



**DEPARTMENT OF THE ARMY
UNITED STATES ARMY INFORMATION
SYSTEMS ENGINEERING COMMAND
FORT HUACHUCA, ARIZONA 85613-5300**



INTEGRATION EVALUATION PLAN

BY

COMMUNICATION SYSTEMS EVALUATION TEAM

TECHNOLOGY INTEGRATION CENTER

OCTOBER 2002

Distribution A

Approved for public release; distribution is unlimited.

DISCLAIMER

The use of trade names in this document does not constitute an official endorsement or approval of the use of such commercial hardware or software. Do not cite this document for the purpose of advertisement.

CHANGES

Refer requests for all changes that affect this document to: USAISEC, ATTN: AMSEL-IE-TI, Fort Huachuca, AZ 85613-5300.

DISPOSITION INSTRUCTIONS

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

INTEGRATION EVALUATION PLAN
BY
COMMUNICATION SYSTEMS EVALUATION TEAM

OCTOBER 2002

U.S. ARMY INFORMATION SYSTEMS ENGINEERING COMMAND
TECHNOLOGY INTEGRATION CENTER

Distribution Statement A

Approved for public release; distribution is unlimited.

Product Certification

Signatures below indicate that this product does not develop a design or require a formal architectural review and complies with all USAISEC standards.



JORDAN SILK
Computer Engineer
Communication Systems Evaluation Team



MARK H. BEATTIE
Team Leader
Communication Systems Evaluation Team



GEORGE H. ROBBINS II
Group Leader
Technology Assessment Group



DANIEL Q. BRADFORD
Director
Technology Integration Center

ACKNOWLEDGMENT

The United States Army Information Systems Engineering Command, Technology Integration Center thanks the following individuals for their participation in this effort:

Mr. Jeff Bhe; Veridian; 101 East Wilcox Drive, Sierra Vista, Arizona; commercial 520-533-3293, DSN 821-3293.

Mr. Paul Carlson; Veridian; 101 East Wilcox Drive, Sierra Vista, Arizona; commercial 520-533-3455, DSN 821-3455.

Mr. Derrick Howard; Veridian; 101 East Wilcox Drive, Sierra Vista, Arizona; commercial 520-533-7242, DSN 821-7242.

Mr. Jim Johnson; U.S. Army Information Systems Engineering Command, Technology Integration Center, ATTN: AMSEL-IE-TI, Fort Huachuca, Arizona; commercial 520-533-3321, DSN 821-3321.

Mr. John Kuginski; Veridian; 101 East Wilcox Drive, Sierra Vista, Arizona; commercial 520-533-7209, DSN 821-7209.

Mr. Scott Lange; Veridian; 101 East Wilcox Drive, Sierra Vista, Arizona; commercial 520-533-3577, DSN 821-3577.

Mr. Mark McFadden; U.S. Army Information Systems Engineering Command, Technology Integration Center, ATTN: AMSEL-IE-TI, Fort Huachuca, Arizona; commercial 520-533-2817, DSN 821-2817.

Mr. Joseph Otero; Veridian; 101 East Wilcox Drive, Sierra Vista, Arizona; commercial 520-533-2838, DSN 821-2838

Mr. Chris Pittman; Veridian; 101 East Wilcox Drive, Sierra Vista, Arizona; commercial 520-533-3791, DSN 821-3791.

Mr. Robert Sacha; U.S. Army Information Systems Engineering Command, Infrastructure Systems Engineering Directorate, ATTN: AMSEL-IE-IS, Fort Huachuca, Arizona; commercial 520-533-2510, DSN 821-2510.

Mr. Tony Schaffer; Veridian; 101 East Wilcox Drive, Sierra Vista, Arizona; commercial 520-533- 3362, DSN 821-3362.

EXECUTIVE SUMMARY

Product Manager, Defense Data Networks (PM, DDN) tasked the U.S. Information Systems Engineering Command (USAISEC) Technology Integration Center (TIC) to perform integration testing on network solutions before they are installed on Army installations. The TIC will conduct the testing at its lab facilities at Fort Huachuca. Integration testing occurs when Army installations require unique network solutions.

The primary purposes of the integration testing include:

- a. Reducing the risk of implementation of inadequate networks designs.
- b. Ensuring the solution meets the requirements outlined in *Statement of Requirement for CUITN*, Appendix B, *Gigabit Ethernet Data System Specification for CUITN* (CUITN specification), dated 19 July 2001.
- c. Ensuring all devices included in the solution will interoperate correctly.

This evaluation plan presents the procedures used in the TIC labs to perform the integration testing.

TABLE OF CONTENTS

	Page
Acknowledgement	iv
Executive Summary	v
1.0 INTRODUCTION	1
1.1 Background.....	1
1.2 Objective.....	1
1.3 Evaluation Overview	1
1.4 Evaluation Summary.....	2
1.5 Scoring.....	3
2.0 System performance.....	3
2.1 Routing Performance	4
2.2 Broadcast Distribution and Leak	6
2.3 Edge Routing	7
2.4 VLAN Tagging – Bridging and Routing.....	7
2.5 Multicast Performance.....	8
3.0 SYSTEM Functionality	9
3.1 Overview.....	10
3.2 System Functionality Tests.....	10
4.0 NETWORK management	15
4.1 Management Questionnaire	15
4.2 Network Management Tests	15
5.0 SECURITY	21
5.1 Security Requirement Traceability	22
5.2 Security Test Methodology.....	22

Appendices

Appendix A. System Performance Data Tables	A-1
Appendix B. System Functionality Data Table	B-1
Appendix C. Network Management Data Tables	C-1
Appendix D. Security Data Tables	D-1
Appendix E. Smartbits Configuration.....	E-1
Appendix F. Vendor Information	F-1
Appendix G. System Functionality Test Configuration	G-1
Glossary. Acronyms and Abbreviations	Glossary-1

Tables

Table 1. Evaluation Summary.....	2
Table A-1. Combined Routing Results.....	A-1
Table A-2. Edge-to-Edge Routing Results	A-1
Table A-3. Edge-to-Edge Routing Results	A-2
Table A-4. Edge-to-Edge Routing Results	A-3
Table A-6. Combined Routing Results.....	A-4
Table A-7. VLAN Tagging, Bridging, and Routing Results	A-5
Table A-8. Multicast Performance.....	A-6

	Page
Table B-1. File Transfer Protocol (FTP) Series Results.....	B-1
Table B-2. Overnight Results	B-2
Table B-3. Network Recovery Results	B-2
Table B-4. Progressive Multicast Results.....	B-3
Table B-5. Channel Surf Results	B-3
Table B-6. Multicast One-to-Many Results.....	B-3
Table C-1. Telnet Results	C-1
Table C-2. SNMP MIB Walk Results	C-1
Table C-3. SNMP SET/GET Requests Results	C-1
Table C-4. SNMP Traps Results	C-2
Table C-5. SNMP Security Results	C-2
Table C-6. Network Element Configuration Results.....	C-2
Table C-7. Port VLAN Identifier Results.....	C-3
Table C-8. Device Performance Monitoring Results	C-3
Table C-9. Network VLAN Configuration Results.....	C-3
Table D-1. Audit Results	D-1
Table D-2. Configuration Management Secure Remote Management	D-2
Table D-3. Product Integrity/Assurance Results	D-3
Table D-4. Network Based Attack Detection Results	D-3
Table D-5. Access Control Filter Results	D-4
Table D-6. Backup/Redundancy Results.....	D-5
Table E-1. SmartBits Hardware.....	E-2
Table F-1. Device Requirements	F-1
Table G-1. RTE 201-236 IP Addressing 6-Subnet.....	G-7
Table G-2. RTE 201-236 IP Addressing 6-VLAN.....	G-8
Table G-3. RTE 201-236 IP Addressing 36-Subnet.....	G-9
Table G-4. RTE Multicast Groups.....	G-10

Figures

Figure 1. Network Configuration	4
Figure 2. Routing Performance Configuration	5
Figure 3. Broadcast Distribution and Leak Configuration	6
Figure 4. FTP Series Logical Traffic Flow for 6-Subnet.....	10
Figure 5. NMS Configuration.....	16
Figure 6. Network Element Configuration	19
Figure 7. Security Lab Network Configuration.....	23
Figure G-1. 6-Subnet Configuration with L3 Building Switch and L2 at Tier 1	G-3
Figure G-2. 6-Subnet Configuration with L3 at Tier 1	G-4
Figure G-3. 6-VLAN Configuration and VLAN Logical Flow	G-5
Figure G-4. 6-VLAN Logical Connections	G-6

This page intentionally left blank.

INTEGRATION EVALUATION PLAN

1.0 INTRODUCTION

This evaluation plan describes how the U.S. Army Information Systems Engineering Command (USAISEC), Technology Integration Center (TIC) will evaluate an installation's network design and implementation.

1.1 Background

The Army's Installation Information Infrastructure Modernization Program (I3MP), administered by Product Manager, Defense Data Networks (PM, DDN) at Fort Monmouth, New Jersey, and engineered by USAISEC at Fort Huachuca, Arizona, evaluates and fields the backbone infrastructure that provides data communications capability to Army installations. The TIC verifies I3MP Gigabit Ethernet designs to determine if they meet the specifications outlined in the *Statement of Requirement for CUITN, Appendix B, Gigabit Ethernet Data System Specification for CUITN* (dated 19 July 2001). The evaluation will consist of an I3MP design slated for implementation on an Army installation executed in the TIC lab on a mock-up of the network design.

1.2 Objective

Our objective is to determine if a site implementation meets the requirements for the U.S. Army I3MP infrastructure. To meet this objective, we will ask the following questions:

- a. Does the entire system meet minimum requirements for interoperability, performance, network management, and security as set forth in the Gigabit Ethernet Specification?
- b. Are there any site unique configurations or hardware not assessed as part of the Layer 3 evaluation that now need evaluating?
- c. Is the design acceptable for implementation?

1.3 Evaluation Overview

Each of the evaluation categories is comprised of tests and subtests to meet the evaluation objectives. The evaluation consists of these four categories:

- a. **System Performance.** Using each device under test (DUT), we configure a network resembling the site implementation. This evaluation measures the performance of the network using a SmartBits packet analyzer. We apply these evaluations to the entire system. Section 2 of the Integration Evaluation Plan contains the evaluation procedure.
- b. **System Functionality.** Using each DUT, we configure a system resembling the site implementation. These system level evaluations measure the functionality of all devices as a complete system. Section 3 of the Integration Evaluation Plan contains the system level evaluation procedure.
- c. **Network Management.** The network management evaluation uses the system functionality test configuration. This evaluation assesses the network management capabilities of the Ethernet switches and the system. Section 4 of the Integration Evaluation Plan contains the network management evaluation procedure.
- d. **Security.** Each core switch, building switch, and edge device go through security assessments to determine the security impact of integrating each switch into the I3MP architecture. Section 5 of the Integration Evaluation Plan contains the security level evaluation procedure.

1.4 Evaluation Summary

Table 1 lists all of the tests performed during the evaluation along with the priority, a summary of the pass/fail criteria, and data tables.

Table 1. Evaluation Summary

Test Ref	Test Name	Priority	Pass/Fail Criteria	Data Table
System Performance				
2.1.1	Combined Routing Performance	Y	PASS if throughput is 70% or greater for all packet sizes.	A-1
2.1.2	Edge to Edge Routing Performance	Y	PASS if throughput is 75% or greater for all packet sizes.	A-2_A-4
2.2	Broadcast Distribution and Leak	Y	FAIL if traffic leaks from one VLAN to another or if traffic is not distributed within its own VLAN.	A-5
2.3	Edge Routing	Y	FAIL if edge device does not support Layer 3 routing or if edge device interferes with core routing.	A-6
2.4	VLAN Tagging - Bridging and Routing	Y	FAIL if packets are not properly bridged or routed.	A-7
2.5	Multicast Performance	Y	FAIL if the device does not support multicast or if packets are dropped with 60% multicast load using 16 groups.	A-8
System Functionality				
3.2.1	FTP Series	Y	FAIL if users do not pass traffic or if throughput rates vary greatly between users.	B-1
3.2.2	Overnight	Y	FAIL if unicast throughput varies by more than 10% from the unicast baseline or if unicast throughput varies by more than 10% from the unicast baseline when multicast traffic is introduced.	B-2
3.2.3	Network Recovery	Y	FAIL if edge does not fully recover within 5 minutes or if core does not fully recover within 5 minutes. FAIL if the network cannot re-converge all routing processes and reestablish traffic flows of all types. FAIL if the network cannot recover within 10 seconds when the disrupted system is brought back into normal service.	B-3
3.2.4	Multicast Streams	N	FAIL if multicast cannot join/leave within a reasonable time or cannot provide minimum rate through the core without dropouts while sending 12 MGENs. Dropouts are periods of inactivity lasting longer than 100 milliseconds or inactivity occurring more than one time in any 3-second period.	B-4
3.2.5	Multicast Channel Surfing	N	FAIL if any group or user receives less than 95% of the traffic.	B-5
3.2.6	Multicast One-to-Many	N	FAIL if any receiver drops from the group.	B-6

Table 1. Evaluation Summary (continued)

Test Ref	Test Name	Priority	Pass/Fail Criteria	Data Table
Network Management				
4.2.1	Telnet - Windows, Solaris, Linux	Y	PASS if valid Telnet sessions are established from the specified systems.	C-1
4.2.2	SNMP MIB Walk	N	FAIL if MIB table information is incorrect, or if requests produce errors.	C-2
4.2.3	SNMP SET/GET Requests	Y	FAIL if information is not correctly stored and recalled, or if ports do not disable and enable correctly.	C-3
4.2.4	SNMP Traps	N	PASS if traps for link status and at least one type of restart are received for the correct conditions.	C-4
4.2.5	SNMP Security	N	FAIL if device accepts requests from unauthorized stations or accepts SET requests with community strings not granting write permission.	C-5
4.2.6	Network Element Configuration	N	PASS if VLAN is established and is isolated from other ports.	C-6
4.2.7	Port VLAN Identifier	N	FAIL if device allows a second PVID assigned to the same port.	C-7
4.2.8	Device Performance Monitoring	N	PASS if displayed port statistics reflect traffic on the device.	C-8
4.2.9	Network VLAN Configuration	N	PASS if VLAN is established and is isolated from other ports across the network.	C-9
Security				
5.2.1	Audit Capability	N	FAIL if logs cannot be exported, unauthorized user can change audit trail, audit events are not selectable, or rejected connection events are not recorded.	D-1
5.2.2	Configuration Management with Secure Remote Management	Y	FAIL if remote management session is not secure, remote administration is unrestricted, or not remotely manageable via web, Telnet and FTP. Secure remote management is required on Layer-3 switches and preferred, but not required on Layer-2 switches.	D-2
5.2.3	Product Integrity and Assurance	N	FAIL if password aging, password timeout, or minimum 8-character password cannot be set.	D-3
5.2.4	Network Based Attack Detection	N	FAIL if unable to detect attacks or unable to react to attacks.	D-4
5.2.5	Access Control Filters	N	FAIL if unable to associate filters with a specific interface, unable to combine multiple filters on one port, or unable to change rules without dropping.	D-5
5.2.6	Backup and Redundancy	N	FAIL if unable to backup and restore system configuration.	D-6

SNMP=Simple Network Management Protocol; MIB=Management Information Base; VLAN = virtual local area network; FTP = File Transfer Protocol; MGEN = Multi-Generators

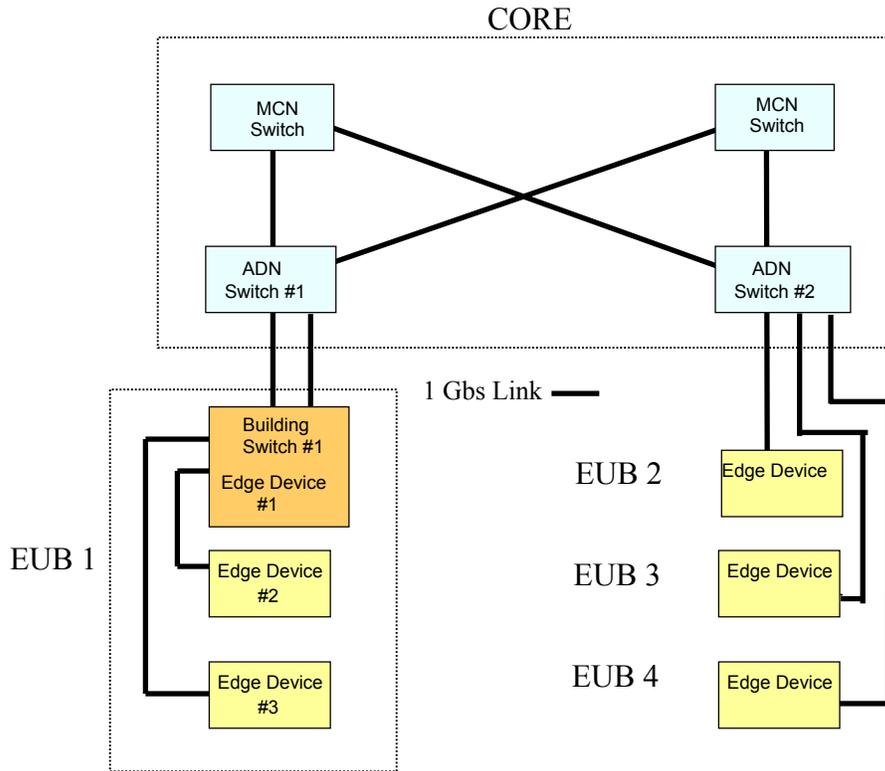
1.5 Scoring

Individual tests within the evaluations are either pass or fail. The system must pass two-thirds of all the individual tests with no priority tests failing to be acceptable for site implementation.

2.0 SYSTEM PERFORMANCE

System Performance evaluations measure the performance of the network as a whole. In other words, the evaluation combines the core and edge devices as a system. A SmartBits

packet analyzer measures the functional and performance capabilities. If the site under test adheres to the standard I3MP architecture, the evaluation network will be set up as Figure 1 shows.



EUB = end user building; MCN = main communication node

Figure 1. Network Configuration

If the site under test does not adhere to the standard I3MP architecture, the evaluation network will resemble the proposed network as closely as possible. See Appendix A for performance data tables. Appendix G provides more details on SmartBits configurations.

2.1 Routing Performance

The tests in this first section evaluate the throughput, latency, and packet loss of traffic through the network. Tests stream through all edge devices as well as the core and from single edge device to another single edge device across the core.

2.1.1 Combined Routing

a. **Objective.** The test objective is to verify interoperability of edge devices' and core switches' 1000-megabits per second (Mbps) interfaces. Performance is measured when bridging Layer 2 traffic between 100-Mbps and 1000-Mbps interfaces on the edge as well as routing Layer 3 traffic in the core.

b. **Configuration.** Figure 2 shows the test configuration. Connect SmartBits to each edge device with ten 10/100 Mbps streams to each edge device. Connect each edge device to the core switch with one 1000-Mbps stream.

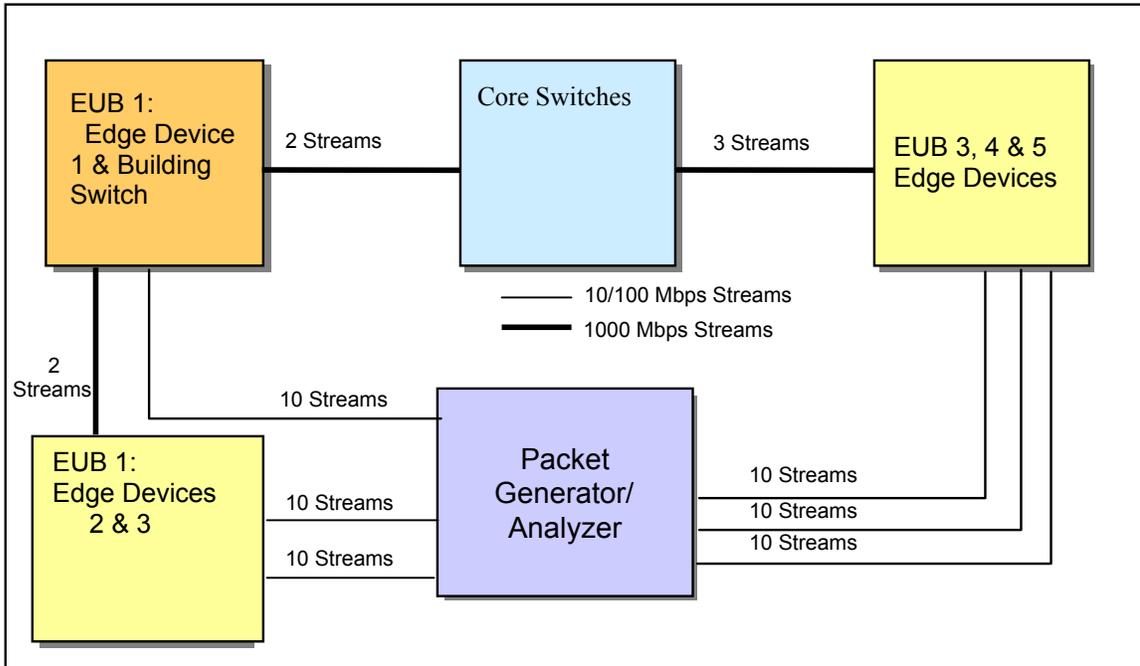


Figure 2. Routing Performance Configuration

c. Procedure.

- (1) Configure SmartBits to transmit 10 full-duplex 66.667-Mbps streams to each edge device.
- (2) Configure each edge device in EUB 1,2,3 and 4 for Layer 2 switching. Configure Building Switch #1 and all core devices to perform Layer 3 switching via Open Shortest Path First (OSPF)
- (3) Use SmartFlow to perform the Throughput and Jumbo tests in backbone mode. Perform these tests on 64, 128, 256, 512, 1024, 1280, and 1518-byte frame sizes.
- (4) Record results in [Table A-1](#).
- (5) PASS if throughput is 70% or greater for all packet sizes.

2.1.2 Edge to Edge

a. Objective. Test objective is to verify interoperability of edge devices’ and core switches’ 1000-Mbps interfaces. Performance is measured when bridging Layer 2 traffic between 100-Mbps and 1000-Mbps interfaces on the edge, as well as routing Layer 3 traffic in the core.

b. Configuration. Figure 2 shows the test configuration. SmartBits connects to each edge device with ten 10/100 Mbps streams to each edge device. Each edge device connects to the core switch with one 1000-Mbps stream.

c. Procedure.

- (1) Configure SmartBits to transmit 10 full-duplex 100-Mbps streams to each edge device.

(2) Configure each edge device in EUB 1, 2, 3, and 4 for Layer 2 switching. Configure Building Switch #1 and all core devices to perform Layer 3 switching via open shortest path first (OSPF)

(3) This test will have three iterations. The test will run from EUB1/ Device 1 to EUB 4. The test repeats for EUB1/ Device 2 and EUB 3. It runs again for EUB1/ Device 3 to EUB 2.

(4) Use SmartFlow to perform the Throughput and Jumbo tests in backbone mode. Perform these tests on 64, 128, 256, 512, 1024, 1280, and 1518-byte frame sizes.

(5) Record results in [Table A-2](#), [Table A-3](#), and [Table A-4](#).

(6) PASS if throughput is 75% or greater for all packet sizes.

2.2 Broadcast Distribution and Leak

a. **Objective.** Test objective is to verify multiple broadcast streams remain in their designated VLAN.

b. **Configuration.** Figure 3 shows the Broadcast Distribution and Leak test configuration. SmartBits connects to the edge devices with ten 100-Mbps streams to each edge device. The edge device configuration consists of two VLANs with five ports in each VLAN. VLANs on one edge device correspond to the VLANs on the second edge device. The edge devices connect to the core with the 1000-Mbps stream using 802.1Q VLAN tags.

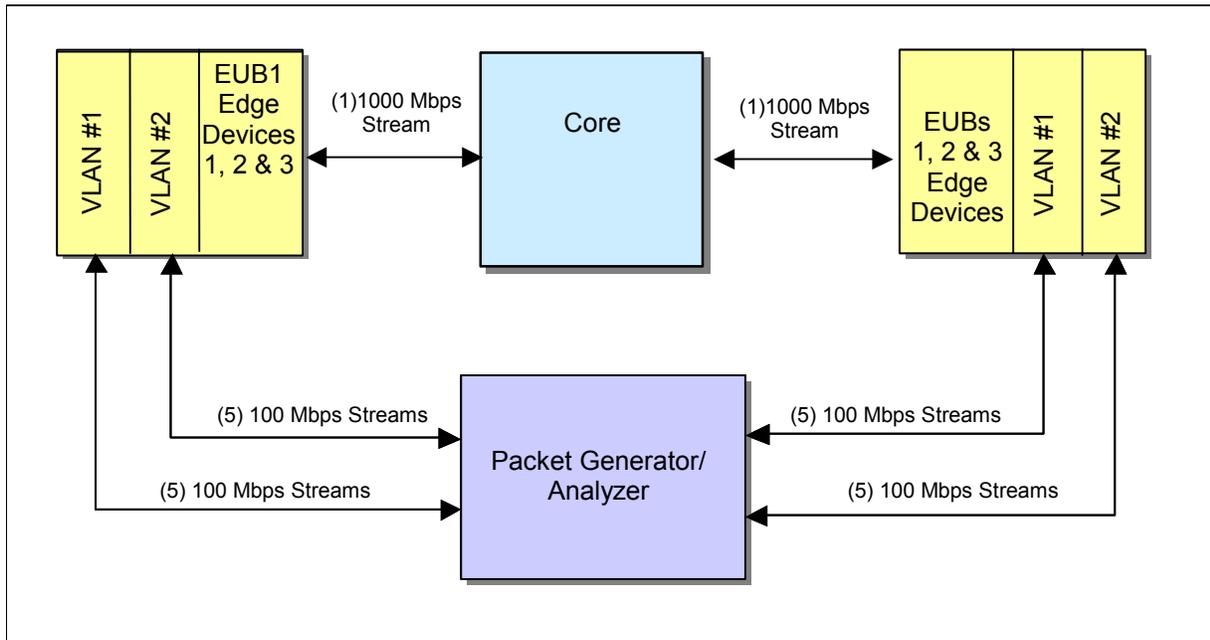


Figure 3. Broadcast Distribution and Leak Configuration

c. **Procedure.**

(1) Configure five 100-Mbps Fast Ethernet ports on each edge device in VLAN 1. Configure five 100-Mbps Fast Ethernet ports on each edge device in VLAN 2.

(2) Configure two ports on each core switch in one VLAN. Configure all the other ports in another VLAN. Connect two other 1000-Mbps ports to each core switch to monitor broadcast leakage.

(3) Configure SmartBits for two VLANs. Use SmartWindow to transmit broadcast traffic within VLAN 1. Verify traffic remains in VLAN 1 on both edge devices. Verify no traffic leaks into VLAN 2 on either edge device.

(4) Verify core traffic appears only on the two core switch ports in use.

(5) Configuring duplicate hardware on the network is not required.

(6) Record results in [Table A-5](#).

(7) FAIL if traffic leaks from one VLAN to another or if traffic does not distribute within its own VLAN.

2.3 Edge Routing

a. **Objective.** Test objective is to measure throughput while the edge device forwards Layer 3 Internet Protocol (IP) traffic between 100-Mbps and 1000-Mbps interfaces and to verify interoperability of the edge and core switch 1000-Mbps interfaces.

b. **Configuration.** Figure 2 shows the Edge Routing test configuration. SmartBits is connected to each edge device with ten 10/100 Mbps streams to each edge device. Each edge device is connected to the core or building switch with one 1000-Mbps stream.

c. **Procedure.**

(1) Configure the switch for Layer 3 switching via OSPF. Configure SmartBits to transmit 10 full-duplex 66.667-Mbps streams, with each 10/100 Mbps stream as a separate subnet. Use SmartFlow to perform the Throughput and Jumbo tests in backbone mode. Perform these tests on 128, 256, 512, 1024, 1280, and 1518-byte frame sizes in the following two scenarios:

(a) Configure Layer 3 IP routing only on the core switches.

(b) Configure Layer 3 Internet Protocol (IP) routing on both the edge and the core switch.

(2) Record results in [Table A-6](#).

(3) FAIL if edge device does not support Layer 3 routing or if edge device interferes with core routing.

2.4 VLAN Tagging – Bridging and Routing

a. **Objective.** Test objective is to verify bridging and routing performance while using 802.1Q VLAN tags.

b. **Configuration.** Figure 2 shows the VLAN Tagging – Bridging and Routing test configuration. SmartBits connects to each edge device via ten 10/100 Mbps streams. Each edge device connects to the core or building switches with one 1000-Mbps stream. There are three configurations:

(1) Bridging 10 VLANs, same 10 VLANs on each edge device.

(2) Routing VLANs, 10 different VLANs on each edge device.

(3) Routing VLANs with access control lists ACLs.

c. **Procedure.**

(1) Connect SmartBits to the edge devices with ten 66.667-Mbps streams. Connect edge devices through the core switch using single 1000-Mbps connections with 802.1Q VLAN tags. Perform the following three subtests:

(a) Bridging with 10 VLANs. Configure SmartBits to transmit tagged traffic from 10 VLANs on one edge device to the same 10 VLANs on another edge through the core. Pair EUB1/Device 1 with EUB 4, EUB1/Device 2 with EUB 3, and EUB1/Device 3 with EUB 2. Verify traffic bridges properly. Use SmartFlow to perform the Throughput and Jumbo tests in a port-pair configuration.

(b) Routing with VLANs. On each edge device, configure each 10/100-Mbps port as a separate VLAN with VLAN tags. Use Table G-8 for the IP addressing scheme. Configure SmartBits to transmit IP traffic via the VLANs, 10 per edge device, tagging each 10/100 Mbps stream. Verify the switch correctly routes tagged IP traffic over multiple VLANs. Use SmartFlow to perform the Throughput and Jumbo tests in full mesh mode.

(c) Routing with ACLs. Using the Routing with VLANs configuration, apply an ACL to determine the effect on switch performance. Use SmartFlow to perform the Throughput and Jumbo tests in full mesh mode.

(2) Perform these tests on 64, 128, 256, 512, 1024, 1280, and 1518-byte frame sizes.

(3) Record results in [Table A-7](#).

(4) FAIL if packets do not bridge or route properly.

2.5 Multicast Performance

a. **Objective.** Test objective is to measure multicast performance on the network including the maximum number of multicast groups supported by the devices.

b. **Configuration.** Figure 2 shows the Multicast Performance test configuration. SmartBits is connected to a pair of edge devices with twenty 100-Mbps streams. Each edge device connects to the core and building switches with a 1000-Mbps link.

c. Procedure.

(1) Enable Internet Group Multicast Protocol (IGMP) snooping on the edge devices, and OSPF and Protocol Independent Multicast (PIM) on the core switch. Using Distance Vector Multicast Routing Protocol (DVMRP) is acceptable if a device does not support PIM. Configure SmartBits to transmit 40 streams of multicast traffic for frame sizes 64, 1408, and 1518 to the edge devices.

(2) This test will have three iterations. The test will run from EUB1/ Device 1 to EUB 4. The test repeats for EUB1/ Device 2 and EUB 3. It runs again for EUB1/ Device 3 to EUB 2.

(3) Use SmartMulticastIP to perform each of the four following subtests:

(a) Multicast Traffic. Configure SmartMulticastIP for multicast only traffic. Configure 20 streams belonging to one subnet and 20 streams belonging to a second subnet. Configure 12 multicast groups with six transmitters on each edge device. Configure each of the 12 multicast groups with the transmitter on one edge device and one receiver on each edge device. Configure SmartMulticastIP in step mode with the following settings:

- Group count 1
- Initial rate 40%

- Maximum rate 100%
- Step rate 20%

(b) Multicast and Unicast Traffic. Configure SmartMulticastIP for multicast and unicast traffic. Use the same 12 groups as the multicast traffic subtest, but gradually introduce unicast traffic at the same rate as the multicast traffic. Configure SmartMulticastIP in step mode with the following settings:

- Group count 1
- Initial rate 10%
- Maximum rate 50%
- Step rate 10%

(c) Scaled Group Forwarding. Configure SmartMulticastIP for scaled group forwarding. SmartBits increases multicast group count from 8 to 32 by increments of 8. Configure one flow per transmitter (a single transmitter and receiver ONLY). Configure a non-member receive port to monitor stray frames. Configure SmartMulticastIP in step mode with the following settings:

- Initial rate 40%
- Maximum rate 100%
- Step rate 20%
- Initial group count 8
- Step group count 8
- Maximum group count 32

(d) Forwarding Latency. Set switch configuration for maximum load using 64, 1,408, and 1,518-byte packets. Record minimum latency, maximum latency, and average latency for each receiver port in each multicast group at each packet size.

(e) Max Group Capacity. Configure SmartMulticastIP for Max Group Capacity. Configure one transmitter port and one receiver port. Configure an initial group count of 50 with a step count of 50 groups to obtain a rough estimate of the maximum number of multicast groups. After determining this number, reconfigure SmartMulticastIP with the following settings to successively join more groups and determine the maximum:

- Rate 10%
- Initial group count 1
- Step group count 1

(4) Record results in [Table A-8](#).

(5) FAIL if the device does not support multicast or if packets are dropped with 60% multicast load using 16 groups.

3.0 SYSTEM FUNCTIONALITY

System level tests evaluate functionality and reliability of the test network. System functionality does not necessarily reflect the capacity of the DUT but more importantly reflects consistency throughout the duration of the test. Remote terminal emulation (RTE)

systems run preprogrammed scripts to measure selected performance parameters of the configured network.

3.1 Overview

System level tests measure the performance of all devices as a complete system. There are 6 edge devices, 4 core switches, and 36 RTE computers installed in a configuration resembling the I3MP architecture to provide user loading that simulates real-world conditions. If the site under test does not adhere to the standard I3MP architecture, the evaluation network will resemble the proposed network as closely as possible. Each RTE provides two 100-Mbps connections resulting in twelve 100-Mbps connections to each edge device. Edge devices 1 through 4 are each connected to core switch #1 with one 1000-Mbps link. Edge devices 5 through 8 are each connected to core switch #4 with one 1000-Mbps link each. The four core switches connect in a partial mesh using 1000-Mbps links. There are four tests run, using two different configuration scenarios. The four test areas are: File Transfer Protocol (FTP) series, Mix, Multicast and Fail-over. These tests apply to the 6-subnet and 6-VLAN configurations. When completed, the tester will have a measure of the reliability and functionality of the network when implemented into a live system. The RTE system accumulates statistics on each test it performs. World Wide Web (WWW), FTP, structured query language (SQL), and Simple Mail Transfer Protocol (SMTP) logs individually and accumulates upon each successful completion of the transaction or session. Timeouts occur at 1 minute if a transaction is not completed. Upon a timeout, the RTE logs the timeout, abandons the transaction, and executes another with no “think delay.” See Appendix B for system functionality data tables.

3.2 System Functionality Tests

3.2.1 FTP Series

a. **Objective.** Test objective is to measure forwarding performance for varying loads and traffic patterns of FTP traffic and to measure the device’s ability to load share traffic across equal cost paths via OSPF equal-cost multi-path and with no equal-cost multi-path.

b. **Configuration.** This test runs on both the 6-subnet and 6-VLAN configurations. Refer to Appendix G for 6-VLAN and 6-subnet configuration details. Figure 4 shows the FTP Series Logical Traffic Flow for 6-subnet.

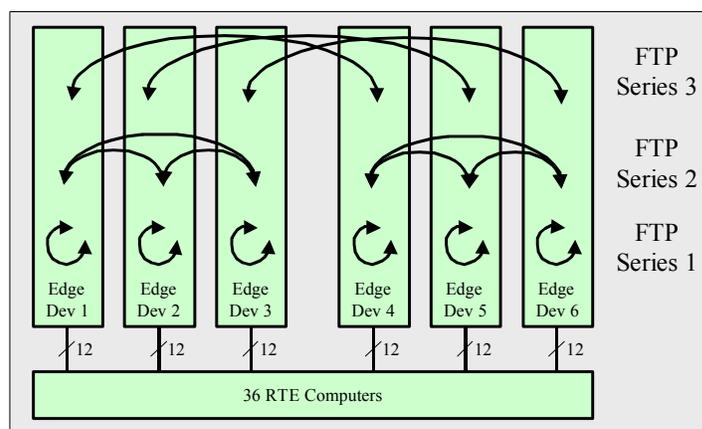


Figure 4. FTP Series Logical Traffic Flow for 6-Subnet

c. **Procedure.**

(1) There are three different series performed in this test. Each series consists of 4 functionally identical programs starting with 32 users in the first program, then 64 in the second, 128 in the third, and finally 256 users in the fourth. Each program is a 7-minute run of FTP put and get commands on a 4-megabyte (MB) text file and are executed with no “think delay” between the commands. The RTE users initially perform FTP and login as a root user to a designated server before it begins its 7-minute run and transaction logging.

(2) Run FTP Series 1. Traffic originates and terminates within the same edge device. In the 6-subnet, the traffic stays within tier 1.

(3) Run FTP Series 2. Traffic originates from one edge device to another edge device on the same side of the core. In the 8-subnet, the traffic extends to network level 2 but returns to the same side of the core.

(4) Run FTP Series 3. Traffic flows from one edge device to another edge device on opposite sides of the core. This series runs with OSPF equal-cost multi-path switched off, and then again with OSPF equal-cost multi-path switched on.

(5) Due to the 6-VLAN architecture of this network, all three FTP series test traffic flows into or through the core because all traffic is destined either to a different subnet or to a different edge device.

(6) Record results in [Table B-2](#).

(7) FAIL if users do not pass traffic or if throughput rates vary greatly between users.

3.2.2 Overnight

a. **Objective.** Test objective is to measure the test network throughput with a mix of various types of unicast and multicast traffic.

b. **Configuration.** This test runs on both the 6-subnet and 6-VLAN configurations. Refer to Appendix G for 6-VLAN and 6-subnet configuration details.

c. **Procedure.**

(1) Run all four phases of the RTE scripts (Pulse, Soak, Mix, and Multicast Mix) against the 6-subnet and 6-VLAN configurations. The tests for these phases include WWW pulse, continuous WWW, FTP, SQL, and e-mail.

(a) WWW Pulse. The network is subjected to 2,520 WWW users pulling real web pages from 36 servers. There are two repetitions of a 15-minute full-speed Hypertext Transfer Protocol (HTTP) transfer and a 45-minute idle time to allow timeouts to age out. The downloading web pages contain three HTML pages and nine 200-kilobyte (kB) Graphic Interchange Format (GIF) images.

(b) Soak. The network is subjected to four different traffic types (WWW, FTP, SQL, and e-mail) for 1 hour. Each traffic type workload is configured as 2,520 users in the $n*(n-2)$ configuration. The following paragraphs describe the four different traffic types.

- WWW Continuous - This is another WWW test identical to the WWW Pulse test but runs continuously for 1 hour with no rest period.
- FTP - This test consists of 1,296 users performing FTP puts and gets, alternating between the two. The FTP session is established at the start of the test, and the users continuously alternate between an FTP get and an FTP

put command of a 4-MB file. Each command execution is logged upon each successful completion.

- SQL - This test consists of 2,520 users, each performing SQL queries on the default *mysql* database loaded on the LINUX servers. The queries consist of requests listing table entries and row counts of some of the default tables in the database.
- E-Mail SMTP - The RTE computers use *qmail* for the SMTP message agent. The test consists of 2,520 users that send and receive varying size mail with SMTP servers.

(c) Unicast Mix. This 2-hour test performs a combination of WWW, FTP, SQL, and SMTP traffic in an $n*(n-1)*2$ configuration. This creates 2,520 streams with the following traffic ratio: 65% WWW, 20% SMTP, 10% SQL, and 5% FTP.

(d) Multicast/Unicast Mix. This 4-hour test divides into two sections. The first section performs a combination of unicast traffic consisting of WWW, FTP, and SMTP traffic for the first 2 hours of the test. In the second section, multicast traffic is added to the existing unicast traffic. For the remainder of the test, traffic is a combination of multicast and unicast traffic. The test is designed so that 12 designated RTE computers are excluded from any unicast traffic and are instead used to transmit and receive multicast streams at a rate of 5% load on each of the six 100-Mbps links. The unicast mix runs to establish a baseline, and then multicast is added to show any global effects it may have on the unicast traffic. The traffic ratio among the various types of traffic remains constant throughout the test.

(2) Record results in [Table B-3](#).

(3) FAIL if unicast throughput varies by more than 10% from the unicast baseline or if unicast throughput varies by more than 10% from the unicast baseline when introducing multicast traffic.

3.2.3 Network Recovery

a. **Objective.** Test objective is to measure network recovery time during fail-over and recovery when subjected to link and device failures and to verify standby routing functionality.

b. **Configuration.** This test runs on both the 6-subnet and 6-VLAN configurations. Refer to Appendix G for 6-VLAN and 6-subnet configuration details. Also, refer to Figure G-1.

c. **Procedure.**

(1) Use the RTEs to generate FTP and ICMP traffic to provide a visual indicator of network status while this test is in progress. Run FTP series 3, using the 256-user program, to monitor traffic flow and use the ping script, sequencing pings through all the RTE computers to monitor route convergence. Watch network activity bars on the RTE graphical user interface (GUI) for changes in the traffic pattern as links and devices are brought down and restored. Perform the test a second time running a multicast test with six transmitters, three on each side of the core and each having six receivers evenly spread across the edge devices.

(2) Verify the following during fail-over and recovery:

(a) Cutover to redundant IP routing with device or link failure - OSPF equal cost multi-path or redundant routing protocol such as Virtual Router Redundancy Protocol (VRRP).

(b) Edge device redundant gigabit uplink cutover with device or link failure.

(c) Recovery after gigabit switch reboot: ADN 1 and ADN 2.

(d) Recovery after edge device reboot: edge device #1 and edge device #5.

(e) Fabric redundancy check.

(f) Processor redundancy check.

(g) Power supply redundancy check.

(3) Layer 2 and Layer 3 Edge - Edge device #1 is dual homed to both ADNs as shown in Figures G-1 and G-2 for the 6-subnet and Figure G-2 for the 6-VLAN. Verify the following:

(a) Verify that ADN 1 has control of the gateway then pull the link between ADN 1 and the edge device. ADN 2 should take control of the gateway.

(b) Once ADN 2 has assumed control, restore the link. ADN 1 should regain control if VRRP is used. ADN 2 may retain control if another redundancy method is used.

(c) Once the network has stabilized, pull the link between ADN 2 and the edge device.

(d) Restore the link after verifying that nothing has changed.

(e) Power down ADN 1. ADN 2 should assume control.

(f) Restore power to ADN 1 and wait for the network to stabilize.

(g) Power down ADN 2. Verify nothing happens, unless ADN 2 had control of the gateway.

(h) Once the network has stabilized, restore power to ADN 2.

(4) Layer 3 Core – Power down each ADN and main communication node (MCN) to see the effect on the network. Restore each device before powering down the next device. Pull the inter-core links one at a time to see the effect on the network.

(5) Record results in [Table B-4](#).

(6) FAIL if edge device does not fully recover within five minutes or if core does not fully recover within five minutes. FAIL if the network cannot re-converge all routing processes and reestablish traffic flows of all types. FAIL if the network cannot recover within 10 seconds when the disrupted system is brought back into normal service.

3.2.4 Multicast Streams

a. **Objective.** Test objective is to measure the networks forwarding performance and functionality for varying loads and traffic patterns of IP multicast.

b. **Configuration.** Refer to Appendix G for 6-VLAN and 6-subnet configuration details. Figure G-3 depicts the logical traffic flow as described in this test. Test both the 6-subnet and 6-VLAN architectures. Enable the network with Protocol Independent Multicast-Dense Mode (PIM-DM) multicast routing and IGMP version 2 snooping. Place a network analyzer in line on one of the RTE client's network connections to analyze IGMP

join/leave functionality, multicast IGMP snooping, and multicast source quenching while the test is in operation.

c. **Procedure.**

(1) Run the Multicast Generator (MGEN) suite.

(2) The MGEN suite, developed by the U.S. Navy, provides the same type of reports as the SmartBits Multicast application. The MGEN suite consists of three programs: a multicast generator, a Dynamic Receiver (DREC) and a multicast calculator (MCALC). RTE scripts run to configure, control, and synchronize the MGEN programs on each RTE computer. Each stream in all of these tests is independent of one another in that each has a unique IP address as well as a unique port number assigned by the script. The DREC generates a statistical log of each received packet and post compiles at the end of each MGEN test.

(3) Run the *runmult* script generating *Progressive and High Capacity Streams*.

This is a series of incrementing multicast streams that start with a single sender generating a stream, and it is followed by a receiver on every edge device simultaneously joining with the sender. The receivers remain joined for five minutes, at which time they simultaneously send leave messages and stop the sender. The test repeats using 4 streams, 8 streams, etc., stepping 4 at a time for each repetition until 36 streams along with 288 receivers (36 per edge) is reached. Each stream is set for 497 packets per second at 1,408-bytes per packet. With 36 streams in place, the core encounters an accumulated traffic rate of 252 Mbps from the senders. Each group has receivers on all six edge devices generating a combined rate of about three gigabits of multicast traffic. A maximum of 1.5 gigabits per second (Gbps) of bi-directional traffic flows on any one-gigabit link. The thirty-six 10/100-Mbps links used by this test transmits 6 Mbps and receives 84 Mbps of multicast traffic.

(4) Record results in [Table B-5](#).

(5) FAIL if multicast cannot join/leave within a reasonable time or cannot provide minimum rate through the core without dropouts while sending 12 MGENs. Dropouts are periods of inactivity lasting longer than 100 milliseconds or inactivity occurring more than once in any 3-second period.

3.2.5 Multicast Channel Surfing

a. **Objective.** Test objective is to verify the system can handle channel surfing, switching one transmit to one receive every minute.

b. **Configuration.** This test runs on both the 6-subnet and 6-VLAN configurations. Refer to Appendix G for 6-VLAN and 6-subnet configuration details.

c. **Procedure.**

(1) Perform *Couch Potato Channel Surfing* by running the *mcsurf* script.

(2) Each RTE transmits 1 multicast stream to the network for a total of 36 constant streams. Each computer also joins a client to the stream of the next computer in sequence. Every 60 seconds all of the receivers rotate to the next computer by performing a leave and a join. This continues until each receiver has surfed all the multicast streams. Also, a network analyzer is placed in line on one of the RTE clients network connections to analyze join/leave functionality, multicast IGMP snooping and multicast source quenching while the test is in operation. Each stream is set for 125 packets per second at 1,408-bytes per packet.

(3) Record results in [Table B-6](#).

(4) FAIL if any group or user receives less than 95% of the traffic.

3.2.6 Multicast One-to-Many

a. **Objective.** Test objective is to verify that the system can handle a commander's briefing with 2 transmitters and 70 receivers, and to measure packet loss during joins/leaves in other users.

b. **Configuration.** This test runs on both the 6-subnet and 6-VLAN configurations. Refer to Appendix G for 6-VLAN and 6-subnet configuration details. This test is only valid after passing MGEN 1 and MGEN 2.

c. **Procedure.**

(1) Perform *All Eyes on the Podium/Commander's Briefing* by running the *mcpodium* script.

(2) The commander's briefing test consists of two multicast streams. Sender 1 is located on edge 1 and sender 2 is located on edge 5. Thirty-five receivers join sender 1. Later, another 35 receivers join sender 2. Once established, 17 receivers leave sender 1 and then 17 receivers leave sender 2. Once completed, the test ends with the remaining receivers sending leave messages. Each stream is set for 497 packets per second at 1,408-bytes per packet.

(3) Record results in [Table B-7](#).

FAIL if any receiver drops from the group.

4.0 NETWORK MANAGEMENT

Evaluate Network Management capabilities while the switches are installed in the system test configuration. The Evaluation Team will examine the SNMP capabilities of network devices and the capabilities of device management products for Network Management Stations (NMS) running Solaris and Windows. The Evaluation Team will assess device responses to various valid and invalid SNMP MIB requests, as well as the remote configuration and monitoring capabilities of the device management applications. See Appendix C for network management data tables.

4.1 Management Questionnaire

In addition to evaluating NMS capabilities, the Evaluation Team will also gather marketing information from each vendor. This data is collected in a management questionnaire in [Table C-10](#).

4.2 Network Management Tests

4.2.1 Telnet – Windows, Solaris, and Linux

a. **Objective.** Test objective is to determine the ability of network devices to accept Telnet connections from systems running various operating systems in a Gigabit Ethernet (GbE) network.

b. **Configuration.** Figure 5 shows the Telnet test configuration (same as NMS configuration). The network consists of a switch and two edge devices. The management workstation connects directly to the switch. One workstation connects to edge device #1 via an Ethernet connection. The second workstation connects to edge device #2 via an Ethernet connection.

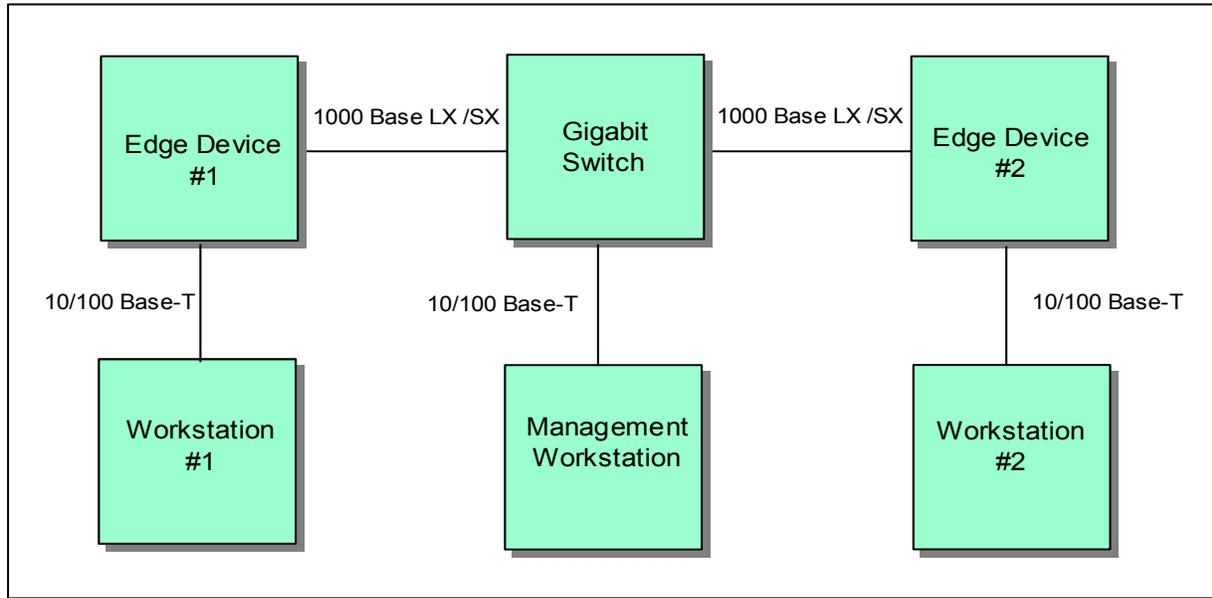


Figure 5. NMS Configuration

c. Procedure.

(1) Contact the network device via Telnet from several platforms, each running a different operating system.

(2) Verify Telnet connections establish correctly from each platform. The platforms include Solaris, Windows, and Linux.

(3) Record results in [Table C-1](#).

(4) PASS if valid Telnet sessions establish from the specified systems.

4.2.2 SNMP MIB Walk

a. **Objective.** Test objective is to determine the ability of a network device to provide the standard SNMP MIB (MIB-II) and the vendor's MIB for the requesting NMS.

b. **Configuration.** Figure 5 shows this test configuration. The network configuration consists of a switch and two edge devices. The management workstation connects directly to the switch. One workstation connects to edge device #1 via an Ethernet connection. The second workstation connects to edge device #2 via an Ethernet connection.

c. Procedure.

(1) Execute SNMP GET and GET-NEXT requests. The network management application requests portions of the MIB tree from the network device and will display or record the results on the NMS.

(2) The network management application on the NMS starts an MIB walk of the MIB-II sub-tree of the SNMP MIB, specifying the IP address and the read-only community string configured on the network device. Inspect the results of the MIB walk to verify all relevant groups of MIB-II returned values. The relevant groups include the system, interfaces, IP, Transmission Control Protocol (TCP), and SNMP.

(3) Check the interfaces group to verify that all device interfaces show, and check the IP group to verify the correct IP address of the network device. Conduct an MIB walk of

the Remote Monitoring (RMON) MIB for the network device. Inspect the results of the RMON MIB walk to verify support of all relevant groups of RMON. The relevant groups include statistics, history, events, and alarms.

(4) Perform an MIB walk of the vendor MIB, located in the *private.enterprises.<vendor>* sub-tree for the network device. Inspect the results of the vendor MIB walk to verify that all relevant groups of the vendor MIB returned appropriate values. Repeat the MIB walk and results examinations for other MIBs that the vendor claims to support.

(5) Record results in [Table C-2](#).

(6) FAIL if MIB table information is incorrect, or if requests produce errors.

4.2.3 SNMP SET / GET Requests

a. **Objective.** Test objective is to determine the ability of a network device to respond correctly to SNMP SET and GET requests.

b. **Configuration.** Figure 5 shows this test configuration. The network consists of a switch and two edge devices. The management workstation connects directly to the switch. One workstation connects to edge device #1 via an Ethernet connection. The second workstation connects to edge device #2 via an Ethernet connection.

c. **Procedure.**

(1) The NMS attempts to reset various MIB values on the network device including device port activation, and requests the variable values to verify the change. Verify the state of the network device as matching the MIB variable settings.

(2) The network manager sets the MIB-II system location variable, *system.sysLocation.0*, on the selected network device to the string *Bldg. 53302 TIC*. Verify the network manager indicates that the set was successful.

(3) The network manager gets the MIB-II system location variable, *system.sysLocation.0*, on the selected network device. Verify the network manager indicates that the GET request was successful and that the system location is *Bldg. 53302 TIC*.

(4) The network manager verifies that the interface of the network device attached to a workstation is up. The network manager turns off the interface of the network device to the attached workstation by setting the interface's variable *interfaces.ifTable.ifEntry.ifAdminStatus.n*, where *n* is the interface SNMP index, to *down*. Verify that the network manager indicates the set was successful.

(5) The network manager verifies that the interface of the network device attached to workstation is down. The network manager turns the interface of the network device back on by setting the above interface variable to *up* and verifies that the connection to the workstation is re-established.

(6) Record results in [Table C-3](#).

(7) FAIL if information is not correctly stored and recalled, or if ports do not disable and enable correctly.

4.2.4 SNMP Traps

a. **Objective.** Test objective is to determine the ability of network devices to generate SNMP traps for reportable failure conditions and send them to a specified network management station.

b. **Configuration.** Figure 5 shows this test configuration. The network consists of a switch and two edge devices. The management workstation connects directly to the switch. One workstation connects to edge device #1 via an Ethernet connection. The second workstation connects to edge device #2 via an Ethernet connection.

c. **Procedure.**

(1) Subject the network device to the following three conditions that should generate SNMP traps. View any received trap events from the network management application on the NMS.

(a) Cycle power on the network device to generate a cold start trap.

(b) Reboot the network device by a system reset to generate a warm start trap.

(c) Disconnect the cable connecting a workstation to the network device for at least 1 minute to generate a link down trap. Reestablishing the connection will generate a link up trap. Do not choose the management workstation connection!

(2) Inspect the event log of the management application to verify receiving the four traps by the NMS.

(3) Record results in [Table C-4](#).

(4) PASS if traps for link status and at least one type of restart are received for the correct conditions.

4.2.5 SNMP Security

a. **Objective.** Test objective is to determine the ability of a network device to reject SNMP SET and GET requests for unauthorized management stations and incorrect community strings.

b. **Configuration.** Figure 5 shows this test configuration. The network consists of a switch and two edge devices. The management workstation connects directly to the switch. One workstation connects to edge device #1 via an Ethernet connection. The second workstation connects to edge device #2 via an Ethernet connection.

c. **Procedure.**

(1) The NMS attempts to reset various MIB variable values on the network device using the read-only community string and an invalid community string, and requests the variable values when the network device does not have the NMS in its access list. The various requests should time out on the NMS to indicate rejection. In addition, each failed request should cause an authentication failure trap to be sent.

(2) Attempt to set the MIB-II system location variable, *system.sysLocation.0*, on the selected network device to the string TIC LAB using the read-only community string of the network device. The network manager times out to indicate that the set failed. Authentication failure events are recorded in the network manager application log.

(3) Get the MIB-II system location variable, *system.sysLocation.0*, on the selected network device using the read-only community string. The network manager should indicate that the GET request was successful and that the system location is not TIC LAB.

(4) Attempt the above operation again, but substitute an invalid community string for the read-only community string for the SET request with the same results as before.

(5) Change the IP address of the NMS in the network device SNMP access list to a different address, using the network device console interface. The address cannot be any universal access address. Attempt to access the MIB-II system location variable, *system.sysLocation.0*, on the selected network device using the read-only community string. The network manager should time out to indicate that the GET request failed.

(6) Change the IP address of the NMS in the network device SNMP access list back to the correct address using the network interface device console.

(7) Record results in [Table C-5](#).

(8) FAIL if device accepts requests from unauthorized stations or accepts SET requests with community strings not granting write permission.

4.2.6 Network Element Configuration

a. **Objective.** Test objective is to determine the ability to configure a network element from the network management platform using the network element manager or configuration tool.

b. **Configuration.** Figure 6 shows this test configuration. The network consists of a switch and an edge device. The management workstation connects directly to the switch and the two workstations connect to the edge device via 10/100Base-T Ethernet connections.

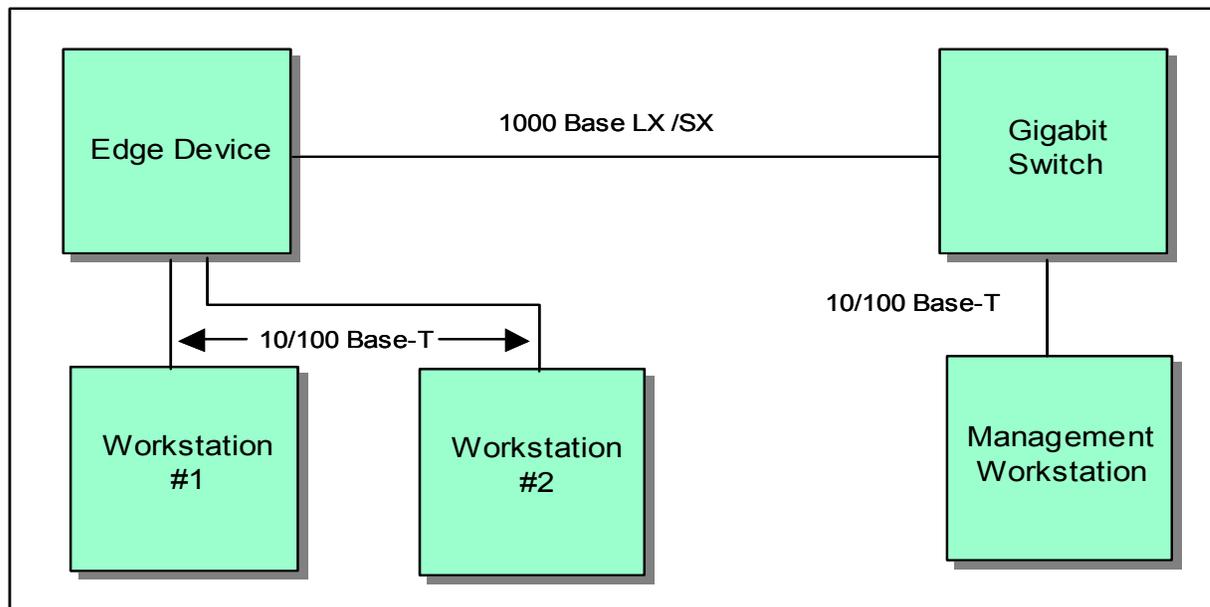


Figure 6. Network Element Configuration

c. **Procedure.**

(1) Attach the two workstations to the edge device. Use the element manager to configure a subnet and a VLAN. View the configuration of the edge device from the management workstation. Workstation #1 will attempt to communicate with workstation #2.

(2) Inspect the initial configuration of the network element using the element manager to verify that no separate VLAN is configured between workstation #1 and #2. Use the element manager to construct a VLAN named *VLAN_nm1* between workstation #1 and #2. Verify the element manager displays the new VLAN and that the workstation device ports are members of the VLAN. Workstation #1 will attempt to contact workstation #2 to verify the subnet connection.

(3) Record results in [Table C-6](#).

(4) PASS if VLAN is established and is isolated from other ports.

4.2.7 Port VLAN Identifier

a. **Objective.** Test objective is to determine whether the network device supports only one PVID per access port.

b. **Configuration.** Figure 7 shows the PVID test configuration (same as NMS configuration). The network consists of a switch and two edge devices. The management workstation connects directly to the switch. One workstation connects to edge device #1 via an Ethernet connection. The second workstation connects to edge device #2 via an Ethernet connection.

c. **Procedure.**

(1) Assign the PVID to a specific port on the edge device via the management workstation. There should be only one PVID assigned to an access port.

(2) Attempt to assign a second PVID to the same port.

(3) Verify the second attempt fails either by not allowing the reassignment or by changing the PVID to the new one.

(4) Record results in [Table C-7](#).

(5) FAIL if device allows a second PVID assigned to the same port.

4.2.8 Device Performance Monitoring

a. **Objective.** Test objective is to determine the element manager's capability to display port information on the management workstation.

b. **Configuration.** Figure 7 shows the Device Performance Monitoring test configuration (same as NMS configuration). The network consists of a switch and two edge devices. The management workstation connects directly to the switch. One workstation connects to edge device #1 via an Ethernet connection. The second workstation connects to edge device #2 via an Ethernet connection.

c. **Procedure.**

(1) Attempt to collect port information from a network device to display on the management station console.

(2) Use the element manager to connect to a device within the GbE network, and select a port to be monitored. The port should be one of the ports to which the workstations

connect or a port on the primary path between them. View the collected information on the management station console.

(3) Transfer a file from workstation #1 to workstation #2. This generates traffic on the monitored port.

(4) The element manager should generate a graph or table that shows all traffic and changes on the monitored port. Note the output characteristics including whether the display is tabular or graphical, and whether collected data includes historical trend storage or only current status.

(5) Record results in [Table C-8](#).

(6) PASS if displayed port statistics reflect traffic on the device.

4.2.9 Network VLAN Configuration

a. **Objective.** Test objective is to determine if the element manager can configure a VLAN across the Ethernet network.

b. **Configuration.** Figure 7 shows the Network VLAN test configuration (same as the NMS configuration). The network consists of with a switch, two edge devices, a management workstation, and two workstations. The management workstation connects to the core switch. One workstation connects to edge device #1 via an Ethernet connection. The second workstation connects to edge device #2 via an Ethernet connection.

c. **Procedure.**

(1) Use the element manager to construct a VLAN named “VLAN_nm2” between the two workstations on the edge devices. Verify the VLAN connection by contacting workstation #2 from workstation #1.

(2) Use the management workstation to contact one of the workstations in *VLAN_nm2*. Since there is no Layer 3 routing, the attempt should fail verifying proper isolation of “VLAN_nm2” from the rest of the network.

(3) Record results in [Table C-9](#).

(4) PASS if VLAN is established and is isolated from other ports across the network.

5.0 SECURITY

The core switch undergoes a security assessment to determine the security impact when the switch integrates into the I3MP architecture. Each device is evaluated against a set of security requirements specified in Army Regulation (AR) 380-19 and other Department of Defense (DoD) regulations. The security evaluation procedure in this section is a summary of a larger evaluation procedure. See Appendix D for security data Tables D-1 through D-6, which list results for questions asked about each device. Security engineers examine the capabilities of the switch to determine the capability of the component to provide secure management, protect itself from security compromise, and provide security access protection to the connected network assets. Security engineers also use Internet Security Systems (ISS) SafeSuite and Network Associates Incorporated (NAI) CyberCop scanning programs to look for high-risk vulnerabilities in the switches.

This is a limited operational test designed to check against a specific set of security vulnerabilities. The test is not an exhaustive examination and not all of the device’s capabilities or vulnerabilities are examined.

5.1 Security Requirement Traceability

The security requirements criteria used in this evaluation are quoted verbatim from the appropriate regulatory documents. The criteria subparagraphs describe the metrics by which the TIC evaluators judge whether the intelligent addressable device meets or does not meet the stated requirements. We use the following documents to evaluate the intelligent addressable device under test:

- a. Information Systems Security [AR 380-19].
- b. Trusted Computer System Evaluation Criteria [DoD 5200.28-Standard (STD)].
- c. Trusted Network Interpretation [National Computer Security Center-Technical Guide (NCSC-TG-005)].
- d. Trusted Network Interpretation Environments Guideline (NCSC-TG-011) (Red Book).
- e. Required network security services have been determined at the TIC via network analysis. They form the basis for the evaluation of the capabilities that network security services offer.

5.2 Security Test Methodology

Use the following techniques to evaluate the intelligent addressable device's compliance with the specified security requirements:

- a. Inspection - Examination of an item or review of design documentation to confirm compliance with specified requirements.
- b. Demonstration - Verification of an operational or functional capability by performance witnessed by a qualified observer. Observance of operation or inspection of generated output data determines compliance with specified requirements.
- c. Testing - Performance of functional operations under specified conditions. Testing involves the generation, acquisition, and recording of test data. Determine compliance with specified requirements by analyzing the data produced by the tests.
- d. Analysis - Review or interpretation of analytical or empirical data under defined conditions or reasoning to show theoretical compliance with the specified requirements.
- e. Validation – Validation of vendor claims through the Technical Support Office or representative for features and capabilities that cannot be verified by other means.

Figure 7 is a layout of the network configuration that evaluators will use for security testing.

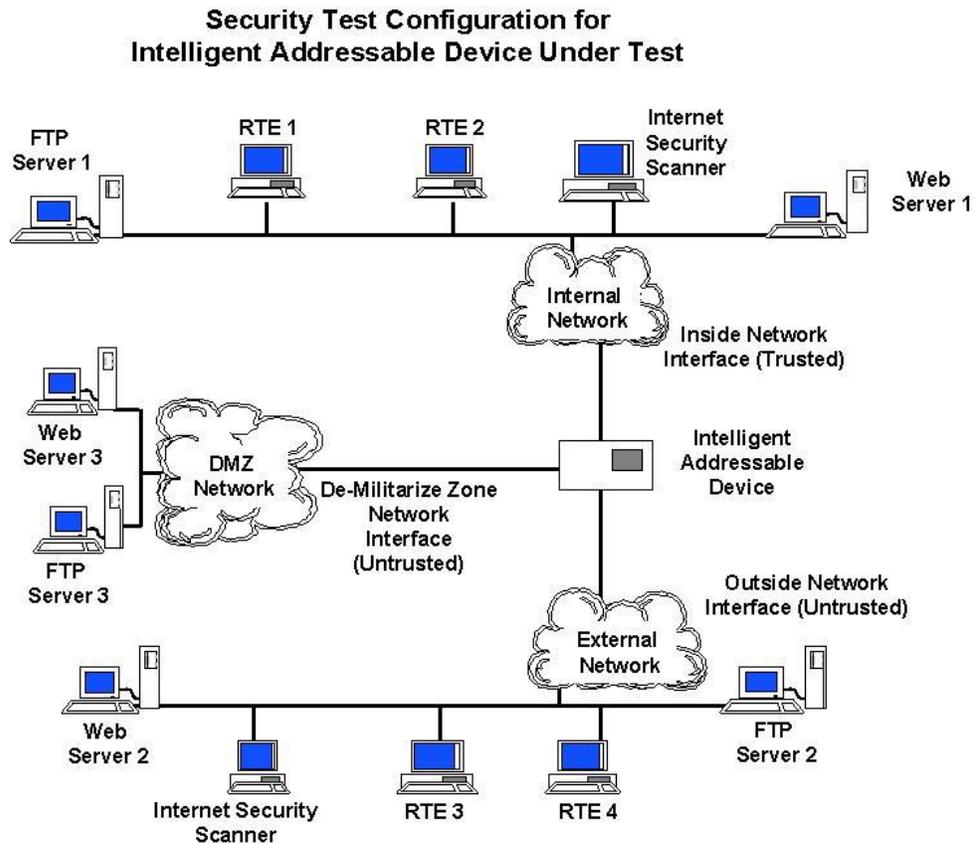


Figure 7. Security Lab Network Configuration

5.2.1 Audit Capability

a. **Objective.** Test objective is to verify the switch's ability to export logs to a centralized audit management station, to prevent unauthorized access of the audit trail, to audit security selectable events, to support local or remote network auditing, and to record connection attempts rejected by ACL rules.

b. **Configuration.** Figure 7 shows the security lab network configuration. Analysis and Inspection methods are used for this test.

c. **Procedure.**

(1) Enable auditing service. Verify the audit file (syslog) exports to another device for storage.

(2) Make changes to the setup configuration. Analyze the audit file and verify product audits all administrative actions.

(3) Scan the product using Cybercop and ISS. Create a VLAN and assign ACL rules. Attempt various types of connections to the product including logins with invalid passwords. Verify all activity is monitored in audit file.

(4) Activate local logging and issue various commands. Log in by remote via Telnet, web, GUI, and Secure Shell(SSH) to review logs. Activate the syslog service on the management station and issue various commands in the switch management console. Review the audit file locally on the management station. Verify the product allows local and remote auditing.

(5) Setup an ACL and try to connect from an unauthorized IP address. Verify the product records connection attempts rejected by the product's access control rules. Verify the log file shows evidence that the necessary information is recorded in the audit file.

(6) Record results in [Table D-1](#).

(7) FAIL if you cannot export logs, unauthorized user can change audit trail, audit events are not selectable, or rejected connection events are not recorded.

5.2.2 Configuration Management with Secure Remote Management

a. **Objective.** Test objective is to verify the switch's ability to provide full session confidentiality, to secure connections prior to transmission across an untrusted network, to restrict remote administration, to be SNMP/Common Management Information Protocol (CMIP) manageable, and to allow remote management via web, Telnet and FTP.

b. **Configuration.** Figure 7 shows the security lab network configuration. This test uses Analysis, Inspection, and Validation methods.

c. **Procedure.**

(1) Using SSH, control the product from a distant location. Log off the remote terminal program and use other options; i.e., Blowfish, Data Encryption Standard (DES), and Triple DES. Use a sniffer to view packets from the mirror port. Verify session confidentiality enforcement through negotiation of key exchanges, secure tunneling, signature verification, or encryption algorithms.

(2) Enabled SSH and monitor actions with a sniffer. Verify the product secures the connection prior to transmission across an untrusted network.

(3) Give administrative rights to a specific IP address. Attempt to make changes from another IP address that was not given permissions. Verify the product does not allow remote administration from the second address.

(4) Configure the ACL to log when a device pings the product and log this information on another server. Verify remote managers have the same capability as local managers to view logs, configure filters, and receive alerts.

(5) Configure various password restrictions. Verify the ability to restrict product management to administrators collocated with and/or directly connected to the product.

(6) Configure an NT terminal with the management software, Internet Explorer, FTP, and SSH. Initiate management sessions using each of these tools. Verify the product allows remote management via web, Telnet, and FTP.

(7) Record results in [Table D-2](#).

(8) FAIL if remote management session is not secure, remote administration is unrestricted, or not remotely manageable via web, Telnet, or FTP. Secure remote management is required on Layer 3 switches and preferred, but not required on Layer 2 switches.

5.2.3 Product Integrity and Assurance

a. **Objective.** Test objective is to verify the switch's ability to set password aging, to protect passwords, to set a password attempt timeout limit, and to require a minimum eight-character password.

b. **Configuration.** Figure 7 shows the security lab network configuration. This test uses Analysis and Inspection methods.

c. **Procedure.**

(1) Verify the switch's ability to set password aging.

(2) Configure a new password, and then try to read the password file. Verify passwords are protected.

(3) Connect to the switch using Telnet, SSH, and SNMP. Verify disablement of the user account, if the user attempts to authenticate more than the established number of authentication attempts.

(4) Review product documentation and set passwords for at least two users. Verify the product can require a minimum eight-character password. Also, note if the switch supports the use of the 36 alphabetic-numeric characters.

(5) Record results in [Table D-3](#).

(6) FAIL if the switch cannot set password aging, password timeout, or minimum 8-character password.

5.2.4 Network Based Attack Detection

a. **Objective.** Test objective is to verify the switch's ability to detect and react to network-based attacks, to specify the reaction to the attack, and to provide alerts and instructions to the administrator.

b. **Configuration.** Figure 7 shows the security lab network configuration. This test uses Analysis and Inspection methods.

c. **Procedure.**

(1) Scan the switch using various scanning tools while monitoring the logs. Verify the product has the ability to detect and react to attacks. Include the following:

- Threat profiles (port scans, ping attacks, etc)
- User Datagram Protocol (UDP) scans
- TCP port scans
- Ping attacks
- Synchronization (SYN) attacks
- IP spoofing attacks
- Ping of death
- ISS attacks

(2) Review product documentation and browse GUI functionality. Verify the switch has the capability to select the events on which to alert or take action and has the

ability to execute a predefined, site-configurable “under attack” action. Note whether the switch provides at least one “under attack” administrator alert.

(3) Verify the switch reacts to the detected attack as established by the system administrator (SA) so that a predetermined action can take place. Predetermined actions may be: trigger an audible alarm, page or send e-mail to the SA, initiate SNMP traps, set up a blind alley, break a network connection, perform special additional auditing, or perform an automatic trace. Verify the switch provides suggested instructions for handling attacks.

(4) Verify the switch reacts to unauthorized login attempts.

(5) Record results in [Table D-4](#).

(6) FAIL if unable to detect attacks or unable to react to attacks. Network-based attack detection is required on Layer 3 switches but not on Layer 2 switches.

5.2.5 Access Control Filters

a. **Objective.** Test objective is to verify the switch’s ability to associate filters with a specific interface, to perform packet filtering/stateful inspection/proxy, to combine multiple filters on one port, and to change rules without dropping.

b. **Configuration.** Figure 7 shows the security lab network configuration. This test uses Analysis and Inspection methods.

c. **Procedure.**

(1) Configure a filter and associate it with a specific port. Verify the switch is able to associate filters to interfaces/ports (e.g. segment networks, designate administration port, etc).

(2) Set up an ACL and apply it to a port. Attempt to pass traffic through the port that should be filtered out (dropped). Verify the switch can perform packet filtering/stateful inspection/proxy on: IP source address, IP destination addresses, protocol, TCP source port, TCP destination port, source interface, and destination interface.

(3) Attempt to configure multiple ACLs on a single port. Verify the switch allows combining filters to form an aggregate filter of very narrow focus.

(4) Transfer a large file between two machines through the switch. While the transfer is in progress, perform configuration changes. Verify making changes without affecting the file transfer.

(5) Record results in [Table D-5](#).

(6) FAIL if unable to associate filters with a specific interface, unable to combine multiple filters on one port, or unable to change rules without dropping traffic. Layer 3 switches require the ability to add Access Control Filters, but Layer 2 switches do not require this ability.

5.2.6 Backup and Redundancy

a. **Objective.** Test objective is to verify the switch’s ability to backup and restore the system configuration.

b. **Configuration.** Figure 7 shows the security lab network configuration. This test uses Analysis and Inspection methods.

c. **Procedure.**

(1) Save configuration settings and control lists in flash memory. Attempt to copy this file to the administration console machine. Verify ability to back up system configurations and control lists.

(2) Attempt to copy the configuration settings and control lists back to the switch. Verify ability to restore data.

(3) Record results in [Table D-6](#).

(4) FAIL if unable to backup and restore system configuration.

This page intentionally left blank.

APPENDIX A. SYSTEM PERFORMANCE DATA TABLES

Table A-1. Combined Routing Results

Test Engineer:		Test Date (yyymmdd):					
Throughput Scenario	Routing						
Packet Size (Bytes)	%						
64							
128							
256							
512							
1024							
1280							
1518							
Latency Scenario	Latency						
Packet Size (Bytes)	Min Latency (μs)		Avg Latency (μs)		Max Latency (μs)		
64							
128							
256							
512							
1024							
1280							
1518							
Latency Distribution Scenario	Latency Distribution						
Packet Size (Bytes)	<= 10	<= 100	<= 500	<= 1000	<= 5000	<= 10000	> 50000
64							
128							
256							
512							
1024							
1280							
1518							
Comments:							

μs = microsecond

Table A-2. Edge-to-Edge Routing Results

Test Engineer:		Test Date (yyymmdd):					
Throughput Scenario	Routing EUB 1/Edge 1 to EUB 4.						
Packet Size (Bytes)	%						
64							
128							
256							
512							
1024							
1280							
1518							

Table A-2. Edge-to-Edge Routing Results (continued)

Latency Scenario							
Packet Size (Bytes)	Min Latency (μ s)		Avg Latency (μ s)		Max Latency (μ s)		
64							
128							
256							
512							
1024							
1280							
1518							
Latency Distribution Scenario							
Packet Size (Bytes)	\leq 10	\leq 100	\leq 500	\leq 1000	\leq 5000	\leq 10000	$>$ 50000
64							
128							
256							
512							
1024							
1280							
1518							
Comments:							

Table A-3. Edge-to-Edge Routing Results

Test Engineer:		Test Date (yyymmdd):	
Throughput Scenario		Routing EUB1/Edge2 to EUB 3.	
Packet Size (Bytes)	%		
64			
128			
256			
512			
1024			
1280			
1518			
Latency Scenario			
Packet Size (Bytes)	Min Latency (μ s)	Avg Latency (μ s)	Max Latency (μ s)
64			
128			
256			
512			
1024			
1280			
1518			

Table A-3. Edge-to-Edge Routing Results (continued)

Latency Distribution Scenario							
Packet Size (Bytes)	<= 10	<= 100	<= 500	<= 1000	<= 5000	<= 10000	> 50000
64							
128							
256							
512							
1024							
1280							
1518							
Comments:							

Table A-4. Edge-to-Edge Routing Results

Test Engineer:	Test Date (yyymmdd):						
Throughput Scenario	Routing EUB 1/Edge 3 to EUB 2.						
Packet Size (Bytes)	%						
64							
128							
256							
512							
1024							
1280							
1518							
Latency Scenario							
Packet Size (Bytes)	Min Latency (μs)	Avg Latency (μs)			Max Latency (μs)		
64							
128							
256							
512							
1024							
1280							
1518							
Latency Distribution Scenario							
Packet Size (Bytes)	<= 10	<= 100	<= 500	<= 1000	<= 5000	<= 10000	> 50000
64							
128							
256							
512							
1024							
1280							
1518							
Comments:							

Table A-5. Broadcast Distribution and Leak Results

Test Engineer:		Test Date (yymmdd):		
Broadcast Handling Capability	Pass / Fail			
	EUB 1/Edge 1 to EUB 4.	EUB 1/Edge 2 to EUB 3.	EUB 1/Edge 3 to EUB 2.	
Broadcast Distribution				
Broadcast Leak				
Comments:				

Table A-6. Combined Routing Results

Test Engineer:		Test Date (yymmdd):					
Throughput Scenario	Routing						
Packet Size (Bytes)	%						
64							
128							
256							
512							
1024							
1280							
1518							
Latency Scenario							
Packet Size (Bytes)	Min Latency (μs)		Avg Latency (μs)		Max Latency (μs)		
64							
128							
256							
512							
1024							
1280							
1518							
Latency Distribution Scenario							
Packet Size (Bytes)	<= 10	<= 100	<= 500	<= 1000	<= 5000	<= 10000	> 50000
64							
128							
256							
512							
1024							
1280							
1518							
Comments:							

Table A-7. VLAN Tagging, Bridging, and Routing Results

Test Engineer:		Test Date (yymmdd):					
Throughput Scenario	Bridging 100 Mbps	Routing 100 Mbps			Routing with ACLs 100 Mbps		
Packet Size (Bytes)	%	%			%		
64							
128							
256							
512							
1024							
1280							
1518							
Latency Scenario							
Packet Size (Bytes)	Latency (μs)	Latency (μs)			Latency (μs)		
64							
128							
256							
512							
1024							
1280							
1518							
Latency Distribution Scenario	Bridging 100 Mbps						
Packet Size (Bytes)	<=10	<=100	<=500	<=1000	<=5000	<=10000	> 50000
64							
128							
256							
512							
1024							
1280							
1518							
Latency Distribution Scenario	Routing 100 Mbps						
Packet Size (Bytes)	<=10	<=100	<=500	<=1000	<=5000	<=10000	> 50000
64							
128							
256							
512							
1024							
1280							

Table A-7. VLAN Tagging, Bridging, and Routing Results (continued)

1518							
Latency Distribution Scenario	Routing with ACLs 100 Mbps						
Packet Size (Bytes)	<=10	<=100	<=500	<=1000	<=5000	<=10000	> 50000
64							
128							
256							
512							
1024							
1280							
1518							
Comments:							

ACL = Access Control List

Table A-8. Multicast Performance

Test Engineer:				Test Date (yyymmdd):		
Mixed Class Throughput Multicast Only	Packet Size (Bytes)	Multicast Loss %	Mixed Class Throughput With Unicast	Packet Size (Bytes)	Multicast and Unicast	
					Multicast Loss %	Unicast Loss %
12 Groups @ 40% Load	64		12 Groups @ 10% Load	64		
	1408			1408		
	1518			1518		
12 Groups @ 60% Load	64		12 Groups @ 20% Load	64		
	1408			1408		
	1518			1518		
12 Groups @ 80% Load	64		12 Groups @ 30% Load	64		
	1408			1408		
	1518			1518		
Mixed Class Throughput Multicast Only	Packet Size (Bytes)	Multicast Loss %	Mixed Class Throughput With Unicast	Packet Size (Bytes)	Multicast and Unicast	
					Multicast Loss %	Unicast Loss %
12 Groups @ 100% Load	64		12 Groups @ 40% Load	64		
	1408			1408		
	1518			1518		
			12 Groups @ 50% Load	64		
				1408		
				1518		
Scaled Group Forwarding	Packet Size (Bytes)	Loss %				
8 Groups, 40% Load	64					
	1408					
	1518					
8 Groups, 60% Load	64					
	1408					
	1518					
8 Groups, 80% Load	64					
	1408					
	1518					

Table A-8. Multicast Performance (continued)

8 Groups, 100% Load	64			
	1408			
	1518			
	1408			
	1518			
16 Groups, 60% Load	64			
	1408			
	1518			
16 Groups, 80% Load	1408			
	1518			
16 Groups, 100% Load	64			
	1408			
	1518			
24 Groups, 40% Load	64			
	1408			
	1518			
24 Groups, 60% Load	64			
	1408			
	1518			
24 Groups, 80% Load	64			
	1408			
	1518			
24 Groups, 100% Load	64			
	1408			
	1518			
32 Groups, 40% Load	64			
	1408			
	1518			
32 Groups, 60% Load	64			
	1408			
	1518			
32 Groups, 80% Load	64			
	1408			
	1518			
32 Groups, 100% Load	64			
	1408			
	1518			
Forwarding Latency Multicast Only	Packet Size (Bytes)	Minimum (μs)	Average (μs)	Maximum (μs)
1 Group, 100 % Load	64			
	1408			
	1518			
Maximum Group Capacity	Packet Size (Bytes)	Groups	Frame Loss	
10 % Load	64			
Comments:				

This page intentionally left blank.

APPENDIX B. SYSTEM FUNCTIONALITY DATA TABLE

Tables B-1 through B-7 present the system functionality data. The following abbreviations may be used in the system testing results:

- NA – Not applicable to the test configuration.
- NT – Not tested due to lack of time.
- NF – Not tested because this test is directly dependent on the results of another test that failed functionality or reliance.
- TD – Technical difficulty in the test platform.

Table B-1. File Transfer Protocol (FTP) Series Results

Test Engineer:		Test Date (yymmdd):		
Tests	Bandwidth (Mbps)			
	5-VLAN	30-Subnet L3 at Edge	6-Subnet	
FTP Series 1 - Network Tier 1				
120 Simulated Users				
240 Simulated Users				
480 Simulated Users				
FTP Series 2 - Network Tier 2				
120 Simulated Users				
240 Simulated Users				
480 Simulated Users				
FTP Series 3 - Network Tier 3				
300 Simulated Users				
600 Simulated Users				
1200 Simulated Users				
Comments:				

Mbps = megabits per second; VLAN = virtual local area network; L3 = Layer 3

Table B-2. Overnight Results

Test Engineer:			Test Date (yyymmdd):			
Tests	5-VLAN		30-Subnet L3 at Edge		6-Subnet	
	Transactions	Time-outs	Transactions	Time-outs	Transactions	Time-outs
Single Type Traffic						
HTTP Pulse						
WWW 1-hour Soak						
FTP Get/Put 1-hour Soak						
E-mail 1-hour Soak						
SQL						
Mix Type Traffic						
WWW Mix						
FTP Mix						
E-mail Mix						
Multicast Mix						
Comments: All tests performed as expected. The 1-hour FTP Soak generates timeouts since it is designed to exceed the core link capacity.						

HTTP = Hypertext Transfer Protocol; WWW = World Wide Web; SQL = structured query language

Table B-3. Network Recovery Results

Test Engineer:			Test Date (yyymmdd):			
Network Recovery			5-VLAN	30-Subnet L3 at Edge	6-Subnet	
L3 redundancy	Device Failure	unicast				
		multicast				
	Link Failure	unicast				
		multicast				
Edge device uplink redundancy	Device Failure	unicast				
		multicast				
	Link Failure	unicast				
		multicast				
Comments:						

Table B-4. Progressive Multicast Results

Test Engineer:		Test Date (yyymmdd):		
Progressive Multicast		Percentage of Traffic Lost		
Senders (Multicast Streams)	Receivers (6 per sender)	5-VLAN	30-Subnet L3 at Edge	6-Subnet
1	6			
6	36			
12	72			
18	126			
24	144			
30	180			
Comments:				

Table B-5. Channel Surf Results

Test Engineer:		Test Date (yyymmdd):		
Channel Surf + Channel Stability	5-VLAN	30-Subnet L3 at Edge	6-Subnet	
Average Packets receives				
Comments:				

Table B-6. Multicast One-to-Many Results

Test Engineer:		Test Date (yyymmdd):		
Commanders Briefing	5-VLAN	30-Subnet L3 at Edge	6-Subnet	
1. Traffic consistency				
Comments:				

This page intentionally left blank.

APPENDIX C. NETWORK MANAGEMENT DATA TABLES

Table C-1. Telnet Results

Test Engineer:		Test Date (yyymmdd):		
SNMP Management		Pass/Fail		
Device Under Test		Core Switch		Edge Device
DEVICE NAME				
Telnet Session from Solaris Platform				
Telnet Session from Windows NT Platform				
Telnet Session from Linux Platform				
Problems Encountered:				
Findings and Observations:				
Engineer's Comments:				

SNMP = Simple Network Management Protocol

Table C-2. SNMP MIB Walk Results

Test Engineer:		Test Date (yyymmdd):		
SNMP Management		Pass/Fail		
Device Under Test		Core Switch		Edge Device
DEVICE NAME				
MIB-II				
RMON (RFC 1757)				
Vendor MIB				
Problems Encountered:				
Findings and Observations:				
Engineer's Comments:				

MIB = Management Information Base; RMON = remote network monitoring

Table C-3. SNMP SET/GET Requests Results

Test Engineer:		Test Date (yyymmdd):		
SNMP Management		Pass/Fail		
Device Under Test		Core Switch		Edge Device
DEVICE NAME				
Location SET Request				
Location GET Request				
SNMP Index, to "down"				
SNMP Index, to "up"				
Problems Encountered:				
Findings and Observations:				
Engineer's Comments:				

Table C-4. SNMP Traps Results

Test Engineer:		Test Date (yyymmdd):		
SNMP Management		Pass/Fail		
Device Under Test		Core Switch		Edge Device
DEVICE NAME				
Cold Start				
Warm Start				
Link Down				
Link Up				
Problems Encountered:				
Findings and Observations:				
Engineer's Comments:				

Table C-5. SNMP Security Results

Test Engineer:		Test Date (yyymmdd):		
SNMP Management		Pass/Fail		
Device Under Test		Core Switch		Edge Device
DEVICE NAME				
Read-only Community Failure				
1 st GET Request				
Invalid Community Authentication Failure				
2 nd GET Request				
3 rd (Access List Change) GET Request				
Problems Encountered:				
Findings and Observations:				
Engineer's Comments:				

Table C-6. Network Element Configuration Results

Test Engineer:		Test Date (yyymmdd):		
SNMP Management		Pass/Fail		
Device Under Test		Core Switch		Edge Device
DEVICE NAME				
Network Element Monitoring				
Problems Encountered:				
Findings and Observations:				
Engineer's Comments:				

Table C-7. Port VLAN Identifier Results

Test Engineer:		Test Date (yyymmdd):	
SNMP Management		Pass/Fail	
Device Under Test		Core Switch	Edge Device
DEVICE NAME			
Port VLAN Identifier			
Problems Encountered:			
Findings and Observations:			
Engineer's Comments:			

VLAN = virtual local area network

Table C-8. Device Performance Monitoring Results

Test Engineer:		Test Date (yyymmdd):	
SNMP Management		Pass/Fail	
Device Under Test		Core Switch	Edge Device
DEVICE NAME			
Device Performance Monitoring			
Problems Encountered:			
Findings and Observations:			
Engineer's Comments:			

Table C-9. Network VLAN Configuration Results

Test Engineer:		Test Date (yyymmdd):	
Element Manager		Pass/Fail	
System Under Test			
System Name			
VLAN Configuration			
VLAN Isolation			
Problems Encountered:			
Findings and Observations:			
Engineer's Comments:			

This page intentionally left blank.

APPENDIX D. SECURITY DATA TABLES

Table D-1. Audit Results

Source Document Paragraph	Operational Requirements	Capable?				
Audit NCSC-TG-005 (2.2.2.2)	Does the product export audit logs to a centralized audit management station for analysis?					
	Is the product capable of auditing all administrative actions?					
	Does the product's audit mechanism selectively audit any security related product event?					
	Does the product allow local or remote network auditing by the system administrator (SA)?					
	Does the product record connection attempts rejected by the product's access control rules? (An unauthorized Internet Protocol [IP] address trying to connect.)					
	Does the product: <ul style="list-style-type: none"> • Create audit trail data? • Maintain audit trail data? • Protect audit trail data from modification? • Protect audit trail data from unauthorized access? • Protect audit trail data from destruction? 					
	Does the product's audit mechanism format reports in useful, human-readable form?					
	Does the product log date, time, source address, destination address, and session oriented event (e.g., FTP get, FTP put, FTP cd, HTTP, Telnet UID and Password)?					

FTP = File Transfer Protocol; HTTP = Hypertext Transfer Protocol; UID = User Identifier

Table D-2. Configuration Management Secure Remote Management

Source Document Paragraph	Operational Requirements	Capable?				
Other Security Services NCSC-TG-005 (9.3.1)	Does the product demonstrate full session confidentiality through, for example, negotiation of key exchange, secure tunneling, signature verification or encryption algorithms?					
	Does the product demonstrate full session integrity enforced through key exchange, secure tunneling, signature verification, and/or encryption algorithms?					
	Can the SA select the security measures to ensure protection of the management link? (key exchange, tunneling, signature verification, and encryption)					
	Does the product secure the connection before transmission across an untrusted (internal or external) network?					
	Does the product allow remote administration only from selected IP addresses?					
ISO/IEC 15408-1:19999(E) paragraph 4.3.3 IT Security Requirements	Do remote managers have the ability to view logs and reports, configure filters, and receive alerts the same as local managers?					
	Does the product provide the option to be managed by Simple Network Management Protocol/Common Management Informational Protocol (SNMP/CMIP)?					
	Is the product configurable to restrict product management to administrators that are co-located with and/or directly connected to the product?					
System Integrity NCSC-TG-005 (2.2.3.1.2)	Does the product provide hardware and/or software features that can periodically validate the correct operation of the on-site hardware and firmware elements of the product?					
ISO/IEC 15408-1:19999(E) paragraph 4.3.3 IT Security Requirements	Can the device be managed remotely (e.g. web-based, Telnet, FTP)?					

Table D-3. Product Integrity/Assurance Results

Source Document Paragraph	Operational Requirements	Capable?				
(AR 380-19, 2-15i)	Does the product set password aging and is it configurable?					
I&A NCSC-TG-005 (2.2.2.1).	Does the product protect the passwords of the product using a mechanism that meets C2 requirements for data protection (shadow passwords, passwords stored in an encrypted format)?					
	Will the management device limit the number of log-on attempts and set a timeout limit on a password attempt?					

Table D-4. Network Based Attack Detection Results

Source Document Paragraph	Operational Requirements	Capable?				
	Is the product capable of detecting: <ul style="list-style-type: none"> • Threat profiles (i.e. port scans, ping attacks, etc.)? • User Datagram Protocol (UDP) port scans? • Transmission Control Protocol (TCP) port scans? • Ping attacks? • Synchronization (SYN) attacks? • IP spoofing attacks? • Ping of death? • Security Administrator Tool for Analyzing Networks (SATAN) attacks? • Information system security (ISS) attacks? 					
	Does the product have the ability to react to detected network based attacks?					
	Is the reaction predefined, site configurable and/or selectable?					
	Can the administrator add or configure predefined intrusion events on which to alert?					
	Does the product have the capability to select the events on which to alert or take action?					

Table D-4. Network Based Attack Detection Results (continued)

Source Document Paragraph	Operational Requirements	Capable?				
	Does the product react to the detected intrusion as established by the administrator so that pre-determined actions take place? (Trigger an audible alarm, page or send e-mail to administrator(s), initiate SNMP traps, set up a blind alley, break a network connection, perform special additional auditing, or perform an automatic trace.)					
	Does the product provide at least one 'under attack' administrator alert? (Several types of configurable alert mechanisms are desired; simple screen flashing, e-mail to administrators, paging alert to administrators.)					
	Does the product give the SA suggested instructions for handling intrusions?					
NCSC-TG-005	Does the product have the ability to react to unauthorized login attempts?					
	Is the reaction predefined, site configurable, and/or selectable?					

Table D-5. Access Control Filter Results

Source Document Paragraph	Operational Requirements	Cap able?				
ISO/IEC 15408-1:19999(E) paragraph 4.3.3 IT Security Requirements	Does the product support association of filters to a particular interface/port?					
NCSC-TG-005	Does the product perform packet filtering/stateful inspection/proxy on: <ul style="list-style-type: none"> • IP Source Address? • IP Destination Addresses? • Protocol? • TCP Source Port? • TCP Destination Port? • The Source Interface? • The Destination Interface? 					
	Does the product allow combining filters to form an aggregate filter of very narrow focus?					
	Does the product support reconfiguration of the rules set without taking the product out of service?					
	Does the product allow viewing of filters during operation?					

Table D-5. Access Control Filter Results (continued)

Source Document Paragraph	Operational Requirements	Capable?				
	Does the product provide syntax error checking before implementing an access control list (ACL)?					
	Does the product provide conflicting rules checking before implementing an ACL?					

Table D-6. Backup/Redundancy Results

Source Document Paragraph	Operational Requirements	Capable?				
ISO/IEC 15408-1:19999(E) paragraph 4.3.3 IT Security Requirements	Does the product have the capability to backup and restore the system configuration?					

This page intentionally left blank.

APPENDIX E. SMARTBITS CONFIGURATION

The main test equipment used for the performance portion of this evaluation plan is Spirent Communications SmartBits network performance analyzer. The following sections describe the SmartBits software and hardware that is used for the Layer 3 evaluations.

E-1.0 APPLICATIONS

The following SmartBits applications are used in the performance portion of the evaluation.

a. **Advanced Switch Tests (AST):** Version 2.10. AST is Spirent Communications' first generation of Advanced Switch tests.

b. **Advanced Switch Tests II (AST II):** Version 2.10. AST II is Spirent Communications' second generation of Advanced Switch tests. Based on RFC 2285 and the Internet Engineering Task Force (IETF) Switch Methodology Draft, AST II provides the TRUE first-level benchmark for all switches. AST II tests include Forwarding, Congestion Control, Address Learning Rate, Address Caching, Error Filtering, Broadcast Forwarding, Broadcast Latency, and Forward Pressure.

c. **SmartMulticastIP:** Version 1.26. Measures IP multicast performance of routers and switches. Designed for network managers, network equipment manufacturers, Internet Service Providers (ISPs), and carriers. Used to perform a comparative analysis of IP multicast devices, to evaluate key performance parameters of IP multicast devices under typical or extreme traffic load conditions, and to re-qualify IP multicast devices after firmware upgrades.

d. **SmartWindow:** Version 7.37. SmartBits™ virtual front panel. Allows the user to access SmartBits™ equipment with greater test control than a pre-programmed application. Used to verify design, improve product quality, perform low-volume production and repair testing, and perform competitive marketing analysis. Within SmartWindow, simply select a protocol, set class of service parameters, and then test any of the following: network interface cards (NICs), servers, bridges, cable modems, xDSL modems, switches, routers, virtual local area networks (VLANs), firewalls, live networks, or multimedia scenarios.

e. **SmartFlow:** Version 1.51. Tests line rate Quality of Service (QoS). Enables both forwarding and policy tests. Analyzes each incoming stream to test a device's (or network's) ability to forward very large numbers of flows. Analyzes the device's ability to correctly handle policies implemented in the network or device under test.

f. **SmartApplications:** Version 2.41. Provides automated performance analysis for bridges, switches, and routers per RFC 1242, Benchmarking Terminology for Network Interconnection Devices and RFC 2544, Benchmarking Methodology for Network Interconnect Devices.

E-2.0 TERMS

The following descriptions explain how common terms are defined when using SmartFlow.

a. **Throughput:** The Throughput test determines the maximum transmission rate at which the device under test (DUT) can forward IP traffic with no frame loss, or at a user-specified acceptable frame loss. By increasing the transmission rate at specified levels, you can determine the DUT's capacity. SmartFlow calculates frame loss as:

$$\text{Frame Loss} = \text{Number of Frames Transmitted} - \text{Number of Frames Received}$$

b. **Frame Loss:** The Frame Loss test measures the percentage of frames lost by the DUT that should have been forwarded. This test is used to determine a DUT's ability to deliver frames in a sequenced flow of streams with specific routing priorities and at a stepped percentage of the wire rate.

$$\text{Frame Loss} = \text{Number of Frames Transmitted} - \text{Number of Frames Received}$$

c. **Latency Test:** The Latency test is used to measure latency above and below the load percentage at which the DUT drops frames. It calculates the minimum, maximum and average latency at different loads. Latency is defined as the length of time it takes a DUT to forward a packet from one SmartBits port to another SmartBits port. The Latency test measures latency for received frames only.

$$\text{Latency} = \text{Receive Timestamp} - \text{Transmit Timestamp}$$

d. **Latency Distribution Test:** The Latency Distribution test measures the latency of each frame on a frame-by-frame basis and places latency results into eight time buckets. SmartFlow reads the time the sending SmartBits port sent the frame (Transmit Timestamp), and the time the receiving SmartBits recognizes the trigger frame, which is the Receive Timestamp. This test uses the specified test duration, a starting percentage load (based on the wire rate), a step percentage by which to increase the load during the test, and a stop percentage at which the test ends. During the test, these three values determine the duration for which the DUT is tested at a specified load. Note: Latency values are for the frames that were not dropped.

$$\text{Latency} = \text{Receive Timestamp} - \text{Transmit Timestamp}$$

e. **Jumbo Test:** The Jumbo test is a combination of the Latency, Latency Distribution, and Frame Loss tests. It also measures latency variation (standard deviation) in addition to frame loss, latency, latency distribution, and sequencing. Note: The Jumbo test updates all types of results in each test (except Latency Snapshot and Throughput) simultaneously.

E-3.0 HARDWARE

Table E-1 lists the SmartBits hardware used in the lab. There are six SMB 6000B chassis fully loaded with 12 each 3201A/B GbE modules. There are two SMB 2000/SMB 10 chassis fully loaded with 10/100 and GbE modules.

Table E-1. SmartBits Hardware

Device Model/Name	Hardware Version	Software Version	Remarks
SmartBits 6000B	SMB 6000B	1.20.004	
SmartBits LAN-3201A SmartMetrics Gigabit Ethernet Module	LAN-3201A	2.10.009	Also known as the LAN-6201A/B
SmartBits 2000 Chassis	SMB 2000	6.69.001	
SmartBits ML-7710 SmartMetrics Card	ML-7710	2.30.001	
SmartBits GX-1405B Gigabit Ethernet Card	GX-1405B	2.30.001	

APPENDIX F. VENDOR INFORMATION

F-1.0 DEVICE UNDER TEST (DUT) REQUIREMENT

Table F-1 identifies the number of devices required from each vendor for this evaluation. This evaluation only addresses single-vendor solutions. The four evaluation categories are performed concurrently to keep test time to a minimum. Vendors must submit the minimum number of devices in order to participate in this evaluation. Due to time constraints, we request vendors submit only one type of core switch, one chassis-based edge device, and one stackable edge device.

Table F-1. Device Requirements

Evaluation Category	Remarks	Core Switch Qty	Building Switch Qty	Edge Device Qty
Performance/ System Functionality	Six edge devices are required for these portions of the evaluation. Each edge device will have a minimum of twenty-four 10/100-Mbps ports and two 1-gigabit SX ports. Four core switches are required for the System Functionality portion of the evaluation. Each core switch will have a minimum of eight 1-gigabit SX ports and dual fabric/processor/power supply.	4	2	6
Network Management	The Network Management portion of the evaluation will use the System Functionality test network. No additional core switches or edge devices are required for this evaluation category. A complete management software package capable of managing all the above devices including VLAN configuration support is required.	N/A	N/A	N/A
Security	One core switch and one edge device are required for the Security portion of the evaluation. Security level tests require a minimum of twenty-four 10/100-Mbps ports.	1	1	1
Total Devices Required from Vendor		5	3	7

Mbps = Megabits per second; VLAN = virtual local area network

F-2.0 CONTACT INFORMATION

Technology Integration Center (TIC) Test Director: Mark Beattie, (520) 533-2807, BeattieM@hqisec.army.mil

Integration Lead Test Engineer: Jordan Silk, (520) 533-7218, silkj@hqisec.army.mil

F-4.2 Shipping Address

The shipping address for equipment to be tested is as follows:

Commander, USAISEC
Technology Integration Center
ATTN: AMSEL-IE-TI (Mark McFadden)
Building 53302
Fort Huachuca, AZ 85613-5300
(520) 533-2690

F-4.3 Laboratory Access

Normal laboratory hours are from 0800 to 1700 hours, Monday through Friday, excluding holidays. Under TIC supervision, vendors are permitted onsite during the evaluation and are expected to perform the setup and configuration of their products.

F-4.4 Vendor Guidelines

The TIC will notify vendors considered for product evaluation and provide them with a copy of this test plan and their proposed test schedule. The TIC must receive vendor responses no later than the specified response cutoff date. Equipment is tested as submitted; code and equipment revisions or substitutions are not permitted once testing begins. All equipment evaluated must be commercially available for purchase on the date tested. Beta versions of code or hardware are not permitted. Vendors are expected to provide the TIC with the following items no later than 1 week prior to the beginning of the scheduled test period:

- a. A technical point of contact available for support and assistance during the evaluation.
- b. Current documentation or detailed instructions concerning the setup, configuration, and operation for each device submitted.
- c. An itemized list of all equipment submitted for test. This listing must include (as applicable) the model name/number, serial number, hardware version, firmware version, software version, and number of units for each chassis and plug-in processing and interface card/module submitted for test.

F-5.0 EVALUATION PLAN REVISIONS

The TIC reserves the right to modify this evaluation plan at any time.

APPENDIX G. SYSTEM FUNCTIONALITY TEST CONFIGURATION

G-1.0 NETWORK PERFORMANCE TOOLS

There are two ways to generate traffic over the test network, using remote terminal emulations (RTEs) or using Chariot.

G-1.1 RTE

The RTE is the primary means for this integrated system test. It is a combination hardware/software platform consisting of Intel Pentium-based personal computers (PCs) running the Red Hat Linux operating system and specialized application software developed by Neal Nelson and Associates. This platform makes practical the capability to mimic thousands of typical Internet users exchanging real world information with each other and pulling files from the built in Linux Apache file servers. The RTE logs the results of these tests as transaction completion counts and time statistics. At the end of the test, the RTE performs post processing of the logs and generates customized reports designed for the specific evaluation. The RTE has many capabilities that are not used in this evaluation.

The RTE generates File Transfer Protocol (FTP) Puts, FTP Gets, World Wide Web (WWW), Telnet, rlogin, multicast streaming, and Simple Mail Transfer Protocol (SMTP) traffic for the test network. The only non-test traffic placed on the test network is usually Simple Network Management Protocol (SNMP), ping, and trace-routes which are for troubleshooting and are not significant enough to skew the test results to any noticeable degree due to the granularity set for the test data accumulation. There are 72 Ethernet connections from 36 RTE computers to the test network edge devices, with the 2 network interface card (NIC) connections on each computer labeled as B-local area network (LAN) and C-LAN. Both are fixed at 100 megabits per second (Mbps), full duplex to help avoid hardware interface issues. Static routing is programmed into the RTEs to control and track the traffic on each NIC. In the unicast traffic programs, the simulated users are evenly distributed across the RTE computers. Most of the unicast tests consist of 70 users per computer across 36 computers for a total of 2,520 functionally identical users that exchange traffic with each other and/or with the 36 Apache servers (across 36 computers). The RTE test traffic programs are set to run in tight loops with essentially no "think delays" between transaction commands.

G-1.2 Chariot

The Technology Integration Center (TIC) also performs secondary testing using the commercially proven Chariot network performance tool from NetIQ (formally Ganymede). Like the RTE, this tool simulates real world traffic using a specialized application program called an endpoint. The endpoint software resides on all computers that are designated to generate test traffic under the control of the Chariot console. The endpoint software is a Layer 7 (L7) application that uses the Transmission Control Protocol/Internet Protocol (TCP/IP) stack within the hardware/operating system platform for which it is installed. The RTE computers are used as the endpoint stations and are dual bootable to either the Linux or Windows 2000 Server operating system on which the endpoint program can reside. The computers can be loaded with any mixture of Linux and Windows 2000 combinations, as the Chariot Console makes no differentiation except to capture information on the particular operating system that each of its endpoints are operating under for logging purposes. The endpoint software has the capability to stuff its packets with compressible and non-

compressible patterns, canned and customized test files that Chariot can use to compare for bit integrity. The Chariot scripts written for this evaluation are similar to but generally shorter in duration than the RTE test programs and are generally performed as needed to provide a “second opinion.” The Chariot Console computer coordinates and receives statistics from the endpoints through an administration network that is independent of the test network. This eliminates having to use the test network to transfer the endpoints statistics to the Chariot Console for evaluation because it would interfere with the tests.

G-2.0 NETWORK CONFIGURATION

Figures G-1 through G-3 show the System Functionality test network. This test network models the I3MP without lateral links between area distribution nodes (ADNs). These lateral links were removed in the test network to increase traffic through the main communication nodes (MCNs) without modifying open shortest path first (OSPF) cost on each link. The top-down architecture of the I3MP network is segregated into three physical tiers as shown on the left side of the figures. Tier 3 consists of the backbone system where most Layer 3 (L3) inter-installation traffic and incoming/outgoing Internet traffic is switched or routed with full redundancy. Tier 2 is a Layer 2 (L2) and L3 hybrid that handles most of the end-user building (EUB) link redundancy and augments the backbone for inter-installation traffic. Tier 1 is also L2 and L3 capable and consists of the installation tenants and EUB devices.

Two logical networks, a 6-subnet (Figures G-1 and G-2) using an untagged virtual local area network (VLAN) network and a 6-VLAN (Figure G-3) using VLAN tagging, are individually tested against identical physical architectures. The ADNs and MCNs are referred to as the core of the network. In both logical networks, the ADNs are the gateway for each VLAN or subnet. We assume that the link between the two MCNs normally serves no function other than to act as a backup in case the MCN A to ADN 2 link and the MCN B to ADN 1 links both fail. The test network conforms to the following parameters for all of the tests in this appendix regardless of whether or not they are a function of a particular test:

- OSPF routing.
- OSPF equal-cost multi-path (generally applies to 6-subnet only).
- PIM-DM (preferred) or DVMRP.
- OSPF area set to anything other than 0.
- Passwords are not necessary.
- Telnet access is activated on all devices.
- VLANs are implemented with 802.1Q.
- PIM is assigned to all core links if possible.
- IGMP version 2 snooping is enabled on edge devices.
- Untagged VLANs (if used) on all end user ports.
- Spanning tree disabled where possible.
- No flow control on any port.
- End user ports are fixed at 100 Mbps, full duplex.
- The defined Gateway IP addresses must be used.

- No QoS structures defined.
- No proprietary “tweaks” are allowed; tuning for performance is okay.

The IP address scheme for the RTE to edge device connections is located in Table G-1.

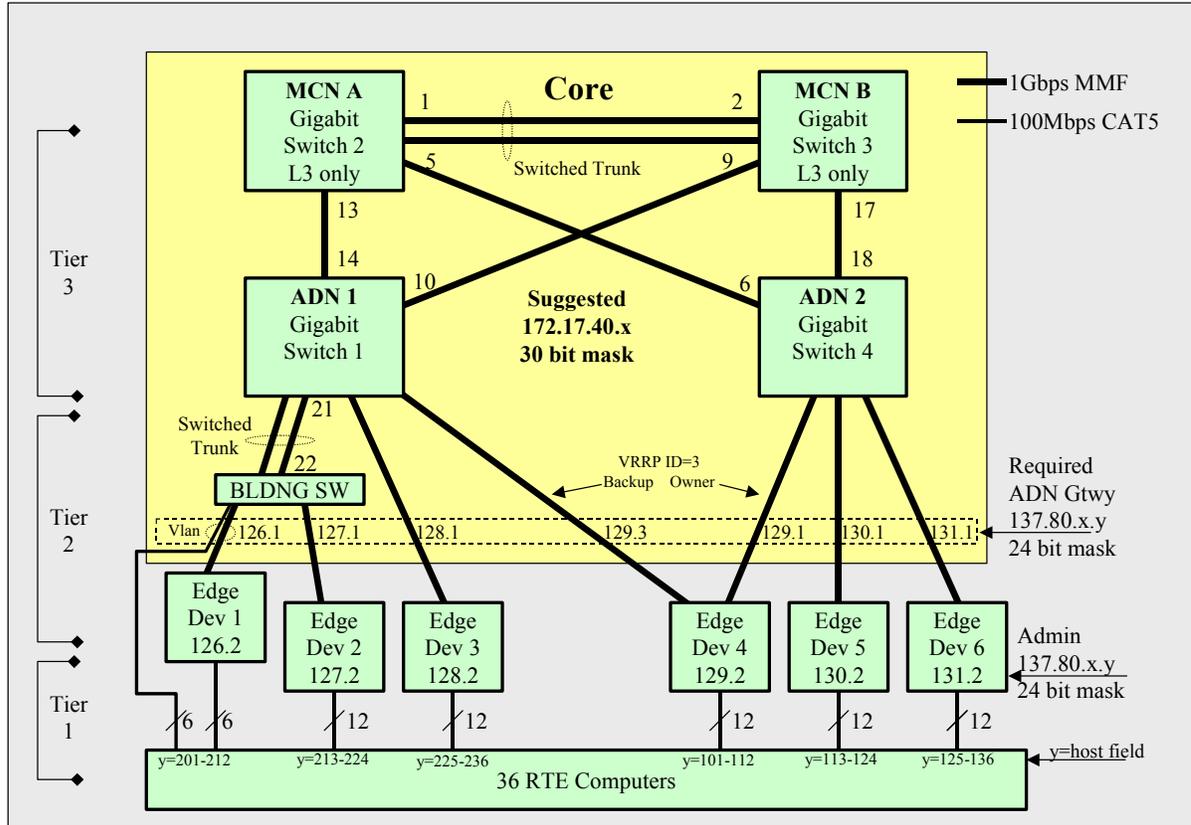


Figure G-1. 6-Subnet Configuration with L3 Building Switch and L2 at Tier 1

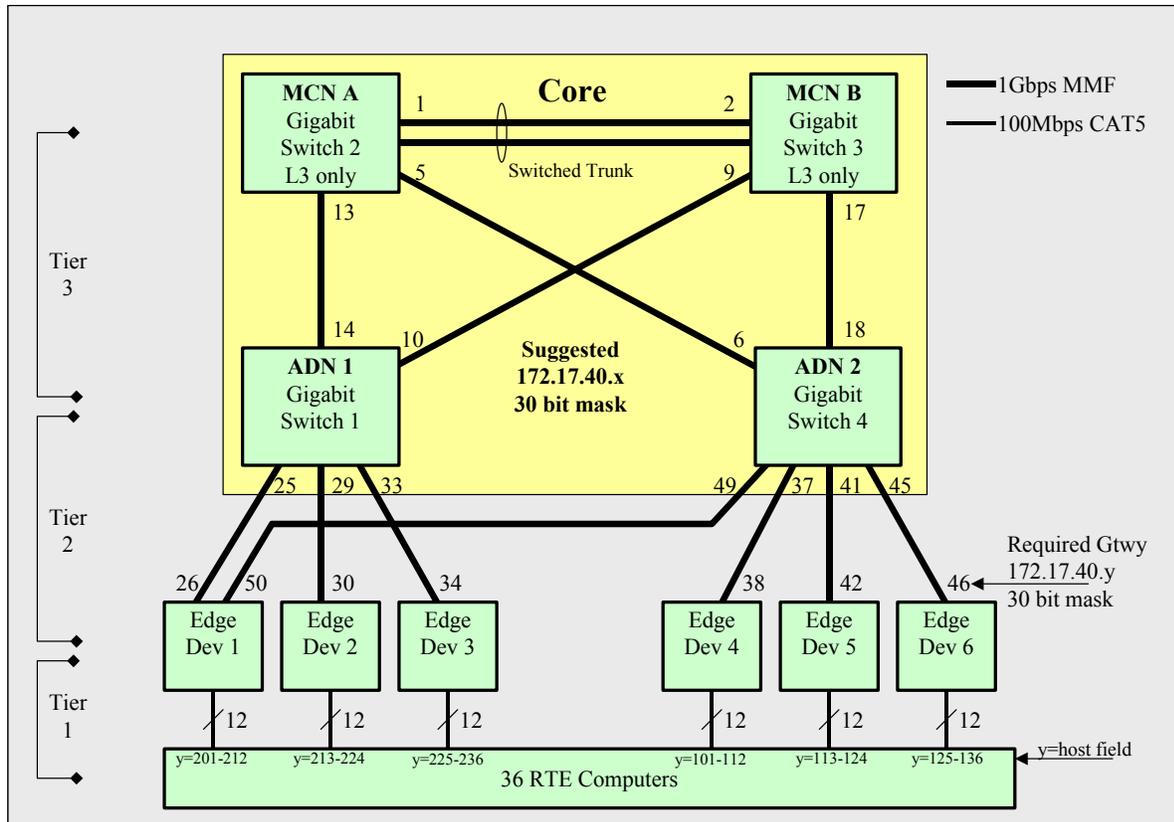


Figure G-2. 6-Subnet Configuration with L3 at Tier 1

G-2.1 6-Subnet

This flat VLAN architecture network follows the physical network architecture where each of the six edge devices is entirely in its own subnet. This test is designed to show basic unicast and multicast functions of the vendor equipment used in a straightforward design and is usually the first test we conduct. This test has two iterations which Figures G-1 and G-2 illustrate. In Figure G-1, the ADNs act as the L3 gateway for each edge device, while in Figure G-2 the edge devices become, if possible, the L3 gateways. In both iterations, the L3 routing allows deactivation of the spanning tree protocol, and open shortest path first (OSPF) equal cost multi-path provides the necessary core device and link redundancy. Although this is not a performance test, the network allows some of the RTE test programs to run at its maximum rate while other tests are regulated to operate at a specific rate. The results of these tests are then compared to a baseline established as a reference. The test is evaluated through this comparison in conjunction with a consistent traffic flow and equal service with all users.

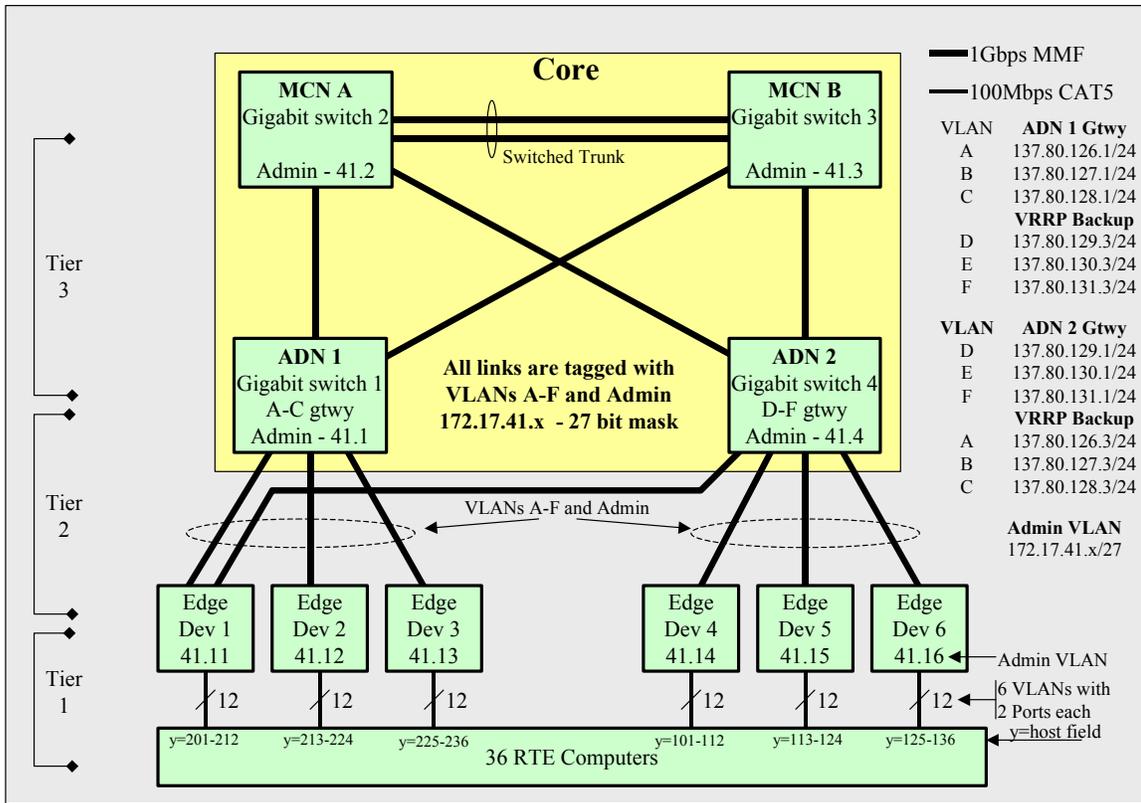


Figure G-3. 6-VLAN Configuration and VLAN Logical Flow

G-2.2 6-VLAN

This configuration is designed to stress tagged VLANs and L3 functionality by routing packets multiple times through the core with L3 routing function redundancy on all VLANs. This is not a performance test, so throughput is not an issue. Rather, this test evaluates the robustness of L2 VLAN tagging and L3 routing functions of the core and edge devices. Spanning tree protocol generally is activated throughout the core links to prevent L2 traffic loops. The test results are not generally compared to any baseline as such, but are analyzed mainly for consistent throughput and equal service for all sessions, indicating functionality and reliance.

Six broadcast domains (RTE test VLANs) and an administration domain all appear at every edge device through the core using VLAN tagging. Figure G-4 is a logical diagram illustrating this concept; Figure G-3 shows how the VLANs map onto the physical network. With the RTE test VLAN L3 gateways located in the ADNs, the core is forced to route packets across the individual core links as many as three times (L21 - L3 - L22 - L3 - L23) before it reaches its destination. Generally, the preferred configuration of the gateways is such that each ADN owns four of the gateways and acts as backup for the other four gateways that are owned by the other ADN, which Figure G-4 illustrates. The ADNs act as backups for each other in case one of them fails. As a less preferred alternative, one ADN can own all eight gateways while the other acts as backup. Regardless of how the gateways are configured, the ADNs still provide L2 redundancy to the edge devices, which is demonstrated by the first edge device with its dual-homed links. We assume that the remaining edge devices will function in the same manner as the first if they also had redundant links. All edge devices are programmed identically with the exception of the

unique administration host IP address for the administration VLAN. At each edge device, with 12 Ethernet ports labeled as 1 through 12, port 1 and 7 are assigned untagged to the first RTE test VLAN, ports 2 and 8 to the second, and so on through the sixth.

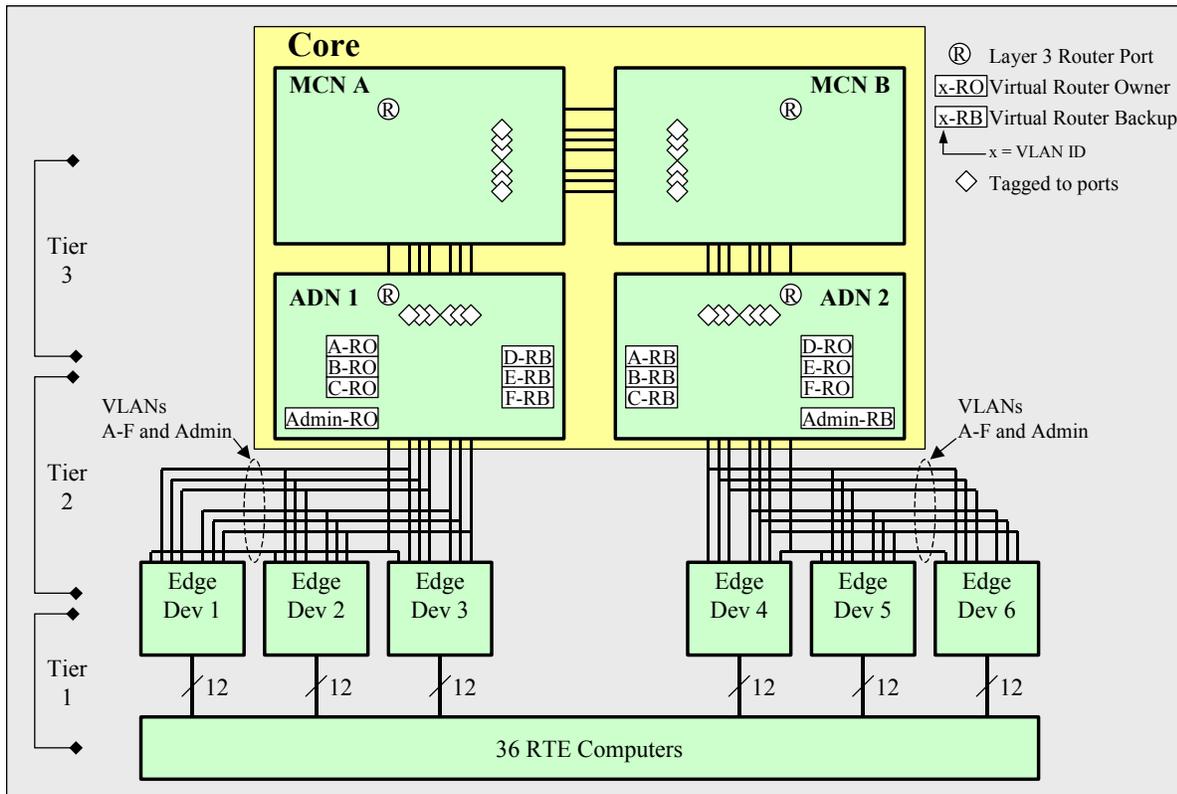


Figure G-4. 6-VLAN Logical Connections

The redundancy method used between the ADNs is usually implemented using an RFC standard such as Virtual Router Redundancy Protocol (VRRP); however, vendor specific solutions may be implemented if VRRP is not possible in the interest of showing progression towards using an RFC standard. The three VLANs, G, H, and I, provide L3 connectivity throughout the core for the six gateways while the Admin VLAN provides an independent management network. Spanning tree is turned on throughout the core and edge devices on all 10 VLANs to prevent L2 traffic loops. If possible, spanning tree priorities are implemented so that the four gateways assigned to each ADN has the best route to all edge devices. This is the suggested method to implementing L2 and L3 connectivity, but it can be implemented in some other method at the vendor's discretion.

H-2.3 Fail-over and Recovery

The fail-over implementation is such that any one link or MCN can fail without causing loss of core network access to any host. Also, a loss of an ADN does not deny core network access to any host of the remaining ADN. Although throughput performance is not a factor in this evaluation, the vendor is encouraged to load share traffic across the core links. It is more important, however, to maintain fail-over capability. In addition, the network manager must be able to Telnet to and manage all devices in this network at all times upon network fail-over states, recoveries, and during non-congestive traffic.

G-2.4 IP Addressing Scheme

Tables G-1 through G-4 show the IP addressing scheme used in the System Functionality test network.

Table G-1. RTE 201-236 IP Addressing 6-Subnet

RTE	IP Address	VLAN	Cable	Edge	RTE	IP Address	VLAN	Cable	Edge
s201b	137.80.126.101	Dflt	1	1-01	s201c	137.80.129.201	Dflt	37	4-12
s202c	137.80.126.102	Dflt	38	1-01	s202b	137.80.129.202	Dflt	2	4-11
s203b	137.80.126.103	Dflt	3	1-03	s203c	137.80.129.203	Dflt	39	4-10
s204c	137.80.126.104	Dflt	40	1-04	s204b	137.80.129.204	Dflt	4	4-09
s205b	137.80.126.105	Dflt	5	1-05	s205c	137.80.129.205	Dflt	41	4-08
s206c	137.80.126.106	Dflt	42	1-06	s206b	137.80.129.206	Dflt	6	4-07
s207b	137.80.126.107	Dflt	7	1-07	s207c	137.80.129.212	Dflt	43	4-06
s208c	137.80.126.108	Dflt	44	1-08	s208b	137.80.129.211	Dflt	8	4-05
s209b	137.80.126.109	Dflt	9	1-09	s209c	137.80.129.210	Dflt	45	4-04
s210c	137.80.126.110	Dflt	46	1-10	s210b	137.80.129.209	Dflt	10	4-03
s211b	137.80.126.111	Dflt	11	1-11	s211c	137.80.129.208	Dflt	47	4-02
s212c	137.80.126.112	Dflt	48	1-12	s212b	137.80.129.207	Dflt	12	4-01
s213b	137.80.127.113	Dflt	13	2-01	s213c	137.80.130.213	Dflt	49	5-12
s214c	137.80.127.114	Dflt	50	2-01	s214b	137.80.130.214	Dflt	14	5-11
s215b	137.80.127.115	Dflt	15	2-03	s215c	137.80.130.215	Dflt	51	5-10
s216c	137.80.127.116	Dflt	52	2-04	s216b	137.80.130.216	Dflt	16	5-09
s217b	137.80.127.117	Dflt	17	2-05	s217c	137.80.130.217	Dflt	53	5-08
s218c	137.80.127.118	Dflt	54	2-06	s218b	137.80.130.218	Dflt	18	5-07
s219b	137.80.127.119	Dflt	19	2-07	s219c	137.80.130.224	Dflt	55	5-06
s220c	137.80.127.120	Dflt	56	2-08	s220b	137.80.130.223	Dflt	20	5-05
s221b	137.80.127.121	Dflt	21	2-09	s221c	137.80.130.222	Dflt	57	5-04
s222c	137.80.127.122	Dflt	58	2-10	s222b	137.80.130.221	Dflt	22	5-03
s223b	137.80.127.123	Dflt	23	2-11	s223c	137.80.130.220	Dflt	59	5-02
s224c	137.80.127.124	Dflt	60	2-12	s224b	137.80.130.219	Dflt	24	5-01
s225b	137.80.128.125	Dflt	25	3-01	s225c	137.80.131.225	Dflt	61	6-12
s226c	137.80.128.126	Dflt	62	3-01	s226b	137.80.131.226	Dflt	26	6-11
s227b	137.80.128.127	Dflt	27	3-03	s227c	137.80.131.227	Dflt	63	6-10
s228c	137.80.128.128	Dflt	64	3-04	s228b	137.80.131.228	Dflt	28	6-09
s229b	137.80.128.129	Dflt	29	3-05	s229c	137.80.131.229	Dflt	65	6-08
s230c	137.80.128.130	Dflt	66	3-06	s230b	137.80.131.230	Dflt	30	6-07
s231b	137.80.128.131	Dflt	31	3-07	s231c	137.80.131.236	Dflt	67	6-06
s232c	137.80.128.132	Dflt	68	3-08	s232b	137.80.131.235	Dflt	32	6-05
s233b	137.80.128.133	Dflt	33	3-09	s233c	137.80.131.234	Dflt	69	6-04
s234c	137.80.128.134	Dflt	70	3-10	s234b	137.80.131.233	Dflt	34	6-03
s235b	137.80.128.125	Dflt	35	3-11	s235c	137.80.131.232	Dflt	71	6-02
s236c	137.80.128.136	Dflt	72	3-12	s236b	137.80.131.231	Dflt	36	6-01

Table G-2. RTE 201-236 IP Addressing 6-VLAN

RTE	IP Address	VLAN	Cable	Edge	RTE	IP Address	VLAN	Cable	Edge
s201b	137.80.126.101	2	1	1-01	s201c	137.80.131.201	7	37	4-12
s202c	137.80.127.102	3	38	1-01	s202b	137.80.130.202	6	2	4-11
s203b	137.80.128.103	4	3	1-03	s203c	137.80.129.203	5	39	4-10
s204c	137.80.129.104	5	40	1-04	s204b	137.80.128.204	4	4	4-09
s205b	137.80.130.105	6	5	1-05	s205c	137.80.127.205	3	41	4-08
s206c	137.80.131.106	7	42	1-06	s206b	137.80.126.206	2	6	4-07
s207b	137.80.126.107	2	7	1-07	s207c	137.80.131.207	7	43	4-06
s208c	137.80.127.108	3	44	1-08	s208b	137.80.130.208	6	8	4-05
s209b	137.80.128.109	4	9	1-09	s209c	137.80.129.209	5	45	4-04
s210c	137.80.129.110	5	46	1-10	s210b	137.80.128.210	4	10	4-03
s211b	137.80.130.111	6	11	1-11	s211c	137.80.127.211	3	47	4-02
s212c	137.80.131.112	7	48	1-12	s212b	137.80.126.212	2	12	4-01
s213b	137.80.126.113	2	13	2-01	s213c	137.80.131.213	7	49	5-12
s214c	137.80.127.114	3	50	2-01	s214b	137.80.130.214	6	14	5-11
s215b	137.80.128.115	4	15	2-03	s215c	137.80.129.215	5	51	5-10
s216c	137.80.129.116	5	52	2-04	s216b	137.80.128.216	4	16	5-09
s217b	137.80.130.117	6	17	2-05	s217c	137.80.127.217	3	53	5-08
s218c	137.80.131.118	7	54	2-06	s218b	137.80.126.218	2	18	5-07
s219b	137.80.126.119	2	19	2-07	s219c	137.80.131.219	7	55	5-06
s220c	137.80.127.120	3	56	2-08	s220b	137.80.130.220	6	20	5-05
s221b	137.80.128.121	4	21	2-09	s221c	137.80.129.221	5	57	5-04
s222c	137.80.129.122	5	58	2-10	s222b	137.80.128.222	4	22	5-03
s223b	137.80.130.123	6	23	2-11	s223c	137.80.127.223	3	59	5-02
s224c	137.80.131.124	7	60	2-12	s224b	137.80.126.224	2	24	5-01
s225b	137.80.126.125	2	25	3-01	s225c	137.80.131.225	7	61	6-12
s226c	137.80.127.126	3	62	3-01	s226b	137.80.130.226	6	26	6-11
s227b	137.80.128.127	4	27	3-03	s227c	137.80.129.227	5	63	6-10
s228c	137.80.129.128	5	64	3-04	s228b	137.80.128.228	4	28	6-09
s229b	137.80.130.129	6	29	3-05	s229c	137.80.127.229	3	65	6-08
s230c	137.80.131.130	7	66	3-06	s230b	137.80.126.230	2	30	6-07
s231b	137.80.126.131	2	31	3-07	s231c	137.80.131.231	7	67	6-06
s232c	137.80.127.132	3	68	3-08	s232b	137.80.130.232	6	32	6-05
s233b	137.80.128.133	4	33	3-09	s233c	137.80.129.233	5	69	6-04
s234c	137.80.129.134	5	70	3-10	s234b	137.80.128.234	4	34	6-03
s235b	137.80.130.125	6	35	3-11	s235c	137.80.127.235	3	71	6-02
s236c	137.80.131.136	7	72	3-12	s236b	137.80.126.236	2	36	6-01

Table G-3. RTE 201-236 IP Addressing 36-Subnet

RTE	IP Address	VLAN	Cable	Edge	RTE	IP Address	Cable	Edge
s201b	137.80.126.101	2	1	1-01	s201c	137.80.144.101	37	4-12
s202c	137.80.127.102	3	38	1-01	s202b	137.80.145.102	2	4-11
s203b	137.80.128.103	4	3	1-03	s203c	137.80.146.103	39	4-10
s204c	137.80.129.104	5	40	1-04	s204b	137.80.147.104	4	4-09
s205b	137.80.130.105	6	5	1-05	s205c	137.80.148.105	41	4-08
s206c	137.80.131.106	7	42	1-06	s206b	137.80.149.106	6	4-07
s207b	137.80.131.107	7	7	1-07	s207c	137.80.149.112	43	4-06
s208c	137.80.130.108	6	44	1-08	s208b	137.80.148.111	8	4-05
s209b	137.80.129.109	5	9	1-09	s209c	137.80.147.110	45	4-04
s210c	137.80.128.110	4	46	1-10	s210b	137.80.146.109	10	4-03
s211b	137.80.127.111	3	11	1-11	s211c	137.80.145.108	47	4-02
s212c	137.80.126.112	2	48	1-12	s212b	137.80.144.107	12	4-01
s213b	137.80.132.113	8	13	2-01	s213c	137.80.150.113	49	5-12
s214c	137.80.132.114	8	50	2-01	s214b	137.80.150.114	14	5-11
s215b	137.80.133.115	9	15	2-03	s215c	137.80.151.115	51	5-10
s216c	137.80.133.116	9	52	2-04	s216b	137.80.151.116	16	5-09
s217b	137.80.134.117	10	17	2-05	s217c	137.80.152.117	53	5-08
s218c	137.80.134.118	10	54	2-06	s218b	137.80.152.118	18	5-07
s219b	137.80.135.119	11	19	2-07	s219c	137.80.153.124	55	5-06
s220c	137.80.135.120	11	56	2-08	s220b	137.80.153.123	20	5-05
s221b	137.80.136.121	12	21	2-09	s221c	137.80.154.122	57	5-04
s222c	137.80.136.122	12	58	2-10	s222b	137.80.154.121	22	5-03
s223b	137.80.137.123	13	23	2-11	s223c	137.80.155.120	59	5-02
s224c	137.80.137.124	13	60	2-12	s224b	137.80.155.119	24	5-01
s225b	137.80.138.125	14	25	3-01	s225c	137.80.156.125	61	6-12
s226c	137.80.141.126	17	62	3-01	s226b	137.80.159.126	26	6-11
s227b	137.80.138.127	14	27	3-03	s227c	137.80.156.127	63	6-10
s228c	137.80.141.128	17	64	3-04	s228b	137.80.159.128	28	6-09
s229b	137.80.139.129	15	29	3-05	s229c	137.80.157.129	65	6-08
s230c	137.80.142.130	18	66	3-06	s230b	137.80.160.130	30	6-07
s231b	137.80.139.131	15	31	3-07	s231c	137.80.157.136	67	6-06
s232c	137.80.142.132	18	68	3-08	s232b	137.80.160.135	32	6-05
s233b	137.80.140.133	16	33	3-09	s233c	137.80.158.134	69	6-04
s234c	137.80.143.134	19	70	3-10	s234b	137.80.161.133	34	6-03
s235b	137.80.140.125	16	35	3-11	s235c	137.80.158.132	71	6-02
s236c	137.80.143.136	19	72	3-12	s236b	137.80.161.131	36	6-01

Table G-4. RTE Multicast Groups

Group #1		Group #2		Group #3		Group #4		Group #5		Group #6	
1	s211a	8	s212a	15	s223a	22	s224a	29	s235a	36	s236a
2	s201a	9	s203a	16	s205a	23	s207a	30	s209a	37	s211a
3	s202a	10	s204a	17	s206a	24	s208a	31	s210a	38	s212a
4	s213a	11	s215a	18	s217a	25	s219a	32	s221a	39	s223a
5	s214a	12	s216a	19	s218a	26	s220a	33	s222a	40	s224a
6	s225a	13	s227a	20	s229a	27	s231a	34	s233a	41	s234a
7	s226a	14	s228a	21	s230a	28	s232a	35	s236a	42	s235a
Group #7		Group #8		Group #9		Group #10		Group #11		Group #12	
43	s201a	50	s202a	57	s213a	64	s214a	71	s225a	78	s226a
44	s203a	51	s205a	58	s207a	65	s209a	72	s211a	79	s201a
45	s204a	52	s206a	59	s208a	66	s210a	73	s212a	80	s202a
46	s213a	53	s215a	60	s217a	67	s219a	74	s221a	81	s223a
47	s214a	54	s216a	61	s218a	68	s220a	75	s222a	82	s224a
48	s225a	55	s227a	62	s229a	69	s231a	76	s233a	83	s235a
49	s226a	56	s228a	63	s230a	70	s232a	77	s234a	84	s236a
Group #13		Group #14		Group #15		Group #16		Group #17		Group #18	
85	s203a	92	s204a	99	s215a	106	s216a	113	s227a	120	s228a
86	s204a	93	s203a	100	s207a	107	s209a	114	s211a	121	s201a
87	s205a	94	s206a	101	s208a	108	s210a	115	s212a	122	s202a
88	s213a	95	s215a	102	s217a	109	s219a	116	s221a	123	s223a
89	s214a	96	s216a	103	s218a	110	s220a	117	s222a	124	s224a
90	s225a	97	s227a	104	s229a	111	s229a	118	s233a	125	s235a
91	s226a	98	s228a	105	s230a	112	s232a	119	s234a	126	s236a
Group #19		Group #20		Group #21		Group #22		Group #23		Group #24	
127	s205a	134	s206a	141	s217a	148	s218a	155	s229a	162	s230a
128	s204a	135	s201a	142	s203a	149	s205a	156	s207a	163	s209a
129	s211a	136	s208a	143	s206a	150	s210a	157	s212a	164	s202a
130	s213a	137	s215a	144	s219a	151	s217a	158	s221a	165	s223a
131	s214a	138	s216a	145	s218a	152	s220a	159	s222a	166	s224a
132	s225a	139	s227a	146	s229a	153	s231a	160	s233a	167	s235a
133	s226a	140	s228a	147	s230a	154	s232a	161	s234a	168	s236a
Group #25		Group #26		Group #27		Group #28		Group #29		Group #30	
169	s207a	176	s208a	183	s221a	190	s222a	197	s231a	204	s232a
170	s204a	177	s201a	184	s203a	191	s205a	198	s207a	205	s202a
171	s211a	178	s206a	185	s204a	192	s210a	199	s212a	206	s209a
172	s213a	179	s215a	186	s217a	193	s219a	200	s221a	207	s223a
173	s214a	180	s216a	187	s218a	194	s220a	201	s222a	208	s224a
174	s225a	181	s227a	188	s229a	195	s231a	202	s233a	209	s235a
175	s226a	182	s228a	189	s230a	196	s232a	203	s234a	210	s236a
Group #31		Group #32		Group #33		Group #34		Group #35		Group #36	
211	s209a	218	s210a	225	s219a	232	s220a	239	s233a	246	s234a
212	s204a	219	s201a	226	s203a	233	s205a	240	s207a	247	s202a
213	s211a	220	s206a	227	s208a	234	s210a	241	s212a	248	s209a
214	s213a	221	s215a	228	s217a	235	s218a	242	s221a	249	s223a
215	s214a	222	s216a	229	s220a	236	s219a	243	s222a	250	s224a
216	s225a	223	s227a	230	s229a	237	s232a	244	s231a	251	s235a
217	s226a	224	s228a	231	s230a	238	s233a	245	s234a	252	s236a

GLOSSARY. ACRONYMS AND ABBREVIATIONS

ACL	Access Control List
ADN	Area Distribution Node
AR	Army Regulation
AST	Advanced Switch Tests
CLI	Command Line Interface
CMIP	Common Management Information Protocol
CUITN	Common User Installation Transport Network
DES	Data Encryption Standard
DOD	Department of Defense
DREC	Dynamic Receiver
DUT	device under test
DVRP	Distance Vector Multicast Routing Protocol
EUB	End User Building
FTP	File Transfer Protocol
GbE	Gigabit Ethernet
Gbps	gigabits per second
GIF	Graphic Interchange Format
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
I3MP	Installation Information Infrastructure Modernization Program
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IGMP	Internet Group Multicast Protocol
IOS	Internetworking Operating System
IP	Internet Protocol
ISO/IEC	International Standards Organization/International Electrotechnical Commission
ISP	Internet Service Provider
ISS	Information System Security, Internet Security Systems
IT	Information Technology
Kb	Kilobyte
L2	Layer 2
L3	Layer 3
L7	Layer 7
LAN	local area network

MB	Megabyte
Mbps	megabits per second
MCALC	Multicast Calculator
MCN	main communication node
MGEN	Multicast Generator
MIB	Management Information Base
MPEG	Motion Pictures Experts Group
μs	Microsecond
NAI	Network Associates Incorporated
NCSC-TG	National Computer Security Center - Technical Guidance
NIC	network interface card
NMS	Network Management Stations
OSPF	open shortest path first
PC	personal computer
PIM-DM	Protocol Independent Multicast-Dense Mode
PM, DDN	Product Manager, Defense Data Networks
PVID	Port VLAN Identifier
QoS	Quality of Service
RMON	Remote Network-Monitoring
RFC	request for comment
RTE	emote terminal emulation
SA	System Administrator
SATAN	Security Administrator Tool for Analyzing Networks
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SQL	structured query language
SSH	Secure Shell
SSL	Secure Socket Layer
SYN	Synchronization
TCP	Transmission Control Protocol
TIC	Technology Integration Center
UDP	User Datagram Protocol
UID	User Identifier
USAISEC	U. S. Army Information Systems Engineering Command
VLAN	virtual local area network

VRRP	Virtual Router Redundancy Protocol
WWW	World Wide Web

Filename: 03-002IntegrationEvaluation.doc
Directory: C:\Walrath\other files\CUITN docs\Finals for PDF
Template: C:\Documents and Settings\wml0221\Application
Data\Microsoft\Templates\Normal.dot
Title:
Subject:
Author: SilkJ
Keywords:
Comments:
Creation Date: 10/24/2002 8:00 AM
Change Number: 25
Last Saved On: 11/5/2002 12:38 PM
Last Saved By: Delle Lambert
Total Editing Time: 1,528 Minutes
Last Printed On: 11/21/2002 10:42 AM
As of Last Complete Printing
Number of Pages: 75
Number of Words: 18,730 (approx.)
Number of Characters: 106,762 (approx.)