CHAPTER ONE

COURSE ORIENTATION AND INTRODUCTION

COURSE OVERVIEW AND ADMINISTRATION

INFORMATION

Your course material consists of a textbook, workbook and commercial material. The course is composed of two blocks. Block one mainly consists of lecture with computer based training (CBT) to supplement some of the lectured material. Topics of discussion will include but not limited to the following: career field, communication systems, circuit actions and network technologies. Block two is primarily multiple hands-on labs with lecture complimenting the labs. You will be required to design and implement a network. Incorporate a network management system into the network and discuss security procedures and tools. The amount of information covered each day may vary depending on how well the class performs. This is a group-paced course requiring approximately twenty academic days.

Chain Of Command

The chain of command is a system designed to resolve problems at the lowest possible level. In most cases, you should start with your supervisor as the lowest level. If your supervisor cannot help you, then continue up the chain. Using the chain of command effectively includes allowing each link in the chain to do all they can and respond to your issue before going further up the chain. You should never jump to the top of the chain or "shotgun" to multiple parts of the chain.

While in training, your chain of command starts with your class leader. If they cannot help you, in order, contact your instructor, instructor supervisor, flight chief and then the First Sergeant.

Training Policies and Student Behavior

The following training policies affect all students and are provided for your reference. This information will help you to succeed as a student and as a member of the Air Force.

Breaks. Break times are posted in each classroom.

Smoking. In accordance with AFI 40-102, Tobacco Use in the Air Force, students are prohibited "…from using tobacco in any professional military education (PME) or formal training school, during school duty hours…."

Casinos. Over the last decade, Biloxi has become home to a number of gambling establishments. Casinos have the potential to get anyone in trouble…especially students in training. Keep in mind only people 21 and older are allowed into the casinos. Wearing the uniform into a casino is NOT permitted for any students. The only exception to this rule is for prior-service personnel who wish to visit a buffet for lunch or dinner. If you opt to go to a buffet, you must go directly to the buffet and may not gamble while at the facility. If you think you may have a gambling problem, help is available through the Family Support Center. Also, beware of the risks of drinking alcoholic beverages at the casinos. Buy a Home Free card or use any of the previously suggested methods to get home if you have been drinking.

Driving Under The Influence (DUI)

Driving Under the Influence (DUI) is prohibited on any Air Force installation. DUI is punishable in several different ways according to base regulations. Suspension of driving privileges, an Article 15 and even dishonorable discharge are a few ways of DUI punishment.

Keesler AFB has initiated a Home Free Program. At Keesler, a Home Free ticket can be purchased from any First Sergeant for $10. The purpose of a Home Free ticket is to provide last minute transportation in case you have something to drink and need a ride home. If you have a Home Free ticket, you can call the cab company listed on the ticket and they will pick you up and take you home anywhere from Highway 49 (Gulfport) to Highway 57 (Gautier). Other alternatives to driving drunk are taking a bus, another taxi or calling a friend for a ride.

Elimination from Training

If you are eliminated from this course for any reason, you will eventually be sent to the Outbound Assignments Section of the Military Personnel Flight (MPF) for further actions. Reasons for elimination include multiple test or progress check failures, major medical problems or conduct incompatible with Air Force standards. Paperwork for elimination is started at the lowest level and is passed up the chain of command to the squadron or group commander, who makes the final decision.

Appointments

Schedule all appointments for times when you are not in class. If there is no way to reschedule your appointment, inform your instructor before the appointment and try to keep the appointment as short as possible. Go directly to and from your appointment.

Graduation Date

Do not make non-refundable travel plans based on your scheduled graduation date. Graduation dates have been changed for many different reasons; these reasons include hurricanes, health or personal problems, etc.

Absent Without Leave

Absent Without Official Leave (AWOL) can permanently harm your military career. If you are going to miss class for any reason, make sure the staff of this course is aware of your situation. Contact your instructor, course management or the First Sergeant. If you have a medical emergency and are in the hospital or dental clinic, you should take the responsibility of telling them you are a student and ask them to contact the proper people for you.

SEXUAL HARASSMENT, PROFESSIONAL RELATIONSHIPS, AND HAZING

Sexual harassment is discrimination that involves unwelcome sexual advances, requests or sexual favors and other verbal or physical conduct of a sexual nature. This includes touching, talking or whistling. The base and squadron commanders have executed a zero tolerance policy on any hazing or sexual harassment. Students found guilty of sexual harassment may undergo courts-martial and would be punished accordingly.

Along with a zero tolerance for sexual harassment, the commanders have also provided a zero tolerance on unprofessional relationships in the training environment. This policy means there is to be no faculty-trainee relationships. Faculty and staff will not solicit gifts from students or accept unsolicited gifts. The staff appreciates the gesture; however, we also appreciate our paychecks! Unprofessional relationships also include the potential relationships between prior service and non-prior service students.

TYPES AND USES OF INSTRUCTIONAL MATERIAL

Student Text

The *student text* is reading material that will help you achieve course objectives. You will be required to return your student text to your instructor before taking the end of course test. Please do not write, highlight or otherwise mark in your student textbook. Take care of the textbook as if it was your own personal book. Any misuse or abuse of the textbook will be addressed promptly and if found at fault, you will be responsible for repairing the damage. Normal wear and tear is not considered misuse or abuse.

Student Workbook

The *student workbook* provides practical work, the application of procedures and problem-solving exercises. It contains questions for you to answer throughout the duration of the block. The questions coincide with the student textbook and lecture; therefore, when you are assigned a textbook section to read, you should also complete any workbook questions for that section. Completion of the workbook is not optional—it is mandatory.

Commercial Material

The *commercial material* used in this course is the Internetworking Technologies Handbook 3rd Ed. published by Cisco. This will be used much like the student textbook except you will not be allowed to write in or keep these books. Please take care of these books or you could be asked to replace a book if found liable for its damage.

INSTRUCTIONAL METHODS

Lecture/Discussion

The *lecture/discussion* instructional method involves an instructor-led lecture and discussion. Your participation in the discussion process is highly encouraged. As a matter of fact, instructors welcome questions and participation.

Demonstration/Performance

The *demonstration/performance* instructional method involves an instructor-led, step-by-step, demonstration of a procedure (i.e., equipment configuration). Students are provided an opportunity to practice the procedures. Oftentimes, student mastery of the skill or skills is measured.

TESTING AND GRADING PROCEDURES

Appraisals

Appraisals are a measurement device comprised of a group of questions and/or projects used to check the day-to-day learning process. Appraisals are used informally to help determine student comprehension and progress. These do not figure into your course average, but are used as a measurement tool for both you and the instructor. Any failure of an appraisal could warrant student-individualized assistance (SIA).

Progress Checks

Progress checks aid in the assessment of student accomplishment of knowledge or performance objectives during the time allocated for classroom or laboratory instruction. Progress checks provide immediate feedback to the student and instructor.

To satisfactorily complete the course, you must pass all progress checks. A progress check may be a written test of your knowledge or a performance check of your knowledge of procedures.

Progress checks are not considered in the calculation of your end of course grade. Unlike appraisals, they are graded with either a satisfactory (SAT) or unsatisfactory (UNSAT). If you receive an UNSAT on your first attempt at a progress check, you will be given a second progress check of a similar nature. Failure to pass two progress checks pertaining to the same objective is grounds for an academic wash-back or elimination.

Block Tests

There will be two tests in this course. Each test will be administered after completion of each block. This test will cover information presented to you throughout the block of instruction. Tests are used to evaluate your retention of information presented throughout this course. You must score at least 70% to pass the test.

EFFECTIVE STUDY TECHNIQUES

In your study, you may encounter material and ideas that are unfamiliar and at times, complex. You probably will not have trouble understanding the subject matter if you follow two important guidelines: pay attention to your instructor in class and spend your out of class time effectively.

It may be that you have just left a formal school environment and will have little trouble reactivating old study techniques; however, if you have never developed effective and satisfactory study methods, we provide the following suggestions.

Carefully choose a time and place for your study. Freedom from distractions is most important. Select somewhere where you can avoid bothersome friends, telephone calls and self-made distractions, such as radio or television. Other factors you should consider are ventilation, room temperature and lighting. One more point, studying in bed does not work! Find a desk and a chair where you'll be comfortable, but not so comfortable that you will fall asleep.

There is no guaranteed effective plan for studying, but there is a systematic approach that has been effective for many students. This is the "SQ3R" method of planned study. SQ3R stands for survey, question, read, recite, review. Let's examine the SQ3R methods more closely.

Survey. This means take a brief glance at what you are going to study. Look for topic and subtopic headings, key paragraphs and terms or words in italics, boldface print or underlined. The survey step shows you where you are going and gives you an objective.

Question. In this step, ask yourself the questions provided by the author at the end of a chapter or subdivision. Most importantly, keep the questions in mind while you study. Often the answers will seem to pop out at you while you read.

Read. This does not mean just passing your eyes over the words. It means reacting to the printed material. This is an active search for questions you asked yourself about a particular subject. It also includes taking notes and making outlines.

Recite. After you have finished a paragraph, topic or chapter, stop reading and in your own words, answer the questions you asked yourself about the subject. This step is where the most learning takes place.

Review. When you complete the assignment, look over the notes that you made and get an overall view of the material covered and the relationship of one part to another. This way you should recognize points that need more study.

This is the SQ3R method of study. It does get results! Though it may seem lengthy, there is no secret formula to make you study well. You must take the responsibility and have the initiative to work for results. Personal motivation is critical. If you know exactly what you want to get from your studying and are interested in learning, success will be your reward.

BENEFITS AND CREDITS AWARDED BY CCAF

A Community College of the Air Force (CCAF) degree is equivalent to an Associate of Applied Science degree. The Southern Association of Colleges accredits CCAF. Award of a CCAF degree requires the accumulation of 64 semester (credit) hours.

The Air Force is the only branch of service that has degree awarding technical schools. Successful completion of the Communications-Computer Systems Control Craftsman course earns students seven credit hours in the technical area.

AIR FORCE FRAUD, WASTE AND ABUSE PREVENTION AND DETECTION

Fraud, waste and abuse concern all military members. If you see it, report it. It's as simple as that. FW&A incidents are not to be tolerated. Fraud is a deliberate deception practiced as to ensure unlawful gains. Waste is defined as the use, consuming and expending of resources carelessly or thoughtlessly. Abuse is defined as the wrongful use of resources.

CONSERVATION OF TRAINING MATERIALS, RESOURCES AND ENERGY

Providing quality training is a very costly operation. Consequently, conservation programs exist to ensure responsible use of our resources. You can help our effort by being energy conscious at all times. When all persons leave the classroom for more than five minutes be sure to turn off the lights. Another way in which energy is lost is through the inefficient operation of lighting. If you see a bulb flicker, report it to the instructor. Lastly, insure all exterior doors are closed behind you when you enter or exit the building.

SAFETY IN THE TRAINING ENVIRONMENT

Every student deserves a safe environment as defined by the AF Occupational Safety and Health (AFOSH) Standards. Additionally, every student has an obligation to report hazards and mishaps as promptly as possible.

- A *mishap* is defined as an accident that results in death, injury or occupational illness to an employee or damage to DOD equipment.

- A *hazard* is any environmental condition that will likely cause a mishap.

Reporting Mishaps and Hazards

During duty hours, report all mishaps and/or hazards to your instructor or squadron orderly room staff. After normal duty hours, notify the Base Command Post (or simply call the operator and ask them to patch you through). Then inform the instructor on the next duty day.

If you don't feel appropriate action was taken on a particular hazard, you may submit AF Form 457, *Hazard Report*, directly to Center Safety.

Fire Safety

Make sure your instructor shows you the nearest emergency egress route and at least the "next best" route from your classroom. There are fire alarms on the wall at all exits. If you detect a fire, evacuate and pull one of the alarm switches on the way out. If a fire alarm is activated, all students must evacuate the building in an orderly fashion and remain outside until further advised.

If your computer equipment starts smoking and catches fire, unplug it and get a HALON fire extinguisher if available. After extinguishing the fire, leave the room and notify the staff immediately. If you cannot put the fire out in a timely manner, evacuate and activate a fire alarm on the way out.

Operational Risk Management

The risk management process is a continuous, sequential methodology consisting of steps that define the logical decision-making process. For many, risk management is based on years of experience; for others it is intuitive. In short:

Know the Risks. Risks are often derived from experience and are easily identified and controlled when identified early in the planning process.

Don't accept unnecessary risks. Take only those risks that are required to accomplish the mission.

Make risk decisions at the proper level. Risk decisions are normally made by the leader directly responsible for the operation. However, when the leader determines that the risk associated with the operation is too high or appears to violate the stated intent of higher authorities, leaders must elevate the risk decision to the appropriate level.

Accept risks if benefits outweigh costs. Risk is inherent in virtually all operations. Risk is also related to gain; normally greater potential gain requires greater risk. Risk management does not seek to "eliminate all risk", but to "manage risk" accomplishing the mission with a minimum loss.

FORCE PROTECTION CONDITION

Because of the potential wartime situations the military is placed in, it is necessary to be prepared for such events. We call the preparation process for these events "force protection conditions" or simply FPCON.

There are five different FPCON levels: Normal, Alpha, Bravo, Charlie and Delta.

- FPCON NORMAL is the condition that applies when there is a general threat of possible terrorist activity, but only warrants a routine security posture.

- During FPCON ALPHA, security is enforced more than normal, signs posted at facility entry points with current FPCON indications, buildings and rooms are surveyed for suspicious people or packages, buildings or rooms not typically in use are locked, random ID checks are performed at entry gates and facility entrances.

- During FPCON BRAVO, all steps from Alpha continued, possible contact via the pyramid telephone recall, only one entrance into a facility, ID checks at entrance to facilities, brief family members on FPCON and encourage their security, buildings or rooms not typically in use are inspected regularly, packages and letters inspected thoroughly at Post Office and delivery points, vehicles and objects are to be moved at least 25 meters from buildings.

- During FPCON CHARLIE, all security measures from Alpha and Bravo continued, Keesler flightlines close, vehicles randomly inspected for contraband, identification will be checked for all personnel entering the base, wear of military clothing off base will be restricted, possible curfew implementation.

- During FPCON DELTA, all security measures from Alpha, Bravo and Charlie continued, all vehicles and belongings of individuals will be inspected before entering the base, all areas where large groups may gather will be closed, i.e. exchanges and commissary, visitors to base will be limited to those who are mission essential and work hours will also be staggered.

HURRICANE CONDITION

Hurricane Conditions (HURCON) are indications that a hurricane is threatening coastal and inland areas. A hurricane is any tropical storm that has winds above 74 miles per hour. They are storms with heavy rainfall and often spawn tornadoes. HURCON warnings will be posted at entrance points to all facilities. They will be categorized as HURCON 1, 2, 3 or 4 depending on the speed and distance of the hurricane.

Evacuation Procedures

During the months of June through November, TDY personnel will be asked to fill out KAFB Form 21, *Sheltering Intentions*. This is to inform the administration of where you will be located in the event a hurricane makes landfall in our area. You may evacuate off base up to 500 miles away. You must have a point of contact for administration to reach you if this is your intention. You may also evacuate to the on base shelter (Thomson Hall). No matter what your intentions are, be prepared. You should have bottled water and non-perishable food to eat while you are evacuated. Remember the electricity is likely to go out so candles may be necessary. Also, the water may be contaminated so there will be little use of the faucets in the shelter.

ENVIRONMENTAL ISSUES

Environmental education is designed to make us realize resources cannot be managed irresponsibly. The Air Force Environmental Quality Program has four disciplines: *cleanup*, *compliance*, *conservation* and *pollution prevention*.

Cleanup. Helping to clean up the area can involve many methods. We should always ensure environmental repairs are performed when the damage is caused by Air Force operations. However, a simpler method for most people to participate in would be the base and community cleanup efforts. People pick up garbage and help beautify the area. Some people plant trees or flowers, while others may clear the beach of debris.

Compliance. This environmental issue is self-explanatory. You should always obey federal, state and local (including foreign) laws. Those people who are hunters need to follow proper channels in getting their license and only hunt during the proper season. You should also make yourself aware of any endangered species to ensure you do not damage their habitat during your adventures.

Conservation. In the back of each classroom, you will notice two garbage cans. One is for regular garbage and the other should only be used for recycling efforts. You should continue recycling even when off duty. You should also try to conserve gas by carpooling when possible. Turn off lights when they are not in use. When attempting to conserve natural resources, just keep in mind all the rules your parents probably told you when you were growing up, "Close the door, we are not trying to air condition the back yard!"

Pollution Prevention. You should reduce the amount of hazardous materials used in the work place and at home. Again, try to carpool when you can. Remember the rules of changing your oil and make sure you dispose of old oil properly. Make sure you dispose of anything containing chemicals in a proper manner. This even includes the smallest batteries, which you will encounter in a computer.

AIR FORCE CORE VALUES

Always keep in mind:

- Integrity First
- Service before Self
- Excellence in All We Do

STUDENT FEEDBACK PROGRAM

The student feedback program is designed to give students a healthy way to voice personal opinions or observations on areas such as training, the classroom environment or

base support facilities. Use AETC Form 736, *Student Feedback*, as the vehicle for submitting student feedback. Forms are conspicuously posted on each classroom's bulletin board. If you need help filling out the form, ask your instructor for assistance.

Students may drop off their feedback forms in our flight commander's suggestion box or return them to the instructor or instructor supervisor. The suggestion box is located on the wall near room 123.

SUMMARY

During your orientation, you learned many things about the way technical training is performed here at Keesler Air Force Base and about some of the policies and procedures that might affect you during your stay here. If you have any questions about this course that have not been answered during orientation, bring them to the attention of the instructor.

CHAPTER TWO

CAREER FIELD OVERVIEW

OBJECTIVES

2a. Identify general principles pertaining to the structure of and progression within the 3C2X1 career field.

2b. Describe the relationship between duties, responsibilities, and qualifications of the 3C2X1 Air Force Specialty Code (AFSC).

INTRODUCTION

In this unit, we will cover the structure of the 3C2X1 Communications-Computer Systems (C-CS) Control career field and the duties related to being a "Tech Controller". This unit endeavors to provide clear insight into how you will fit into this puzzle of many pieces called the U.S. Air Force. Remember each piece plays an important role in the "Big Picture," and you should never take your responsibilities lightly. Let's begin with a close look at our Air Force Specialty Code (AFSC).

CAREER FIELD PROGRESSION

INFORMATION

Objective 2a: Identify general principles pertaining to the structure of and progression within the 3C2X1 career field.

AIR FORCE SPECIALTY CODE (AFSC) STRUCTURE

It is essential everyone involved in the C-CS control career field does their part to plan, develop, manage, conduct and evaluate an effective training program. Adequate training and timely progression from apprentice to superintendent skill levels play an important role in the Air Force's ability to accomplish its mission. The guidance provided in the Career Field Education Training Plan (CFETP) will ensure individuals receive viable training at appropriate career points. Table 2-1 illustrates the breakdown of the 3C2X1 AFSC.

Item	Description
3C2X1	The first character (numeric) in an AFSC denotes a ***career group***. A career group is a functional grouping of related disciplines. There are currently nine career groups defined. The closer to "1" a career group is, the more directly it supports our war fighting operations.
3C2X1	The second character (alpha), when combined with the career group, identifies a ***career field***. A career field is a group of closely related specialties requiring basically the same knowledge and skills.
3C2X1	The third character (numeric), when combined with the career field, identifies a ***career field subdivision***. A career field subdivision is a division of a career field that groups closely related specialties in one or more career ladders.
3C2**X**1	The fourth character (numeric), denotes the ***skill level***. There are currently six skill levels (1, 3, 5, 7, 9, and 0) defined.
3C2X1	Fifth character (numeric), when combined with the first four, denotes an Air Force Specialty Code (i.e., a specific job).

Table 2-1. 3C2X1 AFSC Breakdown.

Administrative AFSCs

There are three types of AFSCs that apply to you for administrative purposes: *primary (PAFSC)*, *duty (DAFSC)* and *control (CAFSC)*.

PAFSC. The PAFSC denotes the AFSC in which an individual is best qualified to perform duty.

DAFSC. The DAFSC denotes the specialty in which an individual is performing duty.

CAFSC. The CAFSC is a management tool used to make airman assignments, to assist in determining training requirements and to consider individuals for promotion.

It's possible for all three AFSCs to be different. For example a 7-level TSgt instructor in the basic 3-level course can have a PAFSC of T3C271, a DAFSC of T3C251, and a CAFSC of 3C271.

Skill Levels

A *skill level* is a level of qualification within an awarded AFS, as shown by the fourth digit of the AFSC. There are five skill levels commonly used.

- The ***1-level*** (*Helper*) identifies personnel initially classified in an AFS when

entering the Air Force or when retraining.

- The ***3-level*** (*Apprentice*) identifies airmen who have obtained basic knowledge within an AFSC through completion of an initial skills course. Apprentices gain duty position experience and, upon completion, enter a structured apprenticeship program to gain qualification and experience required of a 5-level (*Journeyman*). Apprentices implement work activities as directed and perform tasks unsupervised when certifying officials determine them to be qualified.

- The ***5-level*** (*Journeyman*) identifies airmen who, through experience and training, have demonstrated skilled proficiency in their AFSC. Journeymen continue to gain experience and qualification in their AFSC and, upon promotion to staff sergeant, enter a structured training program to gain experience and qualification required of a *craftsman* (7-level). Journeymen plan, coordinate, implement and supervise work activities.

- The ***7-level*** (*craftsman*) identifies airmen who have gained a high degree of technical knowledge in their AFSC and who have additionally acquired supervisory capability through training and experience. Craftsmen continue to gain experience in technical, supervisory and managerial functions. Craftsmen plan, coordinate, implement and direct work activities.

- The ***9-level*** (*superintendent*) identifies airmen who, through experience, training and performance, have shown a high degree of managerial and supervisory ability to fill positions requiring broad general (and sometimes technical) knowledge. Superintendents plan, coordinate, implement and direct a wider scope of work activities and functions.

Air Force Specialty Code Prefixes

When used, an AFSC *prefix* identifies an ability, skill, special qualification or system. Prefixes are not restricted to a single AFS. For example, an instructor in the basic 3-level course will have an AFSC of T3C2X1; an instructor in the programming course AFSC will be T3C0X2. Notice even though the AFSCs in the example differ, the T prefix is applied to both. The T prefix denotes an individual who has met requirements to be a technical training instructor.

AFSC Suffixes

When used, an AFSC ***suffix*** identifies specific equipment or functions and positions of an AFS. Each suffix has a title. For example: AFSC 2A3X2**A** identifies a F-16 Avionic Systems, Attack Control specialist; AFSC 2A3X2**B** identifies a F-16 Avionic Systems, Instrument and Flight Control specialist; and AFSC 2A3X2**C** identifies a F-16 Avionic Systems, Communication, Navigation, and Penetration Aids specialist. In these examples, the suffixes show different equipment specialties.

Special Experience Identifiers (SEIs)

SEIs are a three-character code used to identify special experience and training not otherwise identified in the personnel data system. SEIs may permit rapid identification of individuals with special qualifications to meet peacetime assignments. More importantly, they provide a means for identifying critical manning requirements during wartime or contingency operations when little lead time is available for training personnel in specific technical skills needed to support a weapon system.

As a 3C2X1, you may be assigned the duties as a system administrator and be awarded SEI 177; you may be assigned as a messaging technician for DMS and be awarded SEI 233; or you may be assigned as a COMSEC account manager and be awarded SEI 269.

For additional information about AFSC prefixes, suffixes or SEIs, consult AFMAN 36-2108, *Airman Classification*.

THE EDUCATION AND TRAINING LIFE CYCLE

The E&T life cycle is a coherent architecture that instills more standardization, rigor and discipline for all AFS E&T programs. This structure requires all airmen to complete a formal education or training course to be awarded the 3-, 7- and 9-skill levels. It also adds experience maturation periods of 15 months (9 months for retrainees) to the Upgrade Training (UGT) program of journeymen and 12 months for the craftsman. Additionally, all career fields with a 5-skill level in their AFS must use a CDC to provide journeyman knowledge training as a prerequisite for award of the 5-skill level. The E&T life cycle also defines the minimum qualifications for trainers and task certifiers and determines when airmen will attend PME.

The AFS E&T Life Cycle

A frequently asked question by 3C271 students is: “Who decides what gets taught here”? The answer to this question is YOU do! The Air Force Career Field Managers (AFCFM) utilize the inputs from the troops in the field to make the lofty decisions concerning our career field. The main form of input are the results from the Air Force Occupational

Measurement Squadron (AFOMS), which surveys occupations, analyzes resulting data, and reports findings and observations to interested managers. You probably have seen one of these surveys in your career. It is a very lengthy questionnaire on what activities you perform during normal duty. The AFCFM decide what is taught in formal training courses based on survey inputs from personnel that complete the surveys.
The Air Force E&T life cycle is implemented within each AFS through a ***Career Field Education and Training Plan*** (CFETP). Air Force Career Field Managers (AFCFM) create a CFETP for each AFS they manage, using it to standardize skill-level training requirements and establish the framework for managing career field E&T. The CFETP creates the AFS E&T life cycle by specifying the what, when, where and how of E&T within the AFS.

One of the significant functions of the CFETP in the AFS life cycle is the mandating of minimum E&T requirements. The CFETP specifies what training is required for each skill level and or duty position and what is required for initial skills, advanced, wartime technical training courses, contingency training, and exportable courses and courseware such as CDCs and Qualification Training Packages (QTP). This specific attribute establishes consistency within an AFS and ensures everyone in the AFS meets a basic set of requirements needed to perform effectively in a particular skill level or duty position. Simply put, the CFETP is the core E&T document for an AFS. Its use implements the AFS E&T life cycle and provides airmen within the specialty a cradle-to-grave view of their career field.

Skill-Level Upgrade Training

The Air Force E&T life cycle increases the rigor and discipline in skill-level UGT by mandating minimum requirements that all AFS E&T programs must meet to award the 3-, 5-, 7- and 9-skill levels.

Apprentice. All airmen attend formal 3-skill level awarding technical training. Upon graduation, supervisors make sure apprentices are entered into 5-skill level UGT once they arrive. Supervisors use the initial evaluation period to familiarize the trainee with the organization and mission and evaluate training provided in technical school.

Journeyman. Before awarding 5-skill levels, commanders ensure trainees have been in UGT for a minimum of 15 months and completed the required CDCs and all training requirements listed in the CFETP (or those identified by their supervisors on the appropriate training standards when a CFETP is not available).

Craftsman. The 7-skill level upgrade mandates a minimum time requirement for

training and completion of craftsman-level technical training, if directed by Air Staff functional managers. To be eligible for craftsman technical training (when directed by the AFCFM), trainees must complete 12 months of OJT, the required 7-skill level CDC (if applicable), and all training requirements listed in the CFETP or those identified by the supervisor when a CFETP is not available. For the award of the 7-skill level, trainees must complete 12 months in UGT.

Superintendent. The 9-skill level can be awarded to SMSgts.

Professional Military Education (PME)

All enlisted personnel are required to attend PME. Senior airmen with 48 months of time-in-service or SrA selected for promotion to SSgt will attend Airman Leadership School (ALS). ALS graduation is required to sew on the grade of SSgt. Technical sergeants and TSgt-selectees will attend the NCO Academy. Graduation from the NCO Academy is required to sew on the grade of MSgt. CMSgt-selectees, SMSgts, SMSgt-selectees, and MSgts selected to go will attend the Senior NCO Academy. Graduation from the Senior NCO Academy is required to sew on the grade of CMSgt.

Developing AFS E&T

The AFCFMs are responsible for developing and implementing E&T programs within the AFSs they manage. They use the ***Utilization and Training Workshop*** (U&TW) and the CFETP to accomplish these responsibilities.

U&TW. The U&TW is a forum convened by the AFCFM to determine the AFS E&T requirements as they apply to mission needs. In fact, the term U&TW is derived from the main purpose of this meeting: to determine what the specialty does (utilization) and how it will get its work force qualified to perform (training) the existing or new role.

The AFCFM determines the need for a U&TW based on impending changes within the AFS. AFS personnel may request a U&TW when the established E&T requirements and support materials no longer meet AFS needs. The major benefit to a U&TW is the participation and input from AFS MAJCOM and field experts. This bringing together of Air Force specialty expertise helps the AFCFM determine the most effective mix of formal training and OJT for each skill-level of the AFS, the E&T standards needed and who is responsible for providing E&T.

Specifically, the AFCFM uses the U&TW to review and revise AFS descriptions and qualification requirements, tasks required for performance, core tasks and skill-level

training requirements, formal and exportable (CDC, QTP, etc.) E&T course requirements, wartime and MAJCOM-unique requirements and, in the case of AFS mergers, any transition training requirements. The AFCFM also uses the U&TW to identify the resources available to support Air Force specialty E&T, such as instructor authorizations, training equipment, and authorizations for student training days and the means to acquire them.

CFETP. As discussed earlier, the CFETP is the core E&T standard for an AFS. The AFCFM uses the CFETP to identify E&T requirements and responsibilities; for developing, conducting, and evaluating formal training and OJT; and for implementing the decisions made during the U&TW. Included as parts of the CFETP are the ***Specialty Training Standard*** (STS) and ***Air Force Job Qualification Standard*** (AFJQS). The AFCFM is the approving official for these standards and approving authority for automating these standards.

STS. The STS is included in Part 2 of the CFETP. It lists the skills and knowledge that airmen in a particular AFS need on the job. It further serves as a contract between Air Education and Training Command and the Air Force specialty to show the overall E&T requirements for an AFS the formal schools teach. The STS is used to standardize E&T and to ensure the using command and mission-related E&T requirements are identified. It also identifies the technical references needed for UGT, QT and career knowledge training if a CDC is not available.

AFJQS. An AFJQS is a comprehensive list describing a particular job type or duty position and is included within Part 2 of the CFETP as a separate attachment of the STS. Listed on the AFJQS are the minimum common tasks airmen assigned to similar AFS duty positions, weapon systems or equipment must perform. The AFJQS provides tasks in the detail needed to support OJT and is used only when airmen are assigned to these positions. With the use of an AFJQS, upgrade training and qualification training within a specialty are standardized. AFCFMs may obtain permission to publish the AFJQS separate from the CFETP when other supporting exportable training material, such as qualification training plans, will be distributed with the AFJQS. When this occurs, the AFCFM lists the AFJQS in the OJT support material section in Part 2 of the CFETP.

SUMMARY

This objective has reviewed several fundamental concepts relating to the structure and use of an AFSC. It has also introduced you to the E&T life cycle. Armed with this

knowledge, you are now better prepared to assist your subordinates in maximizing their career progression potential.

In the next objective, we will discuss how 3C2's fit into the Air Force's "big picture."

DUTIES, RESPONSIBILITIES AND QUALIFICATIONS

OBJECTIVE

2b. Describe the relationship between duties, responsibilities, and qualifications of the 3C2X1 Air Force Specialty Code (AFSC).

INTRODUCTION

"Dominating the information spectrum is as critical to conflict now as occupying the land or controlling the air has been in the past."

Ronald R. Fogleman, Gen, USAF
Cornerstones of Information Warfare

It has been said information *is* power. In today's global communications environment, that statement could not be more accurate. The 3C2X1 career field plays a crucial role in ensuring the United States and its allies maintain information superiority during contingency operations.

We all tend to get caught up in the day-to-day grind of our jobs. Consequently, we tend to lose sight of how our job impacts the overall Air Force mission. This section serves as a reminder of what some of your responsibilities as a 3C2X1 are, and reinforces the importance of your work.

INFORMATION

THE AIR FORCE TASK LIST (AFTL)

Everyone has a stake in the Air Force mission. AFDD 1-1, *Air Force Task List (AFTL)*, is a comprehensive framework that expressed how all Air Force activities contribute to the defense of the nation and its national interests. The AFTL is based on the Air Force's core competencies. The AFTL, does not, and was never intended to capture every detail of every activity. Airmen are naturally innovative and flexible with a focus on accomplishing the objective. While the AFTL provides doctrinally correct, overarching direction on the tasks that must be done, tasks are to be expanded upon as needed by lower echelons, to fit their specific needs in describing their tasks.

So how can the AFTL help you understand your role as a 3C2X1? Take a moment to review Table 2-2 on page 2-9. Each major heading relates to one of the levels of war

defined by Air Force basic doctrine. Each sub-heading is a task defined by the Universal Joint Task List (UJTL). Like the AFTL, the UJTL is a framework for integration of all branches of service during contingency operations. Each row in the table represents an Air Force core competency. Pay particular attention to the core competency of providing information superiority. Notice anything peculiar about the relationship of information superiority to all of the UJTLs?

Information superiority is imperative at each level of war. Information superiority is not constrained by a particular task or level of war. It must exist at all levels and at all tasks. Without information superiority, our efforts during contingency will most surely fail.

AFTL Tasks in Relationship to Tactical Level of War Tasks						
	Deploy/ Conduct Maneuver	**Develop Intelligence**	**Employ Firepower**	**Perform Logistics & Combat Service Support**	**Exercise Command & Control**	**Protect the Force**
Air & Space Superiority	X	X	X			X
Precision Engagement	X	X	X	X	X	X
Information Superiority	X	X	X	X	X	X
Global Attack	X		X			X
Rapid Global Mobility	X	X	X	X		X
Agile Combat Support	X	X	X	X	X	X
Command & Control	X	X	X	X	X	X

AFTL Tasks in Relationship to Operational Level of War Tasks						
	Conduct Operational Movement & Maneuver	**Provide Operational ISR**	**Employ Operational Firepower**	**Provide Operational Support**	**Exercise Operational Command & Control**	**Provide Operational Protection**
Air & Space Superiority	X	X	X			X
Precision Engagement	X	X	X	X	X	X
Information Superiority	X	X	X	X	X	X
Global Attack	X		X			X
Rapid Global Mobility	X	X	X	X		X
Agile Combat Support	X	X	X	X	X	X
Command & Control	X	X	X	X	X	X

AFTL Tasks in Relationship to Strategic Theater Level of War Tasks								
	Deploy, Concentrate & Maneuver Theater Forces	**Develop Theater Strategic ISR**	**Employ Theater Strategic Firepower**	**Sustain Theater Forces**	**Provide Theater Strategic C2**	**Provide Theater Protection**	**Establish Theater Force Reqs & Readiness**	**Develop & Maintain Alliance & Regional Relations**
Air & Space Superiority	X	X	X			X		X
Precision Engagement	X	X	X	X	X	X	X	X
Information Superiority	X	X	X	X	X	X	X	X
Global Attack	X		X			X		X

Rapid Global Mobility	X	X	X	X		X	X	X
Agile Combat Support	X	X	X	X	X	X	X	X
Command & Control	X	X	X	X	X	X	X	X

AFTL Tasks in Relationship to Strategic National Level of War Tasks								
	Conduct Strategic Deployment & Redeployment	**Develop Strategic ISR**	**Employ Forces**	**Provide Sustainment**	**Provide Strategic Direction & Integration**	**Conduct Mobilization**	**Conduct Force Development**	**Foster Multinational & Interagency Relations**
Air & Space Superiority	X	X	X					
Precision Engagement	X	X	X	X	X	X	X	X
Information Superiority	X	X	X	X	X	X	X	X
Global Attack	X		X					
Rapid Global Mobility	X	X	X	X		X		X
Agile Combat Support	X	X	X	X	X	X	X	X
Command & Control	X	X	X	X	X	X	X	X

Table 2-2. Information Superiority Plays a Key Part in All Levels of War.

AFTL 3 Provide Information Superiority

Let's define information superiority. According to AFDD 1-2, *Air Force Glossary*, ***information superiority*** is the capability to collect, process and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.

Now that you have some idea of how important 3C2's are to the Air Force mission, let us focus on how we function day-to-day to achieve the goal of information superiority, specifically in the area of network management.

NETWORK MANAGEMENT

Network Management (NM) is crucial to providing effective, efficient, and reliable C4I information network services used in critical Department of Defense (DoD) and Air Force wartime, business and C4I processes. AFI 33-115 Vol. 1, *Network Management*, identifies the responsibilities for supporting critical communications and information networks, primarily through ***Network Control Centers*** (NCC).

The Hierarchy of Network Management

Air Force NM adheres to the Defense Information Infrastructure Control Concept (DIICC). The DIICC consists of three areas of distributed responsibility at global, regional, and local levels.
Table *2-3* identifies major responsible support activities aligned with each NM hierarchy.

Network Management	Responsible Support Activity Examples
Global Operations and Security Center (GOSC)	Global Command and Control System (GCCS) Management Center (GMC), Defense Satellite Communications System Operations Center (DSCSOC), SECRET Internet Protocol Router Network (SIPR-NET) Management Center
Regional Operations and Security Center (ROSC)	Facility Control Office (FCO), Air Force Network Operations Center (AFNOC), Air Force Information Warfare Center (AFIWC), MAJCOM Network Operations and Security Center (NOSC)
Local Control Center (LCC)	NCC, System Administrator (SA), WM Community of Interest—Medical Treatment Facility, tenant system

Table 2-3. AF Hierarchy of Network Management.

NCC Organizational Structure and Relationships

The Network Control Center (NCC) serves as the single focal point for base NM and problem resolution, and is the single logical service delivery point (SDP) for all communications traversing the base network. Communications and information services entering and exiting the base fall under the operational control of the NCC.

The NCC manages network and systems maintenance for all base users. The NCC performs network and system administration to include security, fault, configuration, performance and accounting management in their Area of Responsibility (AOR). It oversees network and system operations and manages the exchange of information through the base SDP. This includes network and systems administration operations conducted by other LCC-level network operations centers (e.g., tenant unit LCCs). The NCC cooperative team includes: network technicians who perform Help Desk (HD) and Information Protection Operations (IPO), NM, and Network Administration (NA) within the NCC, and Functional Systems Administration (FSA), Workgroup Management (WM), and Specific Area Support (SAS) external to the NCC. The NCC trains FSAs and WMs to perform their duties.

Help Desk. The HD is the base's focal point for problem resolution and is the user's primary Point of Contact (POC) for problems that WMs or FSAs cannot resolve. The HD provides a central repository for technical advice and solutions for network systems, software applications assistance, automatic data processing support, hardware exchange and repair service support. It also routes problems it cannot handle to other NCC functional areas, to the Defense Megacenters (DMC) or, if necessary, to other technical support agencies such as DISA, AFNOC and MAJCOM NOSCs. The HD determines the type of reported system problem, reports the status of problem resolution to the affected customer and maintains a historical database of problem resolution.

Network Management. NM provides proactive and reactive management of resources by monitoring and controlling the network, available bandwidth, hardware and distributed software resources. Installs and maintain routers, switches, and hubs comprising the base backbone. Maintains the NMS including system backups. Modifies switch, router, and hub configurations to ensure optimum network performance and configures Access Control Lists to grant/restrict network access to authorized users and processes. NM responds to detected security incidents, network faults (errors) and user reported outages at the time of HD referral. If NM personnel cannot resolve a customer complaint or query, the HD refers the problem to a system specialist in the specific area support function.

Information Protection Operations. IPO is a critical sub-component of the NM function that implements and enforces national, DoD, and Air Force security policies and directives. It provides proactive security functions established to assist Air Force organizations in deterring, detecting, isolating, containing, and recovering from Information System (IS) and network security intrusions. The NCC conducts IPO employing hardware and software tools to enhance the security of their networks. It installs, monitors, and directs proactive and reactive network information protection defensive measures to ensure the availability, integrity, and reliability of base networked and stand-alone information resources. It will coordinate implementation of these solutions with the HD, NM and customer representatives.

Network Administration. The network technician assigned to perform NA is assigned directly to the NCC and centrally manages various functional area LANs from the network hardware software operating systems level. Tasks include all core services provided by the NCC to the base populace. These network operators are the base experts in system administration and provide technical assistance to FSAs and WMs who provide administration support from their servers to their end-user workstations.

Functional System Administrator. A FSA is not assigned to the NCC; however,

they still take direction from the NCC. They must thoroughly understand the customer's mission, and stay completely knowledgeable of the hardware and software capabilities and limitations. The FSA's area of responsibility is from the user's terminal to the server, but does not include the network backbone infrastructure components. FSAs ensure servers, workstations, peripherals, communication devices, and software are on-line and available to support customers. NCC NAs do not operate the end-users' application software, perform data entry, perform database administration or otherwise manipulate customer data. FSAs contact the HD as necessary if they cannot resolve a problem.

Workgroup Manager. The WM is normally a duty supporting a functional community (e.g., work centers, flights, squadrons or organizations) and is the first line of help customers contact to resolve problems. WMs are usually not assigned to the NCC, though are logically an extension of the HD team. WMs take direction from the FSA and NCC. NCC direction takes precedence over FSA direction. WMs possess knowledge of hardware, software, and communications principles, and install, configure and operate client/server devices. They resolve the day-to-day administrative and technical system problems users experience and contact their FSA or HD if they cannot resolve their problem.

Specific Area Support. Specific area support is the set of specialists for resolving those classes of problems associated with the various elements of the base infrastructure that HD personnel are not trained or equipped to address. Specific area support determines if the HD has correctly classified and assigned the problem, dispatches on-site maintenance and reports results back to the HD. Specific area support is not normally assigned to the NCC; however, they are functionally accessible resources both in peacetime, and wartime, in-garrison and deployed.

SUMMARY

We have discussed an overview of our career field progression; the duties, responsibilities & qualifications that go hand in hand with your successful progression in this AFSC. In the next chapter, you will examine requirement documents and circuit action concepts.

CHAPTER THREE

CIRCUIT ACTIONS

OBJECTIVES

3a. Identify general principles pertaining to requirement documents.

3b. Identify general principles pertaining to communication systems correspondence.

REQUIREMENT DOCUMENTS

3a: Identify general principles pertaining to requirement documents.

INFORMATION

AF FORM 3215, C4 SYSTEMS REQUIREMENTS DOCUMENT (CSRD)

The next few paragraphs are going to take a closer look at the information required on an AF Form 3215. Knowing the information required on an AF Form 3215 will ensure we know what to look for on any CSRD regardless of whether it's submitted on an AF Form 3215 or not. Figure 3-1 is an example CSRD that you can reference.

The AF Form 3215 can be used to document a request for any Command, Control, Communications, and Computer (C4) system. It is used primarily to submit requests for C4I systems such as: Computer/LAN, ADPE items, cable TV, Land Mobile Radio, Initial request from users for communications requirements.

Date

The date block is filled in with the date the CSRD was accomplished.

Communications and Information Systems Officer (CSO) Control Number

The CSO control number is nothing more than a tracking number that is assigned to each CSRD that is received. Assigning a unique CSO control number to each CSRD ensures the CSRDs themselves are easy to follow as they are forwarded to other personnel and offices for action. A typical CSO control number might look like this: "AETC KEESLER 99-0021". The letters and numbers that make up the CSO control number are grouped together in a fashion that gives each grouping a specific meaning. As depicted above, all of these groups of information are combined to make up the CSO control number. In any CSO control number there are four mandatory elements. They are:

C4 SYSTEMS REQUIREMENTS DOCUMENT	DATE: 6 Jan 01	CSO CONTROL NUMBER:

REQUIREMENT TITLE:		REQUESTING AGENCY POINT OF CONTACT *(Organization, Office, Name, Grade, Telephone Number)*
PPBIS Inventory Display		81 SFS/XL MSgt Jeff DeLuke 377-4829
DATE NEEDED: 15 Jan 01	MISSION OR SYSTEM SUPPORTED: Law Enforcement/Inmate Processing	

REQUIREMENT: Require the capability to display data stored in Prisoner Personal Belongings Inventory System (PPBIS). PPBIS is a computerized database which stores information regarding the personal effects of inmates. The monitor attached to the computer which contains this system is no longer functioning therefore, we no longer have the ability to display this information or enter new data as new prisoners arrive. To continue using this system to track prisoner belongings, we must be able to display the data contained in the system.

JUSTIFICATION: AFI 51-213 (excerpt attached) mandates that we inventory the personal effects of incoming prisoners. The PPBIS is the standard system used throughout the AF to perform this function. Furthermore, the PPBIS system allows us to quickly transfer data to and from other AF bases and civilian prisons and penitentiaries. If we are unable to use this system, we will be forced to comply with the requirement through more time-consuming, manual methods and will be unable to transfer data to other facilities. The additional time spent with manual methods may cause delays in prisoner processing and may also dictate a requirement for additional manpower. Furthermore, if we cannot restore our ability to display information on this system, information regarding the personal effects of our current inmates will be unaccessable and could bring about accusations and possible legal issues.

TECHNICAL SOLUTION AND COSTING

CSO'S PROPOSED SOLUTION/ALTERNATIVES:

TECHNICAL SOLUTION AUTHORITY

THIS SOLUTION MEETS ARCHITECTURAL AND INTEROPERABILITY REQUIREMENTS *(Name, Organization, Telephone Number):*	TECHNICAL REFERENCES USED:

APPROVAL AUTHORITY

RECORDS MANAGEMENT APPROVAL AUTHORITY *(Name, Title, Organization):*		APPROVED
		DISAPPROVED
REQUESTER APPROVAL AUTHORITY *(Name, Title, Organization):*		FUNDS AVAILABLE
		UNFUNDED
		APPROVED
		DISAPPROVED
HOST BASE APPROVAL AUTHORITY *(Name, Title, Organization):*		APPROVED/FUNDED
		APPROVED/UNFUNDED
		DISAPPROVED
MAJCOM APPROVAL AUTHORITY *(Name, Title, Organization):*		APPROVE
		VALIDATE

AF FORM 3215, AUG 95 ***(EF-V5)*** *(PerFORM PRO)* PREVIOUS EDITIONS ARE OBSOLETE.

Figure 3-1. C4 Systems Requirements Document.

- ***Requiring Command.*** The MAJCOM under which the requirement is being submitted. With the exception of tenant units, the MAJCOM portion of the CSO control number will be the parent MAJCOM of the host wing.

- ***Originating Base.*** Some CSRDs may be forwarded to other bases as the technical solution is being developed. Others may be sent to the MAJCOM and perhaps even HQ USAF for approval purposes. The "originating base" portion of the CSO control number ensures the CSRDs are clearly identifiable as belonging to your base. Added to the other elements of the CSO control number, the "originating base" portion of the CSO control number adds an important element making the CSRD unique.

- ***Fiscal Year.*** Unlike the calendar year, the fiscal year begins on 1 October and ends on 30 September. The fiscal year is established for government accounting purposes. Because CSRDs usually lead to the expenditure of government funds, the fiscal year is a portion of the CSO control number. Typically, the fiscal year portion of the CSO control number is only comprised of the last two digits of the fiscal year.

- ***Sequence Number.*** The sequence number portion of the CSO control number simply indicates the order in which the CSRD itself was received from the customer within the fiscal year. For example, if today were the first day of fiscal year 2002, the first CSRD submitted to us would receive a sequence number of "001". The next CSRD submitted to us would receive a sequence number of "002". Each subsequent CSRD would receive a sequence number of one greater than the CSRD that was submitted before it. This pattern of increasing sequence numbers continues until the next fiscal year begins.

Requesting Agency Point of Contact

The person identified in this block must be someone in the requesting agency who is knowledgeable about the requirement itself. Simply put, if anyone involved in the development of the technical solution has questions concerning the information on the CSRD or requires any additional information regarding the requirement, the person identified in this block should be able to address those questions or concerns. When questions or concerns do arise, being able to contact someone who can quickly address them minimizes delays in the technical solution development process and eliminates guess work that may have to be done when someone cannot be contacted to address the questions or concerns.

Requirement Title

The requirement title block should contain a brief description of the requirement itself. Much like a headline in a newspaper, the requirement title gives the reader an idea of what the requirement is without having to read the entire document.

Date Needed

The date needed block on the AF Form 3215 should contain the date upon which the requesting agency needs their requirement fulfilled. Although this may seem like one of the easier blocks on the form to fill in, it is one that requires some thought because if the customer does not have funds available to fulfill the requirement(s) identified on the form, then the date needed block may not mean anything. Another area of consideration concerning the date needed block is consideration of the complexity of the requirement itself. Some requirements can be fulfilled very easily and very quickly while others take a significant amount of planning, coordination and time. For these reasons, the user must consider funds availability and the complexity of the requirement before entering a date in the date needed block.

Mission or System Supported

This block must be filled in with the major mission or other systems supported by the requirement. In other words, this block gives a quick indication to someone reading the form of the areas and systems involved in the requirement. For example, if the requirement title stated "Alarm system upgrade" and the "mission or system supported" block stated "Fire Safety", someone reading the form could probably put these pieces of information together to determine there are some problems with some of the fire alarms installed on the base.

Requirement

For the purposes of developing a technical solution, the "requirement" block is the most important block on the AF Form 3215. The requirement must spell out what capability is required by the requesting agency. It is very important that the requirement state the capability required and not what the requesting agency feels they need to fulfill the requirement. The requirement must be stated in **functional** terms. Functional means we need to know the function that must be accomplished NOT what the requesting agency feels is needed to accomplish the function. Another reason it is important that the requirement be stated in functional terms is because we must ensure that all architectural guidance is adhered to regardless of who develops a technical solution. If the requesting agency states their requirement in functional terms, there will be no doubt as the technical

solution is developed that the equipment and services put together as the technical solution will indeed fulfill the need.

Justification

The justification block on the AF Form 3215 contains the requesting agency's reasons behind the requirement. In other words, it spells out why it is important the requirement be fulfilled. There will be many occasions when the requesting agency does not have the funds to fulfill the requirement even after a technical solution is developed. When that occurs, their CSRD may be sent to higher levels of command so that funding might be supplied at those levels. Bear in mind that hundreds and even thousands of CSRDs are sent to higher levels of command every year by requesting agencies that do not have the funds to fulfill the requirements. The justification lets everyone (including those at higher levels of command) know just how important it is that their requirement be fulfilled. When CSRDs are sent up to higher levels of command for funding, they are compared against others that have been sent up as well. When they are compared with others, decisions are made based on the importance of one requirement compared to the importance of other requirements. Because there are simply not enough funds available to fulfill all communications requirements, the most important ones are taken care of first. Others that may not seem so important may not receive funding. For this reason, any CSRDs that are sent to higher levels of command for funding must have justifications that clearly indicate the importance of fulfilling the requirement.

When developing a justification for a requirement, the requesting agency should include any governing directives that may dictate the need for the requirement. They should also indicate what will and will not happen if the requirement is not fulfilled. The requesting agency should avoid overuse of highly technical terms that may not be understood by those making decisions concerning the importance of their requirement. Too many technical terms dilute the justification and if not understood by the decision makers, may lead to the requirement being misunderstood and not being funded. Again, the purpose of the justification block is to allow the requesting agency to paint a clear picture of why they need the requirement fulfilled and the importance of fulfilling it.

CSO's Proposed Solution/Alternatives

This block will not be filled in by the requesting agency. The individuals who develop the technical solution for the requirement will fill in this block. Once completed, all of the details necessary for fulfilling the requesting agency's requirement to include alternatives are listed in this block. These details are what is known as a "technical solution".

This Solution Meets Architectural and Interoperability Requirements

As the title of this block implies, this is where the developer of the technical solution verifies that the solution itself complies with all architectural and interoperability requirements. Here, the developer of the technical solution places his or her name organization and telephone number.

Technical References Used

This block goes hand in hand with the previous block. It lists the architectural references that were used to ensure the technical solution meets architectural and interoperability requirements. Like the previous block, this block is filled in by the individual(s) who developed the technical solution.

Records Management Approval Authority

When a communications system is to store accountable records, the CSRD and the proposed technical solution must be reviewed by information management personnel who will determine whether or not the proposed solution is suitable for the type of records being stored, transmitted or otherwise processed. After review, the reviewing official will enter his or her name, title organization and signature in the block and will annotate it as "approved" or "disapproved". If disapproved, the technical solution may need to be reaccomplished.

Requester Approval Authority

This block is completed after the technical solution is developed and after it is returned to the requesting agency. Once returned to the requesting agency, they review the technical solution to determine whether or not they "agree" with it. This may sound odd but, although we may develop a technical solution knowing it will fulfill the requesting agency's requirement, the requesting agency makes the ultimate decision as to whether they accept it or not. Perhaps the technical solutions and alternatives offered to fulfill the requirement are more costly than the requesting agency thought they might be or perhaps the technical solution offered lacks some functionality that the requesting agency was expecting but did not make clear when they submitted the CSRD. For whatever reason, the requesting agency makes the final determination of whether they will or will not expend their resources to pursue and implement the technical solution we have provided them. Whether approved or disapproved, the requesting agency fills this block with the name, title organization and signature of the person who reviewed and approved/ disapproved it. Similar to the previous block, this block is also annotated to show the approval or disapproval. Besides approval or disapproval, also annotated is whether the requesting agency has funding to pursue and implement the technical solution.

Funding issues are normally the biggest and toughest issues to overcome with just about any venture in the Air Force. If the "Requester Approval Authority" block is annotated as "approved" and "funds available", the requesting agency is ready to implement the technical solution and in most cases, immediate action can be taken to implement the solution. If the requesting agency annotates the block "approved" and "unfunded", the requesting agency does not have the funds to implement the solution. Important to note here is the requirement documented on the CSRD exists regardless of whether or not the requesting agency has the funds to implement the technical solution. Therefore, when the requesting agency approves the technical solution but does not have the funds to implement it, the requirement and technical solution is sent to the STEM-B who will add them to the C4 Systems Blueprint. The Blueprint Implementation Plan (BIP) portion of the blueprint is where we keep track of and prioritize the unfunded requirements of the base. This is done to ensure that the requirement is not forgotten and to ensure it receives due attention when competing for funding.

MAJCOM Approval Authority

This last block on the AF Form 3215 is only filled in if the host base approval authority does not have the authority to approve the amount of funds needed to fulfill the requirement or when the technical solution does not meet architectural and interoperability requirements. In some cases, the CSO may act in the capacity of the host base approval authority. If the amount of money to implement a technical solution is above a pre-set limit, the wing commander may act in this capacity. Restrictions apply to individuals who are authorized to expend funds to implement technical solutions. For example, a CSO may only be authorized to approve technical solutions costing less than $10,000. If the technical solution costs more than $10,000 to implement, it may have to be forwarded to the wing commander for approval. If implementing the technical solution costs more than even the wing commander can approve, it must be further forwarded to the MAJCOM to obtain authorization to expend the funds. The actual dollar amount limitations may vary from base to base and from MAJCOM to MAJCOM so it is important that we find out what limitations apply at the bases we are assigned to. If the MAJCOM can approve the expenditure of the funds needed to implement the technical solution, the approving official annotates the block with his or her name, title organization and signature. He or she also annotates the technical solution as approved if it is approved. In cases where even the MAJCOM does not have the authority to approve the expenditure of funds for a technical solution, they will validate the requirement and the technical solution and if they are convinced the requirement indeed exists and cannot be fulfilled by any other means. Once validated, they will annotate the validation on the AF Form 3215 and forward it to HQ USAF for possible funding.

The "MAJCOM Approval Authority" block is also used when the technical solution does not comply with architectural guidance or interoperability requirements. There are times when it may be impossible to develop a technical solution that complies with these requirements but the requirement must be fulfilled nonetheless. When this occurs, this block is completed by the MAJCOM signifying approval to deviate from the architectural and interoperability requirements that normally apply to technical solutions.

PROJECT SUPPORT AGREEMENT (PSA)

The PSA formally documents C4 systems requirements and approval for base support. The engineer who conducted the site survey will document the results in the PSA and forward it to the base CSO for concurrence to the tasks

The base CSO must coordinate PSAs with the C4 user and all tasked agencies. The PSA documents the equipment to be installed, the sites or locations agreed on, the required supporting construction, the services required; and operational, technical or other constraints affecting the C4 installation. If there are any disagreements, the CSO is responsible to resolve them and consolidate any concerns in the PSA endorsement.

Until the base CSO endorses the PSA, the engineer cannot finalize the material list and specific installation instructions. This agreement is also referred to as "PSA concurrence" or "PSA endorsement". The procedures and format for the PSA endorsement are included with the PSA itself.

PSA Format

The following are the standard sections of a PSA:

Cover Letter. The cover letter has the format of a standard official memorandum with the following sections:

- Program information
- General support requirements
- Implementation schedule dates
- Funding information
- PSA processing instructions

Attachment . Siting and project installation data. As the title states, this section has generic information about the project siting and installation. This section also contains:

- Stakeholders
- Waivers

- Limitations
- Restrictions
- Proposed Project Installation and Removal
- Related Factors

Attachment 2. Civil Engineering support requirements. You will soon find out that Base Civil Engineering (BCE) has a major role in supporting our project installations. This section specifically identifies the following BCE support requirements:

- Site Work and Exterior Utilities
- Buildings, Towers and Other Structures
- Special Services
- Other requirements

Attachment 3. C4 Systems Support Requirements. As with Base Civil Engineering, Communications support is also vital to the smooth installation of a Communication and Information project. This section identifies the following support requirements:

- Circuit Requirements
- Special Equipment
- Down Time
- Other requirements

Attachment 4. Drawings List. This section contains a list of all drawings applicable to the project

Glossary. The Glossary contains definitions and acronym explanation of terms used throughout the PSA

PSA Concurrence Checklist. The PSA is a contract between the Base CSO and the implementing agency. Therefore, the CSO must concur to all of the content of the PSA. This section provides specific format and instructions for providing the engineer with formal PSA concurrence.

Distribution List. This section identifies all addressees to whom the engineer sent a copy of the PSA. You need to verify that all stakeholders receive a copy of the PSA. If an agency was not included on the distribution list, you need to make a copy and send it to them.

SERVICE LEVEL AGREEMENT (SLA)

SLAs provide one method of documenting agreements between service providers and customers. Other methods are: host-tenant support agreements, memorandum of agreements or other formal documents. IA and C&A requirements should be part of this agreement. Use it to formalize the agreement between the DAAs--the policy for the connection. The agreement should identify connected systems, define connection requirements and document the roles of all participating organizations. Prior to connecting separately accredited systems, each DAA's responsibilities are carefully defined in a SLA. The DAA must have the authority to analyze the overall security requirements relative to the risk of operating the system and provide definitive directions to system developers or owners. The DAA exercises this authority to grant (or deny) a system to process actual data in an operational environment.

The NCC assists the wing or its functional equivalent in developing a standard level of service, that defines the roles of both the NCC and its customers, to include tenant units. This includes, but is not limited to, network service availability rates, fault response times, NCC dispatch responsibilities, configuration change procedures, initial contingency support requirements, fee-for-service charges (where applicable), customer escalation and security management procedures and other NCC-provided services. It also defines the customer's role and responsibilities, to include but is not limited to, reporting and escalation procedures, as well as guidance on configuration and systems management.

The NCC coordinates SLAs with customers whose network support requirements are unique or exceed the standard of service. SLAs define division of responsibilities for network operations and services between NCC and customer functional areas. They also define resources both parties will provide to support delivery of negotiated services. CSOs negotiate all SLAs with tenant and outside organizations. When necessary, they formalize agreements through MOUs or MOAs or supplements to this instruction.

CSOs distribute procedural changes via message traffic or electronic bulletin board. They use electronic bulletin boards, if possible, to distribute handbooks created by the NCC. The wing or its functional equivalent ensures the standard level of service is reviewed at least annually for accuracy.

Service Level Agreement Content Areas

The following is a sample of a SLA format between the service provider and the customer. The sample agreement only shows minimum topics that should be addressed:

1. Introduction. Parties (organizations) involved:
    a. Service provider: (i.e., DAA or NCC).

(1) POC names.
(2) Location or office symbol.
(3) Telephone numbers.

b. End-user organization.
(1) POC names.
(2) Location or office symbols.
(3) Telephone numbers.

2. Purpose. The purpose of this SLA is to state the relationship between the service provider and the end-user organization. It specifies the services and commitments of the NCC as well as the expectations and obligations of the end-user organization.

3. Responsibilities of Service Provider (Name of the Organization). The service provider agrees that it will:
   a. Specify what resources it will use. Describe how they will inform the customer of infrastructure changes and new or changed service.
   b. State security methods that they will use to protect infrastructure resources from unauthorized access, monitoring or tampering.
   c. Describe the process used to notify and coordinate with end-user organization about planned outages of connectivity, equipment or electricity.
   d. Explain the coordination process for service degradation or failure correction and state how customer will be kept informed of status.
   e. Describe materials that will be provided to the customer to minimize procedural errors.
   f. Explain customer support performance criteria and workload limitations (for example, hours of operation, response times, expected maximum calls).
   g. Describe what performance data and analysis reports they will provide to the customer organization to show service quality and level of customer support provided.
   h. State what customer training is available and what role the service provider's will play in customer training.
   j. Perform periodic surveys to monitor customer satisfaction.
   k. State the security measures they will use to protect infrastructure resources from unauthorized access, monitoring or tampering.

4. Responsibilities of End-User Organization.

a. The end-user organization agrees that it will:
    (1) Describe the process used to ensure end-users know procedures for getting help.
    (2) Coordinate with service provider on any major configuration changes (for example, network installation/expansion, TCP/IP port requirements, change in topology, system upgrades, relocation and so forth).
    (3) Describe the process used to notify end-users of planned outages of connectivity, equipment or electricity.
    (4) Workgroup managers and SAs will provide, upon request, equipment layout, network schematic, network connectivity (attached via backbone or stand alone) and their exact location.
    (5) Describe how they will use the performance and trend analysis data from service provider and provide feedback to improve service.
    (6) Develop end-user contingency operations plans and capabilities.
    (7) Identify what resources they will matrix or transfer to the service provider.
    (8) Provide service provider with access to equipment both electronically and physically as needed.
    (9) Agrees to perform the certification effort and comply with wing or NCC security policy.

b. During a trouble call, the end users will:
    (1) Contact end-user organization POC first, if available.
    (2) Describe what minimum information they will provide (for example, name organization, location, telephone number, equipment number, user-id, e-mail address).
    (3) Provide service provider with a description of problem, it's priority and potential mission impact.
    (4) Work with the service provider during fault isolation process, as needed.
    (5) Negotiate for increased workload/expansion for contingencies or new support.

5. Customer Escalation Procedures. The two parties agree to the following procedures in case they need to escalate resolution of the problem (that is, when the customer is not satisfied with the service provided):

6. Conclusion.

a. Parties agree that the terms of this agreement will remain in effect for (5 years, 6 months and so forth) are subject to review (annually, semiannually and so forth).
b. The parties agree to the following mechanism for initiating an out-of-cycle SLA review:
   Service levels and procedures established herein were agreed to by parties represented by undersigned.

   _____ _____

   (Service Provider Representative Signature) (End-User organization Signature)

   Attachments (add as needed):

1. Hours of Operation.
2. Definitions of Terminology.
3. Lists of Support Equipment and Software.
4. Summaries of Applicable Contracts.
5. Contingency Plan.

SUMMARY

As tech controllers we work with many different documents. CSRDs, PSAs, and SLAs are all documents that assist us in completing our jobs and assist us when working with customers. When a customer's needs are known, and our responsibilities are understood, confusion is reduced for all and mission success is ensured. Next, we are going to look at several examples of communication systems and the correspondence required to establish service.

COMMUNICATIONS SYSTEMS CORRESPONDENCE

OBJECTIVE

3b: Identify general principles pertaining to communications systems correspondence.

INTRODUCTION

In this section, we are going to examine some examples of communication systems and the coordination required for service. This is in no way a comprehensive list of systems or requirements, but a sample of the types you may encounter in your duties. Before we discuss the systems, lets take a moment to review Air Force communications hierarchy to better understand the correspondence process.

INFORMATION

DEFENSE INFORMATION SYSTEMS AGENCY (DISA)

History

Before 1960, each service had its own independent communications systems. With the exception of a few minor systems, the Air Force, Navy, and Army were unable to communicate effectively with each other because their respective communication systems were incompatible. Eventually the services decided that combining the defense communications systems would be much more beneficial. In May 1960, the DISA (formally the Defense Communications Agency) was formed to take charge of the newly integrated defense communications.

Mission

DISA performs the systems engineering and analysis for the Defense Information Infrastructure or DII (formerly known as the Defense Communications System). DISA ensures the DII is planned, improved, operated, maintained, and managed effectively, efficiently, and economically to meet the communication requirements of the Department of Defense (DoD) and other authorized government agencies.

DISA System Control Hierarchy

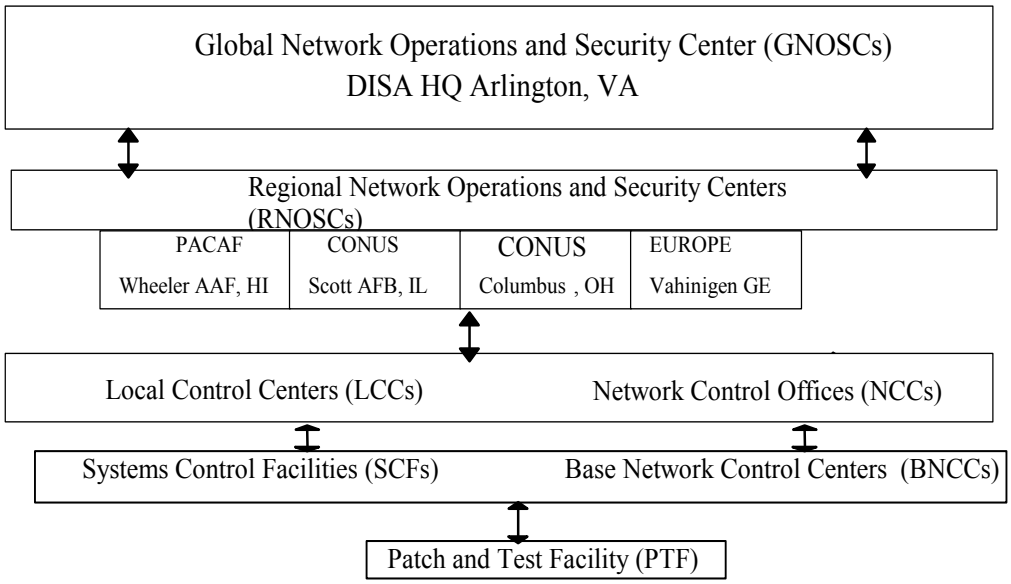

Figure 3-2. DISA System Control Hierarchy.

Global Network Operations and Security Center (GNOSC)

DISA's GOSC is responsible for the worldwide management and operational oversight of the Defense Information Infrastructure (DII). Enterprise network and systems management policy and standards are developed jointly by DISA, the services, and agencies. The Air Force Network Operations Center and Network Control Centers apply and enforce these policies at the regional and local levels. DISA Network Management (NM) span of control ends at the base Service Delivery Points (SDP) for fixed communications, and at the Joint Systems Control (SYSCON) for deployed. DISA will have visibility into the base network, as required, through a read-only capability and the base will have a similar capability into the Defense Information System Network (DISN) and information processing activities. All DoD organizations have a responsibility to share network trouble report information and analysis data. Electronic exchange of this information allows operations and maintenance management and higher level NM functions to retrieve or query raw data to compile analysis reports.

Regional Network Operations and Security Centers (RNOSCs)

ROSCs such as the AFNOC, MAJCOM NOSCs, and DISA ROSCs execute network and system management to ensure operational control and information assurance of a specific geographic or global Area of Responsibility (AOR). DISA ROSCs exist in the continental United States (CONUS), Pacific, and European theaters. The Air Force Forces (AFFOR) NOSC is responsible for deployed Air Force NM and reports to the Joint Task Force Joint Communications Control Center. Communities of interest also have NM capabilities at this level (e.g., Air Force Personnel Center (AFPC), Air Force Global Weather Central (AFGWC), etc.).

Communities of Interest. A global or regional control center may support and control these communities in the resolution of system problems. The global or regional unit may install an NCC compliant network management system (NMS) at each local unit, enabling the local unit to resolve its own network problems within its customer response requirements. This will also decentralize collection of local network performance data for planning purposes. ROSCs ensure LCCs in their AOR collect and forward network and system management data to the GOSC or the appropriate ROSC in a timely manner.

Local Control Centers (LCCs) and Network Control Centers (NCCs)

LCCs, specifically called NCCs in the Air Force, perform network and system element management. NCCs take direction from the GOSC or the ROSC in accordance with established directives and instructions. An NCC may provide service at the regional or global level under special circumstances. Community of interest functions may reside at this level, but usually support only a selected set of centralized information processing customers in a functional community. Community of interest LCCs take direction from the NCC.

Base Network Control Centers (BNCCs)

The BNCC serves as the single focal point for base Network Management and problem resolution traversing the base network. Communications and information services entering and exiting the base or site fall under the operational control of the NCC.

System Control Facilities (SCFs) and Patch and Test Facility (PTF)

A Systems Control Facility functions as the point of interface between the transmission elements (channels, trunks, links, etc.) and customers of the DII. SCFs fall directly under the operational control of the LCC. Patch and Test Facilities are normally associated with a specific function or special user. PTFs fall directly under the operational control of the SCF.

COMMUNICATION SYSTEMS

Non-secure Internet Protocol Router Network (NIPRNET)

NIPRNET contains DoD's Sensitive But Unclassified (SBU) data used primarily for administrative information and connection to the Internet utilizing routers and Asynchronous Transfer Mode (ATM) switches, which are interconnected using high-speed digital trunks. It is managed by DISA and services are provided by supporting bases and Commanders in Chief (CINCs) when organizations are deployed.

The NIPRNET is the way our local base LANs connect to other base LANs. PC-III circuits, medical circuits, financial circuits, and supply circuits all connect to each other through NIPRNET. This network is the DoD access to the World Wide Web through the use of gateways. Though we can access the Internet, NIPRNET is a completely separate network than the Internet. It consists of a collection of government owned and operated routers and multiplexers, interconnected by commercially provided circuits. The entry points from NIPRNET to the Internet are protected by many different methods including gateways, proxy servers, and firewalls

The NIPRNET Management Center provides 24 hours a day, 7 days a week (24/7) network support. They are a contract company providing assistance to the customers of the NIPRNET network in support of the military agencies. They are located at the Regional Operation Security Centers (ROSCs), i.e. Vaihnigen Germany in the European Theater and Columbus Ohio in CONUS.

Secure Internet Protocol Router Network (SIPRNET)

SIPRNET is the Defense Information System Network's (DISN's) Secret Internet Protocol Router. It is a secure Wide Area Network (WAN) that is separated both physically and logically from other DOD networks. It is comprised primarily of routers for transporting data at high speeds. Each access line or circuit and the backbone trunk is encrypted to ensure integrity of information. To control access, SIPRNET's design ensures that restrictions are enforced based on a user's clearance level and privileges (need to know) are incorporated.

SIPRNET is designed for dedicated subscribers, dial-up access, and tactical users. Dedicated subscribers are users on a computer that are directly connected to the SIPRNET backbone routers via serial or Ethernet lines. Dial-up users or remote users who do not have a dedicated connection to access SIPRNET dial in to the network using a Secure Telephone Unit-III (STU-III) and gain access through a communication server. Tactical users access SIPRNET through the Defense Satellite Communication System

(DSCS). SIPRNET provides secure communication for many important DOD systems including Defense Message System (DMS), the Global Command and Control System (GCCS) and the Global Command Support System (GCSS)
The SIPRNET Management Center provides 24/7 network support. They are a contract company providing assistance to the customers of the SIPRNET in support of the military agencies. We as system controllers are considered customers. We would call these experts to help us troubleshoot difficult network problems. The management centers are located at the Regional Network Operation Security Centers (RNOSCs) OCONUS and at the Pentagon serving the CONUS customers.NIPRNET and the SIPRNET both ride over the DISN network. They maintain physical and electrical separation from end-to-end. They provide email or electronic messaging in the email format from writer to reader. NIPRNET is the unclassified data network for DoD customers. SIPRNET on the other hand is a completely separate network allowing only secret and below classification messaging.

Defense Messaging System (DMS)

DMS was put together because of a need to replace the outdated AUTODIN system. Although considered highly effective, it is becoming outdated in its capacity to cost-effectively transmit messages. Discussions began in the late 1980's to formulate the requirements for a replacement messaging system that would function in place of AUTODIN.

The DMS is a flexible, commercial off the shelf (COTS) based network application layer system which provides multi-media messaging and directory services capable of taking advantage of the flexible and expandable underlying DII network and security services. It is designed to reliably handle information of all classification levels (unclassified to TOP SECRET), compartments, and handling instructions. In addition to maintaining high reliability and availability, the DMS must be compatible with approved legacy message systems, formats and protocols. DMS will be implemented in phases. Originally, the goal for full operational capability implementation of the DMS target architecture was 2008.

PROCEDURES FOR ORDERING TELECOMMUNICATIONS SERVICE

General Procedures – Request For Service (RFS)

The initiating agency, usually a field unit, prepares Feeder Request For Service (FRFS) in the format specified in DISA Circular 310-130-1, and DISA DSC notices, then the user submits it to the responsible Major Command (MAJCOM). The responsible MAJCOM

determines the Program Designator Code (PDC) and begins tracking and managing the requirement from the initial submission. The MAJCOM sends the validated RFS via AUTODIN/DMS/E-mail to the responsible DISA DSC for further action. The geographical location of the service determines the DISA office that should process the request.
The appropriate DISA office creates a Telecommunications Service Request (TSR) from the RFS and sends it for further action. The DISA/DSC creates a Telecommunications Service Order (TSO) from the TSR and sends it to the Defense Information Technology Contracting Office (DITCO) or other agency, depending on service requested, for further action. The TSO assigns the lifetime circuit identifier known as the command communications service designator. DITCO creates a Status of Acquisition Message (SAM) or Circuit demand (CD) from the TSO or TSR and sends it to all addressees listed in the TSO or TSR. The SAMs and CDs announce the stage of acquisition for the RFS/ TSR and assign the communications service authorization (CSA).

The organization assigned to accept the service submits the appropriate completion reports in the format specified in DISA Circular 310-130-1. The responsible organization is listed in the TSO.

Some local moves and rearrangements of government-owned equipment do not require submitting a RFS. Those are ones that do not change existing type or grade of service, end equipment or interfaces, or TSP. The DD Form 1367 is used for local moves and minor rearrangements of leased equipment within contractual, financial, and administrative limitations not exceeding maximum CSA limits. An RFS would be submitted for rearrangements or moves needing engineering assistance or causing circuit file updates.

SYSTEM SPECIFIC PROCEDURES

Defense Switched Network

MAJCOMs submit RFSs for DSN requirements through the servicing DISA DSC to the DISA DSN single system manager (SSM) office. The SSM manages and centrally funds DSN access lines from the user location to the switching node. DITCO assigns summary CSAs for calling precedence capability and outward traffic minutes of capability. MAJCOMs submit the request for either continental United States (CONUS) or outside the continental United States service to the Air Force DSN network managers (DSN-NM) at HQ Air Force Communications Agency (AFCA).

The Air Force DSN-NM reviews the request, accomplishes any required coordination and sends an approval/disapproval recommendation to HQ Air Force Communications and

Information Center (AFCIC). Following approval, the MAJCOM will submit the RFS to the servicing DISA provisioning activity.

DISN Data Services

The Air Force Systems Networking (AFSN) program office is responsible for the management of Service Delivery Points (SDPs) that give Air Force systems access to the DISN. These SDPs are directly connected to NIPRNET (unclassified) or SIPRNET (SECRET) DISA-managed internet protocol router networks. It is Air Force policy to connect all users to base local area networks (LAN). Base LANs are directly connected to a base-level SDP, then connected to the wide area SDP controlled by AFSN. Requirements not supported by the base LANs may connect directly to a wide area SDP.

Base LAN requirements processing

Customers located on Air Force installations should first contact the base communications squadron requirements personnel for a connection to the base LAN. If the requirement is not satisfied at the local level, customers should send it to their MAJCOM. After the MAJCOM validates the requirement, it is sent to the AFSN Program Management Office (PMO).

The AFSN PMO registers the requirement and informs the customer of receipt and disposition, as well as technically validating the requirement. Routine requirements are satisfied as soon as possible within existing resources. Special requirements or those with potential network-wide impact meet a Requirements Review Board and a Configuration Control Board to determine technical feasibility and solution options.

After AFSN PMO has validated requirements and recorded them in a database, it will then notify the customer, customer's MAJCOM, or functional PMOs. Customer actions include but are not limited to:

- Complete and submit an AF Form 3215, **C4 Systems Requirements Document** for local circuit action according to AFI 33-103, *Requirements Development Processing*.

- Complete and submit a DISN Data Services requirements form to the AFSN PMO.

- Complete and submit a FRS to the AFSN PMO for DISN circuit action.

- Acquire modems, cabling, connectors, and encryption devices, as necessary, for user system connection.

- Acquire appropriate user system/facility accreditation (SIPRNET).

- Coordinate with AFSN PMO, base-level SDP coordinator, Air Force Internet Control Center (for unclassified systems), Air Force Network Operations Center (for SECRET systems) throughout the installation/implementation process.

SUMMARY

We have covered the different levels of our communications chain of command as well as various systems and the coordination required to bring them into service. As a craftsman level tech controller, you may be tasked to assist in providing service and support to Air Force organizations and an understanding of how the process works is key to your success. Armed with the information you have learned in this chapter you should be able to meet the challenge whatever it may be.

CHAPTER FOUR

NETWORK TECHNOLOGIES

OBJECTIVES

4a: Identify general principles pertaining to broadband technology.

4b: Identify general principles pertaining to SONET.

4c: Identify general principles pertaining to Digital Subscriber Line Technology.

BROADBAND TECHNOLOGY

Objective 4a: Identify general principles pertaining to broadband technology.

THIS OBJECTIVE IS COVERED IN THE COMMERCIAL TEXT
Cisco Internetworking Technologies Handbook, Third Edition

Section I	Intro to Networking	Chapters 1-6
Section II	LAN Protocols	Chapters 7,8
Section III	WAN Technologies	Chapters 10,16
Section V	Bridging and Switching	Chapters 23,26,27
Section VI	Network Protocols	Chapter 31
Section VII	Routing Protocols	Chapters 47,42,40,46,39

SONET

Objective 4b: Identify general principles pertaining to SONET.

SONET/SDH FRAMING

SONET technologies were developed in the early 1980s and were standardized by the joint efforts of the American National Standards Institute (ANSI), the Exchange Carriers Standards Associations (ECSA) and the Bellcore. The initial specification allowed a transfer rate of 50.688 Mbps. The real market interest in SONET began after AT&T Bell Labs utilized it in its Metrobus project. Later, the SONET designers modified the SONET frame size to allow for T-1 mapping into the frame and to the rate of and the multiples of 51.84 Mbps. This resulted also in compatibility between North American and European standards. ANSI's international counterpart, ITU-T, was responsible for the European specification based on optical signaling---Synchronous Digital Hierarchy (SDH).

SONET/SDH is an optical-based transport network, utilizing synchronous clocking. The terminal/service adapter (or multiplexer) maps the user signal, such as T1, E1 and ATM, into a Synchronous Transport Signal (STS). STS is an electrical signal and the basic building block of SONET. Synchronous Transport Module (STM) is an electrical signal and the basic building block of the SDH transmission hierarchy. The base rate in North America is 51.84 Mbps (STS-1). The base rate in the rest of the world is 155.52 Mbps (STM-1), which is three times faster then in North America.

SONET LAYERS

SONET, categorized as a physical layer technology according to the OSI reference model, consists of multiple sublayers, as illustrated in Figure 4-1. The principles of the hierarchical OSI reference model are the basis for this design.

The user layers run on top of the SONET physical layer. The physical layer is divided into three major sublayer entities:

- Transmission *Path*
- Digital *line*
- Regeneration *Section*

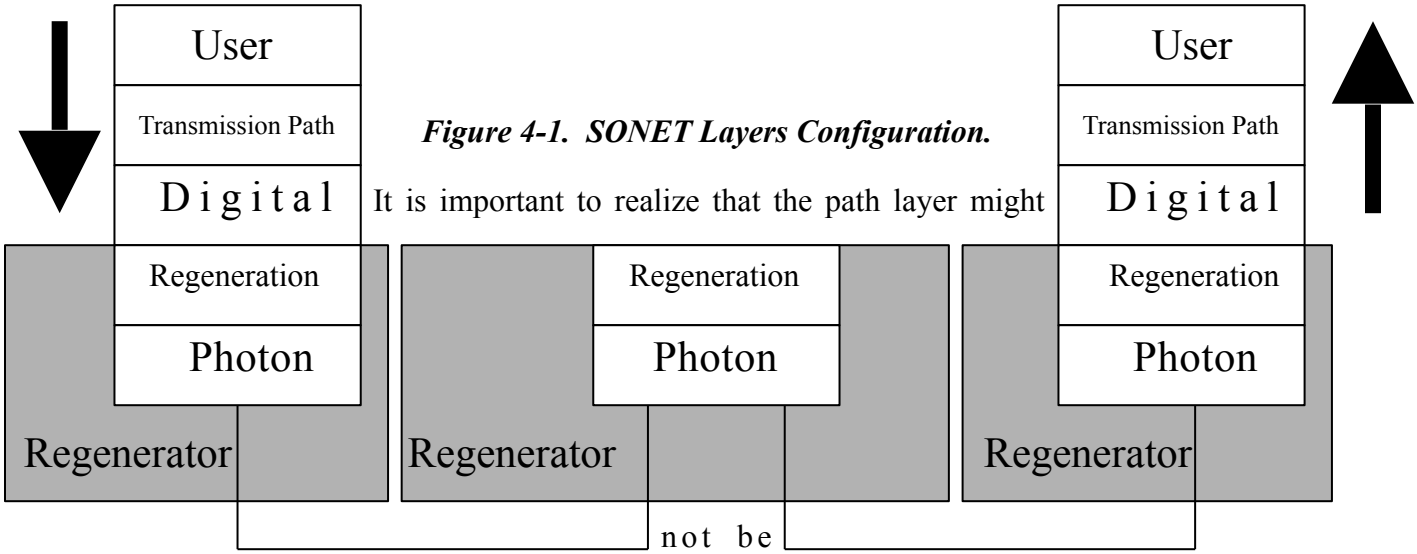

Figure 4-1. SONET Layers Configuration.

It is important to realize that the path layer might not be accessible within the network by the intermediate switches, because the path layer takes care of an end-to-end operation. Traffic is passed from the user layer to the path layer, where the path header or overhead is attached. Some of the responsibilities of the path layer include.

- Performance monitoring
- Path status
- Path trace
- Assembly and disassembly of cells into STS signals

From the path layer, the traffic is passed to the line layer. The layer attaches its header (overhead) and performs some operations, such as multiplexing the signals. The line overhead functions include.

- Multiplexing (or concatenating) signals
- Performance monitoring
- Switching protection
- Line maintenance

Upon completing its functions, the line layer passes the traffic to the regeneration section.

The regeneration section consists of section and photonic layers. The section layer attaches the section header and performs the following functions.

- Performance monitoring
- Framing
- Local orderwire

- Form message-based channel for Operations, Administration, Maintenance and Provisioning (OAM&P)

Upon completing its functions, the section layer sends the traffic to the photonic layer. The photonic layer is responsible for converting the electrical signals to the optical signals and for regenerating the optical signals. The photonic layer does not add the header. It encodes the traffic into bits and transmits them.

You can see that SONET framing constitutes three levels of overhead, as illustrated in Figure 4-2. Above the photonic layer, the section, line, and path layers add their corresponding headers to the payload, consequently forming a SONET frame or envelope. Repeaters or regenerators, which are needed when the signal through the fiber becomes too low due to long distances between SONET/SDH multiplexers, join sections. The multiplexers are responsible for mapping, aligning, multiplexing and stuffing various input rates from asynchronous signals.

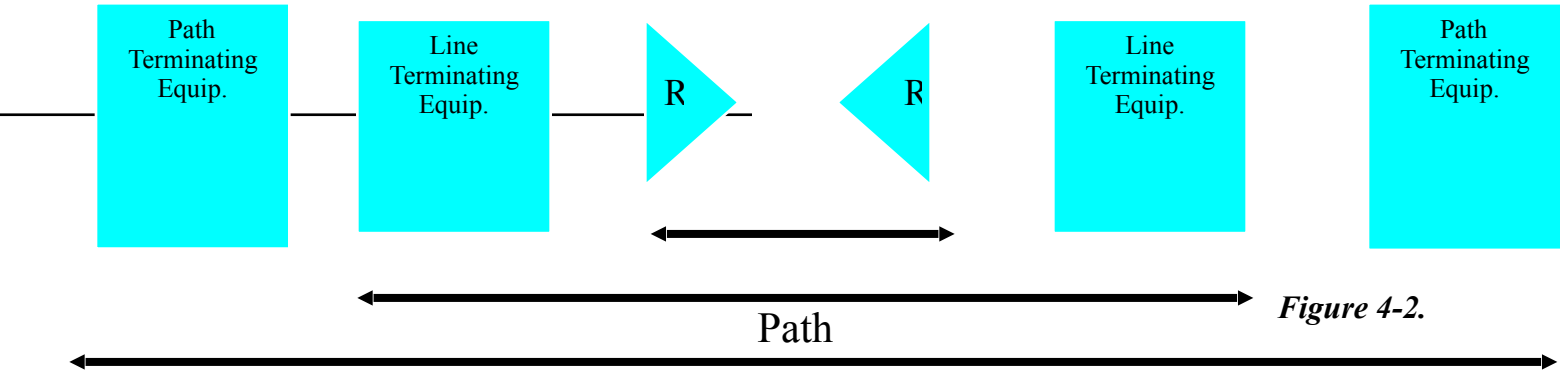

Figure 4-2.

Three Levels of SONET Overhead.

SONET/SDH Signaling Hierarchy

Figure 4-3 shows the SONET and SDH multiplexing signaling hierarchy and both the optical Signaling (OS) and Electrical Signaling (ES) levels. STS-1 forms the basis for the Optical Carrier-1 (OC-1) signal. OC-1 is the foundation for the synchronous optical signal hierarchy; STS-1 forms the basis for the synchronous electrical signal hierarchy in North America and the STM-1 forms the basis for the synchronous electrical signal hierarchy in rest of the world. The electrical rate is used primarily for transport within a specific piece of hardware. When lower levels signals are multiplexed, you can achieve higher level signals, such as OC-192, for example.

The SONET/SDH signaling hierarchy does not stop at OC-192. It carries on up to OC-768 with link speeds of 39 Gbps and more. With new technology developments and growing bandwidth demands, these higher levels of SONET hierarchy no doubt will be deployed to a greater extent than can be imagined today.

Optical Level	Electrical Level	Line Rate (Mbps)	Payload Rate (Mbps)	Overhead Rate (Mbps)	S D H Equivalent
OC-1	STS-1	51.840	50.112	1.728	-
OC-3	STS-3	155.520	150.336	5.184	STM-1
OC-9	STS-9	466.560	451.008	15.552	STM-3
OC-12	STS-12	622.080	601.344	20.736	STM-4
OC-18	STS-18	933.120	902.016	31.104	STM-6
OC-24	STS-24	1244.160	1202.688	41.472	STM-8
OC-36	STS-36	1866.240	1804.032	62.208	STM-13
OC-48	STS-48	2488.320	2405.376	82.944	STM-16
OC-96	STS-96	4976.640	4810.752	165.888	STM-32
OC-192	STS-192	9953.280	9621.504	331.776	STM-64

OC-9, OC-18, OC-24, OC-36, OC-96 are considered orphaned rates.

Figure 4-3. SONET/SDH Transmission Rates.

DIGITAL SUBSCRIBER LINE (DSL)

4c: Identify general principles pertaining to Digital Subscriber Line Technology.

THIS OBJECTIVE IS COVERED IN THE COMMERCIAL TEXT

Cisco Internetworking Technologies Handbook, Third Edition

Section IV	Digital Subscriber Line	Chapter 21

CHAPTER ONE

NETWORK SECURITY

OBJECTIVES

1a: Identify basic facts associated with the Air Force Computer Emergency Response Team (AFCERT).

1b: Identify basic facts associated with Information Operation Conditions (INFOCON).

1c: Identify basic facts associated with Base Information Protection (BIP).

1d: Identify general principles pertaining to security tools.

AIR FORCE COMPUTER EMERGENCY RESPONSE TEAM (AFCERT)

Objective 1a: Identify basic facts associated with the Air Force Computer Emergency Response Team (AFCERT).

INFORMATION

MISSION

Established in 1992, the mission of the AFCERT is to provide Information Protect (IP) assistance to Air Force units. The AFCERT conducts operations involving intrusion detection, incident response, computer security information assistance, and vulnerability assessment of Air Force automated information systems. The AFCERT also provides decision support to the Air Staff, Defense Information Systems Agency, and Air Force Office of Special Investigations, plus guidance on policies and procedures to other government agencies.

AFCERT is the Air Force's global command center for handling worldwide-networked computer system security issues. The AFCERT is the single point in the Air Force for reporting networked computer intrusions and problems. It performs three broad missions: remote security assessments, automated intrusion detection and security incident response.

Remote Security Assessments

The AFCERT performs remote security assessments on worldwide-networked Air Force computer systems through its On-Line Survey (OLS) program. Through the OLS, the

AFCERT employs intruder techniques, tools and capabilities to "attack" unsuspecting Air Force computer systems.

The OLS's goals are to measure the Air Force's networked computer security posture by seeing if systems can be penetrated using well-known, simple vulnerabilities and checking to see if anyone noticed and reported the attack on their system. It also shows the Air Force what an attack looks like and to operationally exercise the Air Force's ability to protect its computer resources.

The AFCERT conducted 62 OLSs at 52 different bases in 1996, surveying 4,309 systems. Of these, only 433 (10 percent) resulted in successful limited intrusions and 48 (one percent) resulted in full access intrusions, or root access. These values showed continued improvement from 1995, when the AFCERT penetrated 15 percent of the tested systems at the user level and three percent at root. The continued downward trend in the AFCERT's ability to penetrate systems shows a satisfactory improvement on the part of Air Force computer systems to repel unauthorized intruders and demonstrates the worth of the Computer Security Assistance Program, the AFIWC's program to help the Air Force defend its computer resources. The AFCERT would like to see detecting and reporting at 95 percent or higher, however, only 14 percent of the attacked systems detected and reported the OLS activity to the AFCERT, down from 16 percent in 1995.

Automated Intrusion Detection.

The AFCERT uses an automated computer intrusion detection system called the Automated Security Incident Measurement (ASIM). The ASIM is a hardware and software system that sits on Air Force networks "listening" for "suspicious activity" that is characteristic of intruder techniques. It processes what it deems suspicious and reports once every 24 hours to the AFCERT. The ASIM is the workhorse of the AFCERT and is extremely effective at detecting and reporting intruder activity, the first two steps necessary to mount an effective response. Now the AFCERT monitors 107 Air Force and three joint ASIM sites. The AFCERT estimates the ASIM now detects over 100 million suspicious Internet connections a month.

ASIM software is enhanced to provide the AFCERT with near real time (NRT) intrusion detection alerts and a "connection denial" capability. NRT alerts give the AFCERT timely notification of an attempted or actual intrusion so it can work with the affected base's computer security personnel to reduce or prevent damage to Air Force computer systems.

Security Incident Response.

The AFCERT also provides computer security education and awareness through AFCERT advisories. AFCERT advisories are issued any-time the AFCERT recognizes a security situation that could apply to users across the Air Force and provides a convenient

way to easily disseminate the word. They ranged from making IP personnel aware of common poor security practices to providing information on known vulnerabilities and recommended preventive measures.

Air Force computer security is global in nature, yet defies geographical limitations. Implementation of computer security tools crosses traditional organizational boundaries. Policies and procedures are needed to define roles and responsibilities between AFCERT, major commands, bases and the information warfare squadrons.

The ASIM works. Hackers have been caught and prosecuted. ASIM continues to identify poor security practices, as well as real intrusions. Research must continue to identify ways for eradicating both, with the result being fewer or no intrusions. With each report or advisory issued, someone in the Air Force community is educated on how to implement better computer security practices.

Although analyzing ASIM data daily reveals possible intrusion activity, fielding a reliable NRT ASIM is critical to providing alert notifications in a timely manner. Improvements to the NRT ASIM, in particular the connection denial capability, will enhance this capability. Once NRT ASIM alerts a possible or actual intrusion, the AFCERT needs to provide the commander the option of denying that connection to prevent damage to Air Force computer systems.

TIME COMPLIANCE NETWORK ORDERS (TCNOs)

Upon receipt of an IAVA, IAVB or DCTA from DoD CERT, a team of AFCERT experts assesses the threat to Air Force information systems and encapsulates the alert, bulletin, or technical advisory into a Time Compliance Network Order (TCNO). A TCNO contains the minimum acknowledgement, dissemination, implementation, tracking and compliance reporting instructions needed to manage the mitigation of vulnerabilities and risks to Air Force networks and operations.

The AFCERT assigns each TCNO a priority according to the DoD level of implementation and specific reporting requirements, the scope of the vulnerability to Air Force networks and to mitigate the potential impacts the exploited vulnerability has on Air Force operations.

Emergency TCNOs. Emergency TCNOs require immediate attention from all agencies. Generally these will identify vulnerabilities being actively used to gain unauthorized access to DoD systems, those that have a high potential for adversely affecting DoD networks, or those that intelligence indications and warnings indicate are specifically being postured for targeting DoD systems.

Urgent TCNOs. Urgent TCNOs identify vulnerabilities not yet being widely exploited in the commercial world or which have not been extensively targeted against

DoD networks. While the implementation and reporting timeframes for urgent TCNOs are longer than emergency TCNOs, events may drive an increase in the priority of an urgent TCNO to an emergency TCNO. For example, the development of hacking scripts or tools may significantly increase the attempts against DoD networks to exploit the vulnerability.

Routine TCNOs. Routine TCNOs identify new vulnerabilities not yet being exploited or vulnerabilities affecting operating systems/applications in limited use. As in the case above, routine TCNOs may be raised to a higher priority if conditions warrant.

Disseminating TCNOs. The AFCERT notifies the Air Force Network Operations Center (AFNOC), Network Operations and Security Centers (NOSCs), and Network Control Centers (NCCs) immediately upon discovering vulnerabilities and incidents. TCNOs are disseminated using the Automated Digital Network (AUTODIN) or Defense Message System-Air Force (DMS-AF).

TCNO Compliance. Compliance with TCNOs is mandatory. At the local level, NCCs notify Network Administrators (NAs), Functional Systems Administrators (FSAs) and Workgroup Managers (WMs) within their area of responsibility of a TCNO. In general, NAs, FSAs and WMs accomplish TCNO implementation. They implement TCNOs according to the step-by-step instructions in the TCNO, or as directed by the system's configuration controlling authority. Compliance with TCNOs is generally reported to the servicing NCC.

INFORMATION CONDITIONS (INFOCON)

Objective 1b. Identify basic facts associated with Information Operations Condition (INFOCON).

INFORMATION

INFORMATION OPERATIONS CONDITION

The purpose of the Information Operations Condition (INFOCON) system is to provide a structured reaction to and a defense against adversarial attacks on Department of Defense (DoD) computers and telecommunications. INFOCON applies to activities throughout the entire conflict spectrum from peacetime through war. Threat Conditions (THREATCON) and Defense Conditions (DEFCON) are also included in the spectrum.

The INFOCON system is a comprehensive defense posture and response based on the status of information systems, military operations, and intelligence assessments of the capabilities and intent of an adversary.

It is important to understand the INFOCON system because a computer network attack (CNA) is an attractive option for our adversaries. Computer network attack is defined as "operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves."

The INFOCON notification process begins at the DoD level and is administered by the Joint Task Force for Computer Network Defense (JTF-CND).The commander of the JTF-CND makes recommendations to the Secretary of Defense (SECDEF) to change INFOCON levels DoD-wide. Once the SECDEF approves the INFOCON level change, the commander of the JTF-CND notifies combatant commands, services, and defense agencies through the Defense Message System (DMS), Automated Digital Network (AUTODIN), or voice message.

The Air Force notification process begins with the Air Force Network Operations Center (AFNOC). The AFNOC executes an Emergency Action (EA) Quick Reaction Checklist (QRC), to initiate immediate voice notification to all.

- Major Commands (MAJCOMs)
- Direct Reporting Units (DRUs)
- Field Operating Agencies (FOAs)
- Air Staff

The AFNOC follows up voice notification with a message. The commander of the Air Force Information Warfare Center for the Joint Task Force for Computer Network

Defense (JTF-CND) is responsible for administering Air Force implementation of an INFOCON level change.

The action addressees on an INFOCON change notification message are responsible for disseminating the change to subordinate units. Downward notification involves the declaration and dissemination of INFOCON changes to major commands and lower echelon units. If warranted, commanders at the major command, numbered air force, wing, or base level may declare an INFOCON that is higher than that imposed by a higher headquarters. Downward notification of a lower-echelon initiated INFOCON change is the responsibility of the local unit. The Chief of Staff of the Air Force must approve up-channel reporting.

When a change to the Air Force-wide INFOCON is made independently of the DoD-wide INFOCON, the commander of Air Force Forces assigned to the JTF-CND reports directly to the JTF-CND commander and the Joint Staff through the AFNOC.

INFOCON LEVELS

The INFOCON system provides five different levels based on the appropriate defense posture. The five levels in ascending order are.

- NORMAL
- ALPHA
- BRAVO
- CHARLIE
- DELTA

INFOCON NORMAL. The first INFOCON level is NORMAL. This level relates to normal day-to-day actions. It is recommended all mission critical information, and information systems and their operational importance are identified during INFOCON NORMAL. You should also ensure all points of access and their operational necessity are identified. Normal security practices should be conducted on a continuing basis. For example, you should:

- Conduct education and training for users, administrators and management.
- Ensure an effective password management program is in place.
- Conduct normal auditing, review and file back-up procedures.
- Conduct periodic internal security reviews and external vulnerability assessments.
- Confirm the existence of newly identified vulnerabilities and install patches.
- Employ normal reporting procedures.
- Periodically review and test higher-level INFOCON actions.

INFOCON ALPHA. The second INFOCON level is ALPHA. This level indicates an increased risk of attack. The criteria for INFOCON ALPHA level are:

- Indications and warnings of a general threat
- Regional events affecting US interests and involving potential adversaries with suspected or known computer network attack capability
- A planned or ongoing military operation, contingency or exercise that requires increased security of information systems
- Information system probes, scans or other activities detected which indicate a pattern of surveillance
- It is recommended all actions required at INFOCON NORMAL continue to be accomplished at ALPHA level.

INFOCON BRAVO. The third INFOCON level is BRAVO. This level indicates a specific risk of attack. The criteria for BRAVO level are:

- Indications or warnings a specific system, location, unit or operation is targeted.
- A planned or ongoing major military operation or contingency
- The detection of a significant level of network probes, scans or activities that indicate a pattern of concentrated reconnaissance
- Attempted network penetration or denial of service with no impact on DoD operations

All action required at INFOCON ALPHA should continue to be accomplished at INFOCON BRAVO.

INFOCON CHARLIE. The fourth INFOCON level is CHARLIE. This level indicates a limited attack. The criteria for this level are:

- Intelligence attack assessments indicating limited attacks are imminent
- Information system attacks detected with limited impact on DoD operations

Limited impact attacks mean:

- The attacks have minimal success and are successfully counteracted.
- There is little or no compromise of data or systems.
- The unit is able to accomplish its mission.

All action required at INFOCON BRAVO should continue to be accomplished at INFOCON CHARLIE.

INFOCON DELTA. The fifth INFOCON level is DELTA. This level indicates a general attack. The criteria that indicate this level has been reached are:

- The detection of one or more successful information system attacks that impact on DoD operations
- Widespread incidents that undermine the system's ability to function effectively
- A significant risk of mission failure
- All actions required at INFOCON CHARLIE should be accomplished at INFOCON DELTA.

INFOCON levels may be lowered or heightened by commanders at the major command, numbered air force, wing or base level. Commanders use three broad categories of factors to determine the appropriate INFOCON level:

- *Operational* factors result from heightened concern due to ongoing or planned contingency operations.
- *Technical* factors result from the assessment of vulnerabilities or effects of attacks on networks.
- *Intelligence* factors result from the assessment of adversary attack through foreign information gathering or law enforcement intelligence.

Those responsible for determining and establishing the proper INFOCON level are MAJCOM, NAF, wing, base or unit commanders. The INFOCON level is based on the evaluation of all relevant factors in the three categories—operational, technical and intelligence.

The decision to change the INFOCON level should be tempered by the overall operational and security context at that time. An intruder for example, could gain unauthorized access and yet not cause damage to systems or data. The commander of the Air Force Information Warfare (AFIWC) JTF-CND reassesses the Air Force-wide INFOCON. Major command, the direct reporting unit and subordinate commanders reassess locally directed INFOCON levels as required by ongoing events or whenever a higher headquarters issues an INFOCON change.

INFOCON levels at each echelon are lowered by the same authority and process that raised them. This is true for all base units, including Air Force tenant units who generally use the host-installation INFOCON level. An exception to this rule would be if the tenant CINC or designated Air Force Component Commander determined the lowering of the level would interfere with CINC directed operational actions.

INFOCON Deconflicting: MAJCOMs, NAFs and units may be subject to conflicting CINC and service INFOCON levels. In such cases, the higher INFOCON

level takes precedence, unless the MAJCOM commander determines it would interfere with the CINC directed operational actions.

INFOCON is the procedures we put into place to assist in the security of our information and network resources. By utilizing these steps and working with AFCERT, we can help to turn away hackers and malicious logic from affecting our systems. Next, we'll look at some specific methods for dealing with these threats.

INFORMATION PROTECTION AND NETWORK SECURITY

Objective 1c: Identify basic facts associated with Base Information Protection (BIP).

INTRODUCTION

The advantages of connecting our information resources to the Internet are almost endless. In fact, since the early 1990's the Air Force has invested itself heavily in the use of internetworking and "Internet" services. However, the benefits of such services do not come without an element of risk. Uncontrolled exposure to the Internet encourages unauthorized users to intrude upon our computer networks. Like many government organizations, the Air Force (AF) is often seen as "the enemy". This makes the AF a target for many forms of attackers: "vandals" out to ruin our reputation, "hackers" who attempt to illegally use our resources or expose our vulnerabilities and "spies" determined to steal information for profit. In this chapter, we are going to look at AF initiatives to define and implement security for information and network resources.

INFORMATION

BOUNDARY PROTECTION

The concept of boundary protection has taken on increased importance over the last few years. Although it has long been a major consideration for classified networks, it has become increasingly important for unclassified networks as well. As more mission essential systems are added to the Air Force inventory, the issue of boundary protection becomes increasingly complex. The explosion of the World Wide Web (WWW) has created new opportunities for the exploitation of our networks. We, as network security professionals, must ensure that the systems we are responsible for protecting are able to communicate freely, yet still prevent unauthorized personnel from gaining access. This is no easy matter, especially considering the fact that many of the users we support do not have a clear idea of their actual requirements. Therefore, it is ultimately the Designated Approval Authority's decision as to how much protection is sufficient. It is based on a balance of security, usability and cost. The Air Force has made this decision easier in the

last few years by implementing standardized boundary protection strategies at all its installations.

Protection Strategies

Three things we put at risk when connected to the Internet: Data, Resources and Reputation. Two primary ways to approach the security of our network are Host Security and Network Security. The host security model involves the discovery of vulnerabilities and the application of security measures on each individual system in the network. As the sole measure, this is certainly not an acceptable model for network security given the possibility of hundreds, or even thousands of individual systems in the network. Such an endeavor would require endless attention to a variety of security details. This is unaffectionately known as "putting out fires". On the other hand, the network security model concentrates on the entrance and exit of the entire network as a whole. It reduces network access to one, or a few, controlled and monitored points. This is akin to placing a huge lock on the front door, instead of every single item in the house. Although the network security model is the preferred method, there is no magic bullet when it comes to network security. A good network security model will also include sound host security measures. The network security model is primarily accomplished using the boundary protection method. Boundary protection involves the physical layout of a network by limiting and controlling access to the protected network. The concept is analogous to the mote around a castle.

Security is an on-going process. There will always be a "weakest link" in our network security program. The objective is to be completely aware of all our vulnerabilities and to take prudent steps to eliminate or reduce the risks they introduce. The Air Force has chosen a boundary protection architecture known as the Barrier Reef concept, which incorporates all of these elements and others.

Barrier Reef

The goal of Barrier Reef is to establish base-level boundary protection from the harmful aspects of attaching to the Internet while providing high-performance wide-area communications links and services. Barrier Reef is the electronic equivalent of the physical perimeter defense provided on AF bases by our security forces. Proxies and firewalls act as electronic "gate guards" inspecting traffic and allowing only authorized traffic. Barrier Reef provides a step-by-step process towards "defense-in-depth," or "layered" protection of network assets. The USAF/SC has established Barrier Reef as the Air Force concept for boundary protection of our information networks.

The Barrier Reef process complements the Combat Information Transport System Base Information Protection (CITS/BIP) Program. While CITS/BIP provides the technical solution, Barrier Reef provides the overall process to secure and protect our information networks. The Barrier Reef process was operationally validated at Barksdale AFB, LA by

a team of AFCA engineers. Information can be found on the HQ AFCA IP Homepage on the World Wide Web. The Barrier Reef process currently consists of 12 steps. These steps provide a systematic approach to establishing boundary protection that is coordinated with the overall Air Force network strategy of providing professional, secure network service. The following is an overview of the 12 steps.

1. Know Thyself
   - Identify and reduce exterior network access points to a manageable number.
   - Conduct traffic analysis to identify the protocols and throughput that currently exist.

2. Requirements Determination
   - Validate that each traffic type identified is mission required.
   - Understand bases will vary due to varying functional area mission requirements.

3. Write Security Policy
   - Create a base-level network security policy involving all tenants and functional areas using AFSSI 5027 as a starting point.
   - Deny all services that are not specifically allowed; enumerate all allowable services.

4. Packet Filtering

   - Take advantage of existing router Access Control List (ACL) capabilities.
   - Block as many unsafe services as possible based on IP headers.

5. Network Monitoring
   - Integrate network monitoring device(s) such as the Automated Security Incident Monitor (ASIM).
   - Place devices outside the boundary protection mechanism to monitor all attempted attacks.

6. Network Time Server
   - Integrate Global Positioning System receivers to provide a reliable, accurate time source for base systems.
   - Protect the base from the injection of false time (i.e., spoofing of Network Time Protocol).

7. Centralized Dial-in Access
   - Assemble multiple functional dial-in solutions into one centralized service (e.g., through a Remote Access Server).
   - Protect access through this service via strong authentication of users.

8. World-Wide Web Proxy
   - Direct all outgoing WWW requests through a proxy device to
   - hide users' identities from Internet eavesdroppers,
   - reduce Wide-Area Network (WAN) utilization and improve user response time,
   - provide an integrated virus scanning capability and
   - deny or identify web access to unauthorized sites.

9. Internet and Intranet Services
   - Place the Web Servers in a “de-militarized zone” to reduce internal network access.
   - Establish a system to keep public data updated and separate from internal web servers.
   - Provide a public "lobby" for e-mail entry and access to data or wide distribution.

10. Proxy Common and Special Services
   - Authenticate outsiders before granting access for "dangerous" services (e.g., Telnet, FTP, Rlogin).
   - Implement controlled access for specialized AF services (e.g., InfoConnect, AFORMS, CHCS).

11. Network Concealment
   - Hide internal network address space from the public domain.
   - Separate public and private Domain Name Services (DNS).

12. Train, Maintain and Certify
   - Establish continuity for training, system changes, and upgrades.
   - Certify and accredit boundary protection systems and the base network.

The Barrier Reef Architecture. The Barrier Reef concept is not a firewall in the traditional sense of the word. The term “Reef” was chosen because the design essentially “filters and controls” data much like a coral reef filters and controls the flow of water. The design of Barrier Reef is based upon a firewall design known as a screened subnet architecture. It consists of an external router connected to the untrusted network (e.g. the Internet), a perimeter network consisting of bastion host servers and proxies, an internal router heavily filtered and bordering the interior, protected network. The advantage of the screened subnet architecture is that is does not present a single point of failure to the interior network. This is accomplished by the layered defenses provided by the external router, perimeter network and internal router. Reference Figure 1-1 for an illustration of the Barrier Reef architecture. Barrier Reef makes some additions to the basic screened subnet architecture by incorporating the following elements:

- Intrusion detection and questionable activity monitoring outside the external router
- An exterior dial-up subnet and communications server for valid remote access and authentication
- Network service proxies for safe and controlled access to services such as: WWW, FTP, Telnet, etc.
- Private IP addressing of the interior network in order to "conceal" the protected systems
- Network Address Translation (NAT) for direct interior system access to exterior network service

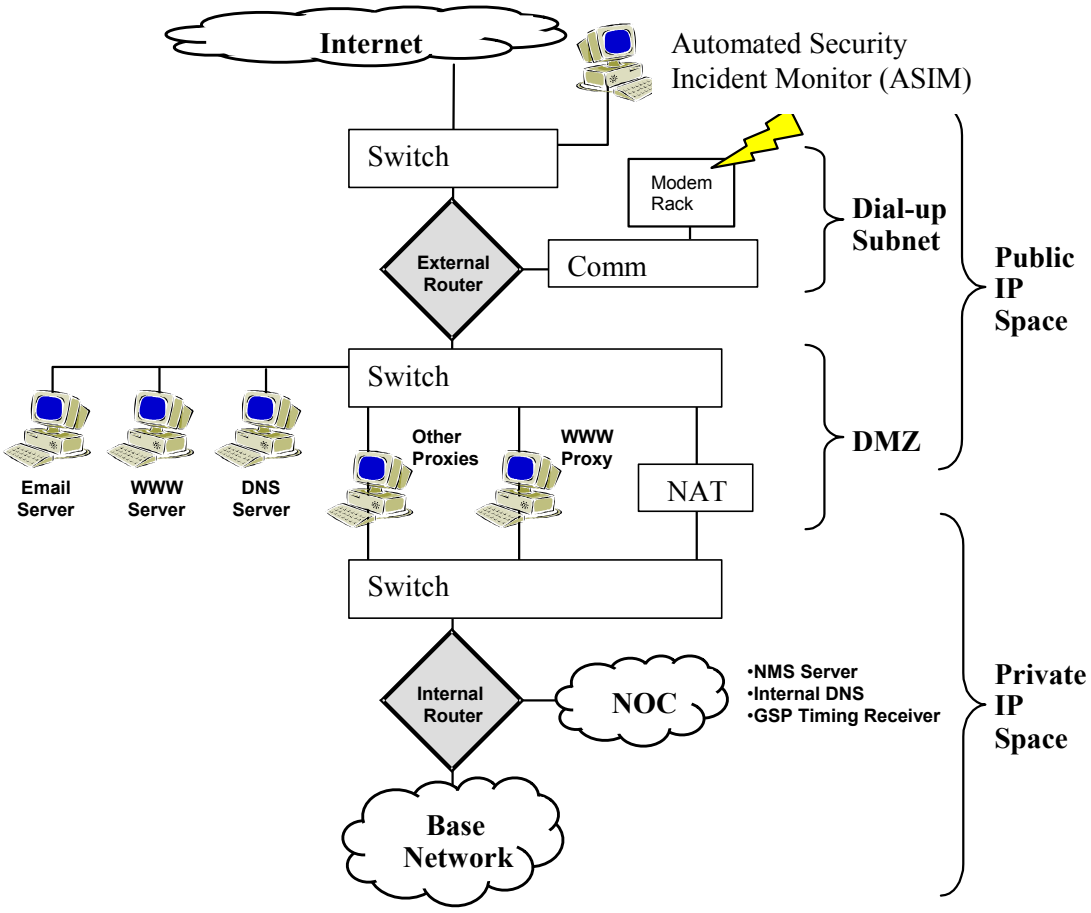

Figure 1-1. Sample Barrier Reef Design.

INTRUSION/MISUSE DETECTION

As a priority resource, the impact of any actions on network resources must be considered constantly. Consistent misuse of network resources, whether intentional or unintentional, is as detrimental to efficient operations as a systematic hacker attack. Both have the potential to degrade operations and deny authorized use of the network. One of the ways to guard against such unauthorized use is through system monitoring.

System Monitoring

System monitoring is one of the primary functions of the Network Control Center(NCC). Unlike system auditing functions, it is usually accomplished real time. Not only does it verify that the system is operational, it also ensures the system is being operated within the parameters established by network security policy and the DAA. One of the most common monitoring functions is the detection of unauthorized intrusions on the network. This may be from sources outside or inside the network. In fact, it is more likely that unauthorized access will come from within the network domain, since most users have at least basic access rights. This is not uncommon, especially where there are little or no restrictions set on network directories and files. Lax control of network resources may lead to data loss or corruption. Outside sources, such as hackers, tend to select easy targets that pose minimal risk of detection and identification. They may also utilize "social engineering" techniques to obtain user id and password information from unsuspecting authorized users by posing as network administration personnel. The NCC Information Protection(IP) operators work closely with the Wing IA Office to identify and protect against such intrusions.

System monitoring may also be configured to detect misuse. Computer misuse may result from a lack of training for newly assigned network users or from trained personnel who intentionally ignore normal operating procedures. In the first case, the NCC and Wing Information Assurance(IA) Office must implement a strong training program. This will ensure that all new network users are fully versed in basic computer security principles and network security policies before access is granted. This may be accomplished in conjunction with the initial Security Awareness Training and Education (SATE) briefing upon arrival or independently. In either case, they must be trained before access is granted. The education of all users on proper computer usage is a continuous process from the moment they arrive until they no longer require access. User's who continually demonstrate a disregard for network operating procedures present a potential security risk to the network and should have network access permissions removed. Network access is a privilege, not a right. IP operators must constantly be on guard to protect the system from improper use.

Virus and Malicious Logic Control

Another important, but often overlooked, element of system monitoring is the control of computer viruses and malicious logic. Viruses come in many forms; some invade the boot sectors of hard drives or floppy disks, and others imbed themselves into the macro-functions of the applications and files that use them (i.e., MS-Word and MS-Excel). Viruses represent a serious threat to the smooth operation of a network and may spread rapidly from system to system until they eventually cause catastrophic system failure. Malicious logic is also a serious threat and may assume many forms. It usually consists of software instructions contained within a data file or application that cause an unexpected event to occur at a specified time. Most malicious logic is triggered upon "opening or running" the file or application. Still other more sophisticated forms of malicious logic sit dormant on the storage media, until a specified date or time, and then perform their instructions. Although you may not have the ability or expertise to identify malicious logic within an application, you can ensure that only AF and DoD approved applications are used on government computers.

Install DoD-approved anti-virus software to prevent many types of computer viruses and malicious logic. Remember to always exercise caution when downloading software from unknown sources. The DoD purchased anti-virus software license applies to all DoD computer systems. This allows all AF employees to download and install the most current anti-virus software from selected sources on their computers. Special provisions also allow the installation of this software on home computers to further prevent the spread of viruses.

The NCC plays an active role in establishing a virus monitoring capability on the base network. Where possible, install anti-virus software to alert NCC personnel every time a user inserts an "infected" disk into a network computer. This ensures that the offending virus is not only eliminated, but that it is not passed along to another computer. The NCC must work closely with the Wing IA Office to identify and contain virus threats. Once a virus or segment of malicious code is identified and contained, forward a report to the MAJCOM to alert other bases of the potential threat.

Damage Assessment

Once an unauthorized intrusion occurs, the NCC IP operators will most likely be tasked to conduct a damage assessment. Damage assessment is a method used to determine if network data was compromised, modified or destroyed. This may also include the introduction of false information into network databases. Review system audit logs and other sources to determine the extent of any intruder activity. Usually, an initial quick assessment is conducted to brief the DAA and other concerned parties, with a more thorough assessment to follow shortly thereafter. The assessment should be thorough enough to answer any questions regarding data integrity, but not delay mission operations

unnecessarily. Ensure that file and directory permissions have not been altered to allow unauthorized access at a later date and that no new accounts have been created.

If data integrity cannot be verified, reload all network software and user data to the last known good backup. Although the decision to rebuild the database is not always a popular one, it is a sure-fire method to guarantee data integrity. Before accomplishing a rebuild however, ensure you brief and receive the DAAs approval. The DAA has the final decision on whether to proceed. One of the most difficult choices of dealing with any intrusion is in determining the proper response. Before you can provide a timely recommendation to the system manager and DAA, you must carefully examine all evidence surrounding the intrusion. Only then will you be in a position to recommend a practical course of action and determine the proper response.

Determining the Proper Response

Determining the proper response to any network intrusion is dependent upon several factors. You should start by determining whether there was in fact a breach of security. An error or system fault may be mistakenly identified as an intrusion if you do not investigate thoroughly enough. If there is an intrusion, you must determine if any actual damage was done to the system, and the extent of that damage. You should preserve evidence for additional investigations or possible criminal prosecution by backing up the system; include any audit logs. Record all pertinent information, including dates and times. Do not delay in taking action merely for the sake of gathering information. Once the intruder is identified, lock his/her account and deny any further access. If root access was obtained, a back door may have been installed to access the system in case of detection.

In most cases, the response consists of merely reporting an attempted intrusion to the proper authorities. If the intrusion identifies serious deficiencies in the network security posture, take additional security measures to reduce or eliminate the threat immediately. A threat to one AF system is a threat to all systems; report all threats promptly. All AF agencies must work together to quickly identify and stop any unauthorized network intrusions. The DAA relies on the NCC and IP operators to provide timely and accurate assessments in order to make informed decisions. Only by keeping abreast of network activity can you accomplish this. AFSSI 5021, *Vulnerability and Incident Reportin*g, outlines the steps to take when an intrusion occurs.

INTERNAL CONTROL

Internal control defines the various mechanisms employed to provide internal system security. They may include but are not limited to access control methods, system identification and authentication programs, and system configuration. Internal control should reflect the requirements set forth by AF directives and DAA policy. The methods

you employ are largely determined by the security policy you create. As with any other endeavor, you should use common sense when deciding or recommending how much risk is acceptable. As a general rule of thumb, you should base your decision on the type of information you want to protect, system usability and the cost of required security measures.

You may employ one of two possible security postures: (1) a "default deny" posture to deny everything that is not specifically authorized, or (2) an "open" posture to allow everything that is not specifically denied. In either case, be consistent with your approach across the entire system. As more threats are identified every day, the default deny posture provides more assurance against unauthorized system access than other security strategies; it is the preferred AF strategy.

Access Control Methods

Employ Discretionary Access Control (DAC) to the maximum extent possible. DAC provides the ability to control access to information according to the authorization granted the user, as opposed to granting all users the same level of access (e.g., Mandatory Access Control). It provides the data owner with the ability to specify permissions (read, write, delete or execute) to information for each of their files and directories contained on the network. Files do not require internal classification labels because access is granted on a "system high" basis. This means that the system is classified at the highest level of information contained on it.

System Configuration

System configuration is an important, but often overlooked, element of internal security control. Many system administrators neglect to change factory defaults that may allow unauthorized access. Configurations that ease system setup and decrease installation times are not always conducive to good network security. Enable or configure the following information system features whenever possible: (1) Configure the system to prevent rapid retries when entering a password incorrectly by allowing several seconds to elapse before requesting another password. This delay deters any automated, high speed, trial-and-error attack on the password system. (2) Inform the user of the last successful access to the account and of any unsuccessful intervening access attempts following a successful login procedure. This aids in uncovering any unauthorized or attempted accesses that may have occurred. (3) Automatically log a user off the system if the workstation is inactive for a period of time. Require users to reauthenticate on an inactive terminal periodically after the initial authentication process.

There is no single method that encompasses all aspects of network security; therefore, they must be used together. In this way, they combine to provide a synergistic approach to the internal security of our networks. You must remain continually alert to any modifications that could affect security and correct them immediately.

ACCESS PRESERVATION

The base network is comprised of both physical and logical high value resources that must be protected from loss or damage. The value of these resources is determined locally, by the owning agency. These resources must be safeguarded in order to provide adequate network security. Physical resources include the network equipment itself, the physical storage media residing on or off the network, and the physical environment where the network servers are located. Logical resources encompass all data and software residing on the network. Since the NCC contains a large portion of these network resources, it should be located in an area with restricted access to prevent damage. All personnel within the NCC must limit unescorted entry to those on the Entry Authorization List. Base network users are responsible for the protection of physical and logical network resources at their locations.

Threats to base network resources may be classified as either intentional or unintentional. These threats may come from natural disasters, physical disasters, human threats or a combination of these items. You must plan properly to reduce or eliminate these threats and address any applicable contingency actions in the network certification and accreditation package. Consult AFI 31-209, *The Air Force Resource Protection Progra*m, and AFI 31-101 Volume I, *The Air Force Physical Security Program,* for additional information on protecting AF resources.

To protect logical resources, you should perform server backups daily and retain them for a minimum of 1 month. It is very important to ensure all critical information is backed up, not just the user data. Some types of information that should be considered for backup include system configuration information and profiles, user login scripts or other pertinent mission-oriented data. Once the information is backed up, you should also store all removable media in a safe location, preferably off-site. Backups should be stored off-site since they may be the only available source of data to restore network connectivity in the event of damage to the network facility. Never leave backup media lying around on desktops or in workstations where they may be lost, corrupted or damaged. Additional removable hard drives may be used as backup sources; however, you must remember to frequently update or "shadow" on-line media to ensure information is current. Mark, store and handle the backups as sensitive at a minimum. Protect them at the highest level of classification on the system.

In addition to backing up network information, you should develop contingency or emergency action plans to enhance system survivability. Since the base network is an essential part of the wing's operation, you should ensure these plans are consistent and integrated with other disaster recovery plans maintained by the wing and any associated organizations. A good contingency plan should cover the most common scenarios you are likely to encounter, as well as those that could have the greatest adverse impact on the

system. Test contingency plans thoroughly to ensure they work as planned and periodically thereafter to ensure they are still valid. Remember to document the results of the testing and implement any corrective actions necessary. Update the system accreditation package to reflect the extent that existing, or potential, weaknesses and vulnerabilities have been reduced or eliminated. You should refer to AFMAN 10-401 for further guidelines on contingency planning. As mentioned earlier, the development of contingency plans is a required part of the system certification and accreditation package. You must provide the DAA with reasonable assurance the system and the data it contains, can be recovered in the event of a catastrophic failure. There is no all-encompassing security method to eliminate all potential threats and vulnerabilities. However, you can greatly reduce them by incorporating a combination of both physical and logical security features.

AUTHENTICATION

One of the key aspects of identification and authentication is the use of unique user Identifications(ID) and passwords. You should keep user IDs unique by assigning them to only one person. This supports the concept of non-repudiation, which may become important if criminal charges are raised against a user. To avoid confusion, do not reissue an obsolete or expired user ID to another person for 1 year after its deletion.

On systems with a high user turnover, such as those in a training organization, you may decide to substitute generic user IDs (stuDent1, stuDent2, caDet001, caDet002, etc.) for user unique IDs. In this case, you should incorporate a tracking method, such as a log sheet, to match individual students with their generic user ID. Expire these passwords once the student no longer requires access.

Occasionally, mission accomplishment may necessitate using group user IDs and passwords. System administrators allowing group accounts and passwords must maintain individual accountability. A manual solution is to require account users to denote access date and time on a log sheet.

Prior to assigning user IDs and passwords, ensure the user has completed all required computer based training according to AFI 33-204, Information Protection Security Awareness, Training and Education (SATE) Program. This is normally coordinated through the Unit SATE Manager. Brief all users on the importance of protecting their user ID and password; reporting any suspicious activity; fraud, waste and abuse; and the use of system monitoring.

You may decide to use passwords generated by the information system or require users to generate their own password. In either case, use passwords with at least eight alphanumeric characters (upper and lower case) and at least one special character (@&+, etc.). AFMAN 33-223, Attachment 3, provides tips for effective password composition.

Discourage the use of passwords related to one's own personal identity, history or environment. Prohibit the use of generic passwords, such as "newpass1," unless the user changes the password immediately upon initial system login. There are many different types of password dictionaries which contain some of the more common words used to construct passwords. You can devise a relatively secure password by using a combination of both upper and lower case alphanumeric and special characters.

You should set system parameters to force users to change passwords every 90 days and establish a 6-month minimum password age on the system to prevent the use of former passwords. This ensures that users do not reuse old passwords. You should also limit the number of password entry attempts according to the sensitivity of the protected data (normally three attempts are permitted). When the maximum amount of password attempts is exceeded, lock out the user ID and/or terminal from use. This provides greater protection against automated password cracking programs by locking out the account after three unsuccessful login attempts.

Protect all passwords according to the sensitivity of the information or critical operations they protect (i.e., a password used to gain access to a SECRET network is itself classified SECRET). At a minimum, you must safeguard all passwords as "For Official Use Only" (FOUO).

User IDs provide an unclassified reference that can be displayed on printouts and audit trails without compromising passwords. Protect passwords during transmission at the same level required for the system or data that the password is protecting. Passwords are typically sent for authentication from a terminal to the system by a communications line. Physically protect or encrypt the line to prevent password disclosure by wiretapping and/or sniffers. You can also increase the password length or change it more often to mitigate this vulnerability.

Whenever you acquire a new hardware or software system, you must delete all unnecessary accounts and change all passwords before allowing user access. Many hardware components, such as servers, routers and other networking devices, come from the vendor preinstalled with a few standard user IDs (such as SYSTEM, TEST, MASTER, etc.) and passwords. These are primarily maintenance IDs that you must remove to prevent unauthorized system access. Strictly control any remaining "supervisory" IDs, and use them for emergency purposes only. Give system administration personnel, who have a valid need for supervisory access privileges, the permissions needed to perform their job. Ensure they use an ID that is unique to them and not the generic supervisory system ID. Test the system and delete all unneeded accounts and permissions prior to placing the system on-line. This will ensure that there are no "back doors" for unauthorized personnel to exploit.

Remove user IDs and passwords from an information system when the user is permanently transferred to another location or terminates employment. If a user is suspended from work or system access for any reason, remove or change the user ID and password immediately. Change a suspected or confirmed compromised password immediately. You should also review user ID and password access to systems every 6 months to help identify dormant user IDs and passwords. Delete, expire, suspend or change user IDs and passwords as appropriate. Establish procedures so the user must request access reinstatement from the system administrator or workgroup manager. Proper management of system passwords is very important and requires continuous attention.

User IDs and passwords are only one method available to identify and authenticate a user's identity. Passwords are popular because of their low cost; however, poor password use and management have left many systems vulnerable and are the key in the majority of system penetrations. This has encouraged the continued pursuit of more reliable methods.

To ensure effective and reliable internal security control, all security features must be used together in a mutually supportive arrangement. Remember to verify all features operate as expected. This will provide additional assurance to the DAA that all security features and controls are fully functional. If you do not have a strong user education program, it will not matter how secure you make your system through the use of internal controls. It is a commonly known fact that people are often the weakest link in the security chain. Without proper education, they may unwittingly provide unauthorized personnel with the keys to your system.

SECURITY TOOLS

Objective 1d: Identify general principles pertaining to security tools.

INFORMATION

IP software tools are divided into two categories: the AF Interim Toolset, and the Combat Information Transport System Base Information Protection Toolset.

AF INTERIM TOOLSET

Automated Security Incident Measurement (ASIM)

ASIM examines how the network is used, which services are used, and data flow sources and destinations for systems security purposes. It provides incident detection and support capabilities. ASIM is a non-intrusive network-monitoring device, not a firewall. ASIM

will not prevent unauthorized users from attempting to enter, or actually entering, an Air Force base network. It functions much like a "sniffer," collecting information and recording transactions for future reference. It identifies how users gain system access, any actions taken and host addresses by keystroke.

The ASIM software enhances network security by logging, analyzing and identifying suspicious network traffic. It uses a combination of three techniques of intrusion detection: attack signature recognition, anomaly detection and a vulnerability risk module.

ASIM software automatically assigns warning values from 1 to 10, with 1 having the lowest priority and 10 the highest. The program uses keywords, Internet Protocol addresses and service requests to assign these warning values. You should be cautious since warning values can be misleading (i.e., all FTP attempts will have the same warning value). In addition to the warning values, analysts should look at items such as the time of day, length of connection, access level, and files accessed to determine if unauthorized activity occurred. ASIM suspicious event reports are organized into five categories according to the degree of threat:

Category I. **I**ncidents are the most severe and involve any suspicious and unauthorized action where an attacker or user has gained root access.

Category II. Incidents are suspicious actions where an apparent attacker is trying to gain less than root access.

Category III. **I**ncidents involve unsuccessful intrusion attempts by an unauthorized user in the form of "sendmail" attack, daemon login, lp login or failed login.

Category IV. Incidents involve probing attacks in the form of Finger probe, FTP breakout, anonymous FTP, Telnet breakout or RPC.

Category V. **I**ncidents involve poor security practices. These include bad password choices, poor knowledge of local computer security policy and leaving a system unattended while the user is still logged in.

There are three types of logs maintained by the ASIM software: the incoming log, the outgoing log and the hot internet protocol log. The incoming log contains a listing of all connection requests coming into the protected domain, sorted by service. The outgoing log contains a listing of connection requests outside of the protected domain. The hot internet protocol log contains a listing, sorted by service, for the connections ASIM recorded coming into or going out of the protected domain. All logs contain the

connection index number, the warning value, the source Internet Protocol (or resolved host name) and the destination Internet Protocol (or resolved host name) for each recorded connection.

Crack

Crack, by design, locates weak, easily guessed passwords on UNIX systems. It uses the same guessing techniques and dictionaries that a cracker uses to break into a system, and the same algorithm a UNIX platform uses to generate its eight-character Data Encryption Standard encrypted passwords. Crack is slow (depending on the size of dictionaries) and ties up Central Processing Unit (CPU) resources, but it has a network option which allows it to automatically spread out the load of password cracking over several machines on a network to improve performance.

Once Crack completes a dictionary pass, it sweeps the list of users looking for the passwords it has cracked. If Crack correctly guesses a password, it marks the user and stores the cracked passwords in both plain text and encrypted forms in a feedback file. When Crack is subsequently run, it generates a list of users that have not changed their passwords since the last run-time.

Washington University (WU) Archive File Transfer Protocol Daemon (WU-FTDP)

WU-FTPD is a secure replacement FTP server for UNIX systems. It adds logging of transfers, logging of commands, on the fly compression and archiving, classification of users by type and location, per class limits, per directory upload permissions, restricted guest accounts, and systems wide and per directory messages. Once installed, this package is especially useful in enhancing security on FTP servers used to support anonymous FTP users.

Information capabilities include the ability to display banners at login time, display messages when a user changes to certain directories, and identify “readme” files to users at login time or when they change specified directories. The logging capabilities provide the ability to specify the logging of all commands issued by users of a certain type. In addition, it allows the ability to log all file transfers by users of a certain type.

The miscellaneous category allows specifying aliases for certain directories and change directory search strings. In addition, you can specify whether compression is enabled for a given type of user. System administrators can specify a number of permissions based on user type and class. These permissions include allowing or denying the commands chmod, delete, write, rename, umask and upload.

Transmission Control Protocol (TCP) Wrapper

TCP Wrapper is a network monitoring program that monitors incoming requests for programs like telnet, finger, FTP, exec, rsh, rlogin, TFTP, talk, comsat and other services that have a one-on-one mapping onto executable files. Whenever a request for one of the Internet services arrives, the INETD daemon runs TCP Wrapper (TCPD) instead of the desired server. TCP Wrapper logs the requests and provides a number of add-on services including a limited form of access control and some sanity checks. These logs are excellent for spotting anyone who has been in your system. Once installed and properly configured, TCP Wrapper reduces a system's exposure to intruders. This mitigates their ability to compromise the security of a system by exploiting software vulnerabilities.
TCP Wrapper sends its logging information to the syslog daemon. Determine the disposition of the wrapper logs by the syslog configuration file (usually located in /etc/syslog.conf). Messages are written to files, to the console or forwarded to @loghost. When access control is enabled, a list is checked to see if the source of a connection is allowed or denied access to a service. If the service is denied, the connection is aborted. If the service is allowed, then the normal daemon is executed. When name checking is turned on, the wrapper verifies that the name to address mapping is the same as the address to name mapping. If there is any discrepancy, the wrapper concludes it is dealing with a host pretending to have someone else's name. If this is detected, it is logged and the connection aborted. Document all steps taken to correct security deficiencies.

Security Profile Inspector (SPI)

SPI is a menu driven software package that helps IP technicians and system administrators keep their system secure. It includes utilities that check binary files used by the operating system to ensure authenticity and patch currency. It also has utilities that scan a disk for key configuration files and directories and look for modifications to the file attributes (such as changes to permission, ownership and dates). The file system can be scanned for undesired links, permission, ownership, dates, and additional or deleted files. It checks network configuration files, password related files, user profile files, dormant user accounts and public directories that support network access, including FTP. The menu-based user interface brings together process status, output report management, run-time parameter management and job scheduling. The menu options can be used to produce a summary of vulnerabilities and weaknesses on systems.

Each security function of SPI produces an output report detailing the findings. These reports are saved in a sub-directory corresponding to the chosen security function. System administrators have these options: (1) view the contents of the reports, (2) print the contents of the reports and (3) make reports for transfer to either the archive or the trash sub-directories. By default, the SPI notifies operators of completed output reports by e-mail. These reports may also be viewed through the SPI output report manager. Document all steps taken to correct security deficiencies.

Message Digest 5 (MD5)

MD5 provides a reliable, unique file signature to ensure that a file has not changed. Even a minor file change causes a significant change in its digital signature and is much harder to fake or "spoof." The slightest variation to a file or character string changes the MD5 algorithm so that the encryption is radically different. The integrity of designated message traffic is ensured by first recording the signature of the message before sending it to recipients. Then the message and recorded signature are sent separately to recipient(s). The recipient(s) then verifies the integrity of the message by running MD5 against it and comparing signatures.

Tripwire

Tripwire is an integrity-monitoring program for UNIX systems. It uses checksum and signature routines to detect changes to files and monitors selected items of system maintained information. Tripwire also looks for changes in permissions, links, and sizes of files and directories. In addition, it can detect additions or deletions of files from watched directories. Tripwire sends a log file to system administrators anytime it detects a change. When changes are noticed that an administrator did not make, an intruder has most likely entered the system.

The Tripwire database contains one entry for each file scanned. This includes the file's path and name, size, date and time stamp, signature information, and a pointer back to the "th.config" line that generated the entry. When executed, Tripwire logs any differences between a specific file and the associated database entry in a log file. These differences can indicate if an intrusion occurred. Trip Wire can be configured to e-mail the detection of non-ordinary events to system administrators.

COMBAT INFORMATION TRANSPORT SYSTEM NETWORK MANAGEMENT SYSTEM/BASE INFORMATION PACKAGE (CITS NMS/BIP)

This program is providing a means to transport information, while ensuring the protection of both the information and its means of transport. The Air Force must be able to support air, land, sea, space and information operational environments while conducting offensive and defensive combat operations. Communication professionals must protect information resources and ensure information needed to perform the Air Force mission is readily available. CITS is composed of two distinct portions, NMS and BIP.

Network Management System

The CITS program installs a Network Management System (NMS) over the information transport system to provide systems and configuration management of local area networks at host and tenant organizations on the base. Consolidation of network

management functions into a single unified network management capability is not only a highly desired capability, but a necessary one. With the tremendous growth in AF networks at a time when manpower resources have been declining, it is necessary to manage the network resources in an efficient manner. One of the goals of the CITS program is to consolidate these network management and maintenance functions and provide unified networking services. The NMS provides trouble reporting functions and automated trouble ticket generation. System configuration, changes to system configurations, network components, applications running on the network and entities using the network can be tracked, recorded and controlled through the NMS functions. Network performance determination is possible with NMS and performance analysis allows the administrators to make adjustments to the network achieving optimal performance and increase user satisfaction.

Base Information Protection

Base Information Protection is critical to the Air Force mission. The **CITS** program provides an information firewall to ensure intruders or hackers are kept from accessing base networks and critical information. BIP provides the information protect tools for each Air Force base to detect, deter, isolate, contain, reconstitute, and recover from information systems and network security intrusions or attacks. This capability is managed by the base network control center through the NMS. It is important that Air Force information resources are protected from unauthorized access. Likewise, it is important that the Air Force not only protect information resources, but also protect resources for storing, accessing and disseminating the information. CITS NMS/BIP uses multiple hardware and software components to meet its objectives. For boundary protection, it uses a series of CISCO routers and Secure Computing Corp's Sidewinder firewall. It uses the Axent Intruder Alert (ITA) server agent to provide intrusion and misuse detection. Internal control is accomplished by the Axent Enterprise Security Manager (ESM) and the Internet Safe Suite (ISS) server agents. It also uses a series of internal and external ethernet switches, proxy servers, protocol analyzers and a Network Management Server. It will provide a robust defense and in-depth protection strategy for all AF installations. Figure 1-2 shows the CITS NMS/BIP logical design.

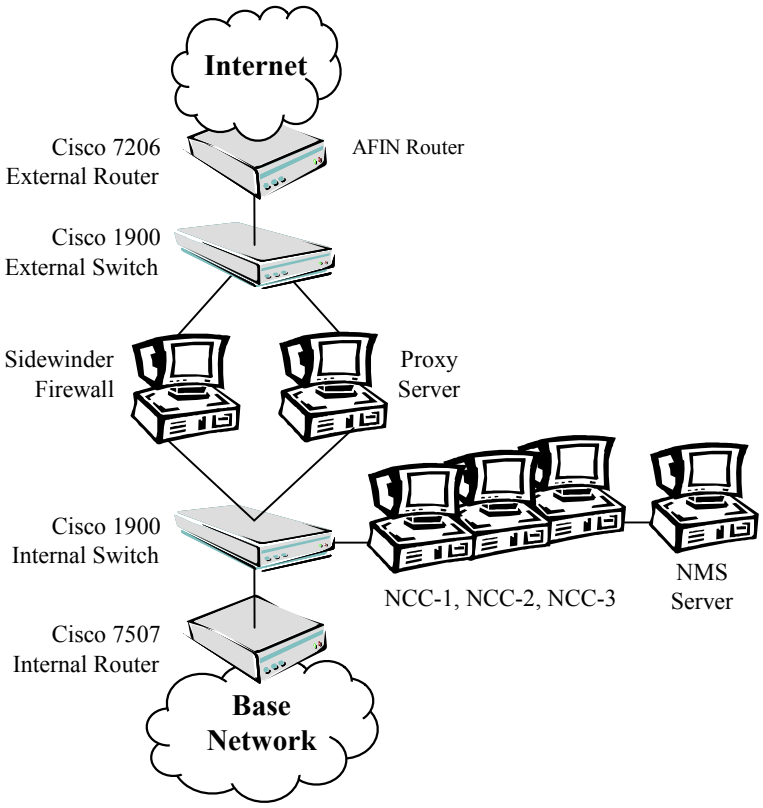

Figure 1-2. The CITS NMS/BIP Phase I Design Concept.

The AF suite of Information Protection tools provides the most reliable means of securing AF assets to date. As we continue to mature our information systems however, more robust tools and protection strategies will be needed. It is no longer good enough to run one or two security tools and expect our problems to be solved. There is no single solution to the security issues we face. We must develop an all encompassing plan or strategy that deals with a wide range of security issues.

The CITS NMS/BIP program will enable us to better manage and secure our network resources, but it is just the beginning. If we are to be truly successful, we must continually reevaluate our protection tools, methods and strategies. One thing is certain, no matter which technology we choose, the human factor will continue to remain a constant. You are the most important tool in the AF arsenal and the keystone to ensuring U.S. information superiority.

SUMMARY

The techniques described in this chapter provide the best method of layered defense for our networks today. However, if we are to maintain our information superiority in this fast paced electronic environment, we must constantly look for better methods of

protecting our resources. Only by keeping alert to adverse trends and vulnerabilities can we keep the enemy at bay.

CHAPTER TWO

NETWORK DESIGN

OBJECTIVES

2a: Using a contingency metric and working as a team member, develop contingency plans for network infrastructure IAW Performance Specification II-2a.

2b: Using a topology handout develop addressing scheme IAW Performance Specification II-2b.

2c: Using microcomputer develop a Request For Service (RFS) IAW Performance Specification II-2c.

2d: Using a topology handout and a AF Form 3215 (CSRD) and working as a team member, assess the impact of requirements documents IAW Performance Specification II-2d.

DEVELOP CONTINEGENCY PLANS

Objective 2a: Using a contingency metric and working as a team member, develop contingency plans for network infrastructure IAW Performance Specification II-2a.

INFORMATION

The contingency planning process develops plans for disaster recovery to provide reasonable assurance that critical mission support can continue, or resume within a specified time frame, if normal system operations are interrupted. These plans outline the procedures to follow in the event of a catastrophic occurrence, how to reduce the impact to the information system from such occurrences and how to expeditiously recover from the occurrence with as little operational and financial impact as possible.

Contingency plans also address procedures that minimize the additional security risk imposed by the partial or complete loss of information system security mechanisms. Contingency plans are required for mission critical and mission essential systems and are highly recommended for mission-impaired systems. Contingency plans must also be developed for unique systems or systems that rely on unique software.

CONTINGENCY PLANS

Computer Security managers are responsible for assuring the adequacy of contingency plans for Automated Information Systems (AIS) under their area of responsibility. Although you may not actually write the plans, you may be called upon for guidance.

The contingency planning process develops plans for disaster recovery to provide reasonable assurance that critical mission support can continue, or resume within a specified time frame, if normal system operations are interrupted. These plans outline the procedures to follow in the event of a catastrophic occurrence, how to reduce the impact to the information system from such occurrences, and how to expeditiously recover from the occurrence with as little operational and financial impact as possible.

Such plans are consistent with disaster recovery plans maintained by wing and unit organizations. The functional Office of Primary Responsibility (OPR) or data automation planner, with security guidance from the Computer System Manager (CSM), will develop plans to ensure the survival and timely recovery of the mission-critical and mission-essential systems. These plans identify which AISs are most vital and the level of protection necessary to ensure mission accomplishment. Manual procedures must be developed to ensure mission requirements are met during periods when AIS support is not available. Contingency plans will ensure AIS security controls function reliably or that adequate backup functions are in place to ensure security functions are maintained continuously during interrupted service. You must also ensure that procedures are in place to allow recovery in the event data is modified or destroyed. AFMAN 10-401 provides guidelines and procedures for the development of contingency plans for critical AISs.

Contingency plans also address procedures that minimize the additional security risk imposed by the partial or complete loss of information system security mechanisms. Contingency plans are required for mission critical and mission essential systems and are highly recommended for mission impaired systems. Contingency plans must also be developed for unique systems or systems that rely on unique software. Although the contingency plan is prepared by the functional user, the Certifying Official must determine the contingency requirements for the system, ensure they are included in the contingency plan, and identify the need for contingency planning in the system security policy.

No AIS is exempt from potential failure. Contingency plans provide safeguards and controls that ensure continuity of operations in the event of a disaster, or restore operations in the event of an AIS failure.

Contingency plans have three phases: backup/preparation, emergency response, and recovery. The scope and contents of the plans will vary depending on the criticality of the AIS. Each owner/user of an AIS should be aware of their responsibilities within their unit's contingency plans. To ensure that all personnel are aware of their contingency responsibilities, the plans should be reviewed at least annually, tested, and the results assessed on a regular and recurring basis. The plans should be revised as needed.

A contingency plan is "a plan maintained for emergency response, backup operations, and post-disaster recovery for an AIS, as a part of its security program, that will ensure the availability of critical resources and information facilitates the continuity of operations in an emergency" (Ref: AFMAN 33-270). Emergency plans, backup procedures, and recovery plans play a specific role, but all are grouped under the heading of contingency plans.

Emergency Plan

An emergency plan is the response phase of contingency plans—things to do while the emergency is in progress. The plans must address unique deployed operating conditions, such as temperature and humidity variations, power fluctuations, and dust, if appropriate. Depending on your location, facilities, and other variables, the emergency plans should contain both a continuity of operations plan and responses to take while the emergency is in progress. These plans should include emergency destruction and declassification procedures, alternate power sources, partial or degraded AIS operation, and approved methods of disposal. The plan should include a description of the baseline environment, additional safeguards and controls for varying threats, and minimum operating conditions. The baseline environment description includes the procedures, conditions, and objects that affect the development, operation, and maintenance of an AIS. We cannot tell you exactly what the plan should have because every AIS mission is different. For example, an early warning system needs a more comprehensive plan than the automated card catalog at the base library. The question you need to answer is “how critical or essential is this AIS I am trying to protect?”

Backup Procedure

Of primary consideration for continuity of operations is the existence of backup procedures for AISs. These procedures include provisions made for the recovery of information and software libraries, and for the restart or replacement of AIS equipment after an AIS failure or disaster. Backup procedures are part of every contingency plan and are accomplished as a defensive measure. Maintain a copy of your backups at an off-site location. It will do you no good to have a plan if, for example, a fire destroys both your facility and your backups within it. When you perform backup procedures, you are preparing for the worst while hoping that it never happens.

Disaster Recovery Plan

A disaster recovery plan involves those actions necessary to recover from a contingency. It includes a specific recovery response before operations can continue. For example: recovering from a hurricane at Keesler AFB, MS is different from a blizzard recovery at Minot AFB, ND. Chances are, Minot will still have electricity after a blizzard, but

Keesler will not have electricity after a hurricane. The steps you take to recover from a disaster depend on the type of disaster incurred.

INDIVIDUAL RESPONSIBILITIES

Functional Manager

The functional manager or OPR is the principal party accountable for the information under their control. The functional manager validates and approves plans developed by the CSM. Their focus is to ensure their information is protected.

Computer System Manager (CSM)

The CSM ensures contingency plans are developed for mission-critical and mission-essential AISs, and that COMPUSEC considerations are included in contingency plans. He or she must review operating instructions and procedures regularly to ensure they are current. The CSM must also ensure local security manuals, operating instructions, and contingency plans are reviewed annually and updated as necessary. Once developed, the CSM maintains copies of contingency and recovery plans for each AIS, and provides a copy of the contingency and recovery plan to the Functional OPR supported by the AIS. The CSM oversees the contingency planning process for all AISs under their control.

End Users

End users must maintain familiarity with the plans through periodic review. This ensures that they perform the necessary backups in support of plans, and can actually implement the contingency and recovery plans in emergency situations and during dry runs.

DEVELOPING, COORDINATING, TESTING, EVALUATING AND IMPLEMENTING CONTINGENCY PLANS

Ensure that emergency plans for each AIS are coordinated with other base agencies, as required. This may include other security professionals on base, as well as the fire department, safety office and disaster preparedness. They should also be coordinated internally with plans and programs personnel, other security program managers, safety, equipment custodians and facilities managers. Why? There are three very good reasons:

1. These other agencies/offices might be tasked to do something unrealistic.

2. They might have a suggestion on a better way to do something.

3. They cannot be expected to accomplish a task if they are not aware they are supposed to be doing it. Contingency and recovery plans provide reasonable measures to provide continuity of support to all AIS users. Plans should be as realistic as possible.

You can help those responsible for developing contingency plans for their AISs by providing direction through base and unit operating instructions, directives and plans. Let people know what is expected of them, using the following items as guidelines.

1. Develop guidelines to help units create their emergency response procedures
2. Plan and test backup plans
3. Plan and provide support in recovery procedures
4. Task your office in responding to emergency situations. Let those people who depend on you for support know you can be trusted for support as well
5. Prepare guidelines for determining mission-essential workloads
6. Provide guidance to determine backup requirements
7. Assist in developing procedures for off-site operations. This might require some effort on your part to help them research and weigh the alternatives
8. Assist in development of plans for recovery actions after a disruptive event
9. Assist in identifying and determining cost justification of recovery alternatives available to management
10. The Wing IA Office should consider and provide methods for planning, testing, training and evaluating. They should consider methods for the following items:
    a. Identifying mission workload
    b. Scheduling backup of critical software/information
    c. Storing and protecting backup software/information
    d. Periodically test backups
    e. Training office personnel
    f. Work scheduling during recovery operations
    g. Reconstruction of information, software, etc.

The basic concepts of contingency planning are preparation through planning and backup of information, emergency response actions and disaster recovery procedures. Contingency planning is required to assure the availability, integrity and confidentiality of information and AISs on your installation. There are many individuals involved in the development, training, testing and evaluation of the contingency plans, but the CSM and/or functional OPR retain(s) overall responsibility for ensuring their completion.

Tailor emergency response plans to fit specific situations (for instance: fire, bomb threat, etc.), yet be flexible enough to apply to any situation that may occur.

Develop Addressing Schema

Objective 2b: Using a topology handout develop addressing scheme IAW Performance Specification II-2b.

INFORMATION

SUBNET DESIGN CONSIDERATIONS

The deployment of an addressing plan requires careful thought on the part of the network administrator. There are four key questions that must be answered before any design should be undertaken:

1. How many total subnets does the organization need today?
2. How many total subnets will the organization need in the future?
3. How many hosts are there on the organization's largest subnet today?
4. How many hosts will there be on the organization's largest subnet in the future?

The first step in the planning process is to take the maximum number of subnets required and round up to the nearest power of two. When performing this assessment, it is critical that the network administrator always allow adequate room for future growth.

The second step is to make sure that there are enough host addresses for the organization's largest subnet.

The final step is to make sure that the organization's address allocation provides enough bits to deploy the required subnet addressing plan.

The All-0s Subnet and The All-1s Subnet

When subnetting was first defined in Request for Comment (RFC) 950, it prohibited the use of the all-0s and the all-1s subnet. The reason for this restriction was to eliminate situations that could potentially confuse a classful router.

Regarding the all-1s subnet, a router requires that each routing table entry include the prefix-length so that it can determine if a broadcast (directed or all-subnets) should be sent only to the all-1s subnet or to the entire network. For example, when the routing table does not contain a mask or prefix-length for each route, confusion can occur because the same broadcast address (193.1.1.255) is used for both the entire network 193.1.1.0/24 and the all-1s subnet 193.1.1.224/27. This is illustrated in Figure 2-1.

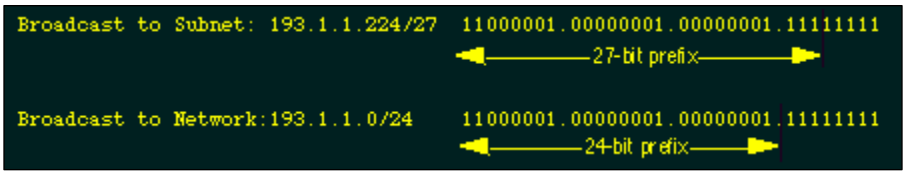

Figure 2-1. Identifying a Broadcast to the All-1s Subnet and the Entire Network.

With the development of routing protocols that supply the mask or prefix-length with each route, the address space defined by the all-0s and all-1s subnets is once again usable despite the cautions in RFC 950. There are two factors that determine when these subnets can be used.

- The interior gateway protocol (IGP)
- The capabilities of other routers in the organization's network.

To support the deployment of the all-0s and all-1s subnets, the IGP must carry extended-network-prefixes. RIP-1 does not carry extended-network-prefixes.

VARIABLE LENGTH SUBNET MASKS (VLSM)

In 1987, RFC 1009 specified how a subnetted network could use more than one subnet mask. When an IP network is assigned more than one subnet mask, it is considered a network with "variable length subnet masks" since the extended-network-prefixes have different lengths.

When using RIP-1, subnet masks have to be uniform across the entire network-prefix. RIP-1 allows only a single subnet mask to be used within each network number because it does not provide subnet mask information as part of its routing table update messages.

Route Aggregation

VLSM also allows the recursive division of an organization's address space so that it can be reassembled and aggregated to reduce the amount of routing information at the top level. Conceptually, a network is first divided into subnets, some of the subnets are further divided into sub-subnets. This allows the detailed structure of routing information for one subnet group to be hidden from routers in another subnet group.

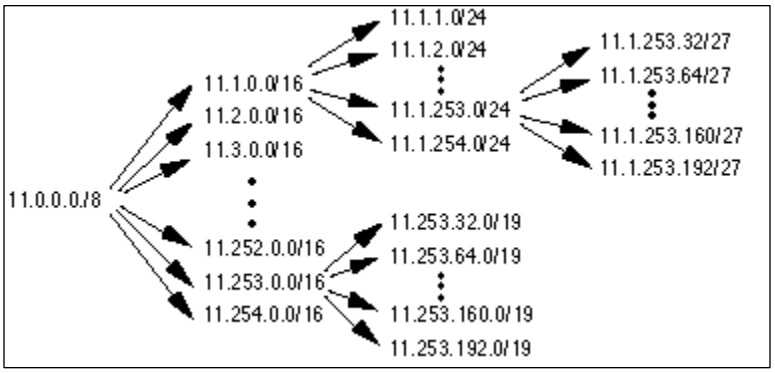

Figure 2-2. VLSM Permits the Recursive Division of a Network Prefix.

In Figure 2-2, the 11.0.0.0/8 network is first configured with a /16 extended-network-prefix. The 11.1.0.0/16 subnet is then configured with a /24 extended-network-prefix and the 11.253.0.0/16 subnet is configured with a /19 extended-network-prefix. Note that the recursive process does not require that the same extended-network-prefix be assigned at each level of the recursion.

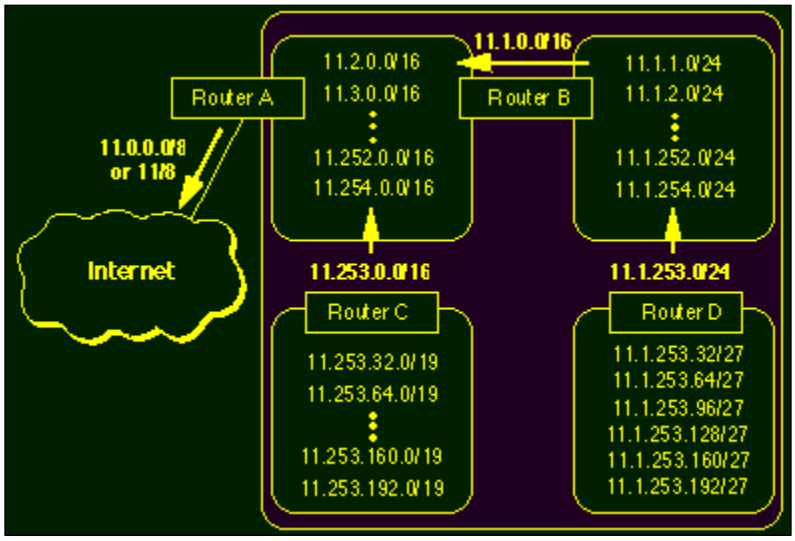

Figure 2-3. VLSM Permits Route Aggregation - Reducing Routing Table Size.

Figure 2-3 illustrates how a planned and thoughtful allocation of VLSM can reduce the size of an organization's routing tables. Notice how Router D is able to summarize the six subnets behind it into a single advertisement (11.1.253.0/24) and how Router B is able to aggregate all of subnets behind it into a single advertisement. Likewise, Router C is able to summarize the six subnets behind it into a single advertisement (11.253.0.0/16).

Finally, since the subnet structure is not visible outside of the organization, Router A injects a single route into the global Internet's routing table -11.0.0.0/ 8 (or 11/8).

VLSM Design Considerations

When developing a VLSM design, the same set of design decisions must be made at each level of the hierarchy.

Assume that a network is spread out over a number of sites. For example, if an organization has three bases today it probably needs 3-bits of subnetting ($2^3 = 8$) to allow the addition of more bases in the future. Now, within each base, there is likely to be a secondary level of subnetting to identify each squadron. Finally, within each squadron, a third level of subnetting might identify each of the individual workgroups. Following this hierarchical model, the top level is determined by the number of bases, the mid-level is based on the number of squadrons at each site, and the lowest level is determined by the "maximum number of subnets/maximum number of users per subnet" in each building.

When the addressing plan is deployed, the addresses from each site will be aggregated into a single address block that keeps the backbone routing tables from becoming too large.

Requirements for the Deployment of VLSM

The successful deployment of VLSM has two prerequisites.

- The routing protocols must carry extended-network-prefix information with each route advertisement.
- For route aggregation to occur, addresses must be assigned so that they have topological significance.

Topologically Significant Address Assignment.

Hierarchical routing requires that addresses be assigned to reflect the actual network topology. If addresses do not have a topological significance, aggregation cannot be performed and the size of the routing tables cannot be reduced.

VLSM Example

Given that an organization has been assigned the network number 140.25.0.0/16 and it plans to deploy VLSM. Figure 2-4 provides a graphic display of the VLSM design for the organization.

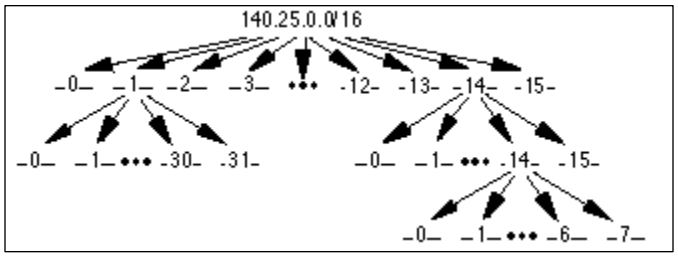

Figure 2-4. Address Strategy for VLSM Example.

The first step of the subnetting process divides the base network address into 16 equal-sized address blocks. Then Subnet #1 is divided into 32 equal-sized address blocks and Subnet #14 is divided into 16 equal-sized address blocks. Finally, Subnet #14-14 is divided into 8 equal-sized address blocks.

Define the 16 Subnets of 140.25.0.0/16. The first step in the subnetting process divides the base network address into 16 equal-size address blocks. This is illustrated in Figure 2-5.

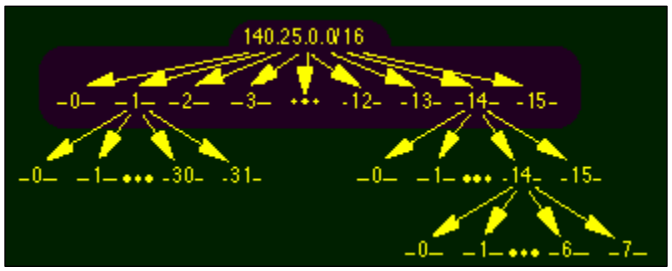

Figure 2-5. Define the 16 Subnets for 140.25.0.0/16.

Since $16 = 2^4$, four bits are required to uniquely identify each of the 16 subnets. This means that the organization needs four more bits, or a /20 in the extended-network-prefix to define the 16 subnets of 140.25.0.0/16. Each of these subnets represents a contiguous block of 2^{12} (or 4,096) network addresses.

The 16 subnets of the 140.25.0.0/16 address block are as follows. The subnets are numbered 0 through 15. The italicized portion of each address identifies the extended-network- prefix, while the **bold** digits identify the 4-bits representing the subnet-number field:

Base Network: 10001100.00011001 .00000000.00000000 = 140.25.0.0/16
Subnet #0: *10001100.00011001*.**0000** 0000.00000000 = 140.25.0.0/20
Subnet #1: *10001100.00011001*.**0001** 0000.00000000 = 140.25.16.0/20
:
:
Subnet #15: *10001100.00011001*.**1111** 0000.00000000 = 140.25.240.0/20

Define the Host Addresses for Subnet #3 (140.25.48.0/20). Let's examine the host addresses that can be assigned to Subnet #3 (140.25.48.0/20). This is illustrated in Figure 2-6.

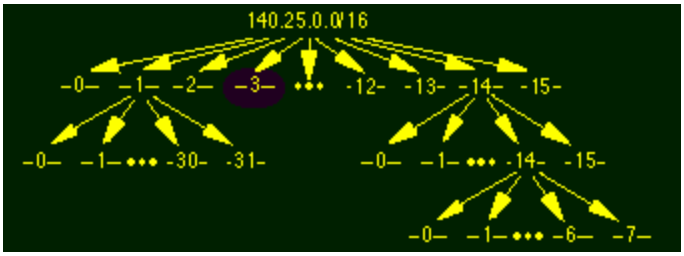

Figure 2-6. Define the Host Addresses for Subnet #3 (140.25.48.0/20).

Since the host-number field of Subnet #3 contains 12 bits, there are 4,094 valid host addresses (2^{12} -2) in the address block. The hosts are numbered 1 through 4,094.

The valid host addresses for Subnet #3 are given below. The italicized portion of each address identifies the extended-network-prefix, while the **bold** digits identify the 12-bit host-number field:

Subnet #3: 10001100.00011001.0011 0000.00000000 = 140.25.48.0/20
Host #1: *10001100.00011001.0011* **0000.00000001** = 140.25.48.1/20
:
:
Host #4094: *10001100.00011001.0011* **1111.11111110** = 140.25.63.254/20

The broadcast address for Subnet #3 is the all 1's host address or:
10001100.00011001.0011 **1111.11111111** = 140.25.63.255

Define the Sub-Subnets for Subnet #14 (140.25.224.0/20). After the base network address is divided into sixteen subnets, Subnet #14 is further subdivided into 16 equal-size address blocks. This is illustrated in Figure 2-7.

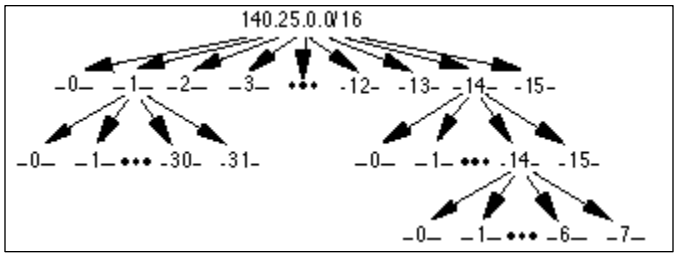

Figure 2-7. Define the Sub-Subnets for Subnet #14 (140.25.224.0/20).

Since 16 = 2^4 , four more bits are required to identify each of the 16 subnets. This means that the organization will need to use a /24 as the extended-network-prefix length.
The 16 subnets of the 140.25.224.0/20 address block are given below. The subnets are numbered 0 through 15. The italicized portion of each sub-subnet address identifies the extended-network-prefix, while the **bold** digits identify the 4-bits representing the sub-subnet-number field:

Subnet #14: 10001100.00011001.1110 0000.00000000 = 140.25.224.0/20
Subnet #14-0: *10001100.00011001.1110* **0000** .00000000 = 140.25.224.0/24
Subnet #14-1: *10001100.00011001.1110* **0001** .00000000 = 140.25.225.0/24
:
:
Subnet #14-15: *10001100.00011001.1110* **1111** .00000000 = 140.25.239.0/24

Define Host Addresses for Subnet #14-3 (140.25.227.0/24). Let's examine the host addresses that can be assigned to Subnet #14-3 (140.25.227.0/24). This is illustrated in Figure 2-8.

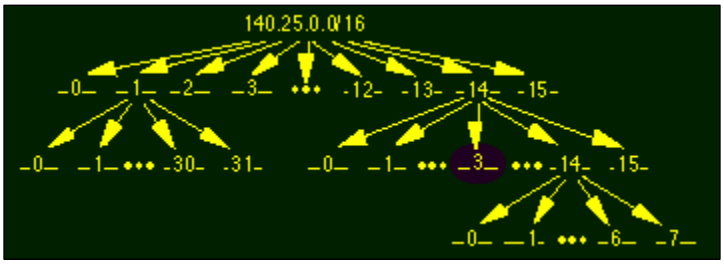

Figure 2-8. Define the Host Addresses for Subnet #14-3 (140.25.227.0/24).

Each of the subnets of Subnet #14-3 has 8 bits in the host-number field. This means that each subnet represents a block of 254 valid host addresses (2^8 -2). The hosts are numbered 1 through 254.

The valid host addresses for Subnet #14-3 as follows. The italicized portion of each address identifies the extended-network-prefix, while the **bold** digits identify the 8- bit host-number field:

Subnet #14-3: 10001100.00011001.11100011 .00000000 = 140.25.227.0/24
Host #1 *10001100.00011001.11100011* .**00000001** = 140.25.227.1/24
Host #2 *10001100.00011001.11100011* .**00000010** = 140.25.227.2/24
.
.
Host #254 *10001100.00011001.11100011* .**11111110** = 140.25.227.254/24

The broadcast address for Subnet #14-3 is the all 1's host address or:
10001100.00011001.11100011.**11111111** = 140.25.227.255

Define the Sub 2 -Subnets for Subnet #14-14 (140.25.238.0/24). After Subnet #14 was divided into sixteen subnets, Subnet #14-14 is further subdivided into 8 equal-size address blocks. This is illustrated in Figure 2-9.

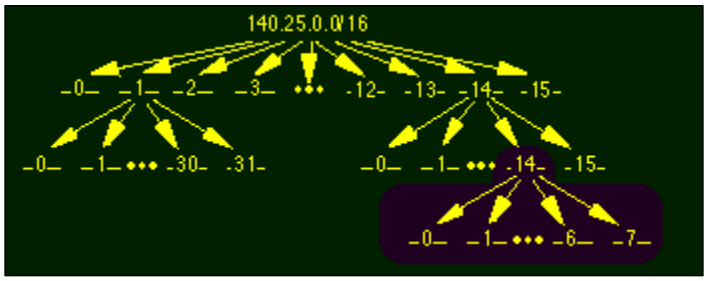

Figure 2-9. Define the Sub 2 -Subnets for Subnet #14-14 (140.25.238.0/24).

Since 8 = 2^3 , three more bits are required to identify each of the 8 subnets. This means that the organization will need to use a /27 as the extended-network-prefix length.

The 8 subnets of the 140.25.238.0/24 address block are given below. The subnets are numbered 0 through 7.

Subnet #14-14: 10001100.00011001.11101110 .00000000 = 140.25.238.0/24
Subnet#14-14-0: *10001100.00011001.11101110*.**000** 00000 = 140.25.238.0/27

Subnet#14-14-7: *10001100.00011001.11101110*.**111** 00000 = 140.25.238.224/27

Define Host Addresses for Subnet #14-14-2 (140.25.238.64/27). Let's examine the host addresses that can be assigned to Subnet #14-14-2 (140.25.238.64/27). This is illustrated in Figure 2-10.

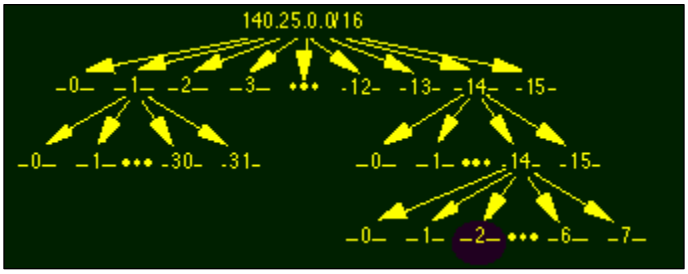

Figure 2-10. Define the Host Addresses for Subnet #14-14-2 (140.25.238.64/27).

Each of the subnets of Subnet #14-14 has 5 bits in the host-number field. This means that each subnet represents a block of 30 valid host addresses (2^5 -2). The hosts will be numbered 1 through 30.

The valid host addresses for Subnet #14-14-2 are given below. The italicized portion of each address identifies the extended-network-prefix, while the **bold** digits identify the 5-bit host-number field:

Subnet#14-14-2: 10001100.00011001.11101110.010 00000 = 140.25.238.64/27
Host #1 *10001100.00011001.11101110.010* **00001** = 140.25.238.65/27
.
.
Host #30 *10001100.00011001.11101110.010* **11110** = 140.25.238.94/27

The broadcast address for Subnet #14-14-2 is the all 1's host address or:
10001100.00011001.11011100.010 **11111** = 140.25.238.95

CLASSLESS INTER-DOMAIN ROUTING (CIDR)

By 1992, the exponential growth of the Internet was beginning to raise serious concerns among members of the IETF about the ability of the Internet's routing system to scale and support future growth. These problems were related to:

- The near-term exhaustion of the Class B network address space

- The rapid growth in the size of the global Internet's routing tables
- The eventual exhaustion of the 32-bit IPv4 address space

The response to these immediate challenges was the development of the concept of Supernetting or Classless Inter-Domain Routing (CIDR).

CIDR was officially documented in September 1993 in RFC 1517, 1518, 1519 and 1520. CIDR supports two important features that benefit the global Internet routing system:

- CIDR eliminates the traditional concept of Class A, Class B and Class C network addresses. This enables the efficient allocation of the IPv4 address space.
- CIDR supports route aggregation where a single routing table entry can represent the address space of perhaps thousands of traditional classful routes.

CIDR Promotes the Efficient Allocation of the IPv4 Address Space

CIDR eliminates the traditional concept of Class A, Class B and Class C network addresses replacing them with the generalized concept of a "network-prefix." Routers use the network-prefix, rather than the first 3 bits of the IP address, to determine the dividing point between the network number and the host number.

In the CIDR model, each piece of routing information is advertised with a bit mask (or prefix-length). For example, a network with 20 bits of network-number and 12-bits of host-number would be advertised with a 20-bit prefix length (a /20). The clever thing is that the IP address advertised with the /20 prefix could be a former Class A, Class B or Class C.

In a classless environment, prefixes are viewed as bitwise contiguous blocks of the IP address space. A /20 prefix can be assigned to a traditional Class A, Class B or Class C network number. Figure 2-11 shows how each of the following /20 blocks represent 4,096 host addresses - 10.23.64.0/20, 130.5.0.0/20, and 200.7.128.0/20.

Traditional A	10.23.64.0/20	00001010.00010111.01000000.00000000
Traditional B	130.5.0.0/20	10000010.00000101.00000000.00000000
Traditional C	200.7.128.0/20	11001000.00000111.10000000.00000000

Figure 2-11. Bitwise Contiguous Address Blocks.

Host Implications for CIDR Deployment

It is important to note that there may be severe host implications when you deploy CIDR based networks. Since many hosts are classful, their user interface will not permit them to be configured with a mask that is shorter than the "natural" mask for a traditional classful address. For example, the software executing on each end station might not allow a traditional Class C (200.25.16.0) to be configured with a 20-bit mask since the natural mask for a Class C network is a 24-bit mask.

CIDR is Similar to VLSM

If CIDR appears to have the familiar look and feel of VLSM, you are correct! CIDR and VLSM are essentially the same thing since they both allow a portion of the IP address space to be recursively divided into subsequently smaller pieces. The difference is that with VLSM, the recursion is performed on the address space previously assigned to an organization and is invisible to the global Internet. CIDR, on the other hand, permits the recursive allocation of an address block by an Internet Registry to a high-level ISP, to a mid-level ISP, to a low-level ISP and finally to a private organization's network.

REQUEST FOR SERVICE (RFS)

TELECOMMUNICATIONS SERVICE REQUEST (TSR)

TELECOMMUNICATIONS SERVICE ORDER (TSO)

Objective 2c: Using microcomputer develop a Request For Service (RFS) IAW Performance Specification II-2c.

INFORMATION

REQUEST FOR SERVICE

When a customer requires an activation, deactivation, or change on a circuit, trunk, link or system, they must inform their servicing systems control facility. The customer will advise what they need and the Systems Control Facility (SCF) will prepare the RFS. It will include the type of service required, its purpose, the location of the required equipment, the hours of operation of the circuit, a point of contact and other pertinent information. The SCF will forward the RFS to the servicing Telecommunications Control Office (TCO).

TELECOMMUNICATIONS SERVICE REQUEST

Once an RFS is received by the TCO, it is validated and the TCO prepares a TSR. The information contained in the TSR includes: service date, nature of requirement, type of action required, funding code, restoration priority (if any), point of contact, user locations, details of service and user equipment plus the type of service. Once the TSR is completed, the TCO will submit the TSR to DISA. The TCO is the only office authorized to submit a TSR to DISA.

TELECOMMUNICATIONS SERVICE ORDER

The TSO is the correspondence prepared by DISA on receipt of a TSR. DISA uses the information submitted, along with information from a database, to issue an order to complete the activation, deactivation or change requested. The TSO is used to authorize the Operation & Maintenance (O&M) agencies to buy equipment necessary to fulfill its service requirements. A TSO is then sent for action to each DISA station, the designated DISA control office, the leasing agency (if applicable) and the other DISA agencies that will be impacted. An information copy is sent to the O&M agency headquarters of the DISA stations, the originating TCO and the using agency. Each DISA region has the responsibility for issuing TSOs on the circuits/systems that travel or terminate within their area.

DEVELOPING AN RFS

DISA Direct

Access to DISA Direct is through the DISA Home Page (http://www.disa.mil), which is shown in figure 2-12. Either Internet Explorer or Netscape may be used as the browser to access DISA Direct. For optimum performance, submitting and authorizing officials should be accessing the Web via the NIPRNET. The DISA Direct allows customers to search for products and services offered by DISA, submit their requests electronically, receive status regarding their requirements, and other capabilities essential for the management of their information systems services.

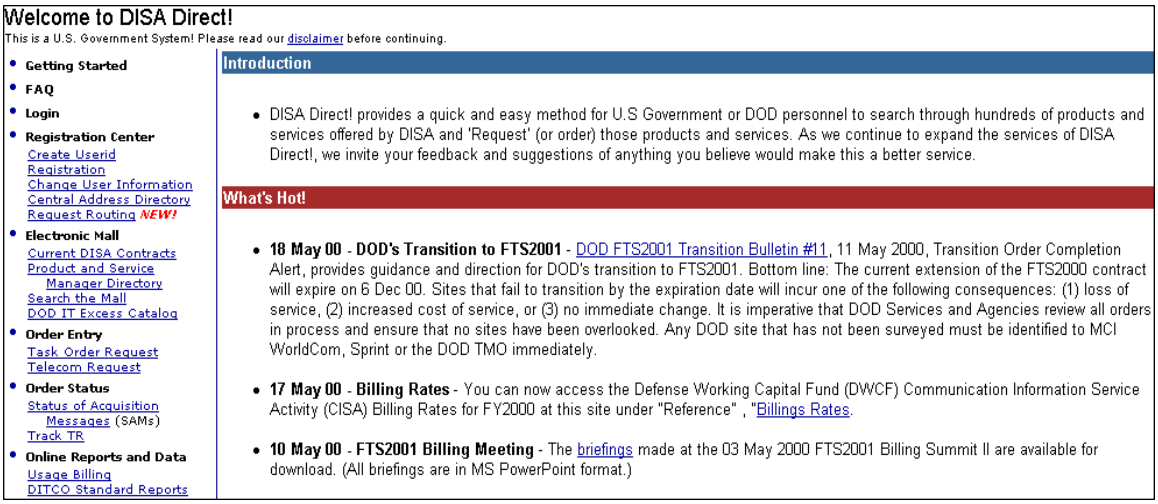

Figure 2-12. DISA Direct Home Page - Initial Starting Point When Requesting Services From DISA.

Registration Center

Create Userid. A userid is not required to view the information in several areas of DISA Direct, to include: Getting Started, Frequently Asked Questions (FAQ), Electronic Mall, and Reference areas. However to request a role, submit a request or check on the status of a requirement, a userid will be required. To create a userid, click on the 'create userid' link and follow the instructions. A userid is provided immediately after submission. Make a mental note of the userid and password since it will be needed to perform various functions within DISA Direct. If you forget your userid and/or password do not create a new one. A link is provided to request your current DISA Direct userid and password before it is e-mailed to you.

Registration. If you will be submitting and/or approving Telecommunications Requests or approving roles via DISA Direct, you must have the appropriate role as described below under Role Officials.

Registration Process. To request a role, click on the "registration" link and then the "request new role" link. You will have the option of selecting 'e-mail' if you want e-mail notices in addition to the DISA Direct notification process. You will also be required to enter the names and phone numbers of your supervisor and security officer within your agency, so have these on hand prior to preparing your request for a role. To identify the appropriate role, highlight the role and select 'continue.' To request multiple roles, hold down the 'ctrl' key while you click on the appropriate selections. You will also be required to select the appropriate Registration Official (RO) who will approve the

request. If an RO has not been established for your agency/organization, this must be done prior to submitting the request. When the requestor's role request has been approved/denied, they will be notified by way of the DISA Direct notification process, which consist of a 'notifications' link at the top of the page in the blue line of the Order Entry area. Requests that are denied must included comments back to the requester. By clicking on the 'notifications' link, all messages addressed to the person logged onto DISA Direct will be displayed. Also, if the requestor selected the option of 'e-mail,' they will receive an e-mail notification as to the status of their request. For requests to become an RO, a DISA representative will approve/deny these requests. All other requests are approved/denied by the appropriate RO from the requester's agency/ organization.

Role Officials

There are role officials who represent the requesting activity. These role officials are assigned various functions to validate the mission requirements, funding, and completeness of the services being requested. The role officials are critical in the provisioning process.

Registration Official (RO). The RO is responsible for approving or denying role requests submitted by persons within their agency and organization. The RO's access is granted through the approval of a DISA representative.

Authorized Requesting Official (ARO). The ARO represents an agency and organization for requesting DISA products and services. The ARO creates and submits electronic requests found on the DISA direct welcome page, under Web Order Entry (Web OE).

Authorized Approving Official (AAO). The AAO will review and approve, modify or deny requests for products and services that are submitted by an ARO in the same or a subordinate organization. This role is usually assigned to an individual/office at the MACOM/major claimant level. This is an optional role and is not required for request approval.

Authorized Funding Official (AFO). The AFO will approve or modify funding assignments on requests for products and services submitted by an ARO. The AFO will also create and maintain funding information in the Web based financial information files for the funding instruments under their control, including the updating of fund cites each fiscal year. This role should be assigned at the level where funding approval authority resides whether it is centralized or distributed. This is a mandatory role and is required for all request approvals.

Authorized Provisioning Official (APO). The APO is a DISA representative assigned to one of the provisioning centers who creates and submits electronic requests via the Web on behalf of DISA or customer agencies. The APO is responsible for coordinating with the customer to ensure the correct funding code is used for the agency represented, and ensuring the requirement and any notifications are routed to all responsible parties. The APO role is granted by an RO within the same provisioning center.

Change User Information. To change one's user information, select this item and update the appropriate areas.

Central Address Directory (CAD). The CAD is a software application used for the storage and retrieval of POC information. The CAD is linked to the DISA Direct welcome page, where users can enter or update POC information. The CAD is also linked to the Web OE requests, where the ARO can retrieve, edit and enter information into the CAD. The CAD is maintained by ADOs at the organizational and DISA levels, who validate POC information for their respective areas.

Retrieve/Enter POC Information. Throughout the requests, a button bar "retrieve/enter POC information" will allow the ARO to retrieve, edit and enter POC information in the CAD.

Search the CAD. This option allows you to search for a POC. Based on the information provided, the CAD will search and provide the results as indicated in the following paragraph. The results of a search will display the search criteria and results. Based on the results, the ARO can then select the POC listed, edit the information, or add a new POC if the proper one does not exist in CAD.

Electronic Mall (E-Mall)

The E-Mall provides two methods for obtaining information on DISA products and services. By using either a drill-down or a key word search method, customers may view detailed information on DISA products and services. The E-Mall also provides customers the capability to easily send inquiries to Product and Service Managers should they have questions regarding any product or service.

Search the Mall. This feature allows users to search the mall area using keywords (i.e., modems, channel banks, etc.). By entering a key word, a search of the mall will find the DISA contracts that could possibly be used to procure the required items. Figure 2-13 shows the results of performing a search with the keyword of “router”, which includes both contracts and individual products and services.

Products & Services Catalog - Search Results

router Search

Contracts with Matching Products and Services:

- DCA200-1995-D-0004 - Bulk Modem Contract

Matching Products and Services:

Item	Price	Chrg Type	Pkg	Action
NMS 6560 MPRouter PRO-Stand Alone	$4,869.00	Non Recurring	EA	Place Request
DCA200-1995-D-0004 - Bulk Modem Contract				
NMS Ethernet MP Router 6520	$2,981.00	Non Recurring	EA	Place Request
DCA200-1995-D-0004 - Bulk Modem Contract				
NMS Ethernet/Hub MPRouter - US	$3,257.00	Non Recurring	EA	Place Request
DCA200-1995-D-0004 - Bulk Modem Contract				
Router Service-NIPRNET	-	-	-	Place Request
(Payment accepted by PDC)				

Figure 2-13. Search results provided from searching the Mall.

Current DISA Contracts. This area displays all DISA Indefinite Delivery/ Indefinite Quantity (ID/IQ) contracts and Basic Ordering Agreements (BOA) for specific supplies or services to be furnished with deliveries scheduled by placing orders with the contractor. The ID/IQ contracts will require the government to order and the contractor to furnish at least a stated minimum quantity of supplies or services and not to exceed a maximum quantity. Check the authorized user listed to see if your agency is authorized to purchase from a particular contract and then contact the contract specialist to place your order.

Products and Services Manager Directory. The directory provides a generic description of the products and services offered by DISA as well as a point of contact for potential customers to direct questions to regarding the DISA offerings. The directory will evolve into a catalog to include additional descriptive details and links to existing DISA programs and online ordering processes as they become available.

Order Entry

Several options will be available in Order Entry (OE), to include establishing the routing that will be applied to each request and the various requests that are available in OE.

Request Routing. Once a request is submitted, a notification will be sent via e-mail to the first office, individual or e-mail address identified on a pre-determined routing list. Upon receipt of the notification, an individual will log into DISA Direct and either approve or deny the request. An approved request will be automatically routed to the next office, individual or e-mail address identified in the routing list. This process will continue until all have approved the request at which time it will be forwarded to DISA for processing. If the request is denied, a comment must be entered (i.e., reason for denial), which will be sent back through the approval chain to the ARO. The routing of a request is based on the funding document cited in the request or a default routing list established by an RLO.

Task Order Request. The Task Order (TO) request is used to create requirements packages for any of DISA's large technical services contracts. Because some information and processes differ slightly among the various contracts, you should thoroughly review the TO guidelines for the specific contract you wish to use before creating your package. The TO guidelines can be accessed from DISA Direct and/or call the appropriate Contracting Officer's Representative (COR)/Contracting Officer (CO) if you have questions.

Telecommunications Request (TR). The TR permits customers to provide the complete details of the requirement for ordering a data, voice, video or other type of service.

Order Status

This area is used for providing status to the customer regarding their requested services. For instance, a copy of the SAM will be posted in this area and can be retrieved using the Web request number or other identifier unique to the requirement. A userid and password is needed to access the information contained in this area.

Prepare the Request

The following are general guidelines for preparing the Telecommunications Request (TR). Detailed instructions are provided in DISAC 310-130-5 (C3.5).

Separate Action. Each request action must be submitted as a separate requirement and be identified by a separate Web request number. However, requests can be copied using the copy feature on the Web, the appropriate items changed, and submitted as a separate requirement.

Classification. All requests submitted via the Web must be unclassified. If classified information is required to describe a requirement, the classified portion will be forwarded under separate cover and handled accordingly. If classified information is being sent separately, the statement "additional information provided under separate cover" should be noted in the remarks field of the request.

Mandatory/Required/Optional Information. The applicable table contained in DISAC 310-130-5, Request Item Submission Matrices, should be used to determine which items are mandatory, required and optional for a specific type of requests (i.e., starts, changes, discontinues, etc.). There are some items which are mandatory for all types of request and these are noted by an asterisk beside the item within the TR. Entries must be made in these items before the user can submit the request. If entries are not made, a warning message will appear stating the information is missing. If this occurs, fill in the required information and click on submit again. If more than one block of information is missing, this cycle will be repeated until all of the required information is filled in.

Submit Request

When all of the applicable information on the request has been entered, click on the 'submit' button. The screen will change to show a confirmation of the information submitted. It is possible to obtain a printout of the information being submitted by clicking the 'print' button on the user's Web browser.

Web Request Number. At the time of a request or saving of a draft request; a Web request number is automatically assigned to the request. This number is tracked throughout the provisioning process and should be used to reference the requirement. The number is comprised of 14 characters (example being WO30Jun990001_).

Request Validation. Once the request is submitted, it is routed through a series of approvals based on the PDC and addresses designated by the ARO. Each person in the approval chain (i.e., AAO, AFO, etc.) will receive an e-mail notification that there is a

request to be reviewed on the Web (DISA Direct). The approving official will log onto the Web, view the request, and either approve or deny the request. If approved, the request is routed to the next approving official. If denied by any one of the approving officials, a notification with comments as to why the request was denied will be sent back through the approval chain. Only after each approver has validated the request will the requirement be forwarded to DISA for processing and to the addressees designated by the requester.

Request Distribution. A copy of the request will be sent to the e-mail addresses provided in the requirement. Likewise, a copy of the order and status messages will be provided to the addressees to keep them informed of the requirement. Organizational e-mail addresses, rather than user addresses, will be used in most cases to distribute information. It is the responsibility of the requester to enter the correct e-mail addresses.

IMPACT OF REQUIREMENTS DOCUMENTS

Objective 2d: Using a topology handout and a AF Form 3215 (CSRD) and working as a team member, assess the impact of requirements documents IAW Performance Specification II-2d.

INFORMATION

IMPACTS

Every requirement must be evaluated individually. The impact of a new requirement may be as simple as documenting a change to an existing circuit or configuration. Or as complex as working with many different agencies on your base, throughout the DoD, other federal, state or local government agencies, civilian corporations and sometimes foreign governments.

Sometimes you will merely be an "info" addressee on requirements, meaning you need to be aware of what is happening and insure your documentation is kept current. Other times, you will be an "action" addressee on requirements, meaning you will be required to perform some kind of action. This action may be coordination or it could be to assist with the design and/or implementation of the new requirement.

ASSESMENT FACTORS

There are a myriad of possible combinations when it comes to assessing the impact of a requirement. Things to keep in mind are:

1. Resources—do you have enough or will you need more? Who will pay for and procure them?

    a. Equipment—will you need to provide the equipment or modify your existing equipment (such as new modules for routers or switches)? Will you need to reserve space in a rack or on a floor? What about power?

    b. Money—will you have to pay for anything out of your operating budget? Will another organization pay for it? Will additional funds be transferred to you.

    c. Personnel—will the new requirement levy new man-hour requirements on your shop? If so, has the manning support issue been addressed?

    d. Time—will you have to dedicate someone to work issues related to the requirement? If so, will this require a "reshuffle" of existing workloads.

2. Authorization—do you need authorization to make changes to the systems being effected by the requirement? If so, do you have to obtain the authorization or will it be provided?

3. Expertise—will you be required to support technologies that are unfamiliar to your shop? Has training been included with the project? Will you have to arrange and fund your own training?

4. Access—do you need to get access to additional facilities on the base? This would bring your unit security manager into the project.

Many of the answers to the preceding questions can be answered by the Program Management Office (PMO), if there is one. They have probably dealt with the issues several times before and are experienced with integrating them. The PMO should be utilized at every opportunity to reduce unforeseen problems that they may know how to easily avoid.

If there is no PMO, your best bet it to work with your own plans and programs (SCX) shop when coordinating with agencies on base. You should consult DISA when coordinating with agencies outside of your base, as they are often responsible for insuring new requirements are implemented on time.

If the requirement has only local significance, such as an addition or change to the base LAN, then it should be handled by the Base Network Control Center (BNCC). In this case, issues such as cabling, port density of existing equipment and IP address space

would need to be considered. Again, the SCX shop can prove to be an invaluable asset when dealing with other agencies on the base. They can help coordinate issues such as; additional power and cooling for new equipment, entrenching new runs of fiber optic cable or the installation of racks that need to be installed either in the communications squadron or any other facility on base.

SUMMARY

Due to the vast number of possibilities, we will not attempt to cover them all here. Suffice it to say, whenever a new requirement comes down, read it carefully to see if you need to take any action. If so, contact the originator or PMO to discuss the issue. It the requirement is local, contact the local point of contact to insure all areas have been addressed. Staying ahead of the game through proper planning will reduce headaches and possibly wasting resources to meet deadlines.

CHAPTER THREE

NETWORK IMPLEMENTATION

OBJECTIVES

3a: Using training equipment and materials provided, perform tasks associated with cable testing, IAW Performance Specification II-3a.

3b: Working as a team member using equipment and materials provided, configure a router IAW Performance Specification II-3b.

3c: Working as a team member using equipment and materials provided, configure a switch IAW Performance Specification II-3c.

3d. Working as a team member using equipment and materials provided, configure ATM IAW Performance Specification II-3d.

3e. Working as a team member using equipment and materials provided, configure an integrated network design IAW Performance Specification II-3e.

CABLE TESTING

Objective 3a: Using training equipment and materials provided, perform tasks associated with cable testing, IAW Performance Specification II-3a.

INFORMATION

Network cabling, which is analogous to arteries that carry blood to your vital body organs, provides a medium for the transport of data among users, servers, printers, switches and routers. A cable blocking the flow of data will seriously degrade or even halt network operations.

Inadequate cabling is one of the most prominent reasons for network problems; therefore, do not take cabling for granted. Not understanding preventative testing and troubleshooting procedures will give you migraines and leave you wishing you would have chosen a different career field. The proper implementation of proactive testing will help minimize network downtime and save a great deal of stress in fixing cable problems. A cable tester is the most effective tool in certifying whether the network wiring is capable of transmitting data successfully.

CABLE TESTING

Cable testing takes place within the Physical Layer of the Open System Interconnection (OSI) Reference Model. The Physical Layer defines the transmission of bits through a medium, and standards at this layer specify electrical characteristics of the signal, cable and connector pin-outs. As you know the most common cable type today is Category 5 unshielded twisted pair (UTP) wire, supporting speeds of 100 Mbps with protocols such as Ethernet, Fast Ethernet, Token Ring, and Fiber Distributed Data Interface.

Most cable testers run tests to certify whether a Category 5 cable installation meets requirements for passing data. Other testers are available that allow you to test other media, such as multimode and single mode optical fiber and thin and thick coaxial cable.

When should you perform cable testing? The obvious answer is when users begin experiencing problems; however, this is a reactive form of testing. You are often under the gun to restore the network back to a functioning system. When a problem first occurs, such as slow or no response from network resources, you should utilize your network management software or protocol analyzer to determine what part of the network is at fault and whether or not the problem may be in the cabling. If you narrow the problem down to the cabling or connectors, then a cable tester will prove its worth.

Common Cable Faults

It is worth repeating that cable problems rank very high as causes of networking troubles. Mechanical elements, such as cabling, connectors and wall plates tend to fail more often than active electronic devices like network adapters and switches. It is also much easier to make unnoticeable mistakes when installing wiring and connectors. Thus if you are experiencing connection problems, there is a good chance cabling is the culprit.

Approximately 85% of cable problems arise from the installation, not from flaws with the cable itself. As examples, a telephone technician working on the telephone system could accidentally snip a network cable; an installer may improperly attach a connector to the cable or exceed distance limitations for a particular cable run. This may have a large or small effect on the network, depending on which devices are on the other end of the cable. Of course, if the server or switch goes down, everyone will notice.

Faults causing intermittent problems are generally improper splices, poor connector attachments, lack of termination, and corrosion. A cable will transfer the energy of a data signal as long as the impedance within the cable remains constant. According to many funny looking equations, maximum power transfer will occur under this condition. However, a signal encountering a sharp change in impedance will cause reflections. The worst case is lack of termination. As the signal reaches the end of a cable, it will collide into a difference in impedance, the air, if there is no terminator on the end of the cable.

The terminator is there to absorb the power and dissipate it as heat, making the cable look infinitely long. If the signal hits a difference in impedance, part of the signal will reflect back, possibly causing a collision with itself or another signal. In addition to the lack of termination, improper splices and poor connector attachments may also cause reflections.

Cabling aliments can also cause excessive attenuation, decreasing the amount of signal power reaching the receiving device. This causes the signal-to-noise ratio to decreases, leading to greater transmission errors.

TYPES OF CABLE TESTS

Wire Map

The wire map test ensures a link has proper connectivity by testing for continuity and other installation mistakes. Continuity tests verify the wire is not broken and that physical connectivity exists throughout the connectors and cabling. Thus, this test will tell you if someone accidentally cut the cable. Sometimes during installation, the installer may inadvertently fail to connect the wires on one connector pin to the corresponding pin on the opposite end of the cable. This of course will not facilitate a connection--the wire map test verifies proper pairing of wiring on opposite ends of the cable.

The twisting of wires in UTP minimizes induction of current flow from other devices emanating electromagnetic waves, such as nearby wires. A Category 5 cable includes four individually twisted pairs of wires. If you do not wire your RJ45 connectors exactly according to a standard, such as EIA/TIA T568A or T568B wiring scheme, you may produce split pairs. A split pair occurs when a wire pair consists of one lead from one twisted pair and another lead from a different twisted pair, creating a pair of wires that are untwisted. The split pair configuration provides a path for data to flow, but problems may occur. The issue is the resulting untwisted wire pair will encounter an excessive amount of external noise, interference and crosstalk, causing transmission errors. The nice thing is that cable testers do a good job of detecting split pairs.

Link Length

Link length measurements tell you whether the cable meets the length constraints expressed by the cabling standard. Cable testers utilize a Time-Domain Reflectometer (TDR) that tells you the length of a cable. The TDR also indicates if there are any improper cable spices or terminations.

TDR works on the principle of reflections. The TDR connects to an end of a cable the technician wishes to test and sends a signal throughout the cable. This signal reflects off changes in impedance, especially the end of the cable, and the amplitude of the reflected wave corresponds to the degree of impedance mismatch. The TDR records the time between sending the test signal and receiving the return, then calculates the distance to the reflecting point based on the speed of the signal.

Attenuation

A data signal loses power while traversing the length of a cable. This loss of power is attenuation. If too much attenuation is present between source and destination, electrical noise becomes significant and transmission errors will occur more frequently. Attenuation tests help you identify problems such as manufacturing defects and corrosion.

In addition to cable length, the amount of attenuation is also a function of frequency. Most cables will offer more attenuation to higher frequency signals than lower frequency ones. Thus, cabling acts like a low pass filter, causing the sharp edges of the digital signal to round.

Cable testers examine attenuation by measuring the effects of sending a series of signals that step through the cable's operating frequency bandwidth. For Category 5 testing, most cable testers cover bandwidth of 1 MHz to 100 MHz by taking a reading in 1 MHz increments. This certifies whether the cable meets specifications in the part of the frequency spectrum where the signal mostly resides

The cable tester will report a passing grade if all frequencies pass specifications. If a cable fails, the tester will tell you the frequency at which it did not meet requirements. Some testers also indicate the amount of attenuation per foot. Cable testers are available that work with metallic or fiber. For example, Microtest Pentascanner measures attenuation among many other impairments on Category 3, 4 and 5 cables.

Near-end Crosstalk (NEXT)

Current flow, resulting from the difference of potential impressed by the data signal, is electrons that move through a metallic wire. This stream of electrons creates an electromagnetic field around the wire that may induce the flow of electrons in an adjacent wire. This crossing of the signal into a different wire is called crosstalk. Near-end Crosstalk (NEXT) is a specific case where signals at one end of the link interfere with weaker signals coming back from the recipient.

You may experience voice signal cross talk while talking on the phone. For example, you may hear another person's conversation while you are talking to someone else. Sometimes this happens if you add an additional telephone line to your house and utilize both phones at the same time. The close proximity of the wire-pairs allows the signals to jump over to the other wires.

Causes of crosstalk generally include improper wire placement and inadequate shielding. The twisting of wire, such as the case with UTP cable, offers some resistance to crosstalk

and other interfering signals. Shielded twisted pair and coaxial cable offer a greater degree of protection. However, optical fiber is immune to crosstalk because fiber uses light instead of current flow to transport the data. The flow of light through the fiber's core does not produce an electromagnetic field that couples to nearby fibers.

In addition to crosstalk, networks may encounter the induction of external electrical noise. This noise can become significant in relation to the signal power, setting up the potential for errors. The noise causing problems within network cabling is usually Gaussian or impulse noise. Gaussian noise has mostly uniform amplitude across the frequency spectrum and mainly results from thermal conditions in the atmosphere. Impulse noise, is normally the outcome of man-made devices such as light switches, spark plugs and heater coils. Impulse noise typically occurs in short blasts, causing transmission errors to occur in bursts. As with crosstalk, external noise produces an electromagnetic field that causes unwanted current to flow through metallic data cables.

The amount of NEXT varies erratically as you sweep through the operating bandwidth of a cable. For an accurate measurement, cable testers record NEXT by stepping though the cable's operating frequency range at very small increments.

The scanner we use in this course is the Microtest Pentascanner, which is a hand-held diagnostic tool that incorporates a graphical user interface, backlit display, menus, arrow keys, on-line help and descriptive menu options. The scanner works in conjunction with an injector device. This allows you to perform wire map, signal generation for attenuation and end link termination for other measurements. Various Microtest Pentascanner configurations are shown in figure 3-1 through 3-3.

Cable Tester Setup

Calibration of the injector’s signal amplitude is required for accurate attenuation measurements and requires user intervention. To maintain accurate attenuation measurements, the injector must be calibrated each calendar day that it is used. Expiration of calibration data is automatically detected by the scanner.

The scanner and injector are connected through their respective test connector ports using the patch cable provided with each instrument, this is shown in figure 3-1. The amplitude of each frequency generated by the injector is measured by the scanner. The resulting calibration values are stored in the scanner according to the injector’s serial number. The scanner maintains five sets of injector calibration data simultaneously.

1. Connect the scanner and the injector using the patch cable supplied with the scanner. If you have a scanner with a 36-pin connector, you may also need to use the Mod 8 Adapter (included).

2. Power on the scanner.

3. Press the **Extended Functions** key.
4. Select **Calibrate Injector**. The Scanner will display:
   Searching for Injector . . .

5. On finding the injector, the scanner displays:
   Calibrating . . .

6. When the calibration is complete, the scanner displays:
   The Injector has been calibrated

7. Press **OK (F1)** to return to the **Extended Functions** menu.

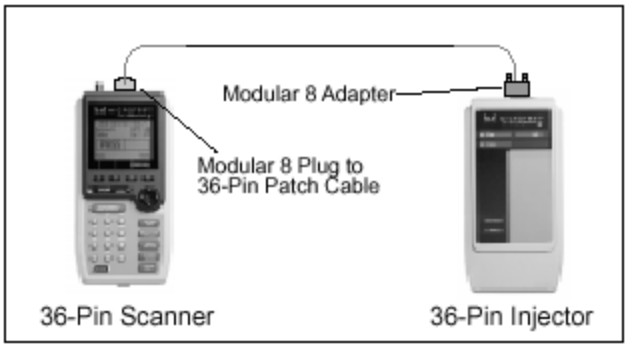

Figure 3-1. Connecting the Pentascanners with Modular 8 Adapters.

Connections

The scanner and the injector are used together to perform measurements that allow the scanner to verify installed links or assist in the diagnosis of network problems at the physical layer. To accomplish these measurements, the scanner and the injector are connected at both ends of a network-cabling link.

Basic Link with Modular 8 Jacks

Figure 3-2 below shows the connection of a scanner to a Modular 8 jack in the wiring closet and an injector to a Modular 8 jack in the work area. Use the Modular 8 plug to 36-pin patch cable to attach the scanner to the Modular 8 jack. At the other end of the link, use the Modular 8 plug to 36-pin patch cable to attach the Injector to the Modular 8 jack.

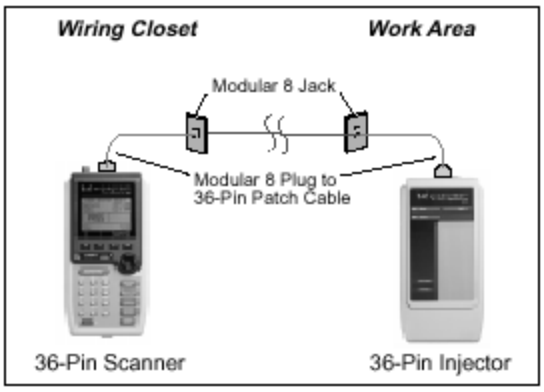

Figure 3-2. Using a Pentascanner to perform end-to-end cable tests.

AUTOTEST

This section explains how to run Autotest, including selecting the cable types and Autotest specifications. It also explains how to customize an Autotest so you can select the pairs that are tested, the PASS/FAIL criteria and select which tests to run during Autotest.

Autotest lets you run cable tests, check test results against standards and get a PASS/FAIL indication — without having to know which tests to select or how to interpret results. Autotest can be customized depending on your site or system requirements. For example, your system may require the use of two wire pairs (instead of four) or you may not need to perform all of the tests that Autotest can run. By customizing Autotest to meet your specific needs, you save time and money! Autotest varies depending on your network type. Autotest supports many network types, including ARCNET, 10BASE-T, Category 5, Category 4 and Category 3 LINK, ISO Class C and D.

Steps for Running Autotest

1. From the **Ready** screen, verify that the cable type matches the cable type you will be testing.

2. Also, from the **Ready** screen, verify that the default Autotest is the Autotest that you want to run.

3. Connect the scanner to the near end of the twisted pair cable you are testing and connect the Injector to the far end. During Autotest, the injector provides the far end termination for measurements made by the scanner. In addition, it generates signals of programmable frequency for measurement by the scanner to determine one-way Attenuation. The injector also generates swept frequency signals and measures the Near End Crosstalk (NEXT) at its end of the installed link. The scanner acts as the termination device while NEXT is being measured by the injector.

4. If you have not used the Injector in the last 24 hours, you will need to calibrate. Press the **Extended Functions** key and select **Calibrate Injector.**

5. Press the **AUTOTEST** key. If you are testing twisted pair cable, the scanner will immediately verify that the injector is attached. If the injector is not attached, the scanner will wait until it is attached before running the Autotest.

6. When the Autotest completes, a PASS or FAIL tone will sound. You can then view the results of individual tests or you can view a summary of test results.

7. You can save Autotest results.

8. You can print Autotest results.

Press the **ESCAPE** key at any time to cancel the Autotest.

Find Cable Faults

Find Cable Faults traces your cable runs and locates intermittent faults. It also incorporates Time Domain Reflectometer so you can find faults in cables less than 10 feet long.

Wire Map determines how the cable and connectors are wired, from one end to the other. It is usually run before any other measurements, to pinpoint cabling problems caused by opens, shorts, split pairs or miss-wires.

Find Cable Faults draws a graphical representation of the cable, showing opens, shorts and miss-wires. When Wire Map is run, Find Cable Faults continuously repeats its

testing so the operator can wiggle connectors and wires to locate intermittent faults. Find Cable Faults repeatedly runs Length and Wire Map and displays the length and continuity of the entire cable.

Wire Map

The Wire Map screen is displayed when you press the Find Cable Faults key. Four primary things can go wrong with a cable or connector.

- A short between wires
- An open on any single wire
- An open across all wires (break)
- An impedance mismatch

If a short or open exists in the cable, isolate the segment you suspect, connect the scanner to it and run the Length test by pressing the Measure Cable Performance key; then selecting Length.

An Impedance mismatch is caused by irregularities in the cable and can show up as an open or a short at an unexpected length.

When troubleshooting wiring problems, look for improperly crimped cables — make sure that the outer insulation fits into the end of the connector.

Press Splits (F1) to display the wire splits screen. The split status is shown to the right of each wire pair. Figure 3-3 shows a variety of cable faults.

Wire Map for Both Ends of the Link

The injector plays an integral part in determining the wire map for a given link. With the scanner and the injector connected at opposite ends of a link or cable, the wire map can be determined. When running Find Cable Faults or Autotest, the scanner and the injector communicate to determine how the link is wired. With the wire map on display, press Splits (F1) to display the wire splits screen. The scanner/injector combination identifies the following wiring configurations.

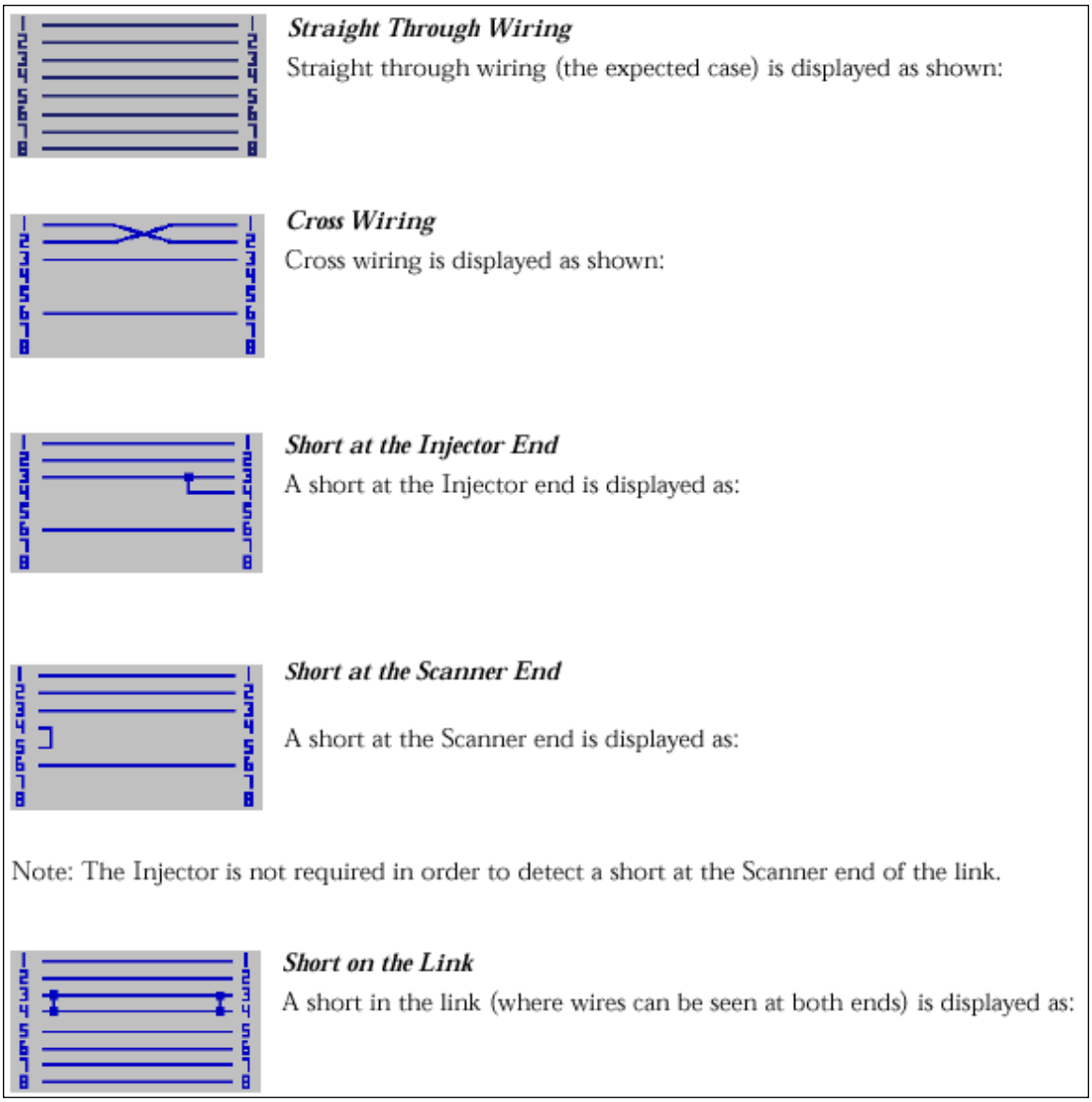

Figure 3-3. Various cable faults found with a Pentascanner.

Length

Length can find opens, shorts and breaks in a cable. The scanner uses Time Domain Reflectometer (TDR) to find the location of faults in cables. The Scanner generates a pulse down the wire, and when the pulse encounters an impedance change (such as an open, short or poor connection), all or part of the pulse energy is reflected back to the Scanner. The Scanner then measures the delay between when the pulse was sent and when the reflection was received. Knowing the speed that the pulse travels down the

cable (Nominal Velocity of Propagation or NVP), the Scanner can then calculate the distance to the fault. The Length measurement is most accurate when the NVP setting you use is set correctly.

SUMMARY

The cable tester is a very useful tool in our job. Wiring is the backbone of our networks and must be installed and maintained at its optimum performance. Cable testers give us more options to isolate problems at the physical layer rather than just a continuity tester. We cannot overlook the benefits of not only having one of these devices in our network facilities, but being proficient at its use.

Router Configuration

Objective 3b: Working as a team member using equipment and materials provided, configure a router IAW Performance Specification II-3b.

INFORMATION

In this section, you will be introduced to the Cisco Internetwork Operating System (IOS). The IOS is what runs Cisco routers, as well as some Cisco switches and also allows you to configure the devices. You will learn how to configure a Cisco IOS router using both the initial setup mode and the Cisco IOS Command-Line Interface (CLI). Through the IOS interface, you can configure passwords, banners, and more. You will also learn the basics of router configurations in this chapter.

USER INTERFACE AND ROUTER COMPONENTS

Cisco Router Internetwork Operating System

The IOS was created to deliver network services and enable networked applications. The Cisco IOS runs on most Cisco routers and on some Cisco Catalyst switches, like the Catalyst 2900 switch. The Cisco router IOS software is used to complete the following on Cisco hardware:

- Carry network protocols and functions
- Connect high-speed traffic between devices
- Add security to control access and stop unauthorized network use
- Provide scalability for ease of network growth and redundancy
- Supply network reliability for connecting to network resources

You can access the Cisco IOS through the console port of a router, from a modem, or even through Telnet. Access to the IOS command line is called an EXEC session.

Connecting to a Cisco Router

You can connect to a Cisco router to configure the router, verify the configuration, and check statistics. There are different ways to connect to a Cisco router, but the first place you typically would connect to is the console port. The console port is usually a RJ-45 connection on the back of the router. This is used to connect to and configure the router using a rollover cable. No password is set on the console port by default. Another way to connect to a Cisco router is through an auxiliary port. This is really the same as a console

port and can be used as such. However, it also allows you to configure modem commands to allow a modem connection to the router. This means you can dial up a remote router and attach
to the auxiliary port if the router is down and you need to configure it. The third way to connect to a Cisco router is through the program Telnet. Telnet is an emulation program that emulates a dumb-terminal. You can then use Telnet to connect to any active interface on a router like an Ethernet or serial port.

The Internal Components of a Cisco Router

In order to configure and troubleshoot a Cisco internetwork, you need to know the major components of Cisco routers and understand what these components do. Figure 3-4 describes the major Cisco router components.

Component	Description
Bootstrap	Stored in the micro code of the ROM, the bootstrap is used to bring a router up during initialization. It will boot the router and then load the IOS.
POST (power-on self test)	Stored in the micro code of the ROM, the POST is used to check the basic functionality of the router hardware and determines which interfaces are present.
ROM monitor	Stored in the micro code of the ROM, the ROM monitor is used for manufacturing testing and troubleshooting.
Mini-IOS	Called the RXBOOT or bootloader by Cisco, the mini-IOS is a small IOS in ROM that can be used to bring up an interface and load a Cisco IOS into flash memory. The mini-IOS can also perform a few other maintenance operations.

RAM (random access memory)	Used to hold packet buffers, routing tables, and also the software and data structures that allow the router to function. Running-config is stored in RAM, and the IOS can also be run from RAM in some routers.
ROM (read-only memory)	Used to start and maintain the router.
Flash memory	Used on the router to hold the Cisco IOS. Flash memory is not erased when the router is reloaded. It is an EEPROM created by Intel.
NVRAM (nonvolatile RAM)	Used to hold the router and switch configuration. NVRAM is not erased when the router or switch is reloaded.
Configuration register	Used to control how the router boots up. This value can be seen with the show version command and typically is 0x2102, which tells the router to load the IOS from flash memory.

Figure 3-4. Cisco Router Commands.

Bringing Up a Router

When you first bring up a Cisco router, it will run a power-on self-test (POST), and if that passes, it will look for and load the Cisco IOS from Flash memory if a file is present. Flash memory is an electronically erasable programmable read-only memory (EEPROM). The IOS will load and then look for a valid configuration called startup-config that is stored by default in nonvolatile RAM (NVRAM). If there is no configuration in NVRAM, then the router will bring up what is called setup mode. This is a step-by-step process to help you configure a router. You can also enter setup mode at any time from the command line by typing the command setup from global configuration

mode. Setup only covers some very global commands, but is helpful if you don't know how to configure certain protocols, like bridging or DECnet, for example.

SETUP MODE

You actually have two options when using setup mode: Basic Management and Extended Setup. Basic Management only gives you enough configurations to allow connectivity to the router, whereas Extended Setup allows you to configure some global parameters as well as interface configuration parameters.

COMMAND-LINE INTERFACE (CLI)

The Command-Line Interface (CLI) is really the best way to configure a router because it gives you the most flexibility. To use the CLI, just say no to entering the Initial Configuration Dialog. After you say no, the router will come back with messages stating the status of all the router interfaces.

Logging into the Router

After the interface status messages appear and you press Return, the Router> prompt will appear. This is called user mode and is mostly used to view statistics, though it is also a stepping-stone to logging into privileged mode. You can only view and change the configuration of a Cisco router in privileged mode, which you enter with the command **enable**.

```
Router>
Router>enable
Router#
```

You now end up with a Router#, which indicates you are in privileged mode. You can both view and change the configuration in privileged mode. You can go back from privileged mode to user mode by using the **disable** command.

```
Router#disable
Router>
```

At this point you can type **logout** to exit the console.

```
Router>logout
Router con0 is now available
```

Press RETURN to get started.

Or you could just type **logout** or **exit** from the privileged mode prompt to log out.

Router>**en**
Router#**logout**
Router con0 is now available
Press RETURN to get started.

OVERVIEW OF ROUTER MODES

To configure from a CLI, you can make global changes to the router by typing **configure terminal** (**config t** for short), which puts you in global configuration mode and changes what is known as the running-config. You can type **config** from the privileged mode prompt and then just press Return to take the default of terminal.

Router#**config**
Configuring from terminal,memory,or network [terminal]? *Press Return*
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#

At this point you make changes that affect the router as a whole, hence the term global configuration mode. To change the running-config, which is the current configuration running in Dynamic RAM (DRAM), you would use the command **configure terminal**, or just **config t**. To change the configuration stored in NVRAM, which is known as startup-config, you would use the command **configure memory**, or **config mem** for short. If you wanted to change a router configuration stored on a TFTP host you would use the command **configure network**, or **config net**. However, understand that for a router to actually make a change to a configuration, it needs to put the configuration in RAM. So, if you actually type **config mem** or **config net**, you will replace the current running-config with the configuration stored in NVRAM or a configuration stored on a TFTP host.

CLI Prompts

It is important to understand the different prompts you can find when configuring a router so you know where you are at any time within configuration mode. In this section, we will demonstrate the prompts that are used on a Cisco router. Always check your prompts before making any changes to a router's configuration.

Interfaces

To make changes to an interface, you use the **interface** command from global configuration mode:

```
Router(config)#interface Ethernet 0
Router(config-if)#
```

Notice the prompt changed to Router(config-if)# to tell you that you are in interface configuration.

Line Commands

To configure user mode passwords, use the **line** command. The prompt then becomes Router (config-line)#.

```
Router#config t
Enter configuration commands,one per line. End with CNTL/Z.
Router(config)#line ?
<0-70>      First Line number
aux         Auxiliary line
console     Primary terminal line
tty         Terminal controller
vty         Virtual terminal

Router(config)#line console 0
Router(config-line)#
```

The line console 0 command is known as a major, or global, command, and any command typed from the (config-line) prompt is known as a subcommand.

Routing Protocol Configurations

To configure routing protocols like RIP and EIGRP, use the prompt (config-router)#.

```
Router#config t
Enter configuration commands, one per line.   End with CNTL/Z.
Router(config)#router eigrp 100
Router(config-router)#
```

To view routing table information, enter the command **show ip route.**

Router#**show ip route**

EDITING AND HELP FEATURES

Help Features

You can use the Cisco advanced editing features to help you configure your router. By using a question mark (**?**) at any prompt, you can see the list of commands available from that prompt.

Router#**?**

You can press the spacebar to get another page of information, or you can press Return to go one command at a time. You can also press any other key to quit and return to the prompt.

If you are typing commands and receive this:

Router#**clock set 10:30:10**
%Incomplete command.

then you know that the command string is not done. Just press the up arrow key to receive the last command entered, then continue with the command by using your question mark. Also, if you receive this error:

Router(config)#**access-list 110 permit host 1.1.1.1**
^
%Invalid input detected at '^'marker.

notice that the ^ marks the point where you have entered the command incorrectly. This is very helpful.

If you receive this error:
Router#**sh te**
%Ambiguous command:"sh te"

it means you did not enter all the keywords or values required by this command. Use the question mark to find the command you need.

Router#**sh te?**
WORD **tech-support terminal**

Figure 3-5 shows the list of enhanced editing commands available on a Cisco router.

Ctrl+Z	Ends configuration mode and returns to EXEC
Tab	Finishes typing a command for you

Figure 3-5. Enhanced Editing Commands.

You can review the router-command history with the commands shown in Figure 3-6

Ctrl+P or up arrow	Shows last command entered
Ctrl+N or down arrow	Shows previous commands entered

Figure 3-6. Router-Command History.

Gathering Basic Routing Information

The command show version will provide basic configuration for the system hardware as well as the software version, the names and sources of configuration files, and the boot images.
Router#**sh version**

Cisco Internetwork Operating System Software
IOS (tm)2500 Software (C2500-JS-L),Version 12.0(8),
RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1999 by cisco Systems,Inc.
Compiled Mon 29-Nov-99 14:52 by kpma
Image text-base:0x03051C3C, data-base:0x00001000

```
ROM:System Bootstrap,Version 11.0(10c),SOFTWARE
BOOTFLASH: 3000 Bootstrap Software (IGS-BOOT-R),Version
11.0(10c), RELEASE SOFTWARE (fc1)

RouterA uptime is 5 minutes
System restarted by power-on
System image file is "flash: c2500-js-l_120-8.bin"

cisco 2522 (68030)processor (revision N)with 14336K/
2048K bytes of memory.

Processor board ID 15662842,with hardware revision
00000003
Bridging software.
X.25 software,Version 3.0.0.
SuperLAT software (copyright 1990 by Meridian Technology
Corp).
TN3270 Emulation software.
Basic Rate ISDN software,Version 1.1.
1 Ethernet/IEEE 802.3 interface(s)
2 Serial network interface(s)
8 Low-speed serial(sync/async)network interface(s)
1 ISDN Basic Rate interface(s)
32K bytes of non-volatile configuration memory.
16384K bytes of processor board System flash (Read ONLY)
Configuration register is 0x2102
```

The **show version** command lets you know how long the router has been running, how it was restarted, the IOS filename running, the model hardware and processor versions, and the amount of DRAM. Also, the configuration register value is listed last.

Setting the Passwords

There are five passwords used to secure your Cisco routers. The first two passwords are used to set your enable password, which is used to secure privileged mode. This will prompt a user for a password when the command **enable** is used. The other three are used to configure a password when user mode is accessed either through the console port, the auxiliary port, or Telnet.

Enable Passwords

You set the enable passwords from global configuration mode.

Router(config)#**enable ?**

last-resort	Define enable action if no TACACS servers respond
password	Assign the privileged level password
secret	Assign the privileged level secret
use-tacacs	Use TACACS to check enable passwords

Last-resort. Is used if you set up authentication through a tacacs server and it is not available. This will allow the administrator to still enter the router. However, it is not used if the tacacs server is working.

Password. Is used to set the enable password on older, pre-10.3 systems. Not used if an enable secret is set.

Secret. Is the newer, encrypted password. Overrides the enable password if set.

Use-tacacs. Tells the router to authenticate through a tacacs server. This is convenient if you have dozens or even hundreds of routers. How would you like to change the password on 200 routers? The tacacs server allows you to only have to change the password once.

Router(config)#**enable secret cisco**
Router(config)#**enable password cisco**
The enable password you have chosen is the same as your enable secret. This is not recommended. Re-enter the enable password.

If you try and set the enable secret and enable passwords to be the same, it will give you a nice, polite warning the first time, but if you type the same password again it will accept it. However, now neither password will work. If you don't have older legacy routers, don't bother to use the enable password. User-mode passwords are assigned by using the **line** command.

Router(config)#**line ?**

<0-4>	First Line number
aux	Auxiliary line
console	Primary terminal line
vty	Virtual terminal

Aux. Is used to set the user-mode password for the auxiliary port. This is typically used for configuring a modem on the router but can be used as a console as well.

Console. Is used to set a console user-mode password.

Vty. Is used to set a Telnet password on the router. If the password is not set, then Telnet cannot be used by default. To configure the user-mode passwords, you configure the line you want and use either the **login** or **no login** command to tell the router to prompt for authentication.

Console Password

To set the console password, use the command **line console 0**. However, notice that when we tried to type **line console 0?** from the aux line configuration, we got an error. You can still type **line console 0** and it will accept it; however, the help screens do not work from that prompt. Type "**exit**" to get back one level.

Router(config-line)#**line console ?**
%Unrecognized command
Router(config-line)#**exit**
Router(config)#**line console ?**
<0-0>First Line number
Router(config)#**line console 0**
Router(config-line)#**login**
Router(config-line)#**password router**

Since there is only one console port, we can only choose line console 0.

OTHER CONSOLE PORT COMMANDS

There are a few other important commands to know for the console port. The **exec-timeout 0 0** command sets the timeout for the console EXEC session to zero, or to never time out. The increment options are in minutes and seconds so you have to be careful what you set it to. For instance, if you set it to 0 1, the console will time out in 1 second. The way to fix that is to continually press the down arrow key while changing the timeout time with your free hand. **Logging synchronous** is a nice command, and it should be a default command, but it is not. What it does is stop console messages from popping up and disrupting input you are trying to type. This makes reading your input messages much easier. Here is an example of how to configure both commands:

```
Router(config)#line con 0
Router(config-line)#exec-timeout ?
<0-35791>Timeout in minutes

Router(config-line)#exec-timeout 0 ?
<0-2147483>Timeout in seconds
<cr>

Router(config-line)#exec-timeout 0 0
Router(config-line)#logging synchronous
```

Telnet Password

To set the user-mode password for Telnet access into the router, use the **line vty** command. Routers that are not running the Enterprise edition of the Cisco IOS default to five VTY lines, 0 through 4. However, if you have the Enterprise edition, you will have significantly more. The best way to find out how many lines you have is to use the question mark.

```
Router(config)#line vty 0 ?
<0-4>Last Line Number
<cr>

Router(config)#line vty 0 4
Router(config-line)#login
Router(config-line)#password router1
```

If you try to telnet into a router that does not have a VTY password set, you will receive an error stating that the connection is refused because the password is not set. You can tell the router to allow Telnet connections without a password by using the **no login** command.

```
Router(config-line)#line vty 0 4
Router(config-line)#no login
```

After your routers are configured with an IP address, you can use the Telnet program to configure and check your routers instead of having to use a console cable. You can use the Telnet program by typing telnet from any command prompt (DOS or Cisco).

ROUTER INTERFACES

Interface configuration is one of the most important configurations of the router. Without interfaces, the router is useless. Interface configurations must be exact to communicate with other devices. Some of the configurations used to configure an interface are Network layer addresses, media-type, bandwidth, and other administrator commands. Different routers use different methods to choose interfaces used on a router. For example, the following command shows a 2522 router with 10 serial interfaces, which are labeled 0 through 9:

```
Router(config)#int serial ?
<0-9>Serial interface number
```

At this point you must choose the interface you want to configure. Once you do that, you will be in interface configuration for that interface. The command to choose serial port 5, for example, would be

```
Router(config)#int serial 5
Router(config-if)#
```

The 2522 router has one Ethernet 10BaseT port. Typing **interface ethernet 0** can configure the interface.

```
Router(config)#int ethernet ?
<0-0>Ethernet interface number

Router(config)#int ethernet 0
Router(config-if)#
```

Some routers, such as the 2500, are fixed configuration routers. This means that when you buy that model of router, you're stuck with that configuration. To configure an interface, you always use the interface type number sequence. However, the 2600, 3600, 4000, and 7000 series routers use a physical slot in the router and a port number on the module plugged into that slot. For example, on a 2600 router, the configuration would be interface type slot/port:

```
Router(config)#int fastethernet ?
<0-1>FastEthernet interface number
```

Router(config)#**int fastethernet 0**
%Incomplete command.

Router(config)#**int fastethernet 0?**
/
Router(config)#**int fastethernet 0/?**
<0-1>FastEthernet interface number

Notice that you cannot type **int fastethernet 0**. You must type the full command, which is type slot/port, or **int fastethernet 0/0**. You can type **int fa 0/0** as well. To set the type of connector used, use the command media-type. However, this is typically auto-detected.

Router(config)#**int fa 0/0**
Router(config-if)#**media-type ?**
100BaseX Use RJ45 for -TX;SC FO for -FX
MII Use MII connector

Bringing Up an Interface

You can turn an interface off with the interface command **shutdown** or turn it on with the **no shutdown** command. If an interface is shut down, it will display administratively down when using the **show interface** command, and the **show running-config** command will show the interface as shut down. All interfaces are shut down by default.

Router#**sh int e0**
Ethernet0 is administratively down, line protocol is down
[output cut]

Bring up an interface with the **no shutdown** command.

Router#**config t**
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#**int e0**
Router(config-if)#**no shutdown**
Router(config-if)#^**Z**

00:57:08:%LINK-3-UPDOWN:Interface Ethernet0,changed state to up
00:57:09:%LINEPROTO-5-UPDOWN:Line protocol on Interface
Ethernet0,changed state to up

Router#**sh int e0**
Ethernet0 is up, line protocol is up

Configuring an IP Address on an Interface

You don't have to use IP on your routers; however, IP is typically used on all routers. To configure IP addresses on an interface, use the **ip address** command from interface configuration mode.

Router(config)#**int e0**
Router(config-if)#**ip address 172.16.10.2 255.255.255.0**
Router(config-if)#**no shut**

Don't forget to turn on an interface with the **no shut** command. Remember to look at the command **show interface e0**, for example, which will show you if it administratively shut down or not. Show running-config will also show you if the interface is shut down. If you want to add a second subnet address to an interface, then you must use the **secondary** command. If you type another IP address and press Enter, it will replace the existing IP address and mask. To add a secondary IP address, use the **secondary** command.

Router(config-if)#**ip address 172.16.20.2 255.255.255.0 secondary**
Router(config-if)#**^Z**

You can verify both addresses are configured on the interface with the **show running-config** command (**sh run** for short).

Router#**sh run**
Building configuration...
Current configuration:
[output cut]
!
interface Ethernet0
ip address 172.16.20.2 255.255.255.0 secondary
ip address 172.16.10.2 255.255.255.0
!

Hostnames and Descriptions

Hostnames. You can set the hostname of the router with the hostname command. This is only locally significant, which means it has no bearing on how the router performs name lookups on the internetwork.

```
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#hostname Keesler
Keesler(config)#
```

Descriptions. Setting descriptions on an interface is helpful to the administrator and, like the hostname, only locally significant. This is a helpful command because it can be used to keep track of circuit numbers, for example.

```
Keesler(config)#int e0
Keesler(config-if)#description Comm Lan
Keesler(config-if)#int s0
Keesler(config-if)#desc Wan to Randolph circuit:6fdda4321
```

You can view the description of an interface either with the **show running-config** command or the **show interface** command.

```
Keesler#sh run
[cut ]
interface Ethernet0
description Comm Lan
ip address 172.16.10.30 255.255.255.0
no ip directed-broadcast
!
interface Serial0
description Wan to Randolph circuit:6fdda4321
no ip address
no ip directed-broadcast
no ip mroute-cache

Keesler#sh int e0
Ethernet0 is up,line protocol is up
Hardware is Lance,address is 0010.7be8.25db (bia
0010.7be8.25db)
Description:Comm Lan
[cut ]
```

Keesler#**sh int s0**
Serial0 is up,line protocol is up
Hardware is HD64570
Description:Wan to Randolph circuit:6fdda4321
[cut]
Keesler#

VIEWING AND SAVING CONFIGURATIONS

Saving Configurations

If you run through setup mode, it will ask you if you want to use the configuration you created. If you say yes, then it will copy the configuration running in RAM, known as running-config, to NVRAM and name the file startup-config.

You can manually save the file from RAM to NVRAM by using the **copy running-config startup-config** command. You can use the shortcut **copy run start** also.

Router#**copy run start**
Destination filename [startup-config]?**return**
Warning:Attempting to overwrite an NVRAM configuration
previously written by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]return
Building configuration...

Notice that the message stated we were trying to write over the older startup-config. The IOS had been just upgraded to version 12.8, and the last time the file was saved, 11.3 was running. You can view the files by typing the command **show running-config** or **show startup-config** from privileged mode. The **sh run** command, which is the shortcut for **show running-config**, tells us that we are viewing the current configuration.

Router#**sh run**
Building configuration...
Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!

```
hostname Router
ip subnet-zero
frame-relay switching
!
[cut ]
```

The **sh start** command, which is the shortcut for the **show startup-config** command, shows us the configuration that will be used the next time the router is reloaded and also shows us the amount of NVRAM used to store the startup-config file.

```
Router#sh start
Using 4850 out of 32762 bytes
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router
!
!
ip subnet-zero
frame-relay switching
!
[cut ]
```

You can delete the startup-config file by using the command **erase startup-config**. Once you perform this command, you will receive an error if you try to view the startup-config file.

```
Router#erase startup-config
Erasing the nvram filesystem will remove all files!
Continue?[confirm ]
[OK ]
Erase of nvram:complete
Router#sh start
%%Non-volatile configuration memory is not present
Router#
```

Verifying Your Configuration

Obviously, the **show running-config** would be the best way to verify your configuration, and the **show startup-config** would be the best way to verify the configuration used the next time the router is reloaded. Another way to verify your configuration is by typing **show interface** commands. The first command is **show interface ?**, which shows us all the available interfaces to configure. The only interfaces that are not logical are Ethernet and Serial.

```
Router#sh int ?
Ethernet IEEE 802.3
Null Null interface
Serial Serial
accounting Show interface accounting
crb Show interface routing/bridging info
irb Show interface routing/bridging info
<cr>
```

The next command is **show interface ethernet 0** and shows us the hardware address, logical address, and encapsulation method, as well as statistics on collisions.

```
Router#sh int e0
Ethernet0 is up,line protocol is up
Hardware is Lance,address is 0010.7b7f.c26c (bia
0010.7b7f.c26c)
Internet address is 172.16.10.1/24
MTU 1500 bytes,BW 10000 Kbit,DLY 1000 usec,
reliability 255/255,txload 1/255,rxload 1/255
Encapsulation ARPA,loopback not set,keepalive set (10 sec)
ARP type:ARPA,ARP Timeout 04:00:00
Last input 00:08:23,output 00:08:20,output hang never
Last clearing of "show interface"counters never
Queueing strategy:fifo
Output queue 0/40,0 drops;input queue 0/75,0 drops
5 minute input rate 0 bits/sec,0 packets/sec
5 minute output rate 0 bits/sec,0 packets/sec
25 packets input,2459 bytes,0 no buffer
Received 25 broadcasts,0 runts,0 giants,0 throttles
0 input errors,0 CRC,0 frame,0 overrun,0 ignored,
0 abort
0 input packets with dribble condition detected
33 packets output,7056 bytes,0 underruns
```

0 output errors,0 collisions,1 interface resets
0 babbles,0 late collision,0 deferred
0 lost carrier,0 no carrier
0 output buffer failures,0 output buffers swapped out

The most important status of the **show interface** command is the output of the line and data-link protocol status. If Ethernet 0 is up, line protocol is up, and the line is up and running.

Router#**sh int e0**
Ethernet0 is up, line protocol is up

The first parameter refers to the Physical layer and is up when it receives carrier detect. The second parameter refers to the Data Link layer and looks for keepalives from the connecting end.

Router#**sh int e0**
Ethernet0 is up,line protocol is down

If you see the line is up, but the protocol is down, you are having a clocking (keepalive) or framing issue. Check the keepalives on both ends to make sure they match; the clock rate is set, if needed; and the encapsulation type is the same on both ends.

If you see the line interface and protocol down, it is a cable or interface problem. Also, if one end is administratively shut down, then the remote end would show down and down. To turn on the interface, type the command **no shutdown** in interface configuration.

Router#**sh int e0**
Ethernet0 is down, line protocol is down
Router#**sh int e0**
Ethernet0 is administratively down, line protocol is down

BACKING UP, RESTORING AND ERASING THE CISCO CONFIGURATION

Any changes that you make to the router configuration are stored in the running-config file. If you do not perform a **copy run start** command after you make a change to running-config, that change will be gone if the router reboots or gets powered down. You may want to make another backup of the configuration information as an extra precaution, in case the router or switch completely dies, or for documentation. The

following sections describe how to copy the configuration of a router and switch to a TFTP host and how to restore that configuration.

Copying the Configuration to a TFTP Host

To copy the router's configuration from a router to a Trivial File Transfer Protocol (TFTP) host, you can use either the **copy running-config tftp** or **copy starting-config tftp** command. Either command will back up the router configuration that is currently running in DRAM or that is stored in NVRAM.

```
Router#copy run tftp
Address or name of remote host []?192.168.0.120

Destination filename [router-confg ] ?router1-confg
!!
487 bytes copied in 12.236 secs (40 bytes/sec)
Router#
```

Notice that this took only two exclamation points (!), which are two UDP acknowledgments. In this example, we named the file **router1-confg** because a hostname had not been set for the router. If you have a hostname configured the command will automatically use the hostname plus the extension – as the name of the file.

Restoring the Cisco Router Configuration

If you have changed your router's running-config and want to restore the configuration to the version in startup-config, the easiest way to do this is to use the **copy startup-config running-config** command (**copy start run** for short). You can also use the older Cisco command, **config mem**, to restore a configuration. Of course, this will work only if you first copied running-config into NVRAM before making any changes. If you copied the router's configuration to a TFTP host as a second backup, you can restore the configuration using the **copy tftp start-config** command (**copy tftp start** for short), as shown below. Remember that the old command that provides this function is **config network** (**config net** for short).

```
Router#copy tftp start
Address or name of remote host []?192.168.0.120
Source filename []?router1-confg
Destination filename [running-config ]?(press enter)
Accessing tftp://192.168.0.120/router1-confg...
```

```
Loading router1-confg from 192.168.0.120 (via Ethernet0):
!!
[OK -487/4096 bytes ]
487 bytes copied in 5.400 secs (97 bytes/sec)
Router#
00:38:31:%SYS-5-CONFIG:Configured from tftp://
192.168.0.120/router1-confg
Router#
```

The configuration file is an ASCII text file. This means that before you copy the configuration stored on a TFTP host back to a router, you can make changes to the file with any text editor.

Erasing the Configuration

To delete the startup-config file on a Cisco router, use the command **erase startup-config**, as follows:

```
Router#erase startup-config
Erasing the nvram filesystem will remove all files!
Continue?[confirm ](press enter)
[OK ]
Erase of nvram:complete
Router#
```

The preceding command deletes the contents of NVRAM on the router. The next time the router boots, it will run in setup mode.

Summary

In this objective, we introduced you to the Cisco Internetwork Operating System (IOS), router components, user interfaces, how routers are configured, as well as how to manage the configuration. It is important that you have a firm understanding of the basics offered in this section before you move on to other areas dealing with integrated network design.

Switch Configuration

Objective 3c: Working as a team member using equipment and materials provided, configure a switch IAW Performance Specification II-3c.

INFORMATION

HIERARCHICAL NETWORK DESIGN

Cisco has devised a hierarchical approach to network design that enables network designers to logically create a network by defining and using layers of devices. The resulting network is efficient, intelligent, scalable, and easily managed. The hierarchical model breaks a campus network into three distinct layers, as illustrated in Figure 3-7.

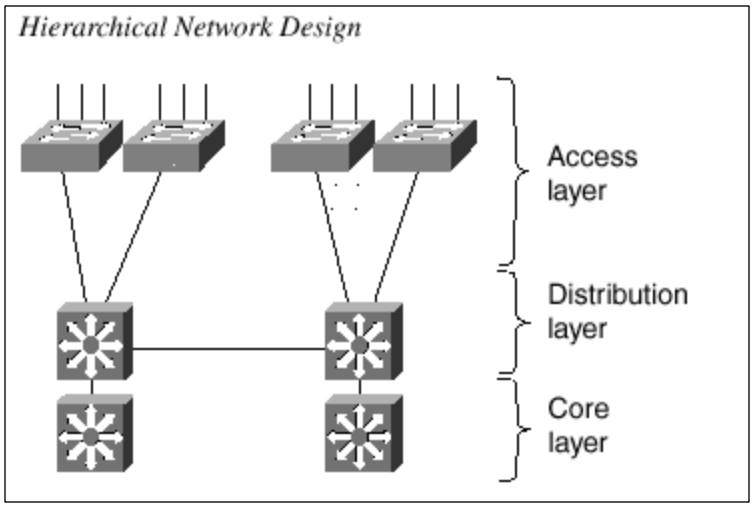

Figure 3-7. Cisco's Hierarchical Design.

These layers are the *access laye*r, *distribution laye*r, and the *core laye*r. Each layer has attributes that provide both physical and logical network functions at the appropriate point in the campus network. Understanding each layer and its functions or limitations is important so that the layer can be properly applied in the design process.

Access Layer

The access layer is present where the end users are connected into the network. Devices in this layer should have the following capabilities.

- Low cost
- High port density
- Scalable uplinks to higher layers
- User access functions—VLAN membership and traffic filtering based on MAC addresses
- Resiliency through multiple uplinks

Distribution Layer

The distribution layer provides interconnection between the access and core layers of the campus network. Devices in this layer should have the following capabilities.

- High Layer 3 throughput for packet handling
- *InterVLAN routing* through Layer 3 operations
- Media translation to transport data between dissimilar access layer media types
- Security and *policy-based connectivity* functions through access lists or packet filters

The Core Layer

The core layer of a campus network provides connectivity of all distribution layer devices. The core, sometimes referred to as the *backbon*e, must be able to switch traffic as efficiently as possible. Core devices should have the following attributes.

- Very high throughput
- No unnecessary packet manipulations (access lists, packet filtering)
- No Layer 3 processing, unless required and very fast
- Redundancy and resiliency for high availability

CONNECTING SWITCHES

Switch deployment in a network involves two steps: physical connectivity and switch configuration. This section describes the connections and cabling requirements for devices in a switch block. Cable connections must be made to the console port of a

switch in order to make initial configurations. Physical connectivity between switches and end users involves cabling for the various types of LAN ports.

Console Port Cables/Connectors

A terminal emulation program on a PC is usually required to interface with the console port on a switch. Various types of console cables and console connectors are associated with each Cisco switch family.

All Catalyst switch families use an RJ-45-to-RJ-45 rollover cable to make the console connection between a PC (or terminal or modem) and the console port. A rollover cable is made so that pin 1 on one RJ-45 connector goes to pin 8 on the other RJ-45 connector, pin 2 goes to pin 7, and so forth. In other words, the cable remains flat while the two RJ-45 connectors point in opposite directions.

To connect the PC end, the rollover cable plugs into an RJ-45 to DB-9 or DB-25 "Terminal" adapter (or a DB-25 "Modem" adapter for a modem connection). At the switch end, the rollover cable plugs directly into the RJ-45 jack of the console port.

Once the console port is cabled to the PC, terminal, or modem, a terminal emulation program can be started or a user connection can be made. The console ports on all switch families require an asynchronous serial connection at 9600 baud, 8 data bits, no parity, 1 stop bit, and no flow control.

Ethernet Port Cables/Connectors

Catalyst switches support a variety of network connections, including all forms of Ethernet. In addition, Catalyst switches support several types of cabling, including UTP and optical fiber.

The 10BaseT ports can be connected only to other 10BaseT-capable devices (including 10/100 autosensing devices), and the 100BaseX to other 100BaseX-capable devices. The 10BaseT and 100BaseTX ports use Category 5 UTP cabling and RJ-45 connectors.

The 100BaseFX ports use two-strand multimode fiber (MMF) with SC connectors to provide connectivity. The SC connectors on the fiber cables are square in shape. These connectors snap in and out of the switch port connector as the connector is pushed in or pulled out. One fiber strand is used as a transmit path and the other as a receive path. Therefore, the transmit fiber on one switch device should connect to the receive fiber on the other end.

The remainder of the Catalyst switch families support 10/100 autosensing (using Fast Ethernet autonegotiation) and Gigabit Ethernet. Switched 10/100 ports use RJ-45

connectors on Category 5 UTP cabling to complete the connections. These ports can be connected to other 10BaseT, 100BaseTX, or 10/100 autosensing devices. UTP cabling is arranged so that RJ-45 pins 1,2 and 3,6 form two twisted pairs. These pairs are connected straight through to the far end.
In order to connect two 10/100 switch ports back-to-back, as in an access layer to distribution layer link, a Category 5 UTP crossover cable must be used. In this case, RJ-45 pins 1,2 and 3,6 are still twisted pairs, but 1,2 on one end connect to 3,6 on the other end, and 3,6 on one end connect to 1,2 on the other end.

SWITCH MANAGEMENT

Cisco Catalyst switch devices can be configured to support many different requirements and features. When a PC is connected to the serial console port, configuration is generally done with a terminal emulator application on the PC. Further configurations can be performed through a Telnet session across the LAN or through a web-based interface.

Identifying the Switch

All switches come from the factory with a default configuration and a default system name or prompt. This name can be changed so that each switch in a network will have a unique identity. This option can be useful when you are using Telnet to move from switch to switch in a network.

Setting the Hostname/System Name

To change the host or system name, enter the following command in configuration mode:

Switch(config)#**hostname** *hostname*

The hostname is a string of 1 to 255 alphanumeric characters. As soon as this command is executed, the system prompt will change to reflect the new hostname.

NOTE: Configuration changes made on switches apply only to the active *running configuratio*n, stored in RAM. To make the changes permanent, in effect even after a power cycle, remember to copy the switch configuration into the *startup configuratio*n, stored in NVRAM. You can do this by using the **copy running-config startup-config** command.

Passwords and User Access

Normally, a network device should be configured to secure it from unauthorized access. Catalyst switches offer a simple form of security by setting passwords to restrict who can log in to the user interface. Two levels of user access are available: regular login, or *EXEC mod*e, and enable login, or *privileged mod*e. EXEC mode is the first level of access, which gives access to the basic user interface through any line or the console port. The privileged mode requires a second password and gives access to set or change switch operating parameters or configurations.

Cisco provides various methods for providing device security and user authentication. Many of these methods are more secure and robust than using the login passwords.

Setting Login Passwords

To set the login passwords on a switch interface, enter the following commands in global configuration mode:

Switch(config)#**enable password level 1** *password*
Switch(config)#**enable password level 15** *password*

Here, the EXEC mode password is set with a privilege level of one (1), while the enable password is set with a privilege level of 15. The password is a string of four to eight alphanumeric characters. Passwords on these switches are not case-sensitive.

To remove a password, use the **no enable password** *level password* command.

Remote Access

By default, the switch login passwords allow user access only via the console port. In order to use Telnet to access a switch from within the network, to use **ping** to test the reachability of a switch, or to monitor a switch by SNMP, you must perform some configuration for remote access.

Although a switch operates at Layer 2, the switch supervisor processor must maintain an IP stack at Layer 3 for administrative purposes. An IP address and subnet mask can then be assigned to the switch so that remote communications with the switch supervisor are possible.

By default, all ports on a switch are assigned to the same virtual LAN (VLAN) or broadcast domain. The switch supervisor and its IP stack must be assigned to a VLAN before remote Telnet and **ping** sessions will be supported.

Enabling Remote Access

An IP address can be assigned to the management VLAN (default is VLAN 1) with the following commands in global configuration mode.

Switch(config)#**ip default-gateway** *ip-address*
Switch(config)#**interface vlan 1**
Switch(config-if)#**ip address** *ip-address netmask*

As demonstrated by the preceding command syntax, an IP address and subnet mask are assigned to the VLAN1 "interface," which is really the switch supervisor's IP stack listening on VLAN1. In order to send packets destined off the local VLAN1 subnet, a default gateway IP address is also assigned.

Again, this default gateway has nothing to do with processing packets that are passed through the switch; rather, the default gateway is only used to forward traffic between a user and the switch supervisor for management purposes.

To view the current switch IP settings, use the **show ip** command.

COMMUNICATION BETWEEN SWITCHES

Because switch devices are usually interconnected, management is usually simplified if the switches can communicate on some level to become aware of each other. Cisco has implemented protocols on its devices so that neighboring Cisco equipment can be found. As well, some families of switch devices can be clustered and managed as a unit once they discover one another.

Switch Port Configuration

The individual ports on a switch can be configured with various information and settings, as detailed in the following sections.

Identifying Ports

Switch ports can have a text description added to their configuration to help identify them. This description is meant as a comment field only, as a record of port use or other unique information. The port description is shown when the switch configuration is displayed.

Assigning a Port Description

To assign a comment or description to an interface, enter the following command in interface configuration mode.

Switch(config-if)#**description** *description-string*

If the description string has embedded spaces between words, the entire string must be enclosed between quotation marks. To remove a description, use the **no description** interface configuration command.

Ethernet Port Mode

Ethernet-based switch ports can also be assigned a specific link mode. Therefore, the port operates in half-duplex, full-duplex, or auto-negotiated mode. Auto-negotiation is only allowed on Fast Ethernet and Gigabit Ethernet ports. In this mode, full-duplex operation will be attempted first, and then half duplex if full duplex was not successful. The auto-negotiation process repeats whenever the link status changes.

NOTE: A 10-Mbps Ethernet link defaults to half duplex, while a 100-Mbps Fast Ethernet link defaults to full duplex.

VIRTUAL LANS

Consider a network design that consists of Layer 2 devices only. For example, this design could be a single Ethernet segment, an Ethernet switch with many ports, or a network with several interconnected Ethernet switches. A fully Layer 2 switched network is referred to as a *flat network topology.* A flat network is a single broadcast domain, such that every connected device sees every broadcast packet that is transmitted. As the number of stations on the network increases, so does the number of broadcasts.

Due to the Layer 2 foundation, flat networks cannot contain redundant paths for load balancing or fault tolerance. To gain any advantage from additional paths to a destination, Layer 3 routing functions must be introduced.

A switched environment offers the technology to overcome flat network limitations. Switched networks can be subdivided into virtual LANs (VLANs). By definition, a VLAN is a single broadcast domain. All devices connected to the VLAN receive broadcasts from other VLAN members. However, devices connected to a different VLAN will not receive those same broadcasts.

A VLAN is made up of defined members communicating as a logical network segment. In contrast, a physical segment consists of devices that must be connected to a physical cable segment. A VLAN can have connected members located anywhere in the network, as long as VLAN connectivity is provided between all members. Layer 2 switches are configured with a VLAN mapping and provide the logical connectivity between the VLAN members.

Figure 3-8 shows how a VLAN can provide logical connectivity between switch ports.

Two workstations on the left Catalyst switch are assigned to VLAN 1, while a third workstation is assigned to VLAN 100. In this example, there can be no communication between VLAN 1 and VLAN 100. Both ends of the link between the Catalysts are assigned to VLAN 1. One workstation on the right Catalyst is also assigned to VLAN 1. Because there is end-to-end connectivity of VLAN 1, any of the workstations on VLAN 1 can communicate as if they were connected to a physical network segment.

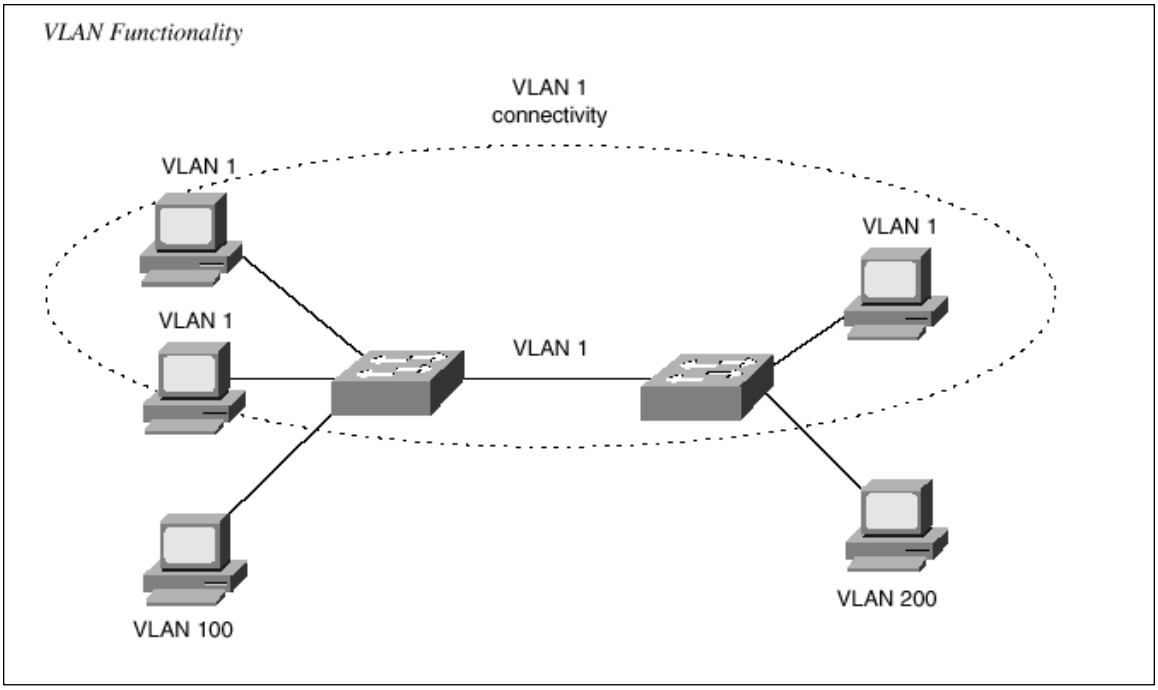

Figure 3-8. VLAN Functionality.

Virtual LANs Membership

When a VLAN is provided at an access layer switch, an end user must have some means to gain membership to it. Two membership methods exist on Cisco Catalyst switches: static VLANs and dynamic VLANs.

Static Virtual LANs

Static VLANs offer *port-based* membership, where switch ports are assigned to specific VLANs. End user devices become members in a VLAN based on which physical switch port they are connected to. No handshaking or unique VLAN membership protocol is

needed for the end devices; they automatically assume VLAN connectivity when they connect to a port. Normally, the end device is not even aware that the VLAN exists. The switch port and its VLAN are simply viewed and used as any other network segment, with other "locally attached" members on the wire.

Switch ports are assigned to VLANs by the manual intervention of the network administrator, hence the static nature. The ports on a single switch can be assigned and grouped into many VLANs. Even though two devices are connected to the same switch, traffic will not pass between them if they are connected to ports on different VLANs. To perform this function, either a Layer 3 device could be used to route packets or an external Layer 2 device could be used to bridge packets between the two VLANs. The static port-to-VLAN membership is normally handled in hardware with application-specific integrated circuits (ASICs) in the switch. This membership provides good performance because all port mappings are done at the hardware level with no complex table lookups needed.

Configuring Static Virtual LANs

This section describes the switch commands needed to configure static VLANs. By default, all switch ports are assigned to VLAN 1, are set to be a VLAN type of Ethernet, have a maximum transmission unit (MTU) size of 1500 bytes, and have a Security Association Identifier (SAID) of 100,000 plus the VLAN number.

First, the VLAN must be created on the switch, if it doesn't already exist. Then the VLAN must be assigned to specific switch ports.

To configure static VLANs on a switch, you would enter the following commands in enable mode:

Switch#**vlan database**
Switch(vlan)#**vlan** *vlan-num* **name** *vlan-name*
Switch(vlan)#**exit**
Switch#**configure terminal**
Switch(config)#**interface** *interface module/number*
Switch(config-if)#**switchport mode access**
Switch(config-if)#**switchport access vlan** *vlan-num*
Switch(config-if)#**end**

The VLAN is created and stored in a database, along with its number and name. The **switchport mode access** command configures the port for static VLAN membership.
To assign a switch port to the VLAN, you would use the **switchport access vlan** interface configuration command.

To verify VLAN configuration, using the **show vlan** command will output a list of all VLANs defined in the switch, in addition to the ports assigned to each VLAN.

Virtual LANs Trunks

At the access layer, end user devices connect to switch ports that provide simple connectivity to a single VLAN each. The attached devices are unaware of any VLAN structure and simply attach to what appears to be a normal physical network segment. Remember, sending information from an access link on one VLAN to another VLAN is not possible without the intervention of an additional device—either a Layer 3 router or an external Layer 2 bridge.

NOTE: Note that a switch port can support more than one IP subnet for the devices attached to it. For example, consider a shared Ethernet hub that is connected to a single Ethernet switch port. One user device on the hub may be configured for 192.168.1.1 255.255.255.0, while another is assigned 192.168.17.1 255.255.255.0. Although these subnets are unique communicating on one switch port, they cannot be considered separate VLANs. The switch port supports one VLAN, but multiple subnets can exist on that single VLAN.

A *trunk lin*k, however, can transport more than one VLAN through a single switch port. Trunk links are most beneficial when switches are connected to other switches or switches are connected to routers.

A trunk link is not assigned to a specific VLAN. Instead, one, many, or all active VLANs can be transported between switches using a single physical trunk link. Connecting two switches with separate physical links for each VLAN is possible. Figure 3-9 shows how two switches might be connected in this fashion.

As VLANs are added to a network, the number of links can quickly grow. A more efficient use of physical interfaces and cabling involves the use of trunking. The right half of the figure shows how one trunk link can replace many individual VLAN links. A trunk link can be associated with a native VLAN, which is used if the trunk link fails for some reason.

Cisco supports trunking on both Fast Ethernet and Gigabit Ethernet switch links, as well as aggregated Fast and Gigabit EtherChannel links. To distinguish between traffic belonging to different VLANs on a trunk link, the switch must have a method of identifying each frame with the appropriate VLAN. Several identification methods are available and are discussed in the next section.

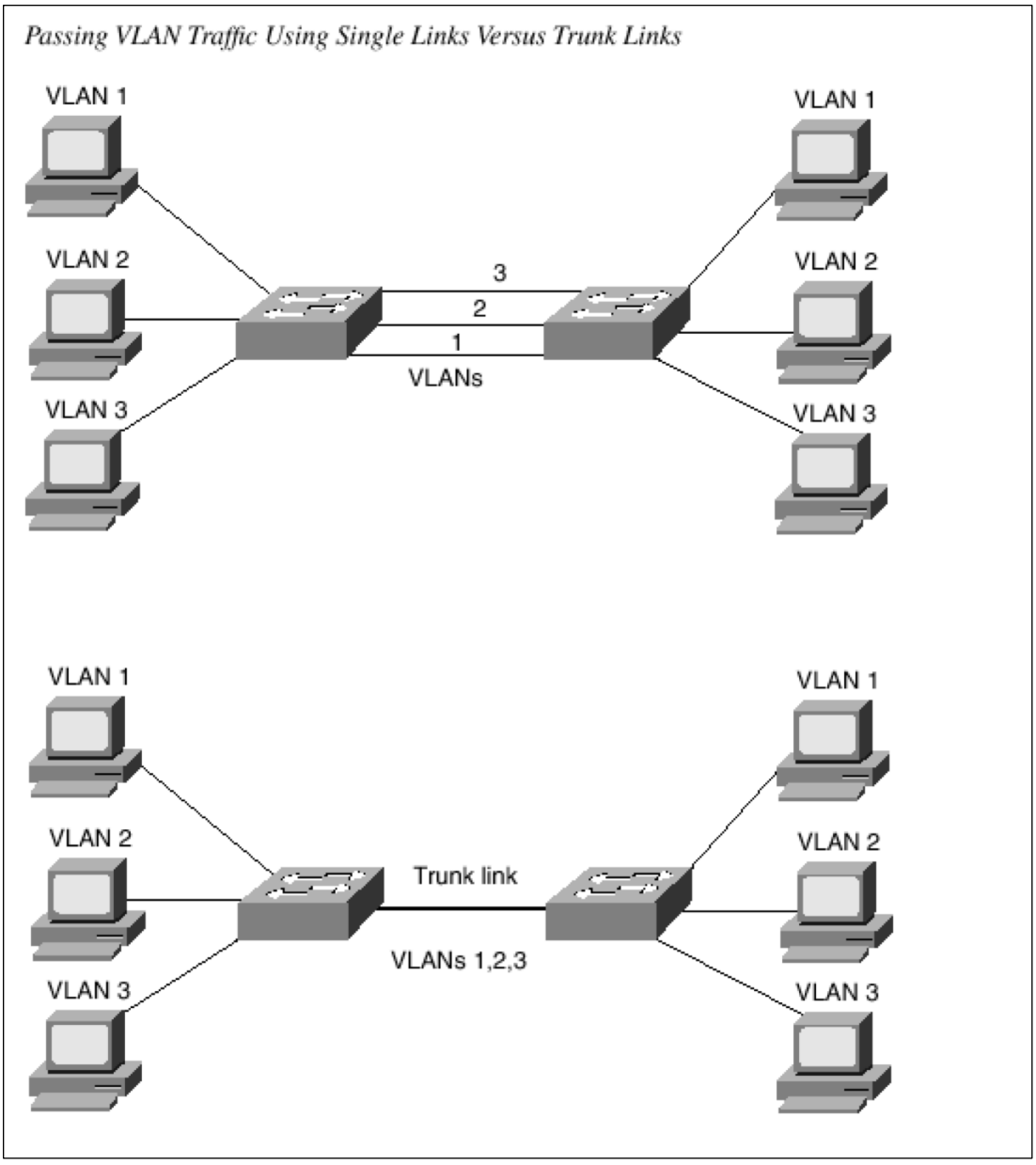

Figure 3-9. Passing VLAN traffic using single links versus trunk links.

Virtual LAN Frame Identification

Because a trunk link can be used to transport many VLANs, a switch must identify frames with their VLANs as they are sent and received over a trunk link. *Frame identificatio*n, or *tagging*, assigns a unique user-defined ID to each frame transported on a

trunk link. This ID can be thought of as the VLAN number or VLAN "color," as if each VLAN was drawn on a network diagram in a unique color.
VLAN frame identification was developed for switched networks. As each frame is transmitted over a trunk link, a unique identifier is placed in the frame header. As each switch along the way receives these frames, the identifier is examined to determine to which VLAN the frames belong.

If frames must be transported out another trunk link, the VLAN identifier is retained in the frame header. Otherwise if frames are destined out an access link, the switch removes the VLAN identifier before transmitting the frames to the end station. Therefore, all traces of VLAN association are hidden from the end station.

VLAN identification can be performed using several methods. Each uses a different frame identifier mechanism, and some are suited for specific network media. These methods are described in the sections that follow.

Inter-Switch Link Protocol

The Inter-Switch Link (ISL) protocol is a Cisco proprietary method for preserving the source VLAN identification of frames passing over a trunk link. ISL performs frame identification in Layer 2 by encapsulating each frame between a header and trailer. Any Cisco switch or router device configured for ISL can process and understand the ISL VLAN information. ISL is primarily used for Ethernet media, although Cisco has included provisions to carry Token Ring, FDDI, and ATM frames over Ethernet ISL. (A frame-type field in the ISL header indicates the source frame type.)

When a frame is destined out a trunk link to another switch or router, ISL adds a 26-byte header and a 4-byte trailer to the frame. The source VLAN is identified with a 10-bit VLAN ID in the header. The trailer contains a cyclic redundancy check (CRC) to assure the data integrity of the new encapsulated frame. Figure 3-10 shows how Ethernet frames are encapsulated and forwarded out a trunk link. Because tagging information is added at the beginning and end of each frame, ISL is sometimes referred to as *double tagging*.

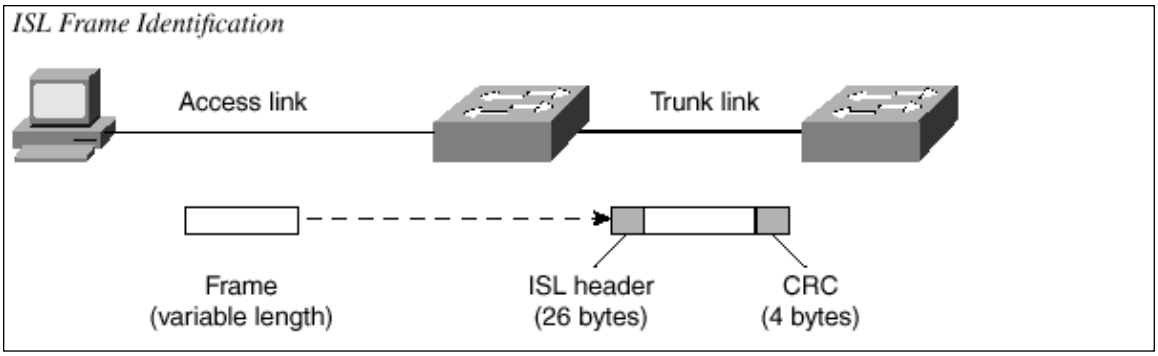

Figure 3-10 ISL frame identification.

If a frame is destined for an access link, the ISL encapsulation (both header and trailer) is removed before transmission. This removal preserves ISL information only for trunk links and devices that can understand the protocol.

Virtual LAN Trunk Configuration

By default, all switch ports are non-trunking and operate as access links until some intervention changes the mode. The sections that follow demonstrate the commands necessary to configure VLAN trunks on both an IOS-based and CLI-based switch.

Use the following commands to create a VLAN trunk link on a switch:

Switch(config)#**interface** *interface mod/port*
Switch(config-if)#**switchport mode trunk**
Switch(config-if)#**switchport trunk encapsulation isl**
Switch(config-if)#**switchport trunk allowed vlan remove** *vlan-list*
Switch(config-if)#**switchport trunk allowed vlan add** *vlan-list*

Individually, these commands place the switch port into trunking mode, using the encapsulation specified as **isl**. The last two commands define which VLANs can be trunked over the link. A list of VLANs is first removed from the trunk because all VLANs (1–1005) are trunked by default. Then, a list of VLANs can be added back into the trunk.

To view the trunking status on a switch port, use the **show interface** *int mod/port* **switchport** command.

Virtual LAN Trunking Protocol

VLAN configuration and trunking on a switch or a small group of switches is fairly easy and straightforward. Network environments, however, are usually made up of many interconnected switches. Configuring and managing a large number of switches, VLANs, and VLAN trunks can quickly get out of hand.

Cisco has developed a method to manage VLANs across the network. The VLAN Trunking Protocol (VTP) uses Layer 2 trunk frames to communicate VLAN information among a group of switches. VTP manages the addition, deletion, and renaming of VLANs across the network from a central point of control.

Virtual LAN Trunking Protocol Domains

VTP is organized into *management domains* or areas with common VLAN requirements. A switch can belong to only one VTP domain, in addition to sharing VLAN information with other switches in the domain. Similar to VLANs, switches in different VTP domains do not share VTP information.

Switches in a VTP domain advertise several attributes to their domain neighbors. Each advertisement contains information about the VTP management domain, VTP revision number, known VLANs, and specific VLAN parameters. When a VLAN is added to a switch in a management domain, other switches are notified of the new VLAN through VTP advertisements. In this way, all switches in a domain can prepare to receive traffic on their trunk ports using the new VLAN.

Virtual LAN Trunking Protocol Modes

To participate in a VTP management domain, each switch must be configured to operate in one of several modes. The VTP mode will determine how the switch processes and advertises VTP information. The following modes can be used:

> ***Server mode***. VTP servers have full control over VLAN creation and modification for their domains. All VTP information is advertised to other switches in the domain, while all received VTP information is synchronized with the other switches. By default, a switch is in VTP server mode. Note that each VTP domain must have at least one server so that VLANs can be created, modified, or deleted, and so that VLAN information can be propagated.
>
> ***Client mode***. VTP clients do not allow the administrator to create, change, or delete any VLANs. Instead, they listen to VTP advertisements from other

switches and modify their VLAN configurations accordingly. In effect, this is a passive listening mode. Received VTP information is forwarded out trunk links to neighboring switches in the domain.

Transparent mode. VTP transparent switches do not participate in VTP. While in transparent mode, a switch does not advertise its own VLAN configuration, and a switch does not synchronize its VLAN database with received advertisements. As well, in VTP version 1, a transparent mode switch does not even relay VTP information it receives to other switches. In VTP version 2, transparent switches do forward received VTP advertisements out of their trunk ports, acting as VTP relays.

NOTE: While a switch is in VTP transparent mode, a switch can create and delete VLANs that are local to itself. These VLAN changes, however, will not be propagated to any other switch.

Virtual LAN Trunking Protocol Advertisements

Each switch participating in VTP advertises VLANs, revision numbers, and VLAN parameters on its trunk ports to notify other switches in the management domain. VTP advertisements are sent as multicast frames. The switch intercepts frames sent to the VTP multicast address and processes them with its supervisory processor. VTP frames are forwarded out trunk links as a special case.

Because all switches in a management domain learn of new VLAN configuration changes, a VLAN need only be created and configured on just one VTP server switch in the domain.

By default, management domains are set to use non-secure advertisements without a password. A password can be added to set the domain to secure mode. The same password has to be configured on every switch in the domain so that all switches exchanging VTP information will use identical encryption methods.

The VTP advertisement process starts with configuration revision number *0 (zero*). When subsequent changes are made, the revision number is incremented before advertisements are sent out. When listening switches receive an advertisement with a greater revision number than is locally stored, the advertisement will overwrite any stored VLAN information. Because of this, forcing any newly added network switches to have revision number zero is important. The VTP revision number is stored in NVRAM and is not altered by a power cycle of the switch. Therefore, the revision number can only be initialized to zero using one of the following methods:

- Change the VTP mode of the switch to *transparent* and then change the mode back to *server.*

- Change the VTP domain of the switch to a bogus name (a non-existent VTP domain) and then change the VTP domain back to the original name.

- Issue a **clear config all** command, which will clear the switch configuration *and* the VTPinformation stored in NVRAM. Power cycle the switch so that it boots up with a non-existent VTP domain name and a VTP revision number of zero. *(Use caution. This is the most drastic method because it will erase all configuration data*.)

If the VTP revision number is not reset to zero, a new server switch might advertise VLANs as non-existent or deleted. If the advertised revision number happens to be

greater than previous legitimate advertisements, listening switches would overwrite good VLAN database entries with null or deleted VLAN status information. This is referred to as a *VTP synchronization problem.* Advertisements can originate as requests from client-mode switches that want to learn about the VTP database at boot-up time. As well, advertisements can originate from server-mode switches as VLAN configuration changes occur.

VTP advertisements can occur in three forms.

> ***Summary advertisements***. VTP domain servers will send summary advertisements every 300 seconds and every time a VLAN topology change occurs. The summary advertisement lists information about the management domain, including VTP version, domain name, configuration revision number, timestamp, MD5 encryption hash code, and the number of subset advertisements to follow. For VLAN configuration changes, summary advertisements are followed by one or more subset advertisements, with more specific VLAN configuration data.
>
> ***Subset advertisements***. VTP domain servers will send subset advertisements after a VLAN configuration change occurs. These advertisements list the specific changes that have been performed, such as creation or deletion of a VLAN, suspending or activating a VLAN, changing the name of a VLAN, and changing the MTU of a VLAN. Subset advertisements can list the following VLAN parameters: status of the VLAN, VLAN type (like Ethernet or Token Ring), MTU, length of the VLAN name, VLAN number, SAID value, and the VLAN name. VLANs are listed individually in sequential subset advertisements.
>
> ***Advertisement requests from clients***. A VTP client can request any lacking VLAN information. For example, a client switch might be reset and have its VLAN database cleared, its VTP domain membership might be changed, or it might hear a VTP summary advertisement with a higher revision number than it currently has. After a client advertisement request, the VTP domain servers respond with summary and subset advertisements.

Catalyst switches in server mode use a separate nonvolatile random-access memory (NVRAM) for VTP, different from the configuration NVRAM. All VTP information, including the VTP configuration revision number, is retained even when the switch power is off. In this manner, a switch is able to recover the last known VLAN configuration from its VTP database once it reboots.

Virtual LAN Trunking Protocol Configuration

Before VLANs can be configured, VTP must be configured. By default, every switch will operate in VTP server mode for the management domain *NUL*L, with no password or secure mode. The following sections discuss the commands and considerations that should be used to configure a switch for VTP operation.

Configuring a Virtual LAN Trunking Protocol Management Domain

Before a switch is added into a network, the VTP management domain should be identified. If this switch is the first one on the network, the management domain will need to be created. Otherwise, the switch may have to join an existing management domain with other existing switches.

The following command can be used to assign a switch to a management domain, where the *domain-name* is a text string up to 32 characters long.

Switch#**vlan database**
Switch(vlan)#**vtp domain** *domain-name*

Virtual LAN Trunking Protocol Mode

Next, the VTP mode needs to be chosen for the new switch. The three VTP modes of operation and their guidelines for use are as follows.

Server mode. Server mode can be used on any switch in a management domain, even if other server and client switches are in use. This mode provides some redundancy in the event of a server failure in the domain. However, each VTP management domain must have at least one server. The first server defined in a network also defines the management domain that will be used by future VTP servers and clients. Server mode is the default VTP mode.

Client mode. If other switches are in the management domain, a new switch should be configured for client mode operation. In this way, the switch will learn any existing VTP information from a server.

If this switch will be used as a redundant server, it should start out in client mode to learn all VTP information from reliable sources. If the switch was initially configured for server mode instead, it might propagate incorrect information to the other domain switches. Once the switch has learned the current VTP information, it can be reconfigured for server mode.

Transparent mode. This mode is used if a switch is not going to share VLAN information with any other switch in the network. VLANs can still be created, deleted, and renamed on the transparent switch. However, they will not be advertised to other neighboring switches. VTP advertisements received by a transparent switch will be forwarded on to other switches on trunk links.

Keeping switches in transparent mode can eliminate the chance for duplicate, overlapping VLANs in a large network with many network administrators. For example, two administrators might configure VLANs on switches in their respective areas, but use the same VLAN identification or VLAN number. Even though the two VLANs have different meanings and purposes, they could overlap if both administrators advertised them using VTP.

Configuring the Virtual LAN Trunking Protocol Mode

The VTP mode can be configured with the following sequence of commands:

Switch#**vlan database**
Switch(vlan)#**vtp domain** *domain-name*
Switch(vlan)#**vtp** {**server** |**client** |**transparent** }
Switch(vlan)#**vtp password** *password*

Virtual LAN Trunking Protocol Status

The current VTP parameters for a management domain can be displayed by using the **show vtp status** command. VTP message and error counters can also be displayed with the **show vtp counters.** This command can be used for basic VTP troubleshooting to see if the switch is interacting with other VTP nodes in the domain.

VLAN Configuration Commands

Task	IOS-Based Command	CLI-Based Command
Create VLAN	**vlan database** **vlan** *vlan-num* **name** *vlan-name*	**set vlan** *vlan-num* [**name** *name*]
Assign port to VLAN	**interface** *interface module/number* **switchport mode access** **switchport access vlan** *vlan-num*	**set vlan** *vlan-num mod-num/port-list*
Display VLANs	show vlan	**show vlan**
Configure trunk	**interface** *interface mod/port* **switchport mode trunk** **switchport trunk encapsulation {isl | dot1q}** **switchport trunk allowed vlan remove** *vlan-list* **switchport trunk allowed vlan add** *vlan-list*	**set trunk** *module/port* [**on | off | desirable | auto | nonegotiate**] *vlan-range* [**isl | dot1q | dot10 | lane | negotiate**] **clear trunk** *module/port vlan-range*
Display trunks	**show interface** *mod/num* **switchport**	**show trunk**

VTP Configuration Commands

Task	IOS-Based Command	CLI-Based Command
Configure VTP domain	**vlan database** **vtp domain** *domain-name*	**set vtp** [**domain** *domain-name*]
Configure VTP mode	**vlan database** **vtp domain** *domain-name* **vtp** {**server | client | transparent**} **vtp password** *password*	**set vtp** [**domain** *domain-name*] [**mode** {**server | client | transparent**}] [**passwd** *password*]
Configure VTP version	**vlan database** **vtp v2-mode**	**set vtp v2 enable**
Display VTP status	**show vtp status** **show vtp counters**	**show vtp domain** **show vtp statistics**
VTP pruning	**vtp pruning**	**set vtp pruning enable** **set vtp pruneeligible** *vlan-range* **clear vtp pruneeligible** *vlan-range*

Table 3-11. VLAN Configuration Commands.

Summary

In this objective, we introduced you to the Cisco Internetwork Operating System (IOS), switch components, user interfaces, how switches are configured, how to manage the configuration, as well as VLANs. It is important that you have a firm understanding of the basics offered in this section before you move on to other areas dealing with integrated network design.

Asynchronous Transfer Mode (ATM)

Objective 3d: Working as a team member using equipment and materials provided, configure ATM IAW Performance Specification II-3d.

INFORMATION

LAN EMULATION CONFIGURATION

This section discusses the procedures for configuring the various LANE components on Cisco Catalyst switches. The order that the components are configured is important because each component is dependent upon another.

On Cisco ATM devices, ELANs are configured on ATM subinterfaces. This configuration makes it possible to support many ELANs over a single ATM link. The LANE components necessary for a specific ELAN must be configured on the respective subinterface for that ELAN (ATM 0.1, ATM 0.2, and so on). The LECS, because it exists for *all* ELANs, must be configured on the major ATM interface (ATM 0).

Figure 3-12 shows an ATM network along with ATM interface and subinterface numbers. Notice that each LEC must be configured on a different subinterface. The LES/BUS pairs must be configured on the subinterfaces where their respective ELANs are present. The LECS must be configured on an ATM major interface because it keeps a database for all ELANs.

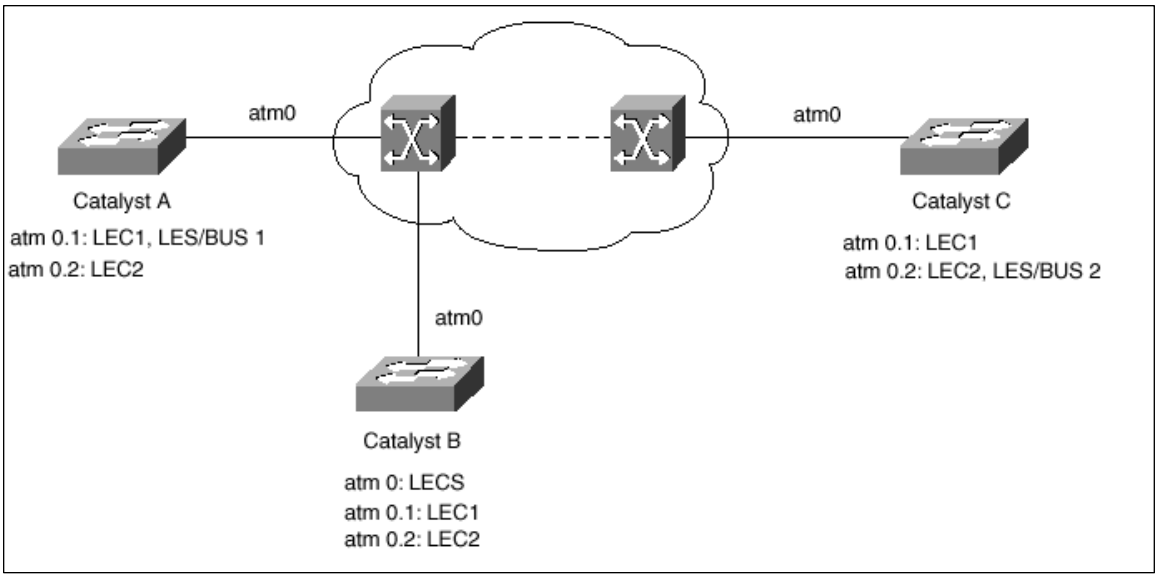

Figure 3-12. ATM LANE.

NSAP addresses on Cisco devices can be either manually configured or automatically generated by the equipment using the Integrated Local Management Interface (ILMI) protocol. Automatic generation is most often used because it offers easy configuration and use. If you want to manually configure the NSAP, you must first shut down the interface, and then disable ILMI. Recall that an NSAP address is made up of a 13-byte prefix, a 6-byte ESI, and a 1-byte selector. The ATM switch provides the prefix value. The ESI value comes from the MAC address assigned to the particular LANE module and ATM interface on the Catalyst switch. The selector byte comes from the ATM edge device itself and is equal to the ATM subinterface number.

The LANE components are also given automatic NSAP addresses, according to the scheme shown in Table 3-13. You should thoroughly understand how these addresses are generated. You might find it useful in some situations to be able to work backwards and locate a LANE component given its NSAP address.

Automatic NSAP Address Generation for LANE components

LANE Component	Prefix	ESI	Selector
LEC	From ATM switch	MAC address	ATM subinterface
LES	From ATM switch	MAC address + 1	ATM subinterface
BUS	From ATM switch	MAC address + 2	ATM subinterface
LECS	From ATM switch	MAC address + 3	.00

Figure 3-13. Automatic NSAP Generation for LANE Components.

Even before configuration, seeing a listing of the automatically generated NSAP addresses on any LANE-capable switch module is possible. For example, because configuring the complete LECS NSAP address into the ATM switches is necessary, you can find that address by using the **show lane default** command on the LANE module where the LECS will be configured. Refer to the **show lane default** command output in Example 3-14 and notice how the NSAP addresses for the LANE components follow the scheme in Table 3-13. (All LANE component addresses are shown with this command, even if none of the components are configured on the switch. You can now see what the automatically generated NSAP addresses would be if the components were configured.)

show lane default *Output Displays NSAP Addresses for LANE Components*

```
CatalystA_ATM#show lane default
interface ATM0:
LANE Client:            47.00001606288000300000000F.0050A28D5880.**
LANE Server:            47.00001606288000300000000F.0050A28D5881.**
LANE Bus:                47.00001606288000300000000F.0050A28D5882.**
LANE Config Server: 47.00001606288000300000000F.0050A28D5883.00
note: ** is the subinterface number byte in hex

CatalystA_ATM#
```

Figure 3-14. ShowLANE Default Output.

Notice that all LANE components are listed with their automatically generated NSAP addresses. To provide human readability, the addresses are output with dots separating the NSAP components. A dot appears after the leftmost byte of the prefix, at the end of the prefix, and at the end of the ESI (MAC address). Although an address is a long string of hex digits, it is easily broken down into prefix, ESI, and selector portions.

Configuring the LAN Emulation Configuration Server

The LECS is configured on a major ATM interface, not on a subinterface. First you must build the LECS database of ELANs and their associated LES NSAP addresses. Configure the LECS database with the following commands:

ATM(Config)#**lane database** *database-name*
ATM(lane-config-database)#**name** *elan1-name* **server-atm-address** *les1-nsap-address*
ATM(lane-config-database)#**name** *elan2-name* **server-atm-address** *les2-nsap-address*
ATM(lane-config-database)#**name …**

The *database-name* argument is a text string that identifies the LECS database as a whole. Several LECS databases can be defined, each with a unique name string, and applied to LECS components on individual ATM major interfaces. Usually, one LECS and one database are sufficient on a LANE module.

Each ELAN in the LANE network must be defined with a single **name** database command using the NSAP address of that ELAN's LES. Remember that you can find the NSAP address of the LES on a switch using the **show lane default** command.

To implement SSRP for redundant LES/BUS entities, use the same commands as above, with multiple NSAP addresses for each ELAN. For example, you can use the following commands.

ATM(Config)#**lane database** *database-name*
ATM(lane-config-database)#**name** *elan1-name* **server-atm-address** *les1-nsap-address*
ATM(lane-config-database)#**name** *elan1-name* **server-atm-address** *les2-nsap-address*
ATM(lane-config-database)#**name** *elan2-name* **server-atm-address** *les1-nsap-address*
ATM(lane-config-database)#**name** *elan2-name* **server-atm-address** *les2-nsap-address*
ATM(lane-config-database)#**name …**

After the database has been built, the LECS must be enabled on the ATM major interface. This is done with the following commands.

ATM(Config)#**interface atm** *number*
ATM(Config-if)#**lane config database** *database-name*

ATM(Config-if)#**lane config auto-config-atm-address**

The LECS database that was first built is now referenced by its name and bound to the LECS process. The **auto-config-atm-address** option is used to tell the LANE module to use the automatically generated NSAP addresses for the LECS component. The LECS NSAP address must now be configured into the ATM switches so that other LANE components can automatically retrieve the LECS address from the switches via ILMI.

To implement SSRP for redundant LECS entities, first create two or more LECS components on different LANE modules. Because the LECS database specifies the order of other redundant components to use, the LECS database must be configured identically on all LECS machines. Then the NSAP addresses of the redundant LECS components can be configured into the ATM switch.

Configuring the LES and BUS

The LES and BUS for an ELAN must be located on the same device and must use the same ATM subinterface. To configure both LES and BUS components for an ELAN, use the following commands:

ATM(Config)#**interface atm** *number.subint* **multipoint**
ATM(Config-subif)#**lane server-bus ethernet** *elan-name*

The subinterface number used can be arbitrarily chosen. Remember that each subinterface (or each ELAN) is segmented from the others. Therefore, you can configure a different LES/BUS pair on one or more subinterfaces. Each pair will operate only for its assigned ELAN. The *elan-name* parameter is a text string (case sensitive) that identifies the name of the ELAN. This name must be defined the same in all LANE components.

To implement SSRP for redundant LES/BUS components in an ELAN, use the preceding commands on other LANE modules to create the redundant pieces. All of the redundant LES/BUS pairs will be configured into the LECS database.

Configuring Each LEC

You must configure a LEC on each device where required. One LEC is necessary for each ELAN that a device participates in. The LEC configuration also specifies which VLAN the ELAN will be bridged to on the switch.

Each LEC is configured on a different ATM subinterface, using the following commands.

ATM(Config)#**interface atm** *number.subint* **multipoint**
ATM(Config-subif)#**lane client ethernet** *vlan-num elan-name*

The *vlan-num* argument references an existing VLAN number on the local switch. The *elan-name* argument references the name of an existing ELAN on the local LANE module. The two are then bridged on the LANE module and become a single broadcast domain.

VIEWING THE LANE CONFIGURATION

The configuration of each individual LANE component is fairly straightforward. However, because each component can be placed on a separate device, determining if all of the components are communicating and operating properly can be difficult. Catalyst LANE modules offer a number of commands that can be used to display and debug LANE configurations and status.

Viewing Default NSAP Addresses

To view the default NSAP addresses for the local LANE module, use the **show lane default** command as demonstrated previously in Example 3-8.

Viewing the LECS Database

To view the current LECS database, use the **show lane database** command on the LECS machine. Example 3-12 demonstrates the output generated by this command.

show lane database *Output Displays the LECS Database Contents*

```
CatalystA_ATM#show lane database

LANE Config Server database table 'company_db' bound to interface/s: ATM0
no default elan
elan 'lan1': un-restricted
  server 47.00001606288000300000000F.0050A28D5881.01 (prio 0) active
elan 'lan2': un-restricted
  server 47.00001606288000300000000F.0050A28D5881.02 (prio 0) active
```

Figure 3-16. Show LANE Database.

The shaded lines in the output in Example 3-16 show that the LECS has a database called company_db, which contains a number of LES and ELAN entries. The LECS is assigned to interface ATM0 (the major physical interface). The contents of the database are then listed by ELAN, each containing a single LES. All LESs are in the active state, and are listed with their complete NSAP addresses.

Viewing LANE Server Status

To view the status of an LES, use the **show lane server** command on the LES machine. Example 3-17 demonstrates this command for a switch that is the LECS for two ELANs:

show lane server *Output Displays LES Status*

```
CatalystA_ATM#show lane server
LE Server ATM0.1  ELAN name: lan1  Admin: up  State: operational
type: ethernet         Max Frame Size: 1516
ATM address: 47.00001606288000300000000F.0050A28D5881.01
LECS used: 47.00001606288000300000000F.0050A28D5883.00 connected, vcd 1460
control distribute: vcd 1485, 2 members, 479995 packets

proxy/ (ST: Init, Conn, Waiting, Adding, Joined, Operational, Reject, Term)
lecid ST vcd    pkts Hardware Addr  ATM Address
   1P O 1474  479994 0050.a28d.5880 47.00001606288000300000000F.0050A28D5880.0B
   2P O 1505       3 0090.6f7a.1c80 47.00001606288000100000000F.00906F7A1C80.01

LE Server ATM0.2  ELAN name: lan2  Admin: up  State: operational
type: ethernet         Max Frame Size: 1516
ATM address: 47.00001606288000300000000F.0050A28D5881.02
LECS used: 47.00001606288000300000000F.0050A28D5883.00 connected, vcd 1415
control distribute: vcd 1427, 2 members, 2 packets

proxy/ (ST: Init, Conn, Waiting, Adding, Joined, Operational, Reject, Term)
lecid ST vcd    pkts Hardware Addr  ATM Address
   1P O 1397       2 0050.a28d.5880 47.00001606288000300000000F.0050A28D5880.0C
   2P O 1511       2 0090.6f7a.1c80 47.00001606288000100000000F.00906F7A1C80.02
```

Figure 3-17. Show LANE Server.

The shaded lines in Example 3-17 show two LES components, one on interface ATM 0.1 and one on ATM 0.2. Both LESs are shown to be fully functional, listed in the operational state. Also note that the ELAN name is given for each LES. Viewing BUS Status To view the status of a BUS, use the **show lane bus** command. Example 3-18 demonstrates this command on the same switch used in Example 3-14. This switch is configured as the LES/BUS for two ELANs.

show lane bus *Output Displays BUS Status*

```
CatalystA_ATM#show lane bus
LE BUS ATM0.1  ELAN name: lan1  Admin: up  State: operational
type: ethernet          Max Frame Size: 1516
ATM address: 47.00001606288000300000000F.0050A28D5882.01
data forward: vcd 1499, 2 members, 523298 packets, 0 unicasts

lecid   vcd       pkts    ATM Address
      1 1489    505572 47.00001606288000300000000F.0050A28D5880.0B
      2 1506     17726 47.00001606288000100000000F.00906F7A1C80.01

LE BUS ATM0.2  ELAN name: lan2   Admin: up   State: operational
type: ethernet            Max Frame Size: 1516
ATM address: 47.00001606288000300000000F.0050A28D5882.02
data forward: vcd 1451, 2 members, 0 packets, 0 unicasts

lecid   vcd       pkts    ATM Address
      1 1433            0 47.00001606288000300000000F.0050A28D5880.0C
      2 1512            0 47.00001606288000100000000F.00906F7A1C80.02
```

Figure 3-18. Show LANE BUS.

The shaded lines in Example 3-18 show two BUS components on interfaces ATM 0.1 and ATM 0.2. Both BUSs are in the operational state and are listed with their respective ELAN names. Each BUS is also shown with a breakdown of packet forwarding activity to individual LECs within the ELAN.

Viewing LEC Status

To view the status of a LANE Client, use the **show lane client** command as demonstrated in Example 3-19 for a switch with two LECs (two ELANs).

show lane client *Output Displays the LEC Status*

```
CatalystA_ATM#show lane client
LE Client ATM0.11   ELAN name: lan1   Admin: up   State: operational
Client ID: 1                        LEC up for 11 days 2 hours 43 minutes 9 seconds
Join Attempt: 20
HW Address: 0050.a28d.5880    Type: ethernet                  Max Frame Size: 1516
            VLANID: 1
ATM Address: 47.00001606288000300000000F.0050A28D5880.0B

 VCD   rxFrames   txFrames   Type          ATM Address
    0             0             0   configure
47.00001606288000300000000F.0050A28D5883.00

1477          1     480139   direct    47.00001606288000300000000F.0050A28D5881.01

1481      480140             0   distribute
47.00001606288000300000000F.0050A28D5881.01

1491          0     505675   send      47.00001606288000300000000F.0050A28D5882.01

1495      17729          0   forward   47.00001606288000300000000F.0050A28D5882.01


LE Client ATM0.12   ELAN name: lan2   Admin: up   State: operational
Client ID: 1                        LEC up for 11 days 2 hours 43 minutes 12 seconds
Join Attempt: 19
HW Address: 0050.a28d.5880    Type: ethernet                  Max Frame Size: 1516
            VLANID: 2
ATM Address: 47.00001606288000300000000F.0050A28D5880.0C

 VCD   rxFrames   txFrames   Type          ATM Address
    0             0             0   configure
47.00001606288000300000000F.0050A28D5883.00

1403              1             2   direct
47.00001606288000300000000F.0050A28D5881.02

1421              2             0   distribute
47.00001606288000300000000F.0050A28D5881.02

1439              0             0   send
47.00001606288000300000000F.0050A28D5882.02

1445              0             0   forward
47.00001606288000300000000F.0050A28D5882.02
```

Figure 3-19. Show LANE Client.

Each LEC that is present on the local switch is listed with the show lane client command. The shaded lines show that there are two LECs on this switch—one assigned to interface ATM 0.11 and one to ATM 0.12. Both are up and operational. The most important information given here are the LEC uptimes and join attempts. Here, both LECs have been up for a little more than 11 days. When a LEC is not operating properly, this command will show that the LEC is down and how many attempts the LEC has made to

join the ELAN. A timer value will also be shown that tells when the LEC will try to join the ELAN again.

Automatic NSAP Address Generation for LANE Components

LANE Component	Prefix	ESI	Selector
LEC	From ATM Switch	MAC Address	ATM Subinterface
LES	From ATM Switch	MAC Address + 1	ATM Subinterface
BUS	From ATM Switch	MAC Address + 2	ATM Subinterface
LECS	From ATM Switch	MAC Address + 3	.00

Summary of Catalyst LANE Configuration Commands

Catalyst Command	Function
show lane default	Display default or autoconfigured NSAP addresses for all LANE components on the switch.
session *module-num*	Open a user interface session with the switch module in slot *module-num*. This is needed to begin a session with a LANE module.
lane server-bus ethernet *elan-name*	Configure LES/BUS pair on an ATM subinterface (subinterface config mode).
lane database *db-name* **name** *elan-name* **server-atm-address** *les-nsap-address* **name** …	Configure LECS database.
lane config-database *db-name* **lane config-auto-atm-address**	Apply LECS database to an ATM major interface (interface config mode); Configure automatic ATM NSAP addressing for LANE components.
lane client ethernet *vlan-num elan-name*	Configure LEC for VLAN number and ELAN name on ATM subinterface (subinterface config mode).
show lane server	Display status of LES on the switch.
show lane bus	Display status of BUS on the switch.
show lane database	Display status of LECS on the switch.
show lane client	Display status of LEC on the switch.

Figure 3-20. ATM LANE Commands.

Summary

In this objective, we introduced you to the Cisco Internetwork Operating System (IOS), ATM LANE components, user interfaces, how ATM switches and ATM router modules are configured, as well as how to manage the configuration. It is important that you have a firm understanding of the basics offered in this section before you move on to other areas dealing with integrated network design.

INTEGRATED NETWORK DESIGN

Objective 3e: Working as a team member using equipment and materials provided, configure an integrated network design IAW Performance Specification II-3e.

INFORMATION

The previous few sections have explained how to configure routers, switches, and ATM components. Now we will take all of this knowledge and use it to create a network that integrates all of these pieces. Network integration is concerned with joining networks and systems together, not creating them from the ground up. The following text assumes there will be a full class load of twelve students to accomplish the lab. The lab consists of the following pieces of equipment.

- Four Cisco LS1010s
- Eight Cisco 4000 series routers
- Four Cisco 3600 series routers
- Twelve Cisco 2900 series XL switches
- Four Cisco 3500 series XL switches
- Twelve workstations running Windows 2000

The interface modules range from ATM and Gigabit to your basic Ethernet RJ-45 and console connections. If you have any problems with the connections or patch panel appearances, bring them to the attention of your instructor.

Note: Remember from the previous sections, a console port requires a rollover cable. The patch panel has been wired to account for this rollover.

During this objective, you will integrate the equipment already configured from the previous text and labs. The lab design has already been accomplished and will require minimal wiring of equipment. The majority of work required for this lab will be modifying configurations. You will need to coordinate with other student groups to confirm IP addresses, subnet masks, routing protocols, etc. The student PCs will remain connected to the existing VLANs, which will be routed within their autonomous systems via their internal routing protocol. The separate autonomous systems will be joined via an external routing protocol, such as BGP, through the ATM network.

IP ADDRESSES

IP addresses are always a concern when integrating two previously unconnected LANs. Although no single classful network is ever assigned to two different organizations by the INTERNIC, problems may arise from joining LANs that have not previously been connected to any external network. In this case, the network could have been configured with any IP network address. Remember, IP addresses must be unique on the Internet. So, prior to integrating any networks together, all IP networks that exist in either LAN should be coordinated. If the same network address is advertised by more that one LAN, it will be difficult for a router to make a correct decision.

LAN TO WAN CONNECTIVITY

There are many ways to connect your LAN to a WAN. Connectivity decisions will be based upon existing equipment capabilities, the ability to acquire new equipment and the requirements of the WAN.

ROUTING PROTOCOLS

Internal routing protocols can be whatever is best for the LAN. Exterior routing protocols are a different story. You must coordinate the exterior routing protocol with the WAN provider and/or the network managers of the LANs you are going to exchange routing information with. In the 7-level lab, you will have to coordinate with students from all other rack groups, as you will be exchanging routing information with all other groups. The routing protocol has to be agreed upon, along with autonomous system numbers, IP network addresses and IP addresses of each border router that you will be integrating with.

TESTING WAN FUNCTIONALITY

Once the equipment has been wired appropriately and all equipment has been configured correctly, the student will be able to verify any interface connection and pass traffic through or to any host on the network. This can be verified through the use of PING, Telnet, tracert, etc.

SUMMARY

Integrating networks cannot be viewed as building a network. It must be undertaking from the viewpoint of changing what already exists to interoperate with another system. Topics such as IP addresses, LAN to WAN connectivity, routing protocols and finally, testing WAN functionality have to be planned for and well coordinated.

Note: This network design will be utilized in the next chapter on network management systems (HP Openview). Notify your instructor upon completion of the integrated network design lab.

CHAPTER FOUR

NETWORK MANAGEMENT

OBJECTIVES

4a: Using network equipment, configure a network management system on a network IAW Performance Specification II-4a.

4b: Using a network management system, analyze network performance IAW Performance Specification II-4b.

4c: Using training equipment and materials provided, perform protocols analysis IAW Performance Specification II-4c.

4d: Using network monitoring software, generate configuration reports IAW Performance Specification II-4d.

INTRODUCTION

This chapter will help you to understand how Network Management Systems (NMS) assist us as network technicians. It will describe the purpose and capabilities of an NMS as well as some of the installation considerations. At the end of the chapter, you will understand how a NMS greatly enhances our troubleshooting ability and the necessity of such a system on the network.

NETWORK MANAGEMENT SYSTEM

Objective 4a: Using network equipment, configure a network management system, on a network IAW Performance Specification II-4a.

INFORMATION

NETWORK MANAGEMENT SOFTWARE

In today's technology-driven world a unit's success can be dependent upon its ability to effectively implement emerging technologies. As the Air Force increases its dependence on these complex technologies for a greater portion of its daily operations, it becomes more dependent on organizations to provide these critical services. As a network technician, you are under increasing pressure to perform the necessary tasks to meet the mission demands of your organization.

Some of the challenges you often face include:

- Dealing with user dissatisfaction in the face of increasing user expectations. Users want to be able to have the tools they want, when they want them to maintain their productivity.
- Deploying network services so end users maintain productivity from their desktop systems.
- Keeping the systems operating 24 hours a day, 7 days a week.
- Producing faster, more predictable response times.
- Integrating and managing diverse and complex technologies — networks, servers, databases, applications, web-based systems—all from different vendors.
- Managing multiple sites and global distribution.
- Moving to proactive management techniques to keep it all running smoothly.

Clearly, the demands on a network technician are great. Network management has become a high-pressure situation where more and more services are requested on tight schedules and with less and less resources. Network Management Software can help you work this miracle.

PURPOSE OF NETWORK MANAGEMENT SOFTWARE (NMS)

Network management can be defined in general terms as the ability to have a single point of control to accomplish the activities required to manage a network. NMS provides an integrated tool for the network manager to control and manage multiple networked systems and applications from a single graphical representation of the network. NMS works for you in the following ways:

- Map out your network for you. The map symbols change color to indicate if something is wrong.
- Collects critical information about your network and maintains a current log of alarms.
- Correlates collected information to help you quickly determine the root cause of problems.

Network Management Software is used to accomplish the ISO Management Model's five areas of management. This software is designed to allow the network administrator to monitor the network devices. It can show you when a device is down, if there is a potential problem on the network, and how to correct network faults. With the increasing size of networks, it is becoming more difficult to effectively manage a network. NMS

enables you to do this with relative ease. The Air Force standard of NMS is Hewlett Packard's Openview®. HP Openview® allows network administrators to effectively manage and control the network.
HP OpenView Network Node Manager (NNM) is a Graphical User Interface (GUI) tool that provides a foundation for network administrators to have a hands on approach to efficient network management. This NNM tool automatically discovers objects on the network using a continual polling process through multiple protocols. Two protocols that will be discussed, are Simple Network Management Protocol (SNMP) and Transmission Control Protocol/Internet Protocol (TCP/IP). The network is polled for the status of objects, topology changes, and configuration changes to ensure that everything is running. A combination of alarm messages and color schemes provides information on how the network is operating. If a node goes down, a message is generated, and the status color of that object will change from green (normal/up) to red (critical/down).

HP OpenView NNM also provides the ability to monitor and identify trends on your network. This enables the Administrator to see how they can best regulate the network and monitor established thresholds in reference to critical node devices. Additional functionality includes the ability to oversee everything discovered on the network and to manage individual subnets. This allows the administrator to manage objects that can be detrimental to the network and unmanage objects that are not of importance. Examples of objects that are unimportant may be workstations and printers. The more objects you manage, the more system resources you use. Increased traffic hampers the network with equal usage of bandwidth, lost time and loss of resources in general. The remainder of this objective will lead you through the process of understanding, configuring, customizing, and using NNM.

Simple Network Management Protocol

In order for NNM to operate, a specific protocol must be running on all smart devices on your network. This protocol is Simple Network Management Protocol (SNMP).

Note: TCP/IP must also be installed and running in order for SNMP to run.

SNMP is the most common management protocol in use in data networks. It provides a means of obtaining information from, and sending information to, network devices. Using the SNMP protocol, a manager can query and modify the status and configuration information on each managed device by making requests to the agent running on the managed device. SNMP operates at Layer 7, the Application Layer, of the OSI Reference Model.

INSTALLING NETWORK NODE MANAGER

The procedure below will help you install your NNM product.
Insert the NNM product disk into the CD drive. The InstallShield setup wizard program starts automatically. If it does not, from the Start menu on the Windows NT operating system task bar, Select Settings: Control Panel and then Add/Remove Programs.

In the Add/Remove Programs Properties dialog, at the Install/Uninstall tab, select Install. The InstallShield Wizard begins and guides you through all the necessary steps in the installation process. The wizard checks to see if the SNMP Trap Service is running. This service is incompatible with NNM. If prompted, specify Yes to shut down this service (or No to exit the wizard program). In the Setup Options dialog, choose the NNM installation you want to do (Table 4-1 describes each installation type):

Installation Type	NNM Components Installed	Description about Installation Type
Typical	- executable program files - background graphics	
Remote Console	See the manual, *A Guide to Distribution and Scalability for Network Node Manager*, for instructions on doing this installation.	Your system will: - have only HP OpenView Windows processes on it - connect to a management server running the NNM common databases and background processes
Compact	- executable program files	
Custom	Choose from: - executable program files - background graphics - contributed applications - SNMP MIBs - SNMP RFC papers - online user manuals - technical white papers	You can specify which NNM components you want to install.

Table 4-1. Installation Options.

1. Choose the installation type you want. The wizard then displays several graphics showing the progress of the installation.
2. If errors occur during the installation, the wizard will ask if you wish to view the setup log file.
3. When the Setup Complete dialog appears, the wizard has finished the installation. You can now choose one or more options:

4. Display online the NNM Release Notes
5. Start NNM immediately
6. End your work session
7. Choose the option or options you want, then select Finish.

RUNNING NETWORK NODE MANAGER

If you did not automatically launch NNM at the end of the installation process, you can use the following procedure to do so now.

1. First, start the background processes which support NNM's native graphical user interface (GUI), HP OpenView Windows. From the Start menu on the Windows NT operating system task bar,
2. Select Programs:HP OpenView:Network Node Manager Admin:NNM Services-Start.
3. Next, start HP OpenView Windows.
4. Select Programs:HP OpenView:Network Node Manager.
5. You will see the HP OpenView welcome banner, followed by an NNM Root submap window with a default map in it. Each time you start the NNM GUI, it will encourage you to register your NNM product if you have not already done so. You have 60 days from the date of installation to complete this registration process (described in Task 5).

Network Node Manager Terms

Before you can setup NNM to meet your needs, there are some terms you need to know. The first of these is the difference between a map and a submap. You can think of the relationship between maps and submaps as being much like the relationships between an atlas and its pages. The atlas is the map. The pages of the atlas are the submaps where you may view a particular continent, country, state, city, or even specific parts of a city. In NMS, when you view a part of your network map, you are actually viewing a submap. The view may be presented in a high-level submap which represents your entire network, or in a more detailed submap of any portion of the network.

Maps. Maps are sets of related objects, symbols, and submaps that provide a graphical and hierarchical presentation of your network and its systems. You can create multiple maps, but only one map is open at a time for any given session of NMS. You do not view a map directly; instead, you always view the submaps that comprise the map. You can display multiple submaps at any given time. Submaps are organized hierarchically to show an increasing level of detail. Different maps can be used for defining different management regions, or for different presentations of the same management region. Different maps can be tailored to the needs of individual users. You can create multiple maps and customize how information about objects is displayed on each map. Different maps can display information about the same object because maps obtain their information from the same source, the object database. In NMS, you can create new maps, delete maps, and choose the map to display from existing maps. When you start NMS, a map is automatically opened. You can specify a map by name, or you

can let HP Openview® open a default map. While a map is open for display, it is simply called an "opened map". Remember, maps are just the files that hold the information (submaps) within it.

Submaps. A submap is a particular view of the network environment. It consists of related symbols displayed in a single window. Each submap displays a different perspective of your map. NMS creates a root submap for each map. Submaps are often organized in a hierarchical fashion for a given map, with the root submap at the top. The submap you have first displayed when you open a map is called a Home Submap. You can also create independent submaps not associated with a hierarchy. You can open and display multiple submaps of the open map at any given time, either by listing all the submaps of the open map and selecting the submaps to open, or by navigating from one submap to another. You can navigate among the submaps of the open map by double-clicking the mouse on explodable symbols. Double-clicking on an explodable symbol opens a submap that displays a more detailed view. For example, if you click on an icon of a computer, it will explode and show the Network Interface Card (NIC) within the computer.

The hierarchical relationship of submaps creates a parent-child relationship between them. A submap may have several child submaps. The hierarchical relationship of submaps enables you to view your network from a distance, or to choose a more detailed view. For example, consider a submap that contains a single symbol that represents an entire organization. From this high-level view of the map, you can double-click on an explodable symbol to open a child submap. The child submap may display a view of your network map from the perspective of a particular location. From there, you can select a specific department, then a specific node-all represented by explodable symbols. You can customize the organization of submaps in a map to suit your purposes, for example, to reflect the organization of your company. There are five default levels of submaps created when you install HP Openview®. They are as follows:

- The root level is created by the system when HP Openview® is installed. It allows for the placement of objects by multiple applications at a very high level.
- The internet level shows any IP networks, gateways and the main routers on the network..
- The network level shows the segments, switches, hubs, and bridges.
- The segment level shows the host computers, routers, hubs, and switches.
- The node level shows network interface cards of the individual device.

Figure 4-2 shows an example of the five different levels of submaps.

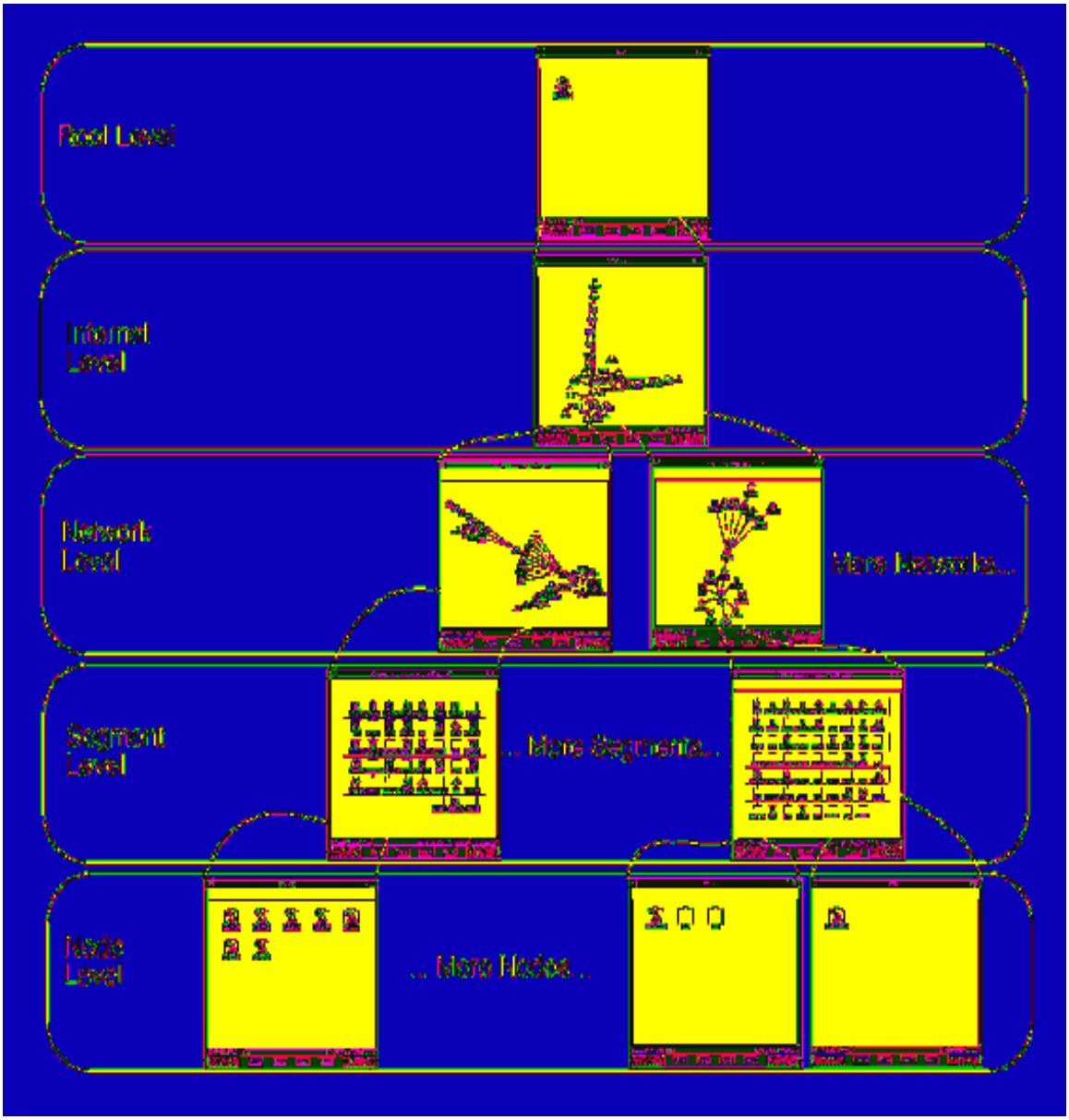

Figure 4-2. Five Submaps of NMS.

Objects. An object represents a particular device or resource in a networked systems environment. An object might represent a physical piece of equipment on the network, the components of a node on the network, or parts of the network itself. The object represents the resource by modeling the characteristics (attributes) of the resource. An object exists on a map by virtue of being represented by a symbol on a submap in a map. An object represents a logical or physical device or resource, or a group of such logical or physical devices or resources that exist in a network environment. An object usually represents any particular thing of interest for the purpose of doing network or

systems management. An object can represent a physical item (such as a PC, a workstation, a gateway, a router, an interface card, or an RS-232 connection), or it can represent a logical item (such as a group of PCs, all NT Workstations, or all nodes in a single department).

An object does not have to have SNMP loaded on it. Now many will think because it does not have SNMP, then the manager cannot manage it. Well, that is true and false. Without SNMP, the manager cannot tell manufacturer, model or configuration of the device, or if thresholds are being exceeded, but it can still tell if the device is up or down using TCP/IP. So if the device has an IP address but no SNMP then the manager has limited knowledge of the device.

Symbols. A symbol is a graphical representation of an object. A single object can be represented by multiple symbols. Multiple symbols for the same object can exist on the same submap, on multiple submaps of the same map, or on submaps of different maps. This enables multiple users on different maps to view a symbol of the same object at the same time. A symbol never represents more than one object at a time. NMS uses two varieties of symbols for display on the map: icon symbols and connection symbols.

In addition to representing objects, symbols have other functions:

- Symbols let you navigate through the submaps of a map. Most symbols are explodable—when you double-click on an explodable symbol, a new submap window opens to let you "look inside" the object represented by the symbol. Some symbols execute actions. When you double-click on an executable symbol, a predefined action is executed on a predefined target.
- Symbols can be configured to reflect the status of the object they represent or of objects in child submaps.

Figure 4-3 shows how symbols and objects are related. This figure contains two submaps having different symbols. Object Y is represented by a single symbol in the root submap, while Object X is represented by symbols in both the root submap and submap2. Changes made to Object X, such as a change in status, can be displayed in both symbols in the two submaps.

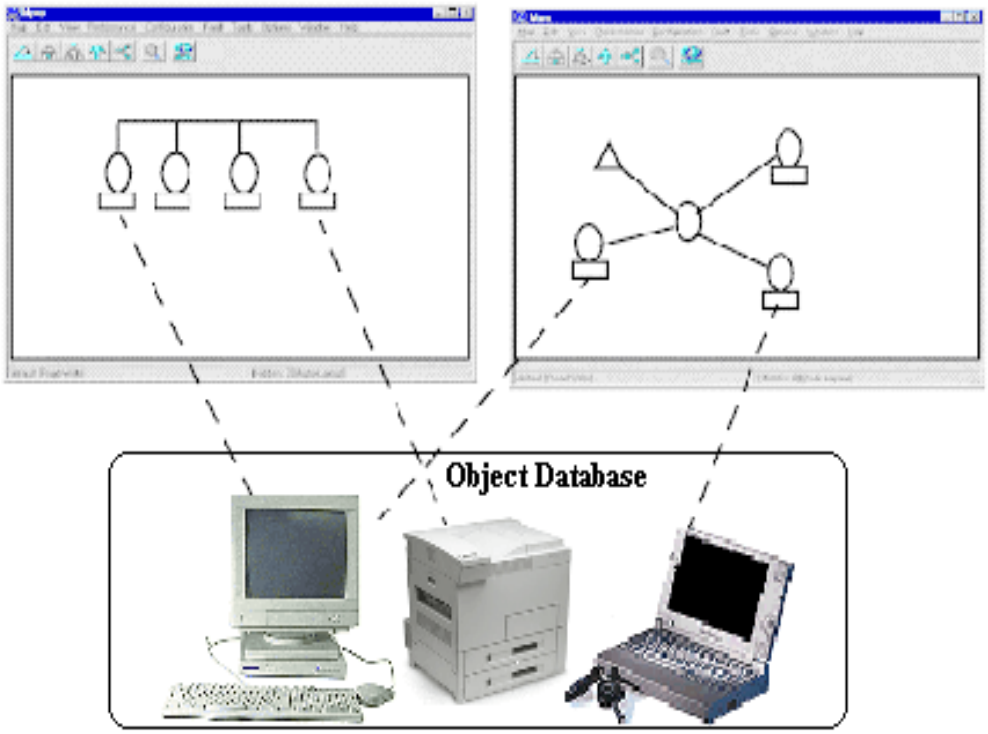

Figure 4-3. Object-symbol Relationships.

AUTOMATIC DISCOVERY AND LAYOUT

When you start NNM's background processes, all IP devices on your network are automatically discovered and mapped out. If you are using NNM on a management station running the Windows NT operating system, IPX devices are also discovered and mapped out. This map is a visual representation of the communications channels established between NNM and the devices in your network. Be aware this map is not a physical representation; rather, it is a logical representation. The accuracy of these communications channels between NNM and your network devices determine whether or not NNM can provide the information you need in order to manage your network. The initial polling process may take several hours, or even over night, to discover all the devices on your network. However, it is worth the wait! You start benefiting from NNM immediately. You will use NNM's default map, and Alarm Browser to pinpoint any gaps in your well-configured network scheme. When Auto Layout is turned on, symbols are placed automatically in the appropriate submap according to the established pattern for that submap. If Auto Layout is turned off, the user will be able to customize the arrangement of the symbols. Consequently, any objects discovered will be placed in a

holding area until they are moved into the map. Figure 4-4 shows an example of a submap using Auto Layout.

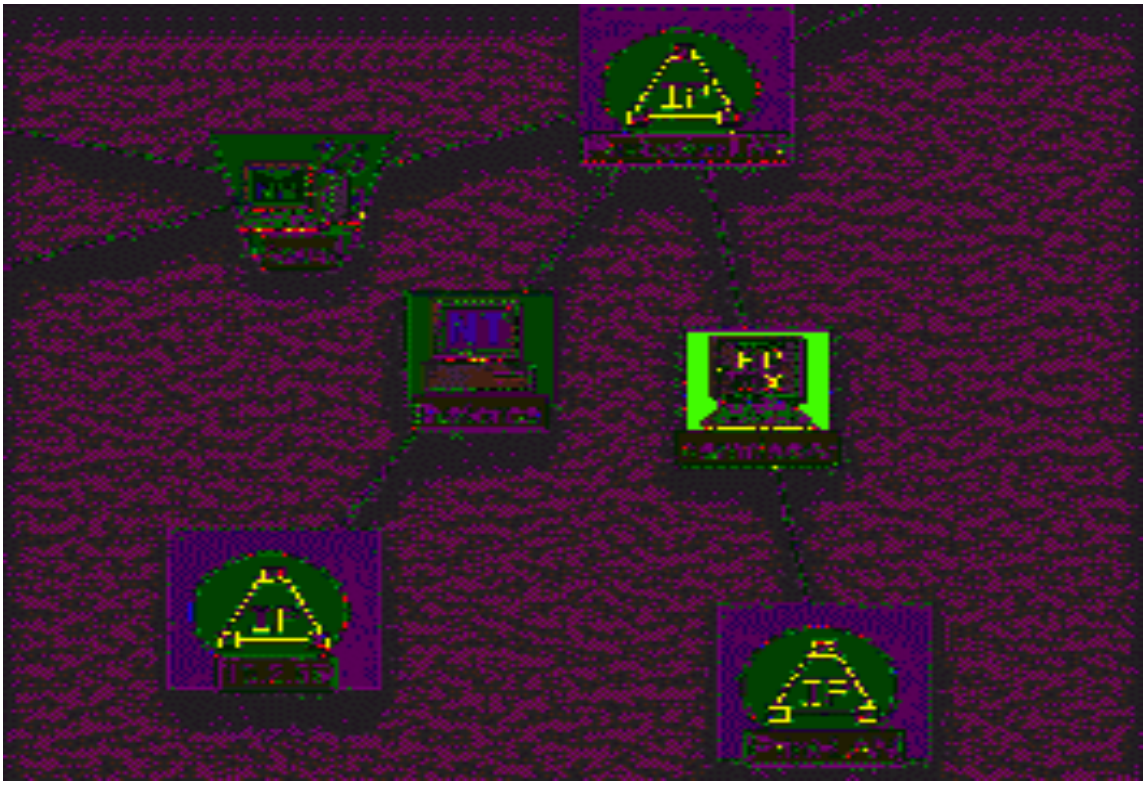

Figure 4-4. An Example of a Submap.

Managed Versus Unmanaged Object

Polling is a function that lets you check if a network device's status is up or down. A managed object is one actively being polled by NNM to determine its status and configuration. An unmanaged object is one that exists in the databases and within maps, but is not being polled by NNM. NNM gives you the choice of managing or not managing objects, depending on your information needs and network resources. When an object is managed, NNM can obtain any information you specify about that object (as long as the object's protocol is supported). The more objects you manage, the more memory and disk space is required on the management station. In addition to the information you specify, the management station will need processing power for the routine status and configuration polling and the event monitoring of each managed object. If an object is critical to the network function, then you should manage it. If the

object is not critical to the functioning of your network, you might choose to unmanage it. This means NNM will not actively monitor the object. When an object is unmanaged, less memory, disk space, and processing time are required on the management station. However, you only get minimal information about that object on your map.

Status Polling

For each managed IP device, a ping is issued to verify if it is still accessible by the management station. The default interval for IP devices is once every five minutes. Often, the default setting of five minutes for every device is not optimal. You will probably want to poll mission-critical devices more frequently. Some customers decide not to poll certain devices at all, such as end-user PCs or certain printers.

As you learned in a previous block, DHCP is used in many networks today. It is useful in environments supporting mobile users who connect to the network from many different places with a laptop. You can specify the range of IP addresses your network assigns mobile devices. The addresses will still assign them dynamically using DHCP. As mobile users connect their machines from the network, NNM will see them and add them to the map. When they disconnect, NNM does not know if the devices are disconnected or if there are problems. So alarms will keep showing up in the Alarm Brower, which causes a good deal of clutter on the map. To reduce this clutter, a filter can be implemented. The default for this feature is OFF (no filter in use). If this filter is enabled, NNM keeps the map clean of unnecessary messages about devices within this address range as they are repeatedly attached and detached from your network. You can control status polling in the following ways:

- Set polling intervals on specific nodes by IP address, IPX address, or hostname. For IP addresses only, you can set polling intervals using IP address wildcards for a group of IP nodes (for example, 15.122.*.*). The IP address wildcard is useful, for example, when you want to configure different values for time-outs or the number of retries for Wide Area Networks (WANs).

- Set the status polling interval to be used for any device not specifically listed. If you set it to 24-hours, polling begins at the time you enter the setting. The actual time may drift depending on network conditions.

- Specify time-out and retry values. For example, you may want to increase the time-out and retry count values to prevent the management station from a premature time-out when making requests across a WAN because latency times

are greater over WANs than LANs. Note the time-out value is set in tenths of a second, and the time-out value doubles with each retry.

NNM CUSTOMIZATION

Now that you are familiar with the terms associated with NNM software, let us look at a scenario. Working at the help desk one day, you decide to look at what is happening on the network. You start the NNM software by clicking on the shortcut on your desktop. When the software starts running, it loads the default map. Figure 4-5 is an example of a Root submap, as indicated by the screen's banner.

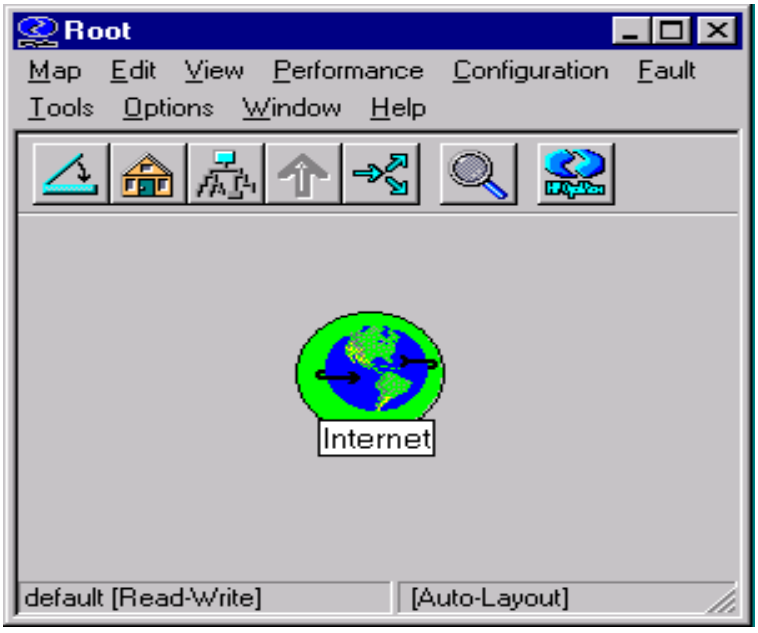

Figure 4-5. Root Submap.

The first thing you see is an icon labeled Internet. The reason for this is you are automatically placed in the root submap so the next level you can go to is the Internet. You need to see how the servers are doing in network 158.157.10, so you explode the Internet submap by double-clicking the Internet icon. Figure 4-6 is an example of an Internet submap.

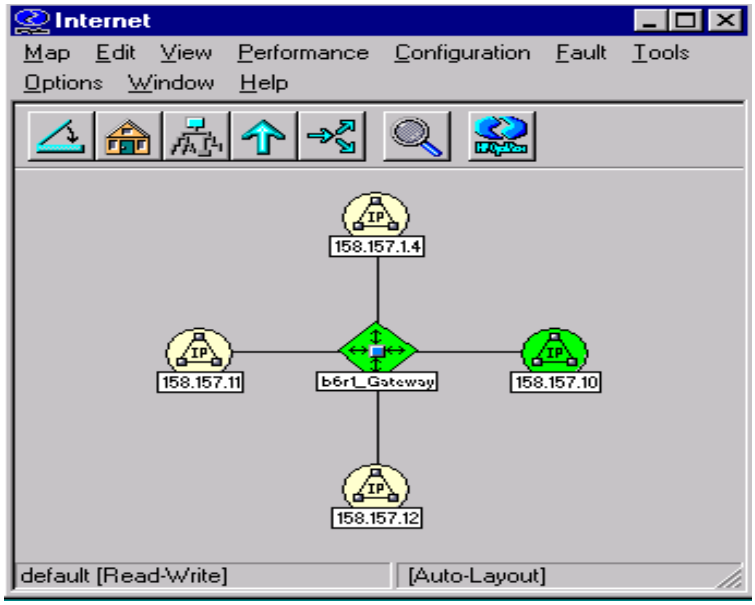

Figure 4-6. Internet Submap.

Now you will see any routers, switches, and networks directly in the Internet submap. These devices should be the main devices on the backbone. There are no computers at this level. However, you do see a router (b6r1_gateway) with an icon connected to it which says 158.157.10. As stated before, this is the network the servers are on that you want to look at. You then explode the 158.157.10 Network submap to find a switch with a segment connected to it. Figure 4-7 is an example of the Network submap.

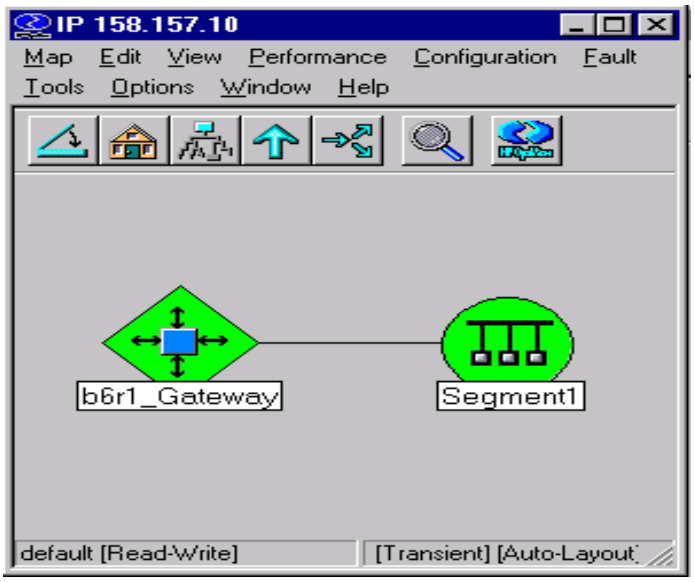

Figure 4-7. Network (158.157.10) Submap.

You then explode the segment to find all the devices. Figure 4-8 is an example of the Segment submap.

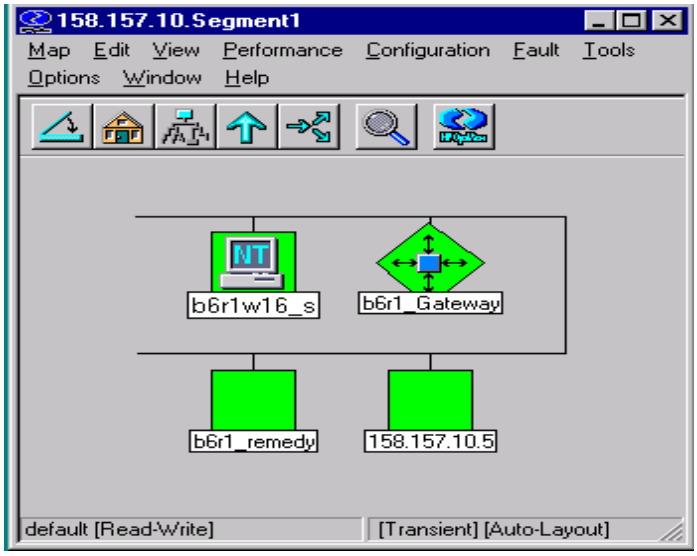

Figure 4-8. Segment (1) Submap.

From there, you can set up polling on each device you want to monitor for problems.

SECURITY OF NNM

HP Openview® has no real security management features, however due to SNMP being used, there are ways to access your devices through the NNM. You can change settings on different devices just by having access to the SET community string. It is important to realize how dangerous it can be to your network if you do not secure access to HP Openview®. There are many ways to protect the databases NNM uses. Two factors determine whether a map is opened with read-write access or with read-only access. First, only one user can have a specific map opened with read-write access at any one time (the first person to access the map). Second, you can use the file system (FAT or NTFS) to purposely allow specific users read-write or read-only access to a map by setting permission to the files. Possible permission settings are:

- **Read-write**. Accessing a map opened with read-write access is completely editable. You can add objects, add connections, create submaps, and change object attribute values. Only one user can have a specific map open with read-write access at any one time. If another user has the map open with read-write

access, when you open the same map, you will have read-only access. This is the case even if you have read-write permission from the operating system. This prevents multiple edits on a single map at the same time.

- **Read-only.** A map opened by a user with read-only access is not editable, although the map still can receive status from applications. Having a map opened with read-only access, you can still view status changes, perform locate operations on objects, and update topological changes using the **Map>Refresh Map** menu item. However, you cannot add, delete, or modify items in the map, including symbols, objects, submaps, and map snapshots.

- **No Access.** You cannot open a map if you have No Access.

It is very important to decide who needs what access. You do not want to give too many people read-write access to the maps. It might seem like deleting a symbol is not that big of a deal, but it can cause your database to become corrupted. Also, if you give everyone read-only access to the database you cause a great deal of bandwidth to be used as everyone goes to view the status of the network

SUMMARY

Due to the growth of our networks, we have become increasingly dependent on automation to help us management and troubleshoot our networks. HP Openview® is the Air Force standard for solving those problems and an understanding of how it works is key to maintaining mission ready systems.

PERFORMANCE ANALYSIS

Objective 4b: Using network management system, analyze network performance IAW Performance Specification II-4b.

INFORMATION

FAULT ISOLATION

Status polling, as you know, polls every device on the list to determine whether the devices are up or down. How does the software let you know when a device is down? The answer is the alarm browser.

Alarm Browser

What is an alarm? An alarm is an indication a noteworthy event has occurred on the network. This could be something as simple as a device being powered on. The alarm browser gives the network administrator instant awareness of failures. NNM's Alarm Browser guarantees the speediest possible response, since your team members know instantly when trouble arises. It allows for watching trends on your network so you can identify bottlenecks.

Configure NNM to post threshold alarms from your mission-critical devices. The help desk can detect developing trouble and start resolving it before users encounter network failures. The alarm browser will identify the device most likely causing the problem. Figure 4-9 shows an example of the alarm browser.

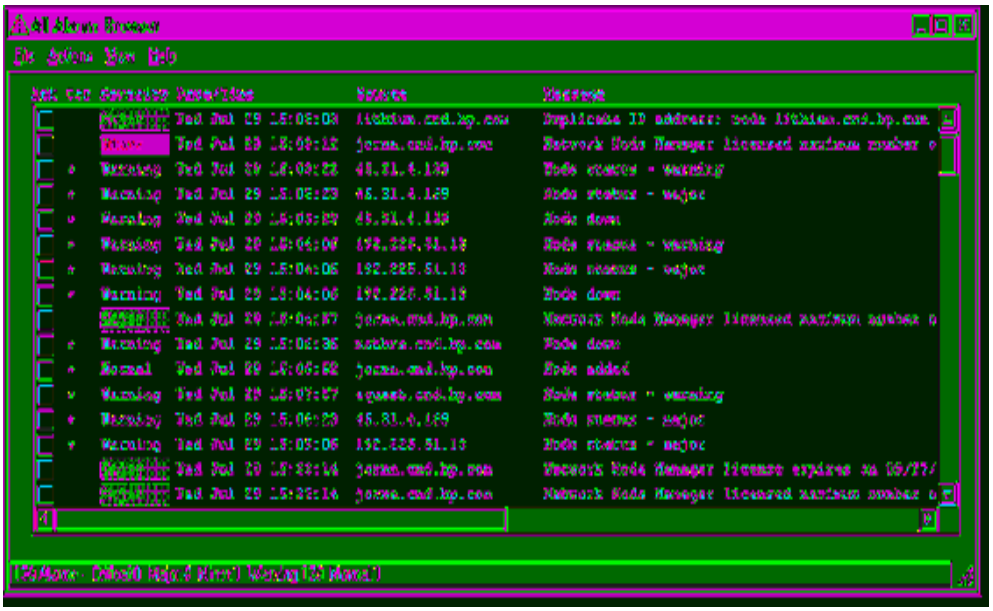

Figure 4-9. Alarm Browser.

Automatic Responses

You can configure NNM to automatically page or email a specific person whenever an alarm is received about a specific device. You can also configure a pop-up window to appear over the NNM map if a certain event occurs. This allows the facilitation of team communication to eliminate duplicate efforts. Your support team can use NNM's Alarm Browser as a prioritized to-do list. Each help desk member can select issues to work on and change the alarm's status to Acknowledged. Everyone on the team will see immediately the alarm is being addressed. This allows the administrator to distribute responsibility. You can set up custom categories for incoming alarms and configure specific devices to post their alarms to your custom categories. For example, configure the alarms generated by devices in each department to post their alarms to a category identifying the department. Your help desk members can access the alarm list that applies to them, without needing to sort through alarms for all departments.

Alarm Categories

NNM has an alarm color scheme to help the administrator quickly identify what sort of problem has occurred on the device. At a glance, the administrator is able to determine what action to take in dealing with that device. The administrator needs to understand when something of importance has occurred. Just looking at the categories will not tell you. This is why administrators need to know what the colors mean. Figure 4-10 shows a table of each color with the corresponding definition.

Status Condition	Meaning of Status
Warning (CYAN)	Object may face a potential problem
Minor/Marginal (YELLOW)	Object has a minor problem, may continue to operate normally
Major (ORANGE)	Object has serious problems; the device probably no longer operates normally
Critical (RED)	Object is not functioning
Unknown (BLUE)	Object status cannot be determined
Normal (GREEN)	Object is in a normal state

Table 4-2. Alarm Colors.

Now that we know what the colors mean, we need to know what to do with the alarms. You can click on the different alarms categories and it will give you details about the alarm. Figure 4-10 shows you the different categories of alarms.

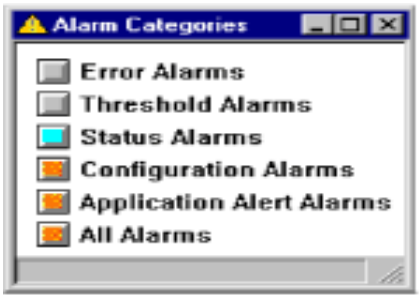

Figure 4-10. Table of Alarms.

Figure 4-11 is an example of the Configuration Alarms Category.

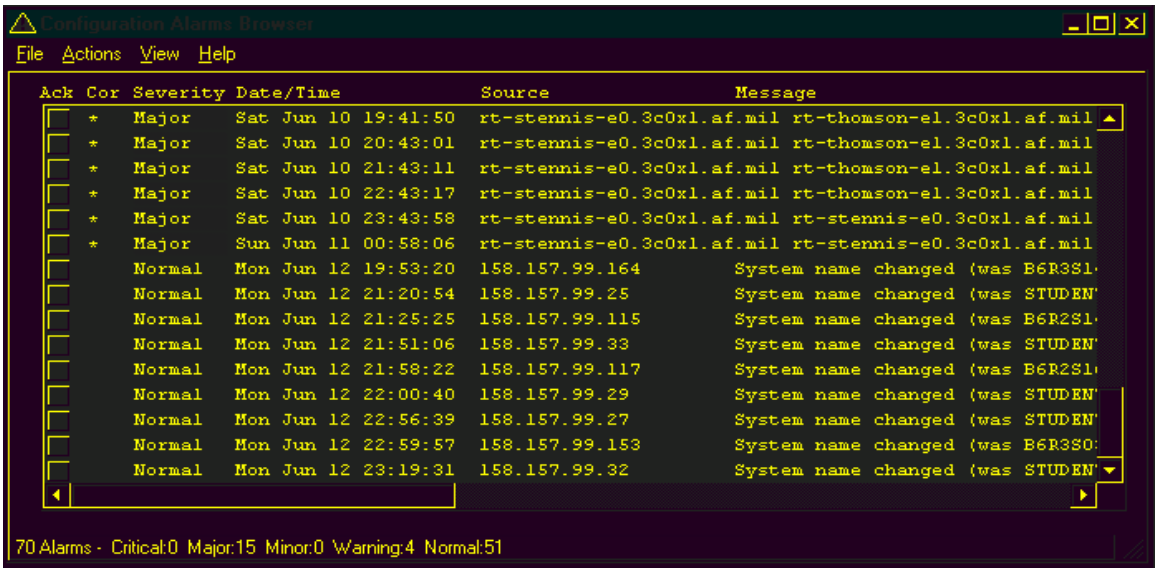

Figure 4-11. Alarm Browser Window.

The Alarm Browser Window divides the alarm into categories. They are as follows.

- Ack – Shows whether the alarm has been acknowledged (check mark) or not
- Cor (Correlation) – Indicates if this alarm is related to other alarms
- Severity – Shows the severity of the alarm
- Date/Time – Shows the date and time the alarm occurred
- Source – Indicates what device had the alarm

- Message – Gives a brief description of the alarm

The above example indicates there is a problem with rt-stennis-e0.3c0x1.af.mil. This alarm has not been acknowledged, meaning no one is currently working on the problem. We can see the alarm severity is major and because of the message column, we know it is due a connection with another device because of the second name in the message box. This is a great deal of information. You can also set up the alarm browser to group the alarms the way you want them. You can see all the alarms by going to the All Alarms category. If you want to see only application alarms, you can click on the Application Alarms category. What if you only want to see alarms about a specific device? All you need to do is select the device, right click on it and go down to the Alarms option. This shows you all the alarms for that specific device. Once you have this information, you acknowledge or even delete this alarm. Deleting an alarm is not always a good idea. Many times administrators keep databases of reoccurring alarms. This helps them know when it is time to get a new device, or if the current device needs repairs.

EVENT CORRELATION SYSTEM (ECS)

The column labeled Cor in the alarm browser is an indicator the Event Correlation System (ECS) is working. It tells you if the alarm is related to other alarms. For example, if a router goes down, then it stands to reason you will not be able to access any devices connected to that router. NNM will show only the one alarm about the router, instead of you receiving forty alarms about all the devices going down. ECS improves the information content of alarms by suppressing unwanted, redundant alarms and adding new, more meaningful alarms. This results in fewer, but more informative alarms that show you the relationships and dependencies between network events. It then becomes easier to identify trends, to isolate important events, and to react more quickly to problems. You view these events through NNM's Alarm Browser. ECS involves processing events based on relationships between individual events. Event correlation system:

- Analyzes events based on previous, current, or subsequent events.
- Can create new events. By analyzing the relationships between events in the stream, single events can replace groups of events. These events may have increased information content, and can be of a different protocol, compared to the original events.
- Dramatically reduces the number of alarms displayed by NNM's Alarm Browser.

To show correlated alarms, select the alarm, and select **Actions> Show Correlated Events**.

With ECS, administrators have an easier time troubleshooting the root cause of the problem. This leads to quicker repair of the problem, thus maintaining a reliable network.

SUMMARY

Performance analysis is an essential task, as it can identify problems before they have a chance to cause an outage.

PROTOCOL ANALYSIS

Objective 4c: Using training equipment and materials, perform protocols analysis IAW Performance Specification II-4c.

INTRODUCTION

With the complexity of modern networks and increasing numbers of attacks by hackers, it behooves every network shop to perform protocol analysis at some level.

INFORMATION

ANALYZING NETWORK PROTOCOLS

There are numerous devices available to the advanced network analyst for performing protocol analysis. They range from dedicated computers built just for network analysis that cost many thousands of dollars to software applications that can be loaded on almost any personal computer (PC) that cost only a few hundred dollars. The choice will depend upon the complexity of the users' requirements and the budget of the purchaser.

A good network technician armed with a protocol analyzer can recover valuable bandwidth on a base or squadron network that has been lost to unnecessary protocols that frequently broadcast their presence. A prime example would be NetBEUI and IPX/SPX, which are installed on many PCs by default. If these protocols are not being actively used to support user requirements, their frequent broadcast traffic is merely wasting bandwidth.

The same technician can also identify malicious and accidental PING traffic that not only wastes bandwidth, but also prevents users from accessing the recipient computer while it processes each and every PING. Another common use is identifying computers that are sending unusually large amounts of traffic across the network. This could indicate anything from gaming between users to large amounts of .mp3 transfers to potential security risks.

In the right hands, a protocol analyzer can optimize a network as well as improve network security.

PROTOCOL ANALYZER FUNCTIONS AND MODES

As there are so many different protocol analyzers available, we will not attempt to describe exactly how to perform procedures in any specific one. Rather, we will discuss some of the more common functions and modes of operation required to monitor and troubleshoot your network.

Monitor

Monitor mode provides real-time views and decodes packets received by a device on a network segment. The data can be viewed in numerous ways and from different perspectives. Display of the data can be either graphical charts or row-and-column tables.

Capture

Capture mode allows you to capture data from a network and place it in system memory space (buffer) on an analyzer device. Filters can be created to only capture the information you want to view and analyze.

Filter

Filter mode simply allows you to separate out all data except what you want to see or capture. Most protocol analyzers let you create capture/display filters to collect and display only the information you want to view and analyze. Filters allow you to select and count data in just about any way you can imagine. These capture/display filters can also be saved for repeated use later.

Save

The Save function moves captured data from a capture buffer to a storage device on the host PC. This enables you to store captured data onto your hard drive for later viewing, analysis or transmission.

Log

Log functions record certain counter information to a file. This is valuable when you want to know the rate at which something has happened, but not necessarily examine the data packets.

VIEWS

There are numerous ways to view data from a protocol analyzer. This section describes the primary windows you use to view data and some of the actual data views you can see within each window.

The data views that can be seen within each primary window are described independently. Although you may be viewing data for different purposes from each primary view, the way the information is presented in a data view is virtually identical no matter which primary view you are using.

Summary View

Summary View is a global monitoring tool for network data. You can view real-time data from any local resource or any resource you can connect to on the network. You can filter the data before viewing by applying a filter. Summary View is intended to give an overall indication of the network, such as network utilization and simple error rates. Use Detail View to get many different views of a single resource or to perform detailed analysis functions on captured data.

Detail View

Detail View is the tool for performing detailed analysis of network data. You can view real-time data from the resource for which you have opened Detail View or you can view and analyze data stored in the capture buffer. You can filter the data before viewing it by applying a display filter. Detail View allows multiple views for a single category of information.

Data Views

Data Views can be applied to both monitored and captured data. The exact set of views available will depend on which mode the protocol analyzer is running in. Once data has been captured, it can be retrieved and viewed in numerous ways, depending on what the technician's needs.

Protocol Distribution View

Protocol Distribution View is available as a chart or a table. Protocol Distribution View shows the distribution of major network protocol types. The view can also be further defined into categories, such as:

NET. Shows percentages of all packets by network layer protocol type, such as IP, IPX and NetBEUI.

IP. Shows percentages of other protocols used within IP packets only, such as BootP, HTTP, ICMP, SNMP and Telnet.

IPX. Shows percentages of other protocols used within IPX packets only, such as Diagnostic, NBIOS, NRIP, NSNMP and SAP.

All. Shows percentages of all packets by application.

Figure 4-1 below show one example of a MAC layer protocol distribution chart. This chart shows 19.43% IPX traffic, 2.22% NetBEUI traffic and 4.79% "other" traffic. Assuming the system was monitoring a standard Air Force LAN (TCP/IP over Ethernet) at the time, there may be cause to investigate and find out why network bandwidth is being taken-up by protocols other than IP.

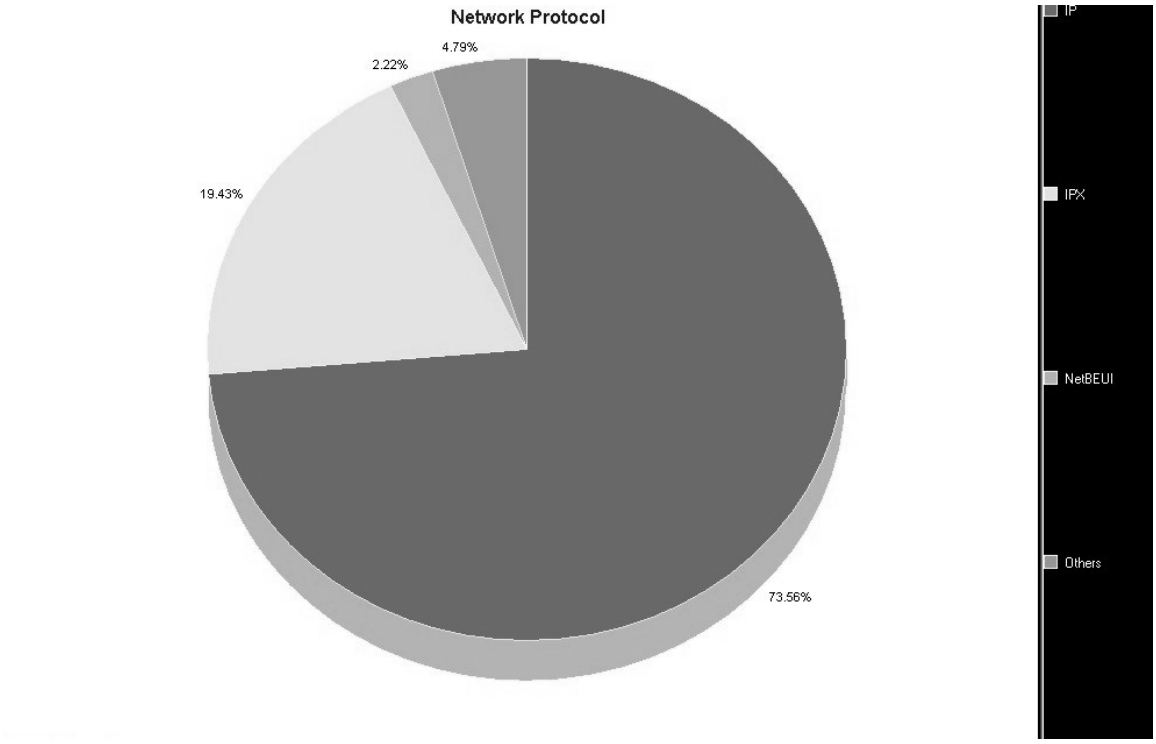

Figure 4-1. MAC layer protocol distribution.

Utilization/Error View

Utilization/Error View is a simple strip chart that plots points for network utilization over time. The scale for network utilization changes on the fly when a new peak percentage is reached. The time scale also scales automatically as the resource is monitored over time. The errors plotted on the graph may be the total number of CRC and Alignment errors.

Host Table View

Host Table View is available as a chart showing the ten MAC stations with the most traffic or as a table showing all MAC stations.

Network Layer Host Table View

Network Layer Host Table View is available as a chart showing the ten network stations with the most traffic or as a table showing all network stations.

Application Layer Host Table View

Application Layer Host Table View is available as a chart showing the ten network stations with the most traffic or as a table showing all network stations.

Host Matrix View

Host Matrix View is available as a chart showing the ten MAC conversations with the most traffic or as a table showing all MAC conversations.

Network Layer Matrix View

Network Layer Matrix View is available as a chart showing the ten network conversations with the most traffic or as a table showing all network conversations. The station addresses and names in the conversation are provided in the table or chart.

VLAN View

VLAN View is available as a table showing statistics or as a chart showing the ten virtual LANs with the most traffic.

Capture View

Capture View is the tool for detailed analysis and editing of packets. You can view the data in the capture buffer or view previously captured information that has been saved to a file. You can filter the data before viewing by using a display filter. Sometimes, the Capture View contains a packet editor for editing packets.

The initial **Capture View** window is normally divided into three parts or "panes." Capture View shows a synopsis of all captured packets, provides a breakdown of the elements of the packet by protocol and shows the hex and ASCII values for all characters in the packet.

Summary Pane

The Summary Pane shows a summary of all packets. Each line in the summary pane is a summary of one packet. Clicking on a packet selects it and displays its detailed protocol breakdown (decode) and its hex values in the remaining two panes of the window.

Detail Pane

The Detail Pane shows the values of the protocol elements associated with each protocol. For example, for the Data Link Control the values for the source address, destination address and packet length are shown. Single clicking on a value highlights the value in both the Detail Pane and the Hex Pane.

Hex Pane

The Hex Pane shows the hex and ASCII values for all the bytes in the packet. Single clicking on a value highlights the value in both the Detail Pane and the Hex Pane.

FILTERS AND ALARMS

Capture and Display Filters

For most data analysis operations, you will want to look at only a subset of all data. There are primarily two types of filters: capture and display.

- Capture filters direct analyzer devices to capture only the information you want to view and analyze. This would be helpful if what you need to capture occurs randomly. You would not have to capture and analyze thousand or millions of packets, just the ones you need for the purpose at hand.

- Display filters allow you to view only a subset of the data you have already captured. For example, you might choose to capture all packets sent/received by a specific IP network station, later, you might decide to look at only the data for specific types of packets that are flowing to/from the station, such as Dynamic Host Configuration Protocol (DHCP) negotiation.

Filter Actions

Very complex filters can be created to recognize almost any specific occurrence of data traversing the network, even custom data patterns. Depending on the specific protocol analyzer being used, filters can be used to trigger actions, such as:

- Capture only each frame or packet that meets the filter condition.

- Monitor the network until a specific condition exists, then capture data from that point until the capture buffer is full and send an email to the administrator.

Hints and Tips for Using Filters

Using filters efficiently takes time and practice. Here are some things to keep in mind:

- Remember to load the Capture filter on the module before you start capture.
- If you want to look at captured data in many different ways, use display filters rather than capture filters. Capture large blocks of unfiltered data and look at different subsets of the data by using a variety of display filters.
- Use conversations for capturing or displaying station-to-station or router-to-router activity.
- Always attach a description to a filter you are saving.
- Be sure to check the **Enable** box to include a conversation as part of your filter.
- AND operations narrow the search results and are typically used between elements that define masks.
- OR operations expand the search results and are useful between filter elements that define masks.

Alarms

Many protocol analyzers have built-in functions that allow the technician to create alarms to automatically monitor network resources. Alarm parameters often include a value that may be the minimum or maximum allowed, a time interval of the condition and actions to be taken when the alarm has been triggered. Examples of such alarms may include.

- Network utilization exceeding 40 percent for one minute
- ICMP Echo (PING) traffic that exceeds 50 packets per second
- Unused protocols (IPX or NetBEUI) traffic of any amount

Alarms can be configured to generate events such as e-mail messages, pages or logging messages to a log file. E-mail recipients, pager recipients and log file names are global parameters that you set. Some examples of these actions are listed below.

- An audible beep
- Generate an administrative alert or e-mail message
- Page a technician

Actions resulting from alarms are varied and flexible because they are assigned to each individual alarm. It is important to note that the protocol analyzer must be actively monitoring or capturing data from the network for the alarm function to work.

It is often possible to pre-configure alarms and save them for use later. They merely need to be loaded and enabled. It may also be possible to combine several individual alarms into an alarm group. When creating alarms, it is important to give them a name that makes sense to others who may need to use them later.

ANALYZER PERFORMANCE

Software protocol analyzers greatly affect a computer's performance. If the computer is being adversely affected by the analyzer software, the protocol analyzer program may need to be optimized to increase system performance. It may also be desirable or necessary to reduce the amount of each packet that is being captured or monitored.

Buffer Size

Protocol analyzer software often requires that a capture buffer size be set. The buffer size is the amount of system memory that will be used to save captured data. Buffer sizes can be set between 64K and 16M in multiples of two. Care needs to be taken when allocating the buffer size as a large buffer will increase the performance of the protocol analyzer application and decrease the performance of the computer system itself, by reducing the amount of system memory available to the operating system and other applications.

Packet Slice

Packet slicing means that a subset of the entire packet is saved in the capture buffer. You can save the first 32 bytes (Mac layer), the first 64 bytes (Network layer), the first 128 bytes (Application layer) or the full length of the packet.

Packet slicing can be set separately for monitor and capture modes. For monitor mode, packet slicing can improve performance when monitoring the entire packet contents is not required. In capture mode, packet slicing can save space in the capture buffer for more packets when analysis of the entire contents of each packet is not required.

SUMMARY

Performing protocol analysis requires in-depth knowledge of networking equipment, protocols and systems. By learning how to utilize alarms and filters correctly, an advanced network technician can optimize network performance, troubleshoot problems and increase security.

CONFIGURATION REPORTS

Objective 4d: Using network monitoring software, generate configuration reports IAW Performance Specification II-4d.

INFORMATION

NETWORK CONFIGURATION REPORTS

One of the main problems plaguing Network Control Centers (NCCs) today is the lack of configuration reports. It is crucial to maintain accurate configuration reports of networks and network equipment. These reports are necessary when considering upgrades or changes to the network. They also help technicians troubleshoot various types of problems and in identifying bottlenecks in network performance. Like any other forms of databases, they are only as good as the information put into them. Likewise, a two-year old configuration report usually causes more trouble than it solves.

NETWORK CONFIGURATION

Network configuration reports provide an overall "picture" of the network. They usually include items such as: quantity of networks, segments, routers, switches and PCs. Just knowing that a segment exists is not enough. You must also know how many users exist in that segment and how much traffic they generate. Knowing the total number of PCs connected to a network is important to maintain compliance with commercial software licensing practices. Simply knowing the quantity of a particular router or switch and the operating system version would greatly speed network upgrades and implementing advanced features, such as VLANs.

NETWORK EQUIPMENT CONFIGURATION

Network equipment configuration reports are specific to one piece of equipment. They usually include items such as: IP routing tables, interface configurations, VLAN membership and switch port configurations, just to name a few. These reports can also be used in a collaborative effort between military and commercial network design technicians to pre-build configuration files for new equipment.

Table 4-1 is an example of an IP address report from a router generated by HP OpenView®.

Title: Addresses : Set.7lvl
Name or IP Address: Set.7lvl

Index	Interface	IP Address	Network Mask	Network Address	Link Address
1	Et0	172.16.2.2	255.255.255.0	172.16.2.0	0x00500F05FF20
2	Et1	172.16.3.1	255.255.255.0	172.16.3.0	0x00500F05FF23
3	Et2	172.16.6.1	255.255.255.0	1	
72.16.6.0		0x00500F05FF26			
4	Et3	172.16.7.1	255.255.255.0	172.16.7.0	0x00500F05FF29
6	Et5	172.16.10.1	255.255.255.0	172.16.10.0	0x00500F05FF2F

Table 4-1. HP OpenView® IP Address report showing router interfaces.

It would be easy to review subsequent configuration reports to identify changes in subnet structure or unauthorized additions. You can also notice there is a skip in numbers from Et3 (Ethernet interface number 3) to Et5 (Ethernet interface number 5). This means there is one available Ethernet interface on this particular router for expansion.

Configuration reports can come from different sources. Most network management systems are capable of generating them, while most pieces of network equipment allow the entire configuration to be downloaded in text form. One of the most helpful reports shows physical connectivity between network equipment. Table 4-2 shows a CDP neighbor list for a Cisco Catalyst® 4006 switch. From this information, it would be easy to draw and document the physical connectivity of the LAN as seen by this switch. This procedure could be repeated for each of the switches in the LAN, which would result in an accurate network configuration report. If this switch had to be replaced, this report would help insure all other switches are connected back into the correct ports.

```
Bldg4227DSW1> show cdp ne
* - indicates vlan mismatch.
# - indicates duplex mismatch.
Port     Device-ID                          Port-ID                 Platform
-------- ---------------------------------- ----------------------- - - - - - - - - - - -          1 / 1
JAB050500W4(Bldg4227DSW2)          1/1                     WS-C4006

 1/2     JAB050500W4(Bldg4227DSW2)          1/2                     WS-C4006
 2/4     069043349(CAT4227.keesler.af.mi    3/1                     WS-C5500
 3/32    Bldg4227ASW_1-100101407A340        B                       cisco 1900
 4/38    Switch                             FastEthernet0/14        cisco WS-C2924-XL
 4/44    Bldg4227ASW_1-6                    FastEthernet0/24        cisco WS-C2924M-XL
 4/45    b4227ASW_2-4                       FastEthernet0/1         cisco WS-C2924-XL
 4/46    Bldg4227ASW_1-7                    FastEthernet0/24        cisco WS-C2924M-XL
 5/2     Bldg4227ASW_1-8                    FastEthernet0/24        cisco WS-C2924-XL
 5/8     Bldg4227ASW_1-2                    FastEthernet0/24        cisco WS-C2924-XL  5/12
Switch                              FastEthernet0/1         cisco WS-C2924M-XL

 5/14    Switch                             FastEthernet0/8         cisco WS-C2924M-XL
 5/32    Bldg4227ASW_1-5                    FastEthernet0/24        cisco WS-C2924M-XL  5/34
Switch                              FastEthernet0/1         cisco WS-C2924M-XL
 5/35    Bldg4227ASW_1-4                    FastEthernet0/24        cisco WS-C2924M-XL
```

Table 4-2. CDP neighbor table.

Of course, the exact information contained in a report will depend on the manufacturer and operating system of the equipment.

During this portion of the lab, you will be shown various types of reports and sources for information. Maintaining current configurations of your equipment is crucial when an unexpected malfunction happens on a core network router or switch. If you have been maintaining current configuration reports, it would simple be a matter of reconfiguring the replacement equipment. Even this can be simplified by using a trivial file transfer protocol (TFTP) server or the standard Microsoft Windows® copy and paste features.

As these configuration reports contain detailed information about our networks and equipment that could be exploited, it is important to keep them safeguarded. Knowing equipment make, model and configuration reduces a hacker's workload by an enormous amount. It just might be enough to let them get their foot in the door.

SUMMARY

Although obtaining and maintaining configuration reports are simple tasks to perform, they are often overlooked. These reports allow for easy identification of network configuration errors, help with optimizing the network's performance and are invaluable in network restoration.