MP 00B0000003

MITRE Product

Collaborative Operations in Joint Expeditionary Force Experiment (JEFX) 99

February 2000 **Version 1.1.1**

Michael S. Cokus
Thomas J. Howley
Michael C. Krutsch
Andrew R. MacBrien
George P. Parton, III
Esther Rhode
Robert L. Shaffer, Jr.

and

The Integrated Collaborative Operations Team

Command and Control Product Lines (CCPL) Contractors
Communication Technology Exchange (CTX)
Paragon Dynamics, Incorporated (PDI)
The MITRE Corporation

Sponsor:	ESC/CXE	Contract No.:	F199628-99-C-0001
Dept. No.:	G061	Project No.:	03006111 BB

Approved for public release; distribution unlimited.

MITRE
Center for Integrated Intelligence Systems
Bedford, Massachusetts

MITRE Department Approval:

Esther Rhode

MITRE Project Approval:

Ronald Doescher

Abstract

This document describes collaborative operations in Joint Expeditionary Force Experiment (JEFX 99). It addresses both the collaborative aerospace environment and the technical aspects of collaboration including the unique CVW system architecture, the supporting networking and security infrastructure, analysis of the loading data collected, and a guide for successful system deployment. It also offers observations on the general impact of virtual environments on distributed operations and recommendations for future experimentation.

Executive Summary

The Expeditionary Force Experiment (EFX) 98 demonstrated that a collaborative tool that provides persistent virtual workspaces is essential to the successful operation of a distributed Aerospace Operations Center (AOC). For the Joint Expeditionary Force Experiment (JEFX) 99, such a tool was included in the planning from the beginning, more as infrastructure than as an experimental initiative. Part way through the ramp-up to JEFX 99 execution the Air Force (AF) decided that several tools should be used in order to reduce risks and achieve the level of stability expected from this infrastructure.

The Collaborative Virtual Workspace (CVW) research tool was added to the JEFX 99 suite of collaboration capabilities to support the single largest community, the operators; those participants involved in the primary mission of the AOC. The scope of this paper is restricted to CVW usage but most of the technical and operational observations are relevant to any collaborative tool. To support this effort the Integrated Collaborative Operations Team was formed of personnel from Paragon Dynamics, Incorporated (PDI), Communication Technology Exchange (CTX), Command and Control Product Lines (CCPL) contractors, US Air Force military and civilian, and The MITRE Corporation. The Team's goal was to capitalize in every way possible, in the limited time available, on what had been achieved in EFX 98. Factors contributing to that success included the following:

- A stable software base, deployed in an integrated system of systems configuration to assure maximum availability to all potential users and minimum vulnerability to external system failures and information warfare attacks, all with efficient systems administration support.

- A robust, stable, secure networking infrastructure that included support for multicasting.

- Concept of Operations (CONOPS) collaborative techniques based on processes and procedures successfully used in previous exercises/experiments.

- Intensive training on a mixture of tool skills and process recommendations taught in the virtual environment. These processes were derived from the CONOPS component discussed above.

- Ubiquitous availability of the collaborative tool, meaning client software on every user workstations, to ensure all that participants have the ability to carry on effective collaboration no matter where they are located at the moment.

- User support throughout the execution phase delivered on-line, and by telephone for all users plus on-the-spot support for users at the primary locations.

- Assessment to capture, record and promulgate valuable lessons learned out of the experiment as a basis for better understanding of collaboration and process improvement in future experiments, exercises and eventually in a real world crisis.

Based on status logs and operators' input, some key functional observations associated with use of this collaborative tool included:

- Over 140 dispersed personnel virtually attended daily CFACC briefings.

- Attack Operations Cell reported a 50% process improvement.

- Target team personnel reported a time saving of 30%.

- Air Defense (AD) and Information Operations (IO) teams reported respectively a 50% and 80% increase in situation awareness.

In summary, the collaborative tool supported over 1650 user accounts. The system was engineered with the expectation of having 500 simultaneous users in a single virtual AOC environment. In actuality, the daily average was over 300 simultaneous users with peak usage at 372. This environment encompassed three primary sites (Langley, Hurtlburt, and Nellis) and 21 remote sites, including an airborne En-route Expedition Operations Center (EEOC) and afloat (USS Coronado) platforms. Over 700 users were trained the week prior to execution and on-site support was provided at all the primary locations during execution.

The concept of a virtual environment was introduced in EFX 98 to experiment with the conduct of distributed AOC operations. Users at JEFX 99 confirmed that a collaborative environment was indispensable for distributed operations and wanted it fielded right away. We recommend the Air Force ensure that collaborative capabilities are institutionalized, that is, incorporated into the Integrated Command and Control (IC2) Concept of Operations (CONOPS) and into systems, plans and procedures. Lessons learned from JEFX 99 need to be applied in training exercises such as Blue Flag and should be the basis for planning JEFX 00.

Collaboration enables virtual teaming and process change. To fully understand how a virtual environment impacts timeliness and effectiveness in the execution of a mission, the Air Force should make detailed analysis of the process by instrumenting the environment in which the process is carried out. Instrumentation is a method of recording and time stamping communications and actions conducted in the environment for later replayed and analysis.

For JEFX 00, candidate processes, such as time-critical targeting, can be singled out for such scrutiny that in turn can lead to further process and tool improvement.

No one of today's collaboration tools fits all needs nor delivers a full spectrum of collaborative capabilities. Besides virtual collocation, a robust collaborative AOC environment needs to be expanded to include the full spectrum of collaborative technologies, such as email for asynchronous collaboration, Web-based JEFX intranet for information sharing and joint publishing, VTC for meetings requiring higher quality video and audio, telephony including FAX when appropriate and application sharing to enable simultaneous control of an application. The Air Force must begin thinking ahead to the eventual use of these tools as an integrated system of systems solution that would greatly enhance and enrich the distributed working experience.

The one aspect of collaboration in JEFX 99 that was not exercised was interaction between US-Only and Coalition Forces. Apart from understanding the collaboration requirements, the biggest challenge lies in the technical and policy issues associated with security. Missions that the US engages in are often coalition based. One of the collaboration goals for JEFX 00 may be to take the first steps toward enabling controlled inter-US/coalition interaction.

Acknowledgments

The authors would like to acknowledge the efforts and contributions of the Integrated Collaborative Operations Team members who engineered, installed, trained, and provided on-site user support for the successful deployment of CVW for the JEFX 99 operational users. We would also like to thank the team for exceptional dedication and cooperation in providing valuable contributions to this document. The full list of team members is as follows:

- Command and Control Product Lines (CCPL)

  -- Richard Cashell and Randall Licota
- Communicatoin Technology Exchange (CTX)

  -- Gary Daigle, Richard Gil, Lucinda McKnight, Sean Lancaster and Eric Sorter
- Paragon Dynamics, Incorporated (PDI)

  -- Sara Hadley, Douglas Hartmann, Pamela Kimminau, Hansel Lee and Roger Stapleton
- The MITRE Corporation

  -- Michael Cokus, Sharon Colangelo, John C. Dominick, Devon Goepel, Clayton Hanright, Thomas Howley, Larry Hughes, Michael Krutsch, Betty Maddox, George Parton, and Esther Rhode
- US Air Force, ESC/CXE

  -- Major Richard Coveno, Lt. Nicholas Harris and Denise Spencer

In addition, we would like to thank Benjamin Hu, MITRE, for the last-minute DII COE segmentation of the CVW client as well as members of the MITRE CVW development team for responding quickly to questions whenever we asked them. We also thank members of the JEFX 99 networking and security teams for ensuring smooth integration of the collaborative capabilities into the JEFX 99 infrastructure as well as monitoring the behavior and capturing loading data related to the use of this tool.

Table of Contents

Table of Contents, continued

Table of Contents, concluded

List of Figures

Figure Page

List of Figures, continued

List of Figures, continued

List of Figures, continued

List of Figures, concluded

List of Tables

Section 1

Introduction

The United States (US) Air Force's Joint Expeditionary Force Experiment (JEFX) 99 consisted of three preliminary spirals and the actual Experiment "execution" that took place in the second half of August. For the execution phase, the Collaborative Virtual Workspace (CVW) was used to support the Command and Control (C2) warfighters, hereafter referred to as operators. In JEFX 99, the Aerospace Operations Center (AOC) was divided into several geographically separated elements that were to function as a single body with real-time support from over 20 distributed organizations spread across the US. (See Figure 1.1.)

Expeditionary Force Experiment (EFX) 98 demonstrated how a collaborative tool that provides persistent virtual workspaces is essential to the successful operation of a distributed AOC. For JEFX 99 such a tool was included in the planning from the beginning, more as infrastructure than as an experimental initiative. Part way through the ramp-up to JEFX 99 execution, the Air Force (AF) decided that several tools should be used in order to reduce risks and achieve the level of stability expected from infrastructure for experimentation.

The AF added CVW to the JEFX 99 suite of collaboration capabilities to support the single largest community, the operators; those participants involved in the primary mission of the AOC. JEFX 99 expanded experimentation with the virtual distributive AOC. This presented increased challenges to the collaboration environment. The group assembled to meet this challenge, hereafter referred to as the Integrated Collaborative Operations Team, was drawn from various commercial sources including MITRE; Paragon Dynamics, Incorporated (PDI); Communication Technology Exchange (CTX); and Command and Control Product Lines (CCPL), a service contract supported by several contractors, in this case Raytheon, as well as Air Force and government civilian personnel.

1.1 Background

JEFX 99 is a Chief of Staff of the Air Force (CSAF)-sponsored, experiment that combines LiveFly forces, live-play ground forces, simulation, and technology insertion into a seamless warfighting environment. JEFX 99 provides the AF a vehicle for experimentation with operational concepts and attendant technologies in support of the Joint Force Air Component Commander (JFACC) and its mission. JEFX 99 expanded on EFX 98 by emphasizing a more complete integration of space-based forces and space-derived information into aerospace operations as well as joint/combined participation, where appropriate.

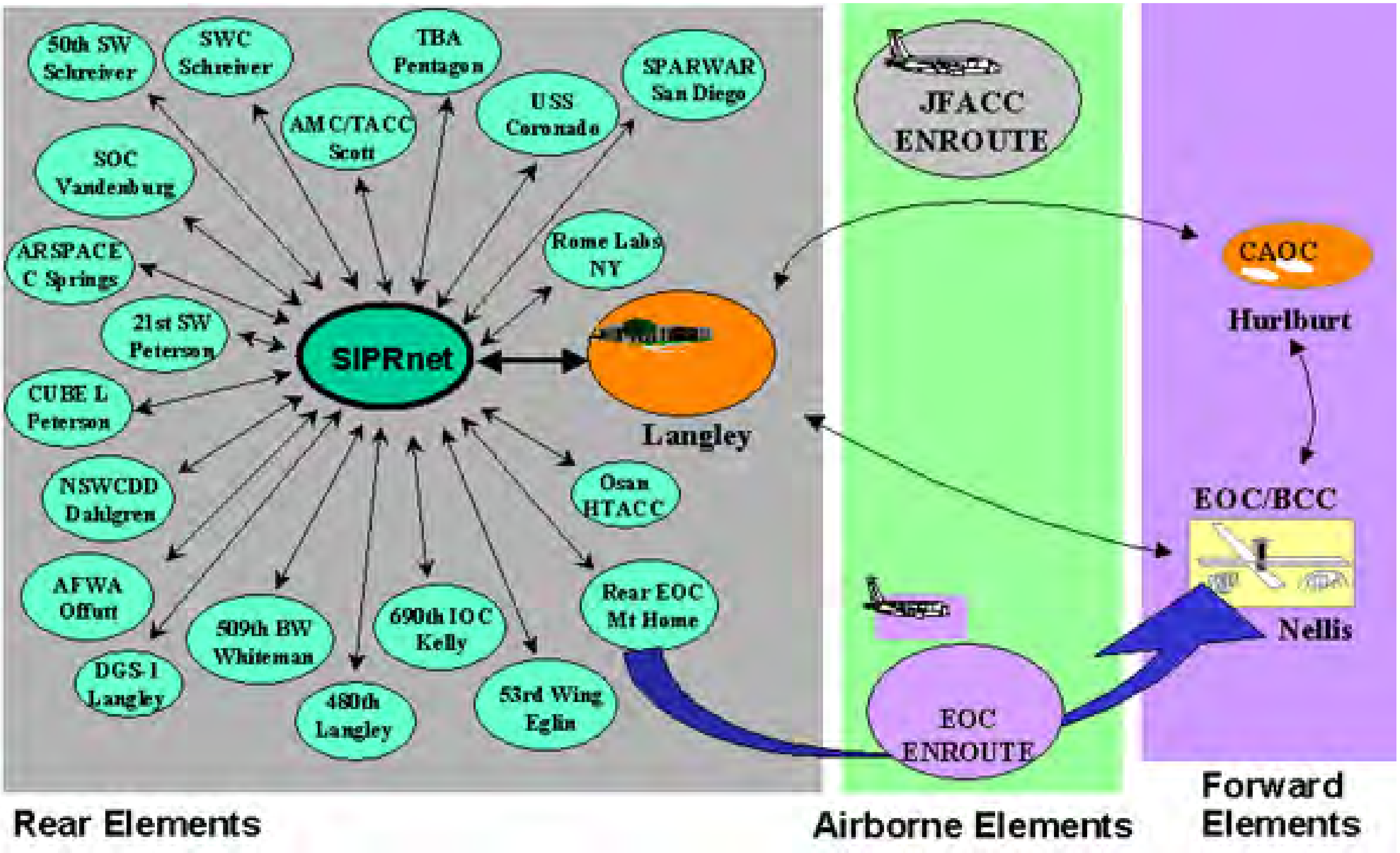


Figure 1.1 – Elements of the Virtual AOC Environment

Both EFX 98 and JEFX 99 involved experimentation with distributed AOC operations. In order to quickly deploy the minimum force necessary, the AOC was divided into forward and rear components. The AOC components and other organizations supporting the AOC were geographically dispersed. This separation presented challenges to conducting AOC operations. In EFX 98 collaborative technology was shown to be an essential enabler for distributed AOC operations, and was therefore employed in JEFX 99 more as infrastructure to further enable innovation in distributed AOC processes.

1.2 Purpose and Scope

The purpose and scope of this document is to describe the deployment and employment of a collaborative environment used to support distributed operations within the scope of JEFX 99. While the discussions in the following sections refer to the actual experience with CVW by the operators and the engineers, many of the issues, lessons learned, and recommendations are applicable to deployment and use of other collaborative tools. In this document, CVW can be viewed as a means to express the way a virtual environment was being used and as an example to illustrate the nature of technical problems encountered and resolved.

This document addresses both the usage of the environment as well as the technical aspects of deploying and operating it, and ends with overall observations and recommendations. Many of the lengthier details are included as appendices. Section 2 is key to understanding the operational use of CVW. While it was not possible to capture the actual interactions of the operators who occupied the virtual rooms, much information and insights of how the space was used could be gleaned from the numerous documents left in the rooms. Since training is an essential element for successful use, Section 3 discusses the training course material, how training was conducted, and offers insights into effective ways to conduct future user training for this type of environment. Section 4 consists of a collection of user feedback on what enhancements they would like to see.

Section 5 captures three critical elements for deploying a collaborative environment: (1) the architecture of the collaborative system for this specific AOC context, (2) the underlying network architecture and analytical data pertaining to CVW traffic, and (3) the application of a security framework that allowed effective collaboration to take place protected from compromise or external attack. Section 6 discusses technical system support necessary to the maintenance of the tool for the conduct of JEFX 99.

Section 7 takes a view one level up from the implementation of CVW for JEFX 99 and offers observations and comments on the general impact of virtual environments on distributed AOC operations. Many of these insights are gained through the culmination of several years of experience in deploying such tools in the context of supporting air operation command and control, ranging from Ft. Franklin V in 96, JWID 97 (JW-068), EFX 98, and continued to JEFX 99. Section 8 offers recommendations for future experimentation and for adoption of this technology for everyday and deployment use.

Appendix A provides definitions for CVW terminology used in this document. Appendix B consists of the day-by-day collection of observations/data logged by the team between 28 August and 2 September. Appendix C contains examples of the procedures followed by the team in maintaining CVW for use during JEFX 99. Appendix D is a collection of network data pertaining to the CVW network traffic profiles gathered for between 30 August and 2 September. Appendix E contains a detailed description of the numerous tasks that need to be performed in preparation for successful roll out of the collaborative environment. Appendix F backs up Section 2 with examples of data produced by the operators and left in the collaborative environment. Lastly, a Glossary is provided.

1.3 Overview of JEFX 99 Collaborative Environment

Collaborative Virtual Workspace (CVW) is a MITRE-developed research prototype for experimenting with collaborative technology and processes. It is a client-server application designed to support temporally and geographically dispersed work teams. From a user's point of view, CVW provides a persistent virtual space within which people, documents and application are directly accessible. The virtual rooms are organized into floors that make up a building. This type of collaborative environment enables "virtual collocation" and is referred to as a "place-based" collaborative tool.

Place-based collaborative tools allow people to gather in the virtual rooms and communicate using text chat and audio/video conferencing. Defining rooms as the basis for communication means that users are not required to set up sessions or know each other's locations; they need only congregate in a virtual room. Whether users choose to communicate through audio, video or text, the communication sessions are established automatically for them.

Virtual rooms are also the basis for file sharing. Users can place any digital file in a room thus allowing anyone else in that room to open the file, make a copy of it or view information about it. Persistence is supported because the rooms exist even when no one is in them. Consequently, a file remains in a room available to all who have room access until some authorized user moves or deletes it.

The use of collaborative technology during JEFX 99 was intended to address two specific Mission Threads identified in the Experiment Project Order.

1. "Develop/distribute/execute aerospace tasking in a geographically-separated, collaborative, distributive joint environment to include accomplishing effects based operations."

2. "Using collaborative tools, provide position specific training to operational level personnel in geographically separated Joint Air Operations Center (JAOC) components."

CVW was the key enabler for the first thread. There was, however, no formal attempt to use the collaborative tool to provide position specific training among distributed components. Formal CVW training was conducted at Langley AFB, VA; Hurlburt AFB, FL; Nellis AFB, NV; and Mountain Home AFB, ID; Scott AFB, IL; Naval Surface Weapons Dahlgren Lab, VA; the Pentagon; Peterson AFB, CO; Vandenberg AFB, CA, USS Coronado, CA; and Naval Station San Diego, CA. Training over the collaborative tool only occurred on an ad-hoc basis.

Section 2

Collaborative Operations

The CVW, MITRE's research prototype collaborative environment was chosen by the Air Force (AF) as the primary collaboration tool for operational activity taking place at the SECRET level throughout the distributed JAOC, Expeditionary Operations Center (EOC), and Battlespace Control Cell (BCC). The place-based, virtual environment provided the basis for collaborative activities among the geographically dispersed staff and command elements. An overview of these activities is presented in Section 2.1. Secret Internet Protocol Routing NETwork (SIPRNET) was the classified network over which the overwhelming majority of activities occurred.

The JAOC virtual building initially consisted of 12 floors and expanded to 16 floors by End of Exercise (ENDEX). Each floor had eight rooms not counting the different sections of the hallway on each floor. Each room was a virtual place where users could congregate to exchange files, and communicate via text chat, audio, and video. The particular floors and rooms for the experiment were configured based on user feedback. Details of the room layouts and contents can be found in Section 2.2. The reader will see the terms, "page," "pop-up," "group object," "folder," and "note" throughout this section. These terms refer to CVW features, explained in Appendix A. Figure 2.1 illustrates the mapping of operators at physically distributed sites into functional virtual teams and placing these teams into rooms that mirror an AOC.

2.1 Overview of Collaborative Activities

The collaborative environment was established to enable the JEFX 99 personnel to coordinate effectively, in spite of the geographical separation involved with distribute AOC operations. Operators ranging from Senior Airman to Lieutenant General were able to find key personnel, pull selected data to avoid information saturation, plan and coordinate actions, exchange and share information, attend and/or participate in major decision and informational briefings, and send out alert notices for immediate action. During JEFX 99, operators developed expanded ad hoc procedures building on collaborative processes developed in EFX 98. Based on actual documents used by the various teams and interviews and discussions with JEFX 99 operators, observations concerning these procedures are discussed in the following sections.

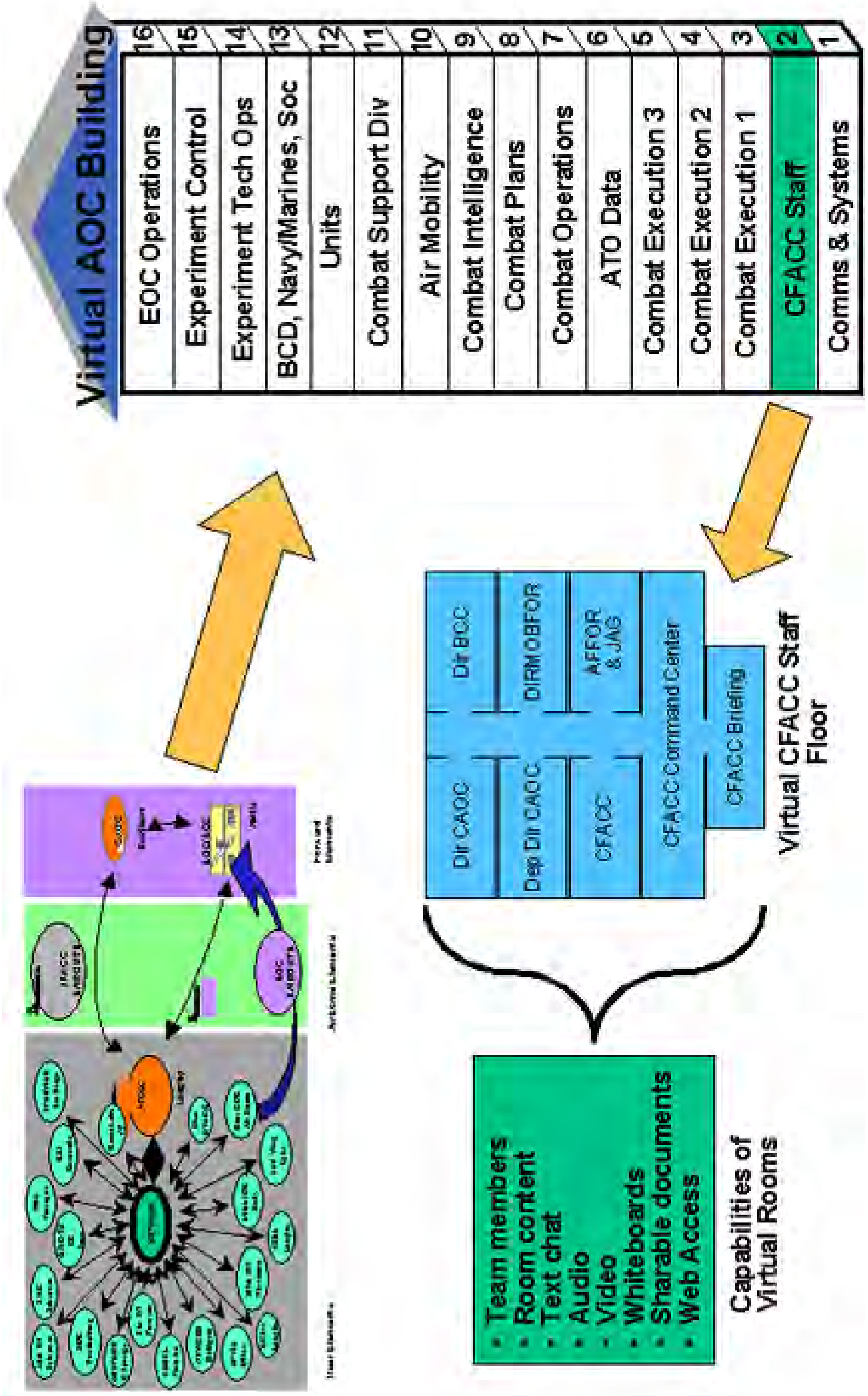


Figure 2.1 – The Virtual Aerospace Operations Center (AOC)

2.1.1 General Observations

- Copy and Paste
  Users made continuous use of the copy and paste functions inherent in the associated word processing functions while in CVW. They also used the text paste feature inherent on the CVW desktop. These features were used typically to copy recurring messages and reports received via external applications into CVW notes or simple notepads to be available as room objects throughout the collaborative environment.

- Screen Captures
  Operators frequently captured screen displays from Theater Battle Management Core System (TBMCS) and other applications and imported these displays as backdrops to whiteboards for collaboration purposes or as reference objects to be placed in various rooms.

  EXAMPLE: Figure 2.2, taken from the Master Air Attack Plan (MAAP) team room, illustrates how the distributed MAAP team members imported a screen capture from TBMCS as a backdrop to a CVW whiteboard. The object contains Air Order of Battle information from the scenario and could be used as reference material or as a graphic for collaboration and further annotation.

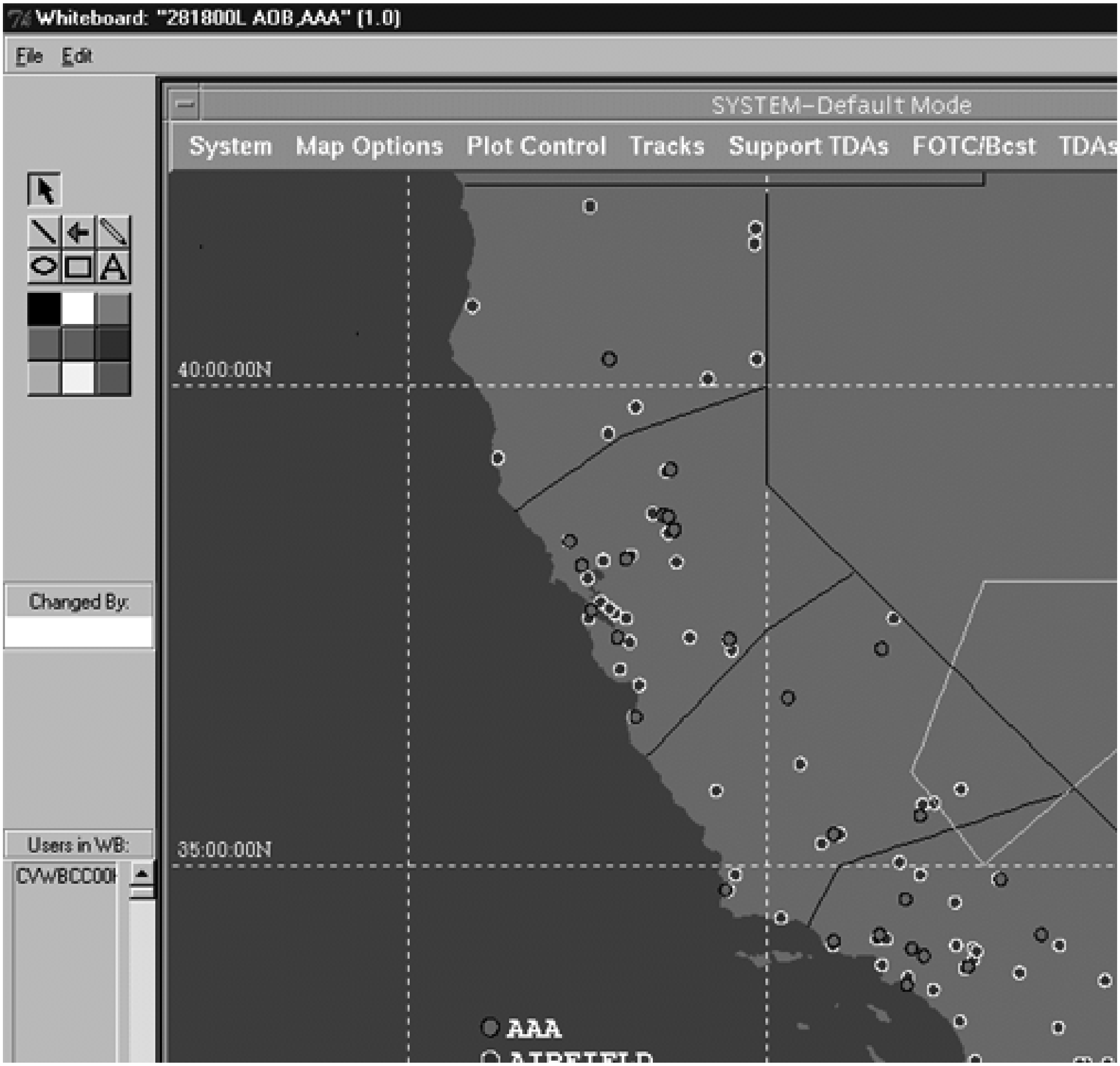
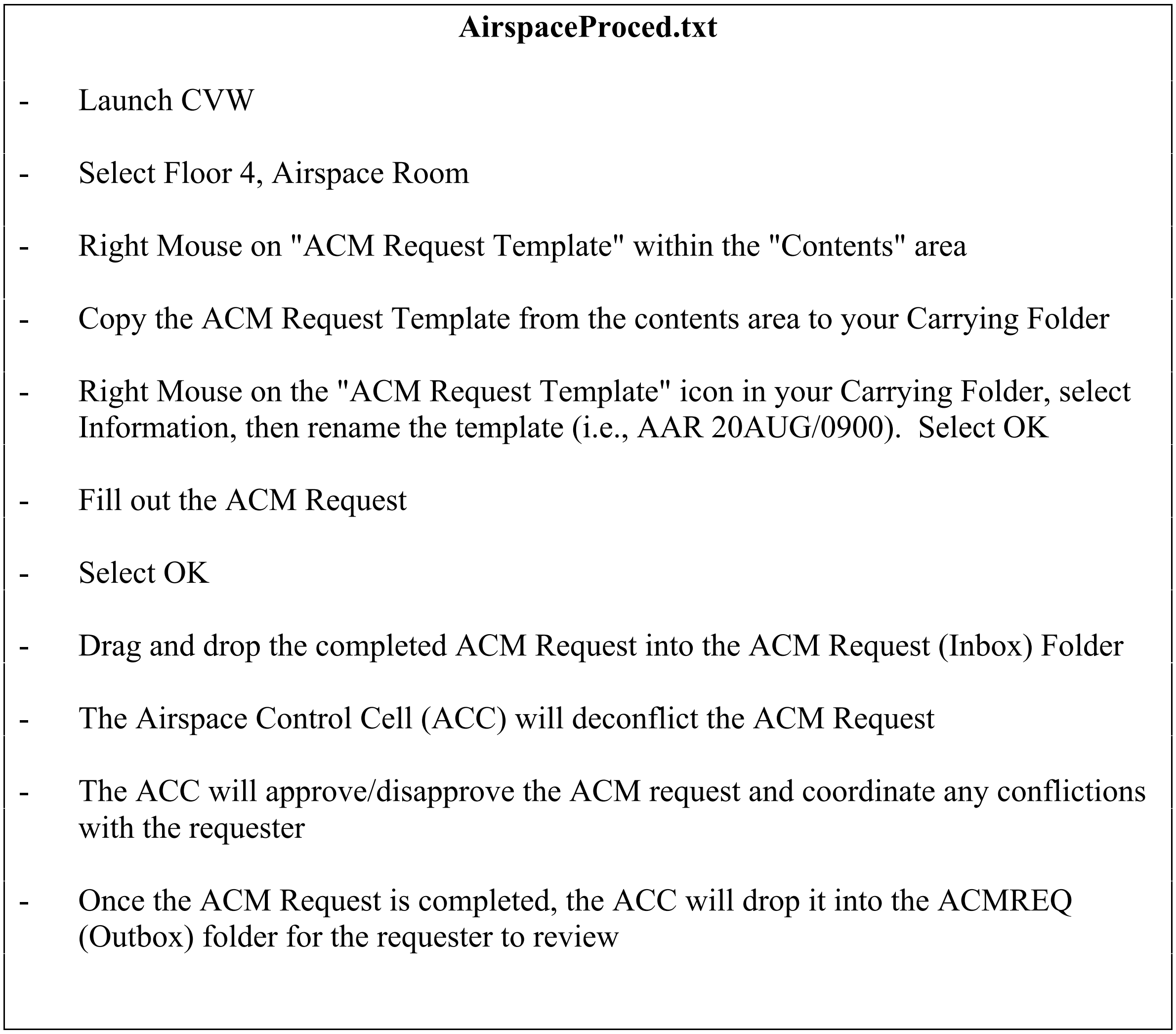


Figure 2.2 – MAAP Team Room

- Procedural Notes
  Since many operational procedures for the use of the collaborative tool were developed spontaneously by cell chiefs and other staff personnel during the experiment, operators found that explanatory CVW notes and simple text documents placed in rooms assured standardized adherence to these new processes.

  EXAMPLE: Figure 2.3, taken from the Airspace room, illustrates how the Airspace Control Cell used a CVW note to explain a simple, effective and expedient procedure for submitting and processing Airspace Control Means (ACM) requests using CVW.



AirspaceProced.txt

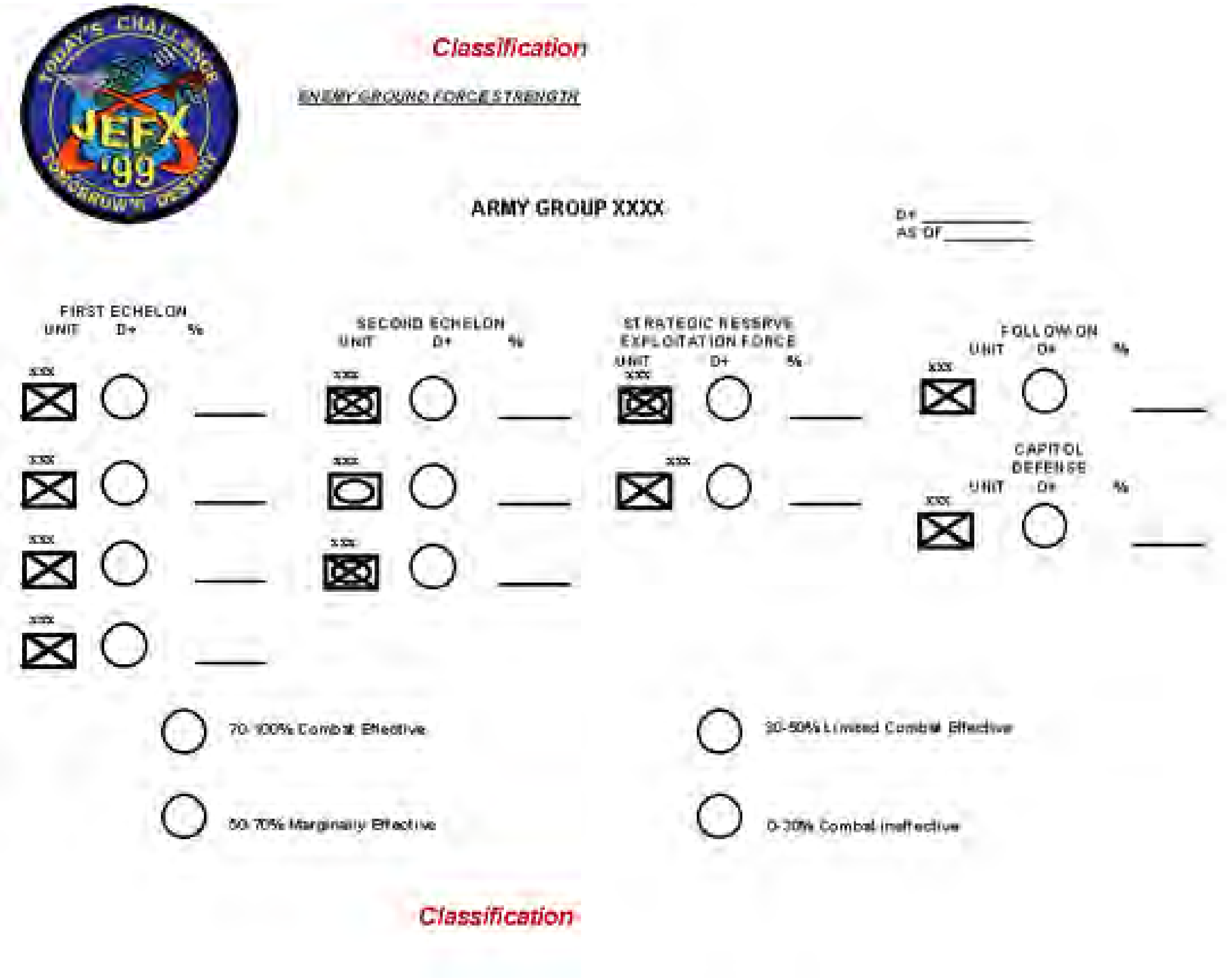
- Launch CVW
- Select Floor 4, Airspace Room
- Right Mouse on "ACM Request Template" within the "Contents" area
- Copy the ACM Request Template from the contents area to your Carrying Folder
- Right Mouse on the "ACM Request Template" icon in your Carrying Folder, select Information, then rename the template (i.e., AAR 20AUG/0900). Select OK
- Fill out the ACM Request
- Select OK
- Drag and drop the completed ACM Request into the ACM Request (Inbox) Folder
- The Airspace Control Cell (ACC) will deconflict the ACM Request
- The ACC will approve/disapprove the ACM request and coordinate any conflictions with the requester
- Once the ACM Request is completed, the ACC will drop it into the ACMREQ (Outbox) folder for the requester to review

Figure 2.3 – Airspace Control Cell (ACC)

- Templates

  Operators designed various functional templates in different formats to include CVW Note, PowerPoint, Whiteboard, and Text to be placed in various rooms for distributed users to accomplish different functional activities. These templates simplified processes and enhanced standardized understanding and presentation.

  EXAMPLE: Figure 2.4, taken from the US Army's Battlefield Coordination Detachment (BCD) operations room, was a templated format for Army intelligence team members to produce Ground Order of Battle information in support of the AOC.



Classification

ENEMY GROUND FORCE STRENGTH

ARMY GROUP XXXX

D+ ____________
AS OF__________

FIRST ECHELON
UNIT D+ %

SECOND ECHELON
UNIT D+ %

STRATEGIC RESERVE
EXPLOITATION FORCE
UNIT D+ %

FOLLOW ON
UNIT D+ %

CAPITOL
DEFENSE
UNIT D+ %

○ 70-100% Combat Effective

○ 30-50% Limited Combat Effective

○ 50-70% Marginally Effective

○ 0-30% Combat ineffective

Classification

Figure 2.4 – Battlefield Coordination Detachment (BCD)

- Mission Folders
  Some staff sections and elements used the Folder feature within CVW to create mission-oriented folders to assemble all of the components for various operational missions, (e.g., Combat Search and Rescue (CSAR) mission folders). These folders typically contained all the relevant associated objects or documents for particular missions to include threat assessments, imagery, unit status reports, checklists, weather, etc.

  EXAMPLE: Figures 2.5 and 2.6 are taken from the Joint Search and Rescue Cell (JSRC) room and are examples of some of the contents that were in the "Hammer 13" Combat Search and Rescue (CSAR) mission folder. This was one of several CSAR mission folders in the room.

Hammer 13 CSARTF assets.txt

CSARTF assets for Hammer 13

1	HH-60	C/S	Jolly 01	MSN	No. 3164
2	A-10	C/S	Puff 06	MSN	No. 7106

Hammer 13 Threat Assessment –1.txt

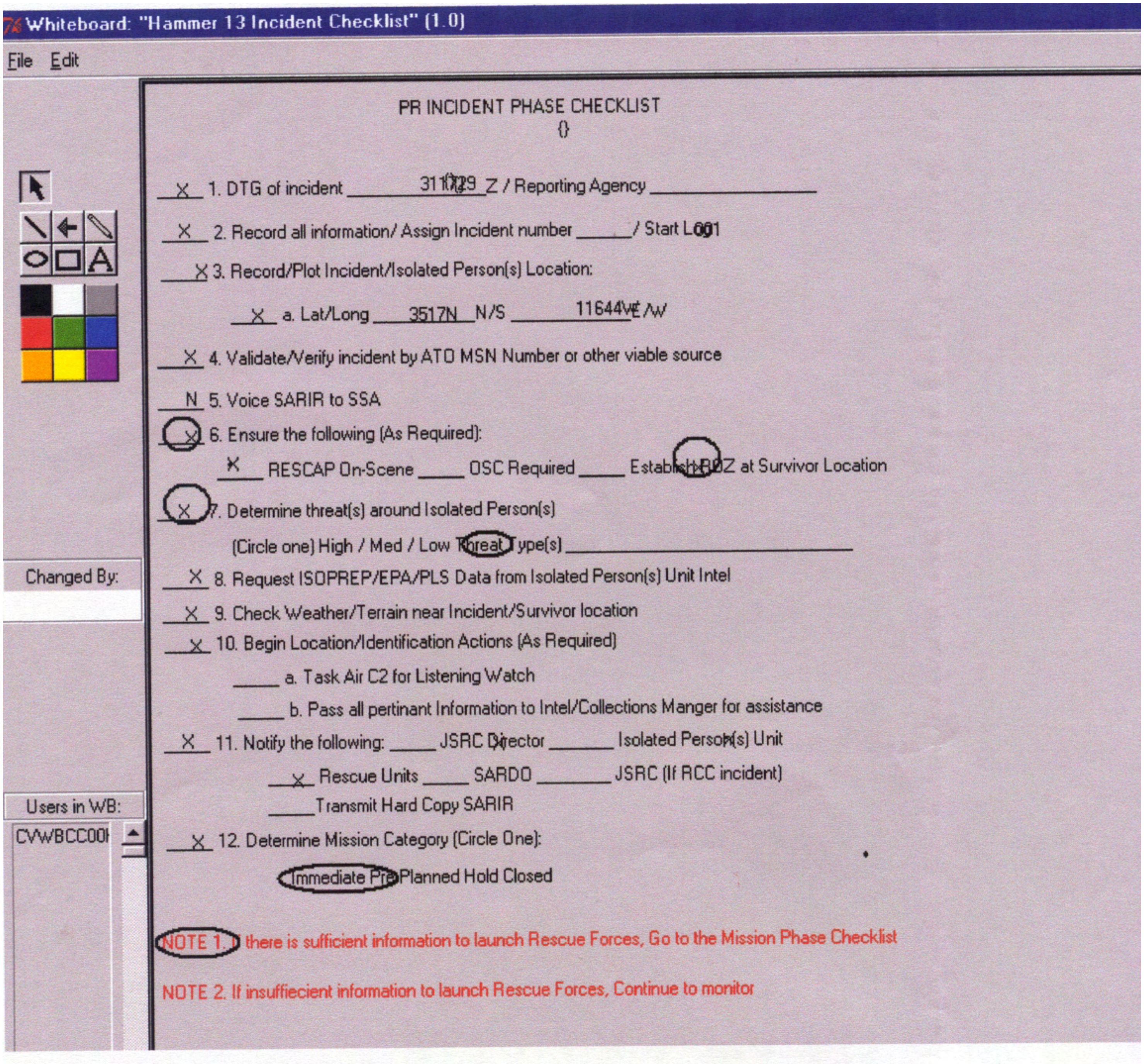
Northeast of last known pilot position: 924 Arty. Bn. at	3522N	11603W,
Also, southeast of pilot position: 31 Armor Bde at	3442N	11628W
According to latest intel the nearest threat is at the 3 3rd Armor Battalion	3453N	11700W

Hammer 13 WX Report.txt

Clear skies, NO clouds, High 82, Low 60 Light data for the mission. Sunset 19:01L, Moonrise 22:26Lll MoonSET 01/11:03L %illum 79% for aircraft 35.17N 116.4 4W. Current WX conditions for F5-A are, Vis – Unrestricted, Winds 330 @02 kts, Temp at 71, Clouds scattered at 8,900 ft and no significant weather. Forecasted winds to become 220 at 10 gusting to 25 after 22Z. MWA has the area in an Isolated thunderstorm area from 10 to 06Z but not forecasted.

Figure 2.5 – Joint Search and Rescue Cell (JSRC)

FROM JSRC ROOM



Whiteboard: "Hammer 13 Incident Checklist" (1.0)

PR INCIDENT PHASE CHECKLIST

{}

X 1. DTG of incident 311729 Z / Reporting Agency ________

X 2. Record all information/ Assign Incident number _____/ Start Log 001

X 3. Record/Plot Incident/Isolated Person(s) Location:

X a. Lat/Long 3517N N/S 11644W E/W

X 4. Validate/Verify incident by ATO MSN Number or other viable source

N 5. Voice SARIR to SSA

X 6. Ensure the following (As Required):

X RESCAP On-Scene _____ OSC Required _____ Establish X ROZ at Survivor Location

X 7. Determine threat(s) around Isolated Person(s)

(Circle one) High / Med / Low Threat Type(s) ________

X 8. Request ISOPREP/EPA/PLS Data from Isolated Person(s) Unit Intel

X 9. Check Weather/Terrain near Incident/Survivor location

X 10. Begin Location/Identification Actions (As Required)

_____ a. Task Air C2 for Listening Watch

_____ b. Pass all pertinant Information to Intel/Collections Manger for assistance

X 11. Notify the following: _____ JSRC Director _____ Isolated Person(s) Unit

X Rescue Units _____ SARDO _____ JSRC (If RCC incident)

_____ Transmit Hard Copy SARIR

X 12. Determine Mission Category (Circle One):

[✓ Immediate] PrePlanned Hold Closed

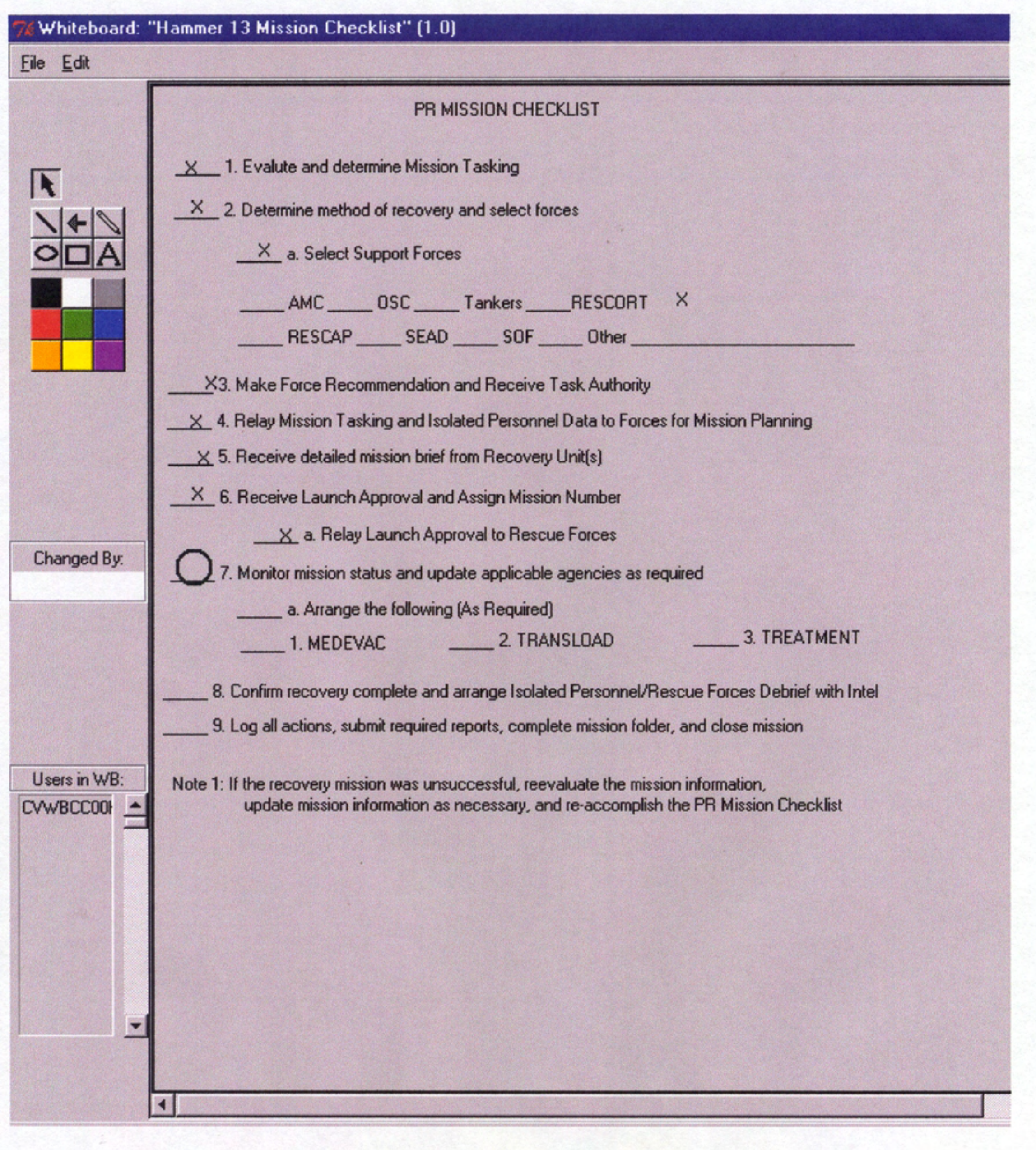
NOTE 1. If there is sufficient information to launch Rescue Forces, Go to the Mission Phase Checklist

NOTE 2. If insuffiecient information to launch Rescue Forces, Continue to monitor

Figure 2.6 – Joint Search and Rescue Cell (JSRC)

- Checklists
  Some sections established preformatted whiteboards to be used as collaborative action item mission checklists.

  EXAMPLE: Figure 2.7, also taken from the Joint Search and Rescue Cell *(JSRC) room, illustrates a separate Personnel Recovery (PR) checklist preformatted on a CVW whiteboard and also used for the "Hammer 13"* Combat Search and Rescue *(CSAR) mission.*



PR MISSION CHECKLIST

__X__ 1. Evalute and determine Mission Tasking

__X__ 2. Determine method of recovery and select forces

__X__ a. Select Support Forces

_____ AMC _____ OSC _____ Tankers _____RESCORT X

_____ RESCAP _____ SEAD _____ SOF _____ Other ________________________

____X3. Make Force Recommendation and Receive Task Authority

__X__ 4. Relay Mission Tasking and Isolated Personnel Data to Forces for Mission Planning

___X_ 5. Receive detailed mission brief from Recovery Unit(s)

__X__ 6. Receive Launch Approval and Assign Mission Number

__X__ a. Relay Launch Approval to Rescue Forces

○ 7. Monitor mission status and update applicable agencies as required

_____ a. Arrange the following (As Required)

_____ 1. MEDEVAC _____ 2. TRANSLOAD _____ 3. TREATMENT

_____ 8. Confirm recovery complete and arrange Isolated Personnel/Rescue Forces Debrief with Intel

_____ 9. Log all actions, submit required reports, complete mission folder, and close mission

Note 1: If the recovery mission was unsuccessful, reevaluate the mission information,
update mission information as necessary, and re-accomplish the PR Mission Checklist

Figure 2.7 – Personnel Recovery (PR)

- Logs
  Users in various cells used logs to capture events for maintaining continuity, and as standard duty logs. They found that having a single log accessible to all of the members at distributed locations was better than maintaining separate logs at each location.

- Duty Rosters
  In EFX 98, many users employed “hotlists” which were personal, sometimes informal groups of other users which the hotlist owner created and then put in his or her carrying folder for rapid access and to decrease the number of formal groups in the “Groups Manager.” In JEFX 99, users were specifically trained to build and use hotlists and adapted that concept into another innovation. They built functional groups to use as section or working cell duty rosters. They inserted these duty rosters as external group objects into functional rooms. This was a significant advantage since there were so many on-line users that finding and communicating with an individual that way could be time consuming. Having the correct list of organizational people congregated together as an object in the room saved much time and increased efficiency.

- In Boxes
  In some sections, senior personnel built an “In Box” folder and put it in the room so selected team members could review, coordinate, or annotate files in that folder, as appropriate.

2.1.2 Functional Observations

- The Combined Force Air Component Command (CFACC) Briefing
  The CFACC briefing was a regularly scheduled meeting in which each AOC division chief briefed the CFACC using CVW, with over 140 personnel in virtual attendance. The briefing charts, compiled by distributed sections and cells, were implemented as web pages for easy access through a web browser, with the Universal Research Locator (URL) for the briefing posted as an object in the CFACC Briefing room. All personnel in the room (as well as in a second room “wired” to the first room) used CVW conferencing audio to listen to the briefers in real time. At the same time, the text chat feature was used for private sidebar discussions.

- Attack Operations (AO) Cell
  Personnel in this distributed cell primarily used audio for coordinating actions along with the pop-up feature for instant notification. The AO cell also used CVW notes for Air Tasking Order (ATO) changes, activity and duty logs and updating cell guidance. They also had engagement log notes that enabled them to capture incident history. AO cell personnel reported CVW increased their situation awareness, reduced their huddle time by two thirds and felt they had a 50 percent improvement in accomplishing processes by using the collaborative tool.

- AOC Operations
  Process participants used audio, text and notes with text chat as back up when audio outages occurred. They shared Predator reports using CVW notes; group pages for rapid JSTARS information dissemination and whiteboards for airspace visualization. Users reported the Collaborative Tool (CT) enabled parallel processes because it provided common knowledge of ongoing events, ID required the group to think through the process increasing group situation awareness. They estimated that CVW improved process time by 40 percent (using the operations at the CAOC in Vicenza, Italy as a benchmark).

- Target Prioritization and Status Cell
  Personnel in this cell used CVW notes for duty logs. They reported an overall improvement in situation awareness and a process time savings of 30 percent. They also reported that the CT made calling meetings easier, and that meetings were held more frequently, which facilitated information dissemination better than in the past.

- Air Defense (AD) and Dynamic Battle Control (DBC) Execution
  This group used whiteboards for Theater Missile Defense Intelligence Preparation of the Battlefield events – indicating launch points on displayed maps. They used audio, text chat and CVW notes for duty log purposes. These personnel reported 35 percent improvement in timeliness of their processes based on the CT providing a ready path for coordination, individual access, and group access. They also felt CT saved 80 percent of energy expended in mission task, and provided a 50 percent increase in overall Situation Awareness. They also reported a decrease in the fatigue that is normally caused by the high noise levels present in the AOC without CVW.

- Information Operations (IO)/Special Technical Operations (STO)
  From the Sensitive Compartmented Information Facility (SCIF) personnel distributed sanitized collateral data to cell planners using the CVW page feature on a collateral workstation in the SCIF. They also passed target locations using group pages. Personnel used CVW notes for gathering and distributing data. They reported their situation awareness was enhanced by 80-90 percent, they were able to get information out of the SCIF faster and without using sneaker net, and that there was a 100 percent improvement in general information flow and the ability to virtually assemble together.

- Weather
  Weather personnel stated their function has always been a distributed operation and CVW brought the distributed team (located at the OSC, CAOC, and both EOCs) virtually together. They published periodic forecast updates to their weather server and then dropped those URL objects in the CVW rooms of associated customers. The collaborative tool enabled the weather section to be actively involved in the DARS (Collection Management) meetings since the ISR team was located in the SCIF, separate from the weather section.

- Special Operations Forces (SOFs)/Intelligence
  The operator in this section stated his information access was improved by the CT room paradigm. He found pushing information, as in the past, was less efficient and involved a time delay – a problem the pull capability inherent in CVW eliminated. He noted he may not have been on automatic distribution for material which was important. The capability to browse the active rooms and review their contents yielded potentially critical data for him. He also felt he could tell very quickly whether a room's contents were valuable for him.

- Air Mobility
  During the process of testing C2IPS, air mobility planners eliminated excessive paperwork when creating airlift missions by importing the airlift request form into CVW. Controllers stated they were easily able to transfer airlift request information from CVW to C2IPS. They reported if C2IPS were to go down, the forward CAOC could take the necessary information to complete the request via CVW and complete the mission themselves.

2.2 Collaborative Operations

Appendix F extracts actual operational data from the JEFX 99 CVW server used for distributed operations. A review of Appendix F will illustrate how the collaborative tool was pervasive and essential for aerospace operations management.

The material in Sections 2, 7, 8, and Appendix F of this document should serve well as a general model for designing procedures and CONOPS for the use of any collaborative tool in any operational environment. It spans various functional disciplines within the distributed Joint Air Operations Center (JAOC), the Expeditionary Operations Center (EOC) and Battle Control Center (BCC). It also illustrates joint service input in a collaborative environment. It should be emphasized that the environment, objects and procedures reviewed here reflect one approach, not the only approach. Also, the methods and techniques here were operator-conceived not prescribed to them. Operators used their own initiative and creativity in developing how they would use the collaborative tool to do their jobs. It can be expected, even with a well formulated collaborative CONOPS, operators will continue to adapt and innovate on the capabilities of the tool to uniquely suit their needs.

Section 3

Training

The Integrated Collaborative Operations Team conducted numerous 4-hour CVW training sessions at Langley Air Force Base (AFB), Virginia; Hurlburt AFB, Florida; Nellis AFB, Nevada and Mountain Home AFB, Idaho, Scott AFB, Illinois; Naval Surface Weapons Dahlgren Lab, Virginia; the Pentagon; Peterson AFB, Colorado; Vandenberg AFB, California, USS Coronado, California; and Naval Station San Diego, California, during the week prior to experiment execution. Though the standard class duration was four hours, scheduling constraints sometimes called for the block of instruction to be curtailed to three or fewer hours. Optimal class size was 10 students, though this number was exceeded on a regular basis with classes of 16 or more. One class at Langley consisted of approximately 150 students, which severely degraded the value of the training session. For each class the instructional staff included an instructor and one or two assistants to help individual students. Training was also provided for users at remote sites, albeit with a much smaller class size. Students were provided a spiral notebook titled, Quick Reference Guides for XV, HyperSnap and CVW as course materials.

The 4-hour academic training was designed to thoroughly educate users in CVW capabilities and was geared to operational use. It was based on a detailed course outline and covered the following skill topics:

- The CVW workplace
- Moving around the CVW (virtual) building
- Getting information about others
- Text Communication
- Scrollback, search, save, and paste functions
- Finding objects in CVW
- Indicating your idle status
- Creating and using groups
- Whiteboards
- Creating and using various objects
- Importing and sharing documents
- Setting preferences
- Changing your password
- Audio and Video Conferencing

Of the 1650 individuals who had user accounts, approximately 700 attended training at various locations as indicated below:

- 300 Hurlburt AFB
- 250 Langley AFB
- 150 Nellis AFB, Mountain Home AFB, and other remote sites

In the optimal 10 student training session, each student should have his or her own workstation, should be able to easily see the instructor s workstation screen via an overhead display, and should not be distracted by extraneous noise. Additionally, it would be preferable to train separately on the UNIX and PC clients since there are slight differences between the two tools. In actuality, the sessions were mixed with UNIX and PC users, there were constant distractions as other activities were ongoing, and class sizes sometimes vastly exceeded 10 students.

CVW training experienced several challenges:

- Training sessions were very fluid and frequently not able to be conducted as scheduled because of last minute organizational and personnel turbulence. The training teams and students adapted to capitalize on any time available.

- Data for creating user accounts was to have been collected during in-processing. This was not always the case and some students arrived for training to discover that they did not have accounts. Creating these accounts on the spot delayed some of the larger classes 15 minutes or longer.

- There were several temporary network outages that disrupted the instruction.

- PC and UNIX users in the same class required different instruction for some of the same actions.

Despite these challenges, CVW training was successfully carried out and proved to be effective for most of the students who took the course. Nevertheless, the criticality of conducting training according to an organized schedule and in a appropriate environment cannot be overemphasized. Being able to efficiently use a collaborative tool in a distributed environment spans multiple functions, and haphazard or no training has the potential to have an extreme negative impact on operations and group interactions. As covered in the operational sections of this report, operators took what they learned in training, used it to their advantage, and developed further operational innovations in using the tool. A thorough understanding of tool capabilities is critical for operators to take that next step.

After training the collaborative tool in both EFX 98 and JEFX 99, as well as in exercises with other services, a recurring pattern related to training can be observed. After training, and as the execution gets underway, some users adapt immediately but many operators new to this technology tend to evolve through four stages towards acceptance of proficient use of this tool. This pattern generally takes about two to three days to reach stage four.

Stage One - Operators are initially apprehensive of collaboration and the tool and are reluctant to use it. This stage requires continued user support by the collaboration support team and staff supervisors, and encouragement to proceed.

Stage Two - Operators begin to more actively use the tool and experience frustration based on simple errors, sometimes correcting themselves and frequently requesting further assistance.

Stage Three - The users become increasingly confident and comfortable with the tool, using all the features they learned in training and enthusiastically developing new innovations for doing their jobs.

Stage Four - Most reach a comfortable mastery of the tool and state how essential it is for them to conduct their jobs and manage operations.

It should be noted that Stage One is reached following some reasonable level of training. It will be noted that several hundred JEFX 99 users were never formally trained during the experiment though some had probably been trained elsewhere. Those who did not attend training tended not to use the collaborative environment or required considerable help from the on site support team and from coworkers. These folks had less of a chance of reaching Stage Four and retarded their fellow operators in the process. Attendance at training should be a precondition for obtaining a user account and every participant regardless of grade or position should have an account.

Section 4

User Suggested Enhancements

This section recounts user feedback collected by the Integrated Collaborative Operations Team during JEFX 99 execution. Although many comments refer to issues related to CVW, they are useful for drawing general conclusions concerning collaborative tools for the C2 warfighter. In addition, some user comments were collected that directly address hardware and infrastructure issues associated with collaborative tools in general.

- Users requested “page forward” and “page reply” buttons for the textual page pop-up window. They wanted to be able to reply directly to the person who sent them a page, and to easily forward the page to other users. Other users thought that the content of a pop-up page should show in the sender and receiver’s scroll back for future reference. Some users found pop-ups annoying when they were trying to work.

- Users expressed the need to be able to move to another room without “walking” down “corridors” or “stairwells.” This was commonly referred to as a "teleport" capability.

- Users reported that a better method of capturing screen images for use in the collaborative environment was needed. They found the screen capturing tools/methods used in JEFX 99 cumbersome.

- Users said they wanted some kind of notification when someone has dropped something into their “carrying folder.”

- Users expressed a need for an easier method/process for preparing and making PowerPoint files available for mass briefings.

- Users said they wanted a better way of providing office applications to the UNIX desktop. They reported that WinCenter was difficult to use, slow, and often unreliable.

- Users requested headsets or audio cards with “Automatic Gain Control (AGC)” to maintain more consistent audio volume levels.

- Users said they wanted a drag-and-drop capability for importing files into the collaborative tool (described as an automated verses manual import capability).

- Users said they wanted to be able to page each other from the list of users in the audio tool window.

- Users expressed a need for an easy-to-use, shared, user storage space. They wanted this space to be accessible via a web browser.

- Users were confused when CVW components like “carrying folders” and “whiteboards” that were already open, but hidden, and would not come to the top when invoked again from within CVW.

Section 5

Technical Description

The technical description of a successful collaborative tool (CT) deployment must include at least three major components: (1) the unique CT system architecture for that deployment, (2) the network infrastructure on which the system would be supported, and (3) the security risks the system would face and the measures that would be taken to mitigate those risks. Sections 5.1, 5.2 and 5.3 report how CVW, networking, and security technologies, respectively, were employed to create a complete system. Inevitably, technical difficulties were encountered and, wherever possible, overcome. Section 5.4 enumerates those difficulties, the related details, and the corrective actions the team was able to take.

5.1 CVW Architecture

5.1.1 Deriving and Defining the Architecture

Early thinking and planning for participation in JEFX 99 was based heavily on EFX 98 experience coupled with scaling factors dictated by the relative size differential of the two experiments. The JEFX 99 collaborative tool requirement was to support up to 500 simultaneous users in a single environment, with upward of 1600 user accounts. The EFX 98 architecture was nearing its limits with approaching 1000 user accounts and 300 concurrent on-line users. With improvements made to the CVW server that included speeding up navigation within the virtual building, the 500 concurrent on-line users for a single CVW server was an achievable goal for JEFX 99. The network and security plans and the maximum number of concurrent on-line users were the first set of major drivers for the CVW system architecture.

The second set of drivers was the physical locations of the users and the numbers of users at those locations. Although exact numbers were not available, it was clear that there would be large (over 100) concentrations of users at the Operations Support Center (OSC) at Langley AFB, VA; the Combined Aerospace Operations Center (CAOC) at Hurlburt AFB, FL; and at Nellis AFB, NV in three facilities. There would also be some number of small sites, each with one to ten machines, and there would be one airborne and one shipboard "site."

The one remaining significant change between EFX 98 and JEFX 99 was the increased number of Microsoft NT workstations and laptops. Their impact on the architecture was small but unlike the UNIX workstations, the majority of which were operated by one initiative, Theater Battle Management Core System (TBMCS), the NT machines belonged to many initiatives and were most common at the smaller sites. This drove the need for an easy end-user installation package. Also, to support TBMCS and others, a DII-COE compliant (level 5) version of the CVW UNIX client had to be provided.

It is always important to plan for adequate penetration (concentration of CT-enabled workstations) when deploying a CT system. The effectiveness of a CT environment from the user perspective requires that enough potential active on-line users actually have the capability so that a critical mass can be reached in each workgroup. In JEFX 99, the latest version of CVW was used that included a fully functional client for NT. With the larger number of client workstations and the much larger percentage of NT workstations the opportunities for achieving adequate penetration were substantially improved.

5.1.2 System Engineering Issues and Goals

The JEFX 99 CVW architecture aimed at an optimal solution within the constraints imposed by the communications links, the numbers and concentrations of users, the security system, and the CVW tool itself. The implementation of that architecture was further constrained by severe resource limitations. The most significant limitation was the lack of preparation and experimentation time, since the effort did not commence until July 1999. The opportunity to gradually build the system and test its components through Spirals 1 and 2 was lost. The accelerated deployment schedule, so close to execution diminished the availability of experienced personnel and significantly impacted the ability to advance the experimentation of virtual AOC operations beyond what was achieved in EFX 98. Consequently, some pieces of the architecture were compromised.

Specific goals and issues for the architecture are listed below followed by further discussion of the steps that were taken to implement and deal with them.

- Start with a complete system design and scale it to what would be possible in the available time with the available resources
- Concentrate on issues that are most important to the operators
- Document what could not be accomplished in the timeframe
- Distribute services as much as possible to reduce network loading and improve response time
- Provide backup support for hardware, software, and network failures (support as many users as possible regardless of type of failure)
- Be prepared for IW Red Team attack
- Support up to 500 simultaneous users
- Provide hot backup for OSC, CAOC, and possibly BCC and SOC
- Provide separate web services for OSC, CAOC, and possibly BCC and SOC
- Provide support for individuals and remote sites to download and install clients configured for their location and connectivity
- Provide web publishing capability
- Interface to VTC, OSC and CAOC room AV
- Provide trained people and their workspaces to support user account creation, training and on-line help

The goals were to provide highly reliable CT services with the best possible performance for all users. Reliability meant distributing CT services so that most, if not all, users would have some CT capability in the event of a significant failure, one that had the potential to impact a large number of users. The two most obvious failure threats were hardware failures in the primary server equipment and failures of the long-haul communications. Performance meant providing key services to all users with the least possible delay regardless of the number of users or of a user's location.

The use and placement of hot backup servers was the approach used to deal with the reliability issue. The backups were placed so as to be local to the largest concentrations of users, one at Langley and one a Hurlburt. Thus, in the case of either a primary hardware failure or a failure of the major communications line between these two locations, the users would have ready and, if necessary, local backup capabilities. The ideal circumstance would have been to provide at least a local server for Nellis. A full backup server was judged impractical because of the difficulty of transferring backup data and the lack of trained personnel to maintain the backup data. (See Backup Procedures in Appendix D.)

The configuration of the CVW and web servers was dictated by the desire to optimize performance as never before for a user population larger than any previously encountered. The networking team was focused on making the best of the available communications circuits, while the Integrated Collaborative Operations Team focused on engineering the optimal tool deployment solution. The JEFX 99 operators required a single virtual environment; thus a single CVW server was implied. The CVW server process is CPU intensive and single threaded. That is, it places a high demand on the CPU and cannot take advantage of multiple CPUs. Thus, the decision was to dedicate a single server platform with a single high performance processor to running the server process and nothing else. The fastest production processor (CPU) available at the time had a 400 MHz clock speed. The Sun Sparc Ultra 2 workstation employed as the CVW server was equipped with a new 400 MHz processor replacing the two 296 MHz processors used in EFX 98. A new Sun Enterprise 250 with two 400 MHz processors was provided by the program and was used for the document server. A second Ultra 2 was reconfigured with the two 296 MHz processors and was used as the local backup and web server. Figure 5.1 shows the placement of the primary and backup CVW servers.

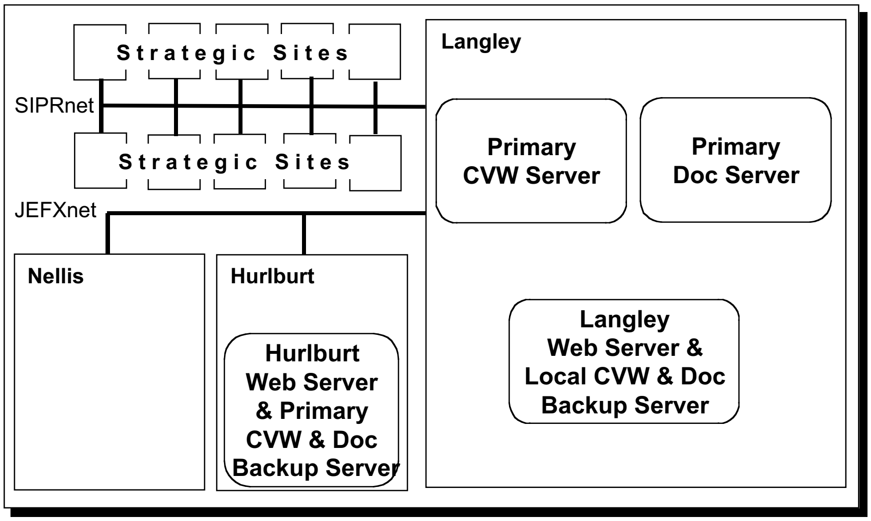

Strategic Sites
SIPRnet
Strategic Sites
JEFXnet
Nellis
Hurlburt
Hurlburt Web Server & Primary CVW & Doc Backup Server
Langley
Primary CVW Server
Primary Doc Server
Langley Web Server & Local CVW & Doc Backup Server

Figure 5.1 – JEFX 99 Software and Hardware Layout

A user working through a CVW client accesses services from several sources: the CVW Server, CVW Document Server and web server. The CVW Server supplies basic functionality supported by the client application with certain data. The CVW Document Server stores individual and shared files and enables users to export/import files from their local file system. Whiteboards may have backgrounds that are resident on the document server or on a web server. User picture icons can be distributed from one or more web servers. Judicious placement of these servers reduces the network distance between clients and servers, thereby providing fast responses from each of these services.

The physical locations of large user groups influenced the design of a robust, multipurpose backup strategy. In this environment the backup systems were planned both as protection in case of CVW hardware failure and to provide local full function capability to the local communities when communications among those locations were down. The goal was to provide full backups at Langley and Hurlburt AFBs and a "local" server at Nellis AFB. Figure 5.2 shows the backup strategy.

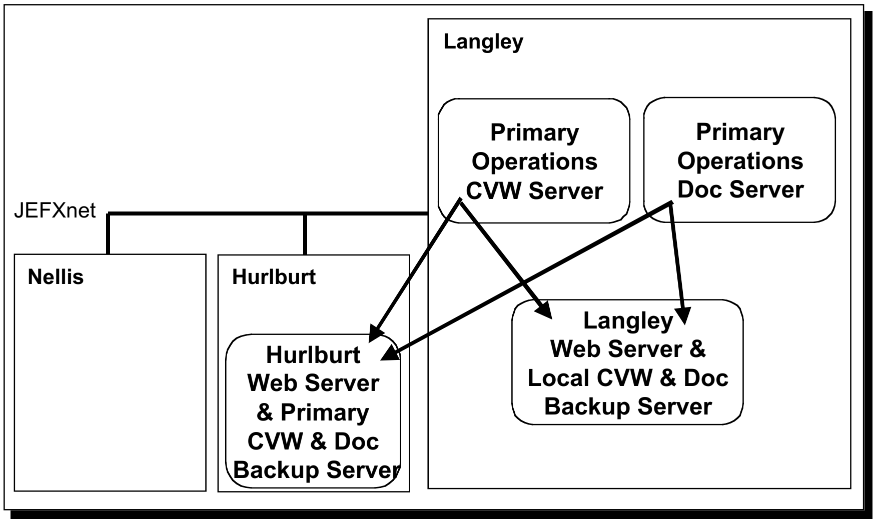

Langley
Primary Operations CVW Server
Primary Operations Doc Server
JEFXnet
Nellis
Hurlburt
Hurlburt Web Server & Primary CVW & Doc Backup Server
Langley Web Server & Local CVW & Doc Backup Server

Figure 5.2 - Daily Backup Plan Layout

The "deployed" backup server and web server were located at the JEFX 99 CAOC (Hurlburt AFB). At the end of each day of execution, the data that constituted the primary server and document server were gathered (without stopping any server processes), compressed and transferred to the Langley and Hurlburt backup machines. The actual transfer was performed during the night when other network traffic was low. The following morning the backup server processes were stopped, the new backup files were uncompressed and written over the previous day's backups. Certain reconfiguration was performed before the backup servers were restarted. (See backup procedures in Appendix C.)

The architecture called for a local server and web server at Nellis AFB. Resource limitations prevented us from implementing that server. Had that server been available, the Nellis users could have continued to work collaboratively among themselves during the several lengthy communications outages between Nellis and Langley. Also, the rate at which Nellis users could navigate among the virtual rooms was slowed because user pictures that would have been hosted on the local web server were instead being transmitted out from the web server at Langley.

We did not anticipate a large number of Space Command users. In fact, there did not seem to be many. At one point, just before execution began, it appeared that there might be more and a separate web server for them seemed desirable.

These web servers had another function, supplying the senior commander briefing slides both for use during the briefing and for review by others following the briefing. The process for preparing these briefings is covered in Section 6.1 (last paragraph) and

Appendix C.4. From a technical standpoint, the key issue is making those briefings available to everyone without relying on one source to supply them and without overloading some of the communications links every time a hundred or more briefing participants flip to the next slide. Again, this capability was realized at Hurlburt and Langley and thus the briefings were sent across the communications link only once when the copy was placed on the second web server. After that the users opened the copy of the briefing stored locally. This capability would have been desirable at Nellis as well.

With the major drivers factored into the architecture, attention turned to addressing the details of deploying CVW in a suitable configuration. In order to take advantage of the architecture, each site, or site cluster, required unique client configurations. Figure 5.3 illustrates the options users had for connecting to various servers and the complications this introduced in terms of providing the right server configuration files for each user cluster.

	Primary CVW Server (at Langley)	**Primary Doc Server (at Langley)**	**Web Server & Local CVW & Doc Backup Server (at Langley)**	**Web Server & Primary CVW & Doc Backup Server (at Hurlburt)**
Langley				
OSC Users				
CVW Server	Primary		Local Backup	Backup
Doc Server		Primary	Local Backup	Backup
Web Server			Primary, Local Backup	Backup
Pictures			Primary, Local Backup	Backup
Hurlburt				
CAOC User				
CVW Server	Primary		Secondary Backup	Local Backup
Doc Server		Primary	Secondary Backup	Local Backup
Web Server			Secondary Backup	Primary, Local Backup
Pictures			Secondary Backup	Primary, Local Backup
Nellis and Sites				
BCC/EOC User, etc.				
CVW Server	Primary			Backup
Doc Server		Primary		Backup
Web Server			Primary	Backup
Pictures			Primary	Backup

Figure 5.3 - User Login and Configuration Files Layout

5.1.3 Architecture as Implemented

Table 5.1 is a brief tabular description of the hardware used to implement this system.

Table 5.1 - Equipment Acquired for Spiral 3 and JEFX 99 Execution

JEFX 99 Requirements	H/W Used	Acquired from
Prime CVW Server*	1 Sun Ultra 2	1 Sun Ultra 2 (fm CUBE)
CVW Web & Langley Backup Server	1 Sun Ultra 2	1 Sun Ultra 2 (fm CUBE)
Prime Doc Server*	1 Sun Ultra 250	1 Sun Ultra 250 Enterprise (from Hurlburt)
Hurlburt Backup Server	1 Sun Ultra 2	1 Sun Ultra 2 (fm Hurlburt)
Headsets	~400	~50 from Hurlburt ~50 from Langley ~50 from Phase 1 balance purchased new
Cameras	few	All from existing stock @ Hurlburt and Langley
Integrated Collaborative Operations Team dedicated workstation	1 Sun Sparc 5 @ Langley	Loaned by MITRE

* CVW functionality is distributed over 2 separate server machines for better performance.

The relative success achieved in JEFX 99 can be attributed in part to the formulation of the technical architecture and the system engineering effort. The degree of success is partially reflected in the daily status logs and in the sample performance data that was collected during execution. This data is contained in Appendix B. Part of the detailed planning that grew out of the architecture is reflected in the technical processes and procedures documents that are contained in Appendix C.

5.2 CVW Network Analysis

As demonstrated in EFX 98 and confirmed in JEFX 99, the network infrastructure plays a critical role in the effective employment of collaborative tools and in particular, persistent virtual environments that demand continuous and reliable connectivity. This section presents the network architecture and discusses the multicast routing protocols and multicast issues from JEFX 99. The discussion of multicast routing is particularly appropriate here because 1) past exercises and experiments have demonstrated the benefits of multicast-enabled collaboration tools and 2) the relative newness of multicast-enabled network technology poses some challenges to their widespread configuration and deployment. Network assessment data related specifically to CVW is presented and analyzed in section 5.2.2.

5.2.1 Network Architecture

An overview diagram of the JEFX 99 network architecture is shown in Figure 5.4. More information about the security aspects of the network architecture for JEFX 99 is contained in section 5.3. This information includes the Virtual Private Networks (VPNs), firewall architecture and intrusion detection mechanisms. Also, a very detailed discussion of this architecture and analysis of the network assessment data can be found in MP-99B0000079, "JEFX 99 Network Assessment."

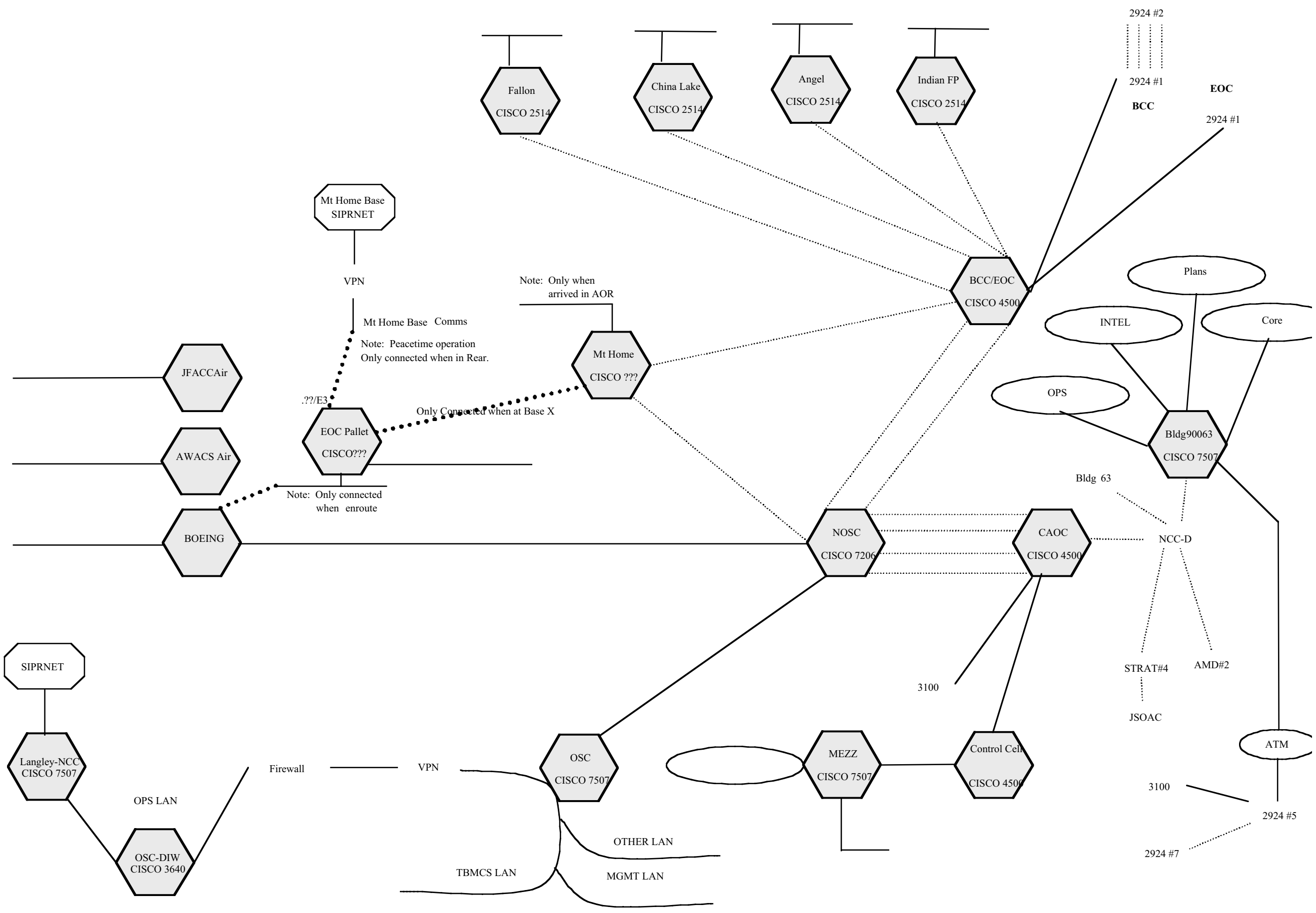


Figure 5.4 - JEFX 99 Network Architecture

Following the problems with implementing a robust multicast architecture in EFX 98, further research into multicast routing and analysis of those issues resulted in a new approach for JEFX 99. It was decided to employ Protocol-Independent Multicast Sparse-Dense (PIM S-D)[1] as the core multicast routing protocol. The JEFX router in the OSC served as the Rendezvous Point (RP) for the PIM S-D protocol.

Because (1) DISA policies prohibit the routing of multicast over DISA WANs and (2) RedCreek's Ravlin VPNs cannot pass multicast IP packets; a solution for routing multicast to the JEFX 99 strategic sites without using PIM S-D was required. Through Spiral 2 of JEFX 99, the communications engineering staff believed that *mrouted* (multicast router demon) hosts at the strategic sites could provide an adequate solution

[1] Additional information on multicast routing using PIM or DVMRP can be found at the Cisco Web site in the document *Configuring IP Multicast Routing*, http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/np1_c/1cprt1/1cmulti.htm.

for implementing multicast for collaboration between the OSC and the strategic site clients. Using *mrouted* was desirable because it could be hosted on an ordinary Unix system and didn't require additional network hardware. Following multicast problems in Spiral 2 and consultation with CISCO engineers, it was verified that networks using the Distance Vector Multicast Routing Protocol (DVMRP) as implemented by *mrouted* to route multicast traffic can have boundary incompatibilities with networks using PIM S-D. The known incompatibilities explained many of the multicast problems that were observed during Spiral 2.

A new solution for Spiral 3 was designed that would install a Generic Route Encapsulation (GRE) Router in addition to a VPN device at each strategic site. The GRE Router serves as the tunnel endpoint for a GRE tunnel between the JEFX 99 router in the OSC and each strategic site. The GRE tunnel operates inside the VPN tunnel between the OSC and the respective strategic site. A GRE tunnel encapsulates traffic between routers in such a way that all of the traffic is unicast, even multicast traffic traveling between the two networks connected by the tunnel. Multicast routing, using PIM S-D, can then be performed through the GRE tunnel. This GRE solution enables the transport of multicast traffic across the DISA WANs which do not natively support multicast routing in a secure fashion without compromising the security architecture. This solution was implemented prior to Spiral 3 and was employed until the end of the JEFX 99 execution phase.

5.2.2 Analysis of CVW Network Data

Ever since the earliest versions of CVW there have been questions about its impact on network resources. It has always been clear that the traffic fell into two categories, (1) unicast traffic for data communications and file transfers between clients and servers and (2) multicast traffic for audio and video data among clients. The analysis in this section is devoted to the first category, traffic that was generated by or destined to the three primary CVW servers during JEFX 99 execution. This traffic was generated by functions such as user logins, collaborative space management data, whiteboard traffic, document server traffic and web server traffic. This data includes most all of the CVW collaboration activities but excludes the more bandwidth intensive multicast traffic, the audio and video data that was routed and managed by the network devices.

Because CVW multicast traffic is client-to-client and not routed through the servers, the only multicast collaboration traffic observed at the three CVW servers in the OSC was the traffic associated with CVW clients being used by administrators on the server machines. The bulk of the multicast collaboration during JEFX was among AOC operators and therefore not visible at the CVW servers.

The data presented here regarding network traffic on the CVW servers was meant to assist in determining network requirements for collaboration in a distributed AOC environment. The data is presented using summary statistics and network traffic profiles to enable the readers to derive their requirements from the observations collected during JEFX 99.

Multicast traffic in JEFX was managed using PIM S-D routing across the network devices. An alternative would have been to use a unicast reflector. The disadvantage of the reflector is that it requires all traffic to be transmitted to a central point in the network architecture where it is then "reflected" out in separate data streams, one per subscriber. A reflector can easily become CPU-bound or network-bound when processing large volumes of traffic such as those seen during JEFX.

PIM S-D routing uses mathematical trees to define coverage for each multicast group as defined by one IP multicast address. In this case the processing burden is distributed across all of the network devices that comprise the multicast network. This approach is more scalable than the *mrouted*-based multicast tunneling approach. These multicast-aware network devices in JEFX 99 included the routers, Ethernet switches, Fiber Distributed Data Interface (FDDI) edge devices and Asynchronous Transfer Mode (ATM) edge devices.

It is impossible to characterize the volume of CVW multicast traffic or any multicast-enable application by collecting network traffic observations at a single or a small number of sampling locations. By the very nature of multicast traffic and multicast routing the multicast packets and streams are distributed across all of the multicast-aware network devices. There are two interfaces in the OSC network architecture where assessing the level of multicast traffic would probably be most valuable and informative: (1) at the Cisco 7206 router where traffic is going to or coming from the WAN circuits to the CAOC, BCC/EOC, and Mt. Home and, (2) at the Sidewinder firewall interface to the external Secret IP-Routed Network (SIPRNET). The ideal points to collect the data for these two interfaces respectively are (1) on the Ethernet connection between the 7206 and 7507 routers and (2) at the Ethernet interface to the external firewall. Unfortunately, the JEFX network assessment team did not manage the probes at these two interfaces and the probes used were not configured to store data in a NetMetrix[2] archive.

An alternative to monitoring the traffic between the 7206 and 7507 would be to watch the traffic on the 7 WAN circuits leaving the OSC using the NetMetrix WAN probes. (See Figure 5.6.) Unfortunately, the WAN probes support V-series serial Remote Monitoring (RMON) data collection and do not support the necessary RMON Management Information Base (MIB) groups required for doing a post-experiment breakdown of the multicast, unicast, and broadcast traffic. Thus, the opportunity to monitor, evaluate, and characterize multicast traffic traversing key segments of the network was lost. This is unfortunate because the operators used audio a great deal and knowing the impact of that use on the network would be helpful in planning future deployments of similar capabilities.

[2] NetMetrix is a registered trademark of Agilent Technologies

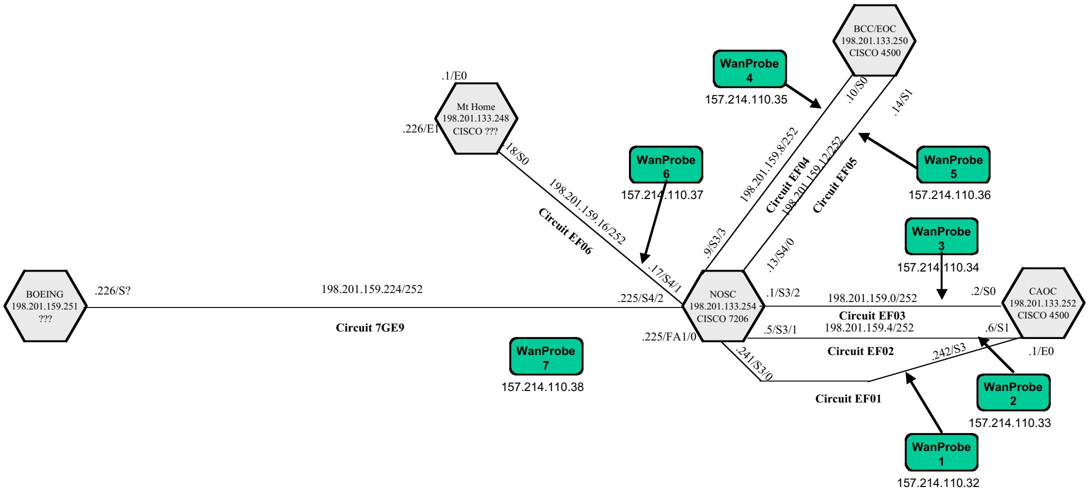


Figure 5.5 - WAN Probe Placement

CVW Server

Analysis of the network traffic to and from the CVW server showed no reasons for concern in the context of JEFX 99 but pointed out an area requiring greater system engineering sophistication for future experiments and for any exercise of deployed system. The backup process for CVW depended on collection, compressing and transmitting a copy of the entire contents of the primary CVW to the backup servers (see Appendix C1). As time passed the server database grew and the size and duration of the transmissions grew. In a true 24 hour operation there might not be a daily window when this large file could be transmitted without adversely effecting operational traffic.

When examining the network traffic collected at the CVW server, the most striking fact was that the top generator of IP traffic on the CVW LAN connection was TBMCS subnet broadcast traffic from the SAA server. The level of this traffic ranged from 420 to 580 megabytes per day over the course of the four days of LiveFly activities. This is an average of 40 to 55 kbps of Common Operational Picture (COP) traffic being disseminated by SAA. Since CVW was not a COP client, and in no way participated in the COP, this was traffic that should not be counted as collaboration related.

There is nothing striking or unusual about the other sources and destinations of the network traffic seen on the CVW server LAN segment. There is the expected traffic for the CVW backup server at the CAOC: CVW2, the CVW Web server, and the CVW server itself. In addition, most of the other top sources and destinations are multicast address groups, representing various audio channels in the CVW virtual architecture. No significance should be placed on the identity of the audio groups since they only indicate what collaborative spaces the CVW system administrators visited.

The level of traffic observed outbound from the CVW server during the first two days of LiveFly exercises was at its greatest levels between the hours of midnight and 6am EDT. This is the traffic associated with the replication of the CVW server onto the backup CVW server, CVW2. Since the replication traffic can be observed to exceed the total volume of CVW server traffic that is outbound over the course of the experiment day this begs the question whether there might be a better way to perform the replication.

Tables 5.2 and 5.3 present a summary of the CVW traffic for the “normal” hours of JEFX 99 operations. The traffic for all users includes the traffic from users at the OSC, CAOC, BCC/EOC, and all strategic sites. With the lack of an RMON probe on the ATM link between the NOSC and the OSC, it is impossible to separate out the traffic from the OSC staff positions.

The average traffic from the CVW server to locations in the CAOC during the 7am to 12 midnight period on LiveFly day 1 was almost 12 kbps. From Figure D.10, it can be observed that there was one half-hour period when the traffic from CVW server to the CAOC exceeded 80 kbps and one when it exceeded 40 kbps. The traffic observed on LiveFly days 2 and 3 averages 18 to 19 kbps. There were periods when the traffic was heavier than on the first day. In fact the traffic exceeded an average of 100 kbps for a half hour period once on day 2 and once on day 3. The traffic for LiveFly day 4 was the lightest of all, due to the end of formal JEFX experimentation in the late afternoon hours and prior to that evening’s start of Y2K testing activities.

In Figures D-17 through D-20 the traffic outbound to the BCC and inbound from the BCC to the CVW server for the first two days of LiveFly is shown. All of these charts clearly indicate two peaks, with these peaks apparently related to the two periods of LiveFly activities on each of the two days.

The traffic for the period of time between 2am and 6am was separated from the rest of the day because this was the time when the CVW servers were backed up from the OSC to the CAOC. While this is valuable data for understanding the network impacts of such operations, these infrastructure support operations should not intermingled with the AOC collaborative operations observed during the 7am to 12 midnight period of time especially given the unusual nature of some of the CVW infrastructure support operations. In real-world operations with a 24-hour battle rhythm the infrastructure support and AOC operations periods will be intermingled and the levels traffic will be correspondingly increased in volume over what was observed during JEFX 99.

Table 5.2 - CVW Server Traffic, 7am – 12 midnight EDT

	OSC-CAOC				OSC-BCC				All Users	
	In		Out		In		Out		Total	
	Total (bytes)	Avg. (bps)	Total (bytes)	Avg. (bps)	Total (bytes)	Avg. (bps)	Total (bytes)	Avg. (bps)	Total (bytes)	Avg. (bps)
30-Aug-99	6,352,549	743	99,743,920	11,666	7,917,166	926	148,673,860	17,389	1,828,263,178	213,83
31-Aug-99	8,966,882	1,049	158,822,945	18,576	15,466,425	1,809	89,125,379	10,424	1,835,290,292	214,65
1-Sep-99	9,749,101	1,140	164,446,073	19,233	11,433,172	1,337	42,023,440	4,915	1,663,524,473	194,56
2-Sep-99	5,797,951	678	98,407,616	11,510	7,323,673	857	71,913,614	8,411	1,109,001,710	129,70

Table 5.3 - CVW Server Traffic, 2am – 6am EDT

	OSC-CAOC				OSC-BCC				All Users	
	In		Out		In		Out		Total	
	Total (bytes)	Avg. (bps)	Total (bytes)	Avg. (bps)	Total (bytes)	Avg. (bps)	Total (bytes)	Avg. (bps)	Total (bytes)	Avg. (bps)
30-Aug-99	0	0	0	0	20,800	12	39,120	22	176,932,076	20,69
31-Aug-99	0	0	0	0	9,360	5	752,520	418	127,873,373	14,95
1-Sep-99	0	0	0	0	36,280	20	37,200	21	113,147,622	13,23
2-Sep-99	0	0	0	0	18,720	10	311,940	173	80,596,575	9,42

CVW Document Server

In Tables 5.4 and 5.5 the traffic for the CVW document server is presented. The traffic volumes were considerably greater than those observed for the CVW server, as would be expected because most of the traffic consisted of data files many of which included images and graphics, thus making the files large.

On LiveFly day 1 there were seven half-hour periods when the traffic exceeded 50 kbps including one half-hour period when the average exceeded 130 kbps. Similar traffic was observed on day 2. The traffic on LiveFly day 3 was slightly less.

The BCC traffic is only a small fraction of the volume of the CAOC traffic with day 1 being the greatest when it constituted approximately 20% the volume of the CAOC traffic. CVW Document Server traffic for the BCC is disproportionately low compared to the CAOC traffic. From this data it appears that the CVW users in the BCC created and opened fewer documents on the CVW Document server than the CAOC users. This might be due to the reduced bandwidth between the OSC and the BCC or it could be the BCC users' response to requests to conserve communications bandwidth.

Table 5.4 - CVW Document Server Traffic, 7am – 12 midnight EDT

	OSC-CAOC				OSC-BCC				All Users	
	In		Out		In		Out		Total	
	Total (bytes)	Avg. (bps)	Total (bytes)	Avg. (bps)	Total (bytes)	Avg. (bps)	Total (bytes)	Avg. (bps)	Total (bytes)	Avg. (bps)
30-Aug-99	41,365,772	4,838	249,459,449	29,177	30,638,282	3,583	46,655,126	5,457	3,583,581,256	419,13
31-Aug-99	17,170,479	2,008	205,676,609	24,056	10,403,796	1,217	7,054,789	825	2,284,077,036	267,14
1-Sep-99	25,561,147	2,990	196,601,114	22,994	4,671,094	546	12,042,982	1,409	2,219,462,251	259,58
2-Sep-99	15,531,181	1,817	90,452,384	10,579	2,630,695	308	6,871,227	804	1,993,780,374	233,19

Table 5.5 - CVW Document Server Traffic, 2am – 6am EDT

	OSC-CAOC				OSC-BCC				All Users	
	In		Out		In		Out		Total	
	Total (bytes)	Avg. (bps)	Total (bytes)	Avg. (bps)	Total (bytes)	Avg. (bps)	Total (bytes)	Avg. (bps)	Total (bytes)	Avg. (bps)
30-Aug-99	5,331,960	2,962	209,814,920	116,564	0	0	14,160	8	1,232,731,391	144,17
31-Aug-99	10,719,160	5,955	452,718,320	251,510	0	0	0	0	2,395,708,205	280,20
1-Sep-99	9,349,960	5,194	457,169,320	253,983	0	0	0	0	2,382,503,927	278,65
2-Sep-99	8,389,480	4,661	418,537,320	232,521	0	0	0	0	1,993,780,374	233,19

CVW Web Server

The CVW Web Server provided a combination of user help files, a download site for CVW clients, user help pages, a repository for CFACC briefings and CVW user pictures. It should be noted that these latter two categories, the briefings and the user pictures, would have been some of the most widely user objects on this server. It should also be noted that a duplicate copy of each briefing and user picture was put on the CAOC CVW web server as well. Briefing web objects in CVW were labeled OSC and CAOC and users were asked to open the “local” copy. Also, the CVW clients at the CAOC were configured to get their user pictures off the local web server while the OSC and BCC clients were configured to get theirs from this server.

Analysis of the relative traffic loads reflect these decisions and point out the valuable role a web server at Nellis would have played. The traffic for the CVW Web server was considerably less for the CAOC than that for CVW and CVW Document servers. Interestingly, the traffic for the BCC to the CVW Web server on live-fly day 1 was almost 75 percent that of the traffic between the CAOC and the CVW Web server. In Tables 5.6 and 5.7 the network traffic data for the CVW Web Server is presented. In Tables 5.6 and 5.7 the network traffic data for the CVW Web Server is presented.

In Figure D.68, Appendix D, it is interesting to observe that the traffic from the CVW Web Server outbound to the BCC on LiveFly Day 1 had a large peak between 12:30 and 2:00 PM EDT and then dropped to very low levels after 4 PM. This appears to correlate with the times when SATCOM communications from the OSC were shutdown due to high winds from a hurricane. From this same figure an increase in outbound traffic volumes can be observed around 10 – 11 PM EDT. This corresponds to the LiveFly activity period for 30 August. Similarly, increases in CVW Web traffic can be observed for live-fly days 2 and 3 in Figures D.70 and D.72 respectively.

Table 5.6 - CVW Web Server Traffic, 7am – 12 midnight EDT

	OSC-CAOC				OSC-BCC				All Users	
	In		Out		In		Out		Total	
	Total (bytes)	Avg. (bps)	Total (bytes)	Avg. (bps)	Total (bytes)	Avg. (bps)	Total (bytes)	Avg. (bps)	Total (bytes)	Avg. (bps)
30-Aug-99	12,434,382	1,454	40,879,036	4,781	3,406,454	398	29,546,855	3,456	2,938,592,974	343,69
31-Aug-99	14,587,574	1,706	72,838,244	8,519	2,956,512	346	25,377,160	2,968	2,119,840,247	247,93
1-Sep-99	22,914,995	2,680	26,673,765	3,120	2,874,141	336	12,801,753	1,497	2,066,531,882	241,70
2-Sep-99	5,637,680	659	36,000,865	4,211	973,538	114	7,500,529	877	1,853,572,183	216,79

Table 5.7 - CVW Web Server Traffic, 2am – 6am EDT

	OSC-CAOC				OSC-BCC				All Users	
	In		Out		In		Out		Total	
	Total (bytes)	Avg. (bps)	Total (bytes)	Avg. (bps)	Total (bytes)	Avg. (bps)	Total (bytes)	Avg. (bps)	Total (bytes)	Avg. (bps)
30-Aug-99	0	0	0	0	0	0	0	0	171,324,900	20,03
31-Aug-99	0	0	0	0	0	0	0	0	121,767,134	14,24
1-Sep-99	0	0	0	0	0	0	0	0	1,370,599,200	16030
2-Sep-99	0	0	0	0	0	0	0	0	76,051,395	8,89

5.3 Security Considerations

5.3.1 Background

Collaboration poses new challenges for network security. Collaboration facilitates the free flow of information to enable dynamically assigned workgroups to work seamlessly across space and time over a system of networks. Network security is concerned with ensuring that information is only available to those with a verified need-to-know and that it does not flow beyond strictly defined boundaries; both real and virtual.

During JEFX, collaborative tools were used throughout the experiment enterprise. This included sites geographically distant (strategic sites, or stratsites) from the enterprise network built specifically to support the experiment. These stratsites were connected to the JEFX network, via SIPRNET, using a Virtual Private Network (VPN) security architecture described below. Use of collaborative tools at the stratsites were impacted by the following constraints:

- The JEFX network was protected from external attacks by a firewall configured to comply with Air Force System Security Instruction (AFSSI) 5027 which specifically prohibits both UDP and multicast traffic across that boundary

- The Sidewinder firewall is the Air Force standard and was used for EFX and JEFX. It does not implement a mechanism for forwarding multicast packets.

- The JEFX network was connected to SIPRNET, which does not support multicast.

These constraints were overcome through the combination of VPN devices and multicast-to-unicast tunneling protocols that allowed collaboration-oriented traffic to flow through the firewall, without rendering the firewall useless.

It should be noted that this technique only addresses the means by which relatively insecure traffic could be safely brought through a firewall. It does not address other collaborative security issues such as robust identification and authentication of users, or segregation of data within the collaborative environment.

5.3.2 Security Architectural Description

The basic security architecture consisted of a firewall installed at the SIPRNET connection point for the JEFX experiment network and bracketed with intrusion detection products. This firewall served as the default route out of the network. A VPN device was placed in line with the firewall so that all traffic exiting the JEFX network would have to pass through it first. The VPN device examined the destination address (DA) of every packet. If the DA matched an entry in the VPN tunnel list, the packet was intercepted, encrypted and encapsulated and sent on to a corresponding VPN device at the distant end. If the DA did not match any of the VPN endpoints, the traffic was passed on to the firewall unmodified. The VPN operated in a hub and spoke configuration with the JEFX enterprise network VPN device as the hub and the site VPN devices as the spokes.

The VPN devices chosen did not recognize multicast packets placed on the network. Before the multicast traffic could be sent to the stratsites to enable them to participate in the audio and video segments of the collaborative environment, the multicast packets had to be converted into unicast. This was accomplished through the implementation of Generic Routing Encapsulation (GRE) on several of the multicast-aware routers deployed on the JEFX network. For those sites that required collaborative participation, an inexpensive, GRE-capable router was supplied along with the requisite Ravlin VPN device. Back on the JEFX network, GRE tunnels were created for each stratsite endpoint with a VPN/GRE router pair. Routers were also established to send multicast traffic through these tunnels to the endpoints. This architecture is illustrated in the figure below.

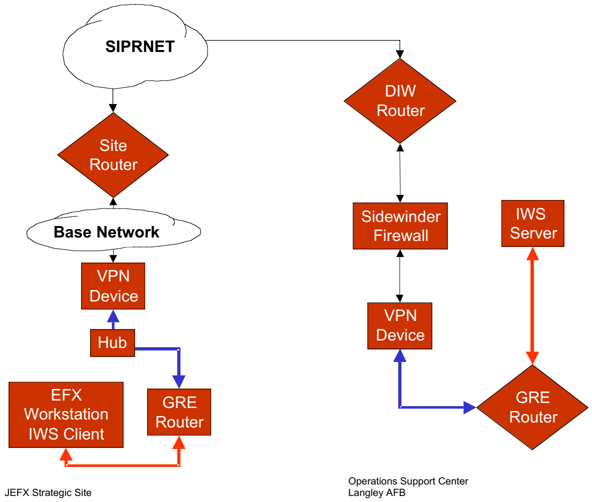


Figure 5.6 – Security Architecture Diagram

As the collaborative tools generated multicast packets, those packets were distributed throughout the network by the multicast-aware infrastructure. As the multicast packets reached the central JEFX router, they were encapsulated into GRE packets that were sent out to the individual stratsites wherever there were subscribers to active multicast sessions. The VPN devices recognized the GRE packets and thus were able to examine the destination addresses. Since all of the destination addresses corresponded to networks that were part of the VPN, the GRE packets were intercepted, encrypted and encapsulated again before being sent on to the firewall. The firewall was configured to pass IPSEC traffic between the central VPN device on the JEFX network and the corresponding VPN devices at the strategic sites located on the SIPRNET. The packets were then routed through the SIPRNET to the VPN device at the distant end. Once there, the packet was examined to ensure that it was a valid VPN packet from a valid originating address before it was unencapsulated and decrypted and sent to the small GRE router located behind the VPN device. At the GRE router the packet was converted back into multicast and put out on the stratsite LAN for use by the local workstations participating in collaboration with JEFX. For multicast packets generated at the sites, the entire process was reversed.

Since the encryption and encapsulation took place at the network level, all of these machinations were both invisible to the end user, easy to implement for a heterogeneous computer inventory and worked across a vanilla TCP/IP network. No additional software had to be loaded onto any workstations beyond that required by the collaborative tools themselves.

5.3.3 Determining Whether to Use VPNs

The following items should be considered when determining whether or not to use VPNs as part of a collaboration strategy.

- Does the underlying infrastructure at each site support multicast?
- Does the infrastructure connecting these sites support multicast?
- Are firewalls installed along any of the needed paths?
- Does the network security policy for these firewalls allow multicast through the firewall?
- If not, does the network security policy allow the use of VPNs to provide tunneling?
- Can the security policies at all of the sites participating in the collaborative environment be reconciled to allow the use of the enabling technologies?
- What other hardware/software will need to be purchased to provide the solution?

If, following the guidance above, the decision is made to implement a VPN solution, the following steps should be followed.

Steps to buy a system

- Identify the number of sites that needs to be supported. This will determine whether or not a robust VPN management program is a requirement. Not all vendors provide feature-rich management suites. For a small number of sites this is probably not too much of a problem. If the sites number more than about a dozen, a strong management program is well worth the investment of money to purchase and the time to learn.

- Specify standards-based products wherever possible. This should make interoperability with future acquisitions less painful. This will also ensure that the encryption algorithms, key distribution mechanisms and tamper resistance of the products meet minimum standards. Standards to consider:

- IPSEC for encapsulation
- DES, 3DES, IDEA for encryption
- MD5, SHA-1 for digital signatures
- PKI, X509 for digital certificates for key management
- FIPS 140-1 for tamper resistance

- Find a vendor that offers a range of products. Not all sites will require a device capable of sustaining a 45Mb/s throughput at a cost of $17,000 a copy, especially if there are only a handful of users who are bandwidth constrained to fractional T1 speeds.

Configuration

After identifying and procuring a product that meets the interoperability, throughput and cost requirements, the individual site equipment must be configured prior to installation. Past experience for EFX 98 and again in JEFX 99 showed that it was much easier to pre-configure the site equipment in one or two main locations using personnel intimately familiar with the devices and then ship the units out to the field with simplified installation instructions.

Placement

Placement of the VPN devices is usually dictated by both operational necessity and security policy considerations. There are different considerations that come into play depending on the architecture implemented.

Firewall Considerations

If a firewall is part of the overall network security infrastructure, a decision needs to be made as to whether the VPN device will be located behind the firewall or in parallel with it.

- Behind the firewall. This was the configuration used in both EFX 98 and JEFX 99. This configuration provides additional protection for the VPN device and requires that the firewall policy be modified to pass the following types of traffic.

  - IPSEC – IP protocol 50, these are the encrypted packets sent between VPN devices.
  - ISAKMP – UDP port 500, this is the traffic that effects the key exchanges between VPN devices.
  - SNMP – UDP ports 60, and 61 may be required for device management (best handled through a proxy if available).

- In parallel with the firewall. This location allows the firewall policy to remain inviolate as far as enabling the VPN is concerned.

- Hubs or switches must be installed on both sides of the firewall to connect the VPN device in parallel. This may require a change to the network security policy.

- The last router before the inside interface of the firewall will have to be programmed to send all packets destined for VPN endpoints to the inside interface of the local VPN device.

- The router just before the outside interface of the firewall will similarly have to be programmed to route all packets destined for protected subnetworks to the outside interface of the VPN device.

VPN Mode of Operation

Most VPN devices can be operated in one of several modes. The modes discussed here apply to the RedCreek Ravlin devices used in EFX 98 and JEFX 99. Devices from other manufacturers will have similar modes under different names. The principles discussed here still apply.

Closed

In closed mode, systems located behind a VPN device can only communicate with systems or networks behind another VPN endpoint. Packets that are destined for VPN endpoints are intercepted encapsulated, encrypted and sent on to the distant end. All other packets are dropped. While this implementation might be useful for a small site that has no information protection infrastructure to protect itself, communication with entities outside the VPN can be convoluted at best.

In EFX 98, users at remote sites would not accept the limitations that this type of configuration would have placed on them. They needed access to systems and networks outside the VPN and were not willing to pay the performance penalty associated with the closed configuration.

Open

In open mode, any traffic between systems located behind VPN devices is encapsulated and encrypted and sent across the VPN. Traffic that is not destined for the VPN is passed in the clear both to and from non-VPN networks and systems. This allows users at a remote site to access non-VPN systems at their site and across whatever WAN they are tied to. Conversely, those non-VPN systems can also reach out and touch the system behind the VPN device.

The risks with such a connection should be intuitively obvious to the casual observer. If one site in the VPN community does not have adequate safeguards, such as firewalls and intrusion detection systems, in place, it is possible for an intruder to compromise a system or systems at that site and then attack other systems and networks that are part of the VPN community.

This is exactly what happened in EFX 98. The Opposing Force (OPFOR) Red team was not able to breach the firewall protecting the EFX 98 enterprise. They asked for and received permission to attack several of the stratsites so that they could ride down the VPN pipes to rape and pillage (in a virtual sense) at will. They succeeded.

Unless all sites participating in a VPN have similar rigorous network defenses and security policies, running a VPN site in open mode is a **BAD** idea.

One additional note, if all sites have similar defenses and policies, and you want to simplify routing rules, etc., by using open mode, place the VPN **BEHIND** the firewalls.

One-way bypass

One-way bypass refers to the mode whereby a VPN device located at a site with little or no network defenses is configured to allow systems located behind the device to initiate contact with non-VPN devices or networks. It is then free to push or pull data as needed. This connection stays open for a set period of time. The VPN device does not allow connections to originate from systems outside the VPN to systems behind that VPN. In a sense, the VPN device is operating as a crude firewall for those systems.

One-way bypass does not provide tight security. There are ways to hijack sessions to remote machines or place Trojan Horse applications on them. It is; however, the best way to bring in a site to which you must provide connectivity and have absolutely no control over the security architecture or policy.

This is the mode that was employed for remote VPN sites during JEFX 99 with great success. The Red team was blocked by both the firewall at the JEFX enterprise connection point but also by the VPN devices running in one-way bypass mode at the stratsites.

5.3.4 Additional Equipment

As described above, VPN devices and firewalls may not support the transmission of multicast packets. In the specific case we have been examining, the wide-area network connecting the sites did not support the transmission of multicast. To implement a VPN solution that maintained the integrity of the security architecture and also allowed non-contiguous sites to exchange multicast traffic, multicast packets were first converted to unicast for transmission to the VPN endpoints. This was accomplished by establishing multicast static routes, or mroutes, between multicast-aware devices and was implemented through use of either *mrouted* (multicast router demon) or Generic Routing Encapsulation (GRE) tunnels.

> *PLEASE NOTE:* The information in this section does not discuss all of the steps that must be taken to enable multicast on a network. It provides a brief overview with regards to enabling multicast converted to unicast through a firewall/VPN combination.

mrouted Environment

The *mrouted* protocol is a public-domain implementation of DVMRP. Using *mrouted* typically means that some or all of the network paths among the sites do not support multicast. If *mrouted* is required to convert multicast packets to unicast, set up a *mrouted* server on each subnetwork that includes workstations intended to participate in multicast groups. This does not mean that a dedicated server is required on each subnetwork, but disk space and processor cycles on a UNIX or LINUX workstations are needed. A *mroute* tunnel is established between pairs of *mrouted* workstations across the VPN network. Since *mrouted* creates a unicast packet with standard source and destination IP addresses, the VPN device will recognize it and then match it against its membership table to determine whether or not the packet gets encapsulated and encrypted.

GRE Environment

Another method available for converting multicast to unicast is by using Generic Routing Encapsulation, or GRE, a Cisco Systems, Inc. proprietary protocol that has been proposed as a draft internet standard. In JEFX 99 an all Cisco routing environment was used. All of the routers in the internal networked system were multicast-aware. One router at the central site was chosen as the rendezvous point for all multicast traffic. GRE tunnels were established between that central router and GRE-capable routers located at the remote sites participating in the VPN. As with the *mrouted* example above, the VPN device installed in line with the default route to the WAN intercepted the unicast GRE packets encapsulated and encrypted them and sent them down the VPN tunnels to the remote site.

Endpoint Equipment

In each of the examples described above, all of the remote sites participating in the VPN needed several pieces of equipment either provided for the sites or identified to them so that they could purchase their own. As a minimum each site required a VPN device to transmit and receive encrypted traffic. In the *mrouted* environment, the correct version of the *mrouted* software was also required. In the GRE environment there was a need for a GRE-capable router. In some instances, where a Cisco router was already installed on the remote network behind the VPN, the GRE option was activated and the necessary configuration changes were made. At those sites where an appropriate router was not available, an inexpensive GRE-capable router was provided and installed in a "one-armed" or "router on a stick" configuration. The router was supplied to provide an end point for the GRE tunnel originating at the central site and as a means of distributing the encapsulated multicast packet onto the remote subnetwork.

5.3.5 Deployment

With the site locations finalized and the mode of operation selected the next concern is how to get the devices in place at the various sites to support the collaboration systems.

Close Coordination Amongst Collaboration, Network and Security Personnel

Collaboration support personnel must coordinate activities closely with both network and security personnel. In some cases, the team that deploys the collaborative tools may be a separate group from those who are responsible for the daily operation and maintenance of the supporting networking infrastructure or who provide security services. It is crucial that the collaborative team seek out the individuals who are responsible for those disciplines at each site. Few networks are multicast-aware and most firewalls could be considered multicast-hostile. In order to get the necessary changes made to network policies, routers, security and firewall policies, significant interaction must take place between these groups before the necessary actions will be taken that to enable effective collaboration across secure communications.

Close Coordination with All Sites

It is impossible to create a collaborative community using VPN technology if you don't know where your endpoints are and close coordination with all sites is critical to success. This may seem intuitively obvious but typically management will not make these fundamental decisions until the eleventh hour. Be assured that the sites identified last will be the ones that are the most politically sensitive and require instant, seamless access.

There is no such thing as too much planning, coordination and confidence building between the security, network and collaboration deployment team(s) members and their counterparts at the individual sites. Good communications and good attitudes are required in an environment that sometimes is conducive to neither.

Personnel required at sites

Establishing good contacts at the remote sites to ensure the smooth installation and integration of the collaborative tools and supporting VPN or other network devices should begin with introductions at higher levels. Management must take the lead in establishing the requirement for the work and for providing properly briefed points of contact. Always bear in mind that whenever you will be crossing network boundaries you may also be crossing security perimeters as well and that is not something that is taken lightly. If it were, there would be no need for all of the extra work that is described here. Listed below are the types of contacts one would need in order to facilitate successful deployment of a secure distributed collaborative system. In some cases several or all of the jobs can be handled effectively by one person at the remote site. More often, the skills of several individuals will be required.

Overall site advocate

This is someone at the site who understands the goal of the collaborative architecture. This individual will help explain the goals and why they are beneficial to the site management. He can help identify the technical points of contacts and may be useful in tracking them down when phone calls and e-mails are not producing satisfactory responses.

Network knowledgeable contact

With the help of the site advocate identify the local networking guru. He or she can make the subsequent planning and deployment easy or impossible. This person will need to understand what's going on the (his/her) network. Be sensitive to local concerns about weaknesses in the infrastructure and about the nature of the systems being proposed. A joint effort can result in an effective deployment that has little or no impact on the site's networks systems or mission.

Security contact

This may also be the network knowledgeable contact. If it is, your life is somewhat simplified in that you should only have to explain things once. Additionally, if security is just another duty as assigned to the alpha network geek, then that person has already had to make myriad decisions which weigh operational necessity against security risks engendered by adding new services or devices on the network. Should the security contact prove to be another person entirely, especially if he or she is in a different organization than the network contact, the situation could become somewhat more involved.

You need to enlist the help of the security contact to make any necessary changes to the site security policy or obtain a waiver for the installation of your tools and devices. Any supporting documentation you can provide them (don't overlook this section of this report) that helps explain what it is you are trying to accomplish and the steps you are taking to mitigate the attendant security risks will help to speed your course. Security people are, by nature, risk averse. They will accept certain risks once they are sure of three things: they understand the magnitude of the vulnerabilities and attendant risks, they believe that there are sufficient countermeasures to offset the risks, and that there is an operational necessity for engendering said risks in the first place. The most important thing you can do when dealing with security organizations is to make it clear that you understand their legitimate need to ensure the safety and security of their sites networked assets.

Issues and Hurdles

Aside from the technical and security issues described above, there are almost always another set of issues that, while not technical in nature can work against the deployment of a distributed collaborative architecture.

Scheduling and Availability of Resources

There is never enough time. Management wants it right now; the users want it yesterday. When dealing with remote sites, these everyday problems are compounded. The sites have their own projects that require their attention first. This is why getting a site advocate as described above is so crucial. It is critical that your task gets in the queue and stays there. Also, by having insight into the demands being placed on them by their management, you have good information to provide to your management should you need top-level intervention.

Political and Provincial

While your management or organization may understand the prospective gains in efficiency to be realized from the adoption of collaborative tools, their enthusiasm may not be universally shared. If all of the sites are part of the same organization your task is somewhat easier. If, on the other hand, you are crossing organizational as well as geographical boundaries, the job is complicated n times. Again, identify the sites. Have contacts identified at those sites. Start the phone calls and e-mails.

If your management thinks that a distributed collaborative architecture is the way to go, but this view is not shared at the other ends, your management needs to know immediately so that these issues could be resolved as quickly as possible. Again, collaboration is the key to successful collaboration.

5.3.6 Summary

This section has illustrated one way of securing a distributed collaborative system. The VPN system described here has been successfully deployed twice. Both times it was successful in preventing direct attacks from breaching the firewalls protecting the enterprise network. Where there were remote vulnerabilities exploited during the first year, they were corrected and therefore not available for exploitation during the second.

One should not draw the conclusion that the method described above is the only means by which a distributed collaborative architecture can be securely implemented. There are many other possibilities. The VPN implementation that was chosen for EFX and JEFX addressed concerns specific to those experiments, some of which were not related to multicast problems. Most of the individuals involved in the three disciplines discussed here, collaboration, networking and security, feel that this type of approach is only an interim solution. There are current efforts on a number of fronts to add security to the collaborative applications themselves, the multicast protocols that carry the traffic and the firewalls and other network security devices that separate the different systems.

VPN technology does not address all collaborative security concerns

VPN technology is not a panacea. The next several paragraphs discuss some of the security concerns that this approach does not address.

- The VPN approach is primarily focused on allowing communication through a firewall. There were several applications, of which collaboration was one, that could not operate over the EFX/JEFX WAN because of network security policy prohibitions. While the addition of the VPN allowed us to permit prohibited traffic to pass through the firewall to specifically designated sites, since it was multicast unaware, it required the addition of even more hardware and software to allow the collaboration tools to work.

- As implemented, VPNs do not provide authentication at the application level. The VPN provided a rudimentary form of identification authentication for traffic originating at remote sites. This functionality was provided indirectly through the use of encryption. If a packet arrived from a remote site that was not protocol 50 (IPSEC), it was blocked by the firewall. If the packet from the remote address was protocol 50, it was passed through the firewall to the VPN device. The VPN device looked at the remote address and selected the appropriate key to attempt decryption. If the decryption was unsuccessful, the packet was dropped as it was either mangled in transmission or encrypted with the wrong key, a strong indicator that the packet did not originate from the correct source. If the packet decrypted correctly, there was a very high likelihood that the packet came from the correct source.

- The approach described in this section also does nothing to protect data transmitted across the network behind the firewall. There are many security implications with the use of multicast that are beyond the scope of this section. It should be kept in mind that from a security purist's standpoint, collaboration through the use of multicast is contrary to classical security objectives.

5.4 Observed Technical Difficulties

The Integrated Collaborative Operations Team encountered the following surprise problems. Each problem is described and in cases where a solution was found it is also presented. In cases where the CVW development community might be able to provide help for the future they have been advised.

- DNS response problem: During the first CVW test in Spiral 3 we encountered serious problems when a number of folks tried to log in at the same time. They were delayed by as much as 10 minutes. We traced the problem to the reverse DNS lookup that the CVW server performs so as to log each connection using the client machine's host name rather that its IP address. The problem was that the JEFX DNS server was provided by another initiative and some initiatives' hosts had not been registered. As a result the CVW server waited until the DNS query timed out before continuing. One delayed lookup would hold up all the logins behind it. It was easy to disable DNS lookup on the CVW server machine. The capability was not needed for any other purpose and by turning it off the CVW server looked only in its own host file and failing to find the client's host name proceeded to use its IP address in the log without further delay. Multiple logins were supported easily after this problem was identified and the corrective measures were implemented.

- Startup with incorrect shell: UNIX operating systems limit the number of simultaneous connections allowed to a single process. In CVW this has the effect of limiting the number of users who can be connected to the server at any one time. This parameter is settable however the command and arguments differ depending on which UNIX shell tool is being used to issue the command. What is not so obvious is that it doesn't matter which shell tool is used to launch the CVW server startup script, instead it matters which shell tool is the default for the user named "cvw", the imaginary UNIX user who owns the CVW server directory and processes. Due to this mix-up we ran into the default process barrier when we thought we were resetting it. Setting the CVW user's default shell to that which matched the command being used in the startup script fixed the problem.

- Audio on PCs and NTs: Various audio problems were encountered with the Windows and Windows NT client machines. This problem is still being investigated and is believed to be caused by incompatibilities between the audio device drivers on particular workstations and vat, the audio tool used with CVW. Further complicating the picture is the number of different audio hardware implementations being offered and the number of drivers each supports (at least one for Windows and another for Windows NT). Generally we were able to get the audio to work. However we were not able to correct or find a workaround for the fact that on a few machines the audio would lock up after a number of minutes of use (listening for a long time seemed to have the most dire consequences), and would sometimes on some machines go so far as to lock up the whole machine. Again, this problem remains unresolved. One possible solution might appear in the form of a new version of the Visual Audio Tool.

- Audio on the network in general: We encountered multicast networking difficulties that diminished (got better) as execution continued. In addition audio breakup was noticed at certain times and on particular machines. Generally the Windows and Windows NT laptops were most prone to this problem. We changed the default codex (compression algorithm) from GSM (very compressed) to PCM (slightly compressed) on those machines and were able to improve audio quality considerably. By reducing the processing these machines had to do both to compress the audio it sent and to decompress the audio it received, we enabled them to keep up with the audio processing load and not drop chunks of audio because they couldn't be processed in time to be useful. Often, the larger number of less compressed audio packets required to convey an audio message meant that any lost packets had a much smaller negative impact on the intelligibility of the whole message.

- The Document Server failed on several occasions. The developers believe that the problem is traceable to known memory leaks in the version of the Java Runtime Environment (JRE) used with the JEFX 99 version of the Document Server. Later versions of the Document Server use a newer JRE. With later version of CVW the Document Server is completely rebuilt using a database that replacing the index file that tended to get corrupted shortly before the Document Server failed. In addition the new server will have a mechanism for authenticating transactions and encryption to protect data being exchanged between the server and clients. The new server code is also better able to take advantage of multiple servers and because each transaction is committed to the database on the fly there is no longer a need to periodically write back the index file (see wide spikes in doc server perfmeter images in Appendix B).

Section 6

Technical Support

The CVW technical support plan, created after Spiral 3, identified the need for staff at each of the major JEFX 99 locations (Langley, Hurlburt, and Nellis AFBs). Langley and Hurlburt were supplied with the largest staffs due to the large concentrations of users and the presence of the primary CVW server (at Langley) and backup servers (at Hurlburt and Langley). Staffing for the technical support component of the Integrated Collaborative Operations Team was drawn from Communication Technology Exchange (CTX); Paragon Dynamics, Incorporated (PDI); Command and Control Product Lines (CCPL); and MITRE. The composition of the team represented a significant level of technology transfer from MITRE to commercial contractors.

Technical support was provided in three areas: system administration, integration, and help desk.

6.1 System Administration

The team carried out a range of system administration support activities to support EFX 98. These included:

- Setting up and maintaining primary and backup servers
- Creating and maintaining over 1650 user accounts
- Setting up and maintaining a web server to host documentation and web-imported briefings
- Preparation/conversion of briefing materials for Combined Force Air Component Commander (CFACC) briefings

Initially, CVW had only limited employment in JEFX 99 Spiral 3, utilizing the same virtual building used in EFX 98 and generic "test" accounts. The team configured a new server for JEFX 99 execution with a new virtual building created in accordance with information supplied by the C2TIG. Subsequent additions to the building (three new floors and several name changes) were incorporated over the course of the experiment. Server backup procedures were followed throughout the experiment. Transfer of backup files via FTP each evening allowed the backup servers to be rebuilt the next morning using the most up-to-date information. After about a week, the volume of information had grown to such an extent that the team had to add a new disk partition to the backup server machine. In addition, earlier backup copies were moved to tape due to concerns over increased disk usage.

To facilitate the creation of operator accounts, the in-processing centers were provided with copies of CVW account request forms and instructions for their completion. Arrangements were also made to take each person's picture. When completed, a system administrator used the information and picture to create the user's account. User pictures were usually taken at the in-processing centers and supplied to the team as GIF or JPG files. In addition, a video station was set up at the OSC where individuals could have their pictures taken and associated with their accounts. Overall, the account creation and associated maintenance for over 1650 user accounts consumed a greater portion of time than originally expected (approximately three persons during the month of August). This was greater than our experience in EFX 98, partly because in EFX 98 much of the user information and many of the pictures were reused from the earlier spirals.

Another significant administrative activity was supporting preparations for CFACC briefings. The CVW web servers were used to host the briefings once they were saved into HTML from PowerPoint. Because of the late start and because JEFX 99 did not provide adequate experiment-wide web support (there was no dedicated JEFX webmaster or full function web site), the CFACC briefings had to be deliberately installed on the CVW web servers with the URL objects placed in the appropriate CVW rooms. Had users been able to "publish" on the JEFX web, the team would not have been involved in this activity. This, and related deficiencies, can be corrected if a comprehensive approach is adopted for planning and rolling out distributed operations support services in future JEFXs, as recommended in Section 8.2.

6.2 Integration

CVW integration for JEFX 99 involved the development, installation, and testing of shell scripts which allowed operators to open PowerPoint, Excel, and Word files from within CVW clients installed on TBMCS (Unix) Workstations. This software initiated sessions on Office Automation (OA) servers running WinCenter. Most of the integration work was conducted at Langley during Spiral 3 and completed just prior to the experiment execution. These scripts were also provided to Hurlburt and Vandenburg. Problems identified during testing at Hurlburt were caused by differences in the TBMCS OA server configurations. In particular, the OA servers at Hurlburt were configured to support automatic load balancing, whereas, the servers at Langley were not. Fortunately, integration software developed during EFX 98 to support load balancing had been retained and was successfully utilized.

6.3 Help Desk

The team provided onsite user support during JEFX 99 experiment execution. The team interacted closely with CAOC personnel to assist them with using collaborative technology to conduct distributed CAOC operations. This user support included consultation concerning which collaborative features would be most useful in facilitating distributed CAOC processes of interest to the particular user as well as answering CVW interface/mechanics questions. During the course of providing user consultation, we also gained insight into how the operators were using collaborative technology to experiment with distributed CAOC processes. These insights are contained in Section 2.

Section 7

Impact of Collaborative Technology on Distributed AOC Operations

7.1 Historical Notes

The notion of distributed Aerospace Operations Center (AOC) operations has been around for several years. During ESC's Ft. Franklin V in 1996, and later in Joint Warfare Interoperability Demonstration (JWID) 97 (JW-068) a collaborative environment (CVW was used in both cases) was used as the basis for concept experimentation. While these earlier experiments were successful proofs of concept with small deployments (i.e., 5 sites, with an airborne element, and 20–30 operators), the merits of the concept itself were still being debated and the technical ability to support larger operations was unproven.

As part of ESC's Ft. Franklin V in 1996, CVW was deployed as a demonstration. In part it was used to extend the Ft. Franklin experience to a larger Washington DC area audience by providing a structured view of Ft. Franklin in the demonstration center at the Theater Battle Arena in the Pentagon. During one of the presentations, then Air Force Deputy Chief of Staff, Plans and Operations, Gen. Jumper, stated that deployment of such an environment would support his concept for a minimal forward deployment of AOC resources with uninterrupted commander situation awareness and control during periods of air travel, particularly during deployment to the forward location. A small group of ESC staffers understood the General's vision and set out to demonstrate the capability using JWID 97 as the vehicle. Experiment JW-068 in JWID 97 was the first application of a virtual environment to enable distributed command and control including full airborne capabilities aboard the Speckled Trout. Experiment JW-068 demonstrated the ability of a collaborative tool to support widely distributed users however the experiences of Blue Flag 98-1 sensitized the team to the importance of understanding the users' environment, CONOPS development, deployment planning, dedicated CT equipment, proliferation of clients to most workstations and top level involvement in the use of the collaborative environment.

As part of their Blue Flag 98-1 exercise the Twelth Air Force experimented with the concept of a distributed AOC. This AOC was divided between two operating locations. The chief of the Strategy Division, the Combat Operations Division and certain key support staff members were deployed to the forward base along with the Joint Forces Air Component Commander (JFACC). The rest of the AOC (e.g., Combat Plans, Intelligence Division, Combat Support, etc.) remained at their home base. The exercise was conducted as if all of the parties were collocated however the collaborative tool was deployed only in a token role and was never seriously used. No changes were made to the operations tempo or the battle rhythm. Some general support for collaboration was provided. In addition to the usual mission applications (i.e., CTAPS 5.1), there were secure telephones scattered throughout both location and a dedicated VTC system for the

Strategy Cell. The SCIF PCs also had access to Windows-based file servers located at the home base.

The exercise was conducted as if all components of the AOC were collocated at the forward base. In addition to the normal stresses of Blue Flags, the staff had to contend (for the first time) with coordinating their planning activities across geographical and temporal boundaries with little automated support. Being industrious, users made do with what they had available. The VTC located in the Strategy Cell provided a mechanism for other teams to coordinate their activities and maintain team awareness. Since it was the only VTC available for general use (the JFACC had a separate dedicated VTC for his use), priority went to the Chief of Strategy and then to others as time permitted.

Secure telephones (predominantly KY-68s) provided secure point-to-point audio coordination but required phone books which became harder to find as the exercise wound down to its final days. Some STU-IIIs were available but hard to find and none of them were configured for conference calls. Multi-party secure conversations were restricted to the VTC and this required all of the parties to travel to the VTC location. In almost all of the cells of the AOC, daily status briefings were created and presented to the JFACC using the VTC.

Secure file transfer was available to cells like the strategy cell, which had personnel with SCIF access. They were able to assemble the JFACC’s PowerPoint briefing from parts that were built in both the forward and rear locations and transferred between the two locations on the SCIF's PC network. Other cells that were not so fortunate would coordinate their activities by VTC or secure phone and then build the briefing in one of the two locations.

Secure facsimile provided a way to transfer, in hardcopy, draft material to be included in a briefing or completed material that needed final coordination and review prior to the briefing. Because of the time difference between forward and rear, there was not much time to coordinate activities. Collecting and collating all of the individual briefings from all of the cells into the daily brief also consumed an inordinate amount of time. Despite these adversities, the AOC was able to do its job and the exercise was successful. The toll on the personnel was obvious. One of the major complaints at both the forward and rear was that participants felt isolated from important information about the situation.

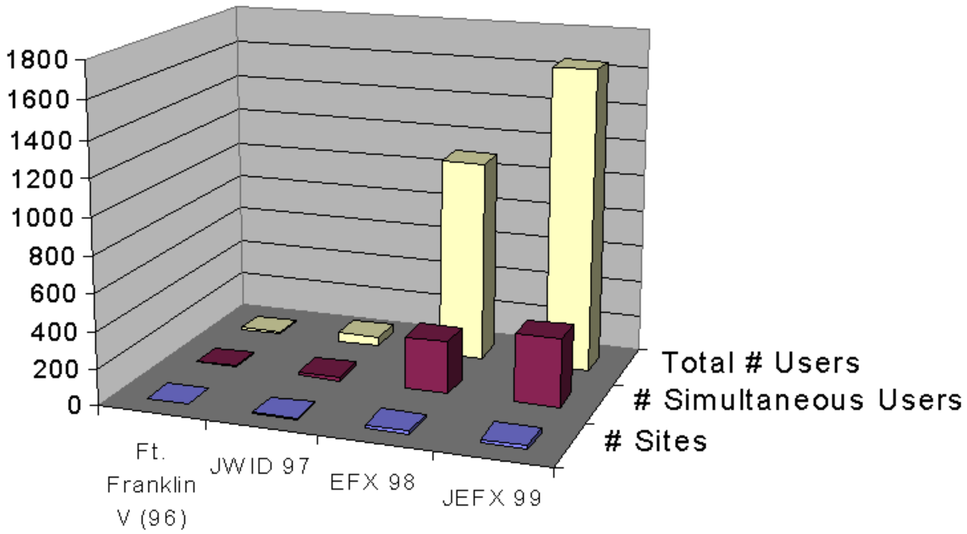
While a collaborative tool (CVW) was available to support the Strategy Cell, it was not used, and therefore had no impact. There were several reasons for this lack of use including the late introduction of CVW into the exercise planning process, a lack of user training, concern about reliance on unknown technology performing a critical role in a graded exercise, and the lack of a client for the Windows platform. For EFX 98 this experience resulted in emphasis being placed on involvement throughout the planning and spiral processes, on general use of the tool across all AOC functions, on supporting both Unix and Windows platforms, on understanding the users’ functions and developing a CONOPS and training plan tailored for the AOC operators, on providing a reliable tool supported by experienced people so that users would be confident about relying on it, and on having exclusive control of the workstations that would host the collaborative servers.

EFX 98 was the first large-scale distributed AOC experiment. The goal was to deploy a segment of the AOC to the forward location while retaining the majority of the organization in one major and several smaller rear (CONUS) locations and enable those distributed parties to function as if they were all collocated. The experiment encompassed almost every operator and support workstation position at 15 sites, including two airborne elements, JFACC en-route and EOC en-route. Over 400 operators were trained in the use of the CVW. The CVW system grew to more than 1000 user accounts and supported over 280 simultaneously connected users. For more details, please refer to MITRE MTR-99B0000004 "Collaborative Virtual Workspace (CVW) Employment in EFX 98: Observations and Lessons Learned," published January 1999.

Operators interviewed following Blue Flag 98-1 and EFX were strong advocates for the incorporation of a collaborative environment into the air command and control software suite. The digression to Blue Flag 98-1 was important because it marked the Air Force entry into distributed operations for organizations as large as an AOC, and it also marked the first opportunity to benchmark operations that could have been supported by a collaborative environment.

JEFX 99 confirmed the importance of an AOC-wide collaborative environment and demonstrated the feasibility for deploying a distributed AOC. In less than two years, the concept of an AOC has evolved from huge difficult to deploy monolith to small mobile core supported by the best talent at fixed CONUS facilities. The introduction of collaborative technology hasn't changed users' desires to be collocated, but it has provided them with a tool set that makes distributed operations practical and relatively painless.

The collaborative experimentation in EFX 98 was an overwhelming success. Much of the time during the spirals of JEFX 99 was spent in beta testing a new collaborative tool, while little effort was invested in improving processes and procedures based on lessons learned from EFX 98. While the collaboration aspect of JEFX 99 was a success and users continued to learn and innovate, the opportunity to take the distributed work environment to a new level of sophistication was lost. Figure 7.1 shows collaboration scalability experiences through four years of experimentation with CVW from Ft. Franklin V in 96, JWID 97 (JW-068), EFX 98 to JEFX 99.



	Ft. Franklin V (96)	JWID 97	EFX 98	JEFX 99
🟦 # Sites	2	5	15	24
🟥 # Simultaneous Users	5	20	280	372
🟨 Total # Users	10	50	1100	1650

Figure 7.1 Number of Users and Sites for CVW Deployments in Exercises and Experiments from 1996-1999

7.2 Use of the Virtual AOC Environment in JEFX 99

7.2.1 The Concept of Virtual Collocation

As has been shown in the preceding sections distributed or "split" AOC operations have evolved over the last two years at JWID and EFX based on collaborative virtual environments. To link various "forward" with "rear" and "en-route" elements required the deployment of a single collaborative space, one that made all participants feel that they were collocated with their fellow team members regardless of physical location. These environments encompassed the entire experiment space to create ubiquitous collaborations for all experiment participants regardless of where they were located physically or what type of workstation they were using. This capability allowed experimentation with the concept of a "minimum forward footprint" AOC comprised of the least number of operators, least amount of equipment and smallest support requirement in theater to execute the mission. Strategies have been tested to understand what functions and, therefore, what personnel need to be placed "forward," how much support can be provided from the "rear," and how long the "forward" element can operate autonomously when communications were cut between "forward" and "rear."

For JEFX 99, participants from 24 sites across the country, whether they were at fixed locations or afloat (USS Coronado) or airborne (EOC en-route), accessed one another on any user workstation at any time through terrestrial and satellite communications links, synchronously and asynchronously, using a single persistent virtual environment. Over 1650 users in total for JEFX 99 had access to the environment. As they were in-processed for the experiment, based on their function in JEFX, they were each mapped to specific virtual floor and room as their home base, regardless of their physically location. As many as 372 operators from a dozen or more physical locations used the environment simultaneously to participate in several dozen concurrent workgroups and meetings.

Virtual collocation enabled virtual teaming. Teams of teams were quickly formed from individuals at diverse geographic locations, in different organizations and from different functional areas, each of whom contributed specific skills and data to the mission of their team.

7.2.2 Benefits of a Persistent Environment

A persistent virtual environment is one that does not disappear or degrade as users log in and out. It remains available on line and continues to exist in the state left by the last user. The state of virtual rooms change as new documents are deposited or removed, the whiteboards record who has changed what and room recorders can keep time stamped records of who comes and goes and what they type in the room. The persistence of room contents give each virtual space a growing context as users share documents, build briefings, conduct meetings, or plan activities using shared whiteboards. Because the system manages the rooms, the people and documents, a particular operator or document can be found quickly and easily by any operator. This almost immediate accessibility to one another and to information, made the virtual environment very suited to supporting any high intensity activity such as military command and control, crisis management or disaster response operations.

Since email capability was not available in JEFX 99 when IRIS was down, many of the users were routing USMTF messages such as TACREPs and others to team members in the room or sent through cut-and-paste into a "page" command. Many operators did not have email accounts and therefore relied entirely on the collaborative environment for messaging support.

While access control was available for locking rooms and controlling documents, most rooms and documents were open for viewing by all participants. Many customized forms were created (see Section 2 and Appendix F), often providing an organized and accountable way to track information and requests. Many rooms had "in boxes" for form submission. Consumers had access to the status of their requests and could seek out providers for consultation.

Since the teams were sharing information within their rooms, more current information was posted in those rooms. Since most of the rooms were functionally oriented and open to all for browsing, other teams would visit looking for pertinent information. This was particularly applicable to the SOF team that would routinely visit various rooms and gather information pertinent to their missions. This type of information sharing bypassed the traditional "go through the chain" and take pot luck getting what you wanted and increased many teams' timeliness and responsiveness.

7.2.3 Improved AOC-wide Awareness of Operations

Collective awareness of the state of the AOC-wide operations is a very critical concern for operators. The virtual environment provides many opportunities of improving situation awareness. Openness of the rooms for browsing mentioned earlier certainly helps but the traditional CFACC daily status briefing(s) normally reserved for his staff, Cell Chiefs, briefers and invited guests can now be opened for all to hear. In fact, during JEFX, almost half of the operators attended these daily briefings from the CFACC Balcony (see Figure F.8, Appendix F) and thus achieved an unprecedented level of understanding that would be difficult to accomplish otherwise. For those who missed it, the briefing was saved in the "Briefing Room" and accessible to anyone at any time. In the future, this meeting might be recorded in audio and available for replay by anyone whenever convenient.

Because the CFACC and his staff had access to the virtual environment, if he so chose to consult with any one he could easily navigate to the appropriate rooms or "page" that someone/group to provide guidance or assess the situation. In fact, during JWID 97 and EFX 98, he and his staff had that ability wherever he was located, including while he was airborne on the Speckled Trout.

While operators gain unprecedented awareness of the battlespace, they are faced with other awareness-related challenges. There are actually two different but complementary problems: (1) competition for attention between virtual environments and real life and (2) competition for attention between multiple obligations in the virtual environment.

1. In the first case, virtual environments extend the user's ability to have awareness of and contribute to non-local events, but the user leaves his workstation, he loses the benefits of the virtual environment, and correspondingly the inhabitants of the virtual environment lose the benefit of access to that user.

2. The second case is similar to the first, but instead of the user leaving the workstation, his attention is spread among the several teams he supports and must choose how to divide his time to satisfy their competing needs. While the tool has "proxy" capabilities that allows each user to have two instances of himself in the workspace to simultaneously monitor/participate in two workgroups, this capability was not trained or generally used in either EFX 98 or JEFX 99.

7.2.4 Process Impact

The potential for collaborative technologies goes beyond the mere functional capability for distributed team members to work together using, text chat, audio, whiteboarding and document exchange, it is about process change and business reengineering. It is about taking advantage of technology to speed AOC deployment and improve AOC operations.

As indicated in many of the diagrams in Section 2 and Appendix F, operators captured their work processes as checklists on whiteboards in some of the rooms. This brings the team of teams together with a common understanding of the sequence of tasks to be performed and a definition of who needs to work with whom. As tasks were completed and the checklist items signed off, the latest status was immediately available for all to see.

Throughout the experiment, operators were very innovative in taking advantage of the virtual environment. As described in Section 2, the Weather Group was extremely entrepreneurial. Instead of having other users come to visit them, they visited other team rooms and, where appropriate, they posted links to their weather information customized to the function of the rooms. In addition, they updated that information at regular intervals so that the latest information was always available. They also manned a distributed help desk, so that when an urgent request came in for a SAR mission, they were ready to respond in a timely manner. This example illustrates how well one information provider group adapted to the virtual space and capitalized on the technology to meet the needs of their consumers. A virtual environment can dramatically change the relationship between information providers and consumers. Virtual collocation can help providers understand the specific needs of their customers and provide information tailored to each customer's needs without overwhelming any of them with extraneous information. In fact, one might argue that in the future many providers could be most effective working at their home facilities, supporting multiple missions, with all their prime resources at their fingertips.

7.2.5 Cultural Issues

Cultural barriers including resistance to change are often the most difficult to overcome when traditional work patterns and tools are suddenly displaced. Despite the paradigm shift the majority of operators at JEFX 99 took to the virtual environment very enthusiastically. This may be because many of them were exposed to the collaborative environment in EFX 98 and liked it. Nonetheless, there were the occasional frustrations because the tool did not do what they wished it would do and with the network that did not deliver images, slides and audio data as smoothly and quickly as desired.

To truly use a virtual environment in a real operational setting, it is critical that operators establish rapport and build mutual trust with distributed team members, many of whom they have never met physically but on whom they are now depending to complete their missions successfully.

Conduct of operations at JEFX 99 was more ad hoc and informal than real world operations. Cross-organizational teams were less hierarchical because of virtual teaming, appeared more autonomous and more participatory. If this portends the way of the future, then the current, more traditional hierarchical organization may need to change to accommodate a wider, more level organization.

7.3 System Impact

7.3.1 Secure Communications/Network Infrastructure

As demonstrated in EFX 98 and again in JEFX 99, the network infrastructure plays a critical role in the effectiveness of collaborative tools; in particular, a persistent environment that demands continuous connectivity, large file transfers, a robust multicast architecture, and sufficient capacity to accommodate both collaboration and the use of mission applications.

Audio was used very heavily throughout the experiment, often to the exclusion of telephones. However, various problems were reported on the use of VAT, mostly with PC and NT platforms. These problems were a source of frustration for both technical support personnel and users alike. It is a complex issue which points to the combination of multicast issues, incompatibilities between audio device drivers and particular workstations as well as the large number of differing audio hardware implementations that resulted in problems ranging from audio breakup to whole workstation lockup. Many hours of patient “tweaking” were performed but no single, clear solution in likely to be found. More experimentation and testing is required.

7.3.2 Collaborative Environment as the “Glue” for C2 Systems

TBMCS is an umbrella name for numerous C2 mission applications that supports the warfighter. Users trained on specific functions operate TBMCS workstations equipped with specific applications. Sharing results from their application with others was often performed using the collaborative tool. Screenshots of results were often pasted onto whiteboards and shared with team members in the same room or carried to other rooms. Very notably, the Common Operating Picture (COP) generated from the application SAA was often shared in this manner. In many ways, the collaborative environment gave users the ability to bring together disparate applications and make their output accessible to all.

As was discussed in Section 2, in bringing about the integrated use of the mission applications, the collaborative environment increased in context and information value for the distributed operators. This was much more evident in JEFX 99 where TBMCS was more functional and robust than it was in EFX 98. Because the virtual environment was stable, performed reasonably well and was scaled to the entire experiment space, operators were able to concentrate on conducting their experiments, improving their processes and executing their missions.

7.3.3 Characteristic Usage of the Environment

Text Chat

While text chat provides several benefits (e.g., unobtrusive, easy to obtain record of interactions, degraded mode conversation when audio fails), it was not heavily used in JEFX 99. Most operators preferred to use the audio capability as it was more convenient and best fit the tempo of most interactions. Users have different comfort levels with typing as a means of carrying on a conversation and the unevenness of participant typing skills lead to latency problems. If a real world interruption takes away one of the participants in a text conversation, the other members of the conversation must just wait, or may improperly misinterpret the latency as intentional. Multiple capabilities are available for indicating absence or delayed response but using these capabilities in the heat of a rapid exchange or in the face of an interruption are advanced skills acquired with experience and regular use of a tool.

Point-to-Point and Multicast Audio

Secure point-to-point and multicast audio was the most used capability in this environment. While secure telephones were still available and used, multicast audio quickly replaced the telephone as primary audio communication device. In fact, when the real life hurricane Dennis hit Langley during JEFX 99 and brought down the phone switch, there was little disturbance to the ops tempo because of the availability of multicast audio. Similarly, in EFX 98 a two hour telephone service outage during the middle of the day in the OSC was never noticed by the operators.

Multicast Video

Multicast video was rarely used as part of the mainstream exercise. The users did not seem to miss or need this capability. Its two greatest enablers, presence detection and rudimentary identification (the person on the other end of a collaborative session is really who you think it is) are easily provided through other less bandwidth intensive solutions.

Shared Whiteboard

Shared whiteboards were widely used, often for mission planning discussions employing map backgrounds. Additionally, operators thought of many other innovative ways to use them for sharing information. A couple of examples were described in Section 2. Users of different TBMCS applications used the whiteboard to share screenshots with one another, e.g., the COP generated by SAA. Also, whiteboards were used extensively to document and track workflow, i.e., checklists of joint tasks that also acted as status reports.

Presence Awareness

Users are adaptive and, given time and the opportunity, they will find methods to overcome limitations of the system. The "online users" window is a good example. While it is useful for individuals to keep it open to see when users are available in the virtual environment, the automatic update feature does consume bandwidth, and at locations where bandwidth is small, users are cautioned with respect to judicious use. To overcome this potential issue, users built duty rosters (which they updated when their schedules changed) and posted these rosters in their virtual rooms where they could be easily consulted to determine who would be available when.

7.4 Collaborative Environment Deployment

Successful deployment of an extensive collaborative environment requires more preparation than most other types of technology. Sections 3, 5 and 6 refer to various tasks that were performed in support of the system deployment. This section contains an abbreviated list of issues and actions that should be addressed as part of any deployment and Appendix E, Deployment Details, provides descriptive details about each item on the list. The order of items in this list does not imply relative importance. The nature and requirements of each deployment will dictate the importance of the individual items. Likewise, collaborative tools have differences. This section assumes that certain capabilities reside in the tool and that it requires certain infrastructure support. With a few terminology substitutions, this list should be useful no matter what tool is being deployed.

7.4.1 System Engineering

Networks and Multicast

- Make friends with a local network guru!
- Learn everything you can about
  - Network topology
  - Known Bottlenecks
  - Long haul bandwidths
- Use multicast enabled routers, if possible
- Avoid mixing workstation based *mrouted* with router-based mulitcast routing

User Locations and Work Patterns

- Find out where users will reside in the network topology
  - Note concentrations of users
  - Note one/two workstation outposts
- Project who will be most active concurrently
- Distinguish modes of use: text chat, audio, document creation and exchange, web access

Predictable Failure Modes

- Server hardware failures
- Network failures
  - Long haul connections
  - Congestion
  - Multicast
  - TCP
- Information warfare attacks

Failure Response Strategies

- Backups
  - Data preservation
  - Maximum availability to maximum users
  - Concurrency vs. bandwidth constraints
  - Continuous backups
- User procedures
  - Detection and notification
  - Published procedures

Accreditation Strategy

- Document architecture
- Get copies of required paperwork
  - Assume stovepipe system
  - Complete questionnaires where appropriate
  - Don’t overdo the details
  - Don’t make claims of capabilities for systems outside the collaborative tool
  - Be accurate

Hosting Strategy

- Multiple server processes (Tool, Document, Web, other)
  - Single host
  - Separate hosts
- Disk speed and size, raids, striped raids
- CPU clock speeds and multiple units
- Memory size

The Collaboration Environment

- The collaborative tool is a piece of the collaboration environment
  - Messaging
  - Telephony
  - Document and data sharing
  - Web
  - Application and screen sharing
- Devise a cohesive whole

7.4.2 System Administration

Admin: Who, Where, How Many, or What

- Who will administer the system
  - Where are they located
  - Are all times covered
  - Will all have access to an appropriate workstation
  - Will shared workstations be enough
- How do Admins collaborate
  - With each other
  - With users

Server Configuration Issues

- Naming the server(s) and host workstations
- Multicast base addresses
- Login messages for each server
- New user email (if applicable)
- Things to be VERY careful of:
  - Keep a list in the virtual admin room
  - For example: avoid using DNS on server

User Naming Conventions

- Multiple naming opportunities
  - Login name (simple, familiar to user)
  - User name (default "pretty" name)
  - Full name (non-functional, appears in user information box and in user lists)
  - Aliases (up to the user)
  - Assumed name(allows user to "hide" User name, is easily reversed)
- Consider how names will be used

Virtual Building Floor Plan

- Floors
  - Workgroups that interact often
  - Political or organizational units (less desirable…)
- Rooms
  - Functional workgroups
  - Avoid general purpose rooms
  - Use center room for public documents, not work
  - Names and descriptions

User Account Creation

- Approval authority
- Training prerequisite
- User information collection forms
- Capturing and processing user images
- Password control and distribution
- Initial home room selection
- Use of "extra" fields

The Collaborative Tool Web Server

- Client downloads
  - client version(s)
  - configured for local use
- Building directory
- User pictures – if used (try to keep local)
- Place URLs in appropriate places in virtual rooms
- Provide publish capability for every user
- FAQ page(s) for the collaboration environment

7.4.3 Client Software Deployment

Client Software Preparations

- Download site(s) prepared and tested (if applicable)
- Configured for each location with appropriate pointers to
  - Primary server(s)
  - Backup server(s)
  - Local web server
  - Office automation applications (re. UNIX clients)

Deployment Strategies

- Media options
  - Web download
  - CD Rom
  - DII-COE segment tape
  - Disk replication
- Adding desktop icons (XWMs)
- Windows Start Menu vs.. desktop icon(s)
- Verify configuration files correctness

7.4.4 Training and User Support

Training Facilities

- Optimum 15 trainee stations or less
- A workstation for each trainee
- Workstation for teacher with projector
- Rooms in collaborative environment for training
  - Special objects in rooms
  - Exercise rooms as required
- Trainer helper

User HELP Strategies

- On-line Help
  - Include other systems (more folks to man desk)
  - Keep test items and FAQ URL in room
- Phone Help
- Asynchronous Help
  - Email
  - FAX
  - FAQ (and use HELP crew to post to FAQ)

Handling Bug Reports

- Have a procedure
- Give feedback regularly
- Many “bugs” are operator error or misunderstanding
  - Add to FAQ
  - Modify training plans
- Filter upgrade suggestions
  - Suggest workarounds

Section 8

Conclusion and Recommendations

The experience of deploying a collaborative tool in JEFX 99 underscored two fundamental themes: (1) preparation is a large and complex business involving several technical teams, and (2) the emergence of "place-based" collaborative environments offers a spectrum of opportunities for the growth and improvement of systems that support distributed work. In this paper we have highlighted many lessons learned. While preparations were greatly hampered because of the lack of time, it was gratifying to see that users were still able to discover many imaginative, innovative and effective ways to take advantage of the capabilities.

Collaboration has been identified as a critical capability for warfighters. While experiments need to continue to discover and understand future requirements for more powerful, more scaleable, more usable and more integrated approaches to collaboration, institutionalization of the currently more mature capabilities into the operational arena needs to begin now. The following recommendations have implications for both the maturation of comprehensive collaboration systems and the institutionalization of those systems in the command and control infrastructure.

The greatest obstacle we see to the successful employment of collaboration technology in future Air Force operations is that key deployment preparation requirements will be forgotten in the heat of preparing for exercises and responding to real world events. In this paper we have tried to document a cross section of the issues, experiences, procedures, lessons learned, and insights that we believe can make a difference to collaboration technology use in future experiments, exercises and engagements. In that spirit, we offer the following recommendations.

8.1 Address Inter US-Only and Coalition Collaboration

While collaboration within the Air Force and across joint operations has been the subject of experimentation in the last two EFXs, little is known about implementing collaboration between US-Only and Coalition forces. Apart from understanding the collaboration requirements, the biggest challenge lies in the technical and policy issues surrounding security. We did not address this aspect of collaboration during JEFX 99 but have been challenged to address it for JEFX 00. The program must be prepared to accept the challenge to grapple with the meaning of and expectations for collaboration between US-Only and Coalition system levels.

8.2 Expand the Distributed Work Environment Beyond a Collaborative Tool

One collaboration tool does not fit all needs and no collaboration tool delivers a full spectrum of distributed work capabilities. Supporting distributed work in an environment as rich and demanding as an AOC must incorporate several complementary tools. Today's workgroup technologies include telephony, application sharing, data and document sharing, virtual collocation and messaging. Many specific implementations cut across several categories. For example, FAX is a collaborative tool in the telephony category that actually implements a form of data/document sharing. Each year JEFX needs to expand, both in scope and depth, the capabilities that support distributed operations.

For example, in terms of scope, plans and preparations should be made to implement a comprehensive messaging system (email) among all participants in JEFX 00. The first bullet in Section 4 amounts to adding email-like capabilities to the collaborative tool. In the long run messaging can and should be a merger of email, messaging within the collaborative tool and voice messaging. Ideally this messaging would be mapped to individual pagers and cell phones for certain message priorities. Just deploying an email system is not a trivial undertaking but requires thoughtful preparation so that each initiative is accommodated, user names and passwords are ready before training begins, and the messaging infrastructure has been tested and found sufficiently robust across the projected network and initiative domains. In the long run JEFX planners should work toward comprehensive messaging as a key part of their distributed work environment.

In terms of depth, JEFX 00 should develop and implement a comprehensive plan and architecture for its intranet (JEFXweb) that addresses integration, usability and support; including web publishing capabilities, personal document transfer folders for every user and experienced webmasters to manage, update and mirror the several "local" web servers. JEFXweb should tie together the web-able elements of the various initiatives with links to each, an overall search capability and hot topic home pages with appropriate links into specific initiatives' web data. There is almost unlimited depth available in web collaboration because of the range of available data sharing capabilities, the variety of applications that make web-able data available and the opportunities to present dynamic views of specific topical data.

Application sharing offers another rich set of potential capabilities that would expand the scope of the distributed work environment in future JEFXs. In the near future web-able views of mission applications and data will provide a partial capability by enabling any number of users to view (and possibly manipulate) the same data, viewed at the same time. The weather views supplied by the Air Force Weather Agency in JEFX 99 are an early example. Whiteboards are another special case of shared applications in that a static background can be annotated collaboratively. Whiteboard usefulness in this context is proportional to the ease with which the background image or text can be imported.

8.3 Expand Collaborative CONOPS Development and Training

EFX 98 and JEFX 99 have demonstrated the value and importance of developing CONOPS in preparation for collaborative tool training. Now that approach must be expanded to include the available range of distributed work capabilities. As in previous years the CONOPS would be used in the distributed work capabilities training sessions to help users understand how they might use the various tools in support of routine operations and in response to emergencies.

The object is not to create cookie cutter solutions but to promote creativity in approaching work processes by taking advantage of the range of tools and capabilities. The EFX spirals can play a valuable role in this process because they provide the opportunities to practice teaching the CONOPS merged with tool skills for the current suite of capabilities. Evaluation data and collected user feedback from these spirals are essential for iteration and refinement of the CONOPS and the course of instruction before the actual experiment.

8.4 Institutionalize Collaboration

Collaboration capabilities and processes cannot be adequately learned and used by personnel who only work with those capabilities a handful of times during their careers. Collaboration (teaming) skills are included in every professional military training program. Likewise, every participant in the AOC both operator and support staff should be proficient with the tools that enable virtual teaming. Like teaming skills, tool skills need to be practiced. If everyone is always a novice we cannot expect to realize the benefits and advantages we could otherwise expect. Unlike mission application skills that are for the few, everyone needs a reasonable level of proficiency with the tools of distributed work, because it is through those skills that teaming goals are met in the distributed AOC.

In addition to tool skills, institutionalization should focus on developing the skills of process improvement. The observations from JEFX 99 indicate that these skills are already present and need only be applied on a more general basis to the opportunities offered by collaboration capabilities. It is time for these capabilities, along with evolving CONOPS, proper training and support, to migrate into the operational mainstream both in-garrison and in the suites of equipment and software to be deployed for exercises (Blue Flag, etc.) and for real world situation responses.

8.5 Instrument the Virtual AOC Environment to Improve Process Development

As noted in Section 2, many of the teams created checklists and procedures that defined processes for accomplishing a mission or completing a product. The example given of the Weather Group activities (in Section 2) was one of many instances that illustrate how different teams used the collaborative tool. Too many processes were undocumented and therefore are unknown. In order to understand and improve these work processes, it would be extremely worthwhile to instrument a collaborative tool to provide a basis for capturing and measuring improvements in the processes, practices and procedures of the AOC.

Instrumentation means that all public conversations, in text chat or audio, and actions such as whiteboarding, file creation and movement, text chat, audio conversations, etc., would be recorded and time tagged for later replay and analysis. This would be very helpful, for instance, when we want to understand the time-critical targeting process, or the MAAP process, as played out in a collaborative environment. By having an accurate timeline-based record that includes people, interactions, data accesses, systems used, etc., we could reconstruct, analyze and compare processes. Different instrumented experiments can then be designed to measure the effectiveness, productivity, accuracy, timeliness, resourcing, etc., of various candidate processes. Also, when coupled with network usage data, we would be able to better understand and more accurately estimate the infrastructure requirements for collaborative operations.

We missed an opportunity for JEFX 99 because there was insufficient time to set up the instrumentation system, but we should select at least one critical thread in JEFX 00 to instrument, if only to have a record and better understand of how certain supporting processes were derived and executed.

8.6 Prepare for the Expected

Because of operator and support dependence on collaborative tools that we saw in EFX 98 and JEFX 99 it is essential that these systems be protected at least from the threats and contingencies we can anticipate. This is no small task because proper preparation requires planning and takes time. As we noted in Section 5 the data backup plan had a significant impact on the system architecture. The finished system architecture must address both hardware and network failure modes. Not only must data be protected but some level of user capability should be immediately available following hardware failures or information warfare attacks.

Conducting “normal” operations with degraded capabilities is a related class of predictable circumstances for which we must prepare. Historically we imposed restrictions on the use of telephones (MINIMIZE) when routine use threatened to overwhelm the available service. Likewise we need to devise MINIMIZE-like guidelines for the use of collaborative capabilities at different degrees of service overload, degradation or dysfunction. These procedures must begin with the accurate detection of failures and overloads and be followed by rapid user notification, problem source definition and correction. Mapped to each level of restriction must be specific practices that users should employ when that level is imposed. In this case “users” refers to everyone who uses the collaborative environment whether in operations or support.

When collaborative capabilities go to war we must have had some documented experience with planning, deploying and testing those systems’ and their users’ ability to respond to and recover from predictable failures. If we do that much we’ll cover some of the unpredicted hurdles as well. Future JEFXs must stress the importance of preparation for predictable problems.

8.7 Importance of Bandwidth Management and TCP Stack Timing

Bandwidth management technology and TCP tuned for SATCOM latency would have resulted in: (1) improved utilization of the available bandwidth, (2) an effective increase in bandwidth available to critical applications, and (3) improved performance of certain operations utilizing reliable TCP connection services on the SATCOM circuits.

The use of bandwidth management would have enabled dynamic allocation of the WAN bandwidth during those times when there was a reduction in bandwidth due to circuit outages or when the demand exceeded the available bandwidth.

Implementing a TCP stack tuned for SATCOM latencies would have increased the effective bandwidth available to applications using reliable TCP file transfer services such as CVW Document Server replication between the OSC and CAOC. This capability would be particularly valuable in future system architectures that should replace daily backups with continuous replication and mirroring.

8.8 Need for Intelligent Replication Services

The CVW Server, CVW Document Server, and CVW Web Server all share the need to maintain concurrency with peer and backup servers. An intelligent replication service would be ideal for this purpose, replicating those data entities that have changed since the last replication cycle. This recommendation would apply to any system that copies or backs up data across the tactical WAN circuits.

Replication has a second very important benefit. It enables the use of identical local data stores for each major user community. This means that documents and images could be saved locally to the owner, replicated to several other servers and made available to other users on the server nearest their workstation. This would be invisible to the user but would greatly reduce traffic on the long haul communications since a file would traverse those lines only once.

8.9 Implement Easy-to-Use Cross-Platform Office Automation

Office applications are fundamental capabilities in an AOC. The applications of choice are those found in the Microsoft Office suite. In JEFX 00 we will continue to have some substantial percentage of users on UNIX workstations for which there are no Microsoft Office applications. In both EFX 98 and JEFX 99 we used one initiative's solution, WinCenter, that runs Office applications on dedicated NT workstations and displays them on the users' UNIX workstations. This solution is slow, hard to integrate, network bandwidth intensive and limited by the available number of user licenses. It is operable only in the network local to the NT server so the small sites have no capability.

In JEFX 99 much of the Office work was done on Windows/NT workstations mainly because users could not be bothered with the problems associated with WinCenter. There is a solution in the form of an office suite that is available for both Windows/NT and UNIX operating systems. Star Office is almost 100% file compatible with Microsoft Office, it runs in native mode on the subject operating systems thus providing good performance and it's look and feel is so similar to Microsoft Office that the two can be used interchangeably.

8.10 Investigate Use of Cordless Headset

The single on-line collaborative tool used more than any other has been audio. In EFX 98 and JEFX 99 the users were supplied with headsets to avoid confusion about which voice came from where and headset mounted microphones to improve audio pick-up and reduce background noise. Headsets have also contributed to a lower noise level in the various AOC facilities.

Headsets also have some undesirable features. For example the wires that connect them to the users' workstations tie the users to those workstations and are the single largest source of audio breakdowns (users unplug them and later replug them incorrectly). A lesser user annoyance is the wires getting in the way, getting caught in clothing and furniture and creating a mess on the limited desk space. Many users need to be able to move around both virtually and physically. Wireless headsets would make it possible to move physically without completely severing all contact with the virtual side.

Cordless headsets represent a possible solution however they must have a reasonable range (50 feet within the same physical room) yet their strength should be low enough so as not to pose a threat of interception outside some reasonable perimeter (say, 1000 feet). They must also support up to 250 distinct channels to avoid crosstalk within the larger facilities.

A small scale experiment should be undertaken to determine whether the advantages of cordless headsets can be realized within some set of constraints (range, channels, audio quality, etc.) and for a reasonable cost.

8.11 Improve the Quality of Multipoint Audio

The most common user complaint about the collaborative tools in JEFX 99 was about audio quality. There are several reasons why audio in the data network environment isn't as good and/or reliable as the telephones we use as our benchmark. Three factors, bandwidth, compression and central processing unit (CPU) speed and load determine audio quality (complete audio failure is a different topic). Keep in mind also that audio packets are not acknowledged or retransmitted (they could never be retransmitted soon enough to be useful).

If low compression is used the resulting audio is of good quality, the load on the sending and receiving workstation CPUs is low and the impact of a lost network packets is minimal, but the network load is high. As compression increases the network load drops but so does audio quality plus the load on the sending and receiving workstations' CPUs increases and the impact of lost packets becomes more pronounced.

Packets of audio data are easy to lose. Since the audio stream depends on the sending and receiving workstations' CPUs, any other load on those CPUs can cause the audio stream to be interrupted and the audio that should have been processed at that moment is lost in either (or both) direction(s). On a busy network there are various conditions that may result in packets failing to leave the sending workstation or failing to reach their destination(s). Since there is no retransmission of audio packets those packets are gone.

We currently allocate bandwidth on our tactical networks for data, telephony and other purposes. Network audio typically takes less bandwidth than a phone conversation (and the network session often reaches multiple listeners rather than just one. It may be time to look at how that bandwidth is allocated. If networks can tolerate more and larger audio packets then less compression could be used thus reducing CPU loading, reducing the impact of lost packets and improving audio quality.

User training must continue to stress the relationship between workstation use and audio quality. With ever increasing use of audio it is conceivable that future audio boards for workstations will have their own processors able to pass audio packets to and from the network interface with little CPU intervention. In the immediate future we should also conduct tests involving network monitoring to determine the minimum level of compression that will be acceptable in various tactical environments.

8.12 Monitoring Multicast Traffic on the Network

Typical contemporary collaborative tools use IP multicasting as the mechanism for implementing relatively low bandwidth audio (and in some cases video) connections among participants in any number of simultaneous virtual “conferences.” In EFX 98 and JEFX 99 the operators relied heavily on multicast-based audio for the bulk of their communications. The effects and behavior of multicast traffic exchanged among several hundred simultaneous users on a combination local and wide area networked system is not well understood particularly because complete multicast traffic data from such an environment has not been gathered and analyzed. JEFX 00 offers the next opportunity to gather such data. Every effort must be made to bring the various network monitoring functions together so that the full spectrum of multicast traffic data can be collected and analyzed.

Appendix A

Collaborative Virtual Workspace (CVW) Terminology

All Users	menu option to display a list of all users that have an account on the server and their current status
Copy	menu option to make a duplicate of a CVW Object
Document	imported copy of an external file (e.g., Microsoft Word, Applix, GIF, Video Clip)
Folder	container for items (Documents, Notes, Web References, Whiteboards, Folders)
Group	configurable collection of CVW users, normally stored in the Group Manager but can be placed in a room or a User's carrying folder
Group Manager	menu option to display a list of public CVW groups
Import/Export	menu options allowing the process of taking objects in or moving them out of the internal CVW server environment
Note	simple text document, resides within CVW
Object	general term which applies to various CVW items which might appear in Room Contents, (e.g., Web Reference, Group, Note, Text Document, etc.)
Online Users	menu item to display a list of all currently connected users and their status
Page	text notification to another CVW user or users
Phone	point-to-point CVW audio communication
Pop-Up	text notification to another CVW user or users which superimposes onto the receiver's desktop, also known as a Pop-Up Page
Room Contents	objects placed in a CVW room
Scrollback Area	area on the CVW desktop where text communication occurs

Shortcut
menu option to make a pointer (similar to an internet bookmark) to the most recent published copy of a document in CVW Web Reference – A reference to a Web Page, also known as Universal Resource Locator (URL)

Whiteboard
shared (multi-user) graphic display for presenting and marking up images

Appendix B

System Data and Observations

Beginning on 28 August 1999, the team collected data from each day's operations. This covered the period of heaviest use and also reflected the significant technical problems we encountered. This section contains the daily status documents for each day followed in some cases by segments from the administrator's scrollback and screen captures of the CVW server and document server performance meters (perfmeters).

B.1 Data Collected from 27 August 1999

Insertions from CVW team members for Friday, 27 August 1999. (Please put your name on each of your entries.)

Server Status and Performance:

In spite of a power problem (see below), the CVW server functioned normally throughout this period. The web and document servers had to be rebooted.

Multicast Performance:

None.

Issues and Problems:

Suspected electric surge caused TBMCS servers as well as CVW web server and document server to freeze/crash. The failure of the UPS to prevent these problems is unclear.

Significant EVENTS hosted in CVW (type, CVW location, # of users participating):

Yesterday ended early due to heavy rains and roof leaks.

Largest Number of OnLine Users:

Largest number of concurrent logins 307

B.2 Data Collected from 28 August 1999

Insertions from CVW team members for Saturday, 28 August 1999

Server Status and Performance:

External (4GB) disk and 4mm tape drive added to CAOC Backup server to accommodate ever growing backup files from OSC server. Rick Cashell

Doc server rebuilt and all three Langley servers taken down gracefully and rebooted. The primary CVW server had been running continuously since training began (Randy and George between 0021Z and 0220Z 29 Aug)

Multicast Performance:

None.

Issues and Problems:

Multiple problems with lost documents and lost whiteboard backgrounds.

Significant EVENTS hosted in CVW (type, CVW location, # of users participating):

None.

Largest Number of OnLine Users:

(no record of peak number of concurrent user)

B.3 Data Collected from 29 August 1999

Insertions from CVW team members for Sunday, 29 August 1999

Server Status and Performance:

A snapshot of the server perfmeter at the time of the 350 user load was saved for analysis and comparison.

A second snapshot was taken for a period when use declined from 300 to 275 users.

Multicast Performance:

Multicast seems to have worked fairly well all day with the exception of the some one-way router problems with the Coronado and possible two unspecified sites.

Issues and Problems:

Today's biggest problem seems to be audio on the Micron NTs. Since it seems to be brand specific one wonders if maybe there is a problem between vat and the NT drivers for the audio board supplied with the Micron machines.

Many users have never logged in and their accounts were hanging around with default passwords. Dee wrote a new command @reset-neverconnected-passwords that enables us to reset all those passwords to something only the admins know. This has been performed for the first time and 549 accounts were found and the passwords reset. (Geo. 2300Z)

Significant EVENTS hosted in CVW (type, CVW location, # of users participating):

"110 users in the CFACC Brief Audio window right now..." (Hansel, 1710Z)

"Might also want to notify everyone that there are approximately 120 users up in audio and viewing a 54 slide briefing (off 2 webservers at Langley & Hurlburt)...." (Pam, 1725Z)

Dep Dir CAOC (Dir OSC) afternoon briefing included a large number of users - I counted 88 in the vat. I listened to part of the briefings - seemed to go very well. (George, 2140Z)

He pages, "337 users and 122 in Audio Window..." (Hansel, 1727Z)

JC reports only one time early in the day when a number of users were disconnected. Throughout the period of heaviest use there was no apparent disconnect event.

EOC flew today. They used CVW in the air, were able to do text chat with the ground and hear audio from the ground. They heard the CFACC briefing including Gen. Trapp's remarks. Denise reports that the EOC Commander was "delighted"!

Largest Number of On Line Users:

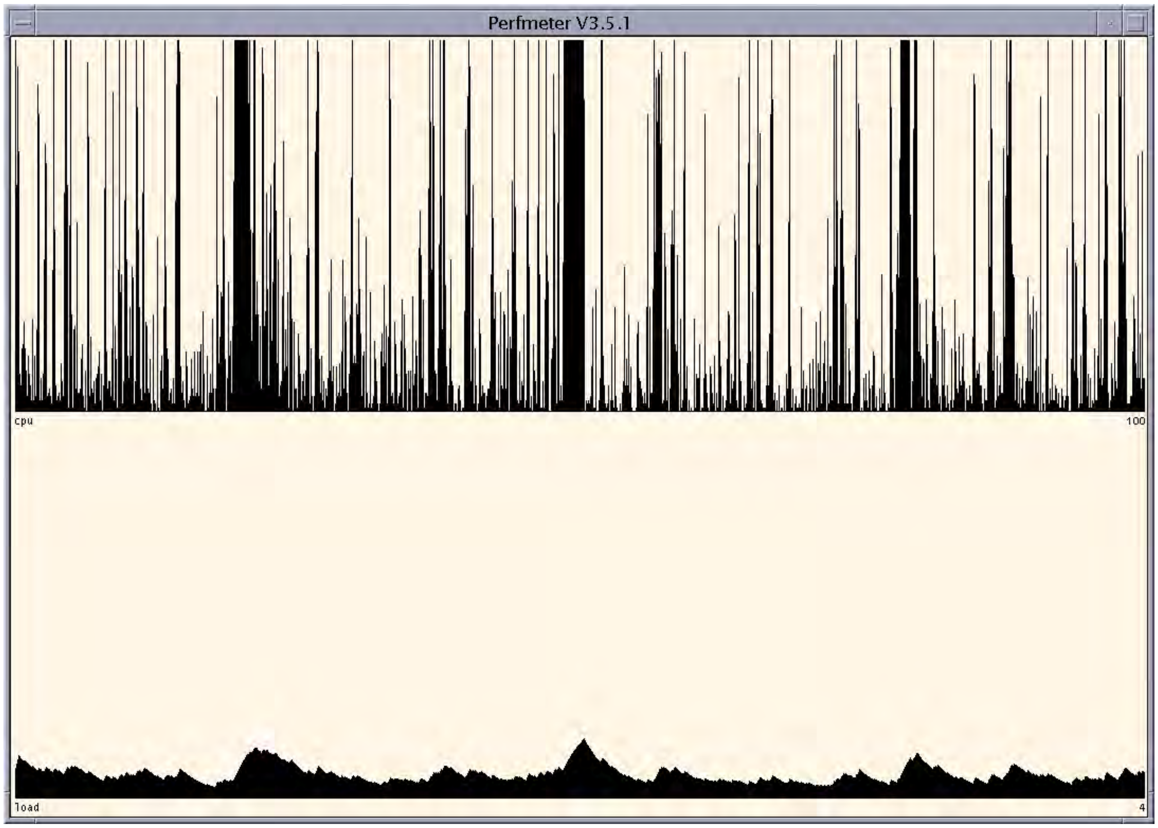
None.

351 Online users (Geo, 2130Z) from the Admin scrollback:

```
< connected: COMMSO4Coveno. Total: 349 >
< connected: EOCO6Reynes. Total: 350 >
< connected: 14AFA55O4Campbell. Total: 351 >
< disconnected: SOFCOMO4Brown. Total: 350 >
< disconnected: DOCCINO3Seiling. Total: 349 >
< disconnected: CSDRLBXE6Buda. Total: 348 >
< disconnected: IMINTE3Wrinkle. Total: 347 >
< disconnected: MAAPO4Polizzi. Total: 346 >
< connected: IMINTE3Wrinkle. Total: 347 >
< connected: VSTARSE7Hamman. Total: 348 >
< connected: OTCOMO6Rea. Total: 349 >
< connected: ASERO4Granville. Total: 350 >
< connected: IME6Parker. Total: 351 >
< disconnected: COMMSO4Coveno. Total: 350 >
< disconnected: SPSYIN03Rodriguez. Total: 349 >
< connected: COMMSO4Coveno. Total: 350 >
< disconnected: ASERO4Nugent. Total: 349 >
```

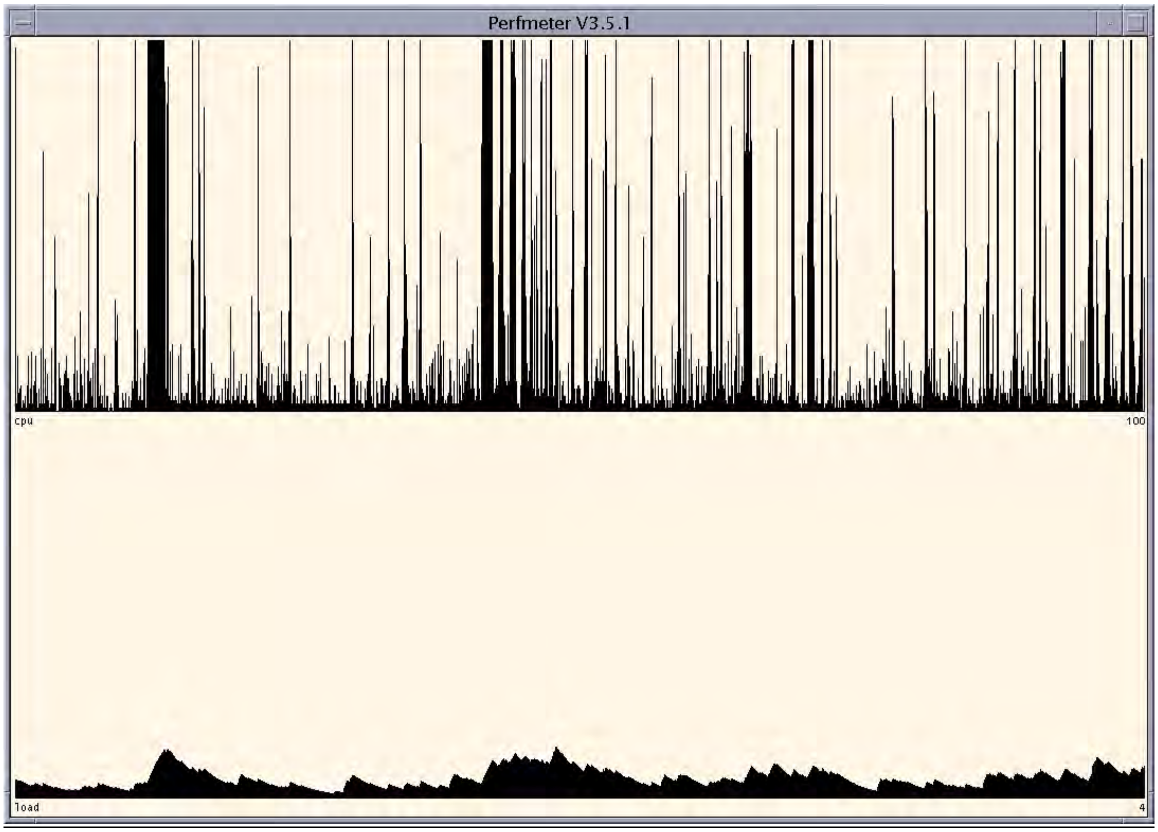
At 2320Z there are still 225 online users.

From a popup: Cashell pages, "!I am happy to report that the external disk storage scheme for saving Doc Server contents on the CVW CAOC backup server has been completed and is a success."



Perfmeter from CVW Server with 350 online users on 29 August

This graph covers a period of about 35 minutes. During this period there were between 345 and 360 online users. Note that the CPU is working hard but still running at less than 50% of full capacity overall. We understand that smooth utilization of 100% of the CPU is not possible or practical, but we also know that this CPU could support a considerably heavier load. Note also the three heavy bars of 100% utilization. These are caused by the periodic (in this case it was set to every ten minutes) update of the Online Users List.



Perfmeter from CVW Server with 275 online users on 29 August

This graph covers a period of about 35 minutes. During this period the number of online users declined from ~ 290 to ~ 270. As the day's activity winds down both the number of users and their level of activity decline. Note that the base level of CPU utilization is below 10%. Many of the spikes we see here are due to users logging off at which time the CVW server performs process intensive housekeeping chores.

B.4 Data Collected from 30 August 1999

Insertions from CVW team members for Monday, 30 August 1999

Server Status and Performance:

Had docserver problems this morning/afternoon - several reports of getting docserver unavailable messages...(PSK 1200)

Docserver performance was more than likely due to network congestion. Two sites reported a slow response time when accessing the doc server, the Corinado (spelling) and the CAOC.

Multicast Performance: Problems with audio from CAOC. No official cause noted. It was suggested that limited BW may have been the cause. There was only one circuit coming out of the CAOC yesterday (from Bob).

Issues and Problems:

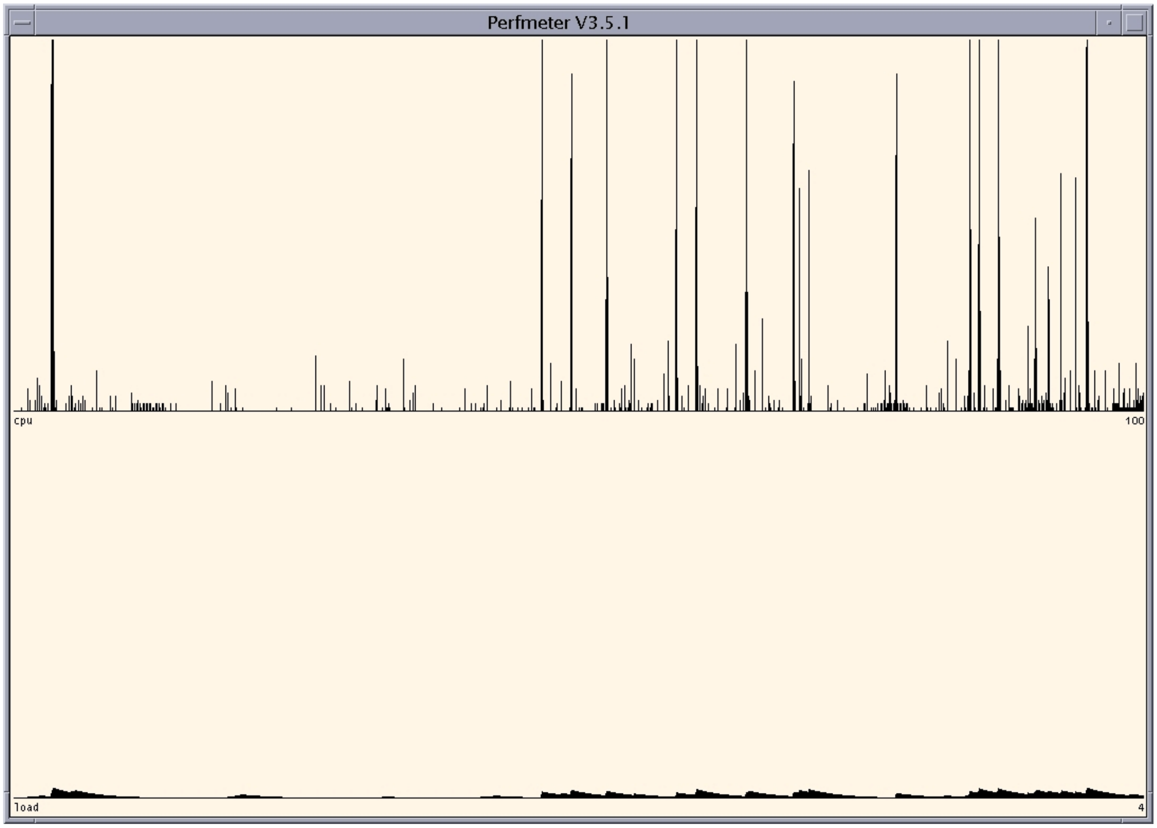
Discovered an interesting problem within a user account....when cutting and pasting text into a page window, the first page the user sent out would be sent and received correctly, as would any page that was typed into a page window. However, any subsequent page that was cut and paste into the page window would not successfully be sent and received -- instead, the receiver would get a page that contained approximately the first 25 characters of the FIRST page; believe that problem is cause by corrupt CVW (or other) application that is part of user's TBMCS profile...(PSK 2200 CDT)

Significant EVENTS hosted in CVW (type, CVW location, # of users participating):

Two Users at Whiteman had their account passwords reset. They were among the 549 users who had never connected to CVW that had their passwords changed yesterday as a security precaution (RWL 1250).

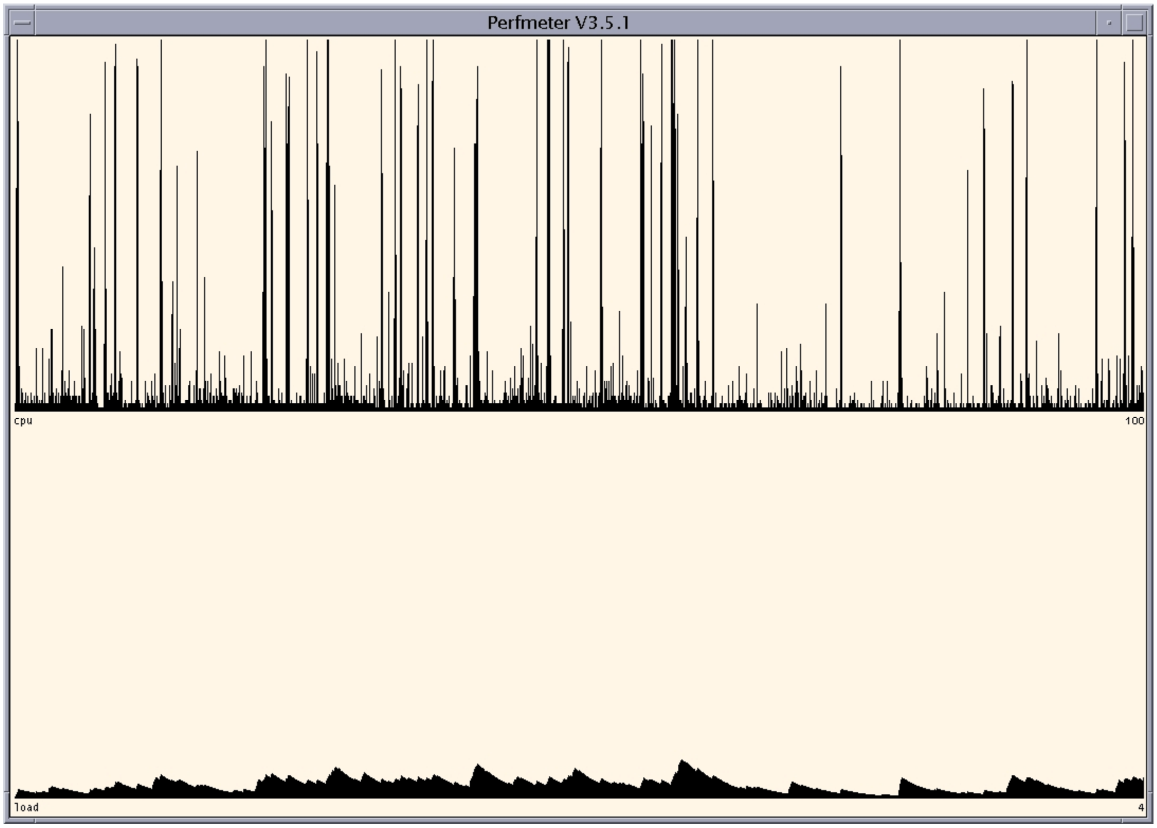
Largest Number of OnLine Users:

```
< disconnected: ASERO3Kays. Total: 366 >
< connected: INTELE4Covington. Total: 367 >
< connected: CSDFNBCE5Werner. Total: 368 >
< connected: SBMCSE2Cases. Total: 369 >
< connected: TAOTO3Susak. Total: 370 >
< connected: TCTE5Reding. Total: 371 >
< connected: IMSPTE4Baker. Total: 372 >
< disconnected: ASER00Koehler. Total: 371 >
< disconnected: JAGOSCO5Gent. Total: 370 >
< connected: JAGOSCO5Gent. Total: 371 >
< disconnected: SPT0E4Wilson. Total: 370 >
< disconnected: ASERO6Wilmoth. Total: 369 >
< disconnected: JASSM00Warlick. Total: 368 >
< disconnected: IMSPTE4Baker. Total: 367 >
< connected: CSARO3Schuller. Total: 368 >
< connected: JASSM00Boyle. Total: 364 >
< disconnected: TPSOPSO4Allison. Total: 363 >
```



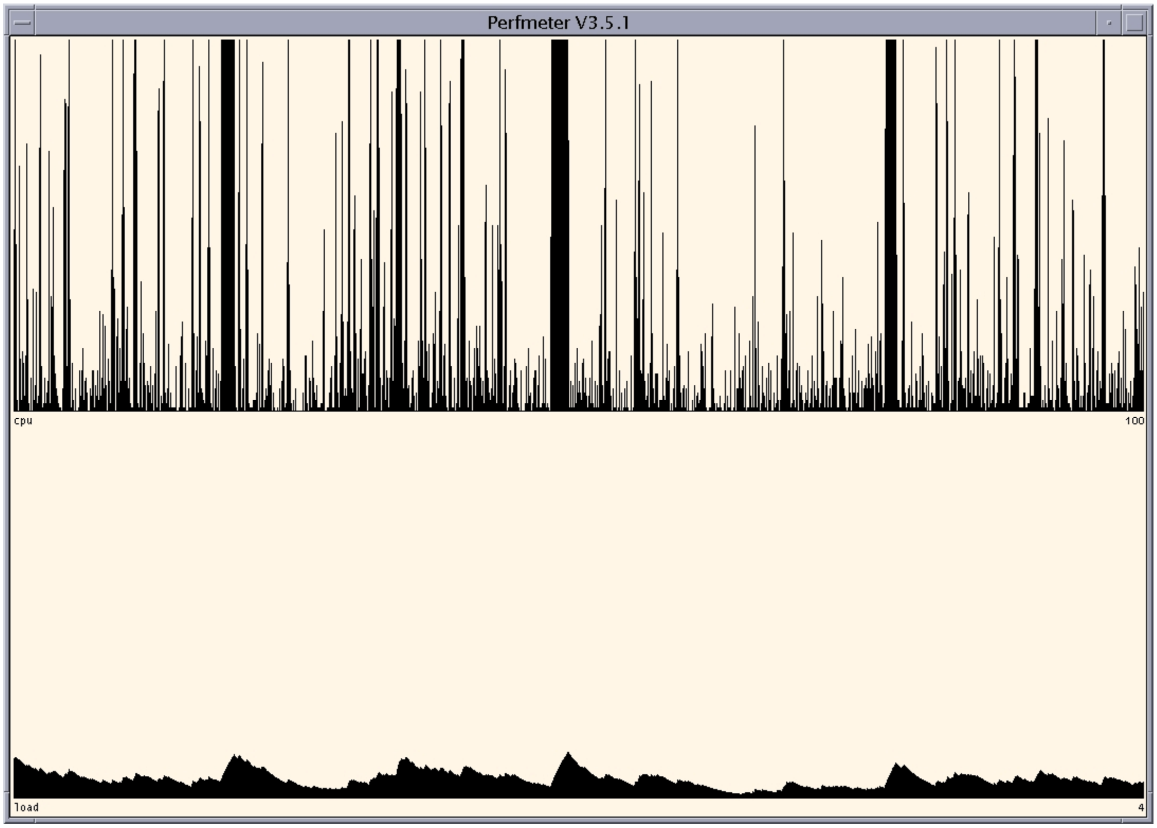
Perfmeter from CVW Server with 50 – 75 online users on 30 August

This graph covers a period of about 35 minutes. During this period the number of online users increased steadily to ~ 75. When compared with the second graph of 29 August it is obvious that user logins load the system less than logouts. Apparently few if any users had opened their Online Users window since the distinctive spikes do not yet appear.



Perfmeter from CVW server with 115 online users on 30 August

This graph covers the 35 minutes just after the period shown on the previous graph. During this period the number of online users continued to increase to a maximum of 115.



Perfmeter from CVW Server with 370 online users on 30 August

This graph shows the perfmeter during the 35 minute period when the maximum number of users were connected to the CVW server (372 at one point) during JEFX 99. This peak happened to correspond with an interval when user activity was relatively low.

> (Note that user activity levels varied considerably. For example, during CFACC briefings, the level of activity slowed because as many as 1 user in 3 was in the briefing room listening and therefore not putting any load on the server. During these same periods activity on the web servers was very high because the briefing slides were served out one at a time, user by user, as they were requested.)

B.5 Data Collected from 31 August 1999

Insertions from CVW team members for Tuesday, 31 August 1999

Server Status and Performance:

- 0700L local all is good. 50+ users logged on when I arrived this morning
- 1200L 140+ users, no problems ATT
- 1436L 334 users logged on

CVWCAOC00Lee in CFACC Balcony is requesting your attention.
He pages, "!Gary - We are having huge doc-server delays. Just moving a web link from a room into a folder is taking at least a minute or two...."

Multicast Performance:

- Nothing reported as of 1200L
- All is good at 1645L

Issues and Problems:

- Received a couple of trouble tickets regarding WinCenter and CVW. Users are having problems when a document is opened, edited, and placed back into the room. CVW does not maintain the permissions originally set, Randy is looking into this.

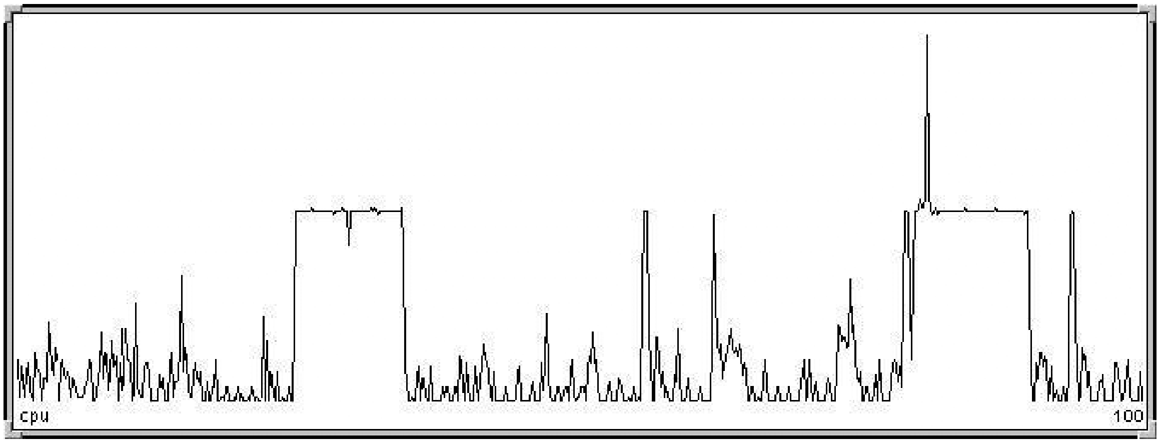
- Issue regarding time required to access large documents on the CVW Doc server. This was handed to Rich Taylor (MITRE), a time out feature was identified as the problem as well as slow network performance. (This timeout was shortened in response to last year's user complaints that they had to wait too long for doc server request to time out when one of the fairly frequent network failures, again this was last year, made the doc server unreachable. The right answer depends on circumstances that could change minute to minute and from one user to another).

- Above problems were also identified as potential indications of doc server failure at around 1600 EST. The doc server failed twice, a server shutdown and re-start were required both times. This problem is being blamed on a lack of memory and the large size of the doc server data, specifically the index.db file that runs in memory. This issue will be re-visited by MITRE developers.

Significant EVENTS hosted in CVW (type, CVW location, # of users participating):

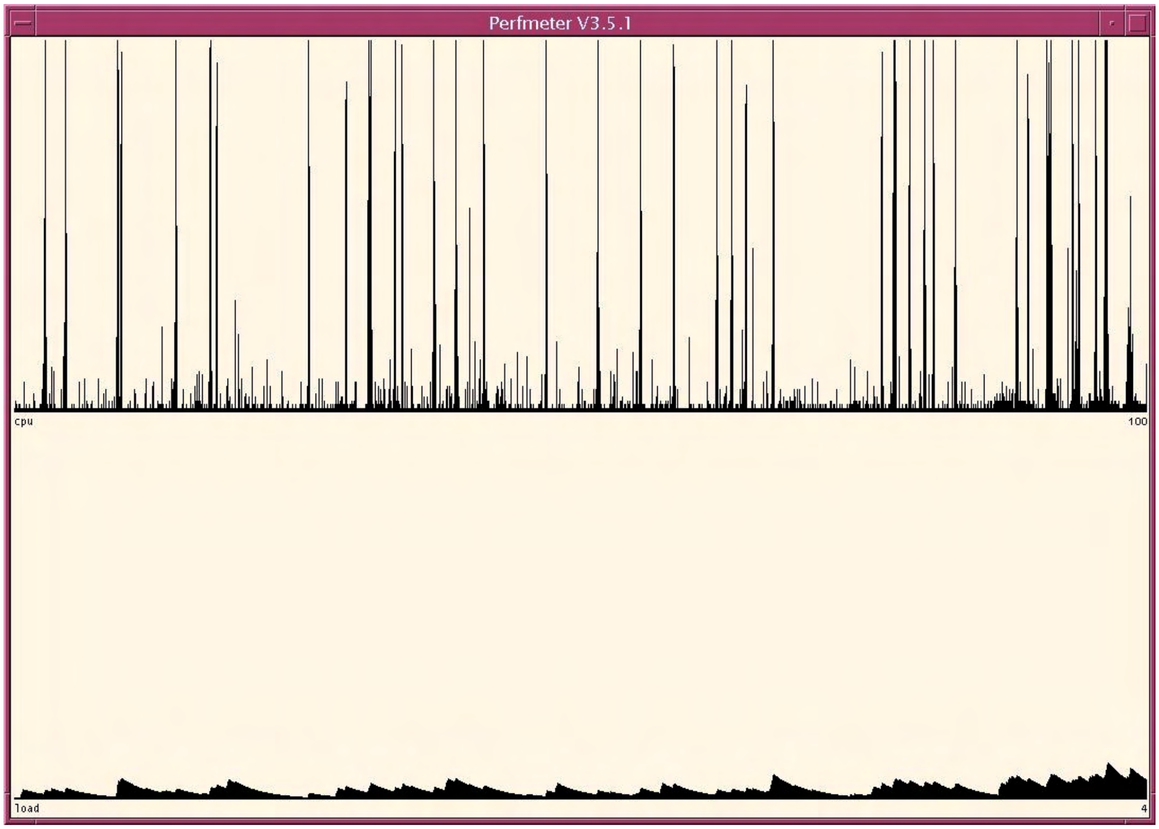
Largest Number of OnLine Users:
As of: 1500L

```
< connected: ASSES00DeRosa. Total: 360 >
< connected: MENTORO8Corder. Total: 361 >
< disconnected: COMMSO4Coveno. Total: 360 >
< disconnected: JICOO4Strickland. Total: 359 >
< disconnected: ASERE6Carley. Total: 358 >
< disconnected: CSDRASERO3Shankles. Total: 357 >
```

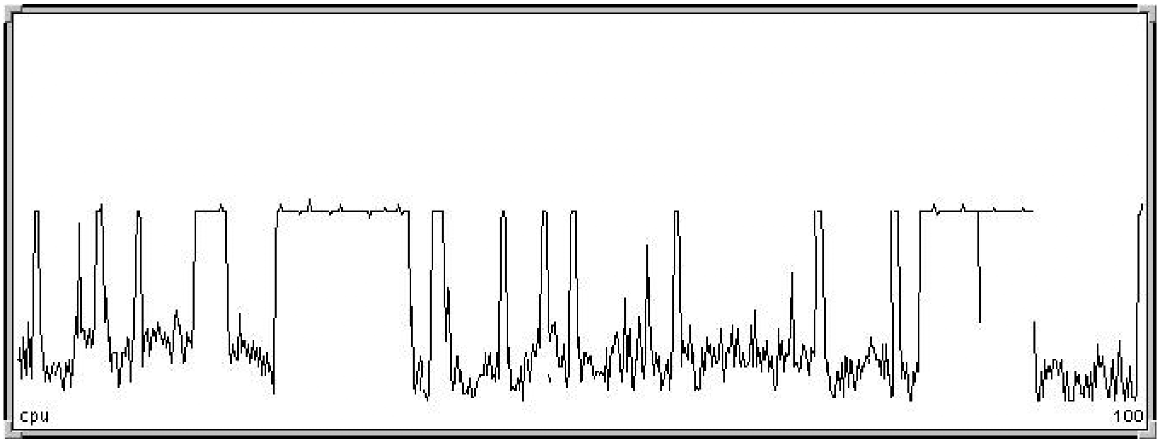


Perfmeter from Document? Server with 92 online users on 31 August

This 30-minute long graph of doc server CPU utilization levels shows a very different performance profile than the CVW server. The spikes represent a document being server to a user. The large buttes correspond with the periodic write back of the document server index file. The duration of this write back is directly proportional to the number of items on the server and therefore to the size of the index. Note also that the graph seems to be half height except for one spike. The lower half of the graph represents the activity on the first CPU. The second CPU did essentially nothing during this period except during the few seconds of that one spike.



Perfmeter CVW Server with 95 online users on 31 August



Perfmeter from Document? Server with 135 online users on 31 August

Despite the relatively small number of users note the heavy load on the document server's first CPU. The added width of the left hand butte is probably due a user request that was serviced immediately before or after the index writeback. If such a request happened to arrive when the write back process was not using 100% of the first CPU's capacity that request would be lumped on the first rather than being launched on the second CPU. Note that the second butte is closer to the same size as those we saw above. It would be ideal to be able to direct the writeback task onto the second CPU thus leaving the first available full time to support users.

B.6 Data Collected from 1 September 1999

Insertions from CVW team members for Wednesday, 1 September 1999

Server Status and Performance:

This morning I stopped the docserver and rebooted the machine. Later when Gary and I looked at the index.db we found that it contained only a handfull of references all dated on 31 Aug and 1 Sept. Knowing that almost nothing would work we found a much better looking index file on the backup server, ftp'd it onto the primary and HUPed the process. The documents we had tried and had not worked were fixed by this process. Whatever caused the problems we had yesterday must have corrupted the index.db during the night. Our hope is that the rebood freed memory enough to assure proper operations for today. A similar reboot will be performed tomorrow morning. The docserver developer is looking for a suspected memory leak.

Late in the evening a problem was reported with missing whiteboard backgrounds. Although the background file was found in the docserver's doc-store directory, it was not referenced in the index.db file. This appears to be the same problem we had noticed last week.

At approximately 1930 62 rooms were occupied for a 48% utilization of the virtual building. The most popular room was DBC execution with 22 occupants. There were around 250 users on-line at that time. Utilization was checked on two other occasions (a few days back) when 200+ users were on-line. In each case, the room utilization was approximately 50%.

Multicast Performance:

None.

Issues and Problems:

The ongoing problems with vat on Micron desktop computers is being investigated. This process is complicated by the fact that there are so many different PC "compatible" but not identical computers. In addition there are many different audio boards and accompanying software drivers. Further complicating the picture is NT and NT-specific audio drivers.

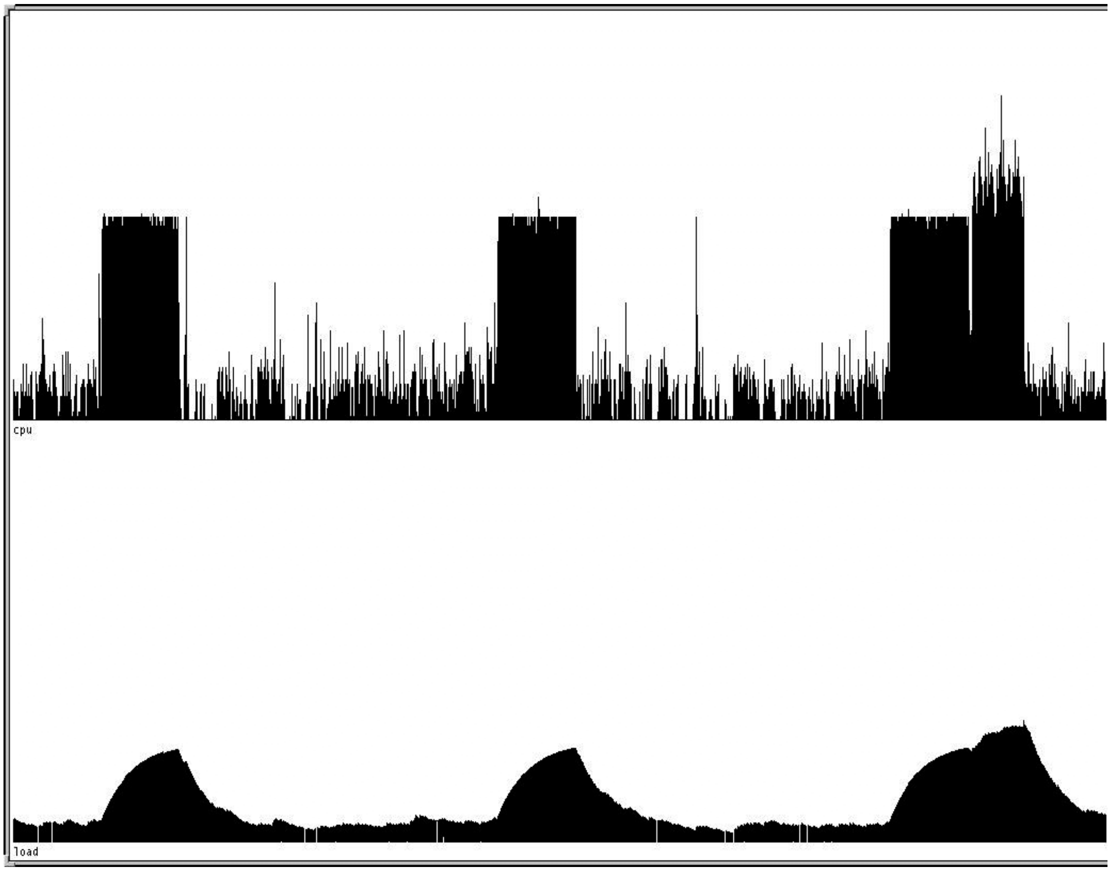
Later in the afternoon problems with the docserver resurfaced. Users reported that documents they had created and dropped into a room yesterday night had disappeared. In addition, some of the old documents in our carrying folder could no longer be opened because they "were not on the docserver."

Significant EVENTS hosted in CVW (type, CVW location, # of users participating):

None.

Largest Number of OnLine Users:

```
< connected: CSDFDDIRO4Leccadito. Total: 343 >
< disconnected: CVWOSC00Daigle. Total: 342 >
< disconnected: PROFILEsE4Morsches. Total: 341 >
< disconnected: ESC-FXO3Hanks. Total: 340 >
< connected: JTSSTO00Nguyen. Total: 341 >
< connected: MTEOCwilson. Total: 342 >
< connected: CVWOSC00Daigle. Total: 343 >
< connected: ESC-FXO3Hanks. Total: 344 >
< connected: PROFILEsE4Morsches. Total: 345 >
< connected: STRATO3Sartino. Total: 346 >
< connected: ASER00Carpenter. Total: 347 >
< connected: CAOCVIPO6. Total: 348 >
```



Perfmeter from Document Server with approximately 340 online users

This is another interesting look at what was happening on the document server. Requests to the server involve small files until we get to the right of the third butte. At that point someone (probably several people) opened a very large document. We suspect that it was more than one request was being served since some of the load was thrown onto the second CPU.

B.7 Data Collected from 2 September 1999

Insertions from CVW team members for Thursday, 2 September 1999

Server Status and Performance:

At approximately 1150 39 rooms were occupied for a 33% utilization of the virtual building. The most popular room was Production with 10 occupants. There were around 94 users on-line at that time.

Multicast Performance:

None.

Issues and Problems:

None.

Significant EVENTS hosted in CVW (type, CVW location, # of users participating):

None.

Largest Number of OnLine Users:

The active Experiment ended on the afternoon of 2 September 1999. Because it was the last day not much happened. No admin scrollback was captured on the 2nd.

Appendix C

Technical Procedures Documents

The following are the contents of a series of short documents that were used by the team to standardize the performance of certain routine tasks. Any deployment of a similar tool should be accompanied by procedures similar to these but tailored to the proper management of that tool.

C.1 Procedure for Creating and Distributing the Server and Docserver Backup Files

and

Procedure for Performing the Server Backup at the OSC

1. On the primary CVW server (.237) check the time when CVW.db.new was last written to

   ```
   cd /opt/CVWserver
   ls -al CVW.db.new
   date
   ```

   Compare the time on the CVW.db.new with the time on the date line. If the time on the CVW.db.new is less than 50 minutes ago then go ahead, otherwise wait 15 minutes and repeat this step.

2. Create the CVW server backup file

   ```
   cd /opt
   tar cvf server8-10.tar ./CVWserver  (where 8-10 is the date, August 10 in this case)
   ```

3. Compress the tar file

   ```
   compress server8-10.tar
   ```

4. FTP the compressed file to two locations, the OSC backup machine and the CAOC backup machine

   OSC Backup: lll.211.232.66
   CAOC Backup: hhh.201.165.139

   Be sure to invoke the binary option on ftp before put-ting the file
   Put the file in /opt on OSC Backup and in /external on CAOC Backup. The transfer to the CAOC will be slow so do the OSC first.

5. On the primary CVW document server machine (.239) create the CVW docserver backup file. This can be done at any time but is safest if performed when the user load is low and at nearly the same time as the CVW server backup.

   ```
   cd /opt
   tar cvf docserver8-10.tar ./CVWserver  (where 8-10 is the date)
   ```

6. Compress the tar file.

   ```
   compress docserver8-10.tar
   ```

7. FTP the compressed file to two locations, the OSC backup machine and the CAOC backup machine.

   OSC Backup: lll.211.232.66
   CAOC Backup: hhh.201.165.139

   Be sure to invoke the binary option on ftp before putting the file
   Put the file in /opt on OSC Backup and in /external on CAOC Backup. The transfer to the CAOC will be slow so do the OSC first.

8. Update the OSC Backup server.

   8.1 Shutdown the OSC Server

   ```
   sh /etc/rc3.d/S99cvw stop
   sh /etc/rc3.d/S99cvwds stop
   ```

   8.2 Uncompress and untar the CVW Server & docserver file over /opt/CVWserver

   ```
   cd /opt
   zcat server8-10.tar.Z | tar xvf -  (For the 10 Aug Server File)
   zcat docserver8-10.tar.Z | tar xvf -  (For the 10 Aug Docserver File)
   ```

   This should overwrite the /opt/CVWserver directory with the updated Server and Docserver files from Langley.

   8.3 Open /usr/openwin/bin/textedit Don't try to use CDE textedit. In textedit open /opt/CVWserver/CVW.db.new. In that file do a find and replace on lll.211.232.73 and change to lll.211.232.66 Save file.
   (We may need additional changes - we'll have to learn as we go along.)

   8.4 Copy the license key from /opt to /opt/CVWserver (copy, don't move)

   ```
   cp /opt/cvw.license /opt/CVWserver/
   ```

8.5 Change the permissions on the CVWserver directory to reflect cvw as the owner.

```
cd /opt/CVWserver
chown -R cvw
chgrp -R 2
chmod 750
chmod -R go-w *
```

8.6 Start the server

```
sh /etc/rc3.d/S99cvw start
sh /etc/rc3.d/S99cvwds start
```

8.7 Launch the CVW client and log into the JEFX-OSC-Backup server.

From the Client go to the "Admin" menu - Then down to "System Settings"

Replace "CVW name: JEFX" with "JEFX-OSC-Backup"
Replace "Host machine name: cvwsvr" with "cvwweb"
Replace "Multicast prefix: 227.4" with "227.8"
press the Apply button

8.8 The backup is complete.

C.2 Procedure for Performing the Server Backup at the CAOC

These instructions assume that the back-up files have been made from the primary server and ftp'd to the CAOC server.

1. Shutdown the CAOC Server

```
sh /etc/rc3.d/S99cvw stop
sh /etc/rc3.d/S99cvwds stop
```

2. Uncompress and untar the CVW Server file over /opt/CVWserver

```
cd /external
cp server8-10.tar.Z /opt  (For the 10 Aug Server File)
cd /opt
zcat server8-10.tar.Z | tar xvf -  (For the 10 Aug Server File)
mv server8-10.tar.Z /external/to_tape  (For the 10 Aug Server File)
```

This should overwrite the /opt/CVWserver directory with the updated Server and Docserver files from Langley.

3. Uncompress and untar the CVW docserver file over /external/CVWserver

```
cd /external
rm server8-10.tar.Z  (For the 10 Aug Server File)
zcat docserver8-10.tar.Z | tar xvf -  (For the 10 Aug Docserver File)
mv docserver8-10.tar.Z /external/to_tape  (For the 10 Aug Server File)
```

4. Open /usr/openwin/bin/textedit Don't try to use CDE textedit. In textedit open /opt/CVWserver/CVW.db.new. In that file do a find and replace on lll.211.232.73 and change to hhh.201.165.139 Save file.
   (We may need additional changes - we'll have to learn as we go along.)

5. Copy the license key from /opt to /opt/CVWserver

```
cp /opt/cvw.license /opt/CVWserver/
```

6. Change the permissions on the CVWserver directories to reflect CVW as the owner.

```
cd /opt/CVWserver
chown -R cvw
chgrp -R 2
chmod 750
chmod -R go-w *

cd /external/CVWserver
chown -R cvw
chgrp -R 2
chmod 750
chmod -R go-w *
```

7. Start the server

```
sh /etc/rc3.d/S99cvw start
sh /etc/rc3.d/S99cvwds start
```

8. Launch the CVW client and log into the JEFX-CAOC-Backup server. Wait 2-3 minutes first.

   From the Client go to the "Admin" menu - Then down to "System Settings"

   Replace "CVW name: JEFX" with "JEFX-CAOC-Backup"
   Replace "Host machine name: cvwsvr" with "cvw2"
   Replace "Multicast prefix: 227.4" with "227.12"

9. Write the backup files to tape and remove them from the disk

```
cd /external
tar cvf /dev/rmt/0h to_tape  (takes a looonnng time)
mt -f /dev/rmt/0 rewoff
cd to_tape
rm *tar*
```

10. The backup is complete

C.3 Procedure for Performing the Server Backup at the SOC

These instructions assume that the back-up files have been made from the primary server and ftp'd to the SOC server. We do not believe this procedure was ever used.

1. Shutdown the AFSPACE Server

```
sh /etc/rc3.d/S99cvw stop
sh /etc/rc3.d/S99cvwds stop
```

2. Uncompress and untar the CVW Server & docserver file over /opt/CVWserver

```
cd /opt
zcat server8-18.tar.Z | tar xvf -  (For the 18 Aug Server File)
zcat docserver8-18.tar.Z | tar xvf -  (For the 18 Aug Docserver File)
```

   This should overwrite the /opt/CVWserver directory with the updated Server and Docserver files from Langley.

3. Open /usr/openwin/bin/textedit Don't try to use CDE textedit. In textedit open /opt/CVWserver/CVW.db.new. In that file do a find and replace on lll.211.232.73 and change to 207.84.12.178 Save file.
   (We may need additional changes - we'll have to learn as we go along.)

4. Copy the license key from /opt to /opt/CVWserver

```
cp /opt/cvw.license /opt/CVWserver/
```

5. Change the permissions on the CVWserver directory to reflect CVW as the owner.

```
cd /opt/CVWserver
chown -R cvw
chgrp -R 2
chmod 750
chmod -R go-w *
```

C.4 Web Replication Procedure

No automated web server mirroring capability was implemented in JEFX 99 therefore it was necessary to manually replicate certain high use documents on remote servers. These are the procedures we used.

To Send the Briefing to the Langley and Hurlburt Servers:

1. Get Decision Brief from Whoever provides it in ppt form. (to be worked out)

2. Use NT machine just to the right inside the CAOC door (insert zip disk and open PPT file in PowerPoint).

3. Chose Save as Html from the file menu in PowerPoint.
   - Use existing profile "jc" and click "Finish"

4. Brief will be saved inside the c:/CFACCBrief/(NAME OF FILE HERE)/ as a number of .htm and .gif files.

5. On the NT Machine change to the directory that contains all the files for the brief. (all the .htm/.gif/etc files).

```
------------------------
To send to Langley:

ftp lll.211.232.66
Log in as root
cd /opt/web/jefx/cfaccdecision/xxaug (xx = date IE: xxaug or xxsep)
          IE: Type: cd /opt/web/jefx/cfaccdecision/01sep
Type: prompt
Type: bin
Type: mput *

AFTER all files have been sent

Type: quit
------------------------
To Send to Hurlburt:

ftp hhh.201.165.139
Log in as root
cd /opt/web/jefx/cfaccdecision/xxaug (xx = date IE: xxaug or xxsep)
          IE: Type: cd /opt/web/jefx/cfaccdecision/01sep
Type: prompt
```

Type: bin
Type: mput *

AFTER all files have been sent

Type: quit

Create WEB Links in CVW in the CFACC Brief Room to each of the briefings as per future guidance...

IE:

For Hurlburt Server Web Link
http://hhh.201.165.139/jefx/cfaccdecision/24aug/index.htm

For Langley Server Web Link
http://lll.211.232.66/jefx/cfaccdecision/24aug/index.htm

C.5 Moving Floors

During Spiral 2 of EFX Dee Goepel wrote a routine for rearranging the order or the floors in CVW. These are her notes on using this new capability.

The following messages were sent to you while you were disconnected:

From: Dee Sun Jul 12 04:29:16 1998 GMT
Dee pages, "Okay, I moved the top floor 'Strat ATOs A - H' to be just below 'Strat ATOs I - L & Misc'... it looked like that's where it belonged. If not, it's easy to change. All you do is type 'move-floor' (without single quotes) as Admin (or me) and it will prompt you for the rest of the info. You can move any floor except the first floor and place it on top of any other floor. It will ask you which floor to move and which floor to put it on top of. Also it is quite thorough about error checking, so you can't easily break it by accidentally entering in the wrong thing. I think it is pretty hard to mess it up."
From: Dee Sun Jul 12 04:32:22 1998 GMT
Dee pages, "P.S. When you move a floor, I don't check to rename the hallways (so you will still see things like Hallway 10, on a floor that may now be the 3rd floor). And also, you shouldn't have to log out to see any of these changes, opening and closing the map is enough."

C.6 Creating a Desktop Icon for CDE

The Common Desktop Environment (CDE) was the most common UNIX desktop in JEFX. Many CDE workstations were also DII COE workstations so they used the segmented CVW client that had its own icon. For systems running CDE without DII COE it was desirable and sometimes essential to create a desktop icon from which to launch CVW. The following procedure was devised to satisfy this need.

From the HELP Room EXPORT the CVW Icon to /.dt/icons directory using file name CVW.m.pm .

Open the Applications Manager from CDE bar.

Open Desktop_Apps

Open Create Action

Enter a Label for the Icon like "CVW" (no quotation marks) in the Action Name box

Press the Find Set... Button and navigate to the /.dt/icons directory

The CVW icon should appear

Press the OK button

Enter "/opt/CVW/bin/xcvw" in the Command When Action Is Opened box

Select Save in the File menu

The Create Action application will tell you where the icon has been created. Go to that directory (probably your home directory) in the File Manager and you'll find the icon. It can be dragged to the Application Manager and/or to one of the scroll ups on the CDE Toolbar.

C.7 Multicast Domain Assignments for the CVW Servers in JEFX 99

Each CVW server in any single network domain must have its unique multicast address space so that there is no crosstalk to/from users on one server from/to users on another server. Several of these assignments were never actually used.

To avoid multicast overlap, we'll use the following prefixes for our JEFX servers. This scheme makes 650250 addresses available for each server - should be enough!

JEFX	227.4
JEFX-OSC-Backup	227.8
JEFX-CAOC-Backup	227.12
JEFX-AFSPACE-Backup	227.16

JEFX-EOC-Backup	227.20
JEFX-CFACC-Enroute	227.24
JEFX-Old-98	227.28

C.8 Notes on NIS and DNS

The following files were added or modified to allow CVW to interact with the TBMCS servers:

/etc/defaultdomain - This file was added to point to the appropriate NIS server domain. Once added, when the machine is rebooted it should be able to access the NIS maps. If deleted, NIS will not start on boot-up.

/etc/nsswitch.conf - This file tells the server which nameservice to use for paticular maps. The choices are "files" "dns" and "nisplus". If NIS or DNS will not be started, then all the maps in nsswitch.conf should use "files" .

/etc/resolv.conf - This file configures DNS resolution. Running the command "nslookup" and doing "ls <domainname>" will show whether the resolv.conf is working correctly.

C.9 Procedures for Updating the Server Configuration Files on CVW Java Clients

Once you've logged onto the machine start the web browser and go to the CVW Windows Client Installation page.

Download the three configuration files (but not the installer) to the CVW home directory (usually C:\Program Files\Mitre\CVW\)

Open the file manager to that directory and select the three new files (select one, hold down the Control key and select the other two). Right click on one of them and select Create Shortcut.

While the shortcut files are still highlighted right click on one of them and select Cut.

Navigate to c:\Winnt\Profiles\All Users\Startmenu\Programs\Mitre CVW\ and paste the shortcuts you're carrying by right clicking on the background of the directory and selecting Paste.

Now select the old shortcuts in that directory, right click on one of them and select Delete.

Test by going to the Start Menu, select Programs, MITRE CVW, JEFX-Prime and logging in.

C.10 Linking the Multicast Groups of Two Rooms (audio and video)

To create a listening gallery or balcony for the CFACC Conference room or to create any other pair of rooms that share the same audio and video multicast group, follow these steps.

There will be one primary room, and a secondary room that shares the first room's multicast.

1) Login as an admin
2) find out the object number of the primary room
   (you can go to the room and type ;here ...to find this out)
   I will refer to this obj num as <proom> in these directions
3) find out the object number of the secondary room
   I will refer to this obj num as <sroom> in these directions
4) type: @copy #3:show_audio_to to <sroom>
5) type: @edit <sroom>:show_audio_to
   an editor window will appear
   the forth line says link_room = this;
6) change "this" to <proom>
   (where <proom> is the object number of the primary room)
7) hit the save button at the bottom left corner of the widow
8) hit the close button at the bottom right corner

You are finished.

-----IMPORTANT-----IMPORTANT-----

When you are finished letting the rooms share multicast be sure to clean this up, so you don't have rooms all over using each other's multicast address and breaking the idea of room specific audio and video.

TO UNDO this, type: @rmverb <sroom>:show_audio_to (where <sroom> is the object number of the secondary room).

C.11 Procedure for Turning on Time Stamping

Entering this series of commands will cause an hourly timestamp to be placed in the user’s scrollback.

```
@program #1:notify
if (is_player(this))
motify(this,tostr(args[1],"<",$time_utils:mmddyy(time())," ",ctime()[12..16],">"));
endif
```

C.12 Procedures for Creating User Accounts

Every collaborative tool deployment where more than one person will be involved in user account creation should develop procedures of this type. These are the procedures used for CVW in JEFX 99.

Complete the fields as follows:

Login name: The user's ULN (all lower case letters, try to accurately distinguish between oh "O" and zero "0"), if no uln use lastnamefirstname (all lower case)

User name: JEFX short position title - GRade Last name in form POSITIONTITLEGRLastname (example: Military: C6-ARO4Parton Civilian: INIT299OOParton

Position title is from JEFX Position Title on in-processing form.
GRades are E1 thru E9 and O1 thru O9 (those are ohs not zeroes)
Civilians are 00 (zeroes)

Home Floor and Room - select as best you can - PLEASE give everyone an initial home room other than Main Entrance.

Let system assign password and be sure to note it on the form when you create the account (it's in the dialog box that appears when you press the Add or OK button)

Full name: Lastname, Grade Firstname MI (Grade can be abbreviated, NO grade for civilians - see Table of Grades)

Examples: Military: Dominick, Col John C .
Civilian: Dominick, John C .

NEW DETAIL: following the name in the full name field add a space followed by a dot. This will make the names alphabatize the same in Windows and Unix client Online Users and All Users windows.

Office: from Job Function in EFX on in-processing form

Phone: Choose one from the in-processing form

ID: extra field

Icon Use ULN as in Login name field (copy and paste here and in email - use middle mouse button to paste)

Military: lastnamegrade (all lower case) example: partonmaj
Civilian: lastnamefirstname (all lower case) example: partongeorge

email address: Military:
OSC: uln@afosc.langley.af.smil.mil

CAOC:uln@caoc.jefx.deployed.af.smil.mil
EOC: uln@eoc.jefx.deployed.af.smil.mil
BCC: uln@bcc.jefx.deployed.af.smil.mil
example: init300@afosc.langley.af.smil.mil

Civilian: firstinitiallastname@<same as military>
example: gparton@afosc.langley.af.smil.mil

C.13 Procedure for Capturing and Processing User Pictures

User pictures are a valuable aid to users enabling them to more quickly recognize their fellow collaborators. This procedure is specific to the JEFX system file structure. The last step was adopted so that the day's finished pictures could be shipped to the two (should have been three) web servers from a central location.

Log in to Openwin, NOT CDE

Launch application: (with vic turned off!)

/opt/SUNWits/Graphics-sw/xil/examples/test/SunVideo

Select 24 bit option under Display

Use STEP function to capture frames 'till you get what you want

Launch xv

Use GRAB in xv to move image into that app

Crop image to approximate shape - ratio of 4 units wide by 5 tall

Under Image Size select Set Size and enter "48 x 60"

Save image in /opt/web/cvw/user-images/newpics/<today's date - mm.dd>
Name files <ULN>.gif or if ULN is not available <lastnamefirstname>.gif

Appendix D

Collaborative Virtual Workspace (CVW) Network Systems Data

D.1 CVW Server

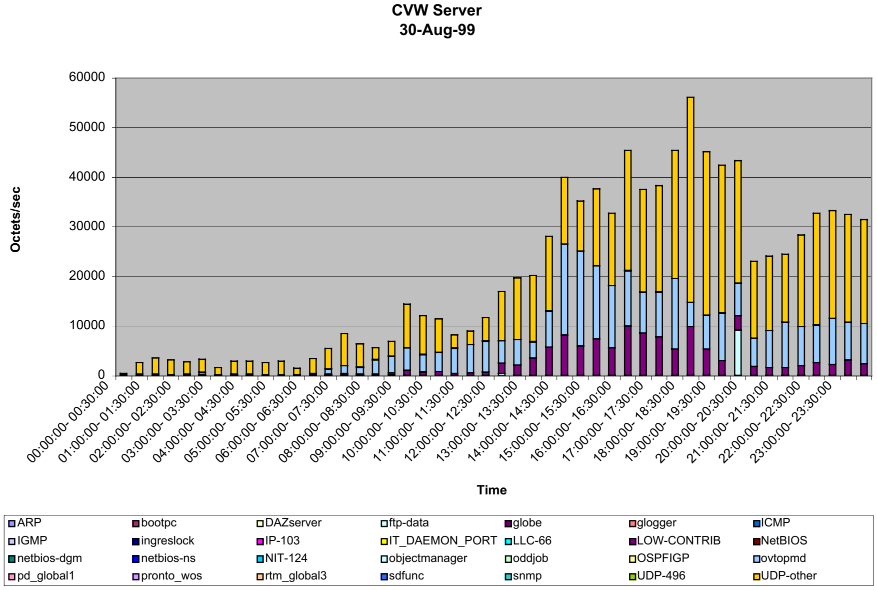


Figure D.1 - CVW Server Network Traffic Profile (RMON2 Probe) – 30 August 1999 EDT (LiveFly Day 1)

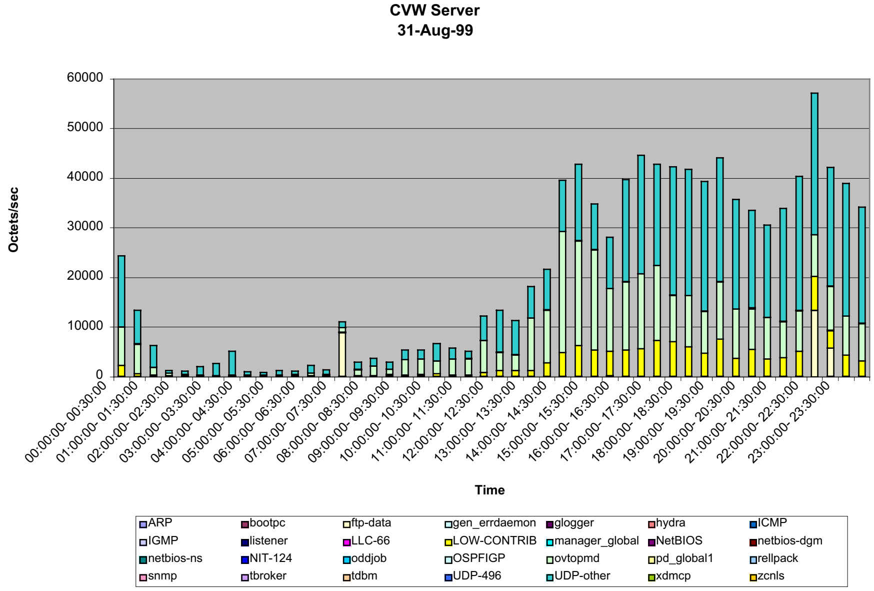


Figure D.2 - CVW Server Network Traffic Profile (RMON2 Probe) – 31 August 1999 EDT (LiveFly Day 2)

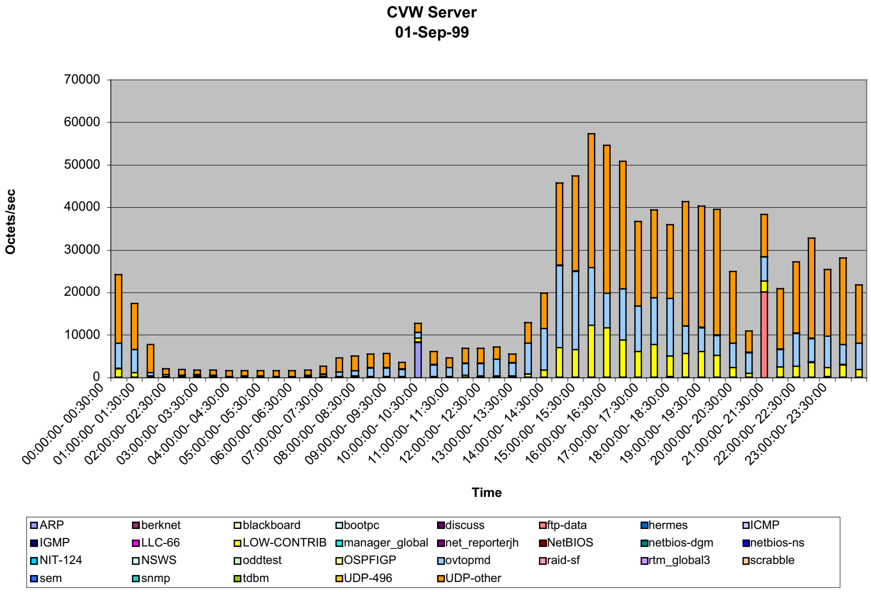


Figure D.3 - CVW Server Network Traffic Profile (RMON2 Probe) – 1 September 1999 EDT (LiveFly Day 3)

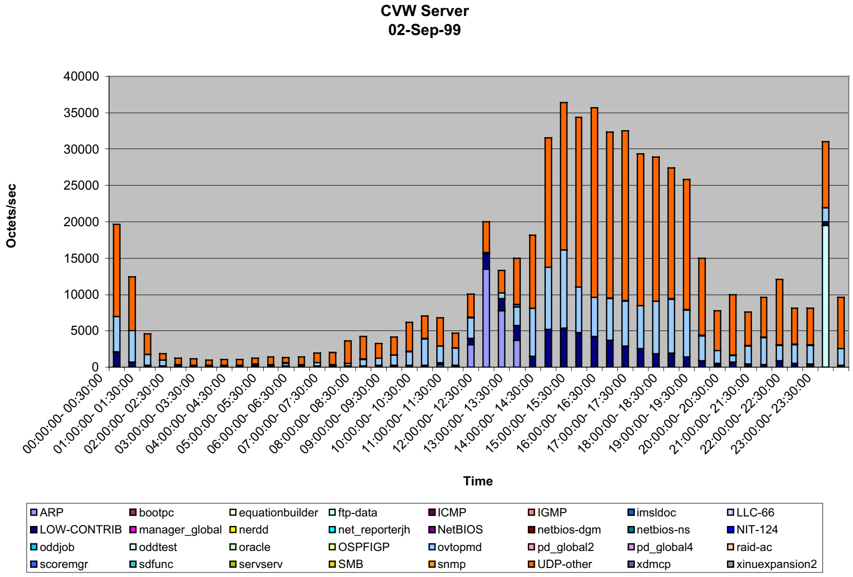


Figure D.4 - CVW Server Network Traffic Profile (RMON2 Probe) – 2 September 1999 EDT (LiveFly Day 4)

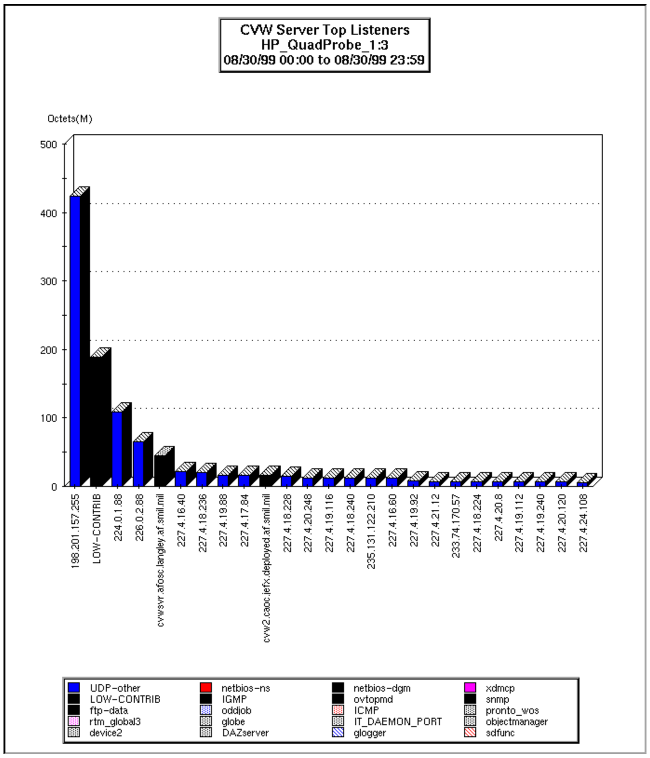


Figure D.5 - CVW Server Top Listeners (RMON2 Probe) – 30 August 1999 EDT (LiveFly Day 1)

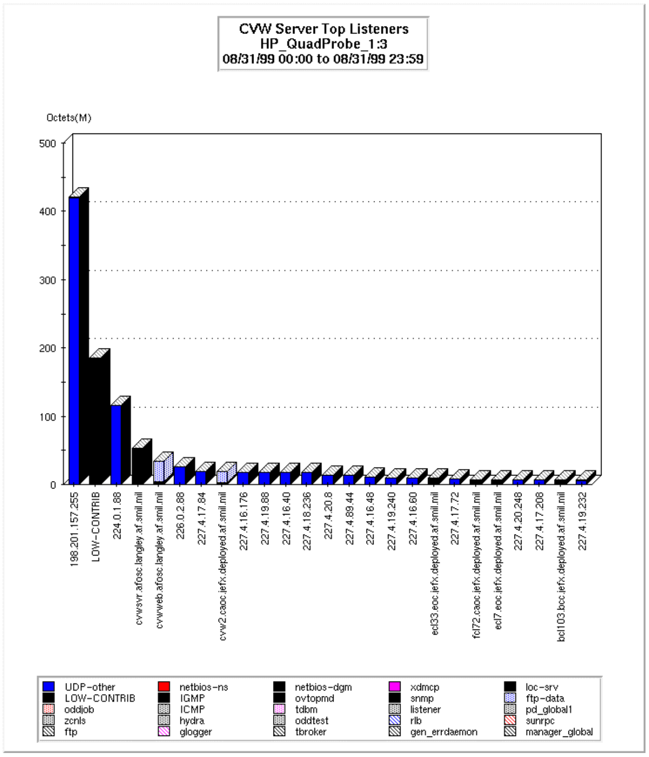


Figure D.6 - CVW Server Top Listeners (RMON2 Probe) – 31 August 1999 EDT (LiveFly Day 2)

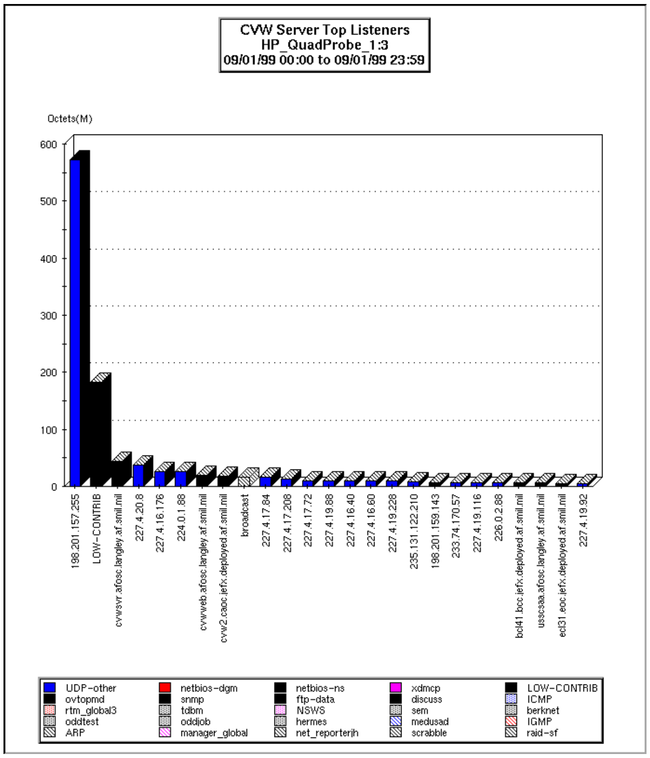


Figure D.7 - CVW Server Top Listeners (RMON2 Probe) – 1 September 1999 EDT (LiveFly Day 3)

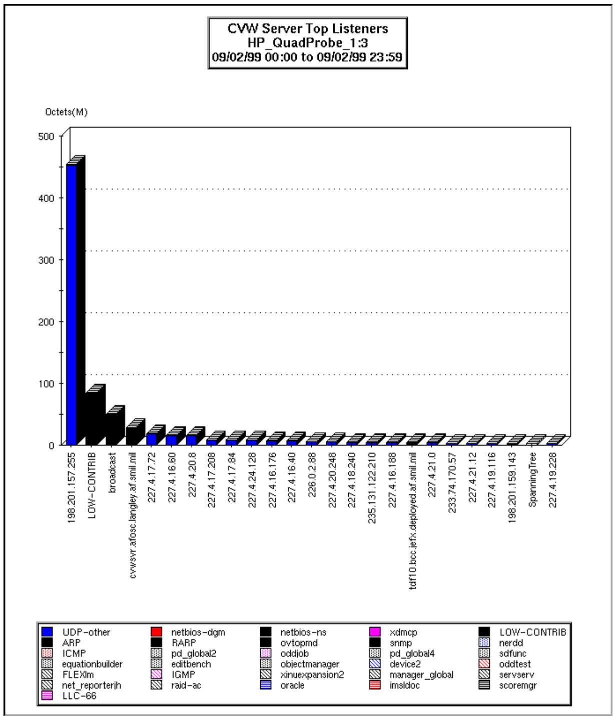


Figure D.8 - CVW Server Top Listeners (RMON2 Probe) – 2 September 1999 EDT (LiveFly Day 4)

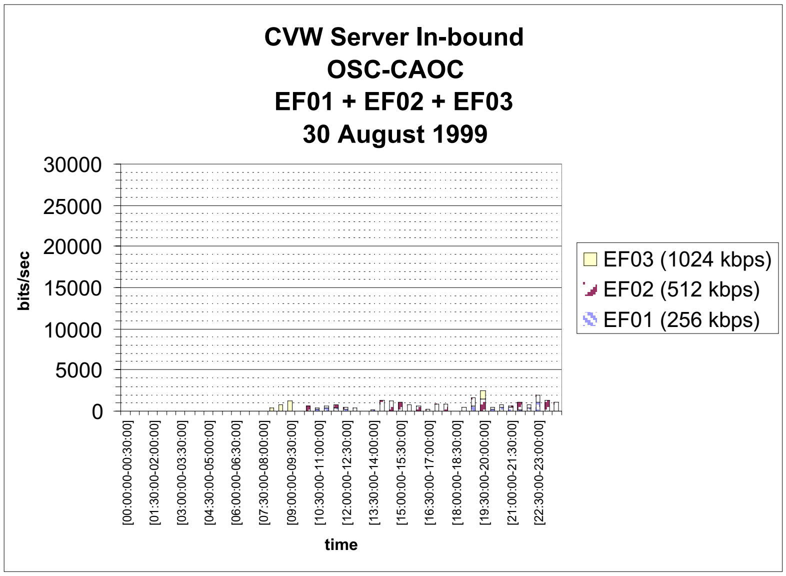


Figure D.9 - CVW Server OSC-CAOC In-bound traffic (RMON2 Probe) – 30 August 1999 EDT (LiveFly Day 1)

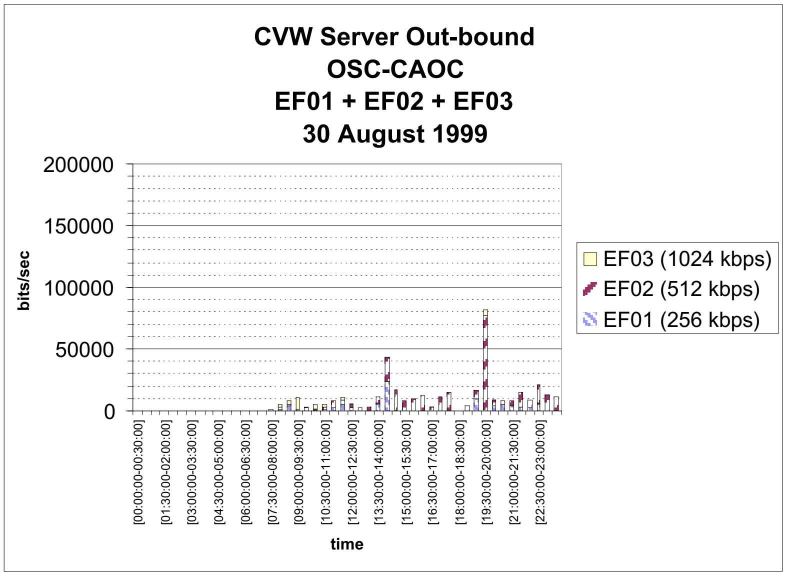


Figure D.10 - CVW Server OSC-CAOC Out-bound traffic (RMON2 Probe) – 30 August 1999 EDT (LiveFly Day 1)

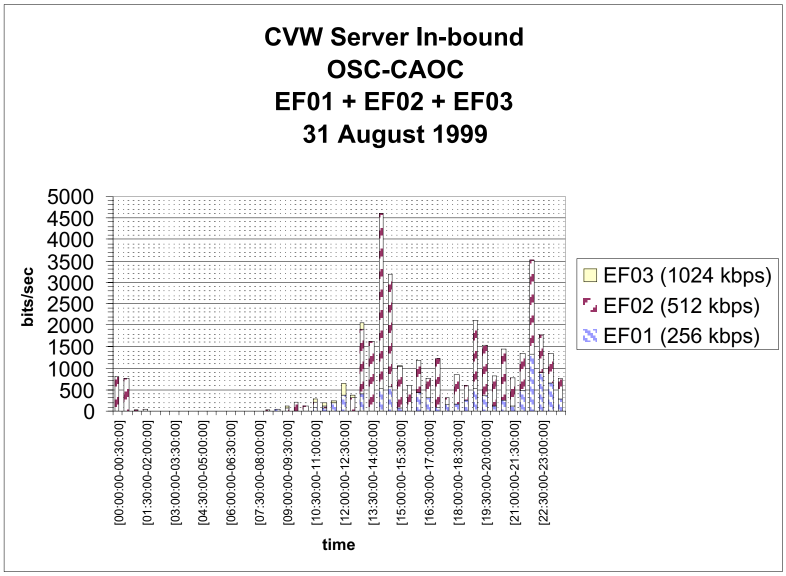


Figure D.11 - CVW Server OSC-CAOC In-bound traffic (RMON2 Probe) – 31 August 1999 EDT (LiveFly Day 2)

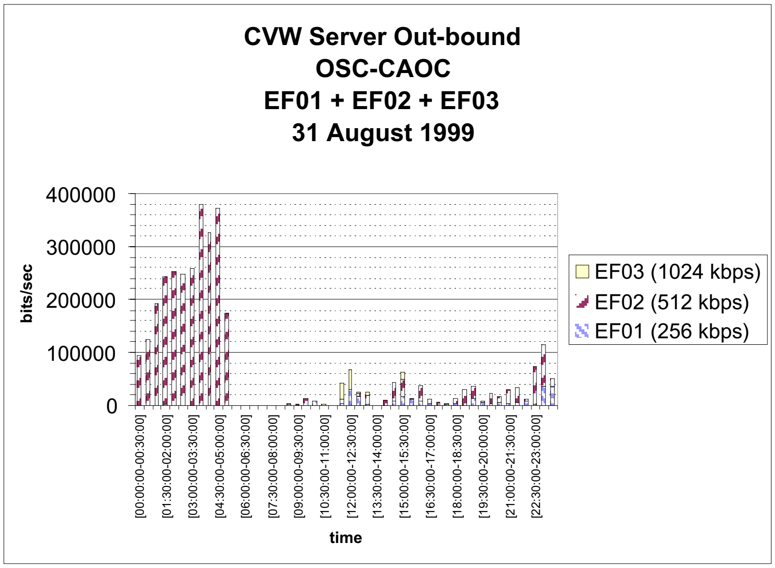


Figure D.12 - CVW Server OSC-CAOC Out-bound traffic (RMON2 Probe) – 31 August 1999 EDT (LiveFly Day 2)

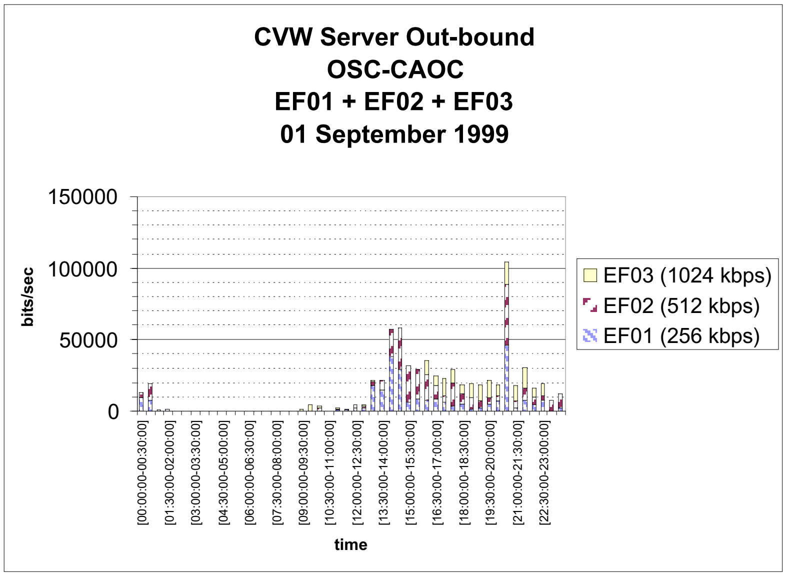


Figure D.13 - CVW Server OSC-CAOC In-bound traffic (RMON2 Probe) – 1 September 1999 EDT (LiveFly Day 3)

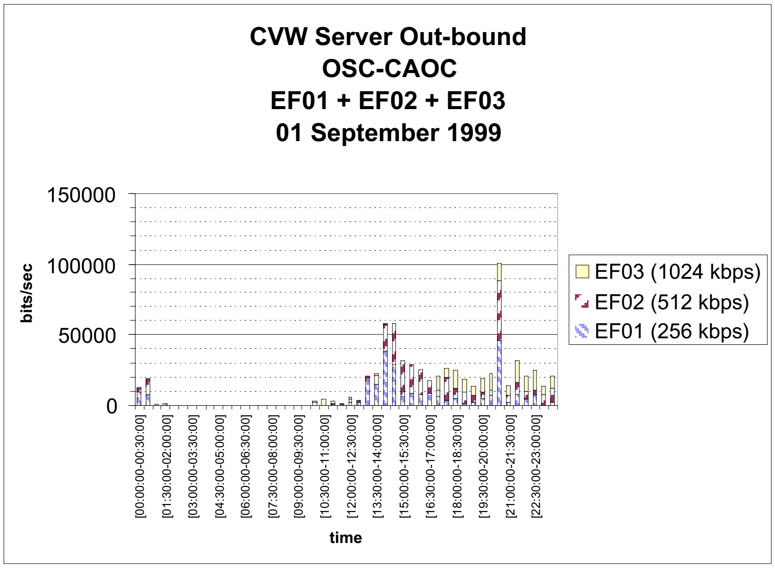


Figure D.14 - CVW Server OSC-CAOC Out-bound traffic (RMON2 Probe) – 1 September 1999 EDT (LiveFly Day 3)

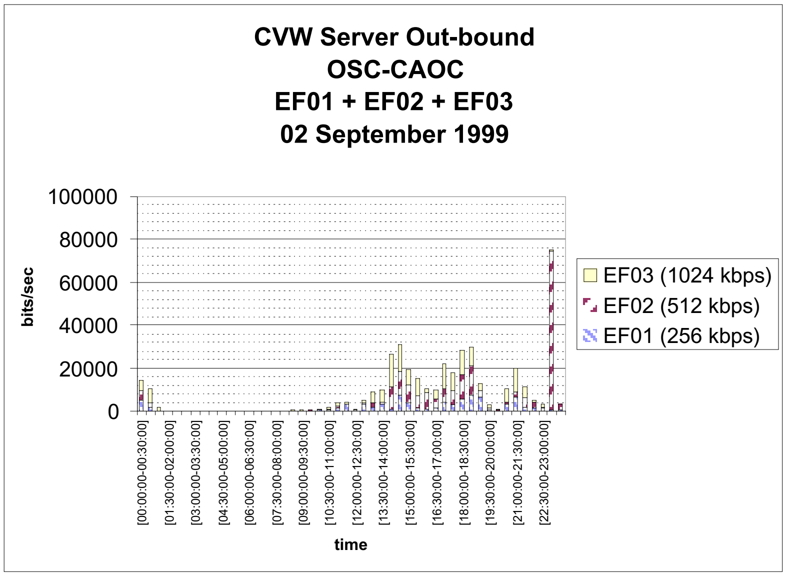


Figure D.15 - CVW Server OSC-CAOC In-bound traffic (RMON2 Probe) – 2 September 1999 EDT (LiveFly Day 4)

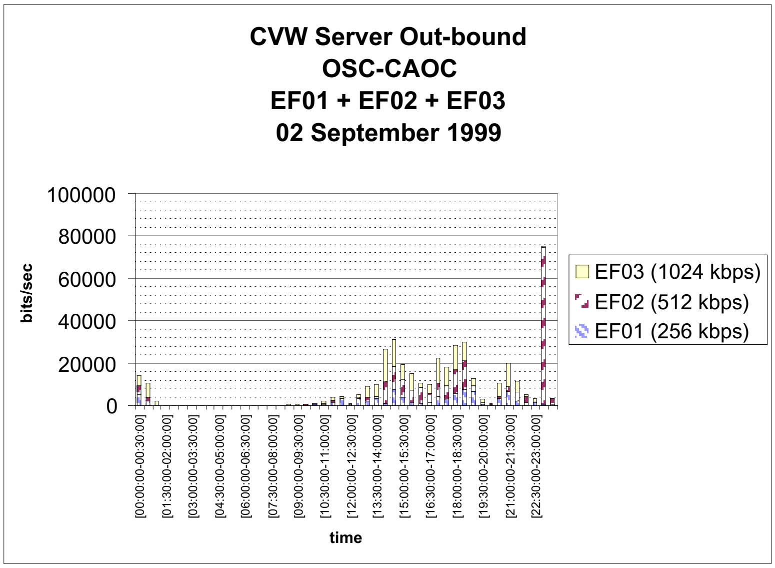


Figure D.16 - CVW Server OSC-CAOC Out-bound traffic (RMON2 Probe) – 2 September 1999 EDT (LiveFly Day 4)

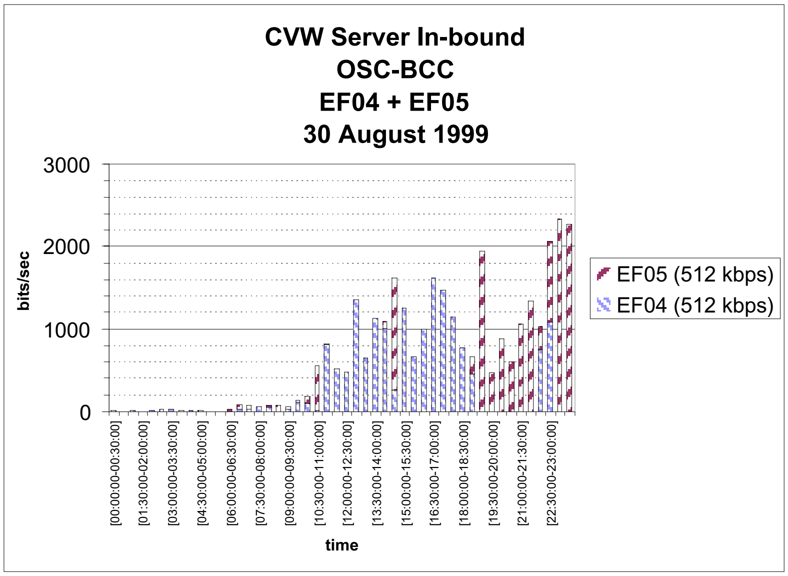


Figure D.17 - CVW Server OSC-BCC In-bound traffic (RMON2 Probe) – 30 August 1999 EDT (LiveFly Day 1)

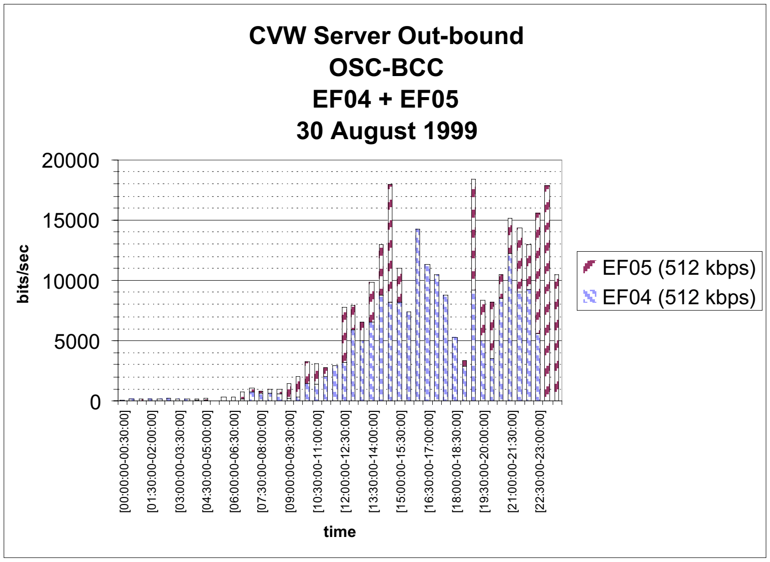


Figure D.18 - CVW Server OSC-BCC Out-bound traffic (RMON2 Probe) – 30 August 1999 EDT (LiveFly Day 1)

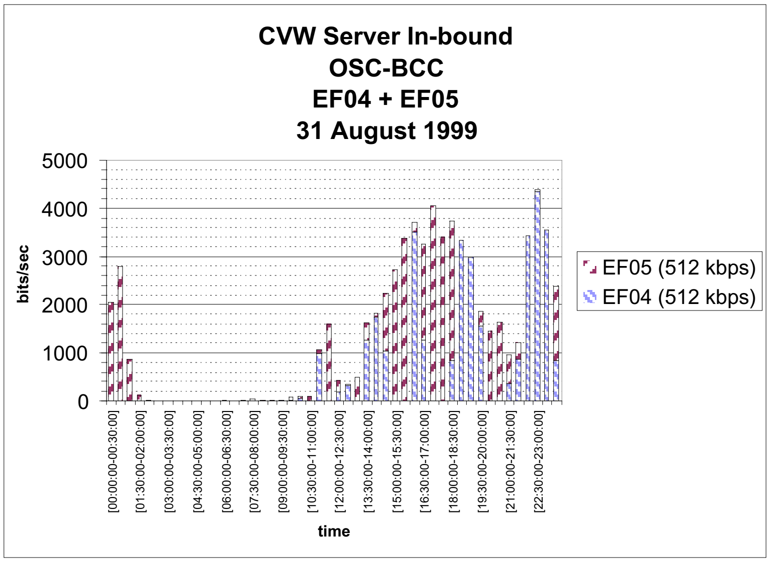


Figure D.19 - CVW Server OSC-BCC In-bound traffic (RMON2 Probe) – 31 August 1999 EDT (LiveFly Day 2)

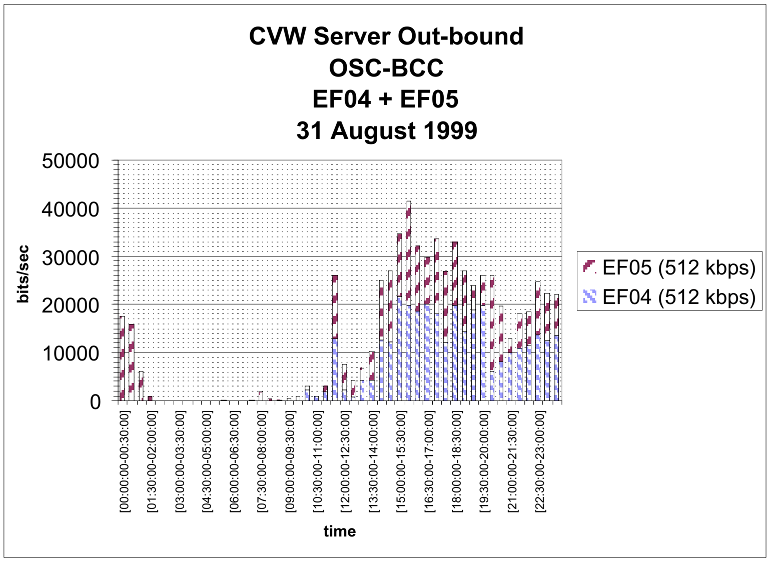


Figure D.20 - CVW Server OSC-BCC Out-bound traffic (RMON2 Probe) – 31 August 1999 EDT (LiveFly Day 2)

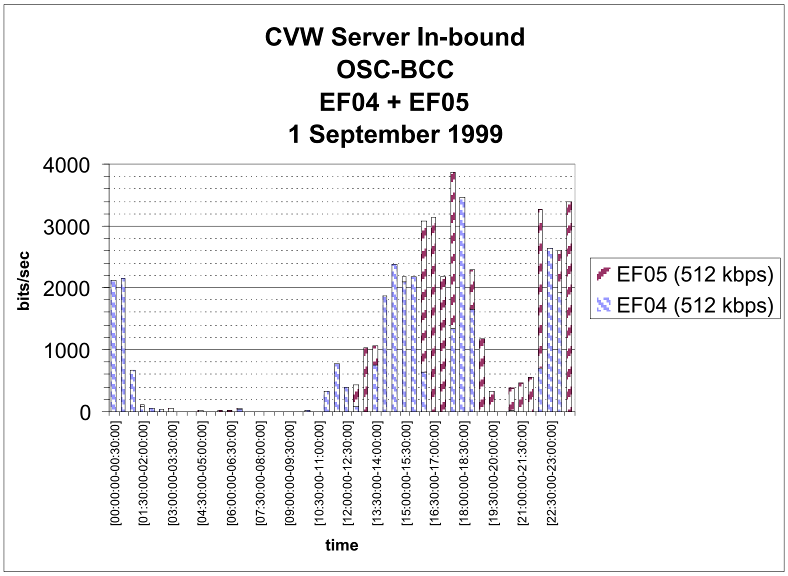


Figure D.21 - CVW Server OSC-BCC In-bound traffic (RMON2 Probe) – 1 September 1999 EDT (LiveFly Day 3)

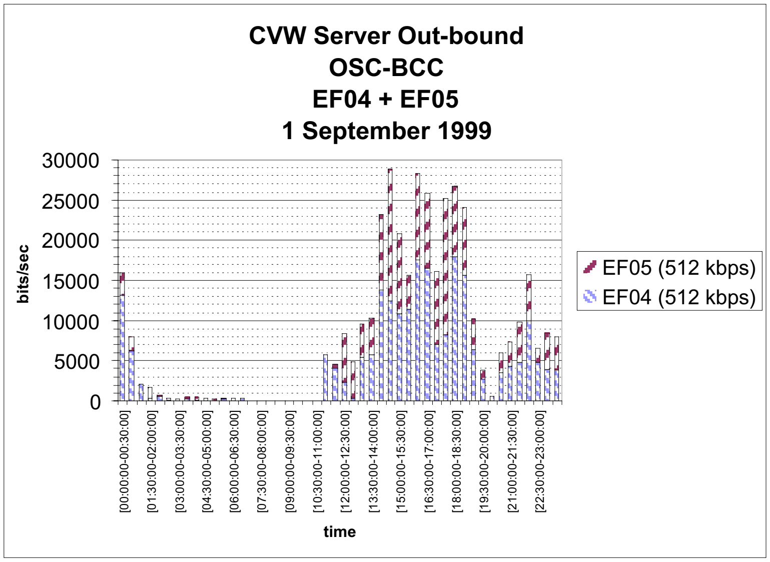


Figure D.22 - CVW Server OSC-BCC Out-bound traffic (RMON2 Probe) – 1 September 1999 EDT (LiveFly Day 3)

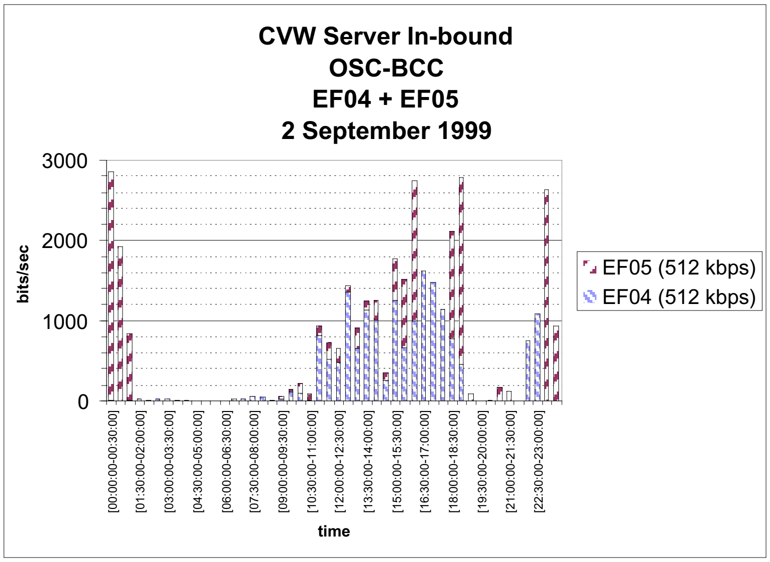


Figure D.23 - CVW Server OSC-BCC In-bound traffic (RMON2 Probe) – 2 September 1999 EDT (LiveFly Day 4)

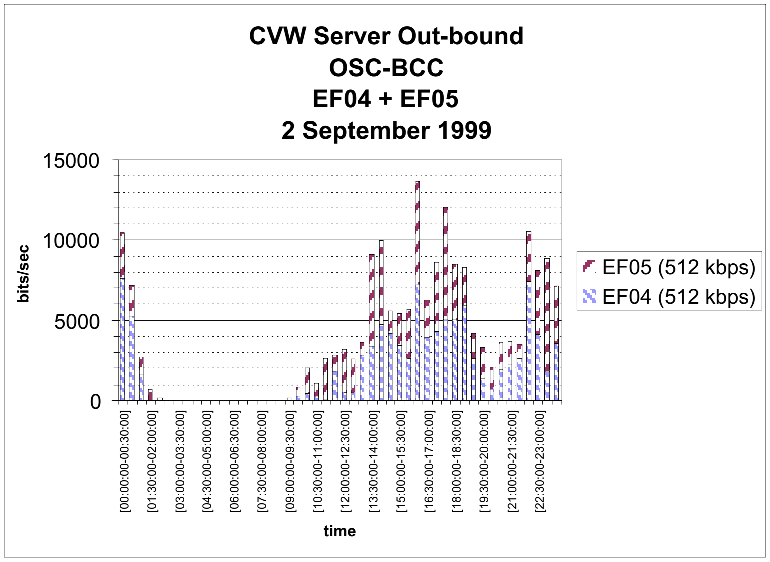


Figure D.24 - CVW Server OSC-BCC Out-bound traffic (RMON2 Probe) – 2 September 1999 EDT (LiveFly Day 4)

CVW Document Server

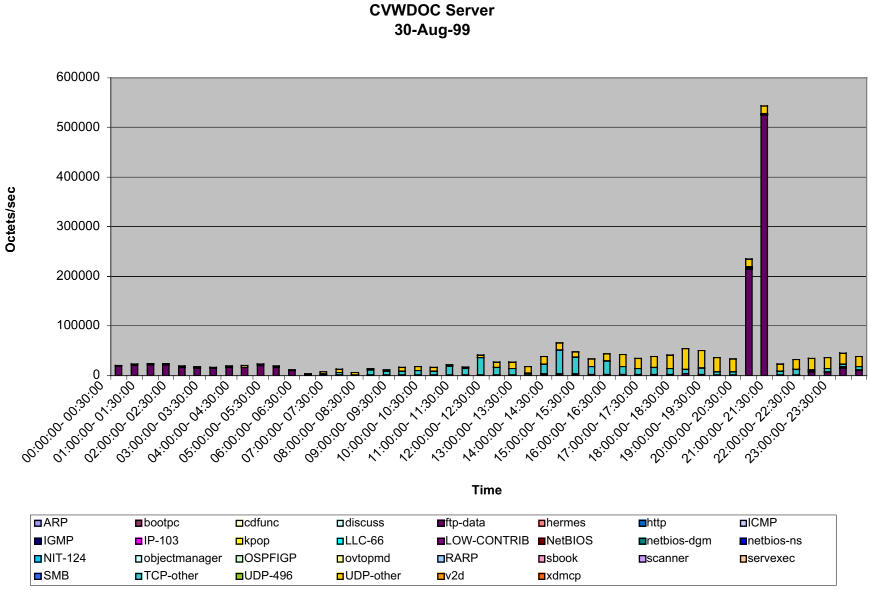


Figure D.25 - CVW Doc Server Network Traffic Profile (RMON2 Probe) – 30 August 1999 EDT (LiveFly Day 1)

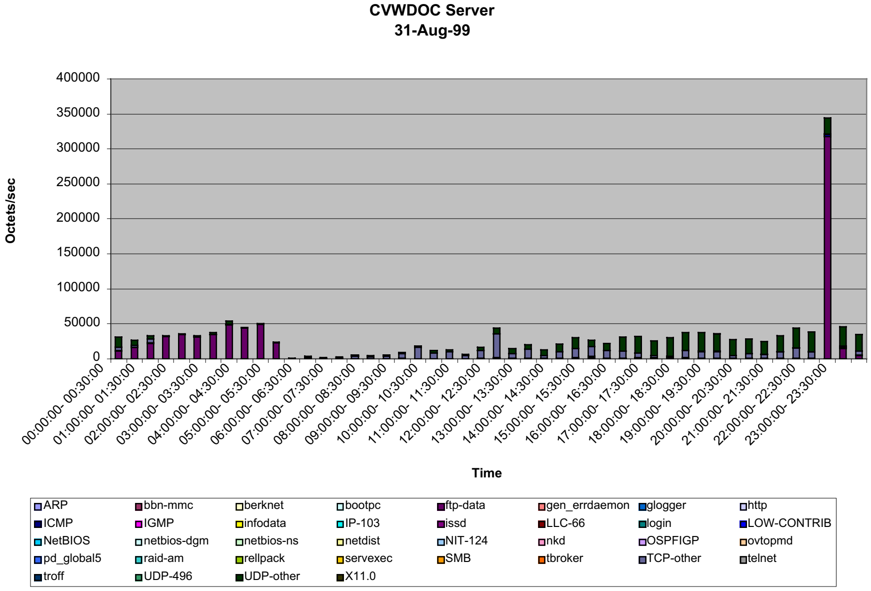


Figure D.26 - CVW Doc Server Network Traffic Profile (RMON2 Probe) – 31 August 1999 EDT (LiveFly Day 2)

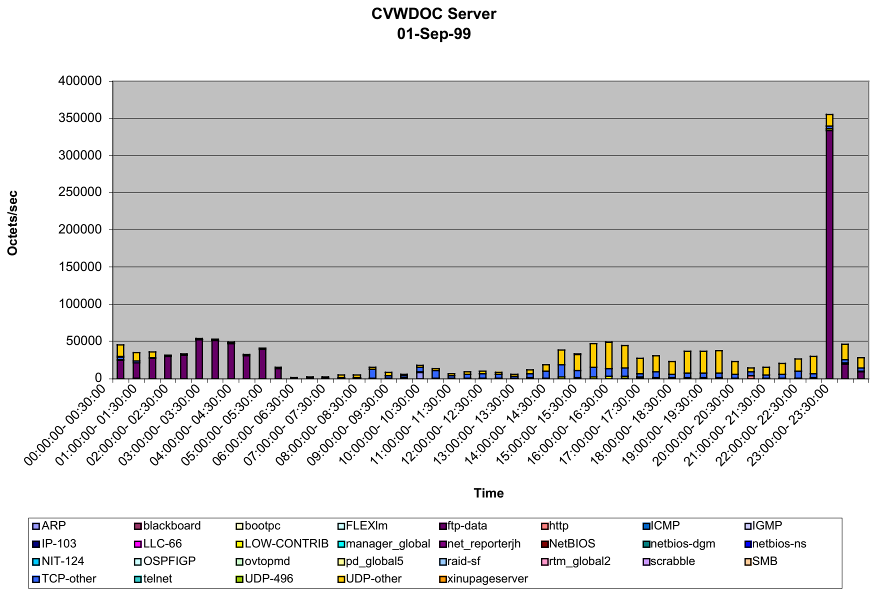


Figure D.27 - CVW Doc Server Network Traffic Profile (RMON2 Probe) – 1 September 1999 EDT (LiveFly Day 3)

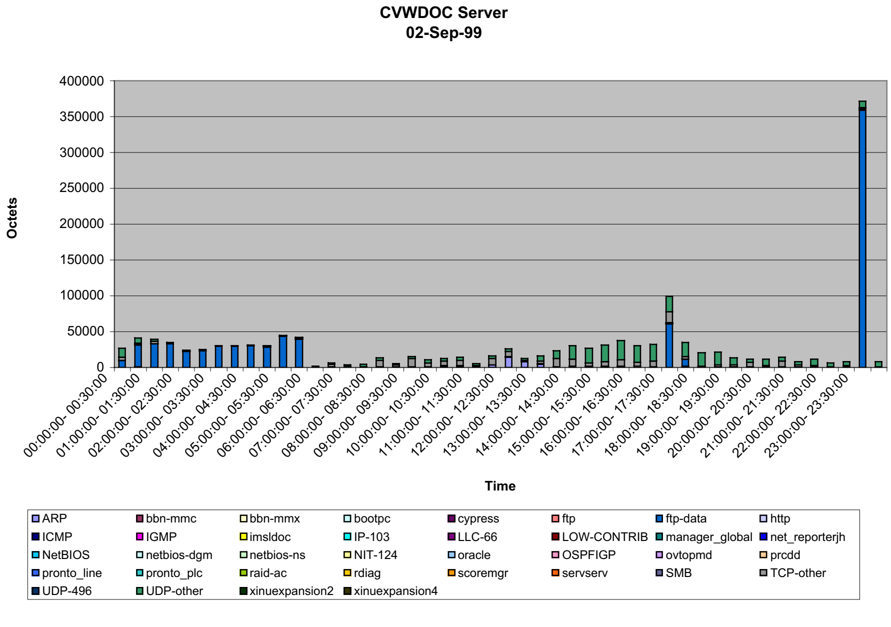


Figure D.28 - CVW Doc Server Network Traffic Profile (RMON2 Probe) – 2 September 1999 EDT (LiveFly Day 4)

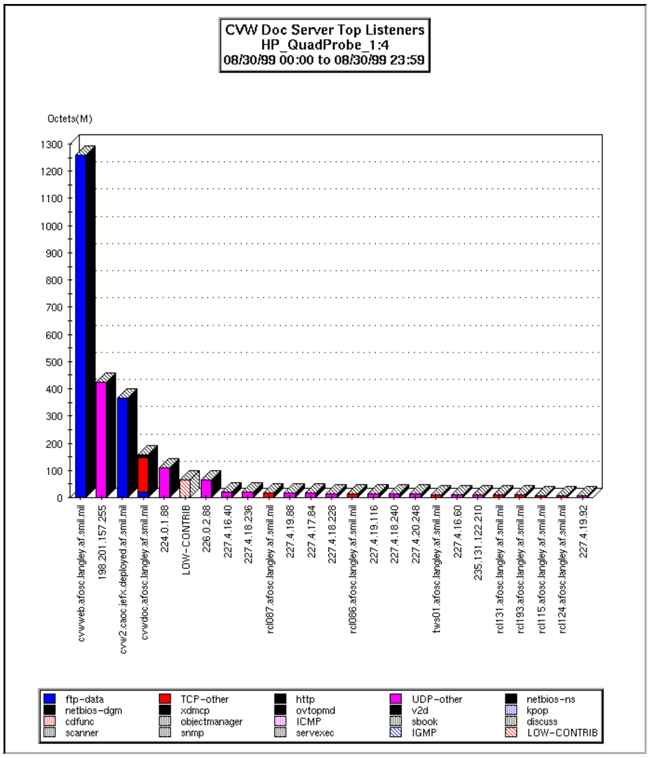


Figure D.29 - CVW Doc Server Top Listeners (RMON2 Probe) – 30 August 1999 EDT (LiveFly Day 1)

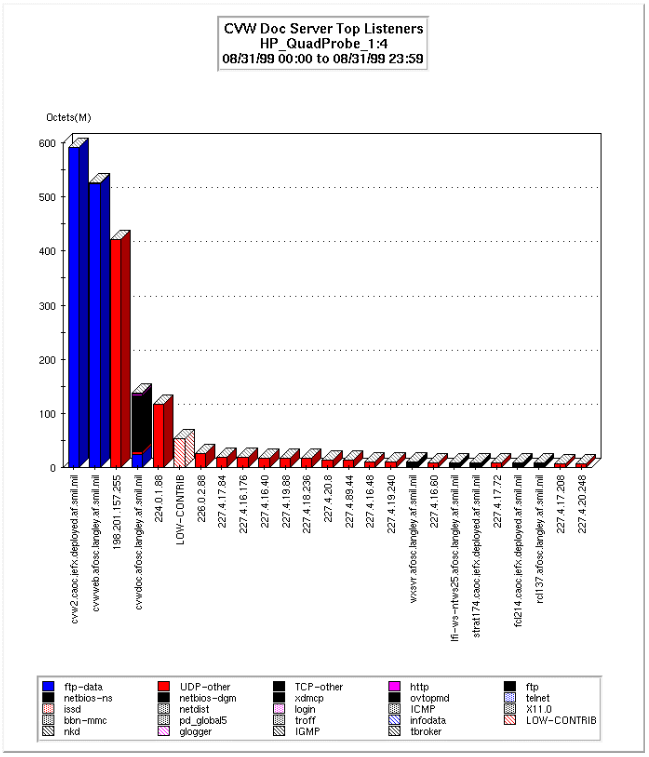


Figure D.30 - CVW Doc Server Top Listeners (RMON2 Probe) – 31 August 1999 EDT (LiveFly Day 2)

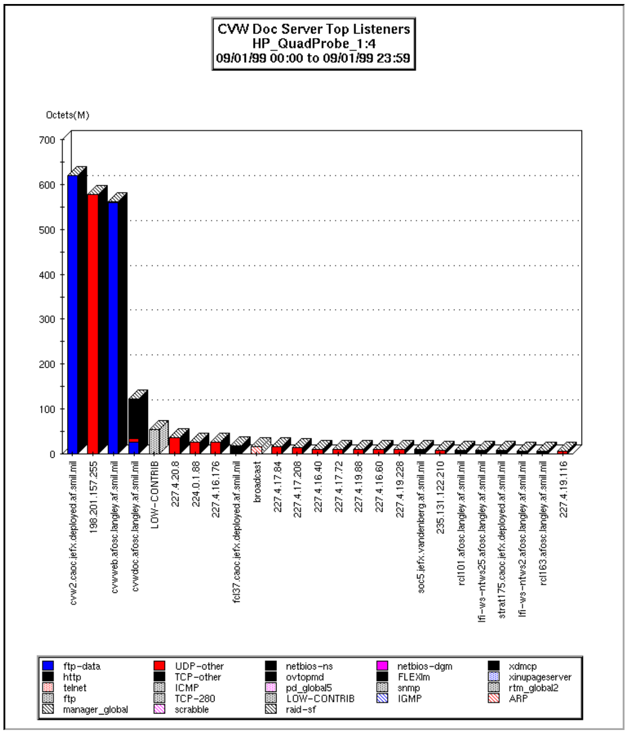


Figure D.31 - CVW Doc Server Top Listeners (RMON2 Probe) – 1 September 1999 EDT (LiveFly Day 3)

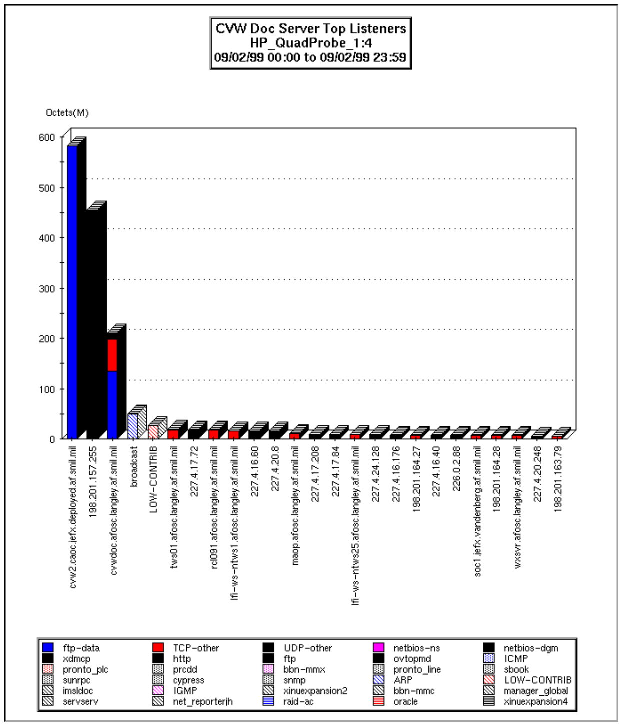


Figure D.32 - CVW Doc Server Top Listeners (RMON2 Probe) – 2 September 1999 EDT (LiveFly Day 4)

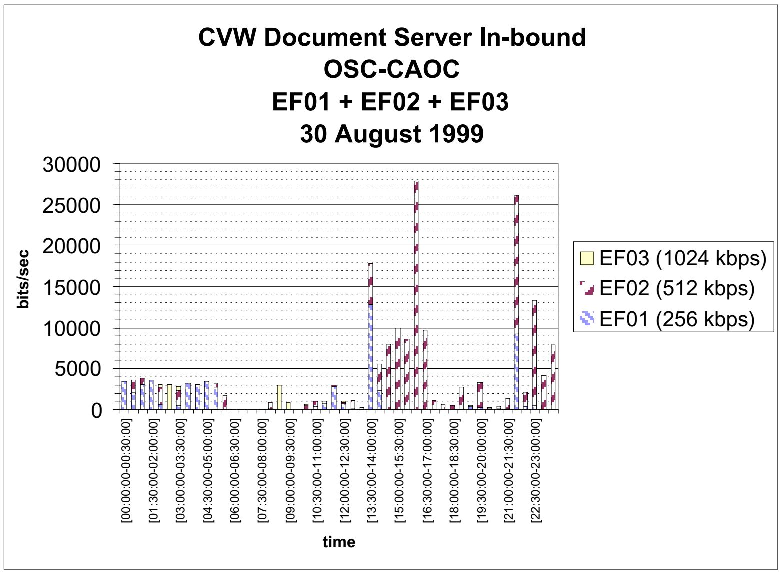


Figure D.33 - CVW Doc Server OSC-CAOC In-bound traffic (RMON2 Probe) – 30 August 1999 EDT (LiveFly Day 1)

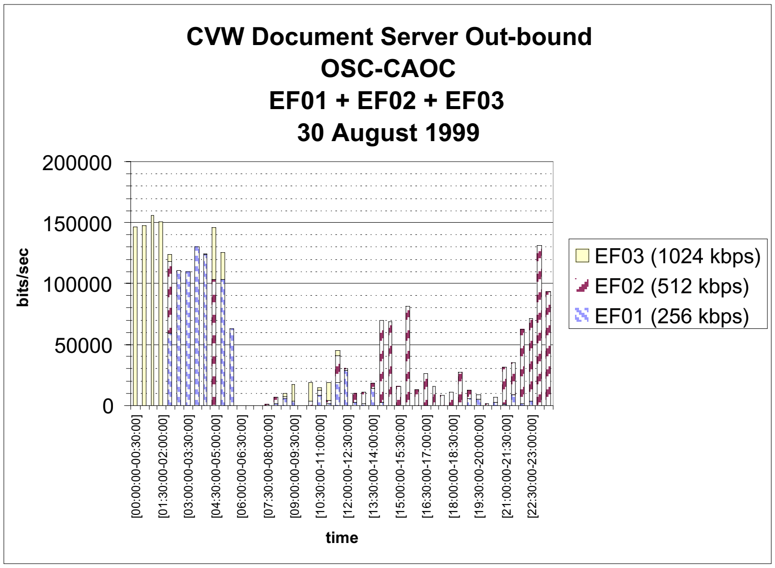


Figure D.34 - CVW Doc Server OSC-CAOC Out-bound traffic (RMON2 Probe) – 30 August 1999 EDT (LiveFly Day 1)

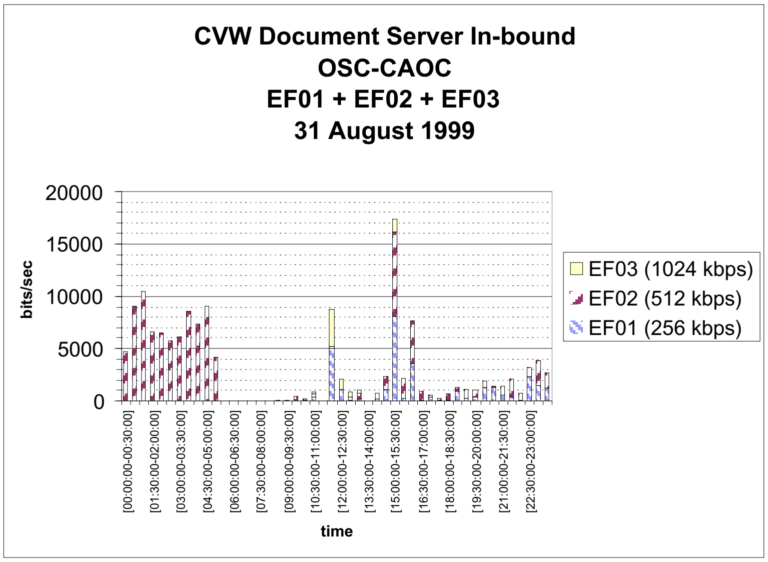


Figure D.35 - CVW Doc Server OSC-CAOC In-bound traffic (RMON2 Probe) – 31 August 1999 EDT (LiveFly Day 2)

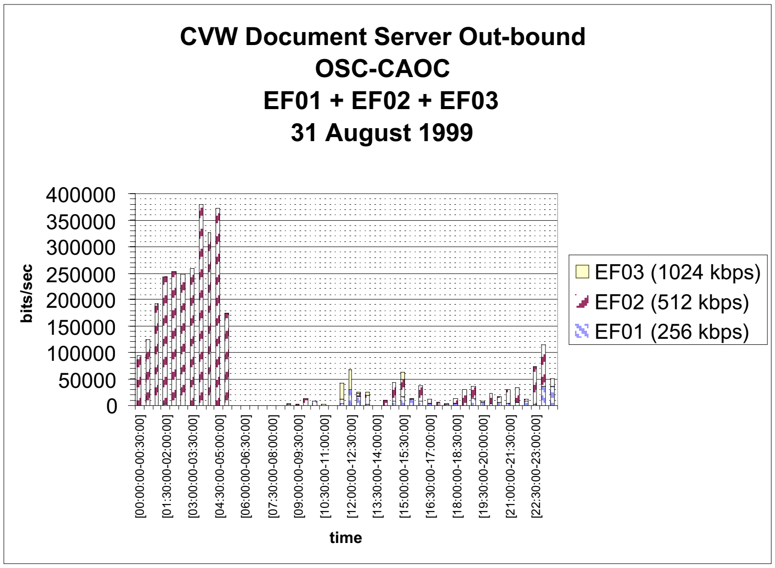


Figure D.36 - CVW Doc Server OSC-CAOC Out-bound traffic (RMON2 Probe) – 31 August 1999 EDT (LiveFly Day 2)

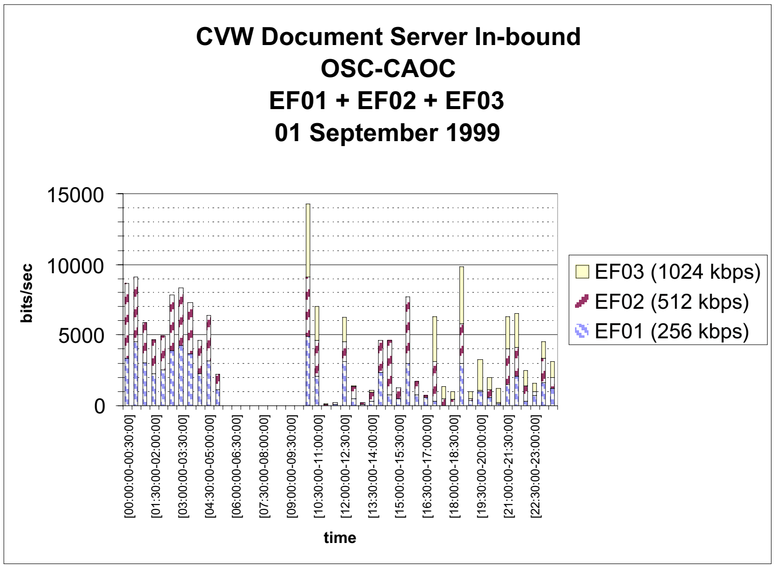


Figure D.37 - CVW Doc Server OSC-CAOC In-bound traffic (RMON2 Probe) – 1 September 1999 EDT (LiveFly Day 3)

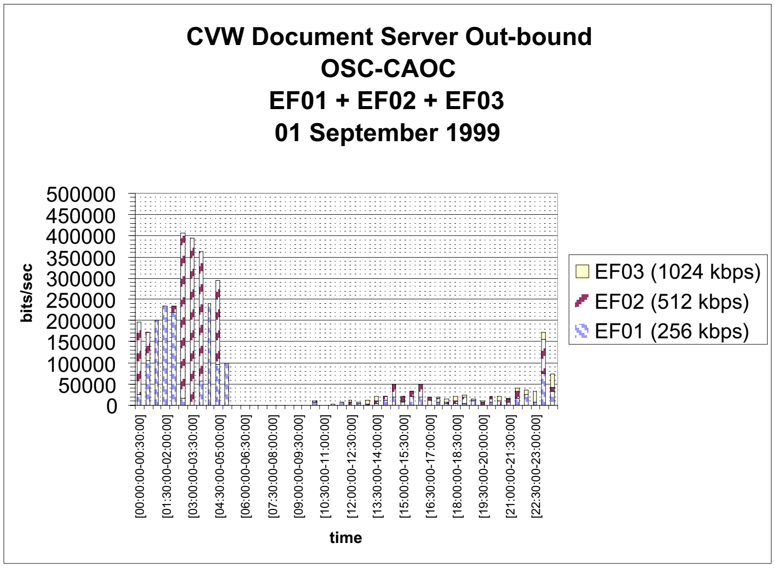


Figure D.38 - CVW Doc Server OSC-CAOC Out-bound traffic (RMON2 Probe) – 1 September 1999 EDT (LiveFly Day 3)

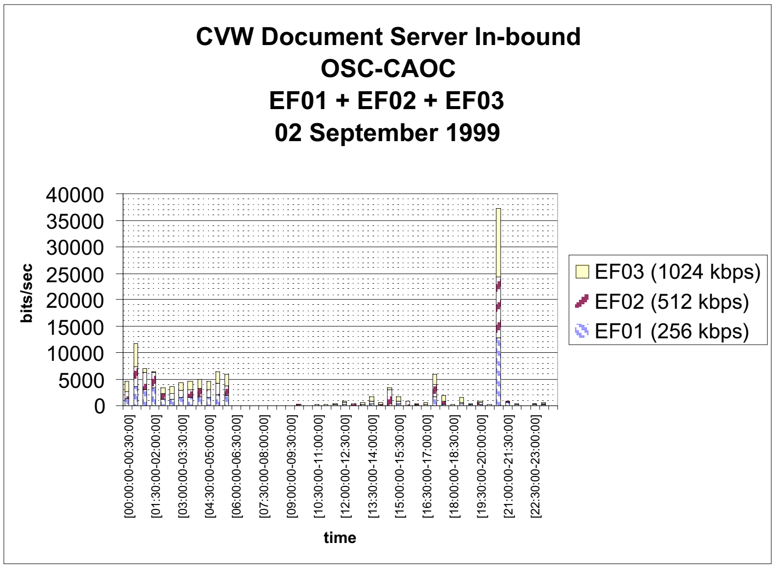


Figure D.39 - CVW Doc Server OSC-CAOC In-bound traffic (RMON2 Probe) – 2 September 1999 EDT (LiveFly Day 4)

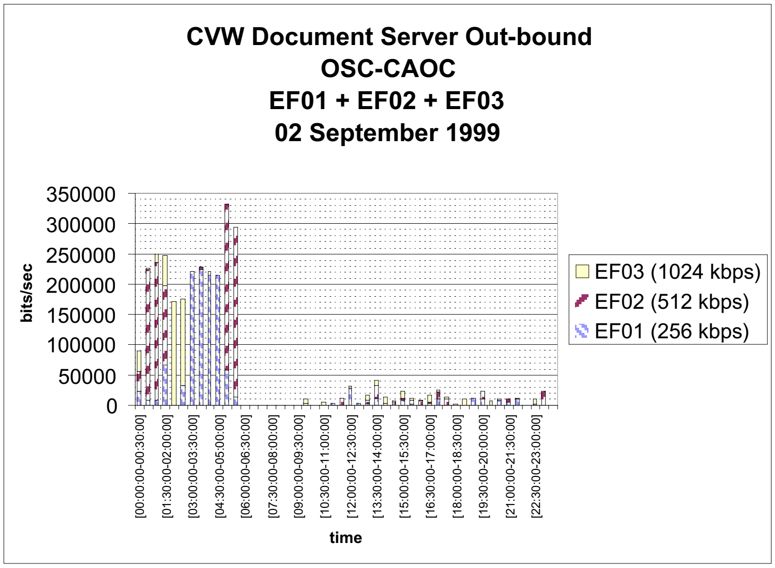


Figure D.40 - CVW Doc Server OSC-CAOC Out-bound traffic (RMON2 Probe) – 2 September 1999 EDT (LiveFly Day 4)

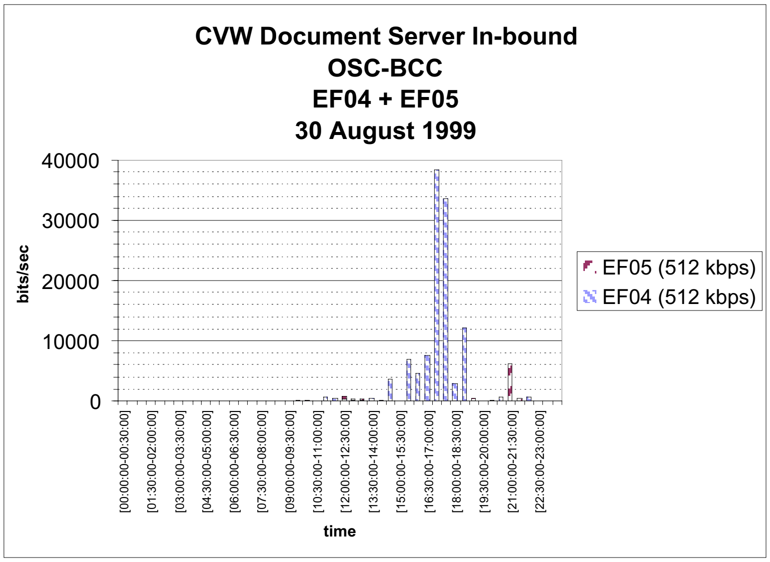


Figure D.41 - CVW Doc Server OSC-BCC In-bound traffic (RMON2 Probe) – 30 August 1999 EDT (LiveFly Day 1)

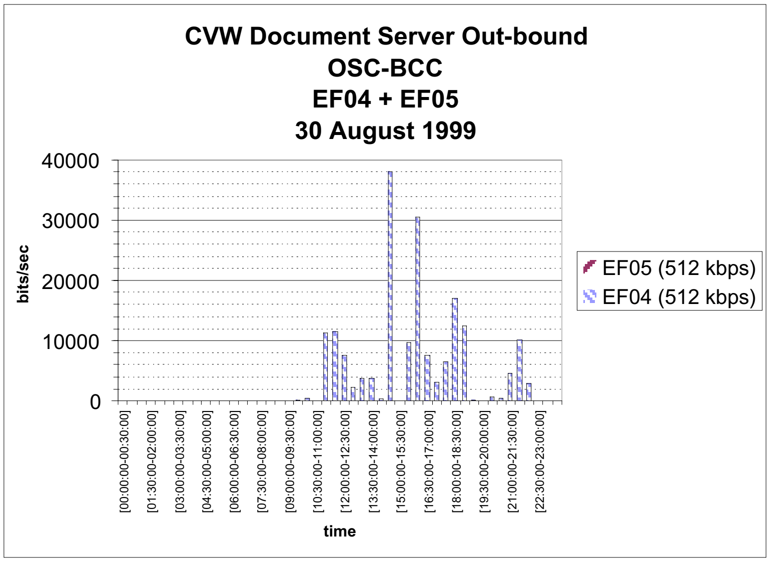


Figure D.42 - CVW Doc Server OSC-BCC Out-bound traffic (RMON2 Probe) – 30 August 1999 EDT (LiveFly Day 1)

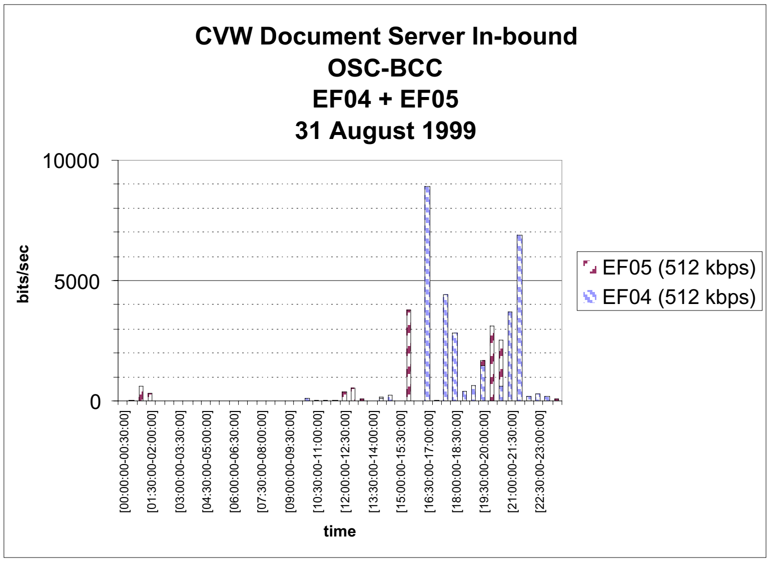


Figure D.43 - CVW Doc Server OSC-BCC In-bound traffic (RMON2 Probe) – 31 August 1999 EDT (LiveFly Day 2)

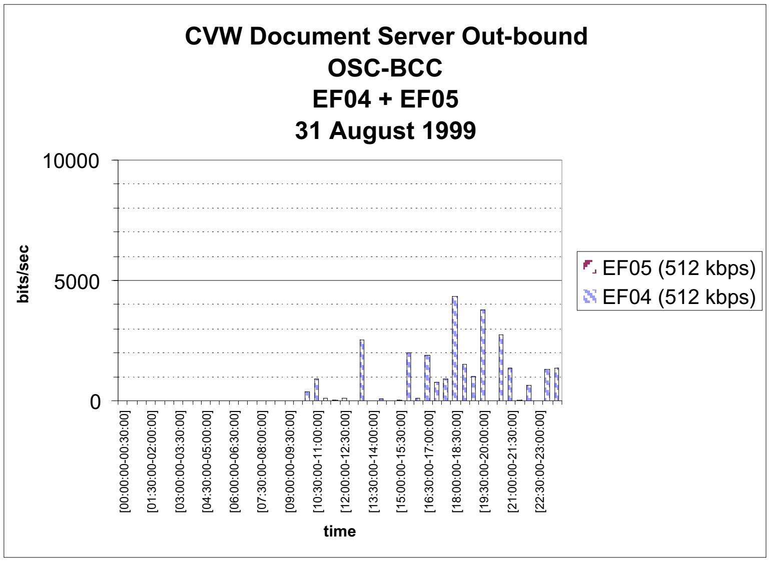


Figure D.44 - CVW Doc Server OSC-BCC Out-bound traffic (RMON2 Probe) – 31 August 1999 EDT (LiveFly Day 2)

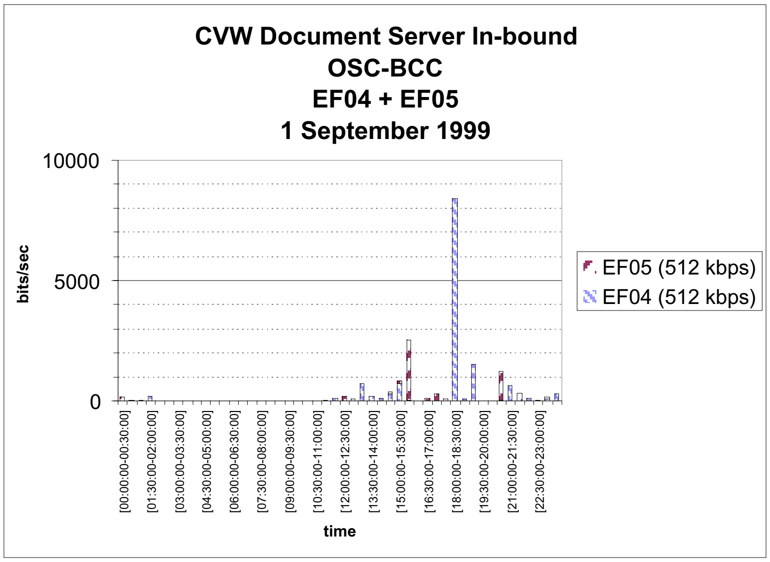


Figure D.45 - CVW Doc Server OSC-BCC In-bound traffic (RMON2 Probe) – 1 September 1999 EDT (LiveFly Day 3)

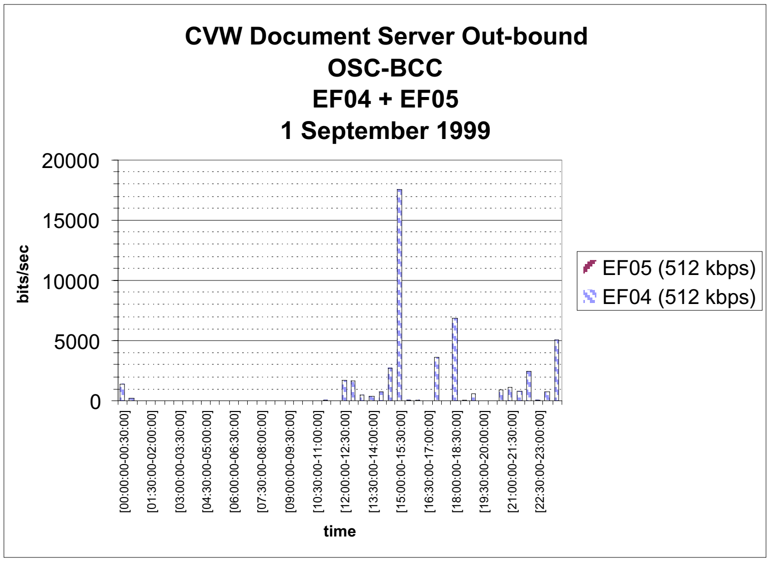


Figure D.46 - CVW Doc Server OSC-BCC Out-bound traffic (RMON2 Probe) – 1 September 1999 EDT (LiveFly Day 3)

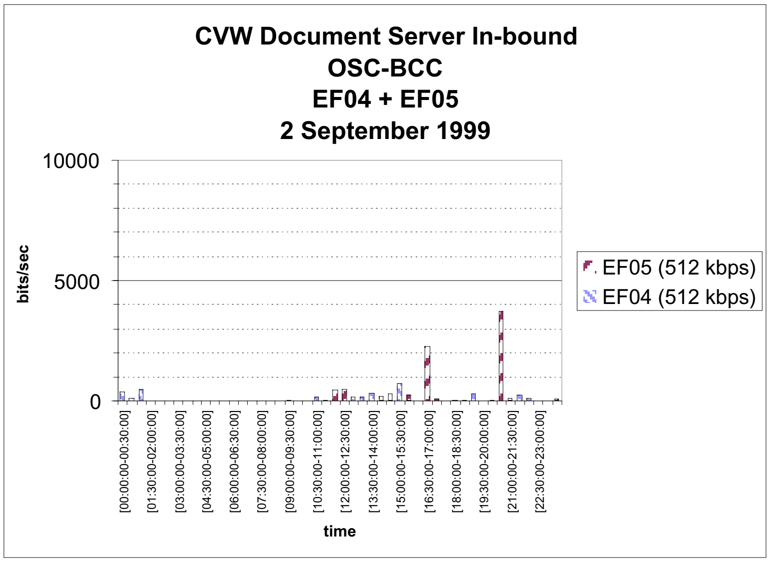


Figure D.47 - CVW Doc Server OSC-BCC In-bound traffic (RMON2 Probe) – 2 September 1999 EDT (LiveFly Day 4)

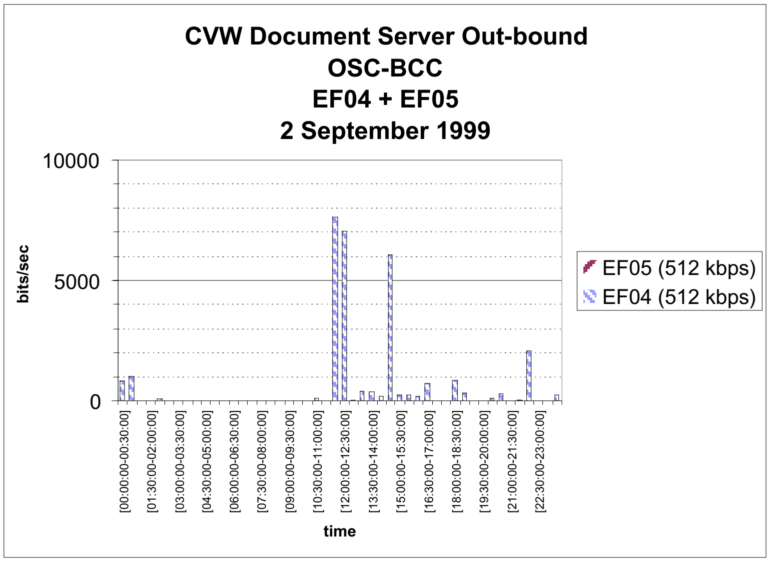


Figure D.48 - CVW Doc Server OSC-BCC Out-bound traffic (RMON2 Probe) – 2 September 1999 EDT (LiveFly Day 4)

CVW Web Server

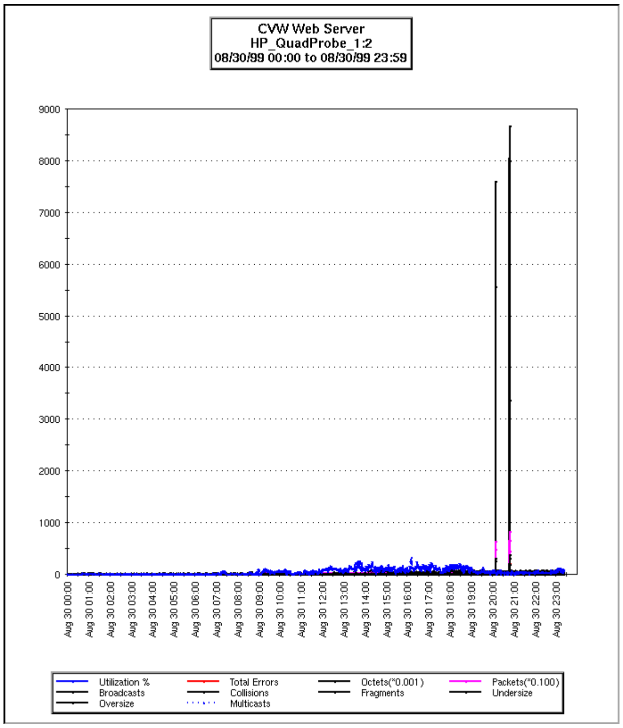


Figure D.49 - CVW Web Server Network Traffic (RMON2 Probe) – 30 August 1999 EDT (LiveFly Day 1)

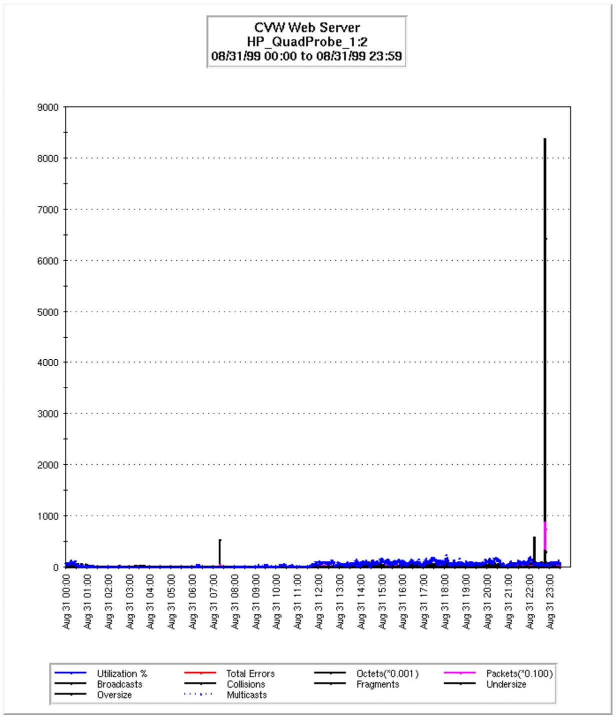


Figure D.50 - CVW Web Server Network Traffic (RMON2 Probe) – 31 August 1999 EDT (LiveFly Day 2)

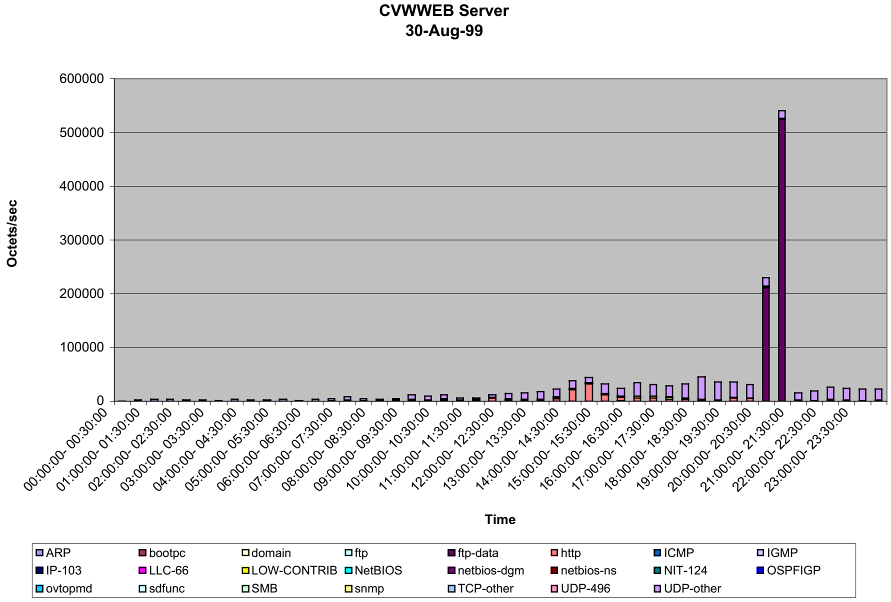


Figure D.51 - CVW Web Server Network Traffic Profile (RMON2 Probe) – 30 August 1999 EDT (LiveFly Day 1)

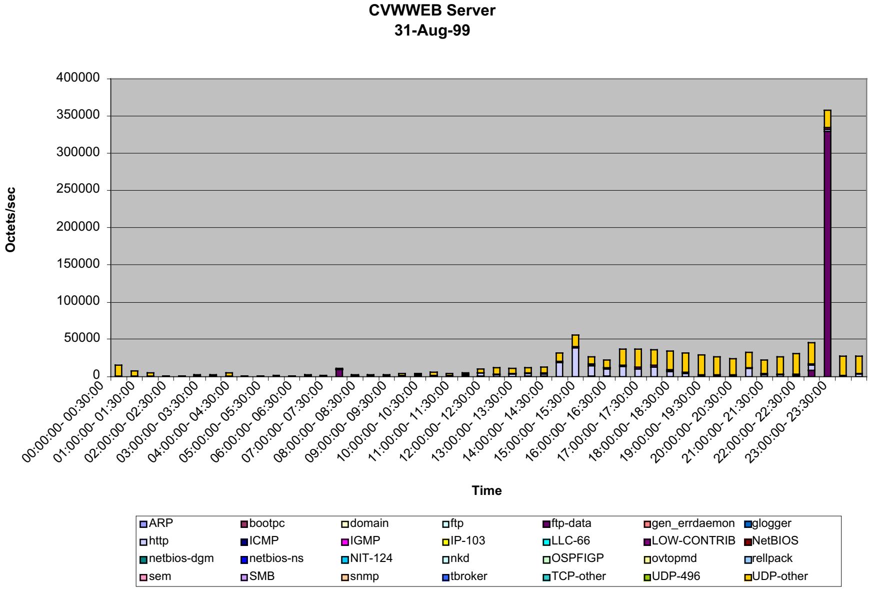


Figure D.52 - CVW Web Server Network Traffic Profile (RMON2 Probe) – 31 August 1999 EDT (LiveFly Day 2)

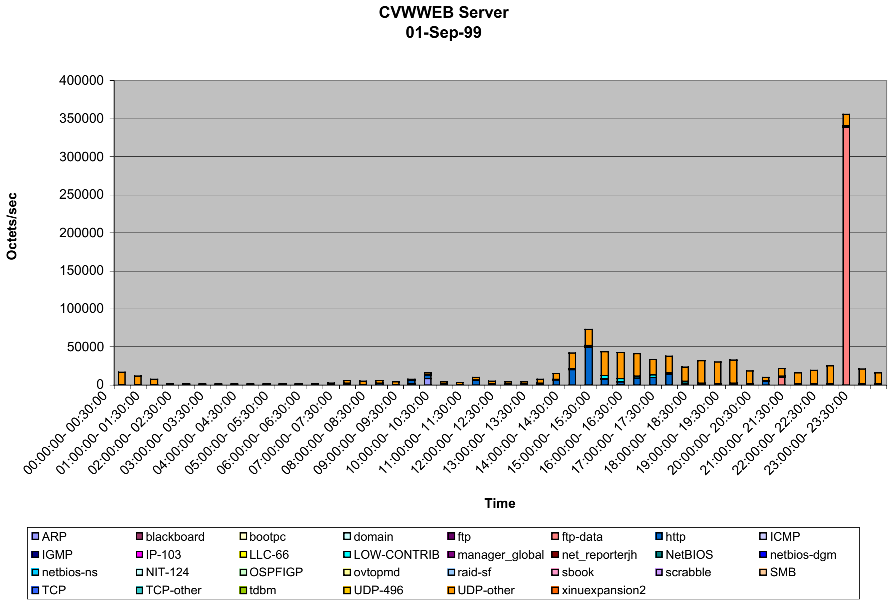


Figure D.53 - CVW Web Server Network Traffic Profile (RMON2 Probe) – 1 September 1999 EDT (LiveFly Day 3)

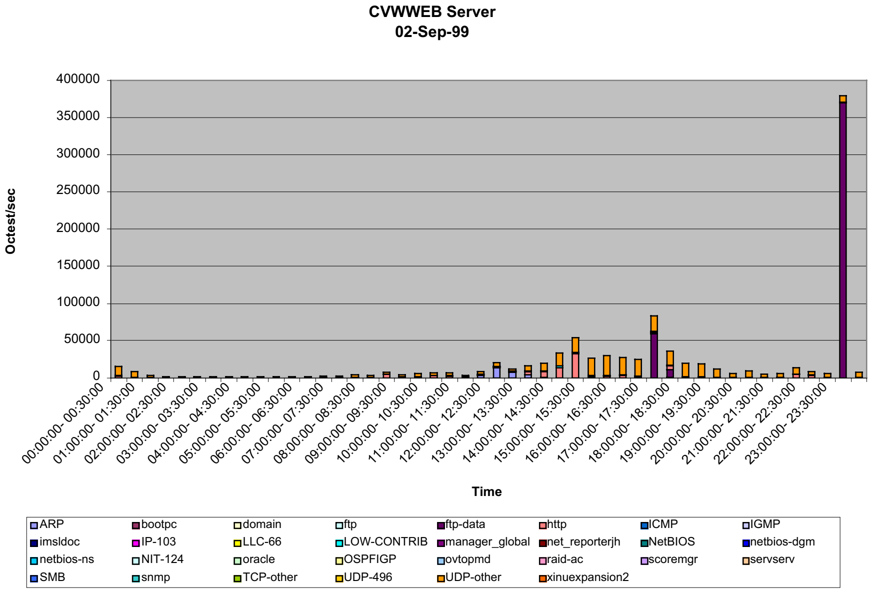


Figure D.54 - CVW Web Server Network Traffic Profile (RMON2 Probe) – 2 September 1999 EDT (LiveFly Day 4)

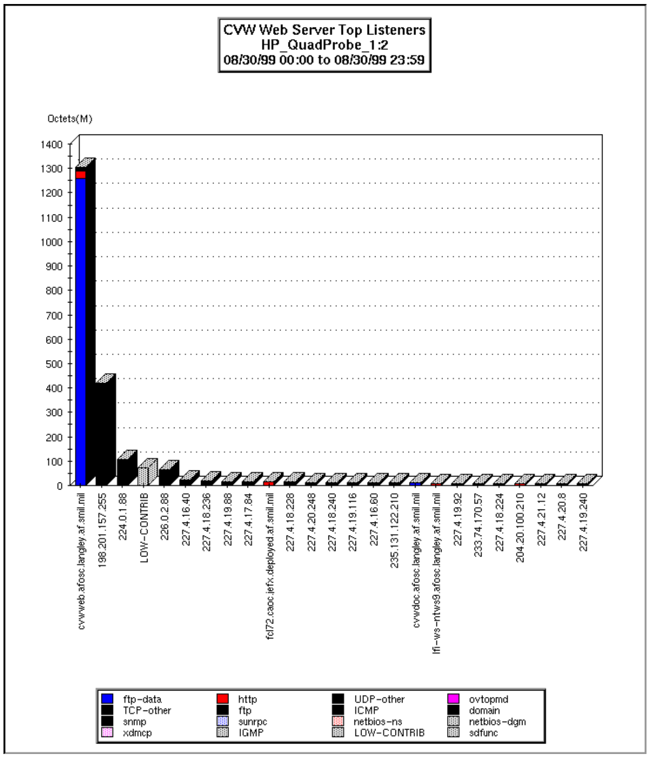


Figure D.55 - CVW Web Server Top Listeners (RMON2 Probe) – 30 August 1999 EDT (LiveFly Day 1)

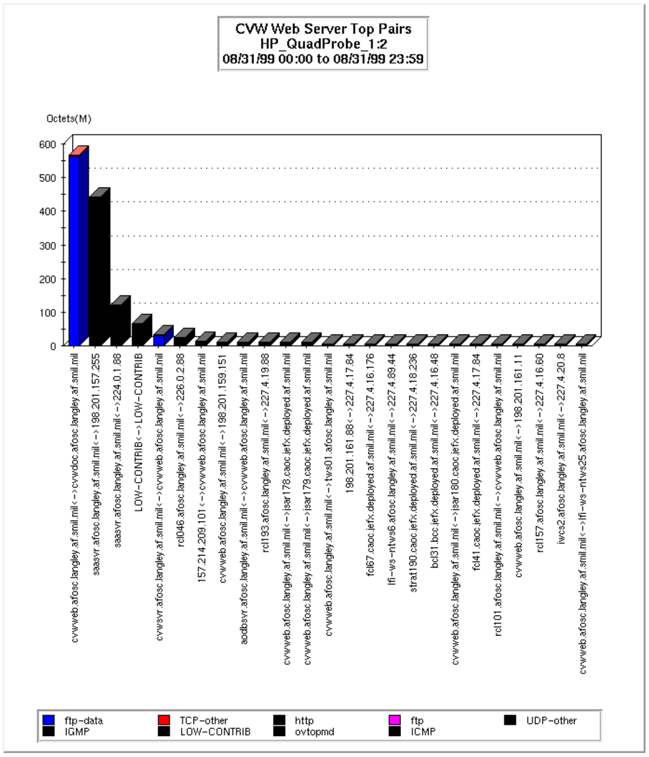


Figure D.56 - CVW Web Server Top Listeners (RMON2 Probe) – 31 August 1999 EDT (LiveFly Day 2)

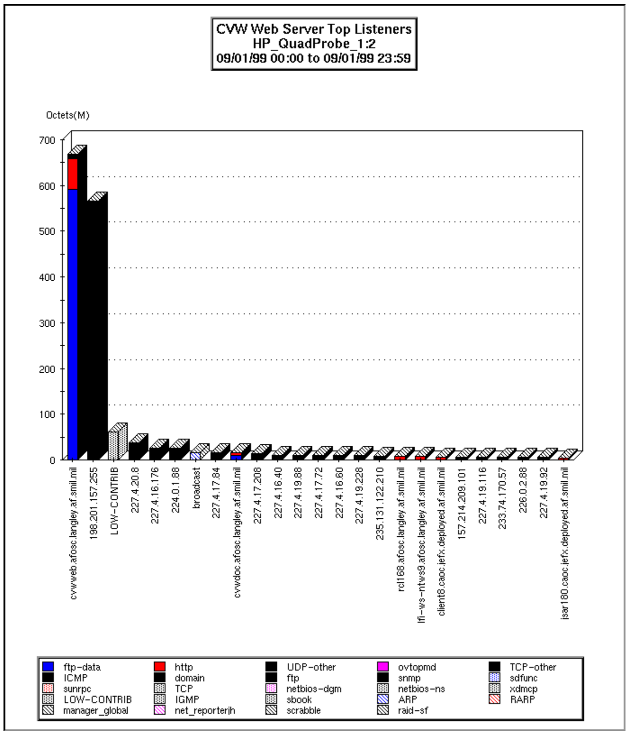


Figure D.57 - CVW Web Server Top Listeners (RMON2 Probe) – 1 September 1999 EDT (LiveFly Day 3)

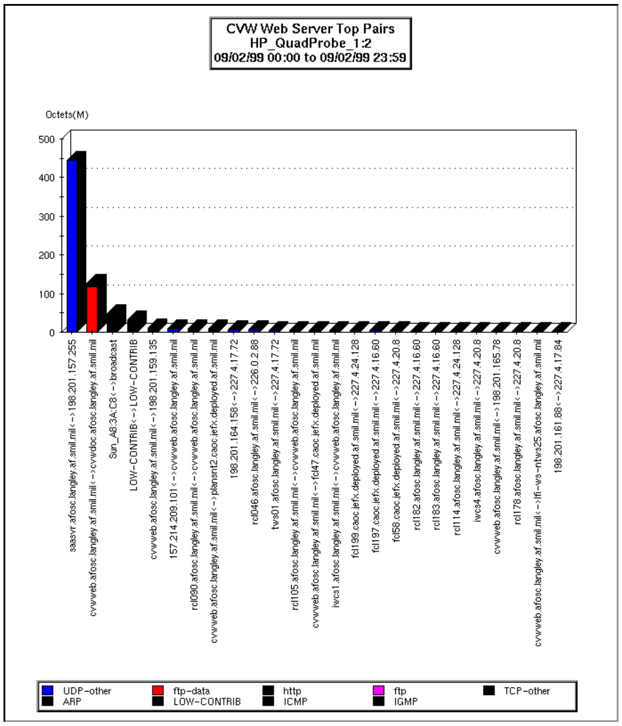


Figure D.58 - CVW Web Server Top Listeners (RMON2 Probe) – 2 September 1999 EDT (LiveFly Day 4)

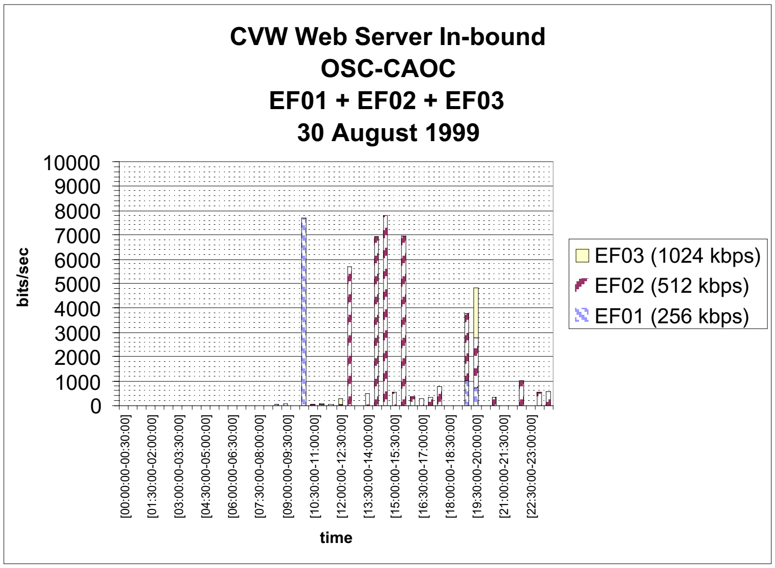


Figure D.59 - CVW Web Server OSC-CAOC In-bound traffic (RMON2 Probe) – 30 August 1999 EDT (LiveFly Day 1)

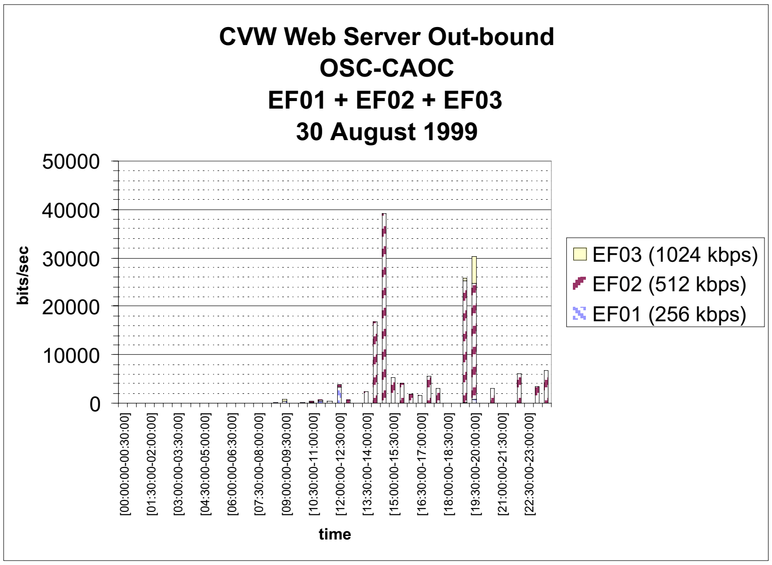


Figure D.60 - CVW Web Server OSC-CAOC Out-bound traffic (RMON2 Probe) – 30 August 1999 EDT (LiveFly Day 1)

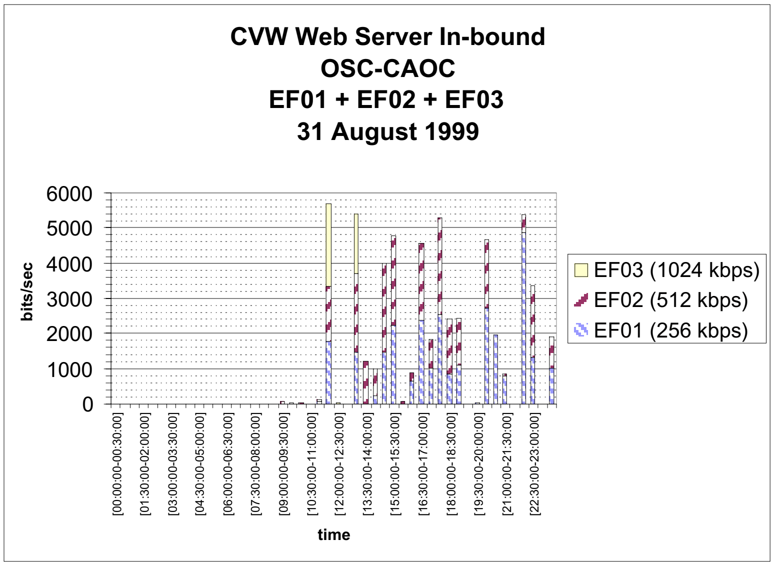


Figure D.61 - CVW Web Server OSC-CAOC In-bound traffic (RMON2 Probe) – 31 August 1999 EDT (LiveFly Day 2)

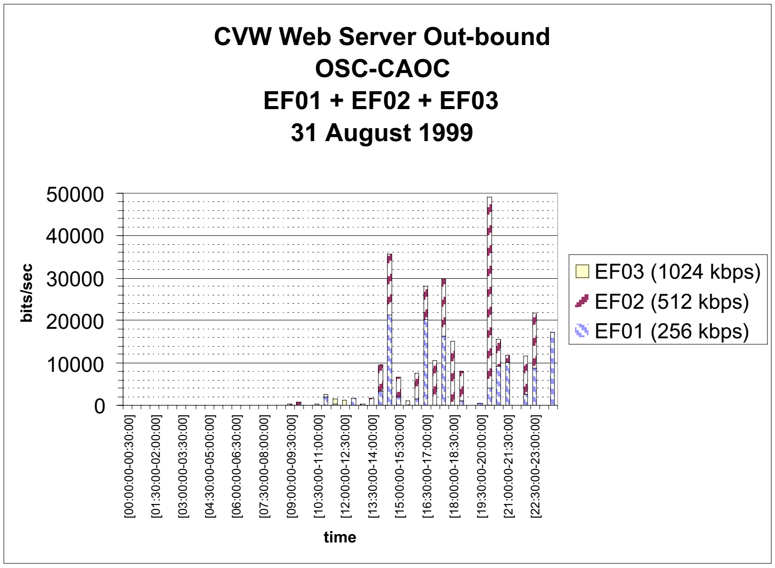


Figure D.62 - CVW Web Server OSC-CAOC Out-bound traffic (RMON2 Probe) – 31 August 1999 EDT (LiveFly Day 2)

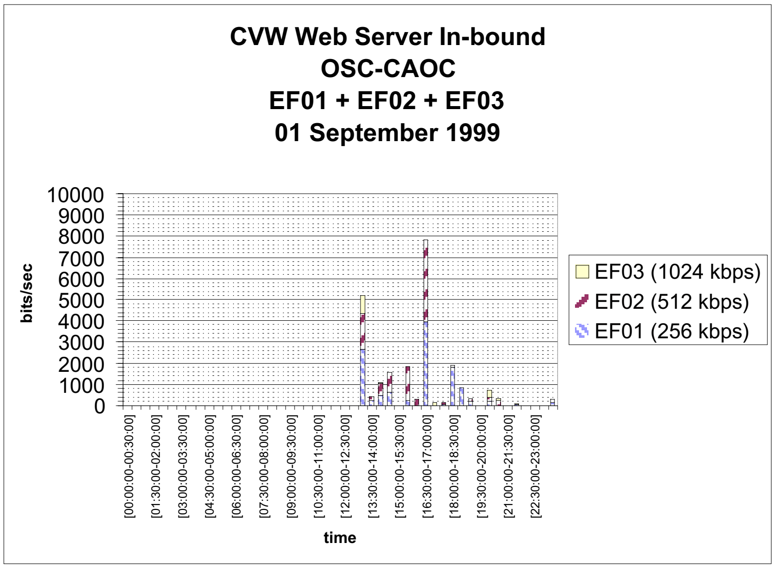


Figure D.63 - CVW Web Server OSC-CAOC In-bound traffic (RMON2 Probe) – 1 September 1999 EDT (LiveFly Day 3)

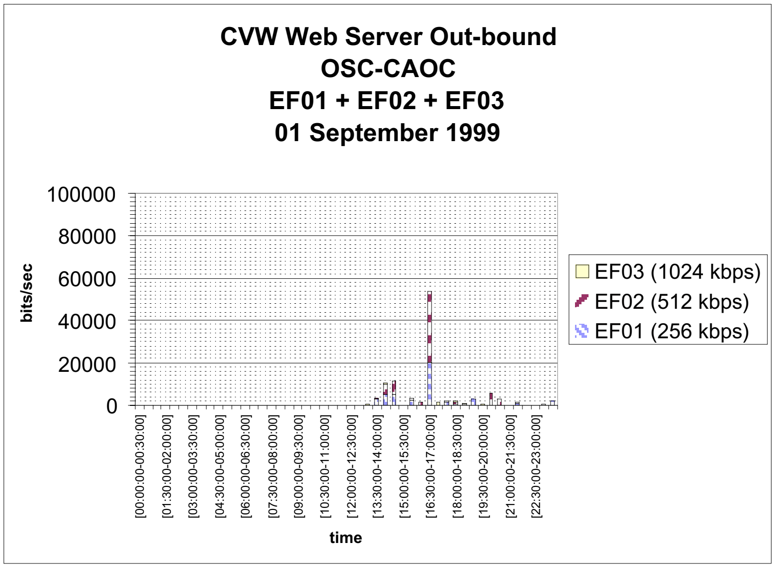


Figure D.64 - CVW Web Server OSC-CAOC Out-bound traffic (RMON2 Probe) – 1 September 1999 EDT (LiveFly Day 3)

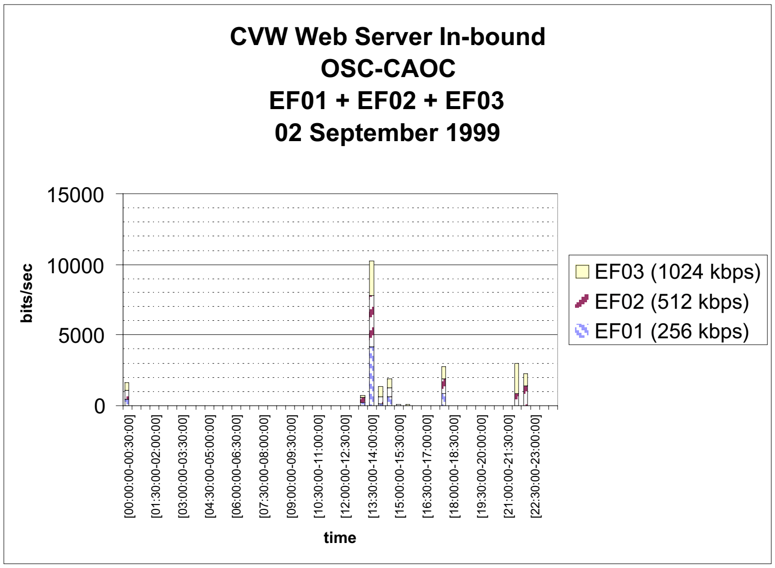


Figure D.65 - CVW Web Server OSC-CAOC In-bound traffic (RMON2 Probe) – 2 September 1999 EDT (LiveFly Day 4)

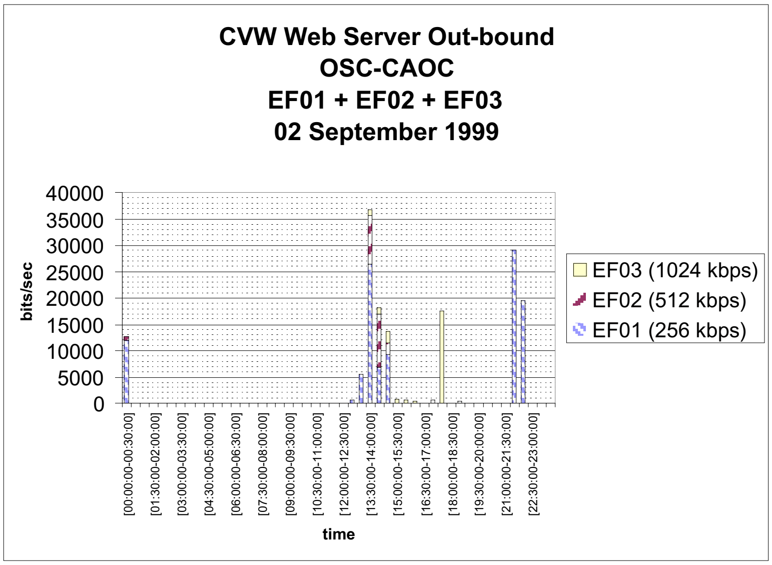


Figure D.66 - CVW Web Server OSC-CAOC Out-bound traffic (RMON2 Probe) – 2 September 1999 EDT (LiveFly Day 4)

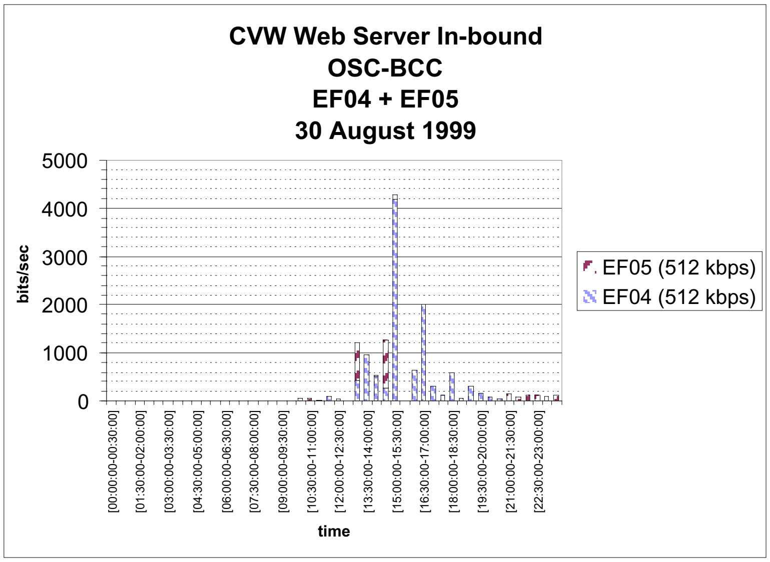


Figure D.67 - CVW Web Server OSC-BCC In-bound traffic (RMON2 Probe) – 30 August 1999 EDT (LiveFly Day 1)

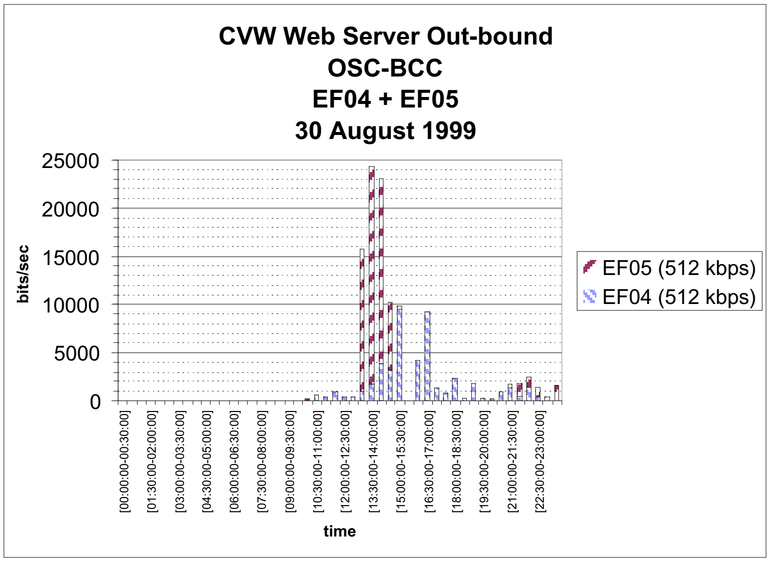


Figure D.68 - CVW Web Server OSC-BCC Out-bound traffic (RMON2 Probe) – 30 August 1999 EDT (LiveFly Day 1)

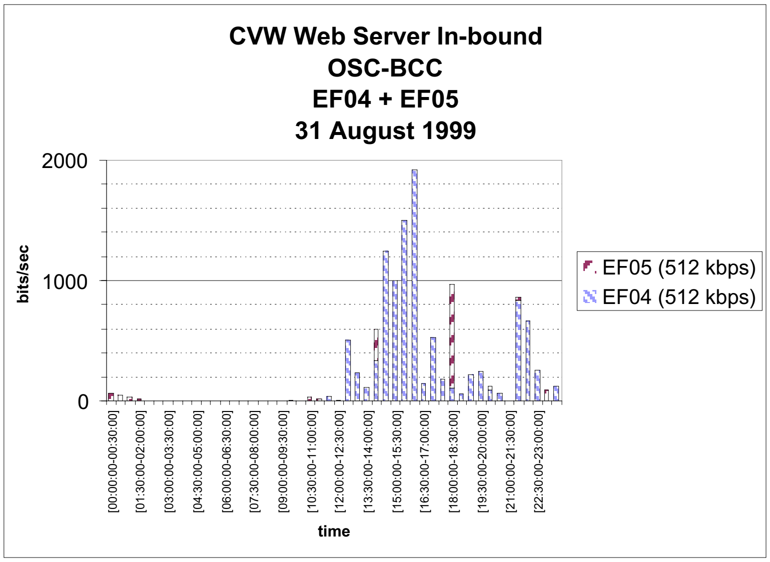


Figure D.69 - CVW Web Server OSC-BCC In-bound traffic (RMON2 Probe) – 31 August 1999 EDT (LiveFly Day 2)

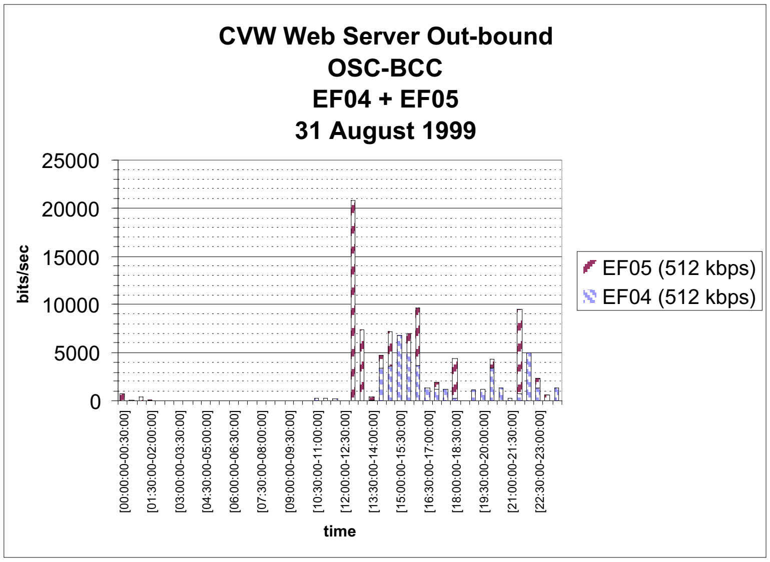


Figure D.70 - CVW Web Server OSC-BCC Out-bound traffic (RMON2 Probe) – 31 August 1999 EDT (LiveFly Day 2)

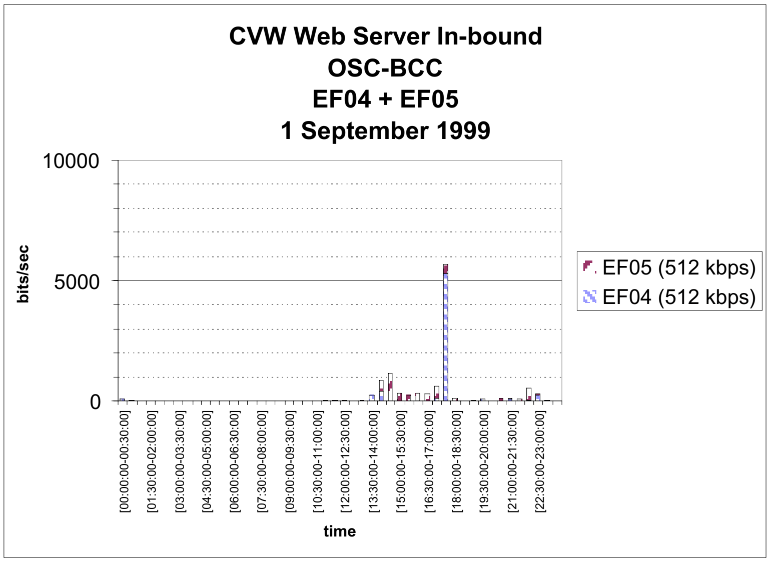


Figure D.71 - CVW Web Server OSC-BCC In-bound traffic (RMON2 Probe) – 1 September 1999 EDT (LiveFly Day 3)

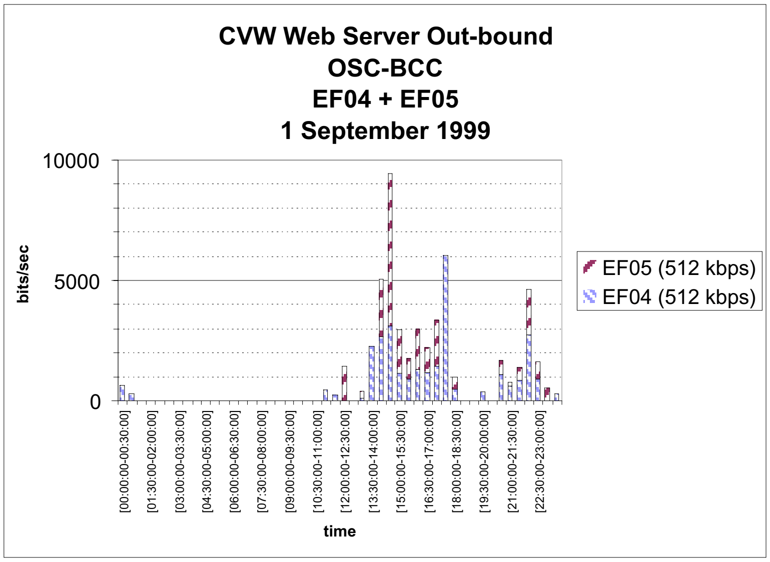


Figure D.72 - CVW Web Server OSC-BCC Out-bound traffic (RMON2 Probe) – 1 September 1999 EDT (LiveFly Day 3)

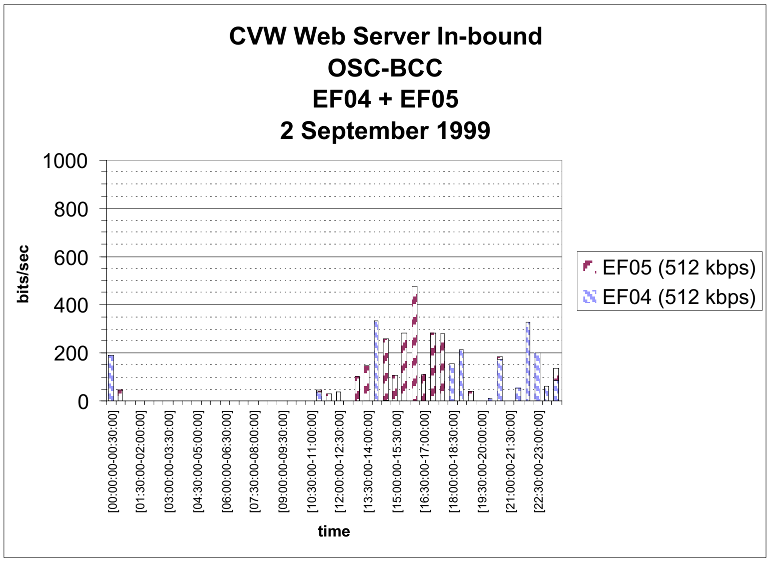


Figure D.73 - CVW Web Server OSC-BCC In-bound traffic (RMON2 Probe) – 2 September 1999 EDT (LiveFly Day 4)

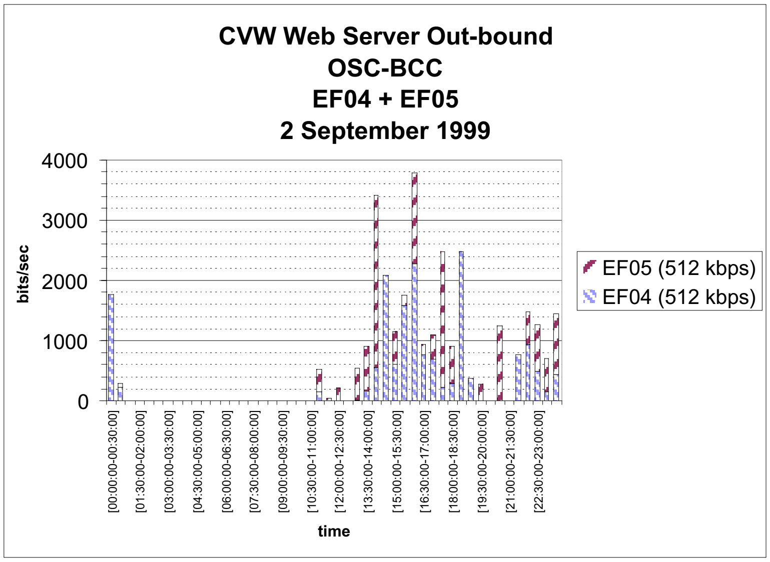


Figure D.74 - CVW Web Server OSC-BCC Out-bound traffic (RMON2 Probe) – 2 September 1999 EDT (LiveFly Day 4)

Appendix E

Deployment Details

Successful deployment of an extensive collaborative environment requires more preparation than most other types of technology. Sections 3, 5 and 6 refer to various tasks that were performed in support of the system deployment. This section provides descriptive details about the list of issues and actions that should be addressed as part of any deployment. The order of items in this list does not imply relative importance. The nature and requirements of each deployment will dictate the importance of the individual items.

E.1 System Engineering

Networks and Multicast:

A collaboration tool is absolutely dependent on the network infrastructure that will hold it together. Unfortunately it is often difficult to get accurate information about how the network really works. Diagrams rarely accurately reflect what is actually installed. Router configurations are seldom documented. Media capacities are usually less than their advertised or nominal bandwidths.

- <u>Make friends with a local network guru!</u>
  If you're lucky there will be one person who has a complete, accurate understanding of the whole network. Try to identify that person and go out of your way to make friends with him/her.

- <u>Learn everything you can about</u>
  - *Network topology*
  - *Known Bottlenecks*
  - *Long haul bandwidths*

  Your first goal relative to networking is to learn as much as you can about its layout and performance. Don't get down in the weeds but concentrate on knowing its strengths and weaknesses at a macro level. In addition try to get a sense of how reliable the key links may be. This is important because part of your job is to deal with expected risks. Assuming you can't cause the network to become more reliable, you'll have to architect the collaborative system so its user services suffer a minimal degradation when such a network failure occurs.

- <u>Use multicast enabled routers if possible</u>
  IP Multicast is used by several collaborative tools to deliver audio and, in some cases, video data among groups of users regardless where the individuals are physically located. Audio has proven to be particularly important for effective collaboration thus elevating the importance of good quality multicast in the networking domain. It is possible for the collaborative team to enable multicast independent of the networking folks but this approach should be reserved for the last resort. Today's routers can be

programmed to pass multicast among themselves and to tunnel multicast through intermediate uncooperative routers. This approach is the most bandwidth efficient and therefore more popular with the network designers even though it requires considerable effort on their part to configure. If all else fails, workstation based multicast tunneling using *mrouted* can be implemented with the unfortunate result that multicast traffic is at least doubled on any one network segment.

- Avoid mixing workstation based *mrouted* with router-based multicast routing
  Experiences with systems that use a combination of router and workstation based multicast have been disastrous. Theoretically, if it is possible to do so, but make sure you have some super-expert help.

User Locations and Work Patterns:
The purpose of collaboration is to bring users together along with their data. Knowing where those users are physically located and mapping their locations onto the network topology is essential to understanding and flagging potential problem areas.

- Find out where users will reside in the network topology
  - *Note concentrations of users*
  - *Note one/two workstation outposts*

  Typically you will have subnetworks that are heavily populated with users and others that support only one or a handful of users. This information necessarily influences where you locate servers and backups, what sort of multicast service you provide and what limitations you highlight. You may need to declare certain segments out of range in the current network topology (the number of users on that network segment can only connect using some subset of the collaborative capabilities).

- Project who will be most active concurrently
  User sites may be located across many time zones or may be engaged in work that is most intense during a particular part of the day. To the extent that you know or can predict these patterns you may be able to scale or distribute the collaborative capabilities so that everyone gets better service than if you had shot at some imaginary average.

- Distinguish modes of use: text chat, audio, document creation and exchange, web access
  The many collaborative services your system offers will be used at different rates by different user communities at different times of the day. For example, in JEFX 99 the CFACC briefings caused a peak load on the collaborative service that delivered the briefing slides to the users. The bulk of that load was at two locations. The strategy was to deploy two copies of the briefing slides, one in each location so that the network bandwidth between the two locations would not receive a hit every minute or two as the slides were flipped by fifty or more users.

Predictable Failure Modes:
We know that something is bound to fail when we least expect it but often the cause of the failure could be predicted even if its timing could not. The least we can do is be prepared for the things we know might happen. If we are lucky this approach will also protect us from some of the failures we could not have predicted.

- <u>Server hardware failures</u>
  We have all experienced system crashes and have known of hard disk failures. Network interruptions though less frequent, still occur and are more likely in tactical communications and recently configured networks.

- <u>Network failures</u>
  - *Long haul connections*
  - *Congestion*
  - *Multicast*
  - *TCP*

  Think about all the ways your network might fail and what each of those failures might mean to your collaboration system users. How can you mitigate those failures by the strategic placement of servers and backups across the network topology? Would mirroring data between your primary and backup servers reduce network loading and improve concurrency?

- <u>Information warfare attacks</u>
  No matter who will use your system or what they use it for, there will probably be someone who will want to break your system in order to deny it to your users. Look at the security provided by the network (VPNs, firewalls). Is that protection adequate? If someone breaks your system you will be blamed no matter who really did the dirty deed. Attacks can also come from within. You can't guard against everything but your system should at least take advantage of whatever security is provided by the operating system and various collaborative tools. User passwords should be handled carefully and blanket passwords should be avoided. Users should be trained to change their passwords. Accounts that have not been used or continue to have their original password should at some point be disabled.

Failure Response Strategies:
Your system architecture and some accompanying procedures will add little to the effort and cost of system deployment and can considerably reduce the impact of the failures discussed above.

- Backups
    - *Data preservation*
    - *Maximum availability to maximum users*
    - *Concurrency vs. bandwidth constraints*
    - *Continuous backups*

  Your backup strategy starts with the desire to make sure the minimum amount of user data is lost. If we get creative with our backup data it offers the opportunity to provide full hot backup for everyone, partial hot backup when some part of the community is cut off while we are getting data preservation almost as a side benefit. The strategy for supporting these backups is more complicated. Periodic bulk updates are the easiest approach but they load the network for periods ranging from several seconds to several minutes. Continuous updates balance the network load and make all instances of the data more closely agree but configuring software to perform the task is non-trivial.

- User procedures
    - *Detection and notification*
    - *Published procedures*

  As we have already discussed there are circumstances that impact the collaborative user that have nothing to do with the collaboration system. Network overloading is the most common. There are parameters you can set that will regulate matters such as the compression algorithm users will default to when using audio and the maximum frame and data rates in video. After that it is up to the network technicians to detect a problem and users to respond by managing to use less of some collaborative services. One approach would be to define several levels of deterioration and assign a name to each. When the network traffic monitors see a problem they match the extent of the problem with their predefined levels and issue an alert (using the various collaborative tools) announcing the condition. User discipline will then have to play the primary role in reducing traffic. Obviously any such scheme would depend on the network traffic monitors notifying the users of status at regular intervals.

Accreditation Strategy:

Systems deployed on government and military networks will require some form of accreditation. There are a number of directives that purport to govern accreditation but the final decision is vested in the local accrediting authority, a senior person who must accept the risk of adding any new system. Gaining accreditation for your system means getting approval to operate on that organization's networks. Your goal is to assemble a factual package of documents that give the accrediting authority an accurate picture of your system and allow him/her to decide whether the benefits of that system outweigh the risks.

- Document architecture

  There is no standard suite of accreditation documentation however every accrediting authority will want a collection of words and diagrams that explain how your particular system works as deployed on their networks.

- Get copies of required paperwork

  Since accreditation paperwork requirements vary, get as much detail as possible about what is wanted. Try to avoid responding to a cryptic list of documents. Ask for samples.

  - *Assume stovepipe system*

    Most existing accreditation requirements were prepared with stovepipe systems in mind.
  - *Complete questionnaires where appropriate*

    Because collaborative tools are not stovepipe systems you will need to be careful to answer any direct questions only for your system. Many items will not apply.
  - *Don't overdo the details*

    The purpose of this paperwork is to help relatively non-technical people understand the security risks your system might pose. If you get too far down in the technical details you run the risk of being rejected because the readers can't figure out how it works.
  - *Don't make claims of capabilities for systems outside the collaborative tool*

    You may have to complete lengthy questionnaires designed with stovepipe systems in mind. Be careful, many of the sections may apply to hardware and software outside the collaborative tool and it's components. Be careful which sections you complete.
  - *Be accurate*

    Every system has security defects. The accrediting authority wants to understand the risks (and what you have done in your architecture and procedures to mitigate those risks). Don't try to snow him/her either with too much detail or with whitewash.

Hosting Strategy:

Server hardware comes in many forms. There are ranges of memory size, CPU speeds, numbers of CPUs, cache sizes and speeds, disk sizes, disk arrays, and so on. In addition, you will almost certainly be running more than one server. The trick is determining the right number of server platforms and the most effective configuration for each.

- Multiple server processes (Tool, Document, Web, Other)
  - *Single host*
  - *Separate hosts*

  Some combination of anticipated use factors will help you determine how to best host your servers. Your backup strategy may drive this decision, or the expected number of concurrent on-line users or the network topology or the number and size of the documents you expect your users to create and exchange. Try to project as many load factors as you can and then size your hardware suite base on your knowledge and experience with the performance of each of your server processes. Each server process will have certain predictable characteristics for CPU utilization, disk accesses, network loading and memory use.

- Disk speed and size, raids, striped raids
  Learn how your server process behaves during a disk access. If the server requires considerable disk space and is dependent on frequent, rapid disk accesses, consider options that reduce disk access time. If large files are involved, look for solutions that reduce disk read time.

- CPU clock speeds and multiple units
  There is a temptation to install multiple CPUs to improve the performance of server processes. Make sure the process you are trying to accelerate can take advantage of extra processors. If not, try to get the fastest (non-beta) CPU available and make sure no other significant process will compete for resources on that hardware platform.

- Memory size
  Memory is not cheap but it is too inexpensive to risk not having enough. Make sure each server has half again as much memory as you can ever imagine it using. Twice as much is nice to have.

- Network connectivity
  Studying the network topology as part of your system architecture task should include consideration of what physical location in that network offered the best connectivity to the largest concentrations of the most important users. Try to get the fastest network interface available on the network segments you have selected. If you need to collocate several servers, try to arrange an independent network interface and connection for each.

The Collaboration Environment:
One tool doesn't make a collaborative environment. The richer the environment the better each component looks. A rich environment is one that provides support for the right variety of collaborative needs within the framework of a concept of operations. A large collection of tools does not make a rich environment, just a confusing one.

- The collaborative tool is a piece of the collaboration environment
  - *Messaging*
  - *Telephony*
  - *Document and data sharing*
  - *Web*
  - *Application and screen sharing*

- Devise a cohesive whole
  The challenge is to work with subject matter experts to understand what the users might want to do and then project that knowledge onto collaborative tools. Try to identify the minimum set of tools that will meet the projected needs. Remember that a number of folks on your collaboration team will be tasked to train the users. Keep training as easy as possible for trainers and trainees by keeping the collaborative environment as simple as possible.

E.2 System Administration

Admin: Who, Where, How Many, On What:
Consider how your system will be administered. Administrators have special powers so you want to keep the number limited however there may be the requirement to cover 24 hour operations, multiple physical locations and multiple administrative functions at one or more locations.

- <u>Who will administer the system</u>
  - *Where are they located*
  - *Are all times covered*
  - *Will all have access to an appropriate workstation*
  - *Will shared workstations be enough*

  Once there are enough of the right administrators at the proper locations the next most difficult issue is finding appropriate places for them to work. If you have decided that server workstations will be dedicated to server processes then running clients and administrator functions on those workstations should be avoided. Plan from the beginning for extra workstations for administrators.

- <u>How do Admins collaborate</u>
  - *With each other*
  - *With users*

  Administrators, like many other system support personnel will benefit from access to the collaborative tool. Make sure they have appropriate spaces in which to congregate, conduct shift changes and keep their notes and procedures. Ideally every support person should be treated like one of the prime mission personnel in terms of collaborative capabilities.

Server Configuration Issues:
Most of these issues will be covered in your server's documentation. That documentation may not cover situations where you have multiple servers either for load balancing or for back up purposes. Consider how the following items become more involved when you add servers. You should have two goals; to keep things as simple and easy to remember as possible and to document everything.

- <u>Naming the server(s) and host workstations</u>

  Your software server may have a naming option. Make it appropriate to the use and keep it simple. The workstation host name may be governed by the network management folks. Whether restricted or not, try to devise simple names expressed in lower case characters. Host names have no security value so complicated names add nothing (passwords are a different matter).

- <u>Multicast base addresses</u>

  If your system uses multicast make sure your scheme for differentiating the multicast sessions among different servers is maintained. A table of base addresses may be needed.

- Login messages for each server
  If the server supports a login message, be sure it is appropriate to the deployment and the role that server plays in the larger deployment. Default messages give the impression that you didn't care enough to make your users feel like they belong to something special.

- New user email (if applicable)
  Some systems can be configured to send email to new users. As with the login message, make sure the canned email message is tailored for this particular deployment.

- Things to be VERY careful of
  Every collaborative tool and every deployment has some small configuration items that will cause you major headaches. Talk to experienced people, review you own experiences and make a list. Then figure out what you'll do to make sure your configuration doesn't bite you.
  - *Keep a list in the virtual admin room*
    Put a copy of your list in an appropriate virtual room and assign responsibility for each item to a member of the collaborative support team. Note the name of the responsible individual next to each item.
  - *For example: avoid using Domain Name Server (DNS) lookup on servers*
    As an example from recent experience, avoid using DNS on any of your server platforms. Investigate which processes on your server make DNS lookups and how they behave if external DNS lookup is disabled.

User Naming Conventions:
The object with user names in a collaborative tool is to uniquely identify each individual participant (user). The sponsoring organization may have an additional agenda for user names. Avoid asking the sponsor for a naming solution without first providing firm guidance (see below). Work with them to devise a simple naming scheme using the available naming options. Naming options will vary from tool to tool. Here is an example.

- Multiple naming opportunities
  - *Login name (simple, familiar to user)*
    This name is what the user enters to login. It may not appear anywhere else. If possible the user should select this name. Unless otherwise specified it should be in lower case.
  - *User name (default "pretty" name)*
    This is the name other users see. It should be pretty in the sense that capitalization should be used where appropriate..
  - *Full name (non-functional, appears in user information box and in user lists)*
    This is the name that appears in the user's personal information box. The system associates this property with the user but does not operate on its field(s).

  - *Aliases (up to the user)*
    A user may have several aliases in addition to the Login and User names. Users can usually be "accessed" by others using any of these aliases.
  - *Assumed name(allows user to "hide" User name, is easily reversed)*
    Some systems allow the user to temporarily replace his User name (the name that appears publicly). This does not change his identity or replace his User name in his list if aliases. It is a handy way for a user to assume a title during a shift and then relinquish it to his replacement at shift change. Users can thus access the "responsible" individual through his assumed title without knowing who is filling that position at the moment.

- <u>Consider how names will be used</u>
  Study the naming options available in your system and the names users will be saddled with in the overall collaborative environment (for example, email name) and in the overall system (for example, workstation login) and try to combine or duplicate them wherever possible. The system's sponsoring organization should have goals for the naming conventions but should not dictate a solution without discussing that solution with the administrator. Be prepared to offer alternatives that will improve usability.

Virtual Building Floor Plan:
Try to get the sponsoring organization or their designated representative engaged in planning the virtual building. Try to prepare them beforehand so that the pitfalls can be avoided. This discussion assumes that the collaborative tool uses a-rooms-organized-into-floors paradigm.

- <u>Floors</u>
  - *Workgroups that interact often*
  - *Political or organizational units (less desirable…)*

  Deciding what goes on each "floor" of the virtual space is the best opportunity to satisfy the demands of political and organizational units. If possible, floors would be organized functionally, each made up of a collection of functionally similar or related workgroup rooms.

- <u>Rooms</u>
  - *Functional workgroups*
    The most effective and the most used rooms are those that are home to small workgroups (about 5 to 12 users) who have a common set of tasks to perform using some common data and applications. These are the rooms where work gets done and where the great majority of users are apt be found.
  - *Avoid general purpose rooms*
    Conference rooms, libraries, and break rooms are examples of room types that generally do not get used. Rooms for frequent regularly scheduled events, like the commander's twice daily briefing, do work both as the place for the briefings and as the repository for the briefing materials available for review between briefings.

- *Use center room for public documents, not work*
  In some tools certain rooms double as passageways and are therefore inappropriate as working rooms. Because of their public nature they do make good public document repositories.
- *Names and descriptions*
  Every room needs both a display name and a (longer – expand the acronyms) descriptive name. Ideally a functional description of each room is desirable. The descriptive name and description should be linked somehow to the name displayed in the building's directory.

User Account Creation:
The goal of every collaborative system administrator is to create user accounts automatically from some external database of user information. Some connection between the two would certainly be desirable to assure naming (and password) consistency. The dangerous assumption is that the information in the external database in both correct and complete. That's more difficult to achieve than the automated interface.

- Approval authority
  Make sure you and the administrators know who has the authority to approve new user accounts and just as importantly who can approve removing user accounts.

- Training prerequisite
  One way of assuring users receive training on tool use and concept of operations for the collaborative environment is to issue user accounts and passwords as the users arrive for training. This implies either that accounts are prepared as the users arrive or that you have some mechanism for gathering user information ahead of time. In the latter case some mechanism is needed for delivering passwords to users as they arrive for training. Generic training accounts are an easy way out but training each user on his own account makes for better training, gives the user some materials to "carry" with him, avoids the security risk of generic accounts and makes sure each user's account is properly created.

- User information collection forms
  If an external database is not going to be used for account creation, the data may be most easily collected and entered into the system using a simple form. Ideally, the form would be available both in hard copy and on line in a web page. The on-line version has the advantage of enforceable required fields and selection lists to limit responses to the set that is meaningful in the system context.

- Capturing and processing user images
  Most collaborative tools provide some mechanism for associating at least a thumbnail picture or icon with each user account. Icons are acceptable in some circumstances but "mug shots" are more useful because they provide both recognition and positive identification. Collaboration among individuals has much of its foundation in mutual trust. That trust is built more quickly among people who can easily recognize and become familiar with each other. Digital cameras make it very easy to capture the

necessary images. The process of associating a picture with the correct user account requires planning and cooperation. One procedure that has worked well is to have the user hold a card with his name boldly lettered at mid-chest height when the picture is taken. When the picture is processed the name is cropped out but is included in the image file name. If a convention has been established, the association of the picture to the account will then be automatic.

- <u>Password control and distribution</u>
  The procedure for creating passwords and delivering them to the respective users can be difficult. Automatic distribution using email is a possibility but assumes that each user has an email account within the network domain, that you have an accurate email address for each new user, that you are willing to give out passwords before training, and that the email system is trusted to deliver passwords. The alternatives are to use a standard or predictable password or no password (all very insecure) or to somehow deliver the password directly to the user (at the time he arrives for training, for example).

- <u>Initial home room selection</u>
  Some collaborative tools allow users to select a home room. Unless a home room is specified when their accounts are created all users will end up in some default location. If the option exists there are at least two possible options. One is to try to determine what room the user will want as his home room through the use of questions about job function on the new user form discussed above. If training is required then every users' home room can be set to the Training room and setting a new home room becomes an exercise for the user during training.

- <u>Use of "extra" fields</u>
  Each collaborative tool provides a collection of fields for information associated with each user (office, phone numbers, email address, etc.). Many of these fields are display only and are not operated on by the tool. In any open field the purpose can be redefined (though the label may be fixed). This allows you to record and display information about the user that is important to other users but is not supported by a field of its own.

The Collaborative Tool Web Server:
To one degree or another most common collaborative tools today employ a web server to some extent. Because that server is present there is much more we can do for the collaborative environment with a minimum amount of effort.

- <u>Client downloads</u>
  Some systems download their client software when the tool is invoked. Others have clients that are downloaded from a web server and installed on the local workstation.
  - *client version(s)*
    System maintenance is simplified by the client download model because new versions of the software need only be loaded on the system web server. Systems that install the client on the local workstation also benefit from the

web server in that the client installer software can be directly downloaded and installed when a new version is made available. This approach has the advantage of introducing less overall network load and performing better in most network environments.

  – *configured for local use*
    Different download pages or servers can be configured for different sites with links to different web resources, different back up servers, etc.

- <u>Building directory</u>
  Some systems do not generate a comprehensive building directory. The collaboration web site is a good place to provide the directory with links in appropriate places in the virtual building.

- <u>User pictures – if used (try to keep local)</u>
  If the collaborative tool supports the capability, use the collaborative web server(s) as the distribution mechanism for user pictures for the local users. One central server is easier to maintain but in systems where users are widely distributed, performance will be improved if the pictures are in several locations close to the larger concentrations of users.

- <u>Place URLs in appropriate places in virtual rooms</u>
  Avoid deploying your collaborative tool and environment without any content. It is reasonable to expect users to supply most of the content but some seed content is helpful. As a bare minimum there are the informational and instructional web pages that come with your tool. Create URL reference objects and place them strategically in the virtual spaces. Don’t overlook your training room(s).

- <u>Provide publish capability for every user</u>
  Web publishing is a valuable collaborative capability that is relatively easy to implement and can be indispensable to completing your concept of operations for the collaborative environment. If the larger system doesn’t provide this capability, investigate the options for making it available on the collaboration system’s web site(s).

- <u>FAQ page(s) for the collaboration environment</u>
  The collaboration environment will be larger and more complex than most users can grasp in a few hours of training. Even with the best training some questions will be asked repeatedly. A web page of frequently asked questions (FAQ) is easy to build and maintain. Be sure it is linked to the collaborative environment home page and that URL reference objects are placed in appropriate virtual rooms.

E.3 Client Software Deployment

Client Software Preparations:
In E.2 we discussed using the web server for client software download. Other common methods of configuring clients might also be implemented. The point here is to

emphasize the importance and complications associated with configuring client software correctly regardless of how it is distributed or installed.

- <u>Download site(s) prepared and tested (if applicable)</u>
  Make sure that each site is loaded with the right combination of client software and configuration files. Conduct several tests at each site and verify that each client goes to the right server(s) and makes the right connections.

- <u>Configured for each location with appropriate pointers to</u>
  - *Primary server(s)*
    Today all clients are probably pointed to the same primary server however with the advent of "federated" servers users may be pointed to the local instance of the federation of servers in which case client pointers to the primary server would vary depending on physical location or some other criterion.
  - *Backup server(s)*
    While every client may, and probably does connect to the same primary server, your architecture may have different groups of clients pointed to different backup servers depending on what kind of outage has occurred.
  - *Local web server*
    You may need to mirror you web servers in several locations to reduce web accesses across the network. In this case clients need to know which web server to go to for their local webable objects.
  - *Office automation applications (re. UNIX clients*)
    In military/warfighting systems, there are a considerable number of UNIX workstations that must support collaboration client functionality. The ability to share Microsoft Office products can be a problem because Microsoft doesn't make a version of Office for UNIX. Today's best solution is to use Sun Microsystems' Star Office. Another solution with which we have considerable experience is WinCenter. WinCenter is clumsy to integrate with collaborative tools and should be avoided.

Deployment Strategies:
Client software that is installed on the local client workstation can be delivered in a variety of ways. It may be desirable to employ all of these techniques in one deployment.

- <u>Media options</u>
  - *Web download*
    Use the collaboration web site to host your client installation download and location-specific configuration files. Download links can be strategically placed in the web page of instructions for completing the installation.
  - *CDROM*
    Some clients will be in locations where the network connectivity is so poor that downloading the client is impractical or where the client must be loaded before network connectivity to the web server is available. An installation CD is desirable for these cases.

  - *DII-COE segment tape, CD, etc.*
    The Defense Information Infrastructure – Common Operating Environment (DII-COE) mandates certain application standards compliance, file structures, file formats, and installation media. If any client platforms in the overall system are DII-COE compliant then a segmented version of the client available on one of the approved mediums will be needed. This can be a long lead time item and can force you to use an earlier "approved" version of your collaborative tool software rather than the latest and greatest as you had planned.
  - *Disk replication*
    Client workstations for some DOD mission applications are built once and the disks are then replicated over and over to produce more clients with relatively little effort. If your collaborative client software is on the master disk(s) every client that is built will include your client. This saves time and effort for everyone.

- Adding desktop icons (XWMs)
  Most client environments include a desktop or menu option for opening the collaborative tool. With some X Windows window managers (XWMs) this task is somewhat more manual (see Appendix C for procedures used with the Common Desktop Environment).

- Windows Start Menu vs. desktop icon(s)
  On MS Windows client workstations the tool icon can be included in the Start menu and/or placed on the desktop. This is a matter of preference and depends on how much else will be on the desktop, what the user is accustomed to or what the local practice is. In cases where multiple servers are involved (Prime, Prime Backup, Local Backup, etc.) it may be better to leave all the icons together in a group off the Start Programs menu.

- Verify configuration files correctness
  Obviously it's not simple to get clients configured correctly. Allow twice as much time as you think you need. It'll take that long to get them right and test all the variations. If you have time left over, think of all the things I've left out and start writing them up!

E.4 Training and User Support

Training Facilities:
Most work areas are not well configured for training. Schedulers see training as a necessary evil that should be allowed a fraction of the time requested. From the beginning you will need to plan and prepare to assure adequate training facilities are available and sufficient numbers of classes are scheduled.

- Optimum 15 trainee stations or less

  Large classes have been taught with some success but the collaboration environment is becoming more complex, forcing training to cover more topics. Class size has a major impact on student comprehension and retention. In large classes students are hesitant about asking questions and trainers can't provide the individual attention that is possible in a smaller class. Even in the small class (under 15) at least two instructors should be used. Team teaching works well but either way the person who is not standing in front of the class is circulating among the students providing individual help.

- A workstation for each trainee

  Every trainee must have a full function client workstation. Students better retain what they have practiced.

- Workstation for teacher with projector

  The teacher must have a dedicated workstation and the display from that workstation must be projected in such a way that every student can see it without moving out of position behind his workstation. Class duration is kept to a minimum (usually about 4 hours) if the students can see what the instructor is doing.

- Rooms in collaborative tool for training
  - *Special objects in rooms*
  - *Exercise rooms as required*

  Have one or more rooms in the collaborative tool set aside for training and put each of your training aids in that room.

- Trainer helper

  Since there will be a helper it may be desirable to have an extra client workstation in the training area for the helper. Problems do arise during training and the helper is the obvious person to straighten things our while the instructor continues with the lesson.

User HELP Strategies:
Training gives users a big boost but something invariably gets left out and users only retain some fraction of what they were taught. In addition, they will encounter problems or generate confusion that no one could have foreseen.

- On-line Help
  - *Include other systems (more folks to man desk)*
  - *Keep test items and FAQ URL in room*

  A room in the collaborative tool is a logical place for a user help room. Since collaboration doesn't make a whole system under any circumstances we can expect other applications to be present. Incorporating them into the help room reduces the need for every application to have someone providing undivided attention to the help room all the time.

- Phone Help

  Phone help should be provided for folks who can't get to the collaborative tool for whatever reason. The same folks who are manning the virtual help room can also cover the phones.

- Asynchronous Help
  - *Email*
  - *FAX*
  - *FAQ (and use HELP crew to post to FAQ)*

  Some help may not require an immediate response or may involve a recommendation for software modification or enhancement. Users should have an email address to which they can send problems and suggestions. A FAX number might also be provided for the same purpose. The help room personnel would be responsible for responding to these inputs and should be identifying questions with easy answers that are being asked repeatedly. These questions and their answers should be regularly added to the on line FAQs.

- Local HELP

  When not involved in training, the trainers should be providing one-on-one and small group help at locations where there are concentrations of users. They should keep in touch with and help man the help room and should use this experience to improve their course of study.

Handling Trouble (Bug) Reports:

There is no universal definition of bug report nor should its use here be interpreted to mean "something broken" report. "A bug is in the eye of the beholder."

- Have a procedure

  Be prepared to distinguish user suggestions for improvement, user complaints about implementations they don't like, and user railings about defects that don't exist (but they forgot the training or more likely didn't come to training) from true bug reports. Each type needs to be responded to promptly and in its own way.

- Give feedback regularly

  Make sure you get back to the user quickly and if the issue can't be "fixed" in short order provide updates so the user knows you're making progress.

- Many "bugs" are operator error or misunderstanding
  - *Add to FAQ*
  - *Modify training plans*

  Make sure that operator errors, misunderstandings and misinformation are straightened out and that the FAQs and training plans are modified appropriately. Don't over react to single events but watch for trends.

- Filter upgrade suggestions
  - *Suggest workarounds*

  Many users are frustrated software engineers. Filter what individuals say, watch for trends and report the great ideas and solutions that seem to address trend concerns. Work with individuals and groups who perceive a problem or shortcoming. Often there are tools in your collaborative arsenal that can be pulled together to do what the users want. Do this a few times and you will be a certifiable hero in that group.

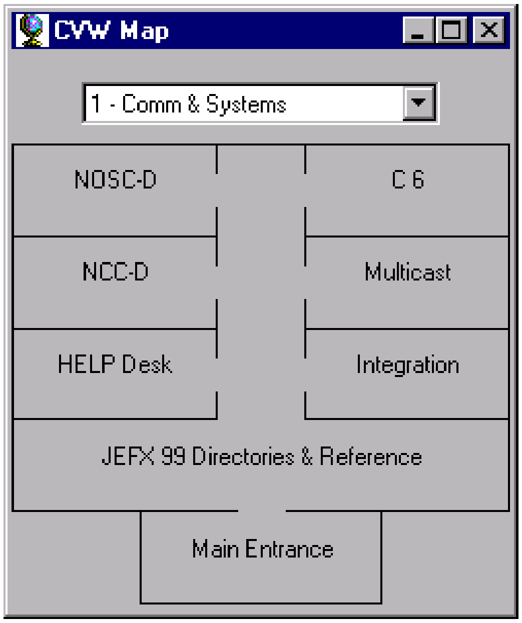
Appendix F

The Collaborative Environment

This appendix consists of a collection of objects found in the JEFX 99 virtual AOC building that were created and used by the operators. This section includes graphics of the actual floors and rooms, a short description of each, a listing of "Significant Room Objects" and a sampling of some selected objects. These objects were listed to illustrate the types of documents, images, whiteboards, etc., that were posted and used to support operations. Objects were also selected which provided techniques and procedures for geographically separated but functionally aligned operators to use the collaborative tool in conducting numerous operations and activities. Selected objects included in the section are those that are highlighted in bold in the floor description pages. Many objects were not included because of their classification or other security concerns. Rooms that have "N/A," i.e., not applicable, meant that the room contents indicate there were no objects in that room, or objects were administrative or personal only.

CVW notes which were standalone objects in the various rooms have been combined in this section for purposes of brevity. For obvious reasons the figures do not include video clips which appeared as room objects. The figures also do not include text and audio communications used collaboratively among the operators. (See Section 8.4 which documents a need for instrumented data collection.)

These figures should serve well as a general model for designing procedures and CONOPS for the use of any collaborative tool in any operational environment. It spans various functional disciplines within the distributed JAOC, the EOC and BCC. It also illustrates joint service input in a collaborative environment. It should be emphasized that the environment, objects and procedures reviewed here reflect one approach, not the only approach. Also, the methods and techniques here were operator-conceived not prescribed to them. Operators used their own initiative and creativity in developing how they would use the collaborative tool to do their jobs. It can be expected even with a well formulated collaborative CONOPS, operators will continue to adapt and innovate on the capabilities of the tool to uniquely suit their needs.



NOSC –D (Network Operations and Security Center-Deployed)
Significant Room Objects: Vulnerability Assessment Reports, (Notes); Air Force Computer Emergency Response Team (AFCERT) Advisories, (Genser messages cut and pasted into Notepad)

C-6 (Director, Communications and Systems)
Significant Room Objects: CFACC COMM Network Architecture (PowerPoint)

NCC-D (Network Control Center-Deployed)
N/A

Multicast (Management of IP multicast for audio in collaborative tools)
N/A

HELP Desk (User help for Communications and Systems)
N/A

Integration (Communications and Systems Integration)
Significant Room Objects: Y2K Test Briefing (PowerPoint)

JEFX 99 Directories & Reference
(People, Places and Common Reference Documents)
Significant Room Objects: JEFX Address Book (Folder); CVW Info and Help (Folder), OSC/CAOC CVW Building Directory (Web Ref.); Cat III Initiative Descriptions (MS Word); Users Help Notes (Folder); URLs folder with Intelink Central, JEFX 99 Homepage and OSC Weather Service web references

Main Entrance (Default room for unassigned personnel)
Significant Room Objects: Miscellaneous documents and images

Figure F.1 – 1st Floor - Comm & Systems

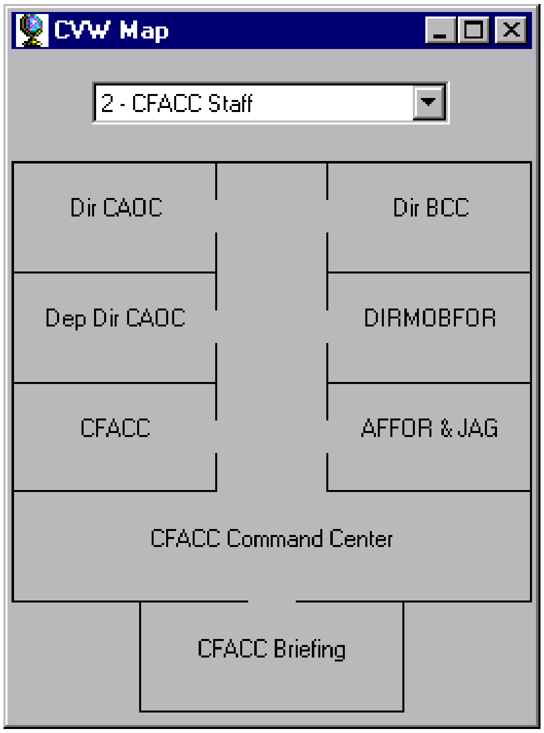


Figure F.2 - 2nd Floor – CFACC Staff

Dir CAOC (Private Office for Director, CAOC)
N/A

Dir BCC (Private Office for Director, Battle Control Center)
N/A

Dep Dir CAOC (Private Office for Deputy Director, Combined Aerospace Operations Center (CAOC))
Significant Room Objects: Numerous CAOC reports in text format, Organizational Descriptions, Advisory Messages (Notes)

DIRMOBFOR (Private Office for Director, Mobility Forces)
N/A

CFACC (Private Office for Combined Forces Air Component Commander)
Significant Room Objects: CFACC itineraries and numerous CAOC reports in text format, Organizational descriptions in Text, Advisory Messages (Notes)

AFFOR & JAG (Judge Advocate Team)
Significant Room Objects: Events Log (MS Word); Rules of Engagement (ROE) Documents; Requests for Information (RFI) (Notes); Assessments (Notes); JAG IN BOX (Folder)

CFACC Command Center
Significant Room Objects: Daily Reports (MS Word); Event Agendas in text; Numerous CAOC reports and Messages; Distinguished Visitor Lists in text

CFACC Briefing (Audio and Video linked to “balcony” on eighth floor)
Significant Room Objects: All CFACC Briefings (web refs); CFACC Briefers Group Object; All CFACC Decision Briefings (HTML and/or PowerPoint); Real World Hurricane Weather Update (web ref)

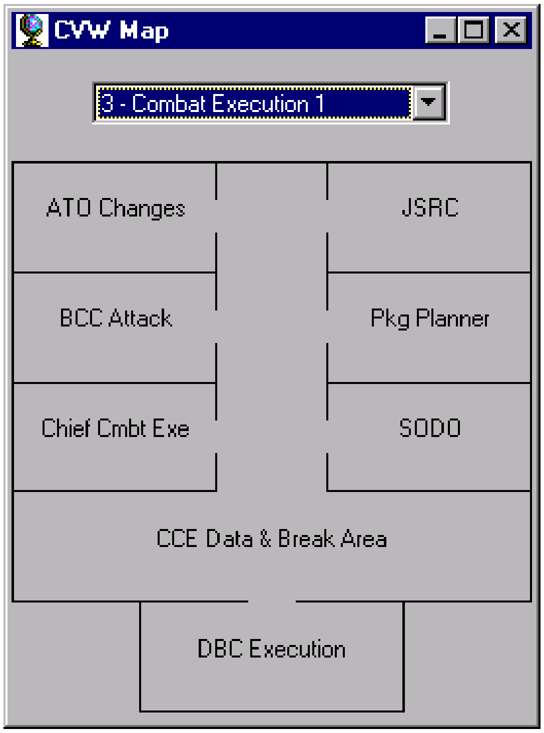


Figure F.3 - 3rd Floor – Combat Execution 1

ATO Changes (Any change information reference Air Tasking Orders (ATO))
<u>Significant Room Objects</u>: ATO Change Sheet (Whiteboard); ATO Change History (Folder with Change Notes by each day); ATO Change IN BOX (Folder with multiple Notes); Data Base Changes (Folder with multiple Notes)

JSRC (Joint Search and Rescue Cell)
<u>Significant Room Objects</u>: Combat Search and Rescue (CSAR) Briefing Inputs Archive (Folder with PowerPoint briefing slides); ***JSRC CSAR Mission Folders (Each folder with Notes,*** Whiteboards, JSRC Group Objects; Open CSAR mission Folder; ***Personnel Recovery (PR) Incident Checklist (Whiteboard); PR Mission Checklist (Whiteboard*)**

BCC Attack (Battle Control Center Attack Reference Room)
<u>Significant Room Objects</u>: BCC Dynamic Battle Control (DBC) Attack Guidance Matrix (XLS); Air Operations Directive (AOD) for ATO PB (MS Word); ATO Guidance documents (MS Word); Target Taskings (Notes)

Pkg Planner (DBC Package Planners team)
<u>Significant Room Objects</u>: Numerous targeting related Notes, Images, and Whiteboards; Package Planners Group Object; Intelink Central (web ref)

Chief Cmbt Exe (Chief, Combat Execution)
<u>Significant Room Objects</u>: ***BCC AO Time Critical Targeting (TCT) Flow Process*** (MS Word); CSAR Incident Information (Whiteboard)

SODO (Senior Operations Duty Officer)
<u>Significant Room Objects</u>: Operational Notes, Whiteboards, Web Refs; ***Updated Guidance to BCC* (Note)**

CCE Data &Break Area (Data Repository for Combat Execution Director)
N/A

Hammer 13 CSARTF assets.txt

CSARTF assets for Hammer 13

1	HH-60	C/S	Jolly 01	MSN	No. 3164
2	A-10	C/S	Puff 06	MSN	No. 7106

Hammer 13 Threat Assessment –1.txt

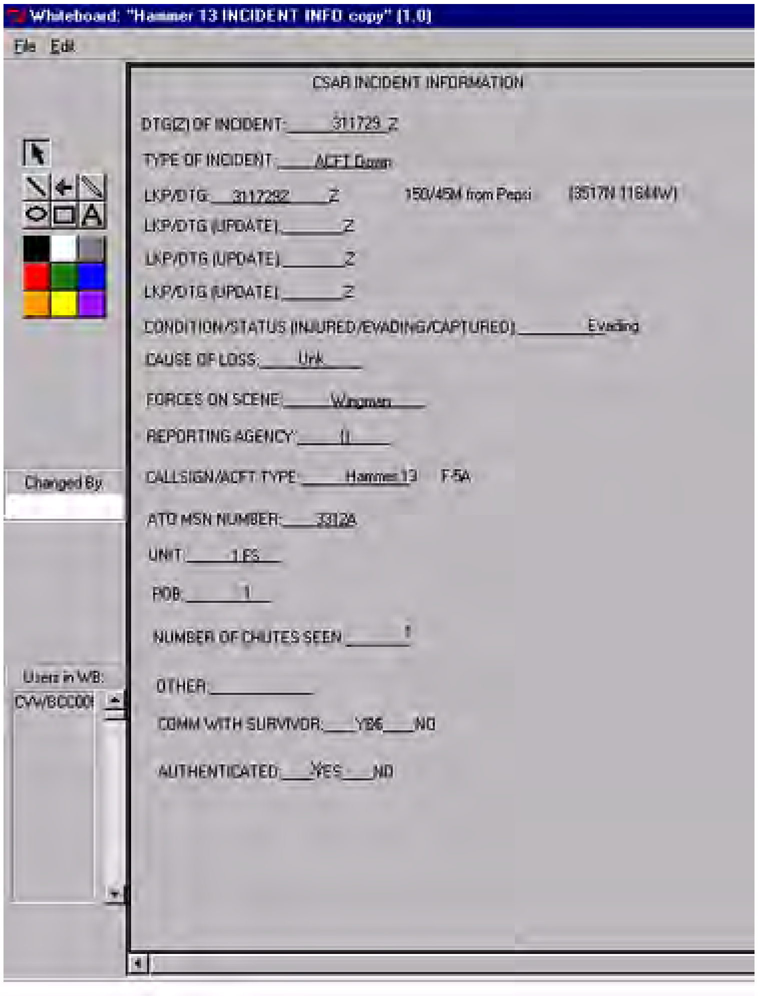
Northeast of last known pilot position: 924 Arty. Bn. at	3522N	11603W,
Also, southeast of pilot position: 31 Armor Bde at	3442N	11628W
According to latest intel the nearest threat is at the 3 3rd Armor Battalion	3453N	11700W

Hammer 13 WX Report.txt

Clear skies, NO clouds, High 82, Low 60 Light data for the mission. Sunset 19:01L, Moonrise 22:26Lll MoonSET 01/11:03L %illum 79% for aircraft 35.17N 116.4 4W. Current WX conditions for F5-A are, Vis – Unrestricted, Winds 330 @02 kts, Temp at 71, Clouds scattered at 8,900 ft and no significant weather. Forecasted winds to become 220 at 10 gusting to 25 after 22Z. MWA has the area in an Isolated thunderstorm area from 10 to 06Z but not forecasted.

FROM JSRC ROOM
FROM "HAMMER 13" MISSION FOLDER

Figure F.3 - 3rd Floor – Combat Execution 1, continued



CSAR INCIDENT INFORMATION

DTG(Z) OF INCIDENT:______311729 Z

TYPE OF INCIDENT:____ACFT Down

LKP/DTG:__3117292______Z 150/45M from Pepsi (3517N 11644W)

LKP/DTG (UPDATE)_______Z

LKP/DTG (UPDATE)_______Z

LKP/DTG (UPDATE)_______Z

CONDITION/STATUS (INJURED/EVADING/CAPTURED)________Evading

CAUSE OF LOSS:_____Unk_____

FORCES ON SCENE:_____Wingman_____

REPORTING AGENCY:_____()_____

CALLSIGN/ACFT TYPE:______Hammer 13 F-5A

ATO MSN NUMBER:____3312A

UNIT:______1 FS____

POB:______1____

NUMBER OF CHUTES SEEN ______1

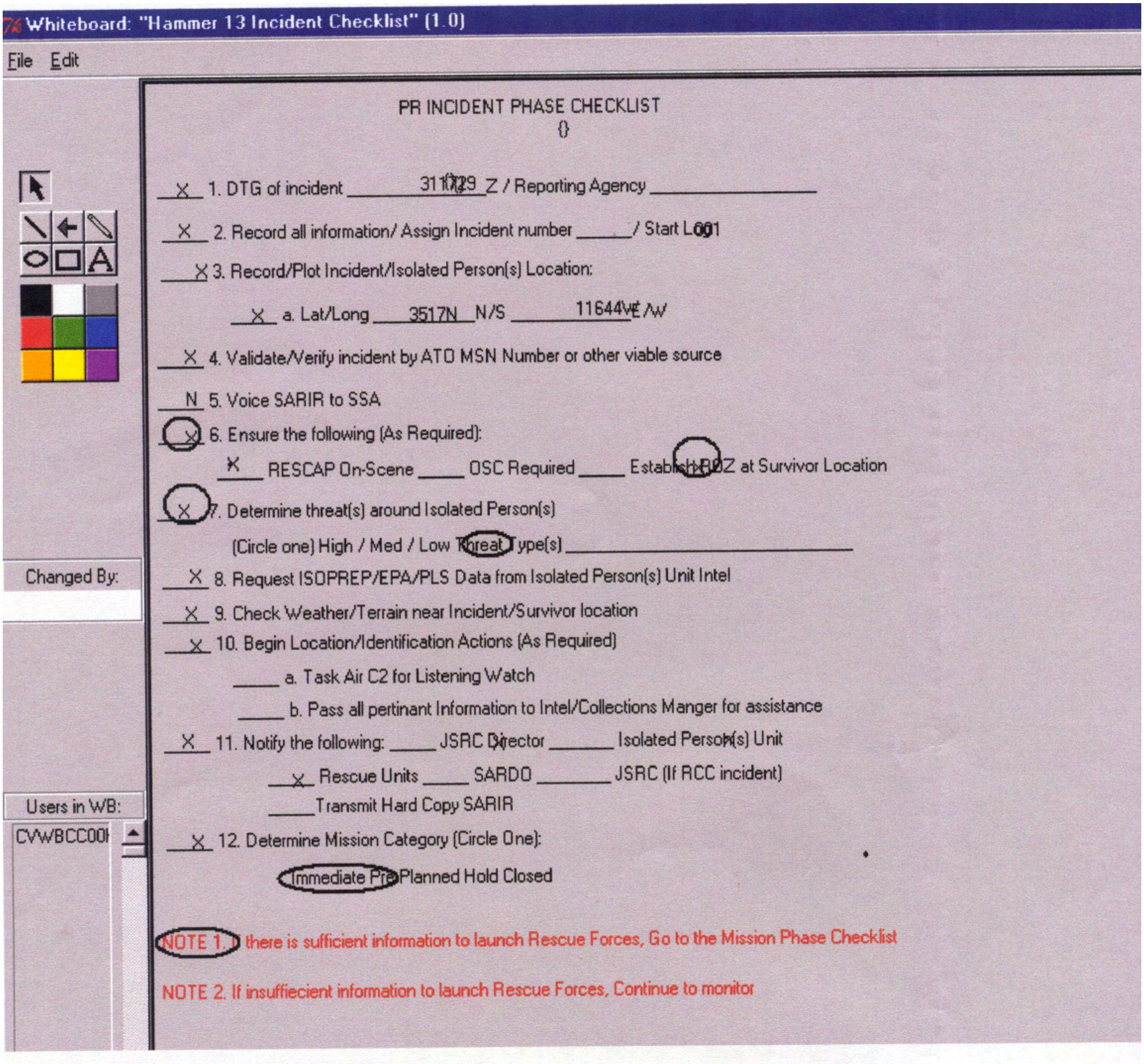
OTHER:___________

COMM WITH SURVIVOR:____YES____NO

AUTHENTICATED:____YES____NO

FROM JSRC ROOM
FROM "HAMMER 13" MISSION FOLDER

Figure F.3 - 3rd Floor – Combat Execution 1, continued



PR INCIDENT PHASE CHECKLIST
{}

_X_ 1. DTG of incident ___311729_ Z / Reporting Agency ____________

_X_ 2. Record all information/ Assign Incident number _____/ Start L001

__X 3. Record/Plot Incident/Isolated Person(s) Location:

_X_ a. Lat/Long __3517N_N/S ____11644W E /W

_X 4. Validate/Verify incident by ATO MSN Number or other viable source

_N 5. Voice SARIR to SSA

_X 6. Ensure the following (As Required):

X__ RESCAP On-Scene ____ OSC Required ____ Establish X ROZ at Survivor Location

_X 7. Determine threat(s) around Isolated Person(s)

(Circle one) High / Med / Low [✓ Threat] Type(s) ________________

_X 8. Request ISOPREP/EPA/PLS Data from Isolated Person(s) Unit Intel

_X 9. Check Weather/Terrain near Incident/Survivor location

_X 10. Begin Location/Identification Actions (As Required)

____ a. Task Air C2 for Listening Watch

____ b. Pass all pertinant Information to Intel/Collections Manger for assistance

_X_ 11. Notify the following: ____ JSRC Director _____ Isolated Person(s) Unit

_X_ Rescue Units ____ SARDO ______ JSRC (If RCC incident)

____Transmit Hard Copy SARIR

_X_ 12. Determine Mission Category (Circle One):

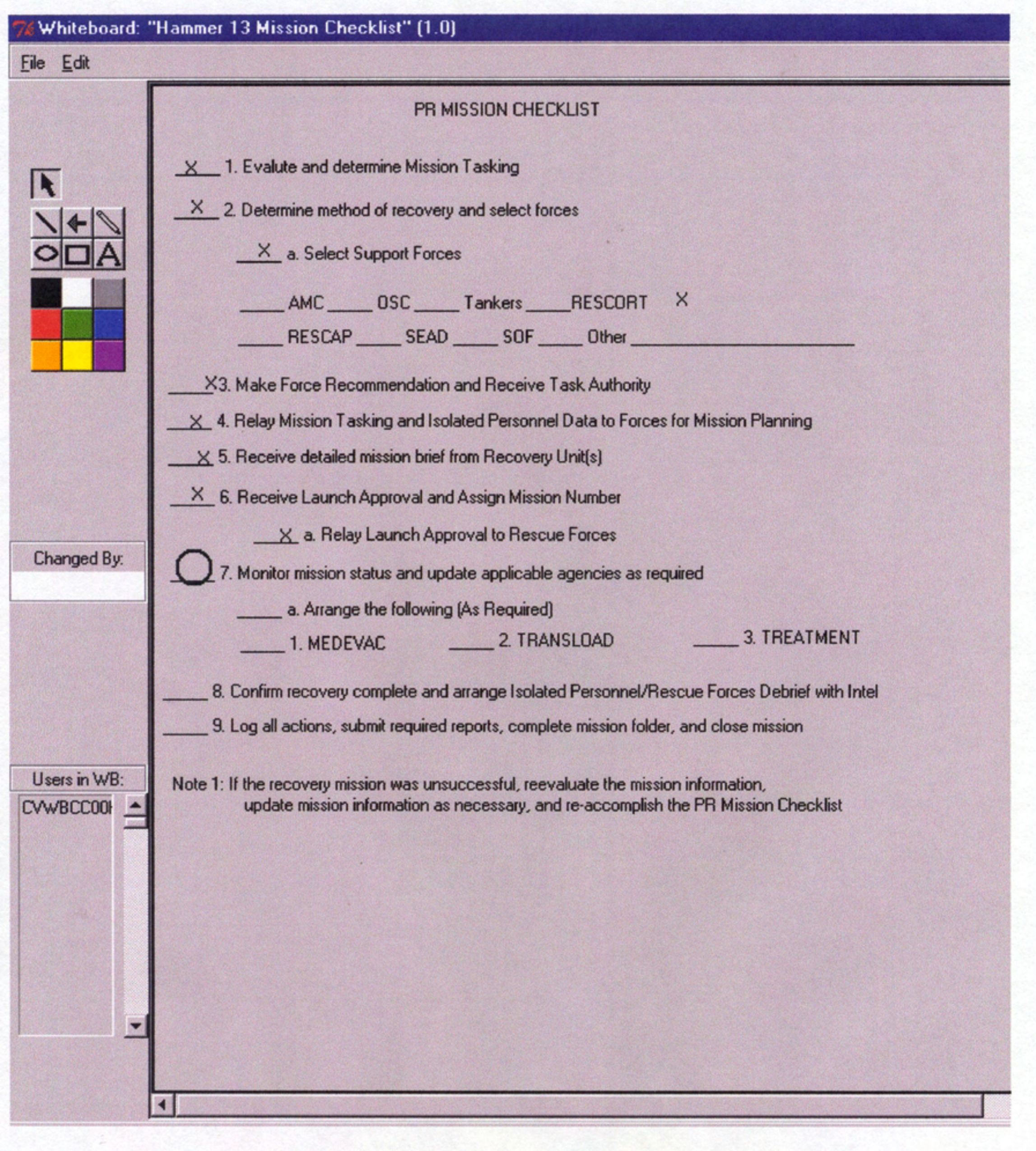
[✓ Immediate Pre]Planned Hold Closed

NOTE 1. If there is sufficient information to launch Rescue Forces, Go to the Mission Phase Checklist

NOTE 2. If insuffiecient information to launch Rescue Forces, Continue to monitor

FROM "HAMMER 13" MISSION FOLDER

Figure F.3 - 3rd Floor – Combat Execution 1, continued



PR MISSION CHECKLIST

___X___ 1. Evalute and determine Mission Tasking

___X___ 2. Determine method of recovery and select forces

___X___ a. Select Support Forces

_____ AMC _____ OSC _____ Tankers _____RESCORT X

_____ RESCAP _____ SEAD _____ SOF _____ Other ________________________

____X3. Make Force Recommendation and Receive Task Authority

___X___ 4. Relay Mission Tasking and Isolated Personnel Data to Forces for Mission Planning

____X 5. Receive detailed mission brief from Recovery Unit(s)

___X___ 6. Receive Launch Approval and Assign Mission Number

___X___ a. Relay Launch Approval to Rescue Forces

○ 7. Monitor mission status and update applicable agencies as required

_____ a. Arrange the following (As Required)

_____ 1. MEDEVAC _____ 2. TRANSLOAD _____ 3. TREATMENT

_____ 8. Confirm recovery complete and arrange Isolated Personnel/Rescue Forces Debrief with Intel

_____ 9. Log all actions, submit required reports, complete mission folder, and close mission

Note 1: If the recovery mission was unsuccessful, reevaluate the mission information, update mission information as necessary, and re-accomplish the PR Mission Checklist

FROM JSRC ROOM
FROM "HAMMER 13" MISSION FOLDER

Figure F.3 - 3rd Floor – Combat Execution 1, continued

BCC Attack Operations TCT Flow

1. Initial Notification {IMINT, SIGINT,HUMINT, COMINT, etc.}
    - Send Pop-Up Message to the “BCCTCT” Group
        - Include ALL amplifying information you have {Coordinates, Type Target, etc.}
        - Include Location of Data for all to view (i.e., Image saved to SIPRNET Website/IPL)
    - Collection Manager (CM) sends tip-off info to CAOC (via CVW) and TES (via voice/E-mail)
    - CM Review Location of Collection Assets for Possible Re-Task
    - TCTO/TP&SO inform “BCCMCC” of Emerging Target
    - TCTA Operator put new Target into TCTA and Export Track (do <u>Not</u> make Time Critical)
    - TCTO/TP&SO/CM Inform CAOC Attack Ops (AO)/TP&S/CM Cells of emerging target
2. Supporting Source(s) Found
    - Send Pop-Up Message to “BCCTCT” Group
    - Include Supporting Evidence of Target Identified in Initial Notification
    - TCTO/TP&SO/CM send target package location (IPL or Website) to CAOC AO/TP&S/CM Cells
    - TP&SO in concert with Collection Manager manage/direct the development of every target
3. TP&SO Validates/Confirms Target
    - Send Pop-Up Message to “BCCTCT” Group
    - Space/IO and JAG review Target to Ensure it is <u>Not</u> on “No/Restricted Hit Lists”
    - Send Pop-Up Message to “BCCMCC”
4. TCTO/TP&SO Coordinate with CAOC TP&S Cell to add Target to Dynamic Target List (DTL)
    - Send Pop-Up Message to “BCCTCT” Group Updating Target as <u>Time Critical</u>
    - TCTO Coordinate with CAOC AO Cell; determine if target will be handled by BCC AO Cell
    - Send Pop-Up Message to “BCCMCC” Notifying them that a TCT is being “Worked”
5. TCTA Operator Updates Target Track as Time Critical
6. AODA “Plans” Assets against the TCT
    - AODA Operator Coordinates with Operational RPTS and JAG to review the Asset Pairing
    - AODA Operator Notifies AO Subject Matter Experts (SMEs) of Plans available for review
7. AO SMEs Review AODA Plan, Determine if Support Package is Required
    - As required, have AODA Operator “Replan” Asset Pairing {Return to Step 6.}
    - Inform “BCCMCC” of Asset Pairing/Brief Plan
8. AODA Operator Receives Authorization to Commit Pairing from TCTO
    - CM forward Strike Package data to CAOC CM
    - CM coordinates with CAOC CM to arrange BDA Collection of Target
9. RPTS Builds Re-Task Mission Package
    - TCTO Informs BCC BC/MCC/SD and Previews Package
    - Weapons Director Confirms Aircraft Able to Accept Re-Tasking
10. Send Retask to Aircraft

FROM CHIEF CMBT EXE ROOM

Figure F.3 - 3rd Floor – Combat Execution 1, continued

Guidance to BCC.txt

Updated Guidance to BCC Attack Ops

Effective Upon Receipt (generated 26 Aug 1930Z)

1. Assets for BCC: BCC will reachback to CAOC for designation of assets to engage emerging DBC targets within the BCC's Engagement Zone. BCC will affirm pre-planned targeted missions within their engagement zone and coordinate attack assets with the CAOC.

2. Engagement Zone UFN: Nellis Range Complex and land mass SW to border of Califon.

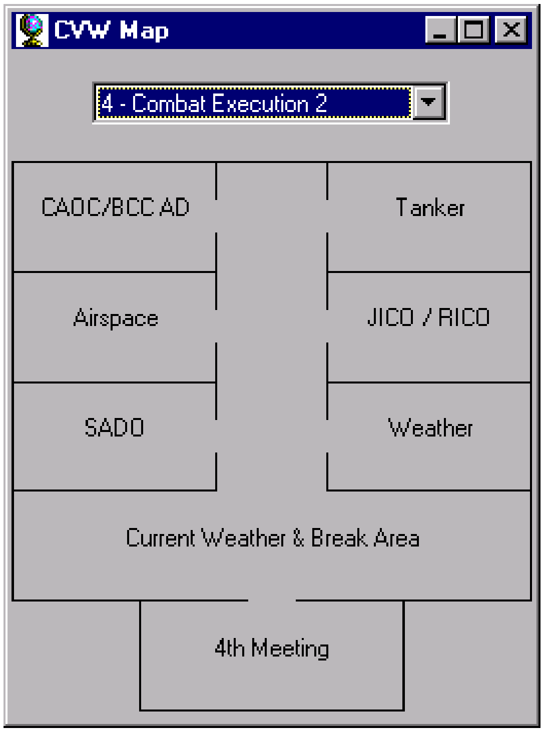
3. Mission Orders: On order, conduct rapid halt of enemy ground forces crossing into Nevidah.

4. CAOC Responsibilities: Designate attack assets to BCC upon request. CAOC maintains theater wide focus (BCC focus on Engagement Zone)

5. CAOC POCs: Lt Col xxx, CCE @ 1337 / Maj xxx, SODO @ 1342

FROM SODO ROOM

Figure F.3 - 3rd Floor – Combat Execution 1, concluded



CAOC/BCC AD (Air Defense)
Significant Room Objects: Defensive Missile Order of Battle (DMOB) documents in text format; AWACS (Folder); BCC Log (MS Word); CFACC Attack Guidance in text format; DBC Activity Log (Note); DDT Log (Note); ***Kill Logs*** (Microsoft Word); "Space Stuff" (Folder with multiple classified images, ***Whiteboards*** and Text Documents)

Tanker (Air Refueling Control Team)
Significant Room Objects: ABL Tanker Refuel Request (Text); Tanker Mission Requests (Notes)

Airspace (Airspace Control Cell)
Significant Room Objects: ACMREQ (Airspace control Means Request) IN BOX (Folder); ACM Request Template (Note); ACMREQ OUT BOX (Folder); ***Procedures for submitting ACM requests*** (Note); ***Airspace Control*** (Whiteboard)

JICO/RICO (Joint and Regional Interface Control Offices)
Significant Room Objects: Numerous data link related logs (Notes); Updates; Status Reports; Matrices; ***Site Sketches****;* Plans and Architectures (MS Office, Notes and Whiteboards)

SADO (Senior Air Defense Officer)
N/A

Weather (Combat Weather Team)
Significant Room Objects: Weather Administration Folder (including the Weather team Group Object); Weather Briefings Folder containing ***numerous mission and geographically tailored briefings in PowerPoint;*** URLs for Theater Weather Services (Web Refs)

Current Weather and Break Area
(Forecast Data and maps for the Area of Operations)
Significant Room Objects: JEFX 99 weather related web references

4th Meeting (Planning and Meeting Space)
N/A

Figure F.4 - 4th Floor – Combat Execution 2

KILL LOG

TYPE/#	A/CTYPE/CALLSIGN	RESULTS	TIME/DATE	NOTES
SU-7/1	F-22/Aviator 41	Splash	1535z/24AUG	
Mig-21/3	F-18/Elmer 67	Splash	2135z/24AUG	
IL 76/1	F-15C/Whoozoe25	Splash	1445z/24AUG	HVA
Mig 29/2	F-22/Bugs 37	Kill	1500z/25 AUG	
Mig 29/2	F-15C/Elmer 61	Splash	1510z/25 AUG	
IL 76/1	F-22/Aviator 41	Splash	1500z/25AUG	HVA
Mig 21/2	F-15C/Elmer 23	SPlash	1430z/25AUG	
SU-24/5				
Su27/2	F-15C/Elmer 63	Splash	1545z/25AUG	
SU-24/1	F-15C/Whoozoe 31	Kill	1656z/25AUG	
Mig 21/2	F-15C/Whoozoe 25	Kill	1656/25AUG	
Mig 23/1	F-15C/Bugs 25	Kill	1915z/25AUG	
Mig 21/5		Kill		
Mig 23/4	F-15C/Whoozoe 23	Kill	1934z/25AUG	
Su-24/3		Kill		
Mig21/5	F-15C/Elmer 65	Kill	1940z/25AUG	
Su27/2 SU23/1	Kill			
Su27/2	F-15C/Bigsky 31	Kill	1520z/26AUG	
Mig29/2 Mig21/2				Kill
Mig29/4	F-15C/Bigsky 15	Kill	1520z/26AUG	
Mig21/2	F-15C/Pokey 47	Kill	1526z/26AUG	
Su-7/2	F-15C/Bigsky 15	Kill	1535z/26AUG	
Su-27/1	F-18/Maple 55	Kill	1536z/26AUG	
Mig29/1 Mig21/2	Kill			
Su24/3	F-16C/Snake 17	Kill	1620z/26AUG	
Su24/6	CF-18/Maple 55	Kill	1628z/26AUG	
Mig21/2 Mig29/2	Kill			
SU7/1	VFA15	KILL	1335z/28 Aug	
SU25/1	BIGSKY 15	KILL	1520Z/28 Aug	
TRANSPORT/1	BIGSKY 15	KILL	1543Z/28 Aug	
MIG29/3	SNAKE 17	KILL	1615Z/28Aug	
Su24/1	SNAKE 17	KILL	1615Z/28AUG	
MIG29/1	BIGSKY31	KILL	1635Z/28AUG	
MIG21/1				
SU24/4				
SU25/2	BIGSKY31	KILL	1643Z/28AUG	
MIG23/1	HANN 71	KILL	1907Z/28AUG	
MIG29/2	MAPLE 61	KILL	1907Z/28AUG	
MIG23/1	SPIKE 23	KILL	1841Z/29AUG	
MIG23/1	BIGSKY 57	KILL	1905Z/29AUG	
SU7/2	PIPE 31	KILL	1905Z/29AUG	
MIG21/4	POKY 41	KILL	1954Z/29AUG	
SU24/2	BIGSKY 21	KILL	1830Z/30AUG	
SU25/1				
MIG23/4	PATRIOT/HAWK	KILL	1900Z/30AUG	
SU7/4				
MI6/2				

FROM CAOC/BCC AD ROOM

Figure F.4 - 4th Floor – Combat Execution 2, continued

AirspaceProced.txt

- Launch CVW

- Select Floor 4, Airspace Room

- Right Mouse on "ACM Request Template" within the "Contents" area

- Copy the ACM Request Template from the contents area to your Carrying Folder

- Right Mouse on the "ACM Request Template" icon in your Carrying Folder, select Information, then rename the template (i.e., AAR 20AUG/0900). Select OK

- Fill out the ACM Request

- Select OK

- Drag and drop the completed ACM Request into the ACM Request (Inbox) Folder

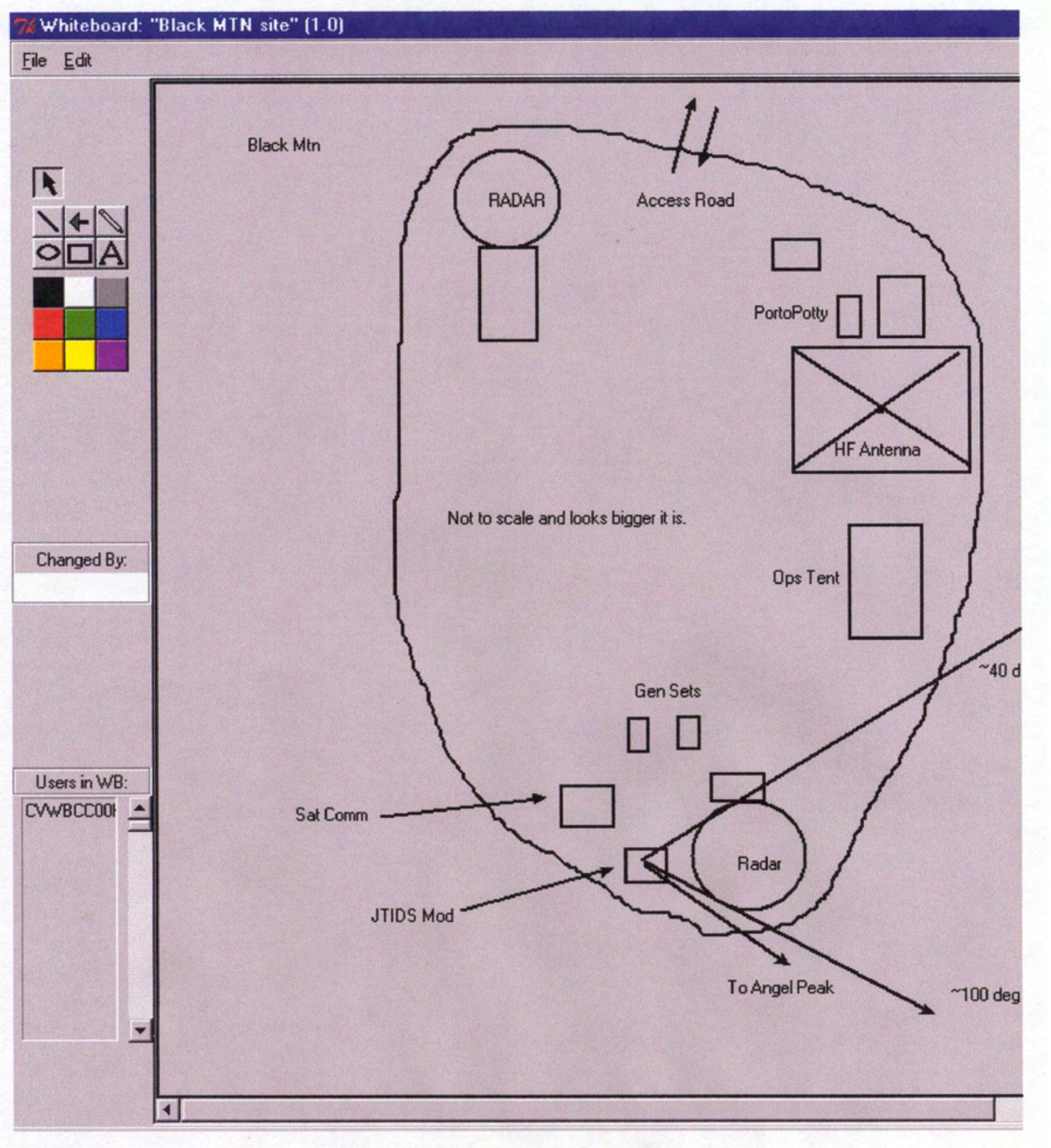
- The Airspace Control Cell (ACC) will deconflict the ACM Request

- The ACC will approve/disapprove the ACM request and coordinate any conflictions with the requester

- Once the ACM Request is completed, the ACC will drop it into the ACMREQ (Outbox) folder for the requester to review

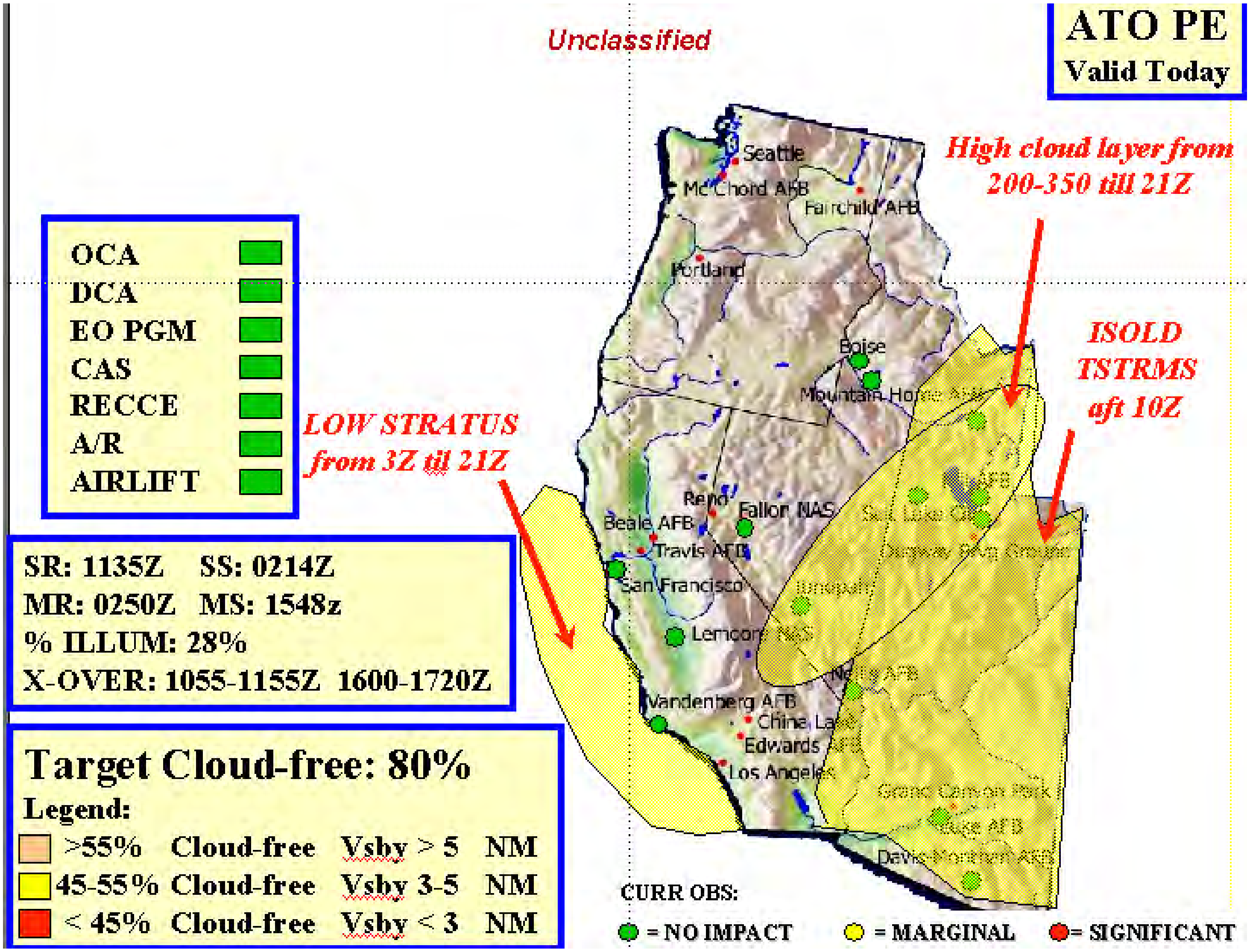
FROM AIRSPACE ROOM

Figure F.4 - 4th Floor – Combat Execution 2, continued



FROM JICO/RICO ROOM

Figure F.4 - 4th Floor – Combat Execution 2, continued



Unclassified

ATO PE
Valid Today

OCA	🟩
DCA	🟩
EO PGM	🟩
CAS	🟩
RECCE	🟩
A/R	🟩
AIRLIFT	🟩

SR: 1135Z SS: 0214Z
MR: 0250Z MS: 1548z
% ILLUM: 28%
X-OVER: 1055-1155Z 1600-1720Z

Target Cloud-free: 80%

Legend:

🟧 >55%	Cloud-free	Vsby > 5	NM
🟨 45-55%	Cloud-free	Vsby 3-5	NM
🟥 < 45%	Cloud-free	Vsby < 3	NM

LOW STRATUS from 3Z til 21Z

High cloud layer from 200-350 till 21Z

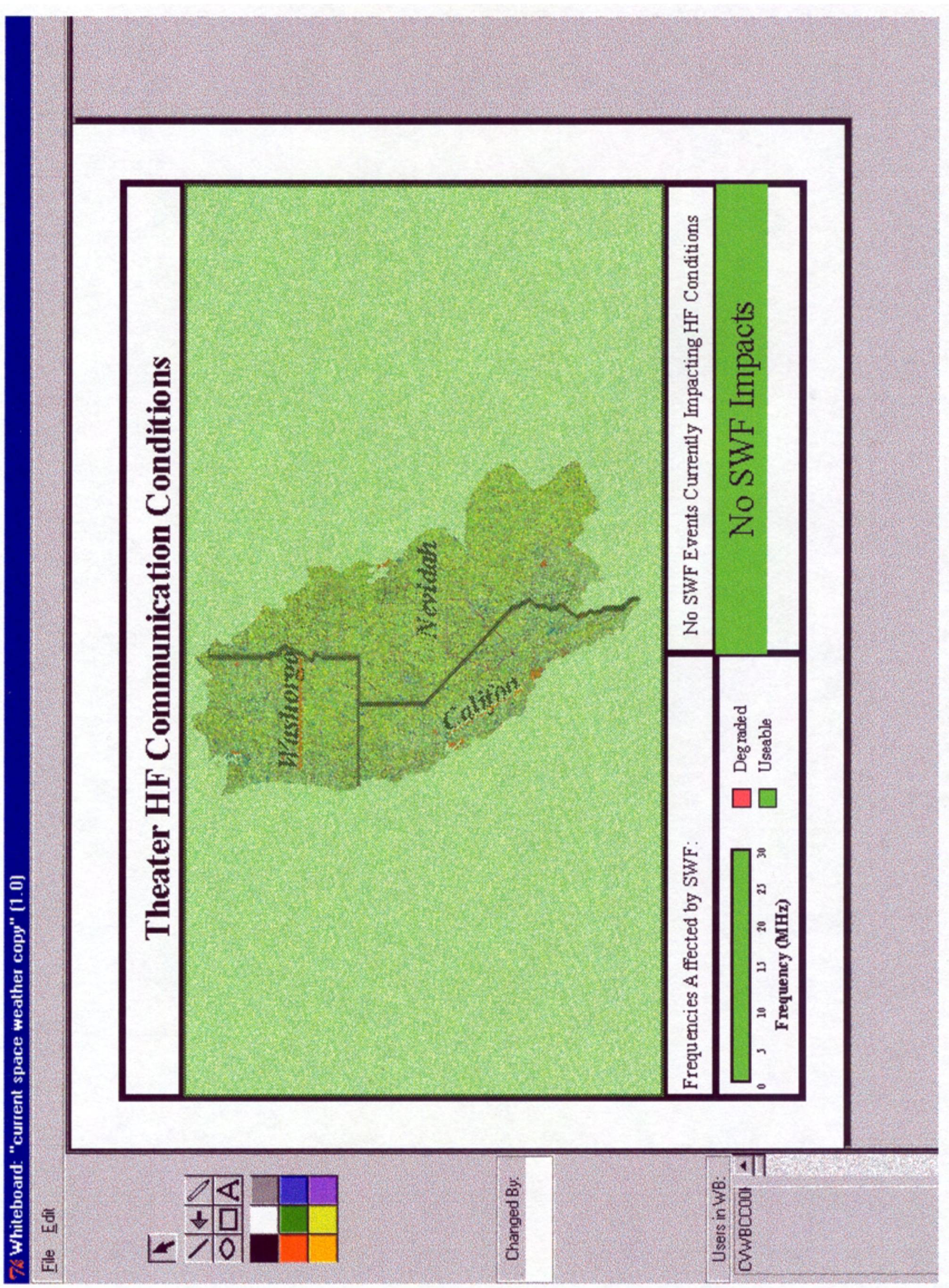
ISOLD TSTRMS aft 10Z

CURR OBS:

🟢 = NO IMPACT 🟡 = MARGINAL 🔴= SIGNIFICANT

FROM WEATHER ROOM

Figure F.4 - 4th Floor – Combat Execution 2, continued



Theater HF Communication Conditions

Frequencies Affected by SWF:

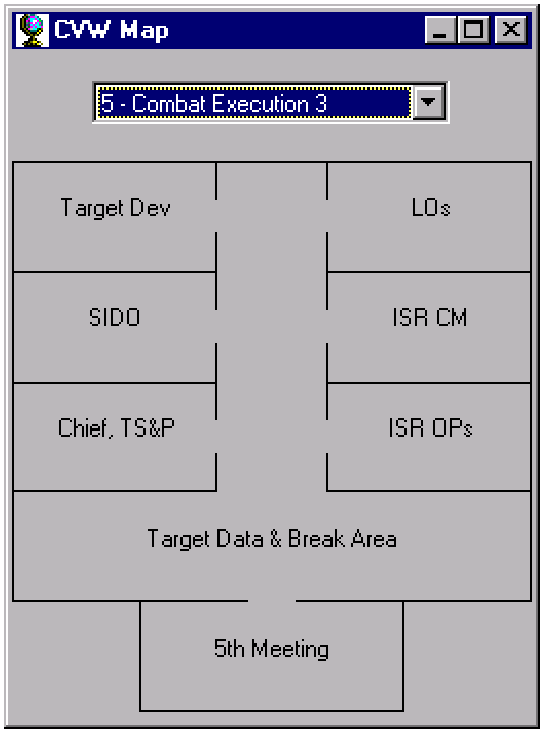
🟥 Degraded
🟩 Useable

No SWF Events Currently Impacting HF Conditions

No SWF Impacts

FROM WEATHER ROOM

Figure F.4 - 4th Floor – Combat Execution 2, concluded



Target Development (Target Development Team)
Significant Room Objects: Multiple spreadsheets containing Designated Mean Point of Impact (DMPI) Information; Surface to Air Missile Threats (Notes); Shortcut to Restricted Target List (XLS); Target Images (JPEG, GIF, Whiteboards)

LOs (Liaison Officers)
Significant Room Objects: Numerous objects in various media formats used by Liaison personnel for reference purposes

SIDO (Senior Information Duty Officer)
N/A

ISR CM (Intelligence, Surveillance, Reconnaissance-Collection Management CM))
Significant Room Objects: CM Administrative Folder containing duty rosters, phone logs, informational notes and text functionally organized into PSYOP, EW, Counterintelligence, MASINT, DISUMS and target data associated with each ATO; Daily Duty Logs (Notes); RFI folder for Info Warfare (IW) containing RFI Format, new, pending and answered RFIs, and the RFI log; ***RFI procedures; CM procedures***

Chief, TS&P_(Chief of Target Plans and Strategy Division)
N/A

ISR OPs_(ISR Operations)
Significant Room Objects: ISR Tracks on Whiteboard; Hyperspectral Images on JPEGs and Whiteboards; ISR related notes; MS Office ISR products; Predator reports folder consisting of multiple Predator-derived information on Notes; TCT folder consisting of TCT guidance, references and ***procedures*** for ISR personnel; Theater Missile Intelligence Preparation of the Battlespace (TM-IPB) folder with PowerPoint graphics for each day

Target Data & Break Area (Reference Repository as required)
N/A

5th Meeting_ (Briefing, Planning and Meeting Space)
N/A

Figure F.5 - 5th Floor – Combat Execution 3

RFI Process.txt

*** INFORMATION WARFARE CELL RFI PROCESS ***

(Note, this only applies to members of the IW cell)

To submit RFIs, through the IWF RFI manager, please follow the proceeding steps:

1. Make a copy of the note called "RFI format".

**** BIG NOTE: please use only note format (not Word, or text editor, or excel, etc). This facilitates getting the RFIs answered as some people do not have access to WinCenter. ***

2. Fill out all sections (it will be returned to you if not complete).

3. Place the note in the "New RFIs" folder (located in the RFIs folder).

4. Either page, or via audio, let 1Lt xxx or TSgt xxx know you have submitted a new RFI.

When one of the RFI managers reviews your RFI, they will then place it in the "Pending RFIs" folder, and annotate it on the RFI log note.

When the RFI is answered, you will receive a page, or via audio, a notice that your RFI is complete. All answered RFIs will be placed in the "Answered RFIs" folder, and annotated on the RFI log. If you are not satisfied with the answer given, please re-submit the RFI using the above steps and note that it is a clarification of a previous RFI.

Any questions, please contact 1Lt xxx (5-1120) or TSgt xxx (5-xxxx).

FROM AIRSPACE ROOM

Figure F.5 - 5th Floor – Combat Execution 3, continued

Collection Management Process Checklist (OSC) copy.txt

0200Z (2300L) MAAP Planning Process begins

1. CMs must ensure all orbits are entered into LOOK FORWARD (SCI & collateral) and all collection platforms are modeled appropriately.

2. Monitor Candidate Target List (CTL) inputs.

3. Monitor draft Target Nominations List (TNL) out of the JTWG (Joint Targets Working Group).

4. Initiate Planning process with draft TNL

   a. Work with Tech support personnel to ensure TNL is plotted/loaded into LOOK FORWARD.

   b. Run multiple queries in LOOK FORWARD against the draft TNL with each reconnaissance asset to obtain "Target Access Lists" (TAL) for each collector. Bring this information to the STAG and MAAP planning working groups.

   c. Ensure current SIGINT tasking includes corresponding ELNOTs to appropriate ELINT-capable targets in the TNL (for both sim and live fly play).

   d. Continue to monitor TNL status and update these lists accordingly by adding and/or deleting new/outdated targets.

5. Draft IMINT Reconnaissance Apportionment Plan (Use Recce TAL as a guide)

   a. Use CFACC guidance and information out of the STAG to set target priorities.

   b. Obtain ATO Strike times for targets; group target sets up by strike times.

   c. Organize top priority targets on the most optimum collector and set TOT time for the corresponding orbit to ensure first priority targets are collected in the post-strike timeframe (as soon as possible after most of the targets have been struck. Collection start position on the orbit should be synchronized with the first target for strike operations, etc. If the geographic layout of the assigned target set does not allign with chronological strike times, collection TOTs for each platform must be set after the last strike TOT of the target set.

   d. After top priority targets have been allocated, follow the same procedure for allocation of lower priority targets. Since target sets are organized by strike times, check to see if lower priority targets in each set can be allocated to the same collection platforms as the high priority targets in each targets set.

   e. Always check to see if the apportionment plan agrees with the TAL!

1200Z (0900L) MAAP Planning Process ends

6. Non-ATO Collection Requirements

   a. Task these requirements to the collection management cell in a variety of methods to include: via STU III and the Collaborative Virtual Workspace (CVW) to the CM cell; through the Production cell RFI Manager; and possibly direct from the Intelligence Operations (IO)/Warfare (IW) Cell. The majority of these requirements will be HUMINT, IO/IW or requests for prior collected IMINT and SIGINT products.

   b. HUMINT: Coordinate requirements with C2TIG Experiment Control personnel to obtain scripted responses; IMINT requirements for existing products will be coordinated through the OSC IMINT analyst for access to the JEFX IPL and assistance with identifying the requested imagery Requests for existing SIGINT products should be coordinated through the SIGINT CM for research in IRIS for the available report/product.

   c. MASINT: Perform an initial effort to emplace all UMS sensors throughout the experiment play area prior to execution. Throughout execution, OSC MASINT CMs will monitor UMS collection activities via

TBMCS/SAA and provide reachback support to DBC collection managers for dissemination, as appropriate.

d. SIGINT: Requests

7. Populate all apportionment information into a Collection Plan Matrix in preparation for the Daily Aerial Reconnaissance Scheduling (DARS) Working group. Matrix should be titled after the ATO it supports and should contain the following fields:

   a. Collection Platform

   b. Orbit/Mission designator (name/number) & TOT

   c. Corresponding targets

   d. Collection Status for each target (this field should also include, whenever possible, whether a target has been deleted or a new one added during the execution phase of the ATO in support of dynamic retasking efforts). DBC collection managers should have access to this matrix to update this level of information.

   e. Remarks/BDA levels (this information should be derived from the OSC Combat Assessment Cell and any BDA information received directly from the DBC should be included in the matrix and coordinated with the Combat Assessment Cell.

8. The DARS will be held on a daily basis and will be chaired by OSC collection managers.

   a. Members shall include:

      (1) OSC CMs (IMINT/SIGINT/MASINT/HUMINT)
      (2) OSC IMINT Analyst
      (3) DBC CMs (same disciplines as OSC)
      (4) DBC Sensor Rep(s)
      (5) Combat Assessment Rep
      (6) Weather Rep
      (7) Recce MAAP planner(s)
      (8) LOOK FORWARD Rep(s)
      (9) C2TIG Control Rep (Recce)

   b. Agenda for discussion will include but not be limited to:

      (1) Threat Update (source: OSC Combat Assessment)
      (2) Weather Update (source: JEFX Weather web site)
      (3) DBC Review of Current ATO collection execution efforts
      (4) OSC Collection Plan
      (5) Discussion
      (6) Final Plan Accepted for tasking on future ATO

9. OSC MAAP collection managers will take recce platforms, orbits, and TOTs and ensure this information is coordinated with Operations MAAP counterparts for ATO input.

FROM ISR CM ROOM

Figure F.5 - 5th Floor – Combat Execution 3, continued

CMPLANNING CYCLE for ATO.txt

1500Z (CVW) BRIEFING IN THE CURRENT INTEL INFORMATION CENTER ROOM ON CVW

PLANNING CYCLE FOR ATO "PA"

25 AUG	(1200Z)	STRAT BEGINS (CVW BRIEF)
26 AUG	(1200Z)	TGT NOMS DUE
	(1400Z)	JTWG -- DRAFT TNL (CVW BRIEF)
	(1500Z)	GAT MTG (CVW)/ DRAFT JIPTL DUE
	(1600Z)	DARS/COLLECTION MTG (CVW)
	(1700Z)	STAG BRIEF (CFACC/CVW BRIEF)
	(2200Z)	"NOTIONAL" JTCB
	(0000Z)	TNL PUSH (NLT)
27 AUG	(1000Z)	MAAP/ATO PRODUCTION BEGINS
	(1900Z)	MAAP BRIEF (CFACC/CVW BRIEF)
	(2300Z)	ATO "PA" RELEASED (NLT)
28 AUG	(0000Z)	ATO "PA" PUSHED (NLT)
29 AUG	(1300Z)	ATO "PA" FLY

PLANNING CYCLE FOR ATO "PB"

26 AUG	(1200Z)	SRAT BEGINS (CVW BRIEF)
27 AUG	(1200Z)	TGT NOMS DUE
	(1400Z)	JTWG -- DRAFT TNL (CVW BRIEF)
	(1500Z)	GAT MTG (CVW)/DRAFT JIPTL DUE
	(1600Z)	DARS/COLLECTION MTG (CVW)
	(1700Z)	(CFACC/CVW BRIEF)
	(1900Z)	STAG BRIEF
	(2200Z)	"NOTIONAL" JCTB
	(0000Z)	TNL PUSH (LATEST)
28 AUG	(1000Z)	MAAP/ATO PRODUCTION BEGINS
	(1900Z)	MAAP BRIEF (CFACC/CVW BRIEF)
	(2300Z)	ATO "PB" RELEASED (NLT)
29 AUG	(000Z)	ATO "PB" PUSHED (NLT)
30 AUG	(1300Z)	ATO "PB" FLY

PLANNING CYCLE FOR ATO "PC"

28 AUG	(1200Z)	STRAT BEGINS (CVW BRIEF)
29 AUG	(1200Z)	TGT NOMS DUE
	(1400Z)	JTWG -- DRAFT TNL (CVW BRIEF)
	(1500Z)	GAT MTG (CVW)/DRAFT JIPTL DUE
	(1600Z)	DARS/COLLECTION MTG (CVW)
	(1700Z)	(CFACC/CVW BRIEF)
	(1900Z)	STAG BRIEF
	(2200Z)	"NOTIONAL" JTCB

	(0000Z)	TNL PUSH (LATEST)
30 AUG	(1000Z)	MAAP/ATO PRODUCTION BEGINS
	(1900Z)	MAAP BRIEF (CFACC/CVW BRIEF)
	(2300Z)	ATO "PC" RELEASED
31 AUG	(0000Z)	ATO "PC" PUSHED
	(1300Z)	ATO "PC" FLY

PLANNING CYCLE FOR ATO "PD"

29 AUG	(1200Z)	STRAT BEGINS (CVW BRIEF)
30 AUG	(1200Z)	TGT NOMS DUE
	(1400Z)	JTWG -- DRAFT TNL (CVW BRIEF)
	(1500Z)	GAT MTG (CVW)/DRAFT JIPTL DUE
	(1600Z)	DARS/COLLECTION MTG (CVW)
	(1700Z)	(CFACC/CVW BRIEF)
	(1900Z)	STAG BRIEF
	(2200Z)	"NOTIONAL" JTCB
	(0000Z)	TNL PUSH (LATEST)
31 AUG	(1000Z)	MAAP/ATO PRODUCTION BEGINS
	(1900Z)	MAAP BRIEF (CFACC/CVW BRIEF)
	(2300Z)	ATO "PD" RELEASED
01 SEP	(0000Z)	ATO "PD" PUSHED
	(1300Z)	ATO "PD" FLY

PLANNING CYCLE FOR ATO "PE"

30 AUG	(1200Z)	STRAT BEGINS (CVW BRIEF)
31 AUG	(1200Z)	TGT NOMS DUE
	(1400Z)	JTWG -- DRAFT TNL (CVW BRIEF)
	(1500Z)	GAT MTG (CVW)/DRAFT JIPTL DUE
	(1600Z)	DARS/COLLECTION MTG (CVW)
	(1700Z)	(CFACC/CVW BRIEF)
	(1900Z)	STAG BRIEF
	(2200Z)	"NOTIONAL" JTCB
	(0000Z)	TNL PUSH (LATEST)
01 SEP	(1000Z)	MAAP/ATO PRODUCTION BEGINS
	(1900Z	MAAP BRIEF (CFACC/CVW BRIEF)
	(2300Z)	ATO "PE" RELEASED
02 SEP	(0000Z)	ATO "PE" PUSHED
	(1300Z)	ATO "PE" FLY

FROM ISR CM ROOM

Figure F.5 - 5th Floor – Combat Execution 3, continued

WF+ to TCT Process.txt

Waterfall + (WF+) will create a package of data containing maps of various scales, optical satellite images, and the current Global Hawk UAV radar image.

A WF+ operator will disseminate this image target package via a system called DPG to a SIPRNET web page accessible on Netscape. The URL for this webpage is:

After an imagery interpreter/analyst has put the target package on the web page he will notify the collection manager, TCT and RPTS personnel via the CVW phone and page function (pop-up window) to tell them what the file name is. These sections can then call up the file and view the target package to do whatever magic they do with it.

TCT File Naming and Target Priorities.txt

This is a recommendation to CAOC personnel on how Waterful Plus imagery interpreters should name TCT target packages during the live fly. Additionally, there is a prioritized list of target types we should look for during the live fly.

When naming the mission (which becomes the file name in Netscape) in DPG, BCC imagery analysts will use the following file naming process:

BCC_1, BCC_2, and increase numerically

COAC imagery anaysts should use the following file naming process:

CAOC_1, CAOC_2 and increase numerically

The suggested prioritized list of target types we should look for during TCT scanning follows:

Priority 1	***SSMs (Scuds and Frogs)***
Priority 2	***Mobile SAMS***
Priority 3	***AAA (Self-propelled, towed)***
Priority 4	***Military convoy***
Priority 5	***Staging areas***

WF+ Imagery Process.txt

All mission active imagery analysts (IAs) will move to the hall immediately west of the ISR OPs room and communicate via CVW phone there. Hurlburt IAs are under BCC control during live fly operations.

When the first Global Hawk image comes in to Water Fall all four imagery interpreters (2 at Nellis and 2 at Hurlburt) will view that image. The senior ranking Imagery Analyst (either xxx or xxx) will be lead IA. If a TCT is found, either the IA that found it will create the DPG product, or the lead IA will assign an IA to create the DPG package (DPG package creation instructions are in note named "WF+ TCT Prosecution" in this room). In the event multiple TCTs are found, a retask request comes in or is identified, or a cross cue from another ISR platform comes in, the lead IA will assign another available IA to process that function(s). If all IAs are engaged in a task, the lead IA will coordinate with them via CVW phone to find who will be available next to perform and assign the task to the appropriate IA.

Once an IA completes the task he was delegated, he will join the continuous scan of current WF images with the lead IA. If all IAs are still engaged in a task and the current image is completed, the lead IA will move to the next WF image. If he finds a TCT before another IA joins him in exploiting the image, he will IA chip the TCT area and verbally tell which IA he wants to create the DPG package. When all directed tasks are complete, all IAs will join the lead IA to scan the image he is currently scanning.

Imagery can come across several in a couple of minutes or one in anywhere from 5 to 20 minutes. If time permits between the next image arriving and previously identified tasks are still pending the lead IA will help complete the backlog of tasks.

WF+ TCT Prosecution.txt

1. ***Detect TCT***
2. ***Create chip and send it to the IPL***
3. ***Notify BCC TCT group of target type, coordinates, filename on IPL. Filename on IPL will be WF+ GLOBALHAWK "DTG" "TARGET NAME"***

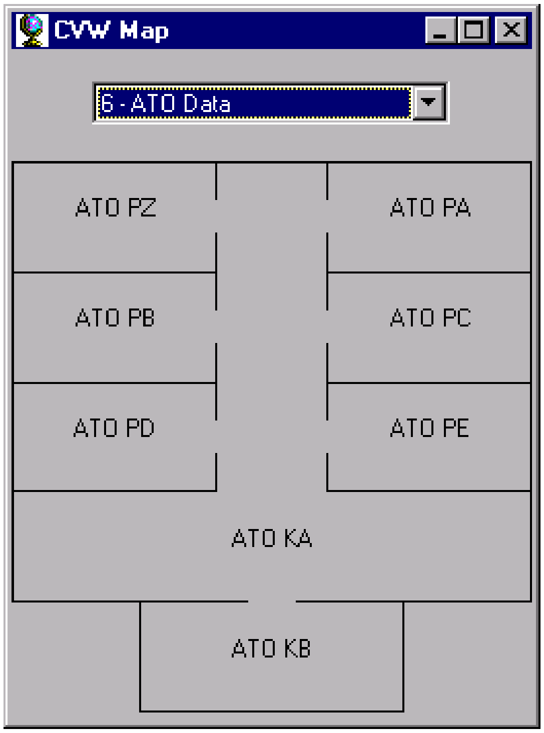
NOTE: DTG is the date time group, not the letters DTG

NOTE: TARGET NAME is whatever the IA names the target

4. ***Create DPG***
5. ***Notify BCC TCT group that DPG is ready to be viewed on our website: httpxxxx***

FROM ISR Ops Room

Figure F.5 - 5th Floor – Combat Execution 3, concluded



ATO PB (Data Repository for ATO PB
Significant Room Objects: ATO PB associated data

ATO PC (Data Repository for ATO PC)
Significant Room Objects: ATO PC associated data

ATO PE (Data Repository for ATO PE)
Significant Room Objects: ATO PE associated data

ATO KA
N/A

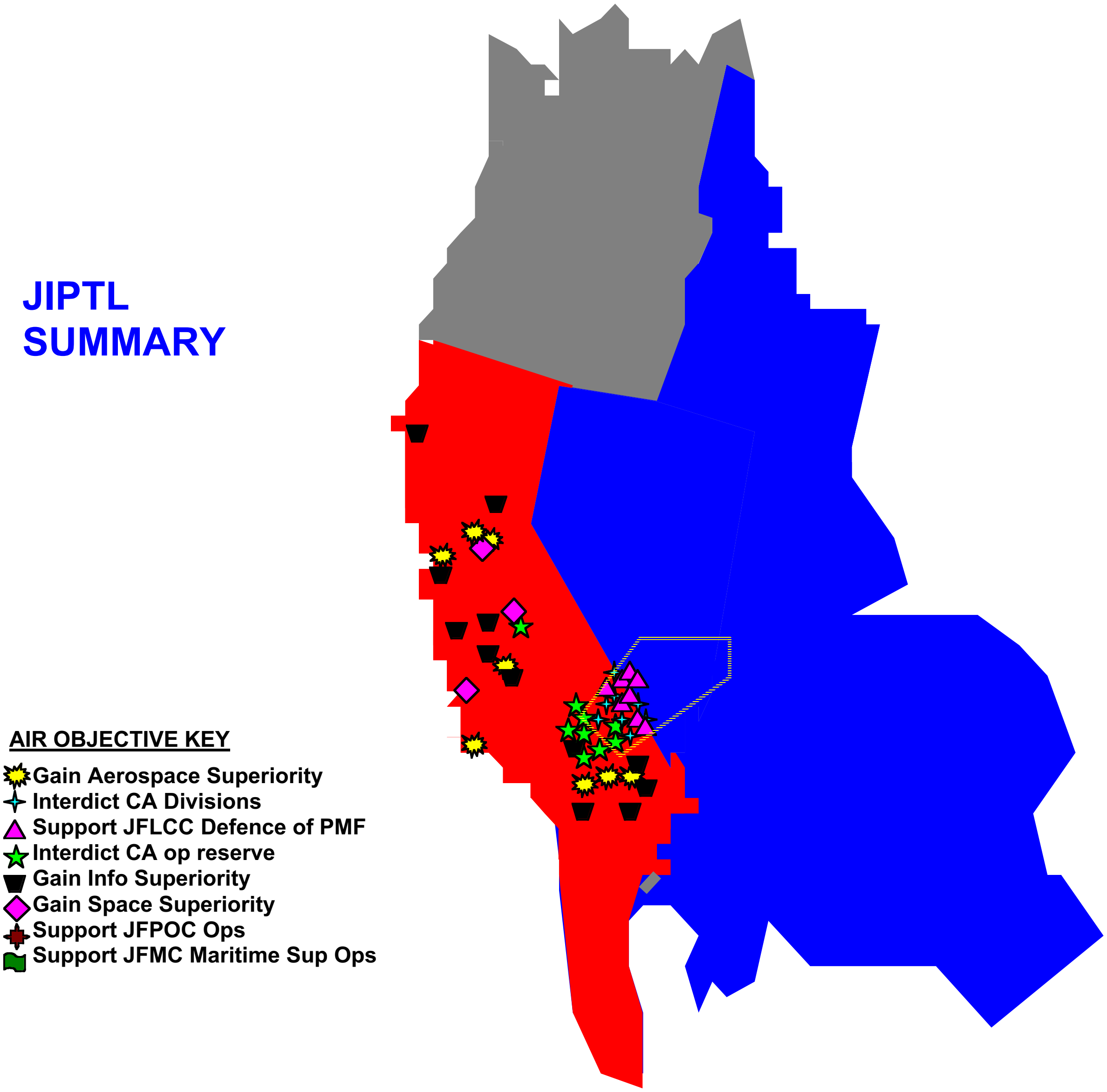
ATO KB
N/A

Figure F.6 - 6th Floor – ATO Data

ATO PZ (Data Repository for ATO PZ)
Significant Room Objects**:** ***ATO PZ Prioritized Task List*** (MS Word); Master Air Attack Plan (MAAP) Briefing for ATO PZ (PowerPoint)

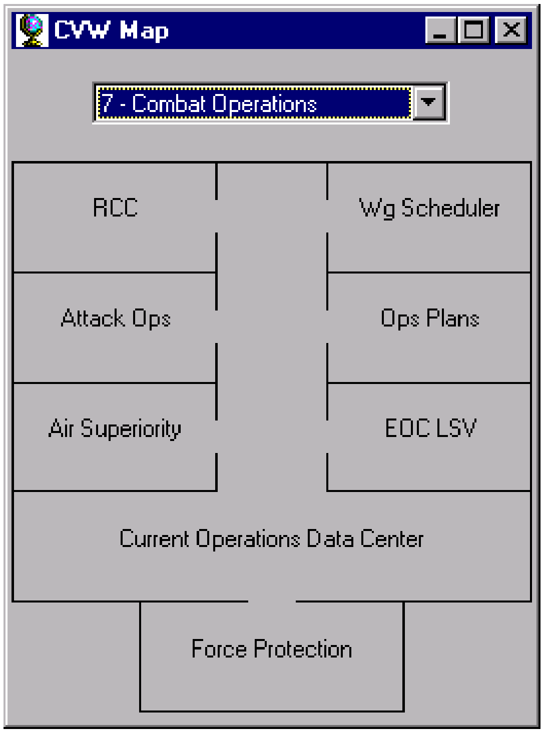
ATO PA (Data Repository for ATO PA)
Significant Room Objects: Target Nomination Lists (TNL), Directives, Briefings associated with ATO PA

ATO PB



FROM ATO PB ROOM

Figure F.6 - 6th Floor - ATO Data, concluded



RCC (Regional Control Center)
N/A

Wg Scheduler (Wing Scheduling Team)
N/A

Attack Ops (Attack Operations Team)
<u>Significant Room Objects</u>: Imagery (JPEG); Rapid Precision Target System (RPTS) reports (Notes); Predator Video Clips (MPEGs)

Ops Plans (Operations Plans)
N/A

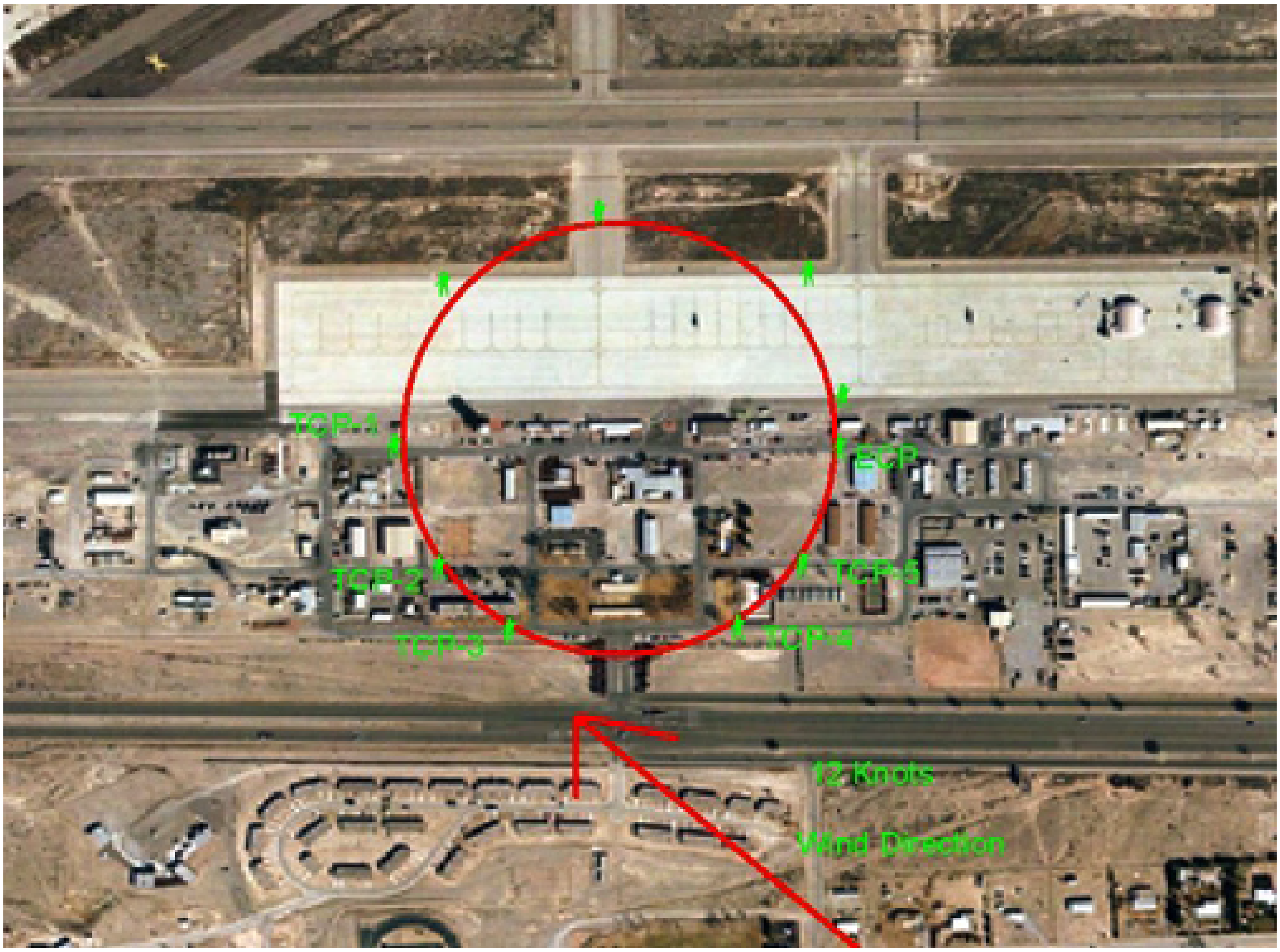
Air Superiority (Air Superiority Team)
N/A

EOC LSV (Expeditionary Operations Center Las Vegas)
<u>Significant Room Objects</u>: ***Force Protection (FP) Base Defense Operations Center (BDOC) SALUTE Form (MS Word); FP Situation Report (JPEG)***

Current Operations Data Center (Repository for Current Operations)
<u>Significant Room Objects</u>: Mountain Home Guidance (Note)

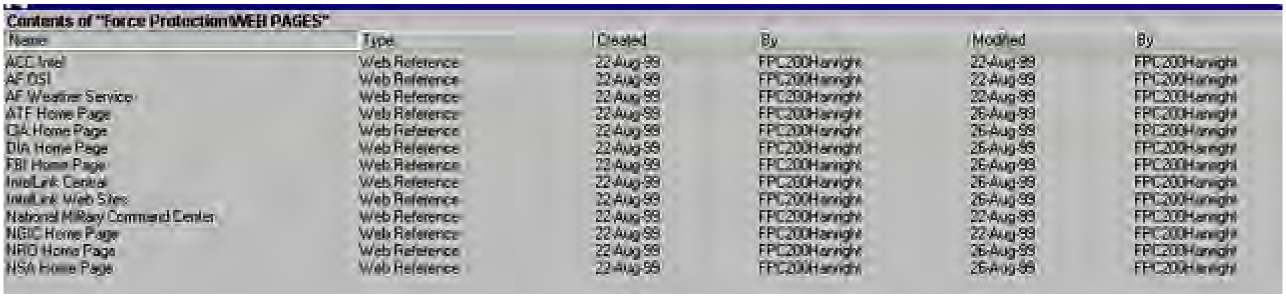
Force Protection (Force Protection Team)
<u>Significant Room Objects</u>: FP Group Object; SITREP documents; ***FP Web Pages Folder consisting of SIPRNET web references***

Figure F.7 - 7th Floor - Combat Operations



FROM EOC LSV ROOM

Figure F.7 - 7th Floor – Combat Operations, continued

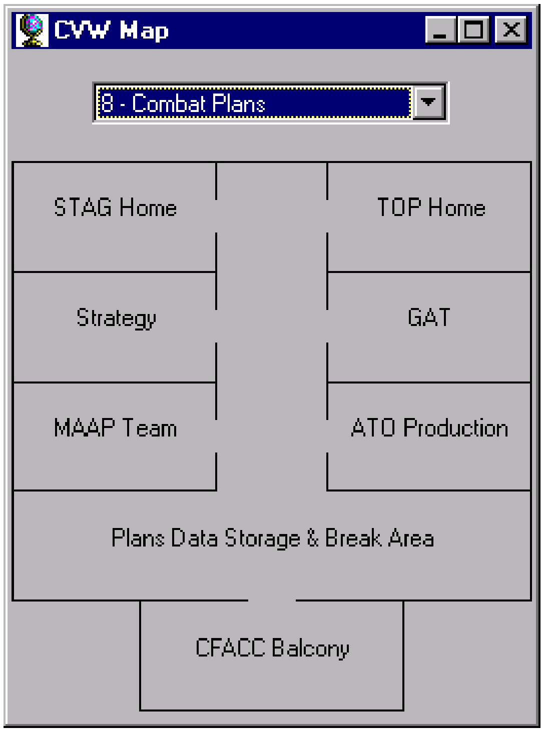


Contents of "Force Protection\WEB PAGES"

Name	Type	Created	By	Modified	By
ACC Intel	Web Reference	22-Aug-99	FPC200Hanright	22-Aug-99	FPC200Hanright
AF OSI	Web Reference	22-Aug-99	FPC200Hanright	22-Aug-99	FPC200Hanright
AF Weather Service	Web Reference	22-Aug-99	FPC200Hanright	22-Aug-99	FPC200Hanright
ATF Home Page	Web Reference	22-Aug-99	FPC200Hanright	26-Aug-99	FPC200Hanright
CIA Home Page	Web Reference	22-Aug-99	FPC200Hanright	26-Aug-99	FPC200Hanright
DIA Home Page	Web Reference	22-Aug-99	FPC200Hanright	26-Aug-99	FPC200Hanright
FBI Home Page	Web Reference	22-Aug-99	FPC200Hanright	26-Aug-99	FPC200Hanright
IntelLink Central	Web Reference	22-Aug-99	FPC200Hanright	26-Aug-99	FPC200Hanright
IntelLink Web Sites	Web Reference	22-Aug-99	FPC200Hanright	26-Aug-99	FPC200Hanright
National Military Command Center	Web Reference	22-Aug-99	FPC200Hanright	22-Aug-99	FPC200Hanright
NGIC Home Page	Web Reference	22-Aug-99	FPC200Hanright	22-Aug-99	FPC200Hanright
NRO Home Page	Web Reference	22-Aug-99	FPC200Hanright	26-Aug-99	FPC200Hanright
NSA Home Page	Web Reference	22-Aug-99	FPC200Hanright	26-Aug-99	FPC200Hanright

FROM FP ROOM

Figure F.7 - 7th Floor – Combat Operations, concluded



STAG Home (Strategy and Guidance Team)
Significant Room Objects: Intelligence reports and messages in text and PowerPoint format; CFACC Decision Briefings (PowerPoint); ***Current Air Operations Directives Guidance (PowerPoint); JEFX STAG Battle Rhythm (MS Word)***; JEFX 99 Allocation Matrix (XLS); STAG process briefing (PowerPoint); Tailored Weather products (PowerPoint)

TOP Home
N/A

Strategy (Strategy Team)
Significant Room Objects: AODs (MS Word); AOD Briefings (PowerPoint); Hurricane Dennis real world web reference; Joint Guidance, Apportionment and Targeting (JGAT) Decision Briefings (PowerPoint); PSYOP proposal (PowerPoint); Strategy Briefings (PowerPoint); Weapons of Mass Destruction (WMD) Targeting Guidance (Microsoft Word)

GAT (Guidance, Apportionment and Targeting Team)
Significant Room Objects: GAT procedures documents

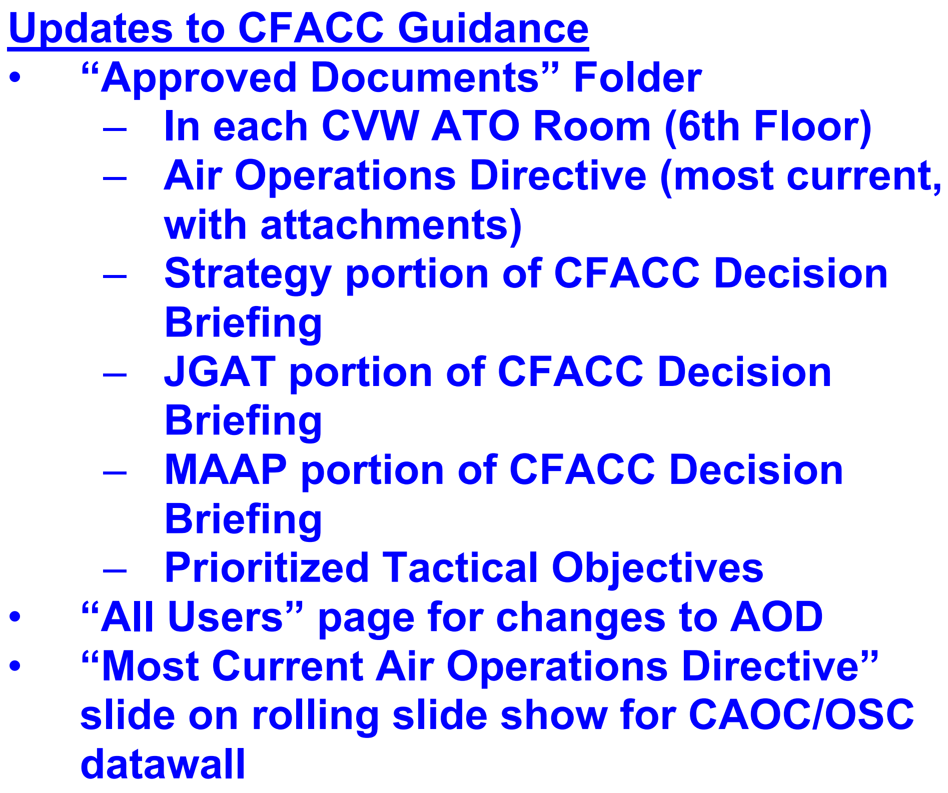
MAAP Team (Master Air Attack Plan Team)
Significant Room Objects: MAAP Briefing Shell (PowerPoint); ***JEFX 99 Bed Down Locations (PowerPoint);*** MAAP guidance (Notes); MAAP Timelines and Resources on XLS and PowerPoint; Navy input to MAAP on Notes and XLS; Weather input on PowerPoint, ***MAAP team whiteboards***

ATO Production (ATO Production Team)
Significant Room Objects: Various Special Purpose Instructions (SPINS) documents in text and Note format, Joint Special Operations Air Component (JSOAC) support packages in text

Plans Data Storage & Break Area
(Combat Plans Data and Information Resources)
Significant Room Objects: EAF C2 Process Manual V15.doc (MS Word); JEFX 99 OPORD (web ref); JEFX Joint Aerospace Plan (JAOP) (MS Word); JEFX Phase II Objectives (MS Word); JAOP in PowerPoint format

CFACC Balcony (Balcony of the CFACC Briefing Center on the 2d floor)
Significant Room Objects: CFACC briefings as web references; JEFX 99 Threads in PowerPoint; *Master Caution Panel Critical Process Flow (PowerPoint)*

Figure F.8 - 8th Floor – Combat Floor



Updates to CFACC Guidance

- "Approved Documents" Folder
  - In each CVW ATO Room (6th Floor)
  - Air Operations Directive (most current, with attachments)
  - Strategy portion of CFACC Decision Briefing
  - JGAT portion of CFACC Decision Briefing
  - MAAP portion of CFACC Decision Briefing
  - Prioritized Tactical Objectives
- "All Users" page for changes to AOD
- "Most Current Air Operations Directive" slide on rolling slide show for CAOC/OSC datawall

FROM STAG HOME ROOM

Figure F.8 - 8th Floor – Combat Plans, continued

StAG
JEFX Battle Rhythm
Wednesday, 25 Aug 1999

Zulu	13	14	15	16	17	18	19	20	21	22	23	00	01	02	03	04	05	06	07	08	09	10	11
EDT	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	00	01	02	03	04	05	06	07
CDT	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	00	01	02	03	04	05	06
PDT	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	00	01	02	03	04

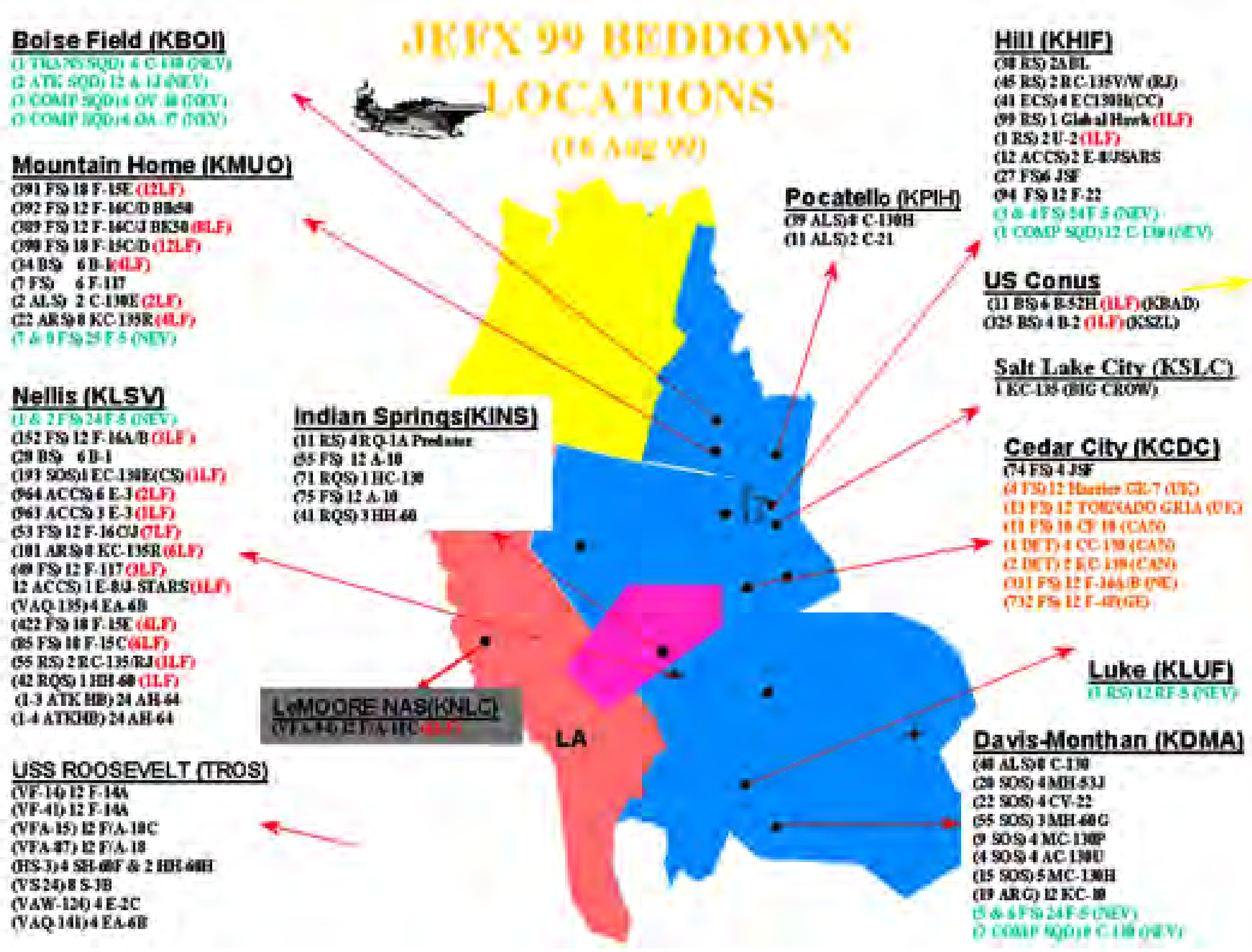
Strategy	**JGAT**	**TOP**	**Execution**
PA	**Open**	**KV25**	**Open**

Time	Event	Deliverable	Primary	Back-up	POC
1200 (Zulu) **0700 (CDT)** **0500 (PDT)**	**Strategy Meeting Preparation (PA)**	**Strat Meeting Slides (PA)**	***CVW* ATO (PA) Room**	*SIPRNET*	**SOC/IM**
1300 (Zulu) **0800 (CDT)** **0600 (PDT)**	**Strategy Meeting (PA)**	**Review**	*CVW* **Strategy Room**	**VTC** **STU III**	**Strat Chief**
1730 (Zulu) **1230 (CDT)** **1030 (PDT)**	**StAG Briefing** Preparation (PA)	**Updated Slides** **Draft AOD**	***CVW* ATO (PA) Room**	**SIPRNET**	**SOC/IM** **Strat Chief**
1900 (Zulu) **1400 (CDT)** **1200 (PDT)**	**StAG Briefing Apportionment (PA)**	**Review**	**CVW StAG Room**	**VTC** **STU III**	**StAG Chief**
2100 (Zulu) **1600 (CDT)** **1400 (PDT)**	**JFACC Guidance (PA)**	**Approved AOD**	***CVW* ATO (PA) Room**	**SIPRNET**	**Strat Chief**

FROM STAG HOME ROOM

Figure F.8 - 8th Floor – Combat Plans, continued

MAAP Beddown



JEFX 99 BEDDOWN LOCATIONS

(16 Aug 99)

Boise Field (KBOI)
(1 TRANS SQD) 4 C-130 (NEV)
(2 ATK SQD) 12 A-1J (NEV)
(3 COMP SQD) 4 OV-10 (NEV)
(3 COMP SQD) 4 OA-37 (NEV)

Mountain Home (KMUO)
(391 FS) 18 F-15E (12LF)
(392 FS) 12 F-16C/D BB50
(389 FS) 12 F-16C/J BK50 (8LF)
(390 FS) 18 F-15C/D (12LF)
(34 BS) 6 B-1 (4LF)
(7 FS) 6 F-117
(2 ALS) 2 C-130E (2LF)
(22 ARS) 8 KC-135R (4LF)
(7 & 8 FS) 25 F-5 (NEV)

Nellis (KLSV)
(1 & 2 FS) 24 F-5 (NEV)
(152 FS) 12 F-16A/B (3LF)
(20 BS) 6 B-1
(193 SOS) 1 EC-130E(CS) (1LF)
(964 ACCS) 6 E-3 (2LF)
(963 ACCS) 3 E-3 (1LF)
(53 FS) 12 F-16CJ (7LF)
(101 ARS) 8 KC-135R (6LF)
(49 FS) 12 F-117 (3LF)
12 ACCS) 1 E-8J-STARS (1LF)
(VAQ-135) 4 EA-6B
(422 FS) 18 F-15E (4LF)
(85 FS) 18 F-15C (4LF)
(55 RS) 2 RC-135/RJ (1LF)
(42 RQS) 1 HH-60 (1LF)
(1-3 ATK HB) 24 AH-64
(1-4 ATKHB) 24 AH-64

Indian Springs(KINS)
(11 RS) 4 RQ-1A Predator
(55 FS) 12 A-10
(71 RQS) 1 HC-130
(75 FS) 12 A-10
(41 RQS) 3 HH-60

LeMOORE NAS(KNLC)
(VFA-94) 12 F/A-18C (8LF)

USS ROOSEVELT (TROS)
(VF-14) 12 F-14A
(VF-41) 12 F-14A
(VFA-15) 12 F/A-18C
(VFA-87) 12 F/A-18
(HS-3) 4 SH-60F & 2 HH-60H
(VS24) 8 S-3B
(VAW-124) 4 E-2C
(VAQ-141) 4 EA-6B

Pocatello (KPIH)
(39 ALS) 8 C-130H
(11 ALS) 2 C-21

Hill (KHIF)
(38 RS) 2 ABL
(45 RS) 2 RC-135V/W (RJ)
(41 ECS) 4 EC130H(CC)
(99 RS) 1 Global Hawk (1LF)
(1 RS) 2 U-2 (1LF)
(12 ACCS) 2 E-8/JSARS
(27 FS) 6 JSF
(94 FS) 12 F-22
(3 & 4 FS) 24 F-5 (NEV)
(1 COMP SQD) 12 C-130 (NEV)

US Conus
(11 BS) 6 B-52H (1LF) (KBAD)
(325 BS) 4 B-2 (1LF) (KSZL)

Salt Lake City (KSLC)
1 KC-135 (BIG CROW)

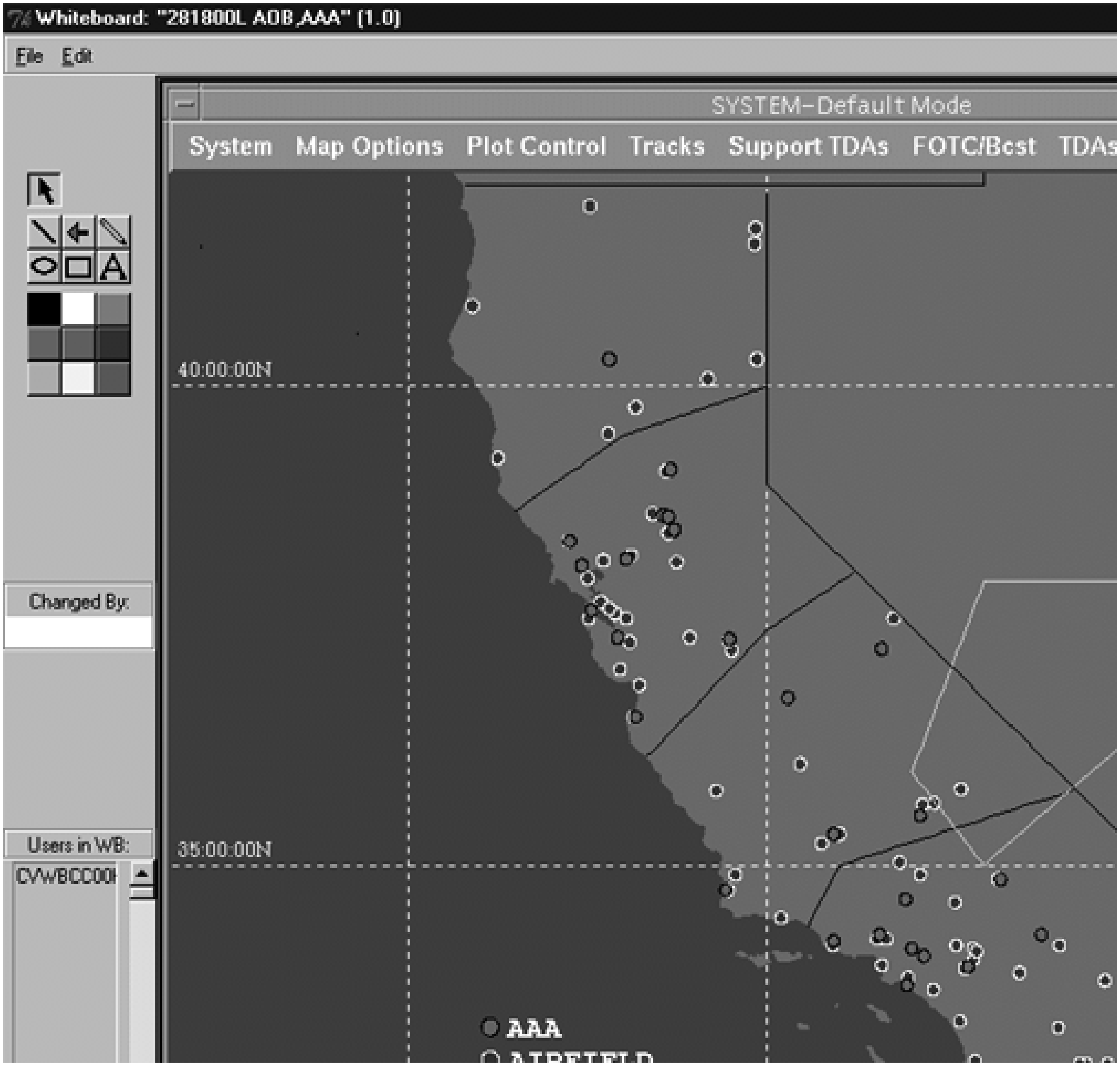
Cedar City (KCDC)
(74 FS) 4 JSF
(4 FS) 12 Harrier GR-7 (UK)
(13 FS) 12 TORNADO GR1A (UK)
(11 FS) 10 CF-18 (CAN)
(1 DET) 4 CC-130 (CAN)
(2 DET) 2 KC-130 (CAN)
(331 FS) 12 F-16A/B (NE)
(732 FS) 12 F-4F (GE)

Luke (KLUF)
(1 RS) 12 RF-5 (NEV)

Davis-Monthan (KDMA)
(40 ALS) 8 C-130
(20 SOS) 4 MH-53J
(22 SOS) 4 CV-22
(55 SOS) 3 MH-60G
(9 SOS) 4 MC-130P
(4 SOS) 4 AC-130U
(15 SOS) 5 MC-130H
(19 ARG) 12 KC-10
(5 & 6 FS) 24 F-5 (NEV)
(7 COMP SQD) 8 C-130 (NEV)

FROM MAAP TEAM ROOM

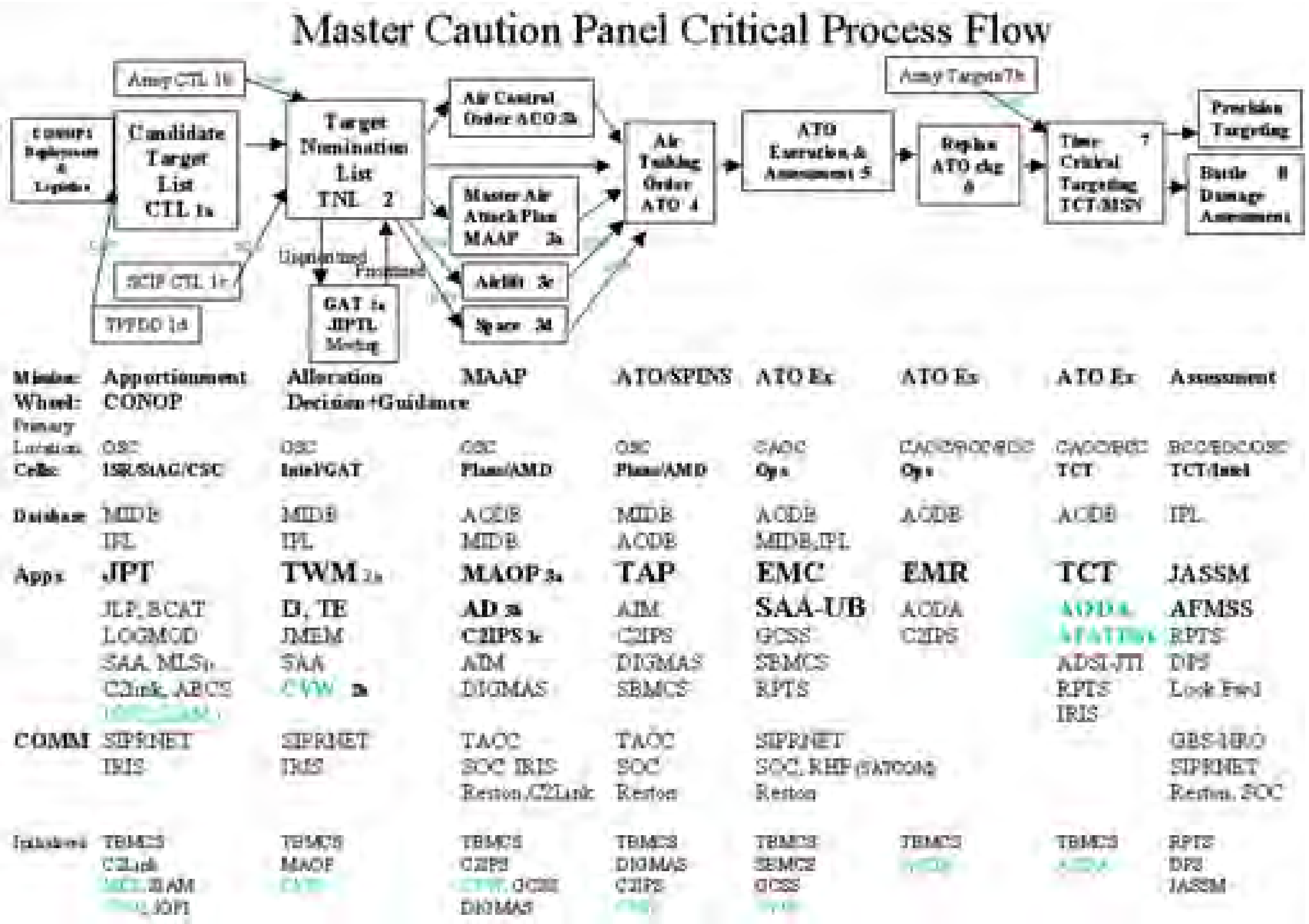
Figure F.8 - 8th Floor – Combat Plans, continued



Whiteboard: "281800L AOB,AAA" (1.0)
File Edit
SYSTEM–Default Mode
System Map Options Plot Control Tracks Support TDAs FOTC/Bcst TDAs
Changed By:
Users in WB:
CVWBCC00I
40:00:00N
35:00:00N
AAA
AIRFIELD

FROM MAAP TEAM ROOM

Figure F.8 - 8th Floor – Combat Plans, continued



Master Caution Panel Critical Process Flow

CONOPS Deployment & Logistics
Army CTL 1b
Candidate Target List CTL 1a
SCIF CTL 1c
TPFDD 1d
Target Nomination List TNL 2
Unprioritized
Prioritized
GAT 1a JIPTL Meeting
Air Control Order ACO 3b
Master Air Attack Plan MAAP 3a
Airlift 3c
Space 3d
Air Tasking Order ATO 4
ATO Execution & Assessment 5
Replan ATO chg 6
Army Targets 7b
Time Critical Targeting TCT/MSN 7
Precision Targeting
Battle Damage Assessment 8

Mission Wheel:	Apportionment CONOP	Allocation Decision+Guidance	MAAP	ATO/SPINS	ATO Ex	ATO Ex	ATO Ex	Assessment
Primary Location	OSC	OSC	OSC	OSC	CAOC	CAOC/SOC/RSC	CAOC/RSC	BCC/EDC/OSC
Cells:	ISR/SIAG/CSC	Intel/GAT	Plans/AMD	Plans/AMD	Ops	Ops	TCT	TCT/Intel
Database	MIDB IPL	MIDB IPL	ACDB MIDB	MIDB ACDB	ACDB MIDB,IPL	ACDB	ACDB	IPL
Apps	JPT JLP, BCAT LOGMOD SAA, MLS[illegible] C2link, ABCS [illegible]	TWM 2a I3, TE JMEM SAA CVW 2b	MAOP 3a AD 3b C2IPS 3c AIM DIGMAS	TAP AIM C2IPS DIGMAS SBMCS	EMC SAA-UB GCSS SBMCS RPTS	EMR ACDA C2IPS	TCT AODA AFATDS ADSI-JTI RPTS IRIS	JASSM AFMSS RPTS DPS Look Fwd
COMM	SIPRNET IRIS	SIPRNET IRIS	TACC SOC IRIS Reston,C2Link	TACC SOC Reston	SIPRNET SOC, RHF (SATCOM) Reston			GBS-HRO SIPRNET Reston, SOC
Interfaces	TBMCS C2Link MCL IBAM [illegible], JOPI	TBMCS MAOF [illegible]	TBMCS C2IPS CVW, GCSS DIGMAS	TBMCS DIGMAS C2IPS [illegible]	TBMCS SBMCS GCSS [illegible]	TBMCS [illegible]	TBMCS AODA	RPTS DPS JASSM

FROM CFACC Balcony

Figure F.8 - 8th Floor – Combat Plans, concluded

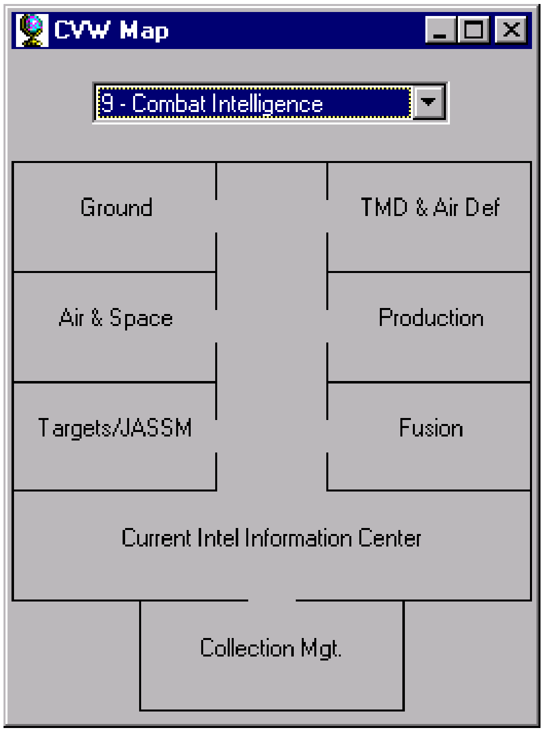


Figure F.9 - 9th Floor – Combat Intelligence

Ground (Ground Intelligence Team)
N/A

TMD & Air Def (Theater Missile Defense and Air Defense Intelligence Team)
Significant Room Objects: TMD IPB Products (PowerPoint)

Air & Space (Air and Space Intelligence Team)
Significant Room Objects: Meetings and Briefings Activity Schedule (Note); Space Phone roster (XLS); Synthetic Aperture Radar (SAR) Imagery on Whiteboards

Production (Intelligence Production Team)
Significant Room Objects: CFACC Briefing folder with production guidance and instructions; Info Operations Briefings (PowerPoint); Space Weather (web ref); RFI folder for ISR RFI Manager consisting of RFI process, New, pending and answered RFI folders, RFI log and Job descriptions in Note format; TACREP Updates folder with TACREPS posted onto notes

Targets/JASSM (Target and Joint Air-to-Surface Missile Team)
Significant Room Objects: Battle Damage Assessment (BDA) spreadsheet (XLS); JASSM-MSEL text document; Joint Integrated Prioritized Target Lists (JIPTL) for ATO's (GIF); Live Target DMPIs (XLS); Package Planning form (Note); Restricted Target List (MS Word); Target Legal Review folder; Space Imagery SAR on Whiteboards

Fusion (Intelligence Fusion Team)
Significant Room Objects: Enemy Order of Battle (OB) on PowerPoint and XLS; ***ISR Analysis Process (MS Word)***

Current Intel Information Center (Current Intelligence Data)
Significant Room Objects: 480th IG web reference; ***Briefing Production Guidance (Note);*** Current CFACC Briefings Folder, Current Live Tracks with Sensors (JPEG); ***DBC Targeting Input (Note);*** Daily Intelligence Summary (DISUM) folder; IRIS procedures (XLS); Meetings, Briefings, Activities Schedule (MS Word); Recce Schedule (PowerPoint); SAA Trouble Shooting Guidance MS Word) Folders for Space IO messages

Collection Mgt (Collection Management Team)
Significant Room Objects; Folders for each ATO with supporting documents (MS Word and PowerPoint); CM Process folder with schedules, planning cycles and procedures; ***CM Daily Aerial Reconnaissance Schedule (DARS) folder consisting of Whiteboards with imagery and DARS Agenda*** (Note); Imagery Folder with GIFs and text data; Live Fly Recce Tracks folder with JPEGs and text documents; Live fly Schedule (Note); Tailored weather web reference; Operational Support Center (OSC) CM Daily Read File (Note); Collection Decks Folders for ATOs

This note describes the process we are using to build and view the ISR input to the daily JFACC Situation Update Briefing

We have created a Blank Template that contains slides with classification markings and titles which conforms to the standards described in the Information Management Plan. This is locked and will only be accessed by the Production Cell. As changes are directed by the C2 and senior leadership, we will modify this file.

The Blank Template is essentially copied into a new document which becomes the active briefing we are working on. It's title will include the delivery date and be stored in the "Current JFACC Brief" folder in the Production room. This is the active briefing we are producing. All of us have access to this file and the ability to modify it. Remember that only one user can actually be modifying the briefing at a time. When you are ready to make your inputs, right click on the file and select "Open for Edit" When you do this, CVW will move the briefing to your Carry folder and launch Wincenter/PowerPoint. Make your changes and save in PowerPoint. Then Quit PowerPoint/Logoff Wincenter. The document will still be in your carry folder. You then need to right click on the file and select Save Changes. Now you can drag the file back into the "Current JFACC Brief" folder in the Production room.

Those who just want to look at the briefing during the production process can view it by "going" into the Current Intel Information Center. Once there, open the "Current JFACC Brief" folder. Double-click on "SC to JFACCdate file". This is a shortcut to the actual file and will allow you to view it. Just as with Opening the active file, this will launch Wincenter/PowerPoint. When you have completed your review, Exit out of PowerPoint/Logoff of Wincenter.

Although there was no specific shortfalls identified concerning OSC support to TP&S, there are several contributions the OSC Targeting Cell can offer the DBC process. Primarily these begin during the “fixed” target development and selection process that results in the JIPTL. Component discussions and priority deliberations during the Joint Target Working Group and the JGAT focus attention on target composition, importance, and time sensitivity. Many targets were moved “below the cut line” during these meetings because they were more appropriate and responsive as DBC targets. The best examples of these targets are ground units and unique airborne threats. Although the OSC targeteer was able to answer TP&S questions concerning some of these targets, the DBC reps could easily attend the JTWG/JGAT since they are held via CVW. This would enhance their knowledge of the targets. Other support included weaponeering data, which was available in TWM. TP&S personnel need TWM access and knowledge of the day’s targeting products, although OSC targeteers can assist them. The imagery support provided by the OSC RPTS operator seemed to facilitate DBC and allowed forward planners to move on to other targets while analysis was completed at the OSC. This type of research and support was also available and provided by all-source intelligence assessments personnel at the OSC; another good example of “distributed” support.

FROM CURRENT INTEL INFORMATION CENTER ROOM

Figure F.9 - 9th Floor – Combat Intelligence, continued

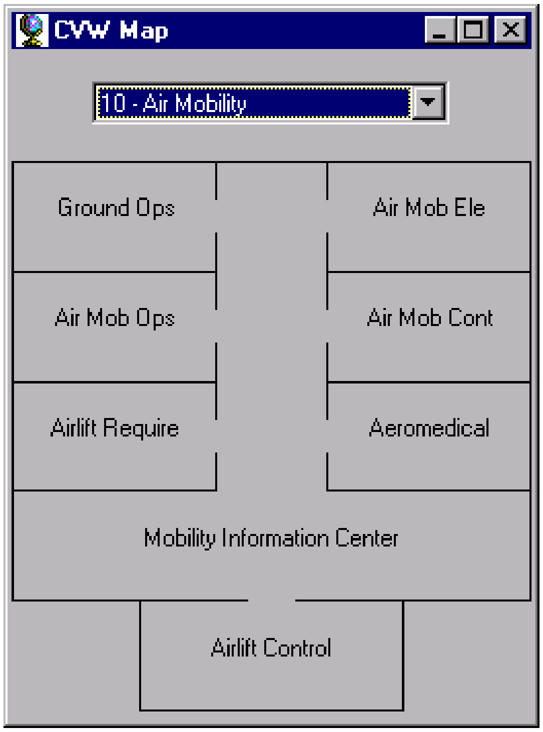
The Daily Aerial Reconnaissance Scheduling (DARS) Working Group will take place over CVW at 1600Z on the 26, 27, 29, 30, 31 in the COLLECTION MANAGEMENT room. The agenda and required attendees are listed below.

A. MEMBERS:
(1) OSC CMs (IMINT/SIGINT/MASINT/HUMINT)
(2) OSC IMINT Analyst
(3) CAOC CMs (IMINT/SIGINT/MASINT/IMINT)
(4) CAOC Sensor Rep(s) - Optional
(5) OSC Combat Assessment Rep
(6) OSC Weather Rep
(7) Recce MAAP planner(s)
(8) LOOK FORWARD Rep(s)
(9) C2TIG Control Rep (Recce)

B. AGENDA:
(1) WEATHER Update (OSC Weather Cell - DARS Weather Link file)
(2) THREAT Update (OSC Combat Assessment - Whiteboard)
(3) OSC ATO PLANNING CYCLE (OSC CM - Note)
-- Flying ATO PD ("Flies" Wednesday, 01Sep99)
-- Finalizing tasking activities for ATO PD (CB)
@ Tasking to AFDRO for Live National Collection today
@ Distributed Live collection plan to exploitation ctrs/Recce Launch locations
-- Finalizing coll plan for PE
**** No more planning***
(4) ATO PE Overview ("Flies" Today, 31Aug99)
-- PE TNL approx 53 live fly tgts; 95 sim tgts
-- Refer to EXCEL File for Collection Plan (proposed)
(5) DISCUSSION (CAOC CM Comments)
(6) Draft STRATEGY/OBJECTIVES & COLLECTION PLAN Acceptance ATO PE
-- Following Synch w/Strike times, OSC CMs will post final collection plan, ATO PE to CVW

FROM COLLECTION MGT ROOM

Figure F.9 - 9th Floor – Combat Intelligence, concluded



Ground Ops (Ground Operations Team)
Significant Room Objects: Theater Airlift Control Element (TALCE) Management Update (XLS)

Air Mob Ele (Air Mobility Element Team)
Significant Room Objects: Mission Notes for ATOs; Numerous Mobility Briefings (PowerPoint); ATO Changes (Notes); Tanker (Notes)

Air Mob Cont (Air Mobility Control Team)
N/A

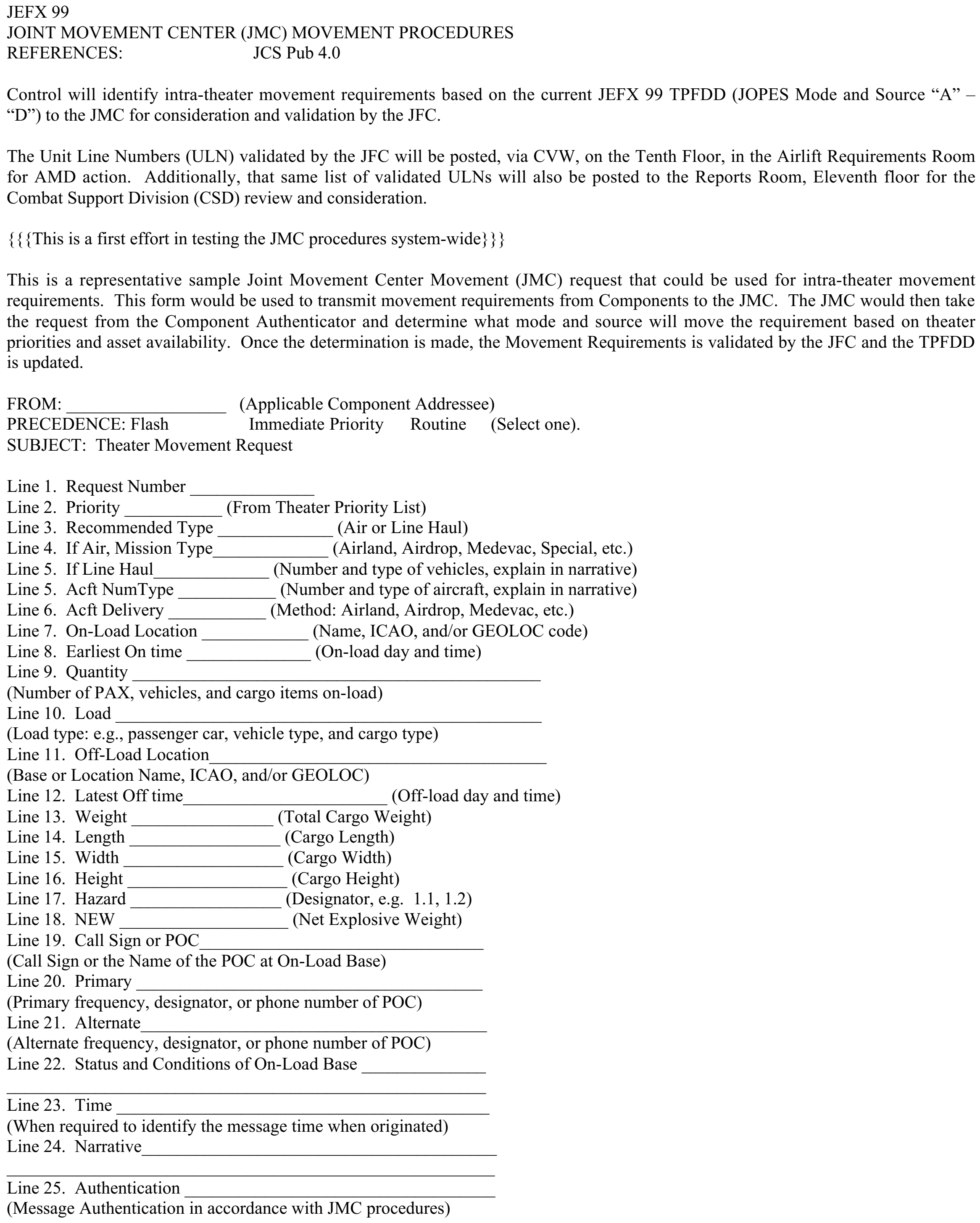
Airlift Require (Airlift Requirements Team)
Significant Room Objects: Time Phased Force Deployment Data (TPFDD) (XLS); ***Joint movement Center (JMC) Updates/Procedures folder with textual guidance documents***

Aeromedical (Aeromedical Evacuation (AE) Coordination Center)
Significant Room Objects: AF Form 3853 folder with text documents on guidance for AE; ***Medical Laydown (PowerPoint);*** Message Tracker text

Mobility Information Center (Air Mobility Information and Resources)
Significant Room Objects: Mission Documents; Air Mobility Division (AMD) Intelligence folder with DISUMs and AMD Intelligence Briefings (PowerPoint); Strategic Airlift daily reports (MS Word)

Airlift Control (Airlift Control Team)
Significant Room Objects: Airlift Control log (Folder with notes); C2 Logs (MS Word); Tanker Plans Log (Folder with daily notes)

Figure F.10 - 10th Floor – Air Mobility



JEFX 99
JOINT MOVEMENT CENTER (JMC) MOVEMENT PROCEDURES
REFERENCES: JCS Pub 4.0

Control will identify intra-theater movement requirements based on the current JEFX 99 TPFDD (JOPES Mode and Source “A” – “D”) to the JMC for consideration and validation by the JFC.

The Unit Line Numbers (ULN) validated by the JFC will be posted, via CVW, on the Tenth Floor, in the Airlift Requirements Room for AMD action. Additionally, that same list of validated ULNs will also be posted to the Reports Room, Eleventh floor for the Combat Support Division (CSD) review and consideration.

{{{This is a first effort in testing the JMC procedures system-wide}}}

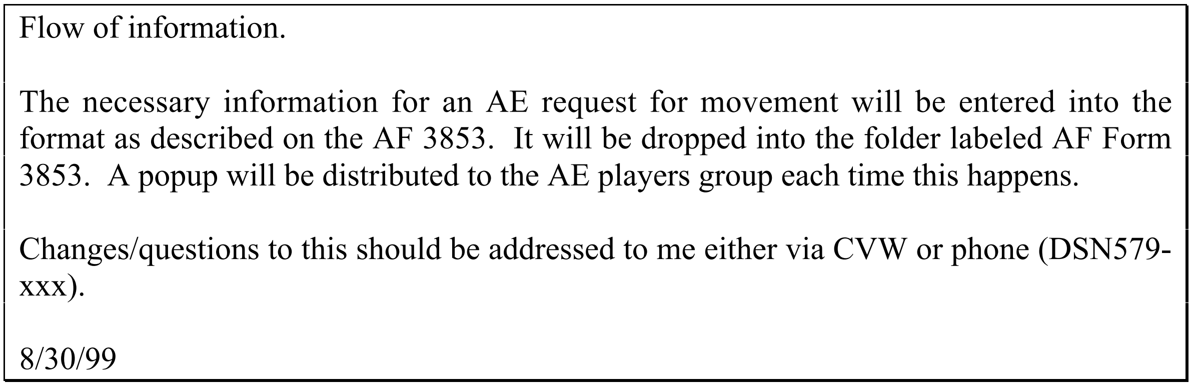
This is a representative sample Joint Movement Center Movement (JMC) request that could be used for intra-theater movement requirements. This form would be used to transmit movement requirements from Components to the JMC. The JMC would then take the request from the Component Authenticator and determine what mode and source will move the requirement based on theater priorities and asset availability. Once the determination is made, the Movement Requirements is validated by the JFC and the TPFDD is updated.

FROM: __________________ (Applicable Component Addressee)
PRECEDENCE: Flash Immediate Priority Routine (Select one).
SUBJECT: Theater Movement Request

Line 1. Request Number ______________
Line 2. Priority ___________ (From Theater Priority List)
Line 3. Recommended Type _____________ (Air or Line Haul)
Line 4. If Air, Mission Type_____________ (Airland, Airdrop, Medevac, Special, etc.)
Line 5. If Line Haul_____________ (Number and type of vehicles, explain in narrative)
Line 5. Acft NumType ___________ (Number and type of aircraft, explain in narrative)
Line 6. Acft Delivery ___________ (Method: Airland, Airdrop, Medevac, etc.)
Line 7. On-Load Location ____________ (Name, ICAO, and/or GEOLOC code)
Line 8. Earliest On time ______________ (On-load day and time)
Line 9. Quantity ____
(Number of PAX, vehicles, and cargo items on-load)
Line 10. Load ____
(Load type: e.g., passenger car, vehicle type, and cargo type)
Line 11. Off-Load Location_____________________________________
(Base or Location Name, ICAO, and/or GEOLOC)
Line 12. Latest Off time______________________ (Off-load day and time)
Line 13. Weight _______________ (Total Cargo Weight)
Line 14. Length ________________ (Cargo Length)
Line 15. Width _________________ (Cargo Width)
Line 16. Height _________________ (Cargo Height)
Line 17. Hazard ________________ (Designator, e.g. 1.1, 1.2)
Line 18. NEW __________________ (Net Explosive Weight)
Line 19. Call Sign or POC_______________________________
(Call Sign or the Name of the POC at On-Load Base)
Line 20. Primary ____________________________________
(Primary frequency, designator, or phone number of POC)
Line 21. Alternate_____________________________________
(Alternate frequency, designator, or phone number of POC)
Line 22. Status and Conditions of On-Load Base _____________
____
Line 23. Time ____
(When required to identify the message time when originated)
Line 24. Narrative_____________________________________
____
Line 25. Authentication __________________________________
(Message Authentication in accordance with JMC procedures)

FROM AIRLIFT REQUIRE ROOM

Figure F.10 - 10th Floor – Air Mobility, continued



Flow of information.

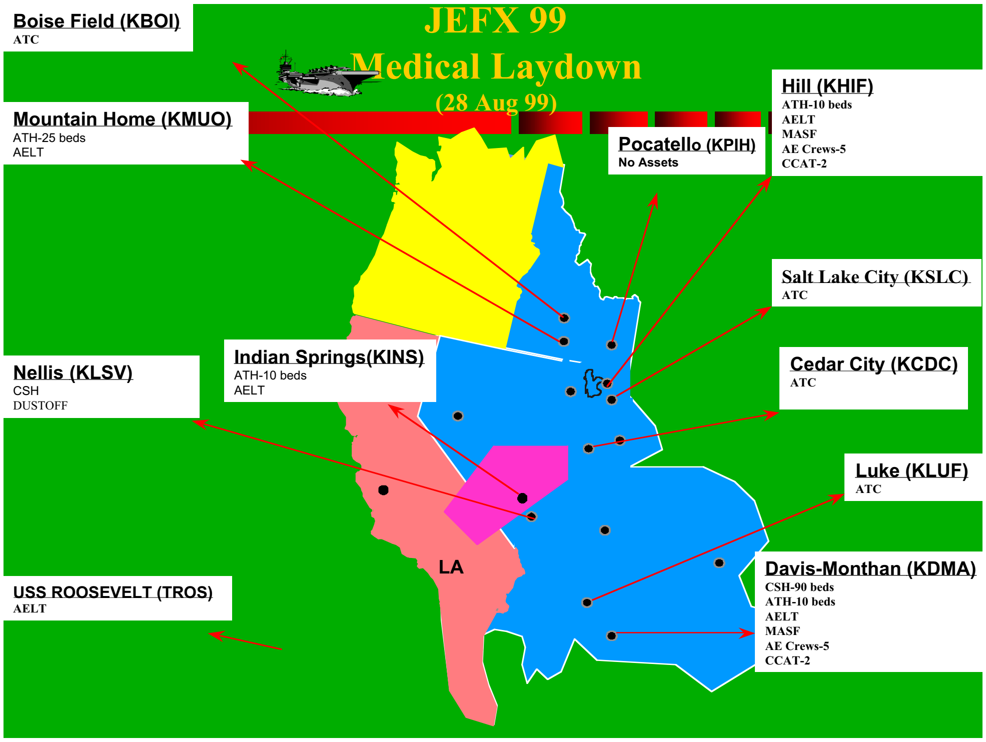
The necessary information for an AE request for movement will be entered into the format as described on the AF 3853. It will be dropped into the folder labeled AF Form 3853. A popup will be distributed to the AE players group each time this happens.

Changes/questions to this should be addressed to me either via CVW or phone (DSN579-xxx).

8/30/99

FROM AEROMEDICAL ROOM

Figure F.10 - 10th Floor – Air Mobility, continued



JEFX 99
Medical Laydown
(28 Aug 99)

Boise Field (KBOI)
ATC

Mountain Home (KMUO)
ATH-25 beds
AELT

Pocatello (KPIH)
No Assets

Hill (KHIF)
ATH-10 beds
AELT
MASF
AE Crews-5
CCAT-2

Salt Lake City (KSLC)
ATC

Indian Springs(KINS)
ATH-10 beds
AELT

Nellis (KLSV)
CSH
DUSTOFF

Cedar City (KCDC)
ATC

Luke (KLUF)
ATC

USS ROOSEVELT (TROS)
AELT

Davis-Monthan (KDMA)
CSH-90 beds
ATH-10 beds
AELT
MASF
AE Crews-5
CCAT-2

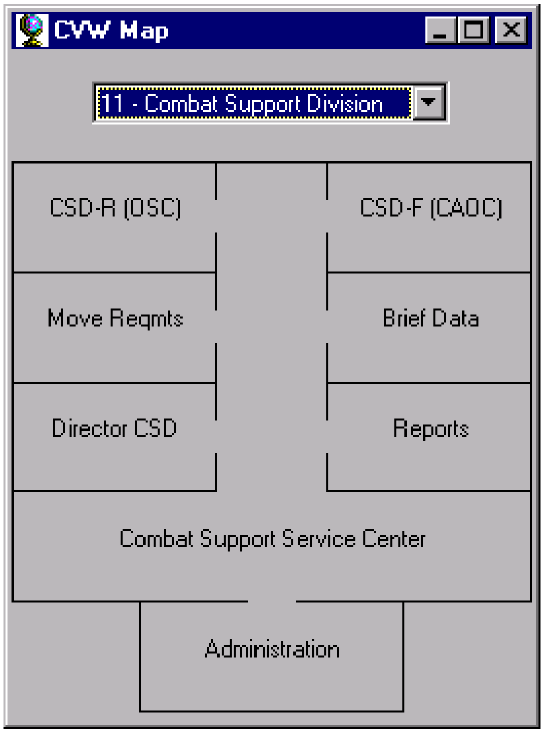
FROM AEROMEDICAL ROOM

Figure F.10 - 10th Floor – Air Mobility, continued

NAME	RANK	ROOM
xxx, VIC	*MAJ*	
xxx, CARL	MAJ	
xxx, ROBERT	MAJ	
xxx, CRAIG	MSGT	
xxx, JOSHUA	SSGT	Airlift Req.
xxx, SCOTT	SRA	Mob. Info. Cnt.
xxx, DAVE	SSGT	Mob. Info. Cnt.
xxx, TRAVIS	SRA	Mob. Info. Cnt.
xxx, STEPHEN	COL	CFACC Staff/Air Mob.
xxx, GINA	SRA	Mob. Info. Cnt.
xxx, NICOLE	2LT	Airlift Req.
xxx, JURGEN	MSGT	Mob. Info. Cnt.
xxx, DAVE	CIV	N/A
xxx, ANTONIO	MSGT	Mob. Info. Cnt.
xxx, JOHN	LT COL	Air Mob. Cont.
xxx, AMY	MAJ	Aeromedical
xxx, DAN	MSGT	Mob. Info. Cnt.
xxx, PHLAVAOUS	SRA	Mob. Info. Cnt.
xxx, DAVID	MAJ	Air Mob. Cont.

FROM MOBILITY INFORMATION CENTER

Figure F.10 - 10th Floor – Air Mobility, concluded



CSD-R (OSC) (Combat Support Division – Rear (Operational Support Center)
Significant Room Objects: CS division Position Descriptions (Notes and MS Word)

CSD-F (CAOC) (CSD Forward (Combined Air Operations Center)
N/A

Move Reqmts (Movement Requirements Team)
N/A

Brief Data – (Repository for briefing materials in production or under review)
Significant Room Objects: PowerPoint Briefing material

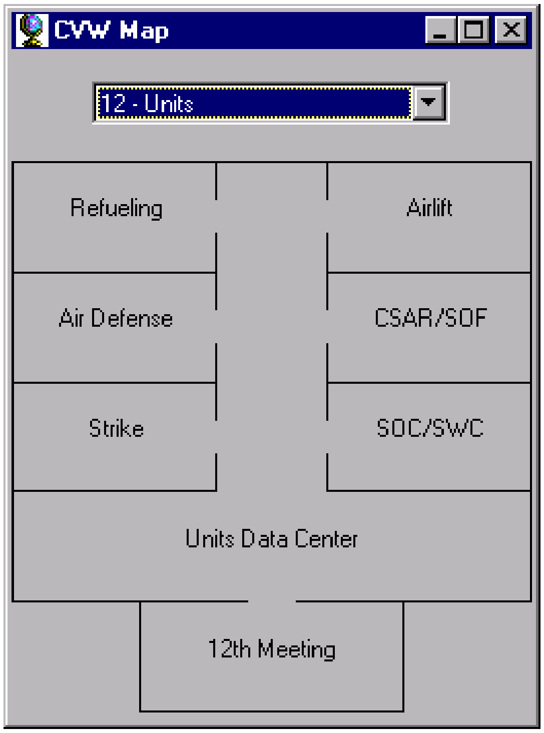
Director CSD – (Director's Office)
N/A

Reports – (Repository for CSD reports and related end-products)
Significant Room Objects: Close Air Support (CAS) munitions inventory (Folder); CSD Events Log (Note); Chemical Downwind Message (XLS); Current TPFDD folder; Logistical reports folder with text data documents; MSEL log (Note); MSELs (Folder); numerous other CSD reports

Combat Service Support Center (Resource Area)
N/A

Administration (General Administration activities for CSD personnel)
Significant Room Objects: Numerous CSD notes and text documents

Figure F.11 - 11th Floor – Combat Support Division



Refueling (Tanker Support Team)
Significant Room Objects: Refuel Requests (Notes)

Airlift (Airlift Units Team)
N/A

Air Defense (AD and Electronic Countermeasures (ECM) Support Team)
N/A

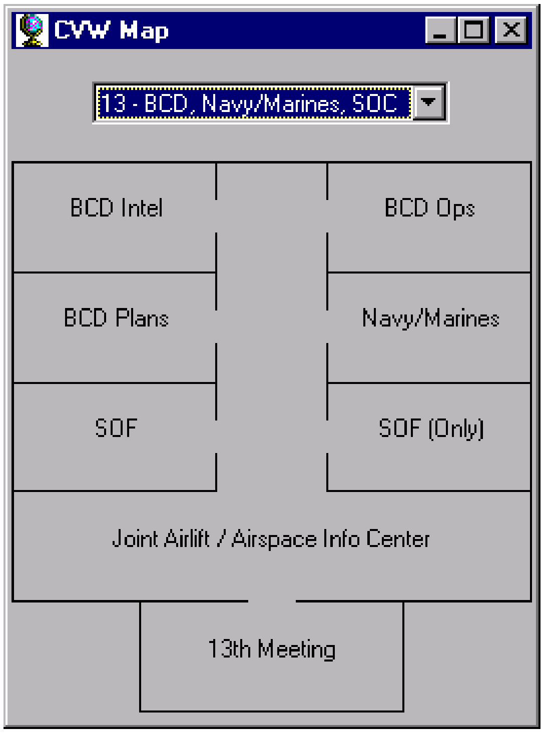
Strike (Wing Strike Force Fighters and Bombers Team)
N/A

SOC/SWC (Space Operations Center/Space Warfare Center)
Significant Room Objects: Space Intelligence Briefings (PowerPoint); AFSPACE IPB for each ATO (PowerPoint); Archived Info Ops Messages folder with text IO messages by each day; ARSPACE messages in text format; Hyperspectral Imagery folders for each day consisting of Whiteboards, JPEGS, and text; Mobile Laser Blinder Status Reports (XLS); Space weather (web ref); Satellite Pictures folder with JPEGS; Space Battle Management Cores Systems (SBMCS) Users Manual (MS Word); Space Phone Roster (XLS); Space Info Ops Daily Message folder

Units Data Center (Units planning and execution data)
N/A

12th Meeting (Planning/Meeting Space)
N/A

Figure F.12 - 12th Floor - Units



13 - BCD, Navy/Marines, SOC

BCD Intel (Battlefield Coordination Detachment (BCD) Army Intel Team)
N/A

BCD Ops (BCD Operations Team)
Significant Room Objects: Daily ARFOR OPS/INTEL briefings (PowerPoint); Deep Operations Coordination Cell (DOCC) briefings (PowerPoint); Notes on immediate information activities; ***Template for Army Intelligence Briefings (PowerPoint)***

BCD Plans (BCD Plans Team)
Significant Room Objects: ARFOR EOB briefings (PowerPoint); ARWEST CONOPS Briefing (PowerPoint)

Navy/Marines (Navy/Marines Air Coordination Teams)
Significant Room Objects: CSAR Briefing Input (PowerPoint); Maritime Picture (PowerPoint); Daily Naval SITREPs (Notes)

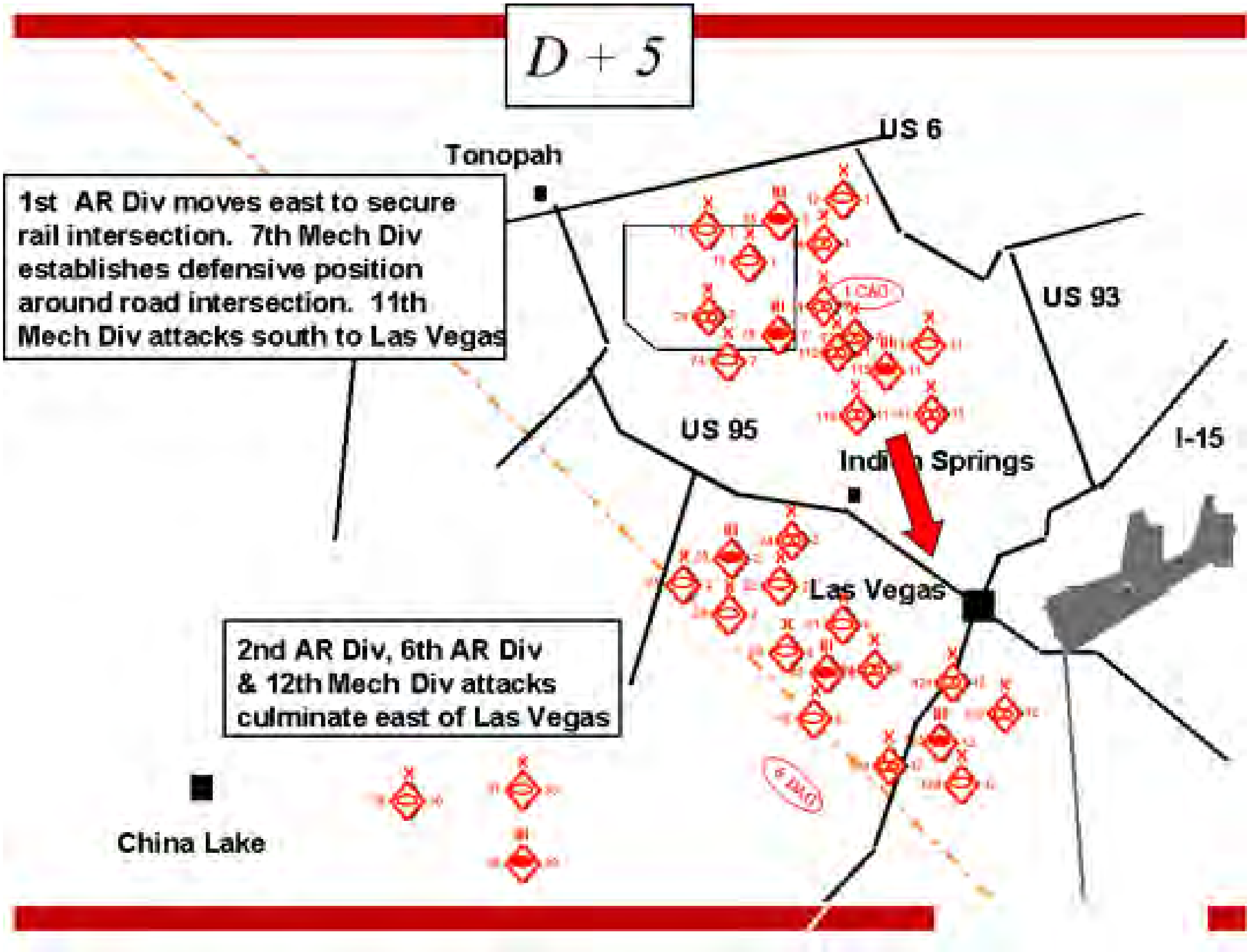
SOF (Special Operations Forces Team)
Significant Room Objects: SOF Group Object; SOF ATO Inputs (PowerPoint); SOF Drop Zones (DZ) (XLS)

SOF (Only) (Locked SOF Room)
N/A

Joint Airlift/Airspace Info Center (Resource Center)
N/A

13th Meeting (Planning and Meeting Space)
N/A

Figure F.13 - 13th Floor – BCD, Navy/Marines, SOC

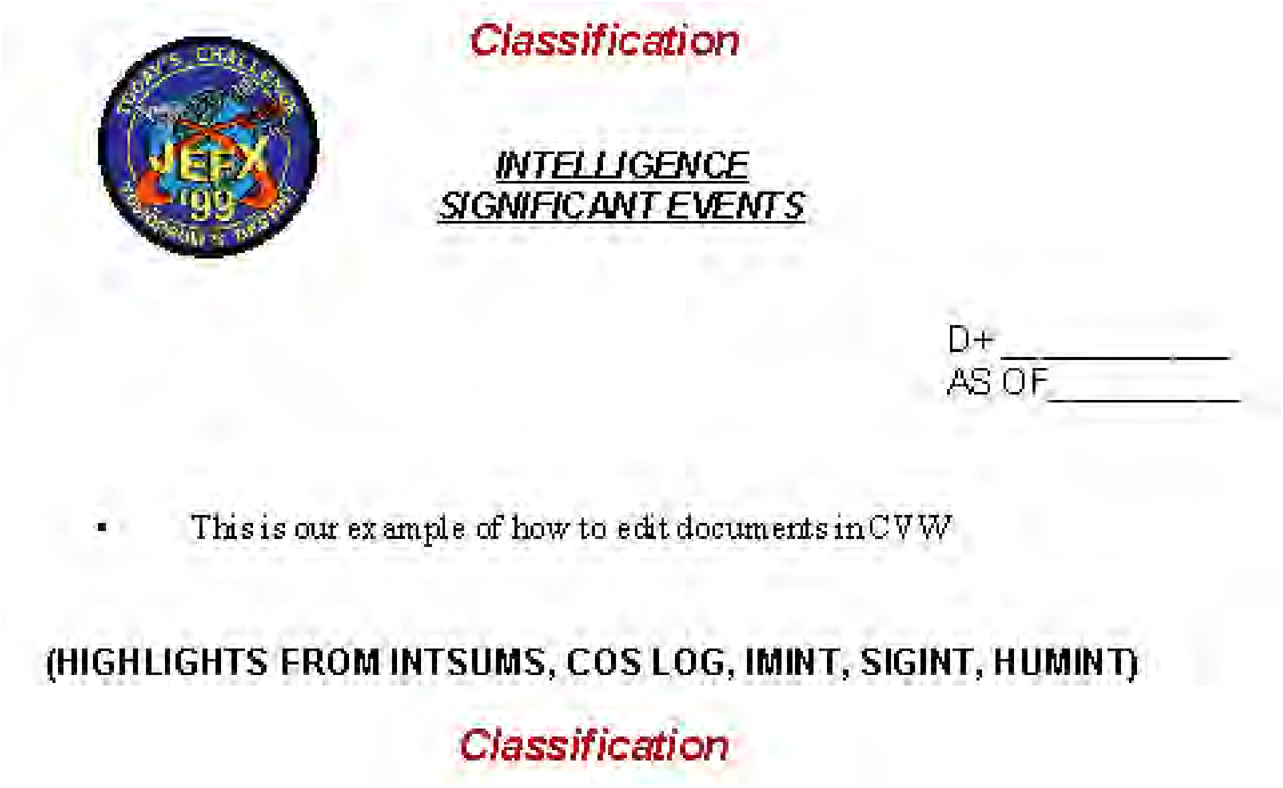


1st AR Div moves east to secure rail intersection. 7th Mech Div establishes defensive position around road intersection. 11th Mech Div attacks south to Las Vegas

2nd AR Div, 6th AR Div & 12th Mech Div attacks culminate east of Las Vegas

FROM BCD OPS ROOM

Figure F.13 - 13th Floor – BCD, Navy/Marines, SOC, continued



Classification

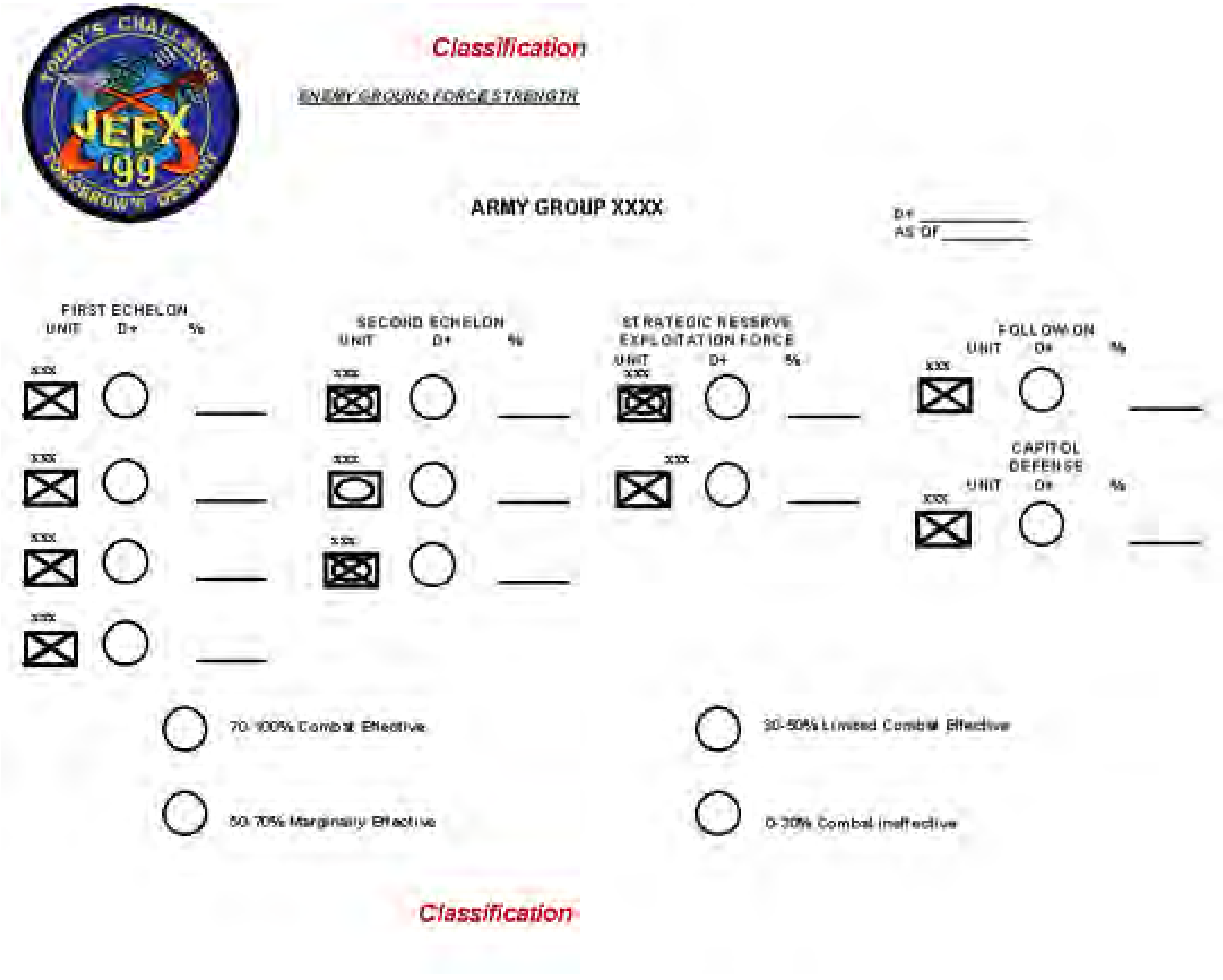
INTELLIGENCE
SIGNIFICANT EVENTS

D+ ____________
AS OF__________

- This is our example of how to edit documents in CVW

(HIGHLIGHTS FROM INTSUMS, COS LOG, IMINT, SIGINT, HUMINT)

Classification



Classification

ENEMY GROUND FORCE STRENGTH

ARMY GROUP XXXX

D+ ________
AS OF ________

TODAY'S CHALLENGE
JEFX '99
TOMORROW'S DESTINY
FIRST ECHELON
UNIT D+ %
xxx
xxx
xxx
xxx
SECOND ECHELON
UNIT D+ %
xxx
xxx
xxx
STRATEGIC RESERVE
EXPLOITATION FORCE
UNIT D+ %
xxx
xxx
FOLLOW ON
UNIT D+ %
xxx
CAPITOL
DEFENSE
UNIT D+ %
xxx

○ 70-100% Combat Effective

○ 30-50% Limited Combat Effective

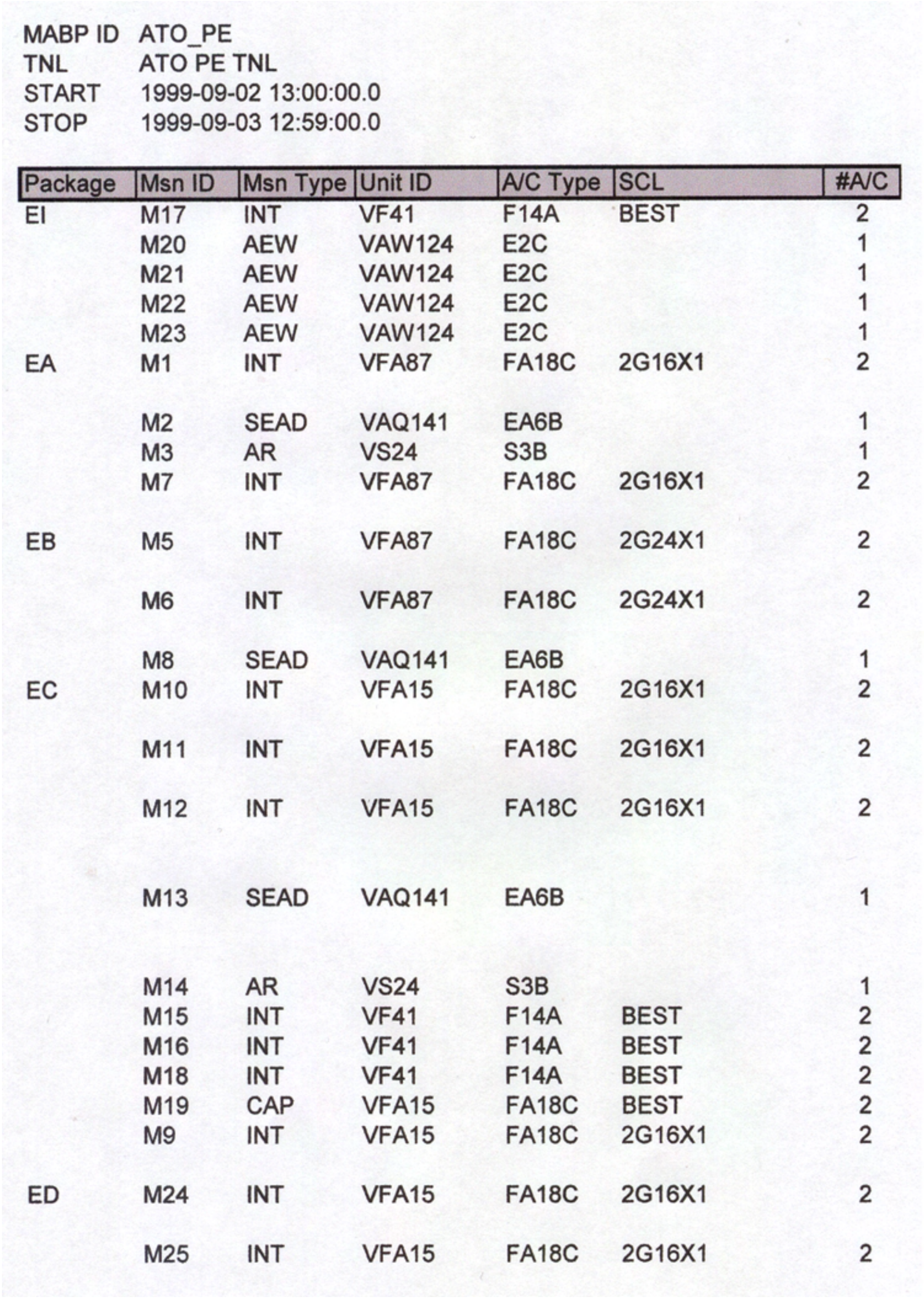
○ 50-70% Marginally Effective

○ 0-30% Combat ineffective

Classification

(Extract) FROM BCD OPS ROOM

Figure F.13 - 13th Floor – BCD, Navy/Marines, SOC, continued

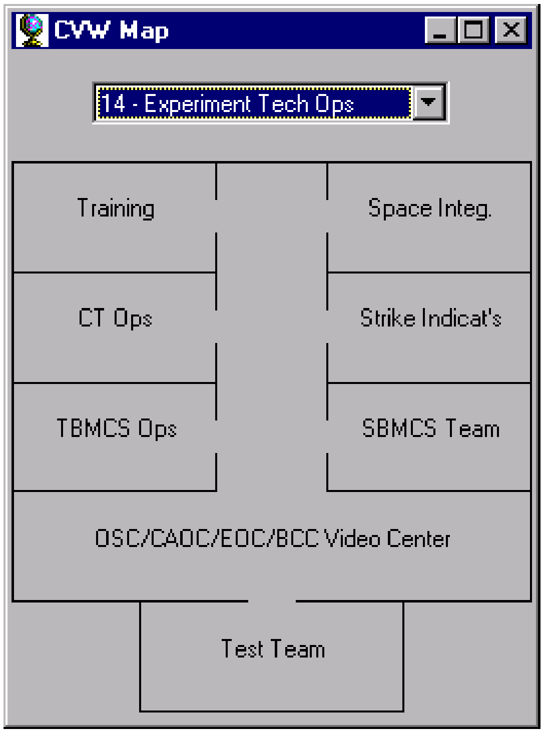


MABP ID ATO_PE
TNL ATO PE TNL
START 1999-09-02 13:00:00.0
STOP 1999-09-03 12:59:00.0

Package	Msn ID	Msn Type	Unit ID	A/C Type	SCL	#A/C
EI	M17	INT	VF41	F14A	BEST	2
	M20	AEW	VAW124	E2C		1
	M21	AEW	VAW124	E2C		1
	M22	AEW	VAW124	E2C		1
	M23	AEW	VAW124	E2C		1
EA	M1	INT	VFA87	FA18C	2G16X1	2
	M2	SEAD	VAQ141	EA6B		1
	M3	AR	VS24	S3B		1
	M7	INT	VFA87	FA18C	2G16X1	2
EB	M5	INT	VFA87	FA18C	2G24X1	2
	M6	INT	VFA87	FA18C	2G24X1	2
	M8	SEAD	VAQ141	EA6B		1
EC	M10	INT	VFA15	FA18C	2G16X1	2
	M11	INT	VFA15	FA18C	2G16X1	2
	M12	INT	VFA15	FA18C	2G16X1	2
	M13	SEAD	VAQ141	EA6B		1
	M14	AR	VS24	S3B		1
	M15	INT	VF41	F14A	BEST	2
	M16	INT	VF41	F14A	BEST	2
	M18	INT	VF41	F14A	BEST	2
	M19	CAP	VFA15	FA18C	BEST	2
	M9	INT	VFA15	FA18C	2G16X1	2
ED	M24	INT	VFA15	FA18C	2G16X1	2
	M25	INT	VFA15	FA18C	2G16X1	2

FROM NAVY/MARINES ROOM

Figure F.13 - 13th Floor – BCD, Navy/Marines, SOC, concluded



Training (Systems Training and CONOPS Team)
Significant Room Objects: Various training objects

Space Integ. (Space Integration Team)
Significant Room Objects: Numerous objects collected from other rooms; AFSPACE Command Briefing (PowerPoint)

CT Ops (CVW Systems and Administrative Team)
Significant Room Objects: Numerous CVW related reference and system objects

Strike Indicat's (Space Based Strike Indications Team)
Significant Room Objects: Delog Results folder; Historical folder; Strike Indications Target folder; Strike Indications Result folder; ***Strike Indications Briefing (PowerPoint)***

TBMCS Ops (Theater Battle Management Core Systems Team)
N/A

SBMCS Ops (SBMCS Team)
N/A

OSC/CAOC/EOC/BCC Video Center
(Video feeds from various JEFX locations)
N/A

Test Team (Test Operations Team)
N/A

Figure F.14 - 14th Floor – Experiment Tech Ops

STRIKE INDICATIONS PROCESS FLOW EXTRACT

Process Execution

COMAFSPACE AOC (Plans)

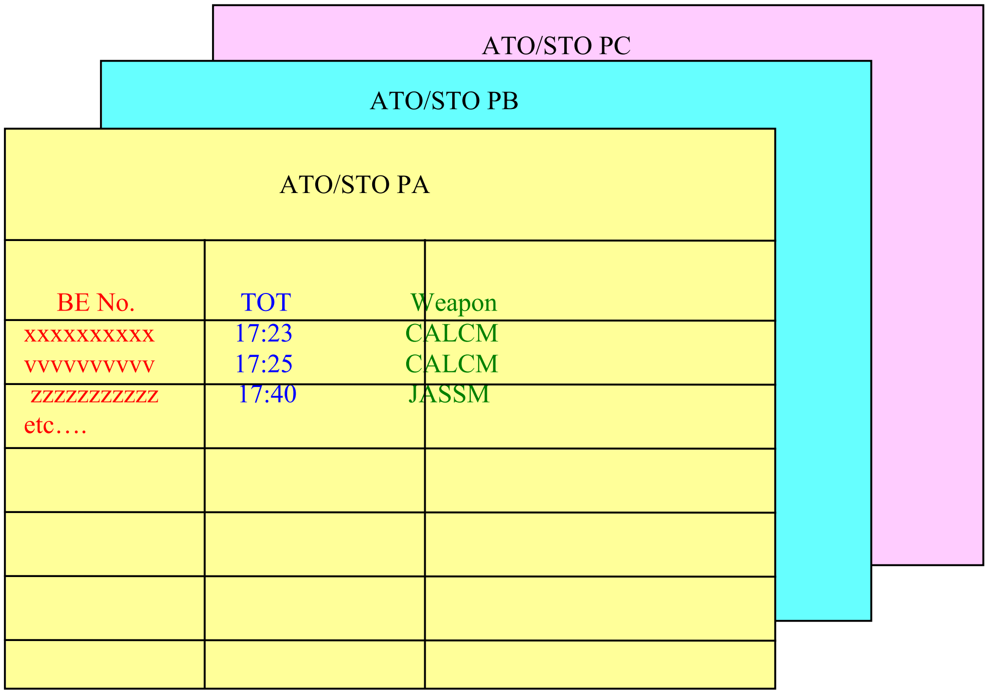
- Generate Space Tasking Order: Task 11 SWS to execute SI Ops, with details to be collaborated over CVW within the “SI room”
- Coordinate “Other” sensor availability as available

(EXTRACT) FROM STRIKE INDICAT’S ROOM

Figure F.14 - 14th Floor – Experiment Tech Ops, continued

Process Execution

OSC (Plans) - Forward daily target list over CVW to COMAFSPACE AOC Plans NLT ATO production/distribution



BE No.	TOT	Weapon
xxxxxxxxxx	17:23	CALCM
vvvvvvvvvv	17:25	CALCM
zzzzzzzzzzz	17:40	JASSM
etc….		

Amplifying data, if multiple DMPIs associated with a single BE

(EXTRACT) FROM STRIKE INDICAT'S ROOM

Figure F.14 - 14th Floor – Experiment Tech Ops, continued

Process Execution

COMAFSPACE AOC (Plans) - Generate SI tasking based on:

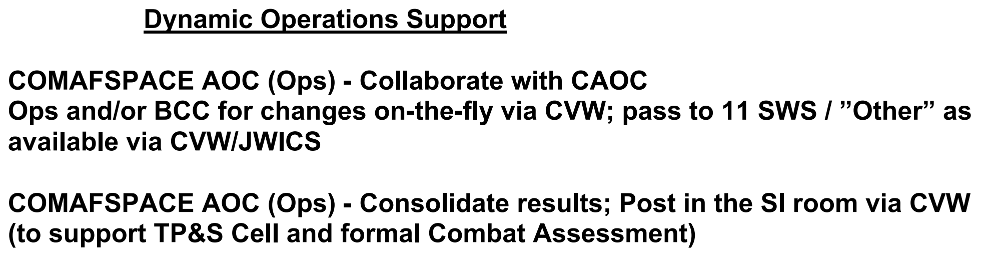
- **Sensor availability/processing capability**
- **Strike Indications “Historical Effectiveness” Manual**
- **AOR Wx**
- **? (i.e. lessons learned as we go…)**

COMAFSPACE AOC (Plans) - Generate proposed
SI target list on CVW; collaborate with OSC (Plans) for
“thumbs up”

(EXTRACT) FROM STRIKE INDICAT’S ROOM

Figure F.14 - 14th Floor – Experiment Tech Ops, continued

Process Execution



Dynamic Operations Support

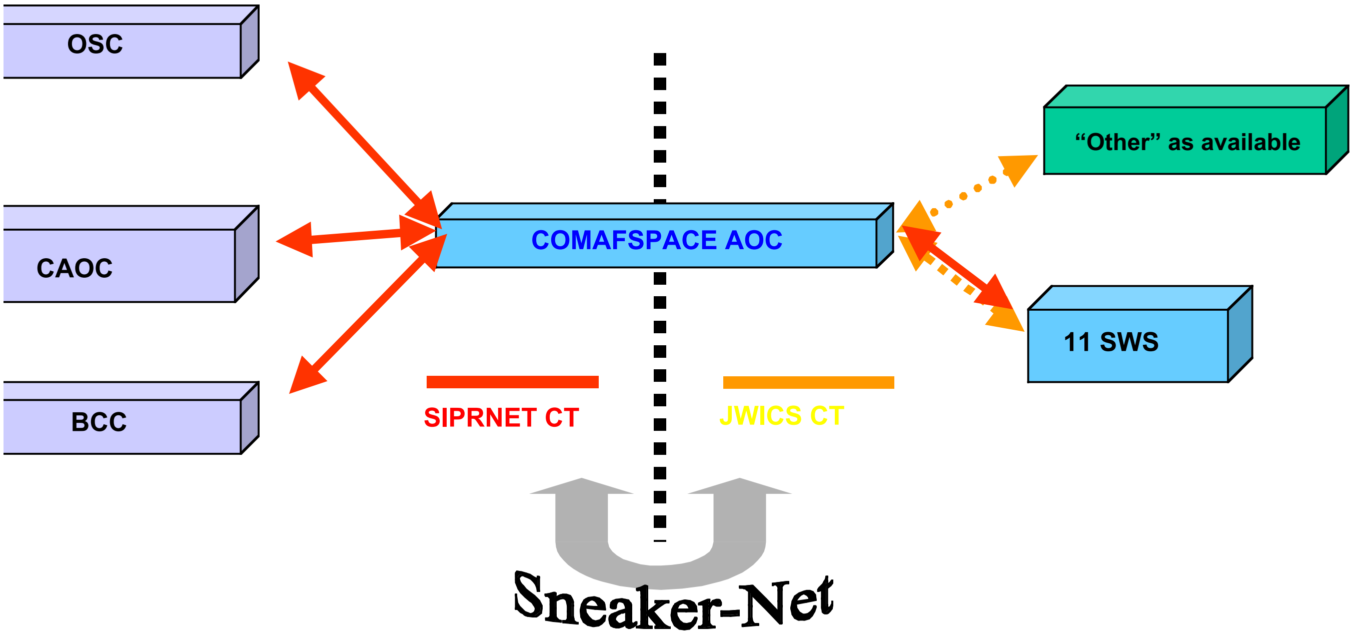
COMAFSPACE AOC (Ops) - Collaborate with CAOC Ops and/or BCC for changes on-the-fly via CVW; pass to 11 SWS / ”Other” as available via CVW/JWICS

COMAFSPACE AOC (Ops) - Consolidate results; Post in the SI room via CVW (to support TP&S Cell and formal Combat Assessment)

(EXTRACT) FROM STRIKE INDICAT’S ROOM

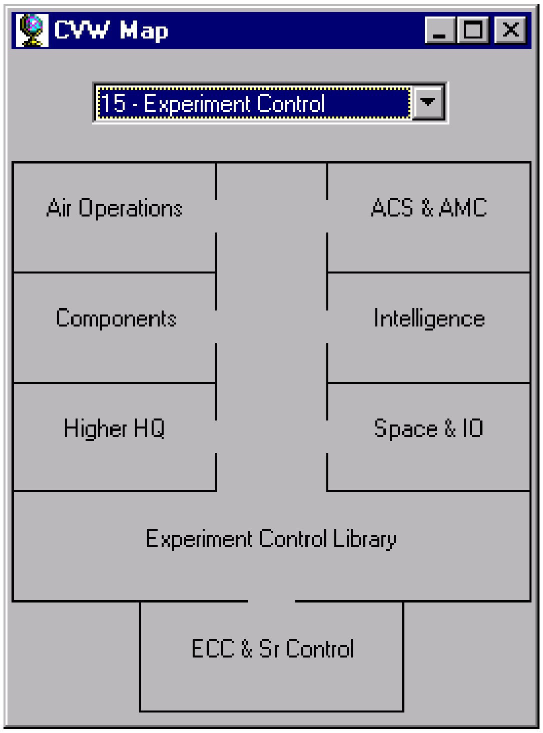
Figure F.14 - 14th Floor – Experiment Tech Ops, continued

Strike Indications Architecture



(EXTRACT) FROM STRIKE INDICAT'S ROOM

Figure F.14 - 14th Floor – Experiment Tech Ops, concluded



Air Operations (Control Team)
N/A

ACS & AMC (Medical Control Team)
Significant Room Objects: Medical Message folder

Components (Control Team)
N/A

Intelligence (Control Team)
N/A

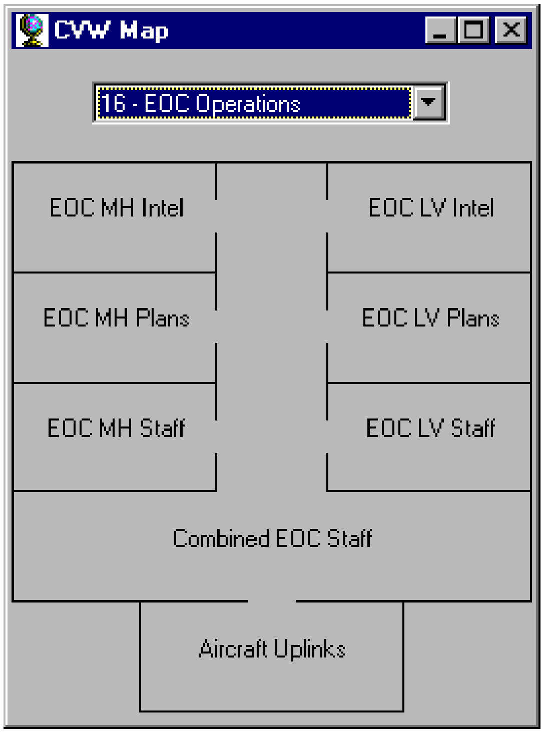
Higher HQ (Control Team)
Significant Room Objects: CINCWEST Orders folder; Joint Targeting Coordination Board (JTCB) folder with targeting data in PowerPoint and text format; NO HIT list (MS Word); USWESTCOM Joint Restricted Target List (MS Word)

Space and IO (Control Team)
Significant Room Objects: Space and IO data collected from other rooms

Experiment control Library (Resource Center)
N/A

ECC & Sr Control (Senior Control Team)
N/A

Figure F.15 - 15th Floor – Experiment Control



EOC MH Intel (EOC Mountain Home Intelligence Team)
Significant Room Objects: Gunfighter MISREP folder with Mission Notes; Guidance Info (Notes)

EOC LV Intel (EOC Las Vegas Intelligence Team)
Significant Room Objects: Nellis EOC Intelligence folder with numerous notes, documents, GIFs; MISREP folder

EOC MH Plans (Plans Team)
N/A

EOC LV Plans (Plans Team)
N/A

EOC MH Staff (Staff Room)
N/A

EOC LV Staff (Staff Room)
N/A

Combined EOC Staff (Combined Staff Room)
N/A

Aircraft Uplinks (Resource Room)
N/A

Figure F.16 - 16th Floor – EOC Operations

Glossary

ABL	Airborne Laser
AD	Air Defense
AF	Air Force
AFB	Air Force Base
AFCERT	Air Force Computer Emergency Response Team
AFFOR	Air Force Forces
AFLD	Airfield
AFOSC	Air Force Operational Support Center
AFSPACE	Air Force Space
AGC	Automatic Gain Control
AMD	Air Mobility Division
AO	Attack Operations
AOC	Aerospace Operations Center
AOD	Aerospace Operations Directive
ATO	Air Tasking Order
AWACS	Airborne Warning and Control System

BCC	Battle Control Center
BCD	Battle Coordination Detachment
BDA	Battle Damage Assessment
BDC	Dynamic Battle Control

C2	Command and Control
C2IPS	Command and Control Integrated Processing System
C2TIG	Command and Control Technical Integration Group
CAOC	Combined Air Operations Center
CAS	Close Air Support
CCPL	Command and Control Product Lines
CDE	Common Desktop Environment

CFACC	Combined Force Air Component Commander
CM	Collection Management
CM	Collection Manager
COMM	Communication
CPU	Central Processing Unit
CSAR	Combat Search and Rescue
CSCT	Computer Supported Collaborative Tools
CSAF	Chief-of-Staff of the Air Force
CSD	Combat Support Division
CT	Collaborative Tool
CTAPS	Contingency Theater Automated Planning System
CTL	Candidate Target List
CTX	Communication Technology Exchange
CVW	Collaborative Virtual Workspace
DARS	Daily Aerial Reconnaissance Schedule
DBC	Dynamic Battle Control
DII COE	Defense Information Infrastructure / Common Operating Environment
DIRMOBFOR	Director of Mobility Forces
DMOB	Defensive Missile Order of Battle
DMPI	Designated Mean Point of Impact
DNS	Domain Name Server
DOCC	Deep Operations Coordination Cell
DTL	Dynamic Target List
DZ	Drop Zones
ECM	Electronic Countermeasures
EFX	Expeditionary Force Experiment
ELINT	Electronic Intelligence
ELNOT	Electronic Notation
ENDEX	End of Exercise

EOC	Expeditionary Operations Center
ESC	Electronic Systems Center
FTP	File Transfer Protocol
GIF	Graphic Image Format
HTML	Hypertext Markup Language
HUMINT	Human Intelligence
IMINT	Imagery Intelligence
INTSUM	Intelligence Summary
IO	Information Operations
IP	Internet Protocol
ISR	Intelligence Surveillance and Reconnaissance
IW	Information Warfare
JAG	Judge Advocate General
JAOC	Joint Air Operations Center
JEFX	Joint Expeditionary Force Experiment
JFACC	Joint Force Air Component Command
JGAT	Joint Guidance, Apportionment and Targeting
JICO/RICO	Joint and Regional Interface Control Office
JIPTL	Joint Integrated Prioritized Target List
JMC	Joint Movement Center
JPG	Joint Photographic Expert Group
JRE	Java Runtime Environment
JSOAC	Joint Special Operations Air Component
JSRC	Joint Search and Rescue Cell
JSTARS	Joint Surveillance/Target Attack Radar System
JTCB	Joint Targeting Coordination Board

JTWG	Joint Targets Working Group
JWID	Joint Warfare Interoperability Demonstration
LO	Liaison Officer
MAAP	Master Air Attack Plan
MASINT	Measurement and Signature Intelligence
MHz	Megahertz
NAF	Numbered Air Force
NOSC-D	Network Operations and Security Center - Deployed
OA	Office Automation
ORI	Operational Readiness Inspection
OSC	Operations Support Center
PDI	Paragon Dynamics, Incorporated
perfmeters	performance meters
PR	Personnel Recovery
RFI	Requests for Information
ROE	Rules of Engagement
RPTS	Rapid Precision Target System
S-D	Sparse-Dense
SADO	Senior Air Defense Officer
SBMCS	Space Battle Management Core Systems
SCIF	Secure Compartmented Information Facility
SI	Special Intelligence
SIDO	Senior Information Duty Officer
SIGINT	Signal Intelligence

SIPRNET	Secret Internet Protocol Routing NETwork
SME	Subject Matter Expert
SOF	Special Operations Force
STAG	Strategy and Guidance
STO	Special Technical Operation
SW	Space Weather
TAL	Target Access List
TALCE	Theater Airlift Control Element
TBMCS	Theater Battle Management Core System
TCT	Time Critical Targeting
TNL	Target Nominations List
TOT	Time Over Target
TPFDD	Time-Phased Force and Deployment Data
URL	Universal Resource Locator
USAF	United States Air Force
VPN	Virtual Private Network
VTC	Video Teleconference or Teleconferencing
WMD	Weapons of Mass Destruction
XLS	Attack Guidance Matrix
Y2K	Year 2000