APPLICATION INTEGRATION SYSTEM INTEGRATION TEST (AISIT) TEST PLAN FOR GLOBAL BROADCAST SERVICE (GBS) WITH CONSOLIDATED AFLOAT NETWORKS AND ENTERPRISE SERVICES (CANES) FORCE LEVEL AND UNIT LEVEL

February 13, 2017

PREPARED FOR:

Program Executive Officer‒Command, Control, Communications, Computers, Intelligence (PEO C4I), Program Manager, Warfare (PMW) 160



DISTRIBUTION STATEMENT D. Distribution authorized to the Department of Defense (DoD) and U.S. DoD contractors operational use only (03AUG15). Other requests shall be referred to PEOC4.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **SIGNATURE PAGE**  ***Submitted By:***   |  | | --- | |  |   ***Concurrence By:*** | | | | |
| 2/27/17 | | | |
| Benjamin McCoy  GBS T&E Lead | |  | Date |
| ***Approved By:*** | |
| 2/28/17 |
| Patricia Fontecchio  GBS APM | |  | Date |
|  | |  |  |

RECORD OF CHANGES

\***A**–ADDED **M**–MODIFIED **D**–DELETED

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version No. | Date | Figure/Table/ Paragraph No. | Code | Title or Brief Description |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

TABLE OF CONTENTS

Section Page

1.0 overview 1-1

1.1 1-1

1.2 objective 1-1

1.3 Scope 1-1

1.4 test schedule 1-1

1.5 test personnel 1-1

1.6 reference documentS 1-2

1.7 risks 1-2

2.0 system description 2-1

2.1 mission description 2-1

2.2 system description 2-1

2.2.1 Transmit Segment 2-1

2.2.2 Space Segment 2-1

2.2.3 Receive Segment 2-1

2.2.4 Spilt IP Overview 2-1

2.2.5 Key Features And Subsystems 2-4

2.2.6 Physical Interfaces 2-5

2.2.7 Logical Interfaces 2-5

3.0 TEST overview 3-1

3.1 previous test events 3-1

3.2 satisfactory/unsatisfactory 3-1

3.3 entrance/exit criteria 3-1

3.3.1 Entrance Criteria 3-1

3.3.2 Exit Criteria 3-1

3.4 Expected End Product 3-1

3.4.1 Data Collection Plan 3-2

3.4.2 Reporting 3-2

3.5 qualifcations and certifications 3-2

3.6 safety 3-2

3.7 security 3-2

3.8 test limitations 3-2

4.0 test conduct 4-1

4.1 test architecture 4-1

4.2 baseline test equipment Configuration 4-2

4.2.1 Software Configuration 4-2

4.2.2 Hardware Configuration 4-2

4.3 test case summary 4-1

5.0 test procedures 5-1

5.1 Detailed Test Procedures 5-1

5.1.1 Objective 1: Verify GBS 6.X core functions 5-1

5.1.2 Objective 2: GBS Data Product Distribution 5-2

5.1.3 Objective 3: GBS Video Product Distribution 5-3

5.1.4 Objective 4: GBS Split IP Operation and Reachback 5-4

5.1.5 Objective 5: Verify GBS 6.X Core Functions with HBSS 5-5

APPENDIX A – acronyms 5-1

APPENDIX b – Video Quality Data Collection Worksheet 5-1

List of Figures

Title Page

Figure 2‑1 UNCLASS System Boundary 2-4

Figure 2-2 SECRET System Boundry

Figure 4-1 UNCLASS Test Bed Topology

Figure 4-1 SECRET Test Bed Topology

List of Tables

Title Page

Table 1‑1 Test Schedule 1-1

Table 1‑2 Test Personnel 1-1

Table 1‑3 Reference Documents 1-2

Table 2‑1 List of Feature and Subsystems 2-4

Table 2‑2 Physical Interfaces 2-5

Table 2‑3 Logical Interfaces 2-5

Table 4-1 Software Configuration…………………………………………………………………………..

Table 4-2 Hardware Configuration………………………………………………………………………….

Table 4‑3 Test Cases 4-1

Table 5‑1 TC #1 Detailed Test Procedures 5-1

Table 5-2 TC#2 Detailed Test Procedures…………………………………………………………………..

Table 5-3 TC#3 Detailed Test Procedures…………………………………………………………………..

Table 5-4 TC#4 Detailed Test Procedures…………………………………………………………………..

Table 5-5 TC#5 Detailed Test Procedures…………………………………………………………………...

# overview

## The Navy Global Broadcast Service (GBS) Program is fielding the new AN/USR-10B(V) Receive Broadcast Manager (RBM) starting in Q1FY17. As part of the GBS integration testing the new RBM hardware configuration with the currently fielded software of GRS Client v6.0.4.373 is required to complete testing with PMW 160’s Application Integration (AI) Consolidated Afloat Networks and Enterprise Services (CANES) to ensure GBS data and video products are distributed to the end user systems properly. The testing will also verify, specific Navy GBS Sources such as the Navy Asymmetric Network configuration for Automated Digital Network System (ADNS) Secret Internet Protocol Routing Network (SIPRNet) data known as Navy Split Internet Protocol (IP).

The purpose of the AISIT Test Plan for the AN/USR-10B(V) is to document all test expectations, requirements, resources, etc. that must be satisfied before and during the test event. A key component of the application/ system test plan is the identification of test objectives, e.g., Key Performance Parameters (KPPs), Key Support Areas (KSAs), and Information Exchange Requirements (IERs) that will be tested for during the System Integration Test (SIT). The test plan should provide a traceability matrix to the supporting test cases and/or test procedures that will be used during the test event.

## objective

The desired outcome of this event is to reduce the risk for integration and interoperability between the GBS RBM and the CANES UNCLASSIFIED (UNCLASS), SECRET, SECRET Releasable (SR), and Sensitive Compartmented Information (SCI) enclaves, and all other applications/systems that will operate in this environment for the targeted platform type.

## Scope

The scope of this SIT document is limited to testing with the GBS RBM during AISIT-7. It also includes testing requirements of interfaces with required supported or related systems to include Automated Digital Network System (ADNS), Navy Information/Application Product Suite (NIAPS), Navy Integrated Tactical Environment System (NITES) - Next, Global Command and Control System - Maritime (GCCS-M), CANES, Defense Common Ground System - Navy (DCGS-N), Simple Message Queue (SMQ) -11, Classified Video Distribution System (CVDS), Geographical Intelligence Unified Naval Streaming System (GUNSS), Integrated Broadcast Service (IBS), Windows Server Update Services (WSUS) and The Intelligence Carry-On Program (ICOP).

## test schedule

The high-level test schedule with milestones is shown in the table below. Note that this is part of a pending overarching AI schedule that is flexible.

Table ‑ Test Schedule

| Date | Milestones | Deliverables/Comments |
| --- | --- | --- |
| 06 MAR 17 | Test Bed Setup | Equipment set-up in appropriate lab |
| 14 MAR 17 | Intra-System Testing | Test internal GBS connectivity |
| 16 MAR 17 | Inter-System Testing | Test external GBS interfaces |
| 20 MAR 17 | USR-10B Testing | Test GBS USR-10B system with CANES |

## 

## test personnel

The test team for this event is listed in the table below.

Table ‑ Test Personnel

| **Name** | **Role & Organization** | **Phone Number** | **Email** |
| --- | --- | --- | --- |
| Tuan Vo | Space and Naval Warfare Systems Command (SPAWAR) Systems Center Pacific (SSC PAC) Engineering Support | 619-357-6504 | tuanavo@spawar.navy.mil |
| Damian McNeal | GBS Event Lead  Code 5.5 SSC PAC | 619-553-8931 | damian.mcneal@navy.mil |

## reference documentS

This section lists the primary documents used to either flow down or derive functional, technical, performance, or interface requirements.

Table 1‑3 lists all references used as guidance in the design process and development of this test plan. Only documents that have been approved and released are referenced herein.

Table ‑ Reference Documents

| **Ref #** | **Document Number** | **Title** | **Date** | **Revision** |
| --- | --- | --- | --- | --- |
| 1 | SRF-16-0151 | Global Broadcast Service (GBS) USR-10B for CANES | 28 JUN 2015 | 6.X |
| 2 | EE130-MZ-OMP-B10 | AN/USR-10B(V) Technical Manual | 23JAN 2017 | PRELEM |

## risks

None.

# system description

## mission description

GBS is a joint Military Satellite Communications (MILSATCOM) service which provides high speed (up to 45 megabits per second [mbps] on Wideband Global Satellites (WGS)), one-way information flow of high volume data to users afloat, ashore or in supported special operations. GBS provides the rapid dissemination of live video, large data files and other information to warfighters for: intelligence; reconnaissance; weapons targeting; special requirements; and training exercises.

## system description

### Transmit Segment

The primary Satellite Broadcast Manager (SBM) located at a Defense Enterprise Computing Center (DECC) facility is located in Oklahoma City, OK (OKC), with the backup SBM at a DECC facility is located in Mechanicsburg, PA (MECH) which is designed as a Continuity of Operations (COOP) location. Data and streaming products are transmitted from sources to the GBS primary SBM at the DECC facility (videos are simultaneously transmitted to the COOP SBM at the MECH DECC facility) and then across the Department of Defense Information Network (DoDIN) core to DoD Teleports, DoD Gateways, and terminals for broadcast over the WGS satellites (Ka- & X-bands).

The GBS architecture is a content priority based broadcast. This ensures the most critical information is delivered first. The IP architecture allows higher content priority products to interrupt the broadcast of lower priority broadcasts after which the delivery of lower level priority content will resume. GBS is a MAC-II Level information technologies mission-essential national security system providing network centric communications. GBS does not have nuclear survivability or hardening features incorporated. GBS is vulnerable to the same threats as most commercial SATCOM systems.

### Space Segment

The space segment consists of GBS broadcast streams utilizing bandwidth on WGS satellites (1-7). Other X-, Ka- and Ku-band satellites, US and non-US, could also be used to augment the space segment if necessary.

### Receive Segment

The receive segment provides the capability of receiving the GBS broadcast signal, extracting the information products of interest to local forces, and disseminating the products to the forces using local network/communications infrastructure. The receive segment, referred to as the Receive Broadcast Manager (RBM), is on a common architecture configured for transportable, shipboard, subsurface, and airborne applications.

### Spilt IP Overview

GBS Split IP allows an asymmetric communication path with the RBM where the ADNS SIPRNet forward data signal flows over the high bandwidth unidirectional GBS system and the return ADNS SIPRNet data signal flows over the ADNS assigned primary path bandwidth links. Split IP automatically detects when there is a high bandwidth GBS forward link available and automatically configures the ADNS SIPRNet to route the forward traffic through GBS. It leverages the existing ship satellite communications to determine when a link is available. It also leverages existing GBS scheduling services to configure the SBM (Satellite Broadcast Manager) to route the Split IP Streaming Service Source to the appropriate transponder.

When Split IP is turned on and the Shipboard / submarine end user requests data from an External Website, the request goes from the End User computer through ADNS to the Fleet Router in the NOC (Network Operating Center). From the Fleet router the request goes through the SIPRNet to the External website. On the return path to the ship/sub end user BGP Router re-routes the packets destined for the End User through the Fleet router using Quagga on the Split IP server. This is where the GBS data encapsulation begins. In the encapsulation process, the data starts as an IP packet from Quagga on the Split IP server. OpenVPN (Virtual Private Network) is configured to have one tunnel per a Kencast channel. Based on which transponder the end user box is located under, Quagga routes IP packets destined for the end user box into the corresponding OpenVPN tunnel. It then gets encapsulated by OpenVPN from a TCP packet to a UDP packet to prepare for one way delivery of the data. Then Fazzt Enterprise Server encapsulates the OpenVPN packet into a Fazzt transport stream. One Fazzt transport stream is configured per an OpenVPN tunnel to encapsulate any data that goes into the corresponding OpenVPN tunnel. The transport streams travel over the Fazzt Enterprise Server channels to the SBM via GRE tunnel. While in the SBM the Fazzt Enterprise Server transport streams are forwarded to the appropriate transponder.

The SBM encrypts the broadcast using Type 1 encryption for the classified enclave as well as CAS Type 2 encryption for the unclassified enclave and then sends the Kencast Channel product to the RBM over the high bandwidth satellite. The type 1 decryptor on the RBM removes the broadcast encapsulation leaving the Fazzt transport stream identified as Split IP Channel xxx.

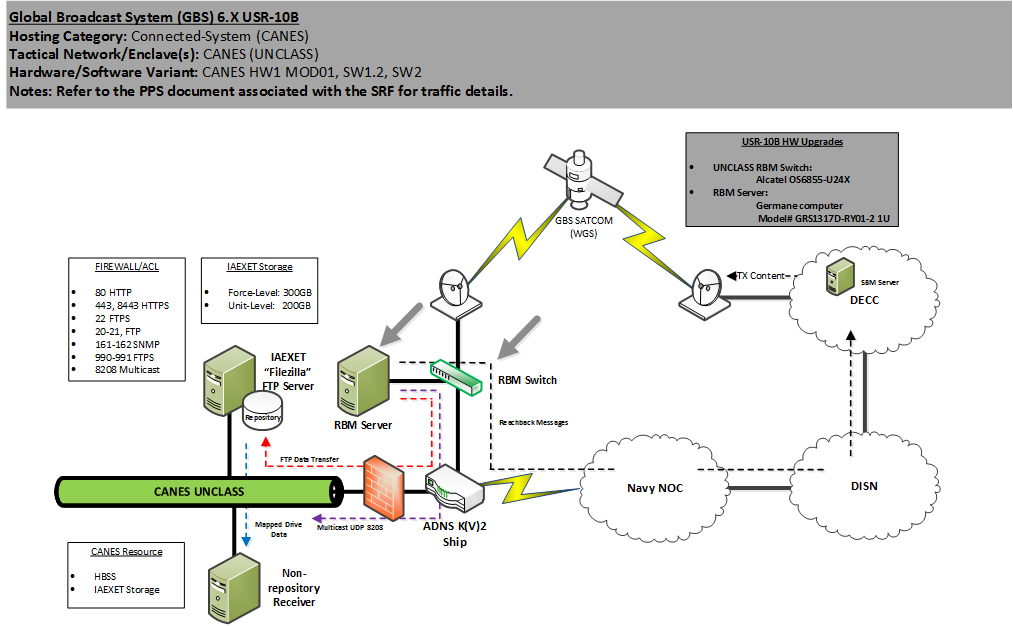
Then Kencast on the RBM removes the Fazzt transport stream encapsulation leaving the OpenVPN tunnel. The OpenVPN client on the RBM removes the OpenVPN tunnel encapsulation changing the UDP packets back into TCP packets leaving the original data reply. Then the data is passed as an IP packet onto the appropriate network server which finally delivers to the ADNS SIPRNet to complete the data path. This full circuit architecture is displayed in figure 1 and 2 for ADNS INC III and ADNS INC II.

Figure ‑ UNCLASS System Boundary

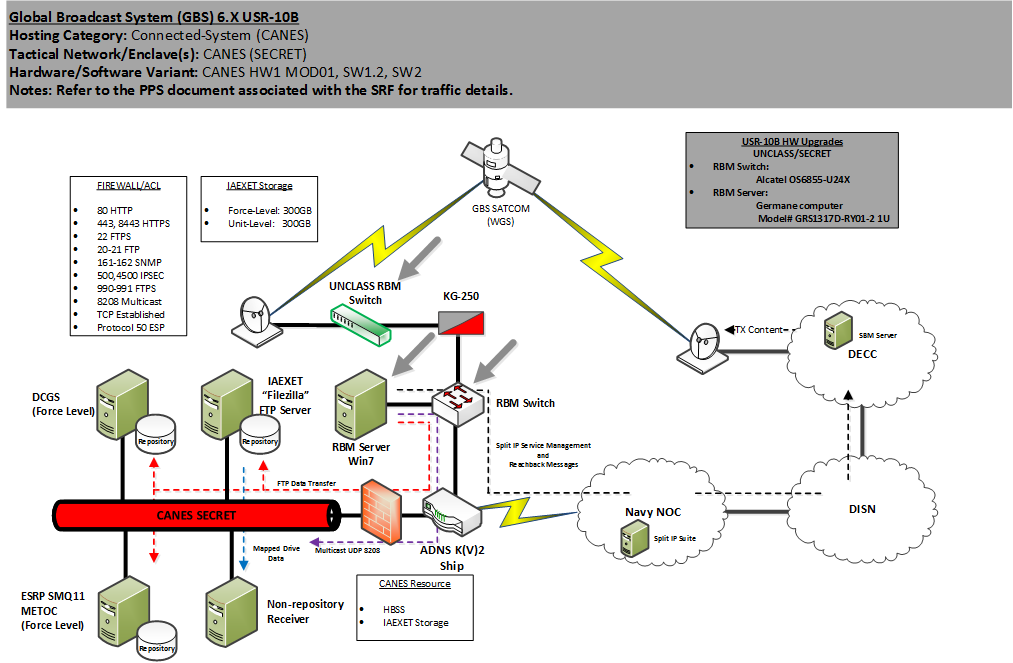


Figure ‑2 SECRET System Boundary

### Key Features And Subsystems

Major hardware and software are listed in table 2-1.

Table ‑ List of Feature and Subsystems

| **Device** | **Manufacturer** | **Function** | **Model Number** | **Software Version** |
| --- | --- | --- | --- | --- |
| Computer | Germane | RBM | GRS1317D-RY01-2 | GBS 6.X |
| Switch | Alcatel | Network switch | 6855-U24X | 6.4.6.361.R01 |
| Switch | Cisco | Split IP Router | CISCO 2911 | 15.0 (2) SE7 |
| Server | Dell | Split IP server | R330 | RHEL 6 |
| Server | Dell | SBM Shore server | PowerEdgeR515 | Microsoft (MS) Windows Server 2003 R2 |

### Physical Interfaces

Physical and logical interfaces are listed in table ‑.

Table ‑2 Physical Interfaces

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Application/System** | **Interface Class** | **Physical Interface Connection** | **Interface type** | **Standards/ Protocols** |
| ADNS INC III | UNCLASS | G 1/.108 | Gigabit Ethernet | TCP, UDP, Simultaneous Media Access Control (MAC) Transfer Protocol (SMPT), Simple Network Management Protocol (SNMP), Encapsulating Security Payload (ESP) |
| ADNS INC III | SECRET | G 1/.108 | Gigabit Ethernet | TCP, UDP, SMPT, SNMP, ESP |
| Fleet Router Media Converter Switch | SECRET | G 0/2 | Gigabit Ethernet | TCP, UDP, SMPT, SNMP, ESP |

### Logical Interfaces

Physical and Logical Interfaces are listed in table ‑.

Table ‑3 Logical Interfaces

|  |  |  |
| --- | --- | --- |
| **Application/System** | **Data Transmitted** | **Direction** |
| CANES (U/S) | File Transfer Protocol (FTP), TCP, Hypertext Transfer Protocol (HTTP), Hypertext Transfer Protocol Secure (HTTPS), UDP, SNMP, SMTP, ESP | Bidirectional |
| DCGS-N | FTP, HTTPS, HTTP | Bidirectional |
| SMQ-11 | FTP, HTTPS, HTTP | Bidirectional |
| HBSS | TCP, HTTP, HTTPS, UDP, SNMP | Bidirectional |
| IBS | UDP / ESP | Bidirectional |
| NITES-NEXT | FTP, SFTP | Bidirectional |
| GUNSS | UDP | Unidirectional |
| GCCS-M | TCP, UDP | Bidirectional |
| NIAPS | FTP, SFTP, FTPS | Bidirectional |
| ICOP | TCP, UDP | Bidirectional |

# TEST overview

## previous test events

## The AN/USR-10B(V) and AN/USR-10A(V) both support the previous AISIT-5 with both RBM’s utilizing the latest GRS Client version to support the SIT with CANES requirements.

## satisfactory/unsatisfactory

## All previous test events with CANES and the AN/USR-10A(V) and AN/USR-10B(V) RBM’s have been satisfactory. The AN/USR-10A(V) and AN/USR-10B(V) both utilize the same GRS Client software version with a difference hardware baseline as shown in Table 2-1.

## entrance/exit criteria

Each test procedure shall have entrance/exit criteria. Adherence to these pre-configuration requirements shall be documented and maintained in accordance with the test plan.

### Entrance Criteria

* Ensure Interim Approval to Test (IATT), Interim Approval to Operate (IATO) or Approval to Operate (ATO) exists
* Verify all hardware, software, and network are fully functional and available to support the test
* Verify end-to-end connectivity between systems and interfaces are fully functional
* Network is established and system of systems venue setup and verified
* Objectives clearly defined and articulated to the test and event manager
* Detailed test procedures are available
* Test environment and architecture is fully documented and distributed
* Security requirements are satisfactorily addressed
* Configuration Management for the test documented
* Information Assurance fully addressed
* Successful completion of the Test Readiness Review

### Exit Criteria

* All test objectives are addressed
* Data collection is complete and data was archived
* Test results documented
* All tests included within this test plan are completed successfully or acceptable mitigation plans have been identified
* Preliminary analysis of test data
* Inform appropriate stakeholders

## Expected End Product

* Document the results of test cases used during this evolution
* Document all system defects discovered during the test event, if applicable
* Provide fielding recommendations for System Under Test in a CANES environment based on documented test results
* Host Based Security System (HBSS) Policy Verification
* IA assessment (to be provided in a separate report)

### Data Collection Plan

The data collected will be the results of the test cases (Pass, Fail, Not Testable [NT], or Non-Applicable [NA]). The data collected will be reduced, analyzed, and traced to test cases in Section 4, and issues will be reported appropriately.

### Reporting

If, in the course of testing, a documentation or system discrepancy is discovered, it will be documented and the request will be submitted to the GBS Test Points of Contact (POCs). Upon completion of testing, the test team will generate and submit a final System Test Report to GBS Test POCs. Copies of the final reports will be submitted to the CANES event test director.

## qualifications and certifications

Test personnel shall be properly trained and certified where appropriate, to operate the instrumentation and recording equipment during test events. All test equipment shall have current calibration certificates where appropriate.

## safety

Standard safety precautions shall be in effect while working on electronic equipment in a laboratory environment. The following is a list of safety regulations in effect:

* SPAWARINST 5100.9, Navy Shore Electronics Safety Precautions
* Occupational Safety and Health Act (OSHA), Code of Federal Regulations Title 29
* Occupational Safety and Health Act (OSHA), Code of Federal Regulations Title 40

## security

The CANES Application Integrations SIT (AISIT)-7 test will take place on classified and unclassified equipment for the duration of the event. The SPAWAR laboratory facilities are accredited to support testing at the classified and unclassified classification level. All test participants are required to ensure the integrity of the facility and the test data.

## test limitations

Test will be limited to lab renditions of fielded GBS shipboard and shore systems

# test conduct

This test plan covers all the necessary testing needed to successfully verify proper operation of the GBS CANEStest. The required test architecture is shown in figures 4-1 and 4-2.

## test architecture

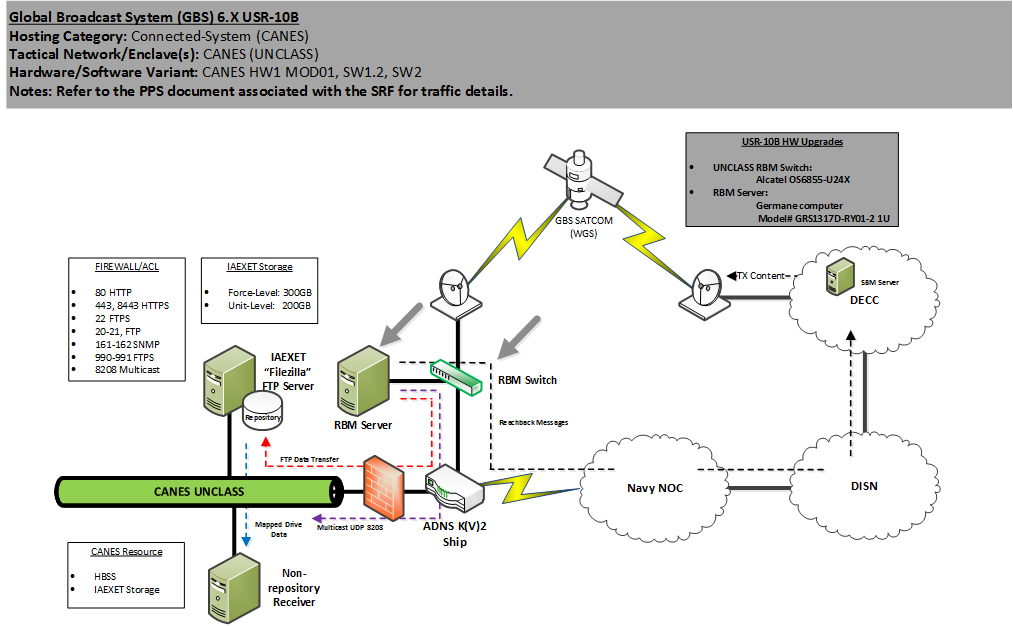


Figure ‑ UNCLASS Test Bed Topology

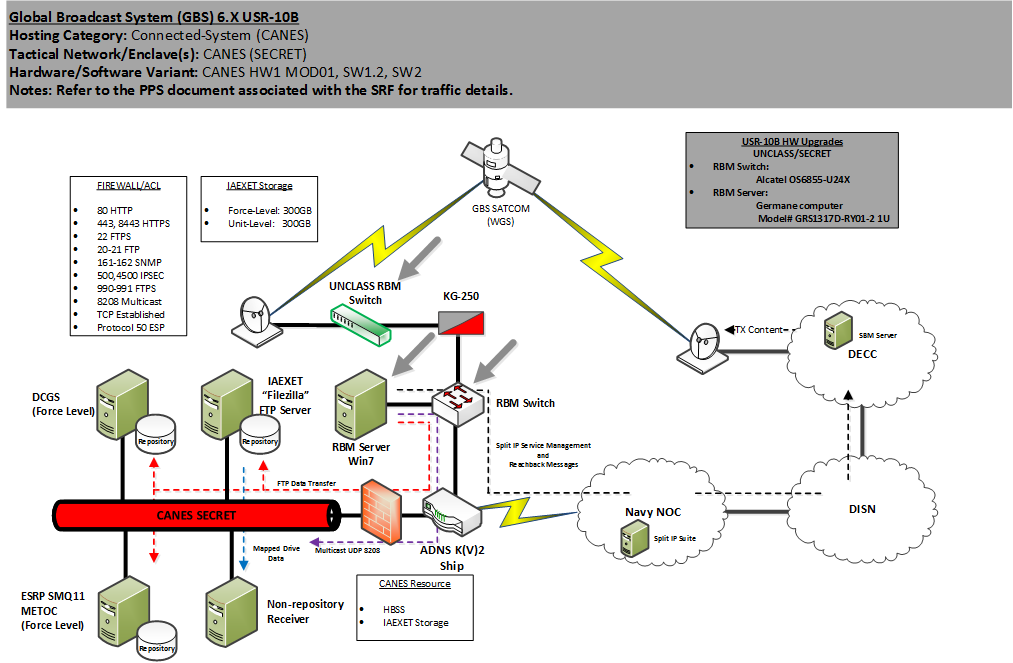


Figure ‑2 SECRET Test Bed Topology

## baseline test equipment Configuration

The tables below provide additional detail of the actual hardware, software, configuration for the devices that make up the test bed.

### Software Configuration

Table 4-1 Software Configuration

|  |  |  |  |
| --- | --- | --- | --- |
| **Software** | **Role** | **Software Version** | **Template Version** |
| Windows 7 | GBS 6.X RBM Operating System (OS) | SP1 | 6.X |
| RHEL 5/6 | Split IP Server OS | RHEL 5/6 | 2.0/3.0 |
| Cisco IP Services x IOS | Split IP Switch IOS | 15.0 (2) SE7 | 2.0 |

### Hardware Configuration

Table ‑2 Hardware Configuration

| **Hardware** | **Role** | **Hardware Version** | **Template Version** |
| --- | --- | --- | --- |
| Germane Computer | Ship UNCLASS and SECRET RBM | GRS1317D-RY01-2 | 10B |
| Alcatel Switch | Ship UNCLASS and SECRET GBS Switch | 6855-U24X | 10B |
| Cisco 2911 | Shore Split IP Router | 2911 | 2.0/3.0 |
| Dell R330 Server | Shore Split IP Server | R330 | 2.0/3.0 |

## test case summary

Table 4-3 provides an overview of the test cases (TCs). Detailed procedures of each test case are listed in Section 5.0. Repeat each TC five times with each CANES Compose version (3.5, 4.0 and 4.0.1).

Table ‑3 Test Cases

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **TC #** | **Test Case (TC) Description** | **Objective (OBJ)** | **Pass/Fail Criteria** | **Requirement** | **Verification Method** |
| TC-1 | GBS operations | **OBJ 1:** Verify GBS core functions (Apache/MSSQL/FAZZT services running, FTP, Split IP) | Expected Results are shown | ECRs GBS-00134 & GBS-00688 | Test |
| TC-2 | FTP/FTPS product distribution | **OBJ 2:** Verify GBS Data Product Distribution to end users | File received with no error/retransmission | ECRs GBS-00134 & GBS-00688; Measure of Effectiveness (MOE)-21 | Test |
| TC-3 | Multicast video distribution | **OBJ 3:** Verify GBS Video Product Distribution to end users | Video quality rating > 3 (Appendix B) | ECRs GBS-00134 & GBS-00688; MOE-22 | Test |
| TC-4 | GBS Split IP operation/Reachback | **OBJ 4:** Verify GBS Split IP Operation and Reach back path | Expected Results are shown | ECRs GBS-00134 & GBS-00688; MOE-23, MOE-1 | Test |
| TC-5 | HBSS operations | **OBJ 1:** Verify GBS Core Functions (JBOSS/SQL/FAZZT services running, FTP, Split IP) with HBSS | Expected Results are shown | ECRs GBS-00134 & GBS-00688 | Test |

# test procedures

The following sections detail the test cases and procedures that shall be completed for this testing. The following test cases are grouped to verify if each test objective has been met.

## Detailed Test Procedures

### Objective 1: Verify GBS 6.X core functions

TC#1

Description: Verify GBS operates correctly

Requirement(s): GBS ability to functionally operate

Prerequisites: Ensure GBS ports, protocols, and services are operational

Setup: Ensure proper physical and logical connections have been configured

Table ‑ TC #1 Detailed Test Procedures

| Step | Operator Action | Expected Results | Observed Results | Pass/ Fail |
| --- | --- | --- | --- | --- |
| 1 | Login to the GBS RBM. On the desktop, right click on “My Computer” and select “Manage.” Then select navigate to “Services” and verify RBM JBOSS, Search and Query Language (SQL) Server, and Fazzt service are running. | Services should be running |  |  |
| 2 | Navigate to Start > Run >cmd.exe. Type “route print” in the command and hit the enter key. A list of routes will populate. Verify persistent routes to shipboard end points and the shore Split IP server. | All necessary routes will be show under persistent routes. |  |  |
| 3 | In the command line, type “ftp (end point IP address).” Enter specified FTP username and password. Repeat this step for each FTP end user. | FTP session will establish successfully with no errors |  |  |
| 4 | On the desktop, double click on “VLC” to open Video Local Area Network (LAN) Client. Click “Media,” then “Open A Network Stream.” Type “udp://@(Video IP Address):(port),” then press the “Play” button. Close VLC. | The test video should begin streaming in the media window. |  |  |
| 5 | Open a web browser by clicking on the Internet Explorer icon on the Windows toolbar. In the Uniform Resource Locater (url) window, type “(IP address of Split IP Server)” and press the enter key. | Split IP Red Hat Linux test page will appear |  |  |

### Objective 2: GBS Data Product Distribution

TC#2

Description: Verify GBS FTP/FTPS product distribution

Requirement(s): GBS must be able to distribute received products to the end user

Prerequisites: TC#1

Setup: Ensure proper physical and logical connections have been configured

Table ‑2 TC #2 Detailed Test Procedures

| Step | Operator Action | Expected Results | Observed Results | Pass/ Fail |
| --- | --- | --- | --- | --- |
| 1 | Verify CANES configuration in accordance with Reference 2. | Access Lists (ACLs) are in place |  |  |
| 2 | Login to CLASS RBM by using RBMOperator as the user login name. Enter the standard GBS password. Press the Enter key.  Double-click RBM Client. Login using Username and Password created. Press the Enter key. Go to Configuration then Auto-Push.  Under End User Hosts, select CANES Information Assurance Exchange Edge Transport (IAEXET) and click the “Edit Host” button. Click “Test” Button. | A popup window indicates a successful push |  |  |
| 3 | Go to Configuration then Auto-Push.  Under End User Hosts, select Meteorological and Oceanographic (METOC) and click the “Test” button. | A popup window indicates a successful push |  |  |
| 4 | Go to Configuration then Auto-Push.  Under End User Hosts, select DCGS-N and click the “Test” button. | A popup window indicates a successful push |  |  |
| 5 | Go to Configuration then Auto-Push.  Under End User Hosts, select NITES-Next and click the “Test” button. | A popup window indicates a successful push |  |  |
| 6 | Login to UNCLASS RBM by using RBMOperator as the user login name. Enter the standard GBS password. Press the Enter key.  Double-click RBM Client. Login using Username and Password created with the GBS\_RBM\_UserCreator. Press the Enter key. Go to Configuration then Auto-Push.  Under End User Hosts, select CANES IAEXET and click the “Test” button. | A popup window indicates a successful push |  |  |

### Objective 3: GBS Video Product Distribution

TC#3

Description: Verify GBS multicast video distribution

Requirement(s): GBS must to be able to distribute multicast video to the end user

Prerequisites: TC#1

Setup: Ensure proper physical and logical connections have been configured

Table ‑3 TC #3 Detailed Test Procedures

| Step | Operator Action | Expected Results | Observed Results | Pass/ Fail |
| --- | --- | --- | --- | --- |
| 1 | Login to the SECRET GBS RBM. On the desktop, double click on “VLC” to open Video LAN Client (VLC). Click “Media,” then “Open A Network Stream.” Type “udp://@(Video IP Address):(port),” then press the “Play” button. Close VLC. | The test video should begin streaming in the media window. Assess quality In Accordance With (IAW) Appendix B. |  |  |
| 2 | Repeat Step 1 on the UNCLASS RBM | The test video should begin streaming in the media window. Assess quality IAW Appendix B. |  |  |
| 3 | Repeat Step 1 on each SECRET end user workstation (i.e. DCGS-N workstation, CANES workstation) | The test video and metadata should begin streaming in the media window. Assess quality IAW Appendix B. |  |  |
| 4 | Repeat Step 1 on each UNCLASS end user workstation. | The test video should begin streaming in the media window. Assess quality IAW Appendix B. |  |  |

### Objective 4: GBS Split IP Operation and Reachback

TC#4

Description: Verify GBS Split IP operations and Reachback path

Requirement(s): GBS Split IP and Reachback functionality needs to function properly

Prerequisites: TC#1

Setup: Ensure proper physical and logical connections have been configured

Table ‑4 TC #4 Detailed Test Procedures

| Step | Operator Action | Expected Results | Observed Results | Pass/ Fail |
| --- | --- | --- | --- | --- |
| 1 | Login to the SECRET GBS RBM. On the desktop, right click on the satellite dish inside of a box on the tool bar and select “Restore.” Verify the “Auto” button is selected and the “Status” is “Active.” | Status “Active” is green. |  |  |
| 2 | Navigate to the desktop and double click on “Wireshark.” Click “Capture,” then “Interfaces…” Find the appropriate tunnel interface and click “Start” to begin a packet capture. | Wireshark Capture begins on appropriate tunnel interface |  |  |
| 3 | Verify with ADNS split IP items are being marked | ADNS should have Split IP Items Markes |  |  |
| 4 | In the SECRET GBS RBM client gui application, click on the configuration tab.  - click the rbm profile link on the left side of the gui screen.  - Select "send" to conduct a reachback path check. If the reachback path is correctly in place then there should not be an expected success window and there should not be any error windows.  - If no window appears then contact the GBSOC to verify receipt of the RBM profile info. You can also call the COCOM TIM to verify if the GBSOC is busy. If there is an error window then write down the error message before contacting the LAN admin to troubleshooting possible network connectivity problems. | No error windows or success window should pop up. GBSOC should have received RBM profile info. |  |  |
| 5 | Verify ACLs for Reachback | ACLs for Reachback (right next to ACLs for Split IP) |  |  |

### Objective 5: Verify GBS 6.X Core Functions with HBSS

TC#5

Description: Verify GBS operates correctly with HBSS

Requirement(s): GBS ability to functionally operate after implementing HBSS

Prerequisites: TC#s 1-4

Setup: Install HBSS on the GBS RBM

Table ‑5 TC #6 Detailed Test Procedures

| Step | Operator Action | Expected Results | Observed Results | Pass/ Fail |
| --- | --- | --- | --- | --- |
| 1 | Login to the GBS RBM. On the desktop, right click on “My Computer” and select “Manage.” Then select navigate to “Services” and verify RBM JBOSS, SQL Server, and Fazzt service are running. | Services should be running |  |  |
| 2 | Navigate to Start > Run >cmd.exe. Type “route print” in the command and hit the enter key. A list of routes will populate. Verify persistent routes to shipboard end points and the shore Split IP server. | All necessary routes will be show under persistent routes. |  |  |
| 3 | In the command line, type “ftp (end point IP address).” Enter specified FTP username and password. Repeat this step for each FTP end user. | FTP session will establish successfully with no errors |  |  |
| 4 | On the desktop, double click on “VLC” to open Video LAN Client. Click “Media,” then “Open A Network Stream.” Type “udp://@(Video IP Address):(port),” then press the “Play” button. Close VLC. | The test video should begin streaming in the media window. |  |  |
| 5 | Open a web browser by clicking on the Internet Explorer icon on the Windows toolbar. In the url window, type “(IP address of Split IP Server)” and press the enter key. | Split IP Red Hat Linux test page will appear |  |  |

# APPENDIX A – acronyms

ACL Access List

ADNS Automated Digital Network System

AISIT Application Integration System Integration Test

AI Application Integration

ATO Approval to Operate

BGP Border Gateway Protocol

CANES Consolidated Afloat Networks and Enterprise Services

CAS Conditional Access System

CDVS Classified Video Distribution System

COOP Continuity of Operations

DCGS-N Defense Common Ground System - Navy

DECC Defense Enterprise Computing Center

DISN Defense Information Systems Network

EC Engineering Change

ECR Enterprise Change Request

EOLIST End of Life System Integration Test

ESP Encapsulating Security Payload

FTP File Transfer Protocol

FTPS File Transfer Protocol

FY Fiscal Year

GBS Global Broadcast Service

GCCS-M Global Command and Control System - Maritime

GUNSS Geographical Intelligence Unified Naval Streaming System

GRE Generic Routing Encapsulation

HBSS Host Based Security System

HTTP Hypertext Transfer Protocol

HTTPS Hypertext Transfer Protocol Secure

IAEXET Information Assurance Exchange Edge Transport

IER Information Exchange Requirements

IATO Interim Approval to Operate

IATT Interim Approval to Test

IAW In Accordance With

INC Increment

IP Internet Protocol

KPP Key Performance Parameter

KSA Key Support Area

LAN Local Area Network

MAC Media Access Control

mbps megabits per second

MC Media Converter

MECH Mechanicsburg, PA

METOC Meteorological and Oceanographic

MILSATCOM Military Satellite Communications

MOE Measure of Effectiveness

MS Microsoft

NIAPS Navy Information/Application Product Suite

NITES Navy Integrated Tactical Environment System

NOC Network Operating Center

NA Non-Applicable

NT Not Testable

OBJ Objective

OKC Oklahoma City, OK

OS Operating System

OSHA Occupational Safety and Health Act

PAC Pacific

PMW Program Manager, Warfare

POC Point of Contact

Q1 First Quarter

RBM Receive Broadcast Manager

SBM Satellite Broadcast Manager

SCI Sensitive Compartmented Information

SSC SPAWAR Systems Center

SIPRNET Secure Internet Protocol Router Network

SIT System Integration Test

SMPT Simultaneous MAC Packet Transfer

SMQ Simple Message Queues

SNMP Simple Network Management Protocol

SPAWAR Space and Naval Warfare Systems Command

SQL Search and Query Language

SR SECRET Releasable

TC Test Case

TCP Transport Control Protocol

UDP User Datagram Protocol

UNCLASS UNCLASSIFIED

URL Uniform Resource Locator

USR-10B AN/USB-10B

VLC Video LAN

VPN Virtual Private Network

WGS Wideband Global Satellite Communications (SATCOM)

# APPENDIX b – Video Quality Data Collection Worksheet

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **VIDEO QUALITY DATA COLLECTION WORKSHEET** | | | | | | | | | |
| **Data Collector:** | | | | | | | | | |
| **Date/Time:** | | | | | | | | | |
| **Location:** | | | | | | | | | |
| **Name of Video:** | | | | | | | | | |
| **Multicast Address:** | | | | | | | | | |
| **RBM ID:** | | | | | | | | | |
|  | | | | | | | | | |
| Please use the following when reporting video quality (table below is provided for reference). Please include **COMMENTS** in an effort add fidelity to the observations (e.g. intermittent freezing, pixilation, etc.). | | | | | | | | | |
| **Score** | **Reference** | | | **Definition** | | | | | |
| **1** | Unusable | | | Permanent or freq freezing, Extreme pixilation, unable to identify objects | | | | | |
| **2** | Poor | | | Intermittent freezing, substantial pixilation, objects identified, not crisp | | | | | |
| **3** | Average | | | Acceptable quality but intermittent freezing still present | | | | | |
| **4** | Good | | | Slight pixilation present, no freezing, handles fast motion well, exploitable | | | | | |
| **5** | Excellent | | | No pixilation present, no freezing, approaching quality | | | | | |
|  | | | | | | | | | |
| **1-Unusable** | | **2-Poor** | | | **3-Average** | | **4 -Good** | | **5- Excellent** |
| vlcsnap-15829711.png | |  | | |  | | vlcsnap-15820039.png | |  |
|  | | | | | | | | | |
| **AUDIO**  (N/A if no audio expected) | | | | | | | | | |
| **1 – Unusable** | | | **2 – Poor** | | | **3 – Average** | | **4 – Good** | **5 - Excellent** |
|  | | | | | | | | | |
| **Comments:** | | | | | | | | | |
|  | | | | | | | | | |
|  | | | | | | | | | |
|  | | | | | | | | | |
|  | | | | | | | | | |
|  | | | | | | | | | |
|  | | | | | | | | | |
|  | | | | | | | | | |
|  | | | | | | | | | |
|  | | | | | | | | | |