unless it is necessary. Virus-check any disks before accessing files on the disk.
2. Do not share your software. Only use original software on your computer. Do not share software with anyone else or put copies of someone else's software on your machine.
3. Always back-up your files. If you are infected with a virus that wipes out your hard drive, you can still recover up to the last backup.
4. Schedule time to scan your system's hard drive. Scan removable media for viruses before each use. Hard drive media scans can be automated if antivirus software is configured properly.

### Malicious code

While malicious code is not considered software, it is important to be aware of the vulnerability to your system. Malicious code is the kind of harmful computer code or web script designed to create system vulnerabilities leading to back doors, security breaches, information and data theft, and other potential damages to files and computing systems. Not all anti-virus protection can treat certain infections caused by malicious code, which is different from malware. Malware specifically refers to malicious software, but malicious code includes website scripts that can exploit vulnerabilities in order to upload malware. Scripts, worms and viruses can harm your computer by finding entry points that lead to your data. Visiting infected websites or clicking on a bad e-mail link or attachment are major gateways for malicious code to sneak its way into your system.

## Self-Test Questions

**After you complete these questions, you may check your answers at the end of the unit.**

### 025. Operating systems

1. The OS organizes and controls what two things on a computer?

2. Name three commonly used OS used today.

### 026. Infectious and malicious software

1. List four damages that can result from viruses on a computer.

2. What type of malicious software is keystroke logging?

3. Name two ways malicious code can be introduced onto a computer.

## 3–3. Unix Operating System

Unix was touched on briefly earlier in the OSs section. This section will dig deeper into Unix, identifying characteristics and some basic commands for the system.

### 027. Unix characteristics

Unix is one of the most widely used OS in the world. It has gained success in personal use markets, such as desktop PCs (with Unix-based OSs like Linux and Mac OS X), and in smartphones with the Android OS. Used by individuals, companies, and organizations for a variety of applications, commercial Unix systems include: Oracle Solaris, International Business Machines (IBM), Advanced Interactive eXecutive (AIX), and Hewlett Packard Unix (HP-UX).

#### Components

All versions of the Unix OS have three major components: kernel, shell, and user programs (also called commands). The kernel and the shell combined do the same job as a Windows OS. Windows controls disk, file and memory management while facilitating a user interface one task at a time. However, Unix allows multiple tasks/processes to run simultaneously while the kernel keeps track of them all. In addition to that, Unix allows multiple users to run multiple processes at a time.

##### *Kernel*

The kernel is the software that interacts most closely with the hardware. Its primary functions are to control user processes (schedules) and manage system resources (allocating memory and disk storage). The kernel executes the shell, supervising the execution of the user programs (or commands), while controlling access to the filing system.

##### *Shell*

The program that you will interact with directly from your terminal or workstation is called the "shell." The shell is a command interpreter that recognizes and interprets commands that you enter. The shell, besides being an interpreter, is also used as a programming language. The shell provides a uniform and flexible means for directing and redirecting the standard input and output. Users can redirect the output from a command to the screen, to the printer, to disk, or to another command. This allows the user to have a single command to perform several distinct tasks. Unix normally has several different shells available.

Some of the common shells and their purposes are:

- Bourne shell—Standard all-purpose shell most commonly used.
- Korn shell—Same as the Bourne but with added options.
- C shell—A special shell for programmers who write C-language programs.
- Restricted shell—A shell that prevents its users from doing certain commands.

Note that you can run any shell simply by typing its name. For example, if you are running the csh (C shell) and want to switch to ksh (Korn shell), simply type ksh, and a ksh will start. All commands from that point on will be read and processed by the ksh. To switch to another just type its name and press enter.

### *Programs (commands)*

File manipulation commands include such operations as copying, removing, and listing files and directories. Remember, when dealing with any program or command that Unix is case sensitive so directories and files need to be entered just as they appear. Due to the enormous amount of commands for Unix, it is impossible to list them all here. Refer to applicable commercial manuals to find a listing for commands.

## File system

Before the advent of Unix, OSs stored information sequentially, (i.e., each file's relationship to other files was based on its physical location on the disk). In order to access a specific file, the OS searched through every file on the disk to find the requested file. The Unix OS was the first to develop a file structure using directories and path names (hierarchical) that allowed quicker search time and access of files. By providing the path to where a file was located, the OS avoided having to sequentially search through the entire system, instead it went directly to the location of the file (fig. 3–1).

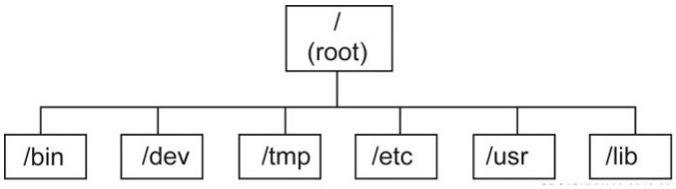


**Figure 3–1. Unix hierarchical file system structure.**

### *Partitions*

Partitions are physical areas of disk allocated with specific sizes to hold file systems, they enable a hard drive to be organized in a manner helpful to the user by making the drive seem like it is more than one entity. Partitions are established during system configuration (fig. 3–2).

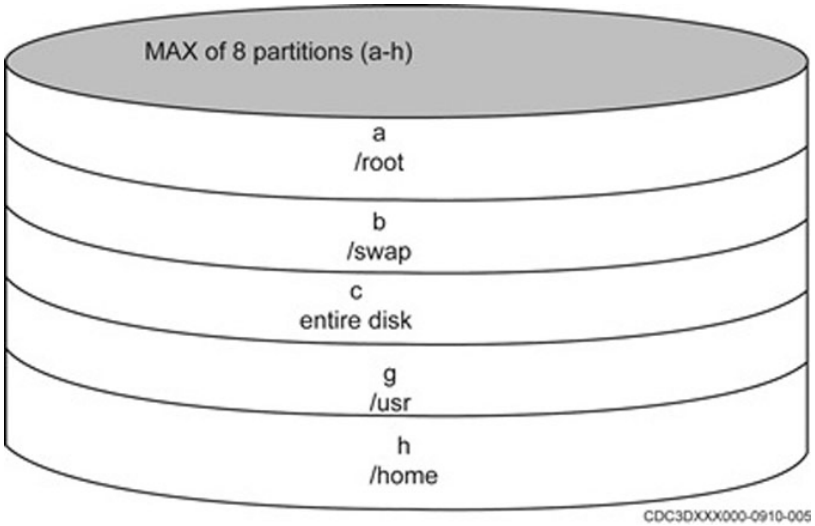


**Figure 3–2. Disk partitions.**

### *Files*

Files are the basic unit for storing and manipulating a collection of logically related information known as data. Files can be symbolic which means that people can recognize the data within the file (e.g., letters, numbers, special characters, etc.). Files can also contain executable programs written in machine language (i.e., binary digits [bit] of ones and zeros). User files are those created and accessed by users, while the OS creates and accesses system files. There is a distinct category of files within

the Unix environment referred to as “special” files. They are used to reference physical devices such as monitors, printers, and disk and tape drives.

### *Directories*

Unix provides a method for keeping track of files using a directory system. A directory is a collection of logically related files. The entire Unix file system structure can be compared to an office filing cabinet. Each drawer of the cabinet represents a directory. Each folder or document in each drawer represents a file. Directories, like files, are created and accessed by users, but there are some traditional directories provided in every Unix OS.

### *Traditional Unix directories*

The seven traditional directories provided with the Unix OS system are root, bin, dev, tmp, etc, usr, and lib as shown in figure 3–1. These directories contain the Unix OS software, and are maintained by system administrators.

1. **root—**The root directory is the master directory and highest-level directory of the Unix file system. All other files and directories are located within or under the root directory. In the previous example, the entire filing cabinet would be considered the root or master directory. The root directory is always identified by the slash symbol (/) and is in the “a” partition.
2. **bin—**The bin (binary) directory contains executable files for the most commonly used Unix commands.
3. **dev—**The dev (device) directory contains device drivers such as printers, disks, terminals, and modems.
4. **tmp—**The tmp (temporary) directory is used by the system for temporary storage files.
5. **etc—**The etc (et cetera) directory contains miscellaneous files primarily used for system administration tasks such as boot and shutdown.
6. **usr—**The usr (user) directory contains common files used by all users. Application programs are contained in usr.
7. **lib—**The (library) directory contains library files used for programming.

### *Sub-directories and parent directories*

A sub-directory is a directory within another directory. For example, the traditional Unix directories are all sub-directories of /root. In this example, /root is considered the parent directory, and all directories immediately below /root are known as children. A parent directory is identified by the “**..**” symbol.

### *Home directory*

The home directory is the directory, which is current when logging-on to the system. A user’s home directory is a sub-directory of the /usr directory. A system administrator’s home directory is /root and a common user might be in /usr/334trs.

### *Current working directory*

The current working directory is the directory presently being used. When a user first logs onto the system, the home directory becomes the current working directory. From here moving in and around the tree structure using pathnames accesses the file system hierarchy.

### *Shared folders*

Most Unix platforms use a simple user/group/other and a read/write/execute combination to set permissions for a specific file or folder. For example, you can set permissions on a file so that it is readable by everybody, but writable only by the user and group owner. There is also some specific

behavior in Unix; for example, users can only access the contents (or the list of files and folders) for folders that have Execute permissions.

### *Prompts*

The prompt is where you, as the user, will view your keystroke entries. On Sun Micro Systems machines, you will get a pound sign "#" at the multi-user level of the machine. If a hostname has been created then you will get the hostname followed by the "#" sign (i.e., Sun8#). On the Sun machines, the firmware prompt is ok (often called the O.K. prompt).

### *Pathnames*

Users move through the file system to access or create files and directories by using pathnames. There are three types of pathnames: absolute, relative, and simple.

#### *Absolute pathnames*

Absolute pathnames begin at the root directory and work down through the file system until reaching the desired directory or file. Each directory specified in the path is separated from other directories using the slash **(/)** symbol as the following illustrates: /earth/usa/kentucky/louisville

When Unix recognizes the slash as the first character in the pathname, it knows to start at the root directory and begin working its way down to the file "louisville."

#### *Relative pathnames*

Relative pathnames begin at the current working directory. If the current working directory in the previous example was /earth/usa, the relative pathname to access the file "louisville" would be: kentucky/louisville.

Each pathname Unix recognizes that does not start with the slash symbol is interpreted as relative to the current working directory. All sub-directories and their respective files of the current working directory can be accessed using relative pathnames.

#### *Simple pathnames*

A simple pathname is used to move to a directory one level below the current directory. For example, if the current directory is /earth/usa, to move to the "kentucky" directory the pathname would simply be "cd kentucky" using no slash symbol. To move one directory above the current working directory, the pathname (..) can be used signifying the parent directory.

## 028. Using Unix

In order to use Unix, you must use a command to direct you or to enter information. Unix makes little distinction between commands for system operation and maintenance, commands of general utility and more general-purpose applications such as text formatting and typesetting packages. As stated before, refer to applicable commercial manuals to find a listing for commands. Below are some descriptions of applications that these commands will operate and help you edit or navigate the Unix system.

### Vi editor

There are many ways to edit files in Unix and using the screen-oriented text vi editor is one of the best ways. This editor enables you to edit lines in context with other lines in the file. The vi is generally considered the standard in Unix editors because it is usually available on all types of Unix systems and implementations are very similar across the board. It requires very few resources and is user-friendly.

You can use the vi editor to edit an existing file or to create a new file from scratch. You can also use the editor to just read a text file. While working with the vi editor, you usually use two modes.

1. Command mode—This mode enables you to perform administrative tasks such as saving the files, executing the commands, moving the cursor, cutting (yanking) and pasting the lines or words, as well as finding and replacing. In this mode, whatever you type is interpreted as a command.
2. Insert mode—This mode enables you to insert text into the file. Everything that is typed in this mode is interpreted as input and placed in the file.

## Remote operation

When working in a distributed environment, you will need to communicate with remote machines or users. There are several Unix utilities that help users compute in a networked environment. Here we will discuss three utilities used in remote operations: ping, File Transfer Protocol (FTP) and telnet.

### *The ping utility*

The ping command sends an echo request to a host available on the network. Using this command, you can check if your remote host is responding well or not. The ping command is useful for the following reasons:

- Tracking and isolating hardware and software problems.
- Determining the status of the networking and various foreign hosts.
- Testing, measuring, and managing networks.

### *The File Transfer Protocol utility*

As stated in a previous section, FTP stands for File Transfer Protocol. This utility helps you unload and download your file from one computer to another computer. The FTP utility has its own set of Unix-like commands. These commands help you perform tasks such as connection and login to a remote host, directory navigation, listing directory contents, and transferring files.

### *The telnet utility*

There are times when it is required to connect to a remote Unix machine and work on that machine remotely. Telnet is a utility that allows a computer user at one site to make a connection, login and then conduct work on a computer at another site. Once you login using telnet, you can perform all the activities on your remotely connected machine.

## Unix system monitoring

A few ways to monitor the Unix system are outlined below with their respective commands:

- uptime—Finds out how long the systems has been up.
- who—Finds who is logged into the system.
- uname—Prints Unix system information.
- runlevel—Reports previous and current Unix OS run level.
- top—Displays tasks and system status in Unix.

## User administration

There are three types of accounts on a Unix system ranging from top (root account) down to the normal user account. These are described below.

### *Root accounts*

These are also called superusers and would have complete and unfettered control of the system. A superuser can run any commands without any restriction. This user should be assumed as a system administrator.

### *System accounts*

System accounts are those needed to operate system-specific components such as mail accounts and the “sshd” accounts. These accounts are usually needed for some specific function on your system, and any modifications to them could adversely affect the system.

### *User accounts*

User accounts provide interactive access to the system for users and groups of users. General users are typically assigned to these accounts and usually have limited access to critical system files and directories.

## Self-Test Questions

**After you complete these questions, you may check your answers at the end of the unit.**

### 027. Unix characteristics

1. What are the three major components of Unix?

2. Name two primary functions of the kernel.

3. Which major component of Unix is used as a programming language?

4. Match the definitions in Column B to the appropriate Unix directory term in Column A. Items in Column B will only be used once.

| *Column A* | *Column B* |
|---|---|
| ____ (1) etc | a. Contains library files used for programming. |
| ____ (2) bin | b. Contains executable files for the most commonly used Unix commands. |
| ____ (3) dev | c. Contains miscellaneous files primarily used for system administration tasks. |
| ____ (4) tmp | d. The master directory and highest-level directory of the Unix file system. |
| ____ (5) usr | e. Contains device drivers such as printers, disks, terminals, and modems. |
| ____ (6) lib | f. Contains common files used by all users. |
| ____ (7) root | g. Is used by the system for temporary storage files. |

### 028. Using Unix

1. Which program is generally considered the standard in Unix editors?

2. List three utilities used in remote Unix operations.

3. What type of user account gives complete control of a Unix system?

## 3–4. Communications and Network Protocols

Cyberspace technology is the fastest changing industry on the planet. New products are obsolete in a matter of months. Within the DOD, the acquisition and implementation process takes much longer than in the civilian world. Because of this, there must be an active effort to ensure that communications networks and systems are not only relatively current, but also follow protocols and standards to be able to interconnect, and communicate with pre-existing network infrastructure and systems. For this, the Air Force uses many civilian standards adopted into the DOD through MIL-STD and DOD protocol developed by organizations such as Defense Information Systems Agency (DISA). This section describes some of the protocols and standard systems in use as well as the Open Systems Interconnection reference model, and delves into the technical side by explaining Internet Protocol (IP) and porting.

### 029. International Organization for Standardization and the Open Systems Interconnection reference model

The International Organization for Standardization (ISO) is an independent, non-governmental membership organization headquartered in Geneva, Switzerland. It is the world's largest developer of international standards and is composed of representatives from 166 various countries that together develop standardized worldwide specifications for products, services, and systems. This helps ensure quality, safety and efficiency, and improves international trade and communications. The ISO publishes standards for nearly every type of industry including food, agriculture, healthcare, technology, energy management, and services to name a few, but the list goes on.

In the information technology (IT) world, ISO creates standards for manufacturing equipment, and the protocol in which much of the equipment operates under. Additionally, the ISO created a framework into which the major network hardware, software components, and protocols could be placed to give every item a common reference point. This framework, called the Open Systems Interconnect (OSI) seven-layer model, provides a means of relating the components and their functions to each other and a way of standardizing some of the components and protocols.

The OSI model provides a framework for engineers to follow to ensure software and network equipment will function together. Each layer of the model represents a particular aspect of network function.

The seven-layer OSI model has two larger layers or groups—the application (upper) layer and data transport (lower) layer.

- The application layer of the OSI model consists of the uppermost three layers: application, presentation, and session. The highest layer in this group, application, is closest to the end user. These layers deal with the user interface, formatting data, and access to applications.
- The data transport layer of the OSI model consists of the lowermost four layers: transport, network, data link, and physical. These layers define how data travels the physical media, through Internetwork devices, to the destination computer, and to the application on the destination machine. The physical layer and data link layer occur in hardware and software. The other lower layers generally occur only in software. The lowest layer, the physical layer, is closest to the physical network medium (the network cabling, for example), and is responsible for actually placing information on the medium. The table below shows the division between the application upper layer (in grey) and the lower data transport OSI layer.

| |
|---|
| **Application** |
| **Presentation** |

| |
|---|
| **Session** |
| **Transport** |
| **Network** |
| **Data Link** |
| **Physical** |

### Layer 1: Physical

The physical layer defines the electrical, mechanical, procedural and functional specifications for activating, maintaining and deactivating the physical link between communicating network systems.

### Layer 2: Data Link

Layer 2, the data link layer, defines the rules for gathering and completion; all the elements that make up a data frame and putting the whole thing together so that it can be passed to a physical-layer device and on to the network. Switches and bridges operate at the data link layer.

### Layer 3: Network

Layer 3, the network layer, is responsible for routing functions and logical addressing.

### Layer 4: Transport

The transport layer implements reliable Internetwork data transport services that are transparent to upper layers.

### Layer 5: Session

The session layer establishes, manages and terminates communication sessions.

### Layer 6: Presentation

The presentation layer provides a variety of coding and conversion functions applied to application layer data.

### Layer 7: Application

Layer 7, the application layer, represents the network-related program code and functions running on a computer system that either initiates or services the request.

### Use of the Open Systems Interconnect model

The OSI model is a theoretical representation of how networks function. Use of this model assumes that an event on one computer system creates data that sets off a chain of events. That data passes down through the layers on the sending machine and then leaves the system, travels across the network and up through the seven layers on the receiving machine, until the data arrives intact at the application layer and is processed by the receiving system.

## 030. Department of Defense standards

Defense Information Systems Agency (DISA) is a combat support agency of the DOD. The agency provides, operates and assures command, control, information-sharing capabilities and a globally accessible enterprise information infrastructure in direct support to joint war fighters, national leaders, and other mission and coalition partners across the full spectrum of military operations.

DISA has a very broad scope of responsibilities to the DOD. They oversee the usage and implementation of nearly every aspect of IT communications. Defense Information Systems Network

(DISN) services are major components of the Department of Defense information networks (DODIN) and building blocks for the C4I support to the nation's warfighters offered by DISA. This section details the services provided within the DISN. Each of these services operates on DISA approved protocol and MIL-STDs for the equipment and means of communication. Additionally, the services are sometimes required to meet tougher Air Force standards. Although this lesson does not detail the protocol each of these services provides, it is important to know that these systems go through extensive tests before fielding to meet DISA requirements.

### Defense Information Systems Network

DISN is a telecommunications network that provides the exchange of information in an interoperable and global space, divided by security demands, transmission requirements, and geographic needs of targeted end-user customers. The DISN offers a selection of integrated standards-based services to fulfill these connectivity needs. These services provide a framework of protocols used by the DOD to support diverse telecommunication requirements for its organizations.

### Standards

Standards, policies and procedures are required to ensure effective, secure, and efficient delivery of DOD IT communications. Within the AF, standards of many different types are used, including but not limited to: MIL-STD, DISA instructions, DISA circulars, and numerous commercial standards. It is very important to understand that DISA is the governing body for IT communications within the DOD and every level of IT communication from the DODIN to the warfighter falls under their scope of control.

## 031. Transport protocols

Transport protocols fall into two categories of classifications based on the way the data is transported: connection-oriented and connectionless-oriented communications. This section describes both methods.

### Connection-oriented communication

In connection-oriented systems, the connection established between the sender and recipient happens prior to transfer of any data. An example of a connection-oriented network is the telephone system. You place a call, a connection is established and then communication occurs. Connection-oriented networks first establish a connection with the recipient and then begin the data transfer. Connection-oriented protocols establish, maintain and break a connection with the receiving system.

#### *Transmission Control Protocol*

Transmission Control Protocol (TCP) is a connection-oriented transport layer protocol that provides reliable full-duplex data transmission. TCP is part of the TCP/IP protocol stack. In a connection-oriented environment, a connection establishes between both ends before transfer of information can begin. TCP is responsible for breaking messages into segments, reassembling them at the destination station, resending anything not received and reassembling the message from the segments. TCP supplies a virtual circuit between end-user applications.

The following protocols use TCP:

- HTTP (HyperText Transfer Protocol).
- SMTP (Simple Mail Transfer Protocol).
- DNS (Domain Name System).

TCP works by providing transport support from the source host to the destination host. It constitutes a logical connection between the endpoints of the network. Transport services segment and reassemble data sent by several upper-layer applications onto the same transport services. The transport layer data stream is a logical connection between the endpoints of a network. The transport layer defines end-to-end connectivity between host applications. The transport layer provides the following basic services:

- Segmenting upper-layer application data.
- Establishing end-to-end operations.
- Sending segments from one end host to another end host.
- Ensuring flow control by providing sliding windows.
- Ensuring reliability provide by sequence numbers and acknowledgements (ACK).

TCP is connection-oriented, so it requires connection establishment before data transfer begins. To do this, TCP uses a three-way handshake (an asynchronous connection mechanism), which is necessary because the mechanisms of a three-way handshake are not tied to a global clock. The handshake contains three steps:

1. The requestor sends a packet specifying the port number it plans to use and its initial sequence number (ISN) to the server.
2. The server acknowledges with its ISN, which consists of the requestor's ISN, plus 1.
3. The requestor acknowledges the ACK with the server's ISN, plus 1.

In the most basic form of reliable, connection-oriented data transfer, receipt of the data packets must occur in the same order of transmission. The following are mechanisms of TCP to ensure reliable delivery of data.

### *Stream data transfer*

The TCP transfers a continuous stream of bytes through the Internet. TCP does this by grouping bytes in TCP segments, and then delivered to IP for transmission to the destination. TCP decides how to segment the data, and it may forward the data at its own convenience. To ensure that all data sends, a push function delivers all remaining data in storage to the destination. A push also occurs at the close of the connection.

### *Reliability*

Reliable delivery guarantees that a stream of data sent from one machine is delivery through a data link to another machine without duplication or data loss. Positive ACK with retransmission is one technique that guarantees reliable delivery of data. Positive ACK requires a recipient to communicate with the source, sending back an ACK message when it receives data. The sender keeps a record of each data packet (TCP segment) that it sends and expects an ACK. The sender also starts a timer when it sends a segment, and it retransmits a segment if the timer expires before an ACK arrives.

### *Flow control and error detection/correction*

TCP uses flow control methods to prevent network congestion by ensuring that transmitting devices do not overwhelm receiving devices with data. There are three commonly used methods for handling network congestions. Buffering by network devices temporarily stores bursts of excess data in memory until the receiving machine uses it. Excess data bursts can exhaust memory, forcing the device to discard any additional datagrams that arrive. The receiving unit sends source-quench messages to sending units to prevent buffer overflow. The receiving device sends source-quench messages to request that the source reduce its current rate of data transmission. Lastly, windowing is another flow-control mechanism that requires the source device to receive an ACK from the destination after transmitting a certain amount of data.

To govern the flow of data between devices, the receiving TCP device reports a window to the sending TCP device. This window specifies the number of octets, starting with the acknowledgment number, that the receiving TCP device currently is capable of receiving. For example, with a window size of three, the source device can send three octets to the destination. It must then wait for an acknowledgment. If the destination receives the three octets, it sends an ACK to the source device, which now can transmit three more octets. If the destination does not receive the three octets because of overflowing buffers, for example, it does not send an ACK. Because the source does not receive an

ACK, it knows that the octets need retransmission and to lower the transmission rate. Error control determines whether transmitted data has become corrupt or otherwise damaged while traveling from the source to the destination.

### Connectionless-oriented communication

Connectionless-oriented protocols simply send out the data packets to the receiving system and do not require a receipt acknowledgment. User Datagram Protocol (UDP) is the format used as the connectionless transport protocol in the TCP/IP stack. UDP is a simple protocol that exchanges datagrams without acknowledgments or guaranteed delivery. UDP is best for sending small amounts of data for which guaranteed delivery is not required and minor packet loss is acceptable. Speed is the primary importance, as with Internet phone, real-time video conferencing, streaming audio and video, and online games. While UDP uses ports, they are different from TCP ports; therefore, they can use the same numbers without interference.

This simplicity is evident when comparing the UDP segment format with TCP. Error processing and retransmission requires handling by upper-layer protocols. For example, if a FTP download interruption occurs for some reason, the human operator can just retry until it successfully delivers. The following list defines the fields in the UDP segment:

- Source Port—number of the calling port.
- Destination port—number of the receiving port.
- Length—number of bytes, including header and data.
- Checksum—calculated checksum of the header and data fields.
- Data—upper-layer protocol data.

The UDP does not use windowing or ACK. Therefore, application layer protocols provide reliability. UDP is for applications that do not need to put sequences of segments together. The following Protocols use UDP:

- Trivial File Transfer Protocol (TFTP).
- Simple Network Management Protocol (SNMP).
- Dynamic Host Configuration Protocol (DHCP).
- Domain Name System (DNS).

## 032. Transmission Control Protocol/Internet Protocol

The TCP/IP is the basic communication language or protocol of the Internet. The TCP/IP is a suite of specialized protocols—including TCP, IP, UDP, ARP and many others. TCP/IP’s roots lie with the US DOD, which developed TCP/IP for its Advanced Research Projects Agency Network (ARPANET), the precursor to today’s Internet in the late 1960s. The TCP/IP is a de facto standard on the Internet and has become the protocol of choice on local area networks (LAN) and wide area networks (WAN).

TCP/IP would not have become so popular if it were not routable. Protocols that can span more than one LAN (or LAN segment) are routable, because they carry network layer addressing information used by a router. Not all protocols are routable; however, the TCP/IP suite offers a number of features and benefits, which offer interoperability, flexibility, and multivendor support. TCP/IP has become the standard protocol suite because of its capability to connect LANs, WANs and the Internet. TCP/IP is the most universally available protocol today.

The multiple protocols within the TCP/IP suite provide for a variety of implementations or flexibility. The choice between TCP, a connection-oriented method of communication that is reliable but slow, and UDP, a fast and efficient yet not as reliable method, is important when determining how a packet travels the network.

Another big benefit of the TCP/IP suite is the fact that almost all network software vendors support its use. Apple, Digital Equipment Corporation, IBM, Novell, Microsoft, and Sun are just a few of the many companies that support the suite. The easiest way to break down the many protocols of the TCP/IP suite is according to where they operate within the OSI model. Each protocol in this stack operates at one of four layers: the data link layer, the network layer (also known as the Internet layer in the TCP/IP model), the transport layer or the application layer.

## Network layer protocols

In the TCP/IP protocol suite, the network layer is known as the Internet layer. The Internet layer is responsible for the logical addressing of devices on the network, as well as routing data between a source and destination.

### *Transmission Control Protocol*

As described earlier, TCP provides reliable data delivery services. TCP is a Connection-Oriented Protocol, which means that a connection requires establishment between communicating nodes before this Protocol will transmit data. TCP further ensures reliable data delivery through sequencing and check sums. Without such measures, data would transmit indiscriminately without checking whether the destination node was offline, or whether the data became corrupt during transmission. Finally, TCP provides flow control to make sure that a node is not flooded with data.

### *Internet Protocol*

IP provides information about how and where to deliver data including the data's source and destination addresses. IP is the protocol that enables TCP/IP to Internetwork, which means to pass through more than one LAN segment and more than one type of network through a router.

The network layer of the OSI model occurs when data forms into packets. In the context of TCP/IP, a packet, also known as an IP datagram, acts as an envelope for data and contains information necessary for routers to transfer data between different LAN segments. IP is an unreliable, connectionless protocol, which means that it does not guarantee delivery of data. However, higher-level protocols of the TCP/IP suite use IP to make sure data packets are delivered to the right addresses. Note that the IP datagram does contain one reliability component, the header checksum, which verifies only the integrity of the routing information in the IP header. If the checksum accompanying the message does not have the proper value upon receipt of the packet, the packet is presumed to be corrupt, discards, and at that point, the packet resends.

## Internet Protocol Version 4

The Internet Protocol Version 4 (IPv4) addressing method is used throughout the entire Internet community. Its popularity is due to the wide acceptance and use of TCP/IP suite. This addressing occurs at layer 3 of the OSI model. An IP address identifies both the individual node and the network to which the node attaches.

IPv4 addresses are represented as four sets of 8 binary bits, four Octets or Bytes, for a total of 32 bits. The IP address is represented by a decimal conversion of each byte separated by a period (.).

Each IP address has specific components and follows the same format. Each TCP/IP network has a 32-bit logical address assigned that divides into two main parts: the network number and the host number.

### *Network number*

The network number identifies a specific network and requires assignment by Internet Assigned Numbers Authority (IANA) if the network is to be part of the Internet. Network numbers are obtainable from authorized representatives of IANA, Internet or online service providers, which have obtained blocks of numbers from one of the authorized representatives of IANA.

### *Host number*

The host number identifies a specific host (or any node) on a network and assigned by the local network administrator.

### *Dotted decimal notation*

Dotted decimal notation (DDN) is a representation of a binary IP address in a more user-friendly manner. The notation uses the combination value of each bit that is turned on (represented by a 1), in each byte or octet and adds them together. This occurs for each octet individually; octet values never add together.

The 32-bit binary address of 1101 0001 0001 1111 0100 1011 0010 0011 is represented as 209.31.75.35. This format, known as DDN representation is easier to write and to remember than binary representation. The minimum value for any given octet is zero (represented by 0000 0000) and the maximum value for any given octet is 255 (represented by 1111 1111). The table below displays binary and DDN of an IP address.

| Type | First Octet | Second Octet | Third Octet | Fourth Octet |
|---|---|---|---|---|
| Binary | 1101 0001 | 0001 1111 | 0100 1011 | 0010 0011 |
| Decimal | 209 | 31 | 75 | 35 |
| DDN | 209.31.75.35 | | | |

### *Five classes*

There are five classes of IP addresses: Class A through E. Class D and E are reserved for broadcast and experimental networks. IANA manages the network allocations for classes A through C. IANA generally allocates super-blocks to Regional Internet Registries, who in turn allocate smaller blocks to Internet service providers and enterprises.

By looking at the *first* octet of an IP address in either its decimal or its binary form, you can easily identify the “class” of the address. In the decimal version, the number of the first octet tells you immediately which class the address is. In the binary version, the first bit or bits in the first octet—the high-order bits—tells you the address class.

#### *Class A address*

Class A addresses used for large networks. The first bit (**0**) identifies the address class and, together with the next seven bits, identifies the network number. The last 24 bits identify the node number. There are 126 class A networks (addresses 1–126), with 16,777,214 hosts on each network.

#### *Class B address*

Class B used for intermediate sized networks. The first two bits (**10**) identify the address class and together with the next fourteen bits, identify the network number. The last sixteen bits identify the node number. There are about 16,384 class B networks (addresses 128–191), with 65,534 hosts on each network.

#### *Class C address*

Class C addresses used for networks with about 250 nodes. The first three bits (**110**) identify the address class and, together with the next twenty-one bits, identify the network number. The last eight bits identify the node number. There are about 2,097,152 class C networks (addresses 192–223), with 254 hosts on each network.

#### *Class D address*

Class D addresses reserved for multicast addressing. The first four bits (**1110**) identify the address class and, together with the rest of the address, identify the network number.

### *Class E address*

Class E addresses reserved for research and development. The first four bits (**1111**) identify the address class and, together with the rest of the address, identify the network number.

The first few bits in the string of binary digits that comprise the address identify the class of an IP address. For the course, only classes A, B and C will be discussed. Each class uses a different quantity of octets to identify the network portion of the address, as shown in the table below.

| 32-Bit Binary Address Composition | | | |
|---|---|---|---|
| Class A | Network | Node | |
| | 1 octet | 3 octets | |
| Class B | Network | Node | |
| | 2 octets | 2 octets | |
| Class C | Network | Node | |
| | 3 octets | 1 octet | |

The table below shows the five network classes and the corresponding decimal values of the address of an IP's' *first* octet.

| IP Address Class Breakdown | |
|---|---|
| **Address Class** | **First Octet** |
| * | 0 |
| Class A | 1 – 126 |
| * | 127 |
| Class B | 128 – 191 |
| Class C | 192 – 223 |
| Class D | 224 – 239 |
| Class E | 240 – 254 |
| * | 255 |
| *Commonly, the octets 0, 127, and 255 are not included as part of the class structure as they are reserved for special use. | |

## Reserved Internet Protocol Addresses

In addition to the addresses assigned for use by each node in the network, there are some addresses serving special purposes, denoting networks or sets of computer nodes. Hosts never receive these addresses. The table below displays a few basic reserved IP addresses used in IPv4.

| Network field | Host field | Type of Address | Purpose | Example |
|---|---|---|---|---|
| All 0s | All 0s | This computer | Used during bootstrap | 0. 0. 0. 0 |
| 127 | Any | loop back | Testing | 127. 0. 0. 1 |
| 255 | 255 | Limited broadcast | Broadcast on local network | 255.255.255.255 |
| Network address | All 0s | Network | Identifies network | 203. 82.104. 0 |
| Network address | All 1s | Directed broadcast | Broadcast on a specified network | 207. 55.157.255 |

### *Internet Protocol Version 4 subnet masking*

Subnet masking is a mechanism that allows a network device to divide an IP address into a network and host number. When a network device wants to send an IP packet, it must make a decision. If the destination IP address is on its own network, the IP packet simply transmits onto the same network. If the destination IP address belongs on a different Network, the IP packet routes to another network. The subnet mask allows the network device to make this decision.

In a subnet mask, bits represented by ones identify the network address and bits represented by zeroes identify host addresses. There are two methods of subnet masking: classful and classless. An example of a classful subnet mask is 255.255.0.0 and a classless would be 255.252.0.0.

### *Classful subnet masking*

Classful subnet masking uses the default mask to separate the network number, given by IANA, from the host number. The table below displays the default mask of classes A, B, C, and D. Classful subnet masks must have all ones (1) or all zeroes (0) in each octet.

| **Default Mask** | |
|---|---|
| ***Class A*** | 255.0.0.0 *or* 11111111.00000000.00000000.00000000 |
| ***Class B*** | 255.255.0.0 *or* 11111111.11111111.00000000.00000000 |
| ***Class C*** | 255.255.255.0 *or* 11111111.11111111.11111111.00000000 |
| ***Class D*** | 255.255.255.255 *or* 11111111.11111111.11111111.11111111 |
| Example | |
| ***157.28.13.114*** | The 157 signifies an address of Class B thus indicating a class full boundary of 2 octets (16 bits) for network address. |
| ***Converting to binary*** | 10011101 00011100 00001101 01110010 |
| ***Partitions*** | Network= 10011101 00011100<br>Host= 00001101 01110010 |
| ***Subnet mask*** | 255.255.0.0 |
| ***Network identity (ID)*** | 157.28.0.0 |
| ***Host ID*** | 0.0.13.114 |

### *Classless subnet masking*

If a further subdividing of the network is necessary beyond the class-full boundary, then the system borrows bits from the host or node field to create a subnet field. This means that the octets beyond the class boundary can become values to mask out the subnet field. Classless subnet masking, also known as Classless Inter-Domain Routing (CIDR, pronounced *cider*), offers more flexibility over the class-full address ranges of A-D. CIDR uses variable length subnet. The table below displays classless subnet values.

| **Classless subnet** | |
|---|---|
| ***Subnet masks*** | 11111111 = 255; 11111110 = 254; 11111100 = 252; 11111000 = 248; 11110000 = 240; 11100000 = 224; 11000000 = 192; 10000000 = 128 |
| Example | |
| ***Address*** | 172.16.32.4 |
| ***Subnet mask*** | 255.255.255.252 |
| ***CIDR notation*** | 172.16.32.14/30 (30 bits are used for the subnet mask)<br>The 172 signifies an address of Class B thus indicating a class full boundary of 2 octets (16 bits) for network address. The mask identifies how many bits to use for the subnet. |
| ***Address conversion*** | 10101100 00010000 00100000 00001110 |
| ***Mask conversion*** | 11111111 11111111 11111111 11111100 |
| ***Partitions*** | Network= 10101100 00010000 |

| Classless subnet | |
|---|---|
| | Subnet= 00100000 000011<br>Host= 10 |
| ***Network ID*** | 172.16.0.0 |
| ***Subnet ID*** | 0.0.32.12 |
| ***Host ID*** | 0.0.0.2 |

As you can see, an IP address consists of a network number ID and a host number ID. A third field, subnet number ID, expresses to system administrators that “sub” networks are in use. Subnets ease administration; improve network performance, and security. Because of the subnet mask, the network device still only sees a network number and host number. Keep in mind the network concept that there is a network and host number, as the next lesson discusses IP version 6.

## Internet Protocol Version 6

Internet Protocol Version 6 (IPv6) or Internet Protocol Next Generation (IPng) is the successor to IPv4. IPng took the next step from IPv4 by creating addresses that are 16 octets long, four times as large as IPv4 addresses (128 bits vs. 32 bits). With this extremely large addresses space, IPng can support up to 3.4 x $10^{38}$ addresses (340,282,366,920,938,463,463,374,607,431,768,211,456), approximately 6.7 x $10^{20}$ (6.7 billion billion) addresses per square centimeter of the Earth’s land mass.

Unlike IPv4, IPv6 is expressed in 16-byte fields and is considerably more user friendly. Instead of using DDN, IPng uses a colon hexadecimal format. Essentially, hex numbers are base 16. Decimal is base 10, counting from 0 to 9, as done in decimal, and then adding a column to make 10. Counting in hex goes from 0 to F before adding a column. The characters A through F represent the decimal values of 10 through 15. The table below shows corresponding decimal, hexadecimal and binary values.

| Decimal | Hexadecimal | Binary |
|---|---|---|
| 1 | 1 | 0001 |
| 2 | 2 | 0010 |
| 3 | 3 | 0011 |
| 4 | 4 | 0100 |
| 5 | 5 | 0101 |
| 6 | 6 | 0110 |
| 7 | 7 | 0111 |
| 8 | 8 | 1000 |
| 9 | 9 | 1001 |
| 10 | A | 1010 |
| 11 | B | 1011 |
| 12 | C | 1100 |
| 13 | D | 1101 |
| 14 | E | 1110 |
| 15 | F | 1111 |

### *Colon hexadecimal format*

The colon hexadecimal format is a comparison between the following two address formats:

- IPv4: 192.168.123.100
- IPv6: FEDC:BA98:7654:3210:FEDC:BA98:7654:3210

If the above IPv6 address was converted into decimal, it might look like the following: 65244:47768:30292:12816:65244:30292:12816.

### *Compressing*

In the IPv6 format, there are two ways to shorten the expression of its addresses: leading zero compression and zero compression.

1. Leading Zero Compression drops leading zeroes in an address, in any field, as long as there is at least one number left:
   - Original IPv6 format—1234:1234:0000:0000:1234:0000:0000:1234.
   - Using leading zero compression—1234:1234:0:0:1234:0:0:1234.
2. Zero compression allows suppression of consecutive fields of zeroes. This method is allowed once per address:
   - Before suppression—1080:0:0:0:8:0:0:417A.
   - After suppression—1080::8:0:0:417A (48-bits suppressed) or 1080:0:0:0:8::417A (32-bits suppressed).
   - Suppression not allowed—1080::8::417A.

In the last example above, this expression of suppressing zeroes is un-allowed because it is impossible to determine the number of suppressed bits.

### *Address range*

The text representation of IPv6 address prefixes is similar to the way IPv4 addresses prefixes are in CIDR notation. An IPv6 address prefix utilizes the following notification for representation: ipv6-address/prefix-length. The following is an example of IPv6 address range:

- FEDC:BA98:7654:3200::/56—The number 56 signifies that from the leftmost part of the address and counting to the right 56 places belongs to the prefix.
- FEDC:BA98:7654:3200::—This address is the start of the address range for host numbers using the prefix given above.
- FEDC:BA98:7654:32FF:FFFF:FFFF:FFFF:FFFF is the end of the address range for host numbers.

### *Assignment*

IPv6 provides more efficient and useful addressing. In IPv4, CIDR allowed to “borrow” bits from the host portion of the address in order to create a greater number of networks, with fewer hosts per network. In most cases, the IPv6 host address portion is a fixed 64-bit field and will never have bits borrowed from it to be able to create more networks. IPv6 addresses are 128-bit identifiers for interfaces and sets of interfaces. IPv6 covers three main types of addresses: unicast, multicast, and anycast should remain one word anycast.

1. Unicast addresses identify a single interface. A packet sent to a unicast address delivers to the interface identified by that address.
2. Multicast addresses (FF00::/8) identify a group of interfaces belonging to different nodes. Multicast packets send to all interfaces identified by that address.
3. Anycast addresses also identify a set of interfaces, but the packets deliver to and are accepted by the closest interface.

IPv6 does not use a broadcast address. The multicast address in IPng has taken over the function of the broadcast address from IPv4.

### *Transition mechanisms*

IPv6 is underway, but transitioning fully from IPv4 will take a long time and perhaps indefinitely. There may be IPv6 network infrastructures out there that do not need IPv4 interoperability, if so the following mechanisms are unnecessary. However, in an environment where IPv4 and IPv6 resources need to interoperate, the following mechanisms are the initial core set of transitions:

- Dual IP layer (also known as Dual Stack): A technique for providing complete support for both Internet Protocols: IPv4 and IPv6 (in hosts and routers).
- Configured tunneling of IPv6 over IPv4: Point-to-point tunnels made by encapsulating IPv6 packets within IPv4 headers to carry them over IPv4 routing infrastructures.
- IPv4-compatible IPv6 addresses: An IPv6 address format that employs embedded IPv4 addresses.
- Automatic tunneling of IPv6 over IPv4: A mechanism for using IPv4-compatible addresses to automatically tunnel IPv6 packets over IPv4 networks.

The dual-stack Protocol implementation in an OS is a fundamental IPv4-to-IPv6 transition technology. Dual-stack Protocol implements IPv4 and IPv6 Protocol stacks either independently or in a hybrid form. The hybrid form is common in modern OS supporting IPv6.

Modern hybrid dual-stack implementations of IPv4 and IPv6 allow today's programmers to write networking code that works transparently on IPv4 or IPv6 networks. The software may use hybrid sockets designed to accept both IPv4 and IPv6 packets. When used in IPv4 communications, hybrid stacks use an IPv6 application-programming interface and represent IPv4 addresses in a special address format using the IPv4-mapped IPv6 address.

## 033. Internet Protocol ports

A TCP/IP client computer initiates contact with a server computer and uses specific values, called port numbers, to request a particular service. Network servers listen to ports that correspond to services they offer. A web browser, for example, contacts a server at the destination port number 80; the Web server listens to port 80 so it knows that the client wants to access a Web page.

By using port numbers, servers are capable of providing multiple services. For example, one server handles internal Web pages for mission essential communication. It also acts as a file server and print server. Finally, it handles Web traffic such as Internet searches and video streaming. Clients through different port numbers request each of these services.

As discussed earlier, every popular, or well-known, TCP/IP application has clearly defined port numbers. A port number is a 16-bit value between 0 and 65535. Port numbers from 0 to 1023 are called well-known port numbers and are reserved for specific TCP/IP applications. As a rule, no TCP/IP services can use port 0; it is reserved.

### Destination and source port numbers

A client uses a destination port to request a service. The server in turn uses the port number applied by the client. The Web client, in essence, says, "Hey server. I am requesting service on port 80. Please send service response to my port 50012." In this example, port 50012 is the source port number. Port numbers that devices allocate dynamically for a source port number are ephemeral ports.

### Registered and dynamic port numbers

Registered ports fall between the ranges of 1024 to 49151. Less-common TCP/IP applications may register their ports with IANA. Unlike well-known ports, anyone can use these port numbers for

servers or for ephemeral numbers on clients. Most OS steer away from using these port numbers for ephemeral ports, instead they use dynamic/private port numbers. Below is the full list of ports:

- 0–1023 are well-known ports.
- 1024–49151 are registered ports.
- 49152–65535 are dynamic or private ports.

## Self-Test Questions

**After you complete these questions, you may check your answers at the end of the unit.**

### 029. International Organization for Standardization and the Open Systems Interconnection reference model

1. What is the world's largest developer of international standards that develops standardized worldwide specifications for products, services and systems?

2. What is the framework that identifies major network hardware, software components and Protocol placement in order to give every item a common reference point?

3. What are the two larger layers or groups that make up the OSI model?

### 030. Department of Defense standards

1. What network provides a framework of protocols used by the DOD to support diverse telecommunication requirements for its organizations?

2. Who is the governing body for IT communications within the DOD?

### 031. Transport protocols

1. In connection-oriented communications, when can the sender and recipient transfer data?

2. What are the three things that must take place during a TCP "handshake"?

3. In TCP, what is used to prevent network congestion by ensuring that transmitting devices do not overwhelm receiving devices with data?

4. What important element is not required in connectionless-oriented communications?

### 032. Transmission Control Protocol/Internet Protocol

1. In the TCP/IP protocol suite, the network or “Internet” layer is responsible for what?

2. What protocol enables TCP/IP to Internetwork?

3. How are IPv4 addresses represented?

4. What information can you gather by looking at the first octet of an IP address?

5. In an IPv4 subnet mask, what do the “1” and “0” bits represent?

6. How much larger are IPv6 addresses than IPv4 addresses?

7. What are the three main types of IPv6 addresses?

### 033. Internet Protocol ports

1. What are ephemeral ports?

2. Name the three-port number ranges, and list the types of ports that are associated with each range.

## 3–5. Network Types

This section covers the types of networks used within the Air Force and DOD, and describes the network topology of how the networking equipment interconnects.

### 034. Network architecture

Network architecture is the design of a communications network. It is a framework for the specification of a network’s physical components and their functional organization and configuration, its operational principles and procedures, as well as data formats used in its operation. In telecommunication, the specification of a Network Architecture may also include a detailed description of products and services delivered by a communications network, as well as detailed rate and billing structures under which services are compensated. Network Architecture is predominantly expressed by the use of the IP suite versus a specific model for interconnection network or nodes in a

network, or the usage of specific types of hardware links. The following paragraphs describe the principle components that make up a network and the theory of how each works.

### Internet

What is the Internet? The standard answer to this question has been, "*The Internet is a network of networks.*" The Internet is a series of private computer networks connected to each other often referred to as the World Wide Web or public Internet. Each individual private network is composed of a series of connected computers within an organization. Each organization takes responsibility for only the computers in its area of influence.

### Intranet

Intranets use the same software (i.e., Web browsers) and the same Protocols as the public Internet, but Intranets exist as a portion of a company's private network. Intranets are comprised of one or more inter-connected LANs within the company. Nevertheless, unlike the Internet, the content is restricted to authorized company users only. Essentially, an Intranet is a private Internet.

### Extranet

Extranets are Intranets that share a portion of their content with customers, suppliers, or other businesses, but not with the public. As with Intranets, they use the same Web browsers and other software to enable access to their content.

## 035. Types of networks

The basic need to connect computers together fostered the birth of the network. Advanced Research Projects Agency (ARPA) began networking research by providing grants to computer science departments at many universities and a few private corporations during the early 1970s. The research led to the network creation among universities, corporations and DOD conducting the research. The network, under ARPA was later termed ARPANET. ARPANET was controlled by the DOD and managed by the Defense Advanced Research Projects Agency.

During the 1990s, the National Science Foundation decided that there was a need for a faster means of transmitting information because ARPANET was unable to keep up with the increase of network traffic. They wanted to replace the ARPANET with a faster network able to handle larger traffic loads. Eventually through time, this was accomplished and many different types of networks were needed for varying demands. The following are the most prevalent network types in use today.

### Local area network

A LAN is a group of computers and associated devices that share a common communications line and typically share the resources of a single processor or server within a small geographic area (for example, within an office building). Usually the server has applications and data storage shared by multiple computer users. A LAN may serve as few as two or three users or as many as thousands of users.

### Metropolitan area network

A metropolitan area network (MAN) is a network that interconnects users with computer resources in a geographic area or region larger than that covered by even a large LAN but smaller than the area covered by a WAN. The term applies to the interconnection of networks in a city into a single larger network. MANs also indicate the interconnection of several LANs (also known as a campus network) by bridging them with backbone lines.

### Wide area network

A WAN is a network that links LANs and MANs by using long-distance communication links leased or purchased from a telecommunications company. Long-distance communication links can be described as telephone lines, microwave or satellite communications. A WAN connects networks that

are typically separated by geographical distances. These distances are between two cities within a state, between two states, across a country, or around the world.

### Wireless local area networks

Like Ethernet, wireless local area network (WLAN) technology is a frame-based form with header and trailer. Primary addressing still occurs through media access control (MAC) destination and source addresses. Instead of sending these frames over physically installed media (wire, fiber); the information is radiated through the air.

## 036. Network topologies

A network's topology consists of the physical and logical arrangement of its stations in relation to one another. For LAN, the term "stations" is used rather than the more traditional "nodes." A node in a traditional data communications network sits at the intersection of two or more transmission paths and switches traffic among those paths. On most LANs, a station attaches to a single transmission link at one point and transmitting signals along the single path to other similar stations. There is a variety of topologies available to LANs. Within this topic, topologies will be described as well as the relationship between them physically and logically.

### Network topology fundamentals

Network topology commonly describes the properties of various types of networks. Topology is the branch of mathematics that examines the characteristics of geometric shapes. Networks have shapes, and the shape a network takes affects the way it functions.

When referring to a network's topology, it may be referred to by either its physical or its logical topology. When used alone, the word "topology" often refers to a network's physical topology. A physical topology is a "map," or description, of the layout of the network media that interconnects the devices on a network. The physical topologies implemented today include the bus, ring, star, and a hybrid of several topologies combined into one network. A logical topology defines the way in which devices communicate and transmit data throughout the network. This may be in the form of a bus or ring. The following rule of thumb distinguishes physical from logical topology:

- If you can see it and touch it, it is physical.
- If you cannot see it or touch it, it is logical.

You soon discover that similar-looking networks can have quite different logical topologies. A network's topology affects its capabilities. The choice of one topology over another will have an impact on the:

- type of equipment the network needs.
- capabilities of the equipment.
- growth of the network.
- way the network is managed.

Developing a sense of how to use the different topologies is a key to understanding the capabilities of the different types of networks. Computers have to connect to each other before they can share resources or perform other communication tasks. However, it is not as simple as just plugging a computer into a cable connecting other computers. Different types of cable—combined with different network cards, network OSs, and other components—require different types of arrangements. To work well, a network topology takes planning. For example, a particular topology can determine not only the type of cable used but also how the cabling runs through floors, ceilings and walls. Topology can also determine how computers communicate on the network. Different topologies require different communication methods, and these methods have a great influence on the network.

## Physical topology

The type of physical topology you choose for your network will affect how devices on your network communicate. All networks stem from three basic topologies—bus, star, and ring.

A bus topology consists of devices connected to a common, shared cable. Star topology consists of devices connected to cable segments that branch out from a central point, or hub. Ring topology occurs when devices connect to a cable that forms a loop. Combining these three topologies form a variety of more complex or hybrid topologies.

Before choosing any topology, some of the factors to consider are:

- Cost.
- Scalability.
- Bandwidth capacity.
- Ease of installation.
- Ease of troubleshooting.

### *Bus topology*

The bus topology also called a “linear bus” because the computers connect in a straight line. All device connections use a single cable that runs throughout the network (fig. 3–3). These devices share the responsibility for getting data from one point to another. Each node on a bus network passively listens for data directed to it. When one node wants to transmit data to another node, it broadcasts an alert to the entire network, informing all nodes that a transmission is underway; the destination node then picks up the transmission. Nodes other than the sending and receiving nodes ignore the message.

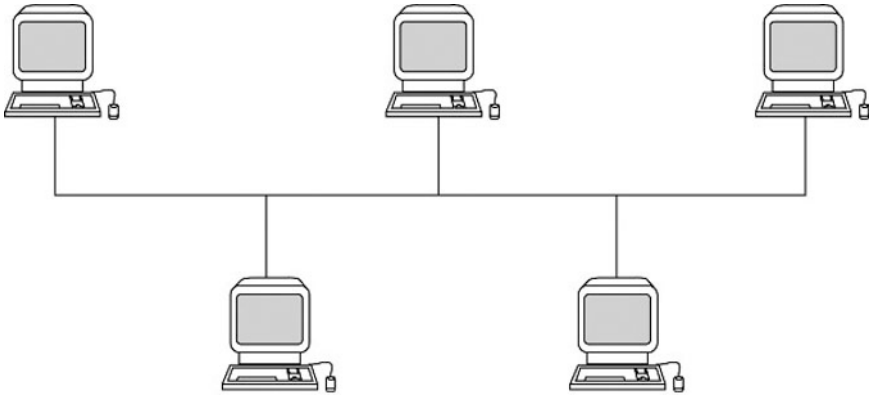

**Figure 3–3. Bus topology.**

Most bus networks use coaxial cable as their physical medium. At the ends of each bus network are 50-ohm resistors known as terminators. Terminators stop signals after they have reached the end of the wire. Without these devices, signals on a bus network would travel endlessly between the two ends of the network a phenomenon known as signal bounce and new signals could not get through. On a network, terminators prevent this problem by halting the transmission of old signals. In some cases, a hub provides termination for one end of a segment. A bus network requires grounding at one end to help remove static electricity that could adversely affect the signal.

Networks that have a physical bus topology usually use thin coaxial cable that connects to the network interface card (NIC) using a Bayonet Neil-Coleman (BNC) connector. This connects two or more computers in a daisy-chain fashion, or terminates at one end of the cable.

The IEEE 802.3 standard has set the length of a cable segment and the number of devices on an Ethernet bus network. For a Thinnet network, also referred to as 10Base2 and Thin Ethernet, the maximum segment length is about 600 feet, which connects a maximum of 30 devices. You may use

up to four repeaters joining a maximum of five segments (three of which can be populated with devices), for a total cable length of 3,035 feet. The total number of nodes allowed is 150.

Another less commonly found option is [cabling, also known as Thick Ethernet and 10Base5. Thicknet cabling uses a thicker-gauge coaxial cable than Thinnet, and was once a frequent choice for backbone installations. The cable segment limitation is 1,625 feet, with a maximum of 100 nodes per segment. Thicknet allows four repeaters for a total cable length of 8,125 feet, with 300 total nodes.

### *Advantages*

The advantages of a bus topology include the following:

- Inexpensive to install, Thinnet in particular.
- Easy to add more workstations.
- Require less cable than other topologies.
- Work well for small networks (2–10 devices).

### *Disadvantages*

The disadvantages of a bus topology include the following:

- It is no longer a recommended option for new installations.
- If the backbone breaks, the network is down.
- Only a limited number of devices can be included.
- It is difficult to isolate where a problem may be.
- Sharing the same cable means slower access time.

## ***Star topology***

In the star topology, cable segments from each computer connect to a centralized component (fig. 3–4). The central component can be one of a variety of devices. It can be an active or passive device, like a hub or an intelligent device such as a router, switch or a bridge. Some intelligent hubs can incorporate diagnostic features that make it easier to troubleshoot network problems. A physical star topology installs in the shape of a star, like spokes in a bicycle wheel. Each device in a star network connects to the central component with its own cable. Although this does require more media, it has many advantages over both the bus and ring topologies. Signals transmitted from the sending computer through the central component to all computers on the network. This topology originated in the early days of computing when computers connected to a centralized mainframe computer.

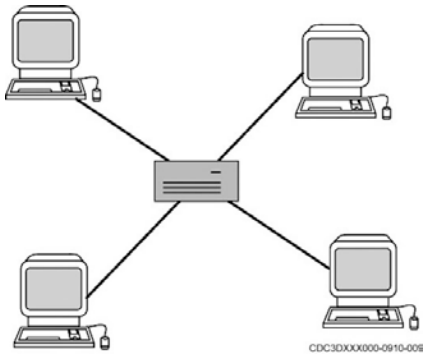


**Figure 3–4. Star topology.**

Star topologies are usually built with twisted-pair or fiber-optic cabling. Any single cable on a star network connects only two devices (for example, a workstation and a hub), so a cabling problem will affect two nodes at most. Devices such as workstations or printers transmit data to the hub, which then retransmits the signal to the network segment containing the destination node.

Star networks and extended star networks have quickly become the predominant topology type for most networks. One of the advantages of a star topology is that it is easy to make changes and additions to the network without disrupting users. You can add a new workstation or expand the network without ever affecting the network's performance. Star networks can support a maximum of only 1024 addressable stations on a logical network.

### *Advantages*

The advantages of a star topology include the following six things.

1. It is easy to add more devices as your network expands.
2. The failure of one cable or one cable break will not bring down the entire network.
3. The hub provides centralized management.
4. It is easy to find device and cable problems.
5. It is upgradable to faster network transmission speeds.
6. It is the most common topology; so many equipment options are available.

### *Disadvantages*

Listed below are the disadvantages of a star topology are.

- A star network requires more media than a ring or bus network.
- The failure of the central hub can bring down the entire network.
- The costs of installation and equipment are higher than for most bus networks.

If a star network expands to include an additional network component connected to the central component, it is an extended star topology.

## ***Ring topology***

The ring topology is a topology in which the stations are connected in the form of a ring or circle (physical ring), in which the data flows in a circle, from station to station (logical ring), or a combination of both (fig. 3–5). It has no beginning or end termination. This allows every device to have an equal advantage accessing the media. The signals travel around the loop in one direction and pass through each computer, which can act as a repeater to boost the signal and send it on to the next computer.

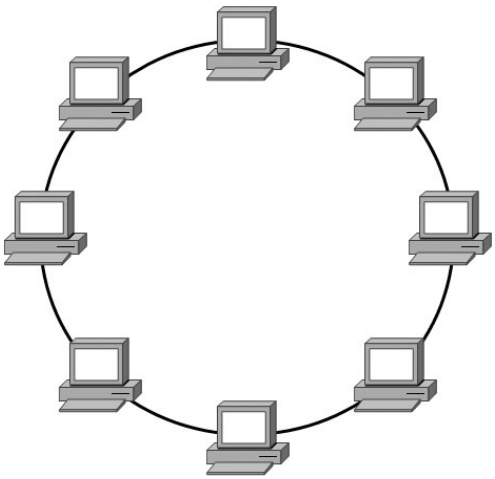

**Figure 3–5. Ring topology.**

Each workstation acts as a repeater for the transmission. The fact that all workstations participate in delivery makes the ring topology an active topology. Ring topology differs in this way from bus

topology. A ring topology also differs in that it has no “ends” and data stops at its destination. In most ring networks, twisted-pair or fiber-optic cabling is the physical medium.

There are two kinds of ring topologies:

1. Single ring.
2. Dual ring.

When first implemented, ring networks used a single-ring topology. In a single-ring network, all the devices share a single cable, and the data travels in one direction like a merry-go-round. Each device waits its turn and then transmits. When the data reaches its destination, another device can transmit. The drawback of a simple ring topology is that a single malfunctioning workstation can disable the network.

In addition, just as in a bus topology, the more workstations that must participate in data transmission, the slower the response time. Consequently, pure ring topologies are not very flexible or scalable. Contemporary LANs rarely use pure ring topologies.

The most common implementation of the ring is in a Token Ring network. Token Ring network installations use a physical ring or a physical star. As technology evolved, a dual-ring topology was developed (fig. 3–6). This topology allows two rings to send data, each in a different direction.

Not only does this let more packets travel over the network; it allows packets to continue along the media, creating redundancy.

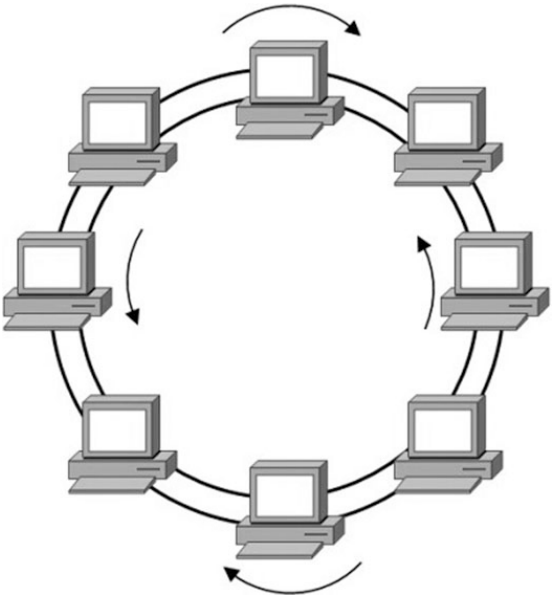

**Figure 3–6. Dual ring topology.**

Fiber distributed data interface (FDDI) is a technology similar to Token Ring, but it uses light instead of electricity to transmit data. FDDI networks use two rings for redundancy. FDDI is unique compared to other types of ring networks because it will keep functioning in the event there is a break in one or both rings.

### *Advantages*

The advantages of a ring topology are listed below:

- Data packets can travel at greater speeds.
- There are no collisions.
- It is easier to locate problems with devices and cable.
- No terminators are needed.

### *Disadvantages*

The disadvantages of a ring topology are listed below:

- A ring network requires more cable than a bus network.
- A break in the cable will bring many types of ring networks down.
- When you add devices to the ring, all devices are suspended from using the network.
- It is not as common as the bus topology, so there is not as much equipment available.

### *Hybrid*

A hybrid topology combines two or more different physical topologies in a single network. The two most common hybrids found today are the star-bus and star-ring topologies.

### *Star-wired ring*

The star-wired ring topology uses the physical layout of a star in conjunction with the ring topology's data transmission method. Data transmits around the star in a circular pattern. This hybrid topology benefits from the fault tolerance of the star topology (data transmission does not depend on each workstation to act as a repeater) and the reliability of token passing. Token Ring networks, as specified in IEEE 802.5, use this hybrid topology.

### *Star-wired bus*

Another hybrid topology combines the star and bus formations. In a star-wired bus topology, groups of workstations are star-connected to hubs and then networked via a single bus. With this design, you can cover longer distances and easily interconnect or isolate different network segments. One drawback is that this option is more expensive than using either the star or, especially, the bus topology alone because it requires more cabling and potentially more connectivity devices. The star-wired bus topology forms the basis for modern Ethernet and fast Ethernet networks.

### *Logical bus*

The term logical topology refers to the way in which data transmits between nodes, rather than the physical layout of the paths that data takes. A network's logical topology will not necessarily match its physical topology.

---

## Self-Test Questions

**After you complete these questions, you may check your answers at the end of the unit.**

### 034. Network architecture

1. What is an Intranet?

2. Extranets are Intranets that provide what extra services?

### 035. Types of networks

1. What is a LAN?

2. A WAN connects networks that are typically what?

### 036. Network topologies

1. When referring to network topologies, what two characteristics describe the topology type?

2. Name the three basic topologies that all networks stem from.

3. A bus topology connects all devices in the network with what?

4. If you were setting up a new network, why should you *not* consider a bus topology?

5. In a star topology network, what are all devices connected to?

6. What are the most predominant types of network topologies used today?

7. What network topology allows every device to have an equal advantage accessing the media?

8. What major disadvantage happens to ring networks when you add devices to the ring?

## 3–6. Network Devices

When you link computers together to share data and communicate, you create a network. Networks come in many different sizes, as little as two computer up to hundreds of thousands, all interconnected through network devices. As a RAWS technician, you will need to have an understanding of the most common devices used to create Air Force Networks.

### 037. Modems

Modems (MOdulator/DEModulator) condition data from a terminal device before transmission over the transmission medium. This process of conditioning will require a signal conversion, for example analog to digital or digital to optical, in order for the signal to pass through other communications equipment. In other cases, multiple signals are combined making effective use of available bandwidth. This objective covers the equipment that performs this conditioning.

#### Modulate and demodulate

A modem is a device that modulates signals to encode digital information and demodulates signals to decode the transmitted information. The modem produces a signal that enables ease of transmission and provides decoding to reproduce the original data. A common type of modem is one that turns the digital data of a computer into modulated electrical signal for transmission over telephone lines and demodulated by another modem at the receiver side to recover the digital data.

The term modem is actually an acronym that stands for modulator/demodulator. The original telephone modems connected users to the Internet by sending and receiving signals in the voice band (20 Hz to 20 kHz) of telephone networks. Two types of commonly used modems are dial-up and dedicated, also known as leased.

### Applications

Today, there is a wide array of modems used in various systems to support diverse media applications. One of today's commonly found modems is a fiber optic modem, which converts a digital signal into light and enables transmission of data over a greater distance with less signal loss and greater bandwidths than traditional copper. In fact, the purpose of many modems today is to enable transmission of data over greater distances with the lowest possible signal loss. Another use for modems is to interface specific equipment through different types of media. For instance, although not typically used in military applications, cable modems enable high-speed digital transmission through existing architecture provided by cable companies. They enable simultaneous use of computer and television signal on the same transmission line without interfering with one another.

## 038. Switches and bridges

Switches and bridges are two data linking devices that are very similar in nature, with one having more capabilities than the other does. Below describes the purpose and gives an overview of each device.

### Bridges

A bridge is a data link layer (Layer 2, see OSI model for more information) network device or software set that logically separates a single network into multiple segments or collision domains in Ethernet networks. The primary use for a bridge is to decrease network congestion but it also propagates a signal like a repeater. In an Ethernet network, if two computers transmit at the same time, a collision occurs. The larger the network, without bridges, the more likely you are to have a collision and attenuation. If using a bridge, computers/devices (nodes) only detect collisions on the same side of the bridge that the collision occurred. However, the nodes will not detect the collision on the opposite side of the bridge on the other segment. A bridge decreases the amount of network congestion by passing only the frames destined for computers/devices on the segment on the other side of the bridge.

### Switches

Switches are data link layer (Layer 2) devices that provide central connection to network devices used in the same way as hubs, but function more like bridges. They can provide higher bandwidth and frame-level filtering as well as dedicated port speed to specific devices on a segment. Many types of switches exist: LAN switches, Asynchronous Transfer Mode switches, and different types of WAN switches.

Switches provide collision-free, high-speed communication between network devices. Switches operate like a one-way bridge with multiple ports. They do this by remembering the MAC address or addresses that are at each port and forward frames directly to the port as discussed in the previous lesson. This provides the full bandwidth for each port, unlike hubs, which must share the bandwidth with each port. Because ports on a switch operate like a bridge, each physical port is logically a separate segment, also referred to as a "collision domain." This will greatly reduce or eliminate collisions on a network. If you connected two file servers to individual ports, up to two simultaneous connections between workstations and file servers can occur. This results in increasing the maximum bandwidth from 10 Mbps on an Ethernet 10 BASE-T to 20 Mbps when operating in full-duplex mode. Switches not only eliminate collisions and speed up the network they offer flexibility.

Physical connections of different speeds such as a 10 Mbps and a 100 Mbps communicate using a switch, which accomplishes this through buffering. Store-and-forward switching is required whenever a frame must be moved from a low-speed connection to a high-speed connection.

## 039. Routers, multiplexers, and converters

Routers are often referred to as a gateway device because they sit on the border or the boundary of your network. It is the last point of contact (POC) as packets move out of the network. It is also the first POC for packets that are coming into the network. Therefore, routers always connect at least two networks together. That can be a LAN to a WAN, a LAN to another LAN within your own organization, or of course, very commonly, your LAN to your Internet service provider. Multiplexers (mux) combine several signals on one transmission line to link between two or more locations. It is then deciphered at the receiving location and sent to the corresponding equipment. This ultimately reduces infrastructure and communications related costs. A converter performs exactly as its name implies, it converts a signal from one medium to another.

### Routers

Routers operate at Layer 3 (network) of the OSI model. A typical router has an internal processor, an OS, memory, input and output jacks for different types of network connectors (depending on the network type); and, usually, a management console interface. They can be devices dedicated to routing, or they can be off-the-shelf computers configured to perform routing services. Routing involves two basic activities: determining optimal routing paths and transporting information groups (typically called packets) through an Internetwork (also known as switching). Although switching is relatively straightforward; path determination can be very complex. You may ask how does a router or multilayer switch determine the best path? The next part of this lesson will explain.

#### *Path determination*

A metric is a standard of measurement, such as path length used by routing algorithms to determine the optimal path to a destination. To aid the process of path determination, routing algorithms initialize and maintain routing tables, which contain route information. Route information varies depending on the routing algorithm used.

Routing algorithms fill routing tables with a variety of information. Destination and next hop associations tell a router that a particular destination can be gained optimally by sending the packet to a particular router representing the “next hop” on the way to the final destination. When a router receives an incoming packet, it checks the destination address and attempts to associate this address with a next hop.

Routing tables also can contain other information, such as data about the desirability of a path. Routers compare metrics to determine optimal routes, and these metrics differ depending on the design of the routing algorithm used. Routers communicate with one another and maintain their routing tables through the transmission of a variety of messages. The routing update message is one such message that generally consists of all or a portion of a routing table. By analyzing routing updates from all other routers, a router can build a detailed picture of network topology. A Link-State Advertisement, another example of a message sent between routers, informs other routers of the state of the sender’s links. Link information also can build a complete picture of topology to enable routers to determine optimal routes to network destinations.

#### *Switching*

Switching algorithms are relatively simple and are the same for most routing Protocols. In most cases, a host determines that it must send a packet to another host. Having acquired a router’s address by some means, the source host sends a packet addressed specifically to a router’s physical (MAC-layer) address, this time with the network-layer Protocol address of the destination host.

As it examines the packet's destination Protocol address, the router determines that it either knows or does not know how to forward the packet to the next hop. If the router does not know how to forward the packet, it drops the packet. If the router knows how to forward the packet, it changes the destination physical address to that of the next hop and transmits the packet.

The next hop, in fact, may be the ultimate destination host. If not, the next hop is usually another router, which executes the same switching decision process. As the packet moves through the Internetwork, its physical address changes, but its Protocol address remains constant.

### *Static versus dynamic*

Routers may use one of two methods for directing data on the network: static or dynamic routing. The following paragraphs describe both methods. You will see that one has clear advantages over the other.

#### *Static routing*

Static routing is a technique in which a network administrator programs a router to use specific paths between nodes. Because it does not account for occasional network congestion, failed connections or device moves, static routing is not optimal. If a router or a segment connected to a router moves, the network administrator must reprogram the static routes. Static routing requires human intervention, so it is less efficient and accurate than dynamic routing.

#### *Dynamic routing*

Dynamic routing, on the other hand, automatically calculates the best path between two nodes and compiles this info into a routing table. If congestion or failures affect the network, a router using dynamic routing can detect the problems and reroute data through a different path if possible. As a part of dynamic routing, by default, routing Protocols update the routing tables when adding a router to a network.

Most networks primarily use dynamic routing, but may include some static routing to indicate, for example, a router of last resort. Termed the gateway of last resort, it is a static route used by the router when no other known route exists to transmit the packet. Routers are not simple to install on sizable networks because of their complexity and network interaction.

## Multiplexers

The term "multiplexing" means either combining (multiplex) many different signals into one serial digital data stream (transmit) or to split apart (demultiplex) a serial digital data stream into many different signals (receive).

Any data communications environment that has more than one line going between common locations can benefit by installing a pair of muxs. A mux performs the function of combining several data or voice communication channels into one composite signal, which can be transmitted between two locations cheaper than the cost of individual lines. The most effective combination of lines in a muxed environment is between 4 and 8. Studies show that as little as 10 to 15 percent utilization of such lines is a common occurrence. Individual users connect to channels and the composite (logical) communication line between the two locations is the link. Link Protocol is the communications discipline used between the two muxes.

Although the primary reason for installing a mux is to save on communications costs, two other benefits are also present. One is the inherent error correction existing in a muxed environment and the other is inherent data security. Since a mux functions by taking individual data and transmitting it as data frames, there is an error detection and retransmission scheme built in. Error correction is so vital in many data transmission types, such as graphic data and program transmission, that many muxes are used mainly for their error correction capabilities. The other benefit is data security (not encryption), which is achieved by the fact that the individual data streams are formatted into a single communication line on one end of the link and then broken up into individual components on the

other end. Someone wishing to “tap” into a muxed signal must have the link protocol and know the individual channel assignment schemes and data formats.

### Converters

A media converter is quite simply an adapter. It has hardware used to enable segments or networks using different media to interconnect and exchange signals. This is a very cost-effective and flexible networking device. There are several different types of converters; however, for example, you can convert between unshielded twisted pair with an RJ–45 connector to fiber and the appropriate connectors. You might also see something like multi-mode fiber being converted to single-mode fiber and vice versa. You may even have to utilize electrical signals found on copper unshielded twisted pair, and convert them to light waves for fiber optic cabling. Now, if you are talking about needing to convert hundreds of cable connections, you probably would not implement hundreds of converters. You would go with a larger scale, more robust, centralized device, capable of handling multiple conversions within that single device. However, for just a few connections, a media converter can certainly do the job. Now, there can be other applications as well.

Converters can be essential if the distance between two network devices is greater than the cable transmission distance. Ethernet still maxes out around 328 feet. If there is a need to go beyond that, then a converter can be used because most of them also have the ability to boost the signal. In other words, they can act as repeaters. This allows two network devices to connect across longer distances than if they were just using a single cable. Now typically, media converters are Protocol specific and support various data rates and network types; but generally, the Protocol itself is specific to the converter. They are usually implemented as physical layer devices, because of the small amount of programming in them. Some higher scale converters do operate at layer 2, and provide some switching functionality as well. They can also implement wavelength division multiplexing wavelength variances. This uses different colors of laser to implement the multiplexing capability of the media, so that you can boost your performance over your present fiber optic links.

## 040. Encryption devices

Cryptographic devices provide the means to protect the sensitive and classified information from the enemy. Each device can both encrypt a signal for transmission and decrypt a signal to restore it back to its original format. Digital cryptographic devices are used to encrypt and decrypt communications links. All encryption uses keys and algorithms to enable securing of signals.

### How encryption and masking devices are used

Like a vault in a bank, information and COMSEC utilize secret combinations to secure the data. The sender locks the transmitted information with the secret combination, or key, and the receiver (the only person with knowledge of the key) can unlock the information assuming they have the same key. In communication links, this is encryption.

Applying the same security principles to communications links provides much the same advantages to the sender, as long as the key remains secret. The economics of the encoding process greatly favor the authorized users of the communications links. The required decoding by an intruder without the secret key would require massive amounts of operations and expenses, which would start over each time a key code changes.

### Fill devices

Fill devices store and load cryptographic keying material. You have to have a way to initiate the use of a coding system. There are many different fill devices available to you as a technician. The keys that are stored on this type of device are either electronically loaded or manually loaded from Mylar tape using a general-purpose tape reader. With modern technology, there have been advances to where one small device can handle hundreds of keys for transfer into encryption devices. The most commonly used fill device currently in use is the simple key loader (SKL). This device holds multiple keys using multiple different formats. The SKL has taken, or is taking the place of many legacy fill

devices you may still have in your work center, such as the KOI–18, KYK–13, AN/CYZ–10 Digital Transfer Device, and so forth.

**NOTE:** The fill device assumes the classification of the highest-level key loaded as soon as it is loaded.

## 041. Communication mediums

In the previous lesson, we discussed several of the most common network devices. Now we will cover how these devices interconnect. As you might imagine, a number of different network media types are available. Some faster than others, some will work over relatively long distances, and some do not require a physical connection to the network at all. This lesson will cover all the major communication relay types and their characteristics, uses and features. In general, most networks use metallic cable for connection at some point; the most common types are coaxial cable and twisted pair cable.

### Coaxial cable

Coaxial cable is the granddaddy of all mainstream network media types and it is associated with the original designs of the Ethernet standard. Today you will typically use coaxial cable when you need a broadband solution.

Coaxial cable consists of a single wire core surrounded by an insulation layer; an outer metal screen made of a woven copper mesh; a metal-covered plastic or foil; and an exterior protective sheath. The metal screen shields the conductor from corruption by external signals, such as radio waves, and other sources of electromagnetic interference (EMI), such as power cables, cellular phones, motors, fluorescent light fixtures and electrical storms. Coax's shield also significantly reduces the amount of radiation given off by EMI, essentially eliminating a source of interference that causes problems for other systems. Coaxial cable gets its name from its physical characteristics, specifically because the conductor wire and the shielding braid share a common axis or centerline.

New LAN installations rarely use coaxial except for highly specialized settings, such as elevator shafts where EMI causes significant problems. Coaxial is widely used in many other settings. This includes military applications, where a high-speed broadband solution is required.

There are many different types of coax cable; each one is suited for a different purpose, such as audio, video, television (TV), satellite, cable, radio, and data transmission. Cable types match the characteristics of the signal they are transmitting. The radio-guide (RG) is an identifier of coaxial cable types. For example, RG–6 defines a specific type of coaxial cable, used to transmit cable TV signals, with a nominal impedance of 75 Ohms. The following are some more common coax cable types:

- RG–58, 50 Ohms, 600 feet distance limitation.
- RG–8, 50 Ohms, 1640 feet distance limitation.
- RG–11, 50 Ohms, 1640 feet distance limitation.

The nominal impedance, a measure of the wire's resistance shows how much the cable impedes or resists the flow of electric current, is one of the factors that determines the RG rating. This difference is why you always use the correct cable types for the job. Mismatched RG types could cause equipment damage and or system failure.

### *Unshielded twisted-pair cable*

Most, if not all, modern networks use a metallic cable known as unshielded twisted-pair cable, commonly called twisted pair. Twisted pair cable is typically a copper wire medium and it is the primary carrier for voice telecommunications. A paired cable consists of two wires individually insulated from one another and twisted together to make one pair. Wire pairs then twist together with other pairs to form a cable. The twisting cancels out induced signals that can interfere with the

communication signals. A protective sheath such as lead or plastic then covers the cable to protect the pairs against physical and or environmental damage.

Twisted-pair cable comes in a variety of grades, called categories, numbered Category 1 through Category 6a. These categories, developed throughout the years, facilitate faster and faster network designs with each new development. The following is a description of each category and their capabilities:

- CAT 1, 1 Mbps, voice only analog phone lines (not used for data communications).
- CAT 3, 10 Mbps, Ethernet (10BaseT).
- CAT 5, 100 Mbps, Ethernet (100BaseT).
- CAT 5e, 1 Gbps (1000 Mbps), Ethernet (1000BaseT).
- CAT 6 and 6a, 10 Gbps, 10 Gigabit Ethernet (10GbE).

Most new cabling instillations will use Category 6 (CAT 6) or Category 6a cabling because they support all current and planned data speeds and standards. In addition, the manufacturers normally print the category of the cable on its sheathing.

#### *Shielded twisted-pair cable*

Shielded twisted-pair cable has the combined features of the twisted pair cable and coaxial cable. With shielded twisted-pair, a thin aluminum foil or a copper braid like the one used in coaxial cable wraps around the pairs. The conductors are spaced uniformly during manufacture. This leaves each wire perfectly balanced capacitive to the surrounding conductor. Maintaining the balance minimizes certain detrimental effects such as high capacitance to ground when grounding the shield. This line does not radiate energy because of the shield, so nearby magnetic fields do not affect it. The system control facility, between the main distribution frame and the patch bays, will often use shielded cables to reduce interference and crosstalk. Cable transmission systems may be placed on poles or other structures above ground or buried using a lead or polyethylene covering for protection, or placed in conduits or ducts. Telephone companies use both aerial and buried cable communication systems to bring telephone service from central offices to their many subscribers. Military installations use cables to connect end communication devices (e.g., telephones, facsimile and computer terminals to the cable). Systems control provides an interface point at the main distribution frame for inter-site communications via cable systems.

### Fiber optic cable

Alexander Graham Bell’s many inventions included the photophone. In 1880, he demonstrated with this device that a beam of sunlight would reflect off a shiny diaphragm mounted on an acoustic horn. The light beam, aimed at a selenium photocell and connected to a speaker, enabled the reproduction of speech transmission at a distance of 700 feet. Due to its limited applications and lack of directional capabilities, light wave communications went unexplored for about 80 years.

In the mid–1960s, the first fiber cables were developed but they attenuated the signal too much to be usable. By 1970, silica glass fibers were in development. They are as thin as a human hair and bendable. These fibers were the first practical optic waveguides, and opened the door to further advances. Simultaneously, semiconductor technology made possible the fabrication of efficient light sources that allowed modulation with an external signal.

#### *Advantages of optical communication systems*

Just as it is possible to send Morse code signals to a receiver some distance away using a flashlight, it is also possible to send signals by LED or light amplification by stimulated emission of radiation (commonly referred to as laser). An LED can generate 2.5 mill watts of wide angle infrared light in a wavelength band measuring 0.87 to 0.92 microns (µm). An optical communications system requires a light source (transmitter), a transmission medium (cable), and a sensor (receiver). Transmission over fiber optic systems promises advantages over conventional cable systems because they have larger

bandwidths, freedom from interference, low attenuation, are lightweight, more secure and are safer to use. Fiber optics enable transmission of much more information than the lower-microwave frequency properties.

### *Fiber systems*

Fiber optics are the result of the merging of the two unrelated disciplines of semiconductor technology, which provided the necessary materials for the light sources and detectors, and optical waveguide technology, which provided the medium—the optical fiber cable. The reason fiber optic is so highly praised is its many advantages over other transmission media, both traditional (copper wire) and non-traditional (microwave) as shown in the table below.

| Property/Type of Cable | Fiber optic | Twisted pair | Coaxial |
|---|---|---|---|
| **Electromagnetic interference (EMI) immunity** | Yes | No | No |
| **Radio frequency interference (RFI) immunity** | Yes | No | No |
| **Electromagnetic pulse (EMP) immunity** | Yes | No | No |
| **High degree of transmission security** | Yes | No | No |
| **Electrical isolation** | Yes | No | No |
| **No crosstalk** | Yes | No | No |
| **No echoes or ringing** | Yes | No | No |
| **Temperatures to 1000º C** | Yes | No | No |
| **Elimination of spark/fire hazards** | Yes | No | No |
| **Low cost** | Yes | Yes | No |

### *Broad bandwidth*

Fiber optic cable systems have more potential bandwidth than any other type of system. The potential information carrying capacity or the amount of information that transmittable over a communications channel increases with frequency. Since the frequencies of light are much higher (in the terahertz range) than radio frequencies, an optical fiber has the potential for a lot of information. Theoretically, the higher bandwidth of fiber permits thousands of channels carried over the same fiber, at the same time.

### *Low attenuation*

Not only does fiber optic cable have a higher information carrying capacity than metallic cable, it also introduces less attenuation and distortion into the system. More important, attenuation in fiber cable does not increase with signal frequency as it does in metallic cables.

### *Electromagnetic immunity*

EMI is unwanted energy given off by electronic circuits and picked up by other circuits. Since fiber optic cable does not radiate or absorb energy through its outer jacket, it is immune to both EMI and RFI. Parallel installation of several fiber optic cables, even in the same enclosure, without the signals interfering with each other, is possible. This is because the fibers in optic cables are made of a dielectric material (glass or plastic).

### *Weight*

Glass weighs less than metal. Weight savings are important, since the bandwidth and low line loss of fiber allow a single fiber to replace several metallic cables.

### *Security*

Fiber is *almost* impossible to tap without affecting the transmission enough for authorized users to notice. In addition, fiber does not radiate energy. This feature makes electromagnetic field (EMF) sensing eavesdropping equipment useless.

#### *Safety*

The dielectric composition of fiber isolates it electrically. The fiber presents no spark hazard, and proves its use in flammable environments where metallic cables present hazards. Fiber cables do not attract or respond inductively to lightning. In addition, they do not short out or produce electric shocks.

### *Disadvantages of optical communication systems*

The advantages of fiber optic cable systems far outnumber the disadvantages. However, there are some drawbacks.

#### *Cost*

Although the cost is decreasing, it is a drawback in some areas, such as installation and end equipment. Unfortunately, the high cost of interfacing equipment somewhat offsets the simplicity and economy of fiber optics.

#### *Physical handling/installation*

Technicians skilled in working with copper cables now have to learn new methods of cable splicing. They must go to special schools to learn these new techniques. Because fiber optics is a relatively new field, there has been rapid progress in solving or reducing the seriousness of the problems involved, and dropping the cost. Fiber optic cables have already shown their cost effectiveness in long distance communications links. The low line loss of fiber optic cables means fewer repeaters are required.

## Wireless medium

Throughout the years, there have been multiple wired and wireless ways to connect IT devices together and more created all the time. The vast majority of networks use twisted pair cabling, with fiber to interconnect LANs and WANs. Arguably, the largest growth in networking is in the wireless domain. In this area, we'll look at 802.11-based networks, lasers, and infrared technologies.

### *802.11 wireless*

The most common standard used for wireless networking is the IEEE 802.11 standard. The IEEE supports four specific standards for wireless networking: 802.11a, 802.11b, 802.11g and 802.11n. All of these standards use radio links to provide connectivity to network nodes through a transmitter/receiver unit (transceiver, commonly known as an access point or wireless access point, which transmits and receives signals to and from the wireless network adapters).

### *Laser links*

Laser links are also an option for wireless data transmission, but setup is a major disadvantage, and laser systems will suffer from weather-related problems as well as loss of signal as the high-power laser emitter ages. Laser systems require line-of-sight path between transmitter and receiver, before installation always address all intermediate obstacles to the laser system.

### *Infrared links*

Infrared devices deliver connection by Infrared Data Association (IrDA) Protocol. IrDA is a widely supported standard and is included in all versions of Windows and Apple as well as Linux.

Infrared data links have disadvantages; data transmission is much slower than most other wired or wireless options. Infrared devices can transfer data at up to 4 Mbps. The maximum distance between infrared devices is 3 feet, and connections must be in direct line of sight. Anything that breaks the light beam will cause interference.

In terms of security, the IrDA Protocol offers exactly nothing in the way of security, zero encryption or authentication. The only security feature is the fact that you have to be literally within arm's length

to establish a link. Infrared is not a solution for a dedicated network connection, but for a quick file transfer or print job, it will do in a pinch.

## Self-Test Questions

**After you complete these questions, you may check your answers at the end of the unit.**

### 037. Modems

1. What two terms make up the acronym “MODEMS”?

2. What is the purpose for many of the modems in use today?

### 038. Switches and bridges

1. What is a bridge?

2. Switches provide higher speeds for communications because they enable what?

### 039. Routers, multiplexers, and converters

1. What are the names of the two basic activities that routing assists?

2. If a router does not know how to forward a packet, what does it do with it?

3. Routers may use what two methods for directing data on a network?

4. Name three benefits to using muxes in a communications network.

5. What network device would you use if you needed to change a communications signal from copper wire to fiber optic cabling?

### 040. Encryption devices

1. In encryption, what is needed by the sender and receiver in order to have successful communication?

2. What is a fill device used for?

### 041. Communication mediums

1. What are the two most common types of metallic cabling?

2. Where does coaxial cable get its name from?

3. What advantage does twisting metallic cable pairs give to communication signals?

4. List six advantages fiber optic systems have over conventional cable systems.

5. List three types of wireless communications.

## Answers to Self-Test Questions

### 022

1. Central processing unit.
2. If the data contents are lost when removing power from a system.
3. It uses a very small battery to trickle a small charge to the BIOS, ensuring that the data is preserved.
4. To reduce CPU access time.

### 023

1. It was designed for hard drives only.
2. The Peripheral Component Interconnect bus.
3. Universal Serial Bus.

### 024

1. Backup critical information, or copy it onto other media.
2. Graphics/video card.

### 025

1. The hardware and software on the computer.
2. Microsoft Windows, Linux, and Unix.

### 026

1. (1) Reformatting a hard disk.
   (2) Erasing programs and files.
   (3) Adding unrecognizable characters to files.
   (4) Destroying disk directories and file allocation tables.
2. Spyware.

3. Visiting infected websites or clicking on a bad e-mail link or attachment.

**027**

1. Kernel, shell, and user programs (also called commands).
2. Control user processes and manage system resources.
3. The shell.
4. (1) c.

   (2) b.

   (3) e.

   (4) g.

   (5) f.

   (6) a.

   (7) d.

**028**

1. vi editor.
2. (1) Ping.

   (2) File transfer Protocol.

   (3) Telnet.
3. Root account (also called “superuser”).

**029**

1. International Organization for Standardization.
2. Open Systems Interconnect seven-layer model.
3. Application (upper) layer and data transport (lower) layer.

**030**

1. DISN.
2. DISA.

**031**

1. After connection is established between the sender and recipient.
2. (1) The requestor sends a packet specifying the port number it plans to use and its ISN to the server.

   (2) The server acknowledges with its ISN, which consists of the requestor’s ISN, plus 1.

   (3) The requestor acknowledges the ACK with the server’s ISN, plus 1.
3. Flow control methods.
4. Receipt ACK.

**032**

1. Logical addressing of devices on the network, as well as routing data between a source and destination.
2. Internet Protocol.
3. As four sets of 8 binary bits; four OCTETS or BYTES, for a total of 32 bits.
4. Address class.
5. Bits represented by ones identify the network address and bits represented by zeroes identify host addresses.
6. Four times larger.
7. Unicast, multicast and anycast.

**033**

1. Port numbers that devices allocate dynamically for a source port number.
2. (1) 0–1023 are well-known ports.

   (2) 1024–49151 are registered ports.

   (3) 49152–65535 are dynamic or private ports.

**034**

1. A private Internet.
2. They share a portion of their content with customers, suppliers, or other businesses, but not with the public.

**035**

1. A group of computers and associated devices that share a common communications line and typically share the resources of a single processor or server within a small geographic area (for example, within an office building).
2. Separated by geographical distances.

**036**

1. Physical and logical topology.
2. Bus, star, ring.
3. A single cable that runs throughout the network.
4. It is no longer a recommended option for new installations.
5. A central component with its own cable.
6. Star and extended star networks.
7. Ring networks.
8. All devices are suspended from using the network.

**037**

1. Modulator and Demodulator.
2. Enable transmission of data over greater distances with the lowest possible signal loss.

**038**

1. A data link layer network device or software set that logically separates a single network into multiple segments or collision domains in Ethernet networks.
2. Collision-free communication.

**039**

1. Determining optimal routing paths and transporting information groups through an Internetwork.
2. It drops the packet.
3. Static or dynamic routing.
4. (1) Save on communications costs.

   (2) Inherent error correction.

   (3) Inherent data security.

5. Converter.

**040**

1. The same key.
2. Store and load cryptographic keying material.

**041**

1. Coaxial and twisted pair cable.

2. From its physical characteristics, specifically because the conductor wire and the shielding braid share a common axis or centerline.
3. Twisting cancels out induced signals that can interfere with the communication signals.
4. (1) Larger bandwidths.
   (2) Freedom from interference.
   (3) Lower attenuation.
   (4) Lightweight.
   (5) More secure.
   (6) Safer to use.
5. (1) 802.11-based networks.
   (2) Laser links.
   (3) Infrared technologies.

**Complete the unit review exercises before going to the next unit**.

## Unit Review Exercises

**Note to Student:** Consider all choices carefully, select the *best* answer to each question, and *circle* the corresponding letter. When you have completed all unit review exercises, transfer your answers to the Field-Scoring Answer Sheet.

**Do not return your answer sheet to the Air Force Career Development Academy (AFCDA).**

50. (022) Where are basic input/output system (BIOS) settings saved?
    a. Cache.
    b. Random access memory (RAM).
    c. Compact disc-read-only memory (CD-ROM).
    d. Complementary metal oxide semiconductor (CMOS) memory.

51. (022) What type of power supply is *most* commonly used in computers today?
    a. Linear.
    b. Switching.
    c. Internal disk.
    d. Non-volatile.

52. (023) What was developed to enhance a computer's video subsystem because of the increased performance requirements on high-end PCs?
    a. FireWire.
    b. Universal Serial Bus (USB).
    c. Accelerated Graphics Port (AGP).
    d. Serial Advanced Technology Attachment (SATA).

53. (024) Why is it essential for critical information from hard disk drives to be backed up or copied onto other media?
    a. Hard drives connect by FireWire and Universal Serial Bus (USB).
    b. Disk drives are subject to mechanical failure.
    c. Stored data is susceptible to hackers.
    d. It is not essential.

54. (024) What performs the function of displaying the screen you see on a computer monitor?
    a. Liquid crystal display.
    b. Cathode ray tube.
    c. Graphics/video card.
    d. Image scanner.

55. (025) Which operating system (OS) is a clone of Unix?
    a. International Business Machines (IBM) Solaris.
    b. Windows.
    c. Kernel.
    d. Linux.

56. (026) Which action is *not* a possible result of computer system damage originating from viruses?
    a. Redirecting power supply voltages.
    b. Reformatting of a hard disk.
    c. Erasing programs and files.
    d. Destroying disk directories.

57. (026) What is a *common* way malicious code can get into your system?
    a. Visiting the Air Force Portal.
    b. Backing up files to external media.
    c. Clicking an e-mail link or attachment.
    d. Logging in to weather systems for maintenance.

58. (027) How many *traditional* Unix directories are there?
    a. 5.
    b. 6.
    c. 7.
    d. 8.

59. (027) What directory is the highest-level directory in the Unix file system?
    a. home.
    b. root.
    c. mstr.
    d. bin.

60. (028) What is considered the standard Unix editor?
    a. File Transfer Protocol (FTP).
    b. Command.
    c. Insert.
    d. vi.

61. (029) What layer of the Open Systems Interconnect (OSI) model provides a variety of coding and conversion functions applied to application layer data?
    a. Session.
    b. Physical.
    c. Presentation.
    d. Application support.

62. (030) Who is the governing body for information technology (IT) communications within the Department of Defense (DOD)?
    a. Defense Information Systems Agency (DISA).
    b. Defense Information Systems Network (DISN).
    c. Open Systems Interconnect Organization (OSI).
    d. International Organization for Standardization (ISO).

63. (031) In positive acknowledgement, what does the sender do?
    a. Receives “CONNECT MADE” packet from recipient when connection is established.
    b. Keeps a record of each data packet sent and expects an acknowledgement.
    c. Sends data packets and is satisfied when sending buffer equals “1”.
    d. Activates a timer in the recipient system to track responses.

64. (031) Flow control methods prevent network congestion by
    a. ensuring transmitting devices do not overwhelm receiving devices with data.
    b. ensuring a window for transmitting devices is established in the error table.
    c. determining whether transmitted data has become corrupt or damaged.
    d. sending data through redundant paths to ensure delivery.

65. (031) Which connection protocol sends out data packets to the receiving system and *does not* require a receipt acknowledgement?
    a. Source Port Protocol (SPP).
    b. Connection-oriented communication.
    c. Datagram Checksum Protocol (DCP).
    d. Connectionless-oriented communication.

66. (031) User Datagram Protocol (UDP) is *best* for what type of transmission?
    a. When minor data loss is not acceptable.
    b. When windowing or acknowledgement is necessary.
    c. Applications that need to put sequences of segments together.
    d. Sending small amounts of data where guaranteed delivery is not required.

67. (032) What is the *basic* communication language or protocol of the Internet?
    a. Transmission Control Protocol/Internet Protocol (TCP/IP).
    b. Advanced Research Projects Agency Network (ARPANET).
    c. Integrated Services Digital Network (ISDN).
    d. Domain Name System (DNS).

68. (032) What protocol enables Transmission Control Protocol/Internet Protocol (TCP/IP) to Internetwork?
    a. Internet Protocol (IP).
    b. Trivial File Transfer Protocol (TFTP).
    c. Dynamic Host Configuration Protocol (DHCP).
    d. Simple Network Management Protocol (SNMP).

69. (032) In what octet of an Internet Protocol (IP) address can you identify the class of the address?
    a. Registry.
    b. Second.
    c. Third.
    d. First.

70. (032) Internet Protocol Version 6 (IPv6) addresses are how much larger than Internet Protocol Version 4 (IPv4) addresses?
    a. Twice as large.
    b. Six times larger.
    c. Four times larger.
    d. Three times larger.

71. (032) What are the three types of Internet Protocol Version 6 (IPv6) addresses?
    a. Anycast, dualcast, and unicast.
    b. Unicast, multicast, and anycast.
    c. Anycast, dualcast, and singlecast.
    d. Unicast, manycast, and universalcast.

72. (033) When a client computer initiates contact with a server, what does it use to request a particular service?
    a. Port numbers.
    b. Web browser.
    c. Hybrid stacks.
    d. Physical topologies.

73. (034) What network type is essentially a private Internet for a company or organization?
    a. Intranet.
    b. Extranet.
    c. Bus topology.
    d. Hybrid topology.

74. (034) What are Intranets that share a portion of their content with customers, suppliers, or other businesses, but *not* with the public?
    a. Subnet mask.
    b. Extranets.
    c. Arpanets.
    d. Dualnet.

75. (035) A wide area network (WAN) connects networks that are typically separated by
    a. firewalls.
    b. different languages.
    c. geographical distances.
    d. different network topologies.

76. (036) What network topology consists of devices connected to a common or shared cable?
    a. Bus.
    b. Star.
    c. Scale.
    d. Dual ring.

77. (036) What network topology consists of cabling segments from each computer connecting to a centralized component?
    a. Bus.
    b. Star.
    c. Scale.
    d. Dual ring.

78. (036) In what network topology does each workstation act as a repeater for a transmission?
    a. Bus.
    b. Car.
    c. Star.
    d. Ring.

79. (037) What device modulates signals to encode digital information and demodulates signals to decode the transmitted information?
    a. Bridge.
    b. Router.
    c. Switch.
    d. Modem.

80. (038) What device logically separates a single network into multiple segments or collision domains in Ethernet networks?
    a. Bridge.
    b. Router.
    c. Switch.
    d. Modem.

81. (039) If a router does *not* know how to forward a packet, what does it do?
    a. Drops the packet.
    b. Retransmits the packet.
    c. Returns the packet to the originator.
    d. Switches the address to a known good address.

82. (039) In what routing method does a network administrator program a router to use specific paths between nodes?
    a. Dynamic.
    b. Default.
    c. Admin.
    d. Static.

83. (040) What term *best* describes when a sender locks transmitted information down with a secret combination, or key, and the receiver can unlock the information assuming they have the same key?
    a. Key defense.
    b. Cryptology.
    c. Encryption.
    d. Algorithm.

84. (041) What could happen if you used the wrong type of radio-guide (RG) cable?
    a. The nominal impedance of the connected equipment will decrease.
    b. The nominal impedance of the connected equipment will increase.
    c. Decreased electromagnetic interference (EMI) impedance.
    d. Equipment damage and or system failure.

85. (041) What is the most common standard used for wireless networking?
    a. Laser links.
    b. Infrared links.
    c. Institute of Electrical Electronics Engineers (IEEE) 801.22.
    d. Institute of Electrical Electronics Engineers (IEEE) 802.11.

# Student Notes

# Glossary of Abbreviations and Acronyms

| | |
|---|---|
| **µm** | micron |
| **A&FRC** | Airman & Family Readiness Center |
| **AAD** | Airman Advancement Division |
| **ACK** | acknowledgement |
| **ACP** | allied communication publication |
| **ACS** | air control squadron |
| **ADX** | aeronautical data exchange |
| **AEF** | air and space expeditionary force |
| **AETC** | Air Education and Training Command |
| **AFCFM** | Air Force career field manager |
| **AFDD** | Air Force doctrine document |
| **AFDPO** | Air Force Departmental Publishing Office |
| **AFE** | aircrew flight equipment flight |
| **AFEMS** | Air Force Equipment Management System |
| **AFETS** | Air Force Engineering and Technical Services |
| **AFFSA** | Air Force Flight Standards Agency |
| **AFI** | Air Force instruction |
| **AFIS** | Air Force Inspection System |
| **AFJQS** | Air Force Job Qualification Standard |
| **AFMAN** | Air Force manual |
| **AFMQCC** | Air Force maintenance quality control checklist |
| **AFMSI** | Air Force maintenance special instructions |
| **AFN** | American Forces Network |
| **AFOSH** | Air Force Occupational Safety and Health |
| **AFPAM** | Air Force pamphlet |
| **AFPC** | Air Force Personnel Center |
| **AFPD** | Air Force policy directive |
| **AFQTP** | Air Force Qualification Training Package |
| **AFR** | Air Force Reserve |
| **AFS** | Air Force specialty |
| **AFSC** | Air Force specialty code |
| **AFSNCOA** | Air Force Senior Noncommissioned Officer Academy |
| **AFTO** | Air Force technical order |
| **AFVA** | Air Force visual aid |

| | |
|---|---|
| **AGP** | Accelerated Graphics Port |
| **AIS** | automated information system |
| **AIX** | Advanced Interactive eXecutive |
| **ALE** | Advanced Leadership Experience |
| **ALS** | Airman Leadership School |
| **ANG** | Air National Guard |
| **ANSI** | American National Standard Institute |
| **AOCI** | Airfield Operations Compliance Inspection |
| **ARC** | Air Reserve Component |
| **ARPA** | Advanced Research Projects Agency |
| **ARPANET** | Advanced Research Projects Agency Network |
| **ART** | Air and Space Expeditionary Force Reporting Tool |
| **ASC** | Allowance Source Code |
| **ASCII** | American Standardized Code for Information Interchange |
| **ASSIST** | Acquisition Streamlining Standardization Information System |
| **AT** | action taken |
| **ATA** | Advanced Technology Attachment |
| **ATAPI** | Advanced Technology Attachment Packet Interface |
| **ATC** | air traffic control |
| **ATCS** | air traffic control squadron |
| **ATM** | air traffic management |
| **BE** | bioenvironmental engineering |
| **BFM** | base functional manager |
| **BIOS** | basic input/output system |
| **bit** | binary digit |
| **BMTS** | Basic Military Training School |
| **BNC** | Bayonet Neil-Coleman |
| **BOEWG** | Bioenvironmental Occupational and Environmental Working Group |
| **C2** | command and control |
| **$C^2$** | in-compliance |
| **C3** | command, control, and communications |
| **C4I** | command, control, communications, computer, and intelligence |
| **CAA** | career assistance advisor |
| **CAGE** | Commercial and Government Entity |
| **CAMS** | Core Automated Maintenance System |
| **CBRN** | chemical, biological, radiological, nuclear |

| | |
|---|---|
| **CCAF** | Community College of the Air Force |
| **CCIP** | Commander's Inspection Program |
| **CDC** | career development course |
| **CDE** | corrected-during-evaluation |
| **CD-ROM** | compact disc-read only memory |
| **CD-RW** | compact disc-rewriteable |
| **CEIG** | cyberspace engineering installation group |
| **CEM** | chief enlisted manager |
| **CEMS** | Comprehensive Engine Management System |
| **CFETP** | Career Field Education and Training Plan |
| **CFR** | Code of Federal Regulations |
| **CIDR** | Classless Inter-Domain Routing |
| **CJCS** | chairman of the Joint Chiefs of Staff |
| **CLC** | Chief Master Sergeant Leadership Course |
| **CMSgt** | chief master sergeant |
| **COI** | commercial operating instruction |
| **COMSEC** | communications security |
| **CONUS** | continental United States |
| **COTS** | commercial off-the-shelf |
| **CPR** | cardiopulmonary resuscitation |
| **CPU** | central processing unit |
| **csh** | C shell |
| **CVTO** | commercial vendor technical orders |
| **CWC** | complies-with-comments |
| **DASR** | digital air surveillance radar |
| **DATCALS** | Deployment Air Traffic Control and Landing Systems |
| **DC** | direct current |
| **DDN** | dotted decimal notation |
| **DHCP** | Dynamic Host Configuration Protocol |
| **DISA** | Defense Information Systems Agency |
| **DISN** | Defense Information Systems Network |
| **DL** | distance learning |
| **DMMTO** | depot maintenance modification technical order |
| **DNS** | Domain Name System |
| **DOD** | Department of Defense |
| **DODIN** | Department of Defense information network |

| | |
|---|---|
| **DOL** | Department of Labor |
| **DRU** | direct reporting unit |
| **DSP** | Defense Standardization Program |
| **DVD-ROM** | digital versatile disc-read only memory |
| **E&I** | engineering and installation |
| **ECIA** | Electronic Components Industry Association |
| **EE** | equipment evaluation |
| **EFR** | electromagnetic field radiation |
| **EIA** | Electronic Industries Alliance |
| **ELE** | executive-level experience |
| **EMF** | electromagnetic field |
| **EMFR** | electromagnetic field radiation |
| **EMI** | electromagnetic interference |
| **EMP** | electromagnetic pulse |
| **EMWG** | Encroachment Management Working Group |
| **EPE** | Enlisted Professional Enhancement; equipment personnel evaluation |
| **EPME** | Enlisted Professional Military Education |
| **EPMEIC** | Enlisted Professional Military Education Instructor Course |
| **ES/TCM** | equipment specialist/technical content manager |
| **ESR** | equipment status reporting |
| **ETIMS** | Enhanced Technical Information Management System |
| **eTO** | electronic technical order |
| **F** | Fahrenheit |
| **FAA** | Federal Aviation Administration |
| **FDDI** | fiber distributed data interface |
| **FOA** | field operating agency |
| **FRAGO** | fragamentary order |
| **FSC** | federal supply class |
| **FTA** | first-term Airman |
| **FTAC** | First-Term Airman Center |
| **FTP** | File Transfer Protocol |
| **Gbps** | billions of bits per second |
| **GCSS-AF** | Global Combat Support System-Air Force |
| **GCSS-D** | Global Cyber Support Systems-Dashboard |
| **GUI** | graphical user interface |
| **HAF/IM** | Headquarters Air Force Information Management |

| | |
|---|---|
| **HHQ** | higher headquarters |
| **HOI** | headquarters operating instruction |
| **HP-UX** | Hewlett Packard Unix |
| **HTTP** | HyperText Transfer Protocol |
| **I/O** | input/output |
| **IANA** | Internet Assigned Numbers Authority |
| **IBM** | International Business Machines |
| **ICT** | information and communications technology |
| **ID** | identity |
| **IDE** | Integrated Drive Electronics |
| **IEEE** | Institute of Electrical Electronics Engineers |
| **IG** | inspector general |
| **IMDS** | Integrated Maintenance Data System |
| **IN** | in-compliance |
| **IN** | intelligence flight |
| **IO** | information operations |
| **IP** | Internet Protocol |
| **IPE** | individual personnel evaluation |
| **Ipng** | Internet Protocol Next Generation |
| **IPv4** | Internet Protocol Version 4 |
| **IPv6** | Internet Protocol Version 6 |
| **IrDA** | Infrared Data Association |
| **ISEA** | International Safety Equipment Association |
| **ISN** | initial sequence number |
| **ISO** | International Organization for Standardization |
| **IT** | information technology |
| **ITPS** | identifying technical publication sheet |
| **JDD** | job data documentation |
| **JETDS** | Joint Electronics Type Designation System |
| **JP** | joint publications |
| **JQS** | job qualification standard |
| **ksh** | Korn shell |
| **LAN** | local area network |
| **laser** | light amplication stimulated emission radiation |
| **lb.** | pound |
| **LC** | lead command |

| | |
|---|---|
| **LCD** | liquid crystal display |
| **LCQCC** | Local Quality Control Checklist |
| **LCSM** | lead command system manager |
| **LED** | light-emitting diode |
| **LIMS EV** | Logistics Installations and Mission Support-Enterprise View |
| **LMR** | land mobile radio |
| **LOAP** | list of applicable publications |
| **MAC** | media access control |
| **MAJCOM** | major command |
| **MAJCOM FM** | major command functional manager |
| **MAN** | metropolitan area network |
| **Mbps** | megabits per second |
| **MFM** | major command functional manager |
| **MICT** | Management Internal Control Toolset |
| **MIL-DTL** | military detail |
| **MIL-HDBK** | military handbook |
| **MIL-PRF** | military performance |
| **MIL-SPEC** | military specification |
| **MIL-STD** | military standards |
| **MISCAP** | mission capability |
| **MOA** | memorandum of agreement |
| **modem** | modulator/demodulator |
| **MPE** | maximum permissible exposure |
| **mph** | miles per hour |
| **MRT** | Mitigation Response Team |
| **mux** | multiplexer |
| **NAS** | National Airspace System |
| **NATO** | North Atlantic Treaty Organization |
| **NCO** | noncommissioned officer |
| **NCOA** | Noncommissioned Officer Academy |
| **NCOIC** | noncommissioned officer in charge |
| **NCOPE** | Noncommissioned Officer Professional Enhancement |
| **NIC** | not in compliance |
| **NOTAM** | notice to Airmen |
| **NSA** | National Security Agency |
| **NWS** | National Weather Service |

| | |
|---|---|
| **OAD** | Occupational Analysis Division |
| **OCONS** | outside the continental United States |
| **OE/AAA** | obstruction evaluation/airport airspace analysis |
| **OEH** | occupational and environmental health |
| **OI** | operating instruction |
| **OLK** | Operating Location Kilo |
| **OPR** | office of primary responsibility |
| **OS** | operating system |
| **OSA** | airfield operations flight |
| **OSD** | Office of the Secretary of Defense |
| **OSHA** | Occupational Safety and Health Administration |
| **OSI** | Open Systems Interconnect |
| **OSK** | weapons and tactics flight |
| **OSO** | current operations flight |
| **OSS** | operations support squadron |
| **OSW** | weather flight |
| **PAR** | precision approach radar |
| **PC** | personal computer |
| **PCI** | Peripheral Component Interconnect |
| **PE** | personnel evaluation |
| **PED** | personal equipment device |
| **PFAS** | personal fall arrest system |
| **PIWG** | Product Improvement Working Group |
| **PL** | priority level |
| **PME** | Professional Military Education |
| **PMI** | preventative maintenance inspection |
| **PMO** | program management office |
| **POC** | point of contact |
| **PPE** | personal protective equipment |
| **psig** | pounds per square inch, gauge |
| **PT** | physical training |
| **QA** | quality assurance |
| **QAR** | quality assurance representative |
| **Q-flight** | Qualification Training Flight |
| **RAM** | random access memory |
| **RAWS** | Radar, Airfield & Weather Systems |

| | |
|---|---|
| **RFI** | radio frequency interference |
| **RG** | radio-guide |
| **RMC** | regional maintenance center |
| **RMS** | root mean square |
| **ROM** | read-only memory |
| **SAC** | self-assessment communicator |
| **SAF** | secretary of the Air Force |
| **SATA** | Serial Advanced Technology Attachment |
| **SBLC** | Standard Base-Level Computer |
| **SCSI** | small computer system interface |
| **SCT** | specialized communications team |
| **SEE** | special equipment evaluation |
| **SII** | special interest item |
| **SIPTO** | standard installation practices technical order |
| **SKL** | simple key loader |
| **SKT** | specialty knowledge tests |
| **SME** | subject matter expert; secure mobile environment |
| **SMT** | specialized maintenance team |
| **SMTP** | Simple Mail Transfer Protocol |
| **SNCO** | senior noncommissioned officer |
| **SNCOPE** | Senior Noncommissioned Officer Professional Enhancement |
| **SNMP** | Simple Network Management Protocol |
| **SOH** | safety and occupational health |
| **SORTS** | Status of Resources and Training System |
| **SPE** | special personnel evaluation |
| **SPF** | sun-protection-factor |
| **SPO** | system program office |
| **SrA** | senior Airman |
| **STARS** | Standard Terminal Automation Replacement System |
| **STRT** | Specialty Training Requirements Team |
| **STS** | specialty training standard |
| **SWIM** | system wide information management |
| **TACAN** | Tactical Air Navigation System |
| **TAG** | Training Advisory Group |
| **TBA** | Training Business Area |
| **TCP** | Transmission Control Protocol |

| | |
|---|---|
| **TCTO** | time compliance technical order |
| **TFTP** | Trivial File Transfer Protocol |
| **TIA** | Telecommunications Industry Association |
| **TO** | technical order |
| **TODO** | technical order distribution office |
| **TOMA** | Technical Order Management Agency |
| **TV** | television |
| **U&TW** | Utilization and Training Workshop |
| **UAV** | unmanned aerial vehicle |
| **UDP** | User Datagram Protocol |
| **UEI** | unit effectiveness inspection |
| **US** | United States |
| **USAF** | United States Air Force |
| **USB** | Universal Serial Bus |
| **UTC** | unit type code |
| **UTCEE** | unit type code equipment evaluation |
| **UTCPE** | unit type code personnel evaluation |
| **UTM** | unit training manager |
| **VOTS** | vendor off-the-shelf |
| **WAN** | wide area network |
| **WD** | when discovered |
| **WLAN** | wireless local area network |
| **WS** | weather squadron |
| **WSR** | Weapons System Review |
| **WUC** | work unit code |
| **WW** | weather wing |
| **WXG** | weather group |

# Student Notes

# Student Notes

**AFSC 1C853**
**1C853A 01 1903**
**Edit Code 01**