

SPAWAR



Systems Center San Diego

***ISNS PPL/QPL Test Report:*
Wireless Local Area Network (WLAN)**

August 31, 2000
Rev 2.1

Prepared by:
Integration Test Facility (ITF)
Space and Naval Warfare Center, San Diego (SSC SD)
San Diego, CA 92152-7309

Report Documentation Page

Report Date 31AUG2000	Report Type N/A	Dates Covered (from... to) -
Title and Subtitle ISNS PPL/QPL Test Report: Wireless Local Area Network (WLAN)	Contract Number	
	Grant Number	
	Program Element Number	
Author(s)	Project Number	
	Task Number	
	Work Unit Number	
Performing Organization Name(s) and Address(es) Integration Test Facility (ITF) Space and Naval Warfare Center, San Diego (SSC SD) San Diego, CA 92152-7309	Performing Organization Report Number	
	Sponsoring/Monitoring Agency Name(s) and Address(es)	
		Sponsor/Monitor's Acronym(s)
		Sponsor/Monitor's Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited		
Supplementary Notes This document is public release even though it's a SBIR per email from Dick Milligan, NAVSEA, dated 30JAN2003., The original document contains color images.		
Abstract		
Subject Terms		
Report Classification unclassified	Classification of this page unclassified	
Classification of Abstract unclassified	Limitation of Abstract UU	
Number of Pages 43		

TABLE OF CONTENTS

	Page
1. INTRODUCTION.....	1
1.1 System/test overview	1
1.2 System/test components.....	1
1.3 Reason for test	2
2. TEST SUMMARY	3
2.1 Test Results.....	3
2.2 Test Objectives	3
2.3 Network Topology.....	4
3. LESSONS LEARNED	5
3.1 System Under Test (SUT)	5
3.1.1 Follow-on Testing.....	5
3.1.2 Wireless Local Area Network (WLAN)	5
3.2 LAN.....	6
3.2.1 Switches	6
3.3 PC's and servers	6
4. INSTALLATION GUIDANCE	7
4.1 Port counts and port setup.....	7
4.2 System Under Test (SUT) Setup	7
4.3 LAN Setup.....	7
4.3.1 DHCP Setup.....	7
4.3.2 IP Addressing setup	7
4.3.3 Switch Setup	7
4.3.4 Port Setup.....	7
4.3.5 MSS/Internal Router	7
4.3.6 VLAN/ELAN Setup.....	7
4.3.7 Bridging setup.....	7
4.4 WAN Setup.....	7
4.4.1 ADNS setup	7
4.4.2 Proxy server setup.....	8
4.4.3 Off-ship router setup	8
4.4.3.1 ACL setup	8
4.4.3.2 Routing protocols.....	8
4.4.3.3 Routing areas	8
4.4.4 DNS setup	8
4.4.5 NOC configuration setup	8
4.5 PC's and Servers.....	8
4.5.1 GotsDelta Clients	8
4.5.2 GotsDelta Servers	8
4.6 Network management setup.....	8
5. SETUP PROCEDURES	9
5.1 Theory of Operation	9
5.2 Assumed Initial Conditions of this System Test.....	9
5.3 Network Setup Procedures.....	10
5.4 WAN/ADNS setup procedures	11
5.5 ISNS Network Servers & PC Clients.....	12
5.6 Aironet Wireless Access Point	12
5.7 Cisco Aironet 340 Series PC Card.....	14
5.8 NetFortress Remote	15
5.8.1 NetFortress Remote Client.....	15

5.8.2	NetFortress Remote Signature	16
5.9	NetFortress 100 VPN.....	17
6.	TEST PROCEDURES	18
6.1	PC clients join the shipboard "Windows NT" domain.	18
6.2	Install GotsDelta via the wireless link.	18
6.3	Web browse via WLAN.	19
6.4	Send & receive e-mail.	19
6.5	Run C2PC, receive tracks.	19
7.	APPENDICES	20
7.1	Appendix A: Test Objectives/Results Matrix	20
7.2	Appendix B: Protocol Usage.	21
7.3	Appendix C: System Baseline Summary	22
7.4	Appendix D: Switch Configurations.....	23
7.4.1	Backbone Switch 1	23
7.4.2	Backbone Switch 2	24
7.4.3	Edge Switch 1	25
7.4.4	Edge Switch 2	26
7.4.5	MSS Configuration	27
7.5	Appendix E: Router Configuration	28
7.6	Appendix F: Workstation/Server Configurations	30
7.7	Appendix G: Wireless Local Area Network Components.....	32
7.7.1	Aironet Wireless Access Point Specification.....	32
7.7.2	Cisco Aironet 340 Series PC Card Specifications	33
7.7.3	NetFortress 100 Specifications	34
7.7.4	NetFortress Model Number Breakdown	35
7.8	Appendix H: Network Addressing Information.....	36

LIST OF FIGURES

	<u>Page</u>
Figure 2-1: Test Network Topology Diagram (Large Deck)	4

LIST OF TABLES

	<u>Page</u>
Table 1-1: Test Information	1
Table A-1: Test Objectives/Results Matrix.....	20
Table B-1: Protocols Usage.....	21
Table C-1: Summary of Baseline Network HW/SW Versions	22
Table C-2: Wireless Local Area Network HW/SW Versions.....	22
Table E-1: Large Deck VLAN Layout.....	36
Table E-2: Large Deck IP Network Phone Book.....	37

ADMINISTRATIVE INFORMATION

This work was prepared by SPAWAR Systems Center, San Diego (SSC SD) for the SPAWAR PMW-158 and PD15. Questions concerning this documentation or the program it describes should be directed to the author of the document:

Jesse R. Baumgartner
 SPAWAR Systems Center San Diego (SSC SD), CA
 (619) 553-6927/5544 voice
 (619) 553-4118 fax
 baumgarj@spawar.navy.mil

The following additional personnel can answer technical issues about the conduct of the test.

<i>Name</i>	<i>Organization</i>	<i>Phone</i>	<i>Email</i>
Chance, Steve	SSC SD D4221	(619)-553-4029	chance@spawar.navy.mil
Barlow, Phil	SSC SD, D87	(619) 553-5640	prb@ spawar.navy.mil
Demuth, Dinah	SSC SD, D87	(619) 553-3148	demuthd@ spawar.navy.mil

DISTRIBUTION LIMITED TO:

SPAWAR 051
 SPAWAR PD15
 SPAWAR PMW-151
 SPAWAR PMW-157
 SPAWAR PMW-158
 SSC San Diego, Code D80 Department Head
 SSC San Diego, Code D82 Division Head
 SSC San Diego, Code D821 Branch Head
 SSC San Diego, Code D42, Division Head

REVISION HISTORY

<i>Date</i>	<i>Version</i>	<i>Who</i>	<i>Description</i>
8/28/2000	2.0	Jesse R. Baumgartner	Completed documentation, submitted for review.
8/31/00	2.1	Steve Chance	Completed document review, ready for release

1. INTRODUCTION

Table 1-1: Test Information

<i>Parameter</i>	<i>Value</i>
Purpose:	Test WLAN software applications on ISNS Network topology
Requester/sponsor:	SPAWAR PMW 157
Location:	ITF San Diego
Applicable ECP's/NCR's:	NIN-00-113u
FBC's used:	FY2000 Large Deck

1.1 System/test overview

The Defense Advanced Research Projects Agency (DARPA) is pursuing integrated advanced research projects that provide seamless, secure, connectivity for mobile data (information) exchange. The goal of DARPA's Mobile Computing Project is to network commercial wireless and cellular technologies, both inside and outside the physical boundaries of the workspace, with existing cable infrastructure.

1.2 System/test components

The Wireless LAN (WLAN) consists of the following components:

NetFortress Components: The NetFortress components consist of the NetFortress 100 and the NetFortress Remote. The NetFortress 100 is a rack mountable unit that provides for secure connection between the ISNS network and the PC client by performing encryption and decryption of the network packets. The NetFortress unit encrypts data at the network layer of the OSI model. The original header information is encapsulated, only the source and destination IP addresses are visible. All headers added at the upper layers are encapsulated in the encrypted portion of the packet. The NetFortress modifies the original look of the IP packet by encapsulating/hiding the original IP header information, modifying the protocol as well as the length of the packet by using compression on the original payload. All original data is kept in the modified packet. The NetFortress Remote is PC client software that works in combination with the NetFortress 100 in order to encrypt/decrypt communications between the RF client and the NetFortress 100 unit.

Cisco Aironet 340 Series Components: The Cisco Aironet 340 series client adapters and access points are designed to provide for wireless communication between the PC and the base station (access point). The Aironet 340 series includes a complete line of client adapters, including PC Card, Personal Computer Interface (PCI), and Industry-Standard Architecture (ISA) cards for both notebook and desktop wireless connectivity. Based on direct sequence spread spectrum (DSSS) technology and operating in the 2.4 GHz band, the Aironet 340 series provides an Ethernet-like data rate of up to 11 megabits per second (Mbps). Understanding the security requirements of both small businesses and the enterprise, Cisco provides up to 128-bit Wired Equivalent Privacy (WEP), an optional security mechanism defined within the 802.11 standard that is designed to make the link integrity of the wireless medium equal to that of a cable. WEP is integrated with standard authentication features, providing a level of data security equal to traditional wired LANs. For investment protection, the Aironet 340 series conforms to the IEEE 802.11b standard.

1.3 Reason for test

The purpose of this test is to ascertain the impact that the Wireless Local Area Network (WLAN) will have on the Integrated Shipboard Network System (ISNS) network. This system is being tested in anticipation of an experimental installation onboard the USS Coronado in AUG-SEP 2000.

2. TEST SUMMARY

2.1 Test Results

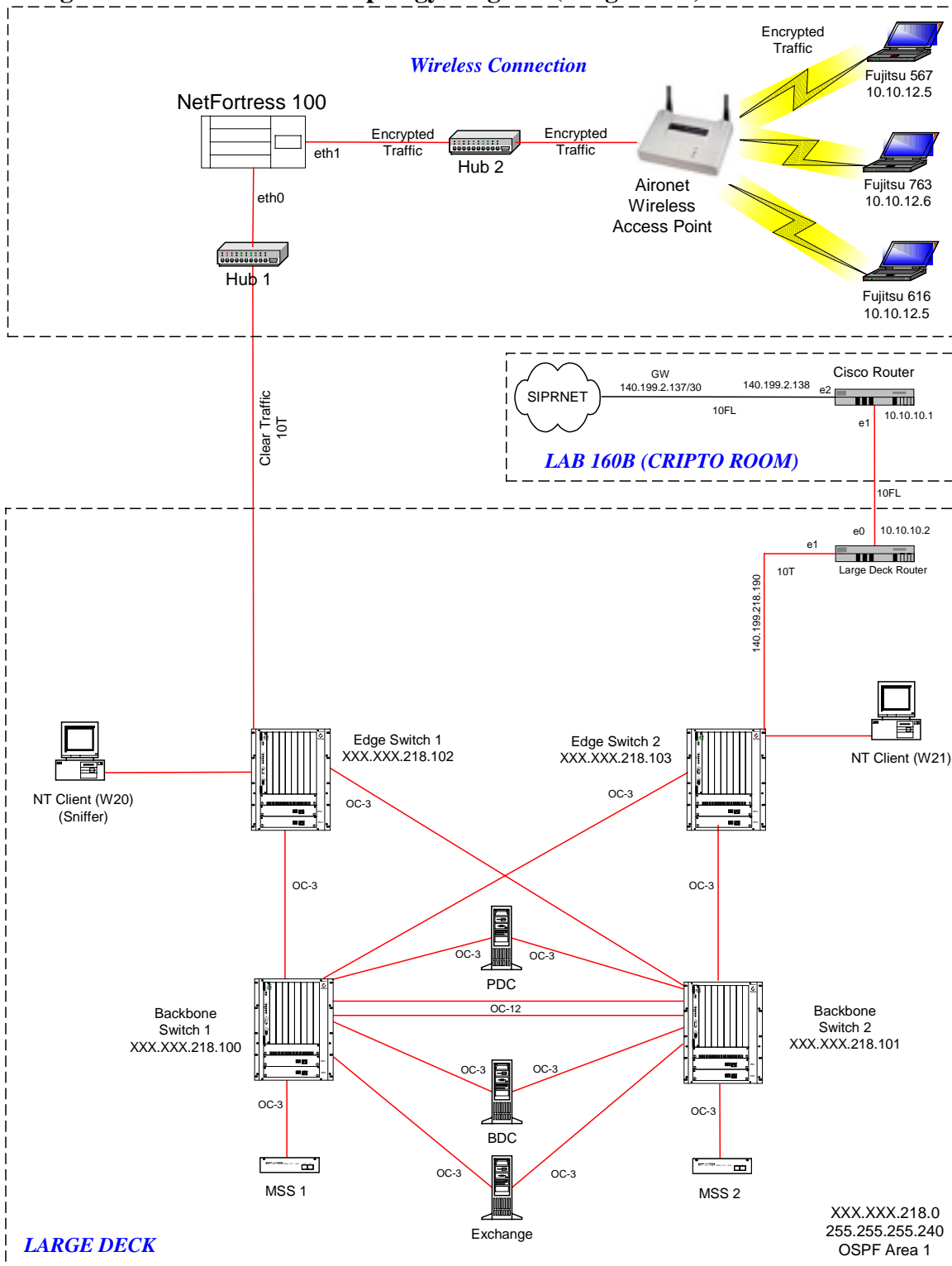
1. The Wireless Local Area Network (WLAN) is recommended for follow-on testing on the USS Coronado. It is considered approved when installed in accordance with the setup instructions and guidance appearing in this test report.
2. All test objectives listed were successfully demonstrated. Some issues were noted. No unusual setup procedures were required. Software and hardware operates per manufacturers description.
3. No negative impact to existing network users was observed. Clients could still send/receive e-mail, web browse and perform C2PC functions.
4. Based on the results from this test, there is no reason to not recommend this system for further afloat evaluation.

2.2 Test Objectives

1. PC clients join the shipboard "Windows NT" domain.
2. Install GotsDelta on PC clients via the wireless link
3. Web Browse SIPRNET
4. Send and receive e-mail
5. Run C2PC, receive tracks.
6. Identify setup/installation issues.
7. Recommend operational policies and procedures for this system that would reduce any adverse impact this system might have on operational networks

2.3 Network Topology

Figure 2-1: Test Network Topology Diagram (Large Deck)



3. LESSONS LEARNED

3.1 System Under Test (SUT)

3.1.1 Follow-on Testing

Currently the Wireless Local Area Network (WLAN) system is not scheduled for follow-on testing. However since this configuration will be used for testing and evaluation onboard the USS Coronado, any deviation from the tested configuration would necessitate that follow-on testing be scheduled.

3.1.2 Wireless Local Area Network (WLAN)

1. ***Cisco Aironet 340 Series Components.*** The “Aironet Wireless Access Point” and the “Aironet 340 Series PC Card Client Adapter both worked as advertised by the manufacturer.
2. ***NetFortress Components:*** After some initial problems, the “NetFortress 100” and the “NetFortress Remote” functioned as advertised by the manufacturer.

NetFortress 100: During the initial testing we did experienced some difficulty as we where in receipt of the incorrect type of NetFortress hardware box. The NetFortress box comes in a variety of configurations and models (see Appendix G, Section 7.7.4). The initial test conducted included a “Classless Activated” model, however the correct equipment for the test was the “Classless Non-Activated” model. The difference between the two is that the “Activated” model will “bind” itself to the class of network that it is on, once this happens the box cannot be moved to another network. The “Non-Activated” model will allow movement from one network to another without the paralyzing security protection.

NetFortress Remote: At the time of the initial test, and while attempting to setup the PC clients, it was discovered that the “NetFortress Remote” client software would not accept a subnet mask other than the standard class “A”, “B”, or “C” subnet mask. If you attempted to change the subnet mask to a .192, .224, .240, etc the PC client would “Blue-screen”. This was a bug unknown to the manufacturer. The manufacturer did provide a fix for the problem, however the bug fix was not consistent, some times it worked and sometimes it did not. Since the ITF Lab utilizes a non-standard subnet (.240) we where required to create a standard subnet for the test. Since most VLAN onboard are a full class C address, this might not present a problem. However this should be kept in mind if an attempt will be made in the future to install this system on a non-standard subnetted network.

3.2 LAN

3.2.1 Switches

The only required change to the switches would be the setting of the port that the WLAN system will be utilizing to “bridged” mode. In order to do this a “MODVP” must be run on the group/slot/port.

3.3 PC's and servers

No changes to the standard configuration are required. The only change takes place on the WLAN clients. The NetFortress unit was designed as a security device; as such it will not pass unsecured protocols. This does include Dynamic Host Configuration Protocol (DHCP). As such the WLAN clients will have to be configured statically.

4. INSTALLATION GUIDANCE

4.1 Port counts and port setup

The system as tested will require one 10T port.

4.2 System Under Test (SUT) Setup

4.3 LAN Setup

4.3.1 DHCP Setup

No changes to the standard configuration are required.

The WLAN clients will not be utilizing DHCP as the NetFortress unit will not pass on the packets, therefore the clients will need to be manually assigned an ip address.

4.3.2 IP Addressing setup

No changes to the standard configuration are required.

4.3.3 Switch Setup

No changes to the standard configuration are required.

4.3.4 Port Setup

No changes to the standard configuration are required.

4.3.5 MSS/Internal Router

No changes to the standard configuration are required.

4.3.6 VLAN/ELAN Setup

No changes to the standard configuration are required.

4.3.7 Bridging setup

No changes to the standard configuration are required.

4.4 WAN Setup

4.4.1 ADNS setup

No changes to the standard configuration are required.

4.4.2 Proxy server setup

No changes to the standard configuration are required.

4.4.3 Off-ship router setup

4.4.3.1 ACL setup

No changes to the standard configuration are required.

4.4.3.2 Routing protocols

No changes to the standard configuration are required.

4.4.3.3 Routing areas

No changes to the standard configuration are required.

4.4.4 DNS setup

No changes to the standard configuration are required.

4.4.5 NOC configuration setup

No changes to the standard configuration are required.

4.5 PC's and Servers

4.5.1 GotsDelta Clients

No changes to the standard configuration are required. GD 3.18.3.4P1 was installed on the Fujitsu laptop clients. No problems were noted.

4.5.2 GotsDelta Servers

No changes to the standard configuration are required.

4.6 Network management setup

No changes to the standard configuration are required.

5. SETUP PROCEDURES

5.1 Theory of Operation

The Wireless Local Area Network (WLAN) will provide the users with the ability to connect to the ISNS LAN without the need for extra drops in the area. In addition it will give users a roaming functionality provided by the use of multiple "Access Points". This will allow wireless users to move freely throughout the facility while maintaining seamless, and uninterrupted access to the network. The "NetFortress" suite of hardware/software will provide encryption from the wireless adapter to the NetFortress box. From the NetFortress box the packets will be sent un-encrypted to the ISNS LAN via CAT5 connection.

5.2 Assumed Initial Conditions of this System Test

This section is used to install and setup the WLAN server and application so that it can be put into a defined state prior to the start of testing in section 3.

The assumed initial conditions of this test are as follows:

1. Network is properly configured with a large-deck VLAN layout.
2. Windows NT servers and clients that will be used in the test are properly configured with the standard GOTS delta software and communicating successfully over the network.
3. The ISNS network Windows NT servers and clients are loaded with GotsDelta 3.18.3.4P1.

5.3 Network Setup Procedures

The only required change to the network would be the setting of the port that the WLAN system will be utilizing to “bridged” mode. In order to do this a “MODVP” must be run on the group/slot/port.

```
ES0001-LD:/ >modvp 1 9/12 <ENTER> (G=Group # S=Slot/P=Port)
```

```
Modify local port 9/12 (Virtual port (#12)) ? (y) : <ENTER>
```

Screen 1

Modify M-Ether/12 Vport 9/12 Configuration

```
1) Vport/Group/Instance/Type : 12/1/1/Brg
2) Description                : Virtual port (#12)
3) Bridge Mode                : Auto-Switched
  31) Switch Timer             : 60
4) Flood Limit                : 192000
5) Output Format Type          : Default(IP-Eth II, IPX-802.3)
6) Ethernet 802.2 Pass Through : Yes
7) Admin, Operational Status  : Enabled, inactive
8) Mirrored Port Status       : Disabled, available
9) MAC address                 : 0020DA:CBCE5B
```

```
Command {Item=Value/?/Help/Quit/Redraw/Next/Previous/Save} Redraw): 3=b
<ENTER>
```

Screen 2

Modify M-Ether/12 Vport 9/12 Configuration

```
1) Vport/Group/Instance/Type : 12/1/1/Brg (unsaved)
2) Description                : Virtual port (#12)
3) Bridge Mode                : Spanning Tree Bridged
  31) Switch Timer             : 60
4) Flood Limit                : 192000
5) Output Format Type          : Default(IP-Eth II, IPX-802.3)
6) Ethernet 802.2 Pass Through : Yes
7) Admin, Operational Status  : Enabled, inactive
8) Mirrored Port Status       : Disabled, available
9) MAC address                 : 0020DA:CBCE5B
```

```
Command {Item=Value/?/Help/Quit/Redraw/Next/Previous/Save} Redraw): save
<ENTER>
```

Screen 3

Modify M-Ether/12 Vport 9/12 Configuration

```
1) Vport/Group/Instance/Type   : 12/1/1/Brg
2) Description                  : Virtual port (#12)
3) Bridge Mode                  : Spanning Tree Bridged
  31) Switch Timer              : 60
4) Flood Limit                  : 192000
5) Output Format Type           : Default(IP-Eth II, IPX-802.3)
6) Ethernet 802.2 Pass Through : Yes
7) Admin, Operational Status    : Enabled, inactive
8) Mirrored Port Status        : Disabled, available
9) MAC address                  : 0020DA:CBCE5B
```

```
Command {Item=Value/?/Help/Quit/Redraw/Next/Previous/Save} Redraw): quit
<ENTER>
```

5.4 WAN/ADNS setup procedures

No setup procedures were required for the WAN or ADNS.

5.5 ISNS Network Servers & PC Clients

The Integrated Shipboard Network System (ISNS) has been setup and configured in accordance with the “IT 21 Installation & Configuration Guide v3.18.3.4P1”. This documentation is included on the GotsDelta CD.

5.6 Aironet Wireless Access Point

This section describes the methods used to access and configure the Console system of the Aironet Access Point.

There are many ways in which you may configure and monitor the Aironet Access Point. However on the unit first powered up, basic configuration must be performed by accessing the Console Serial Port. To gain access through the Serial Port, the Aironet Access Point must be connected to a terminal or a PC running a terminal emulation program. Set the terminal to **9600 Baud, No-Parity, 8 data bits, 1 stop bit, and ANSI compatible**.

The Console system is organized as a set of menus. Each selection in a menu list may either take you to a sub-menu or display a command that will configure or display information controlling the unit. Once the Aironet Access Point has been assigned an IP address, you may then access the Console remotely using:

- Telnet protocol from a remote host or PC
- HTML browser, such as Netscape Navigator from a remote host
- Simple Network Management Protocol (SNMP) from a remote network management node

Configuring the Access Point

To configure the Aironet Access Point so it will communicate with other nodes or repeaters, use the Console Port to set the SSID parameter. If you choose to set an IP address, remote access via telnet or an HTML browser will be possible.

SSID Identifier (SSID)

The SSID (Service Set Identifier) is a unique identifier that is attached to selected packets sent out over the radio network. This functions as a password to join the radio network. Nodes associating to the Access Point must use the same identifier in their configurations, or their association requests will be ignored.

□ Assigning an SSID:

1. Select **1** from the main menu.
2. Enter **→write→press enter**
3. Enter "password" **asdfgh90→press enter**
4. To display the main menu **→press enter**
5. Select **1 "Configuration"** from the Main Menu.
6. Select **1 "Radio"** from the Configuration Menu.
7. Select **1 "SSID"** from the Configuration Radio Menu.
8. Enter a value for the SSID option. You may use up to 32 characters. All devices in the same radio network must use the same SSID. **"tsunami"**

□ Assigning an IP Address:

An IP address must be assigned to the unit before it can be accessed by telnet, HTTP, or SNMP. Other detailed Internet addressing options (such as gateway address or SNMP routing) can also be defined.

□ To assign an IP address:

1. Select **1 "Configuration"** from the Main Menu.
2. Select **3 "Ident"** from the Configuration Menu.
3. Select **1 "Inaddr"** from the Configuration Ident Menu.
4. Enter IP Address **10.10.12.4→press enter**
5. Select **2 "Inmask"** from the Configuration Ident Menu.
6. Enter IP Address **255.255.255.0→press enter**
7. Select **3 "Gateway"** from the Configuration Ident Menu.
8. Enter IP Address **10.10.12.1→press enter**

□ Verifying Association

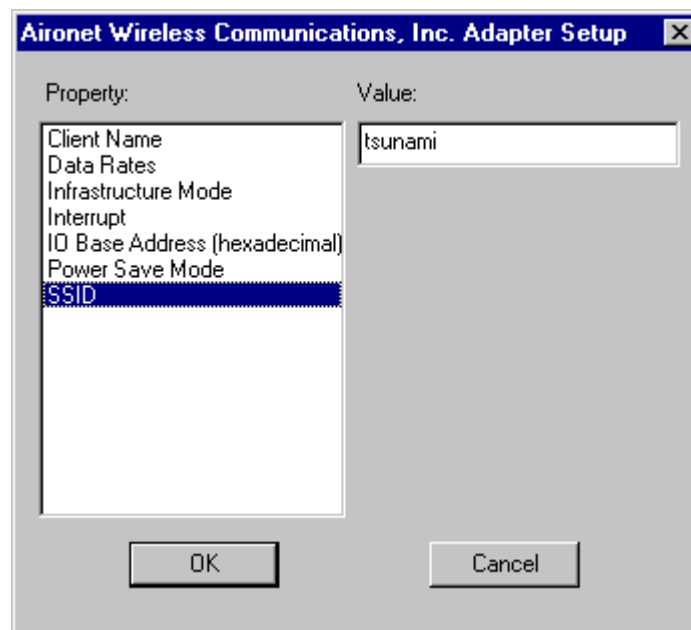
Once you have configured the Aironet Access Point and node devices with the correct parameters, the Radio Indicator will blink green indicating RF data traffic. The Status Indicator will be solid green indicating one or more nodes have associated to the Aironet Access Point.

5.7 Cisco Aironet 340 Series PC Card

1. Log into client as an “administrator”.
2. Click on **Start**→**Settings**→**Control Panel**
3. Double-click the →**Network** icon
4. From the “Network” dialog box select the →**Adapters** tab.

Note: If a previous adapter currently exist ensure that you remove it and re-boot the PC.

5. Single-click →**Add**
6. From the “Select Network Adapter” dialog box, single-click the →**Have Disk** button.
7. On the “Insert Disk” dialog box enter the path for the software.
8. Once the software has been installed, the following window will appear.

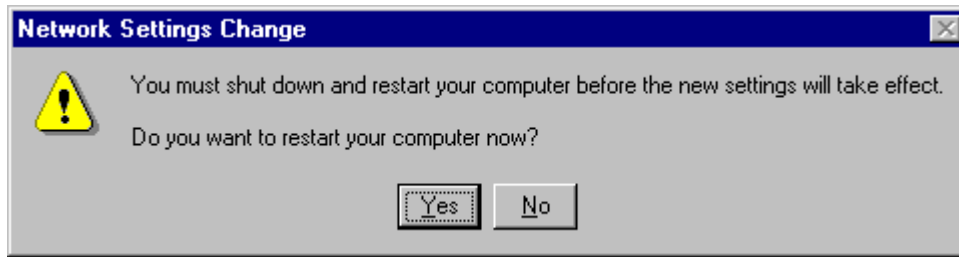


9. Select the “Client Name” property and enter a name in the “Value” box. This name will be used for identification purposes on the “Aironet Wireless Access Point”
10. Select the “SSID” property and in the “Value” box enter the same SSID name entered on the “Aironet Wireless Access Point” unit. This name will be used as a group control. If the names are different the system will not allow use of the “Access Point”
11. Click →**OK**

Note: The IO Base Address (hexadecimal) property might require a change if it conflicts with some other resource (I.E. mouse,com ports,etc.) In the case of this test it required a change to 400.

12. Click →**C**lose

- The following message window will appear.

13. Click →**Y**es

5.8 NetFortress Remote

The NetFortress Remote is PC client that works in combination with the NetFortress 100 to provide encryption and decryption. In order to do this a “Signature” file with a distinct key is used.

5.8.1 NetFortress Remote Client

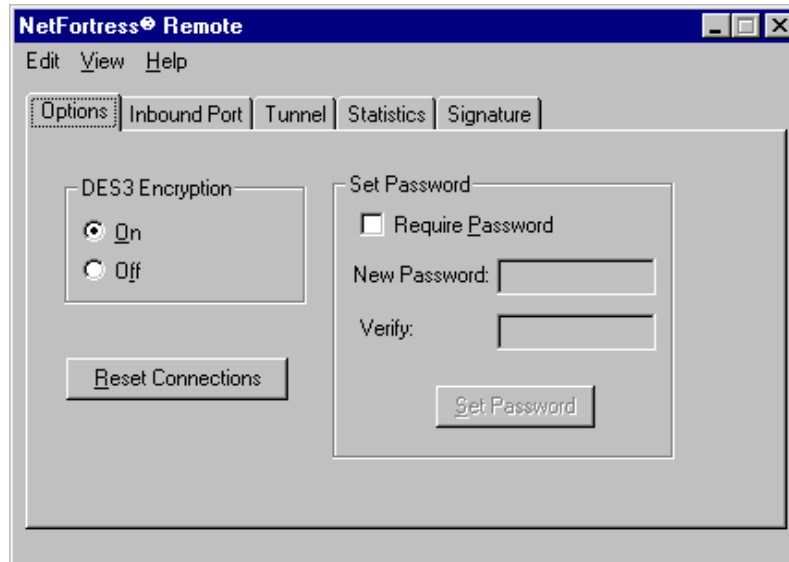
- At the Client PC, insert the “NetFortress Remote” CD-ROM
- Logon as administrator
 - Single-click →**S**tart→**R**un→**D**: \setup.exe
 - Accept all defaults
 - The system will re-boot

5.8.2 NetFortress Remote Signature

- At the Client PC, double-click the padlock icon on the task bar.

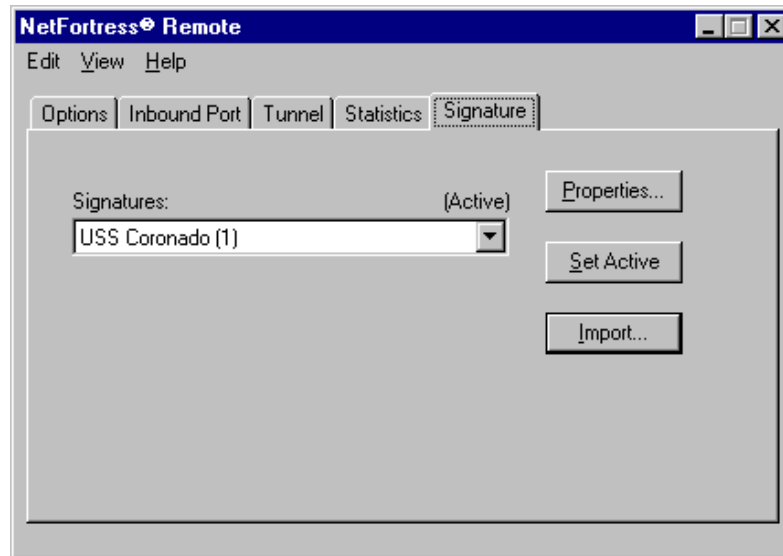


- The following dialog box is displayed:



- Single-click [**Signature**]

- The following dialog box is displayed:



- Insert the signature floppy disk in the floppy drive
- Single-click the [**Import**] button
- From the drop-down menu select desired signature.
- Once the signature is imported single-click the [**Set-Active**] button.
- Close the window

5.9 NetFortress 100 VPN

The NetFortress 100 VPN does not require any configuration. However it does require to be bound to the “network”. In order to perform this “binding” you must initiate a continuous ping from a workstation on the clear side of the network to a workstation in the encrypted side of the network. In other words the “ping” must go through the NetFortress unit in order for the binding to occur. Once the continuous ping is initiated, you can turn on the NetFortress unit. Once the NetFortress unit binds itself to the network, you should then observe that the pings on the client change from “Request timed out” to “Reply from xxx.xxx.xxx.xxx”

6. TEST PROCEDURES

6.1 PC clients join the shipboard "Windows NT" domain.

1.0	Network Communication
1.1	This procedure will test the ability of a wireless PC client to join a shipboard Windows NT domain via the wireless/encrypted link.
2.0	Command List
2.1	Single-click → Run → Settings → Control Panel
2.2	Double-click the < Network > icon.
2.3	On the "Identification" tab single-click the < Change > button.
2.4	On the "Member Off" window single-click the < Domain > window and enter the name of the domain you wish to join.
2.5	<input checked="" type="checkbox"/> Create a Computer Account in the domain.
2.6	In the < User Name >, and < Password > dialog boxes, enter the appropriate account information and pres the < Ok > button.
2.7	The computer will reboot.
3.0	Success Criteria
3.1	The PC clients are able to join the domain.

6.2 Install GotsDelta via the wireless link.

1.0	Network Communication
1.1	This procedure will test the ability of a wireless PC client to properly install and configure a GotsDelta software installation via the wireless/encrypted link.
2.0	Command List
2.1	Logon to the PC client as < installer >
2.2	Select < Workstation > install from the menu.
2.3	Proceed with the installation IAW the "IT 21 Installation & Configuration Guide v3.18.3.4P1".
3.0	Success Criteria
3.1	The installer is able to successfully load GotsDelta on PC client.

6.3 Web browse via WLAN.

1.0	Network Communication
1.1	This procedure will test the ability of a wireless PC client to Web browse SIPRNET via the wireless/encrypted link.
2.0	Command List
2.1	Logon to the PC client as <user1>
2.2	Run Internet Explorer and access various SIPRNET web sites
3.0	Success Criteria
3.1	User is able to web browse

6.4 Send & receive e-mail.

1.0	Network Communication
1.1	This procedure will test the ability of a wireless PC client to send & receive e-mail via the wireless/encrypted link.
2.0	Command List
2.1	Logon to the PC client as <user1>
2.2	Run Microsoft Outlook send e-mail to various users and receive same.
3.0	Success Criteria
3.1	User is able to send and receive e-mail

6.5 Run C2PC, receive tracks.

1.0	Network Communication
1.1	This procedure will test the ability of a wireless PC to run C2PC via the wireless/encrypted link.
2.0	Command List
2.1	Logon to the PC client as <user1>
2.2	Run C2PC and observe that tracks are coming across the wireless link
3.0	Success Criteria
3.1	User is able to receive C2PC tracks

7. APPENDICES

7.1 Appendix A: Test Objectives/Results Matrix

This appendix lists the detailed measurements that will be taken as part of this test. Subsections in section 5: Test Procedures define the detailed steps required to be taken in order to derive all of these measurements. This matrix is intended to be filled in and included as part of the test report for the system.

1. PC clients join the shipboard "Windows NT" domain.
2. Install GotsDelta on PC clients via the wireless link
3. Access "SIPRNET" World Wide Web via the wireless link

Table A-1: Test Objectives/Results Matrix

#	Parameter	Description	Units of measure	Result
I	LAN TESTING			
1.0	PC clients join the shipboard "Windows NT" domain.	The administrator is able to make the PC client a member of the shipboard "Windows NT" domain via the wireless/encrypted link.	Pass/Fail	PASS
1.1	Install GotsDelta on PC clients via the wireless link	The administrator is able to install the GotsDelta software load via the wireless/encrypted link.	Pass/Fail	PASS
1.3	Web Browse SIPRNET	Access "SIPRNET" World Wide Web via the wireless/encrypted link.	Pass/Fail	PASS
1.4	Send and receive e-mail	Send and receive e-mail via the wireless/encrypted link.	Pass/Fail	PASS
1.5	Run C2PC, receive tracks.	Run C2PC and receive tracks via the wireless/encrypted link.	Pass/Fail	PASS

7.2 Appendix B: Protocol Usage.

This section documents the networking protocols and services that are understood to be used by the WLAN system. In reality the WLAN system will pass all protocol types with the exception of “unsecured protocols” like DHCP.

Table B-1: Protocols Usage

<i>Protocol Acronym</i>	<i>Protocol Name</i>	<i>Port Number</i>	<i>Purpose</i>
PING	Packet Internet Groper	9595	Ping Discovery Service
TELNET	TELENET	23	Terminal Emulation Services
SMTP	Simple Mail Transfer Protocol	25	Mail Transfer Protocol
DOMAIN	Domain Name Service	53	FQDN to IP Address

WELL KNOWN PORT NUMBERS = 0 through 1023

Ports in this range can only be used by system (or root) processes or by programs executed by privileged users.

REGISTERED PORT NUMBERS = 1024 through 49151

Ports in this range are used to name the ends of logical connections, which carry long-term conversations. For the purpose of providing services to unknown callers, a service contact port is defined.

DYNAMIC AND/OR PRIVATE PORTS = 49152 through 65535

7.3 Appendix C: System Baseline Summary

This section contains a summary of the versions of hardware and software to be used in the conduct of this test. If you want details on the configuration of a specific device, please consult **Section 1.2:: System/test components**. The listed combination of hardware and software are approved for use together and will be tested together. Any effort to deviate from this tested and approved combination of FY2000 hardware and software may result in an unreliable system with interoperability problems that are undocumented and have no known remedy. Retesting is therefore recommended whenever there is a deviation from this baseline.

Table C-1: Summary of Baseline Network HW/SW Versions

Comp Type:	Title:	Ver:	Included in test?	FY2000 Configuration?	Details:
Hardware	DEC PRIORIS 6000	933WW	Yes	No	
Hardware	Fore Systems PCA-200 NIC	5.0.2	Yes	Yes	
Hardware	SMC ATM Power155	9741F	Yes	Yes	
Hardware	Omni MSS	Ver 2	Yes	Yes	
Hardware	Phys. Optics Corp. bypass switch	POC-912MNB	Yes	Yes	Optical bypass switch
Hardware	Alcatel OmniSwitch	Omni-9wx	Yes	Yes	
Software	Cisco IOS Software	11.2	Yes	Yes	
Software	GOTS Delta	3.18.3.4P1	Yes	Yes	Used on clients
Software	GOTS Delta	3.18.3.4P1	Yes	Yes	Used on servers
Software	Microsoft Back Office	2.5	Yes	Yes	
Software	MS Exchange	5.5 sp2	Yes	Yes	
Software	MS WinNT	4.0 sp3	Yes	Yes	
Software	MS WinNT Server	4.0 sp5	Yes	Yes	
Software	Alcatel MSS Code	2.2.1	Yes	Yes	
Software	Alcatel MSS Firmware	4.0	Yes	Yes	
Software	Alcatel Switch Code	3.4.8	Yes	Yes	

Table C-2: Wireless Local Area Network HW/SW Versions

Comp Type:	Title:	Ver:	Included in test?	FY2000 Configuration?	Details:
Hardware	NetFortress	100	Yes	No	
Hardware	Cisco Aironet Wireless Adapter	340	Yes	No	
Hardware	Aironet Access Point	AP4800	Yes	No	
Software	NetFortress Remote	4.1.0.572	Yes	No	
Software	Cisco Aironet Wireless Adapter Client Software	4.10	Yes	No	

7.4 Appendix D: Switch Configurations

7.4.1 Backbone Switch 1

Large Deck Backbone Switch BS001G-LD							
Lab Nomenclature	BS0001G-LD						
Manufacturer / Model	Alcatel / OMNISWITCH 9W						
Slot configuration	Module-Type	Adm-Status	HW	Board	Mfg	Firmware-Version	
	Slot	Part-Number	Oper-Status	Rev	Serial #	Date	Base-MAC-Address
1*	MPM 1G 5014318	Enabled Operational	B26	83830243	09/21/98	3.4.8	00:20:da:a8:55:90
2	MPM 1G 5014317	Enabled Software FB	B26	80952064	09/30/98	3.1.8	00:20:da:92:f6:90
3	FCSM-II 5018168	Enabled Operational	A4	93320110	08/22/99	3.4.8	00:20:da:f5:b9:40
4	CSM-OC12-M 5013393	Enabled Operational	A15	82852419	07/09/98	3.4.8	None
5	CSM-OC3-M 5011369	Enabled Operational	H2	83051830	07/27/98	3.4.8	None
6	CSM-OC3-M 5011324	Enabled Operational	G2	72850958	07/12/97	3.4.8	None
7	Empty						
8	Empty						
9	M-Ether/12 5015826	Enabled Operational	D5	90883722	02/20/99	3.4.8	00:20:da:cb:ce:50

7.4.2 Backbone Switch 2

Large Deck Backbone Switch BS002G-LD							
Lab Nomenclature	BS0002G-LD						
Manufacturer / Model	Alcatel / OMNISWITCH 9W						
Slot configuration	Module-Type	Adm-Status	HW	Board	Mfg	Firmware-Version	
	Slot	Part-Number	Oper-Status	Rev	Serial #	Date	Base-MAC-Address
	1*	MPM 1G 5014318	Enabled Operational	B26	85250276	03/30/99	3.4.8 00:20:da:be:f6:e0
	2	MPM 1G 5014306	Enabled Config FB	A9	72850252	07/10/97	3.4.8 00:20:da:84:4e:90
	3	FCSM-II 5018168	Enabled Operational	A7	93720288	10/05/99	3.4.8 00:d0:95:0b:cc:40
	4	CSM-OC12-M 5013393	Enabled Operational	A15	82852414	07/09/98	3.4.8 None
	5	CSM-OC3-M 5011324	Enabled Operational	G2	72850963	07/11/97	3.4.8 None
	6	CSM-OC3-M 5011369	Enabled Operational	H3	84870005	12/21/98	3.4.8 None
	7	Empty					
	8	Empty					
	9	M-Ether/12 5015826	Enabled Operational	D2	82270275	06/12/98	3.4.8 00:20:da:ac:1f:30

7.4.3 Edge Switch 1

Large Deck Edge Switch ES001G-LD							
Lab Nomenclature	ES0001G-LD						
Manufacturer / Model	Alcatel / OMNISWITCH 9W						
Slot configuration	Module-Type	Adm-Status	HW	Board	Mfg	Firmware-Version	
	Slot	Part-Number	Oper-Status	Rev	Serial #	Date	Base-MAC-Address
1*	MPM 1G 5014318	Enabled Operational	B13	83151698	07/08/98	3.4.8	00:20:da:a7:79:70
2	FCSM-II 5018168	Enabled Operational	A7	92421789	06/24/99	3.4.8	00:20:da:f5:5d:60
3	CSM-OC3-M 5011369	Enabled Operational	H2	83051829	07/27/98	3.4.8 None	
4	F-Ether/M 5015918	Enabled Operational	B3	75151378	12/18/97	3.4.8	00:20:da:8a:fd:60
5	Empty						
6	Empty						
7	ESM-F16 5019708	Enabled Operational	A2	83451532	08/19/98	3.4.8	00:20:da:af:11:70 00:20:da:af:11:80
8	Empty						
9	M-Ether/12 5015826	Enabled Operational	D7	93083987	08/04/99	3.4.8	00:20:da:e0:60:b0

7.4.4 Edge Switch 2

Large Deck Edge Switch ES002G-LD							
Lab Nomenclature	ES0002G-LD						
Manufacturer / Model	Alcatel / OMNISWITCH 9W						
Slot configuration	Module-Type	Adm-Status	HW	Board	Mfg	Firmware-Version	
	Slot	Part-Number	Oper-Status	Rev	Serial #	Date	Base-MAC-Address
1*	MPM 1G 5014318	Enabled Operational	B13	83151702	07/10/98	3.4.8	00:20:da:a7:90:d0
2	FCSM-II 5018168	Enabled Operational	A4	93920411	09/30/99	3.4.8	00:d0:95:0b:c3:20
3	CSM-OC3-M 5011375	Enabled Operational	H	91480283	06/02/99	3.4.8 None	
4	F-Ether/M 5015906	Enabled Operational	A5	73250827	08/07/97	3.4.8	00:20:da:83:23:10
5	Empty						
6	Empty						
7	ESM-F16 5019708	Enabled Operational	A2	83550113	09/16/98	3.4.8	00:20:da:a2:47:80 00:20:da:a2:47:90
8	M-Ether/12 5015826	Enabled Operational	D7	93182255	08/07/99	3.4.8	00:20:da:e0:86:70
9	Empty						

7.4.5 MSS Configuration

MSS 1	
Make / Model	Xylan / OmniMSS-M1
Product ID	8210-MSS
Version / Release	2 / 2
MOD	0
PTF	1
Feat	8707
RPQ	0
Date	9 Feb 1999 07:31
Build	cc4mv_80PB
Current Configuration	Bank F → Config 3 → 348TestMSS1 20 April 2000

MSS 2	
Make / Model	Xylan / OmniMSS-M1
Product ID	8210-MSS
Version / Release	2 / 2
MOD	0
PTF	1
Feat	8707
RPQ	0
Date	9 Feb 1999 07:31
Build	cc4mv_80PB
Current Configuration	Bank F → Config 1 → ADV SNM OSPF 07 June 2000

7.5 Appendix E: Router Configuration

Current configuration:

```
!  
version 11.2  
service password-encryption  
no service udp-small-servers  
no service tcp-small-servers  
!  
hostname Large_Deck  
!  
enable secret 5 $1$6FZC$Zr.LDgW3bm7514YsjB2350  
enable password 7 095C4F1A0A1218000F  
!  
no ip domain-lookup  
ip multicast-routing  
!  
interface Ethernet0  
 ip address 140.199.218.190 255.255.255.240  
 media-type 10BaseT  
!  
interface Ethernet1  
 ip address 10.10.10.2 255.255.255.0  
 ip access-group 100 out  
 media-type AUI  
!  
interface Serial0  
 no ip address  
 ip accounting output-packets  
 bandwidth 56  
 no keepalive  
 shutdown  
 no fair-queue  
!  
interface Serial1  
 ip unnumbered Ethernet0  
 encapsulation ppp  
 keepalive 30  
 shutdown  
!  
interface ATM0  
 no ip address  
 shutdown  
!  
router ospf 24  
 network 140.199.218.176 0.0.0.15 area 0.0.0.1
```

```
network 10.10.10.0 0.0.0.255 area 0.0.0.1
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.10.10.1
access-list 100 permit tcp any any established
access-list 100 permit ospf any any
access-list 100 permit ipinip any any
access-list 100 permit igmp any any
access-list 100 permit udp any eq snmp host 205.0.144.77
access-list 100 permit udp any eq snmptrap host 205.0.144.77
access-list 100 deny udp any any eq snmp
access-list 100 deny udp any any eq snmptrap
access-list 100 permit gre any any
access-list 100 permit tcp any any eq 135
access-list 100 permit udp any any eq 135
access-list 100 permit 55 any any
access-list 100 permit 29 any any
access-list 100 permit ip host 140.199.218.181 any
access-list 100 permit ip host 140.199.218.121 any
access-list 100 permit ip host 140.199.218.182 any
access-list 100 permit ip host 140.199.218.180 any
access-list 100 permit ip host 140.199.218.183 any
access-list 100 permit tcp any any eq 1521
access-list 100 permit tcp any any eq 1101
access-list 100 permit icmp any any
access-list 100 permit 83 any any
!
!
line con 0
line aux 0
line vty 0
password 7 09455D070A4445425B5C
login
line vty 1 4
password 7 045802150C2E
login
!
end
```

7.6 Appendix F: Workstation/Server Configurations

PDC (Large Deck)	
Make / Model	DEC PRIORIS 6000 / 933WW
Operating System	Windows NT Server 4.0 with SP5 and hot fixes
GOTS Delta Load	3.18.3.4P1
Network Adapter	SMC ATM Power155 (9741F)
Memory	512Mb

BDC (Large Deck)	
Make / Model	DEC PRIORIS 6000 / 933WW
Operating System	Windows NT Server 4.0 with SP5 and hot fixes
GOTS Delta Load	3.18.3.4P1
Network Adapter	SMC ATM Power155 (9741F)
Memory	256Mb

Exchange Server 1 (Large Deck)	
Make / Model	DEC PRIORIS 6000 / 933WW
Operating System	Windows NT Server 4.0 with SP5 and hot fixes
GOTS Delta Load	3.18.3.4P1
Network Adapter	ForeRunner® 200E
Memory	256Mb

WLAN Clients (Fujitsu 567, 616, 763)	
Make / Model	Fujitsu "E" Series Lifebook
Operating System	Windows NT Server 4.0 with SP3 and hot fixes
GOTS Delta Load	3.18.3.4P1
Network Adapter	Cisco Aironet 340 PC Card Client Adapters
Memory	64Mb

WS0020 (Large Deck)	
Make / Model	Micronics PC
Operating System	Windows NT 4.0 with SP3 and hot fixes
GOTS Delta Load	3.18.3.4P1
Network Adapter	SMC 1211TX
Memory	64Mb

WS0021 (Large Deck)	
Make / Model	Micronics PC
Operating System	Windows NT 4.0 with SP3 and hot fixes
GOTS Delta Load	3.18.3.4P1
Network Adapter	Adaptec Cogent Fast Ethernet ANA-6910/FXST
Memory	64Mb

7.7 Appendix G: Wireless Local Area Network Components

7.7.1 Aironet Wireless Access Point Specification

GENERAL	
Description	2.4 GHz Direct sequence spread spectrum (DSSS) Access Point
Antenna	Two 2 dBi diversity dipole; Optional, higher gain antennas available
Cell Coverage	At 1 Mbps: 260,000 sq. ft. At 11 Mbps: 60,000 sq. ft
Data Rates	1, 2, 5.5 and 11 Mbps per channel
Operating Channels	IEEE 802.11 compliant 11 channels (US, Canada); 13 channels (ETSI)
Simultaneous Channel Support	Three (FCC, Canada, ETSI); One (Japan)
Certifications	Meets FCC Part 15 subpart B, Class B; FCC Part 15.247; EN55022; and EN55011; Call for other information on use outside the USA
NETWORK INFORMATION	
Network Protocols Supported	AP4800-E complies with IEEE 802.3 and Ethernet Blue Book AP4800-T complies with IEEE 802.5 Token Ring
Wireless Network Standard	IEEE 802.11 for 1 and 2 Mbps data rates
Network Connection Types	AP4800-E: 10Base2, 0Base5, 10BaseT; AP4800-T: UTP, STP
Wired LAN Capacity	AP4800-E: 10 Mbps; AP4800-T: 4 Mbps/16Mbps
Roaming	IEEE 802.11 compliant at 1 and 2 Mbps
Local Configuration	Direct console port (Serial EIA-232 DB-9 female)
Remote Configuration	HTTP, Telnet, FTP or SNMP
Automatic Configuration	BOOTP
SNMP Compliance	MIB I, MIB II
LED Indicators	System, Ethernet/Token Ring Network Activity, Wireless LAN Activity
RADIO DATA	
Frequency Band	2.400 - 2.4835 GHz (US, Canada, ETSI) 2.471-2.497 GHz (Japan)
Wireless Medium	Direct sequence spread spectrum (DSSS)
Modulation	CCK, BPSK, QPSK
Output Power	100mW (USA and Canada), 50mW (ETSI), 10mW/MHz EIRP (Japan)
ENVIRONMENTAL INFORMATION	
Operating Temperature	-20° C to 50° C (-4° F to 122° F)
Humidity	95% (non-condensing)
Physical Characteristics	Dimensions: 20 cm x 15 cm x 5 cm (7.8 in x 5.9 in x 1.9 in) Weight: 0.7 kg (1 lb 8 oz) Power Supply: Standard Power Pack: 120 VAC, 50/60 Hz to 12 VDC @ 1.5A Universal Power Pack: 90-264 VAC, 47/63 Hz to 12 VDC @ 1.5A

7.7.2 Cisco Aironet 340 Series PC Card Specifications

Radio Specifications		
Item	Specification	Description
Radio Type	Direct Sequence	2.4 GHz ISM Band
Operating Frequency	2400–2497 MHz	North American, ETSI, and Japan channel coverage, factory configurable
FCC ID	LOZ102038	FCC approval
Channeling	1 MHz increments	Programmable for IEEE 802.11
Type of Modulation	BPSK 1 Mbps QPSK 2 Mbps CCK 5.5 and 11 Mbps	Nominal 10 MHz BW (-6 dB)
Power Output (North American Configuration)	30 mW	Meets FCC Part 15.247 Requirements
Receiver Sensitivity	-90 dBm @ 1 Mbps -88 dBm @ 2 Mbps -87 dBm @ 5.5 Mbps -83 dBm @ 11 Mbps	
Antenna Type	Diversity	Integrated antenna (not included on AIR-LMC340 series PC card client adapters)
PCMCIA Connector		Card Connector Per PCMCIA card Physical Specification 4.1 (11/95)

Power Requirements	
Specification	Value
Operational Voltage	5.0V \pm 0.25V
Receive Mode Current	280 mA (250 mA typically)
High Power Transmit Mode Current (30 mW)	400 mA (350 mA typically)
Sleep Mode	10 mA

Physical Specifications	
Specification	Value
Size	3.37" L x 2.13" W x .20" H (8.56 cm L x 5.41 cm W x .51 cm H)
Enclosure	PC Card Type II
Weight	1.3oz
Operating Temperature	0°C to 70°C minimum (32°F to 158°F)
Storage Temperature	-40°C to +85°C (-40°F to 185°F)
Humidity, Shock, Drop, Vibration, Thermal Shock	Per PCMCIA card version 2.01, section 13.6.2 Specifications
ESD	15kV (human body model)
Connectors	68-pin PCMCIA card
Status Indicators	Green and Amber LEDs – link association/activity

7.7.3 NetFortress 100 Specifications

NetFortress 100 Technical Specifications	
Product	NetFortress 100
Model Tested	NF100-C-3DES-L0-SD-NON
Dimensions	7" H x 18.5" D x 19" W
Weight	41lb
LAN Interface	Two BNC ports; Two 10BaseT Ethernet Ports
Protocols supported	IP, IPX
Virtual Private Network Protocol	Secure Packet Shield (SPS)
Encryption Algorithms	128-bit IDEA, 56-bit DES, 168-bit 3DES
Key Management	Dual Encrypted Diffie-Hellman Exchange
Routing	Static
Firewall	Packet and Port Filtering
DHCP	Client and Server
Other Network Support	NAT, PPP
Management	Web interface with logging
Safety Certification	UL, FCC, CSA Approved
Power Requirements	115/230 vac
FCC	FCC Part 15
WAN Interface	Asynchronous Serial PPP (56k Max)
Control Port	Asynchronous Serial ASCII

NetFortress Remote® Technical Specifications	
Encryption Algorithms	128-bit IDEA, 56-bit DES, 168-bit 3DES
Interoperability	NetFortress Virtual Key Ring

7.7.4 NetFortress Model Number Breakdown

The model and configuration tested was the “NF100-C-3DES-L0-SD-NON”. This number can be broken down as follows;

Product	NF001	NetFortress 1
	NF010	NetFortress 10
	NF100	NetFortress 100
Platform	C	Standard
	F	Government Version
	P	NetFortress Plus
Encryption Algorithm	3DES	Triple DES
	IDEA	IDEA
	DES	DES
Type	HO	Single Host
	LC	Class C Network
	LB	Class B Network
	LA	Class A Network
	L0	Classless
Configuration	SD	Standard
	S1	Segmented 1
	S2	Segmented 2
Activation	ACT	Activated
	NON	Non-activated

7.8 Appendix H: Network Addressing Information

Table E-1: Large Deck VLAN Layout

<i>VLAN</i>	<i>ELAN/Group</i>	<i>Group #</i>	<i>Network</i>	<i>Redundant Interface Address</i>	<i>MSS0001G</i>	<i>Redundancy Role</i>	<i>MSS0002G</i>	<i>Redundancy Role</i>	<i>Netmask</i>	<i>Purpose</i>
SED	SED	1	xxx.xxx.218.016	xxx.xxx.218.017	xxx.xxx.218.018	Primary	xxx.xxx.218.019	Backup	255.255.255.240	Secret Embarkee Default
SEA	SEA	2	xxx.xxx.218.032	xxx.xxx.218.033	xxx.xxx.218.034	Backup	xxx.xxx.218.035	Primary	255.255.255.240	Secret Embarkee Airwing
SEM	SEM	3	xxx.xxx.218.048	xxx.xxx.218.049	xxx.xxx.218.050	Primary	xxx.xxx.218.051	Backup	255.255.255.240	Secret Embarkee Marine
SES	SES	4	xxx.xxx.218.064	xxx.xxx.218.065	xxx.xxx.218.066	Backup	xxx.xxx.218.067	Primary	255.255.255.240	Secret Embarkee Staff
SRA	SRA	5	xxx.xxx.218.080	xxx.xxx.218.081	xxx.xxx.218.082	Primary	xxx.xxx.218.083	Backup	255.255.255.240	Secret Releasable Allied
SNM	SNM	6	xxx.xxx.218.096	xxx.xxx.218.097	xxx.xxx.218.098	Backup	xxx.xxx.218.099	Primary	255.255.255.240	Secret Network Management
STC1	STC1	7	xxx.xxx.218.112	xxx.xxx.218.113	xxx.xxx.218.114	Primary	xxx.xxx.218.115	Backup	255.255.255.240	Secret Tactical Computers 1
STC2	STC2	8	xxx.xxx.218.128	xxx.xxx.218.129	xxx.xxx.218.130	Backup	xxx.xxx.218.131	Primary	255.255.255.240	Secret Tactical Computers 2
STC3	STC3	9	xxx.xxx.218.144	xxx.xxx.218.145	xxx.xxx.218.146	Primary	xxx.xxx.218.147	Backup	255.255.255.240	Secret Tactical Computers 3
STC4	STC4	10	xxx.xxx.218.160	xxx.xxx.218.161	xxx.xxx.218.162	Backup	xxx.xxx.218.163	Primary	255.255.255.240	Secret Tactical Computers 4
STS1	STS1	11	xxx.xxx.218.176	xxx.xxx.218.177	xxx.xxx.218.178	Primary	xxx.xxx.218.179	Backup	255.255.255.240	Secret Tactical Support 1
STS2	STS2	12	xxx.xxx.218.192	xxx.xxx.218.193	xxx.xxx.218.194	Backup	xxx.xxx.218.195	Primary	255.255.255.240	Secret Tactical Support 2
AIR	AIR	13	xxx.xxx.12.0	xxx.xxx.12.1	xxx.xxx.12.2	Primary	xxx.xxx.12.3	Backup	255.255.255.0	Testing WLAN

The table below documents the IP addressing used in support of this test. Records are sorted in ascending order by Device Number.

Table E-2: Large Deck IP Network Phone Book

<i>Device #</i>	<i>Interface #</i>	<i>Alias</i>	<i>Host name</i>	<i>IP address</i>	<i>Netmask</i>	<i>Address method</i>	<i>System Manager</i>	<i>Notes</i>
BS0001G	SNM		BS0001G-LD	X.199.218.100	255.255.255.240	Static	Hansen	
BS0002G	SNM		BS0002G-LD	X.199.218.101	255.255.255.240	Static	Hansen	
ES0001G	SNM		ES0001G-LD	X.199.218.102	255.255.255.240	Static	Hansen	
ES0002G	SNM		ES0002G-LD	X.199.218.103	255.255.255.240	Static	Hansen	
ES0003G	SNM		ES0003G-LD	X.199.218.104	255.255.255.240	Static	Hansen	
ES0004G	SNM		ES0004G-LD	X.199.218.105	255.255.255.240	Static	Hansen	
MSS0001G	SED SEA SEM SES SRA SNM STC1 STC2 STC3 STC4 STS1 STS2		MSS0001G-SNM	X.199.218.018 X.199.218.034 X.199.218.050 X.199.218.066 X.199.218.082 X.199.218.098 X.199.218.114 X.199.218.130 X.199.218.146 X.199.218.162 X.199.218.178 X.199.218.194	255.255.255.240	Static	Hansen	
MSS0002G	SED SEA SEM SES SRA SNM STC1 STC2 STC3 STC4 STS1 STS2		MSS0002G-SNM	X.199.218.019 X.199.218.035 X.199.218.051 X.199.218.067 X.199.218.083 X.199.218.099 X.199.218.115 X.199.218.131 X.199.218.147 X.199.218.163 X.199.218.179 X.199.218.195	255.255.255.240	Static	Hansen	
PTR0001G				X.199.218.188	255.255.255.240	Static	Baumgartner	
RTR0001G	STS1	SIPRNET	RTR0002G-STS1	X.199.218.190	255.255.255.240	Static	Baumgartner	
SRV0001G	SED STS1 STS2		SRV0001G-SED SRV0001G-STS1 SRV0001G-STS2	X.199.218.022 X.199.218.180 X.199.218.196	255.255.255.240	Static	Baumgartner	
SRV0002G	STS1 STS2		SRV0001G-STS1 SRV0001G-STS2	X.199.218.181 X.199.218.197	255.255.255.240	Static	Baumgartner	
Fujitsu 567	AIR		Fujitsu 567	X.10.12.5	255.255.255.0	Static	Baumgartner	
Fujitsu 763	AIR		Fujitsu 763	X.10.12.6	255.255.255.0	Static	Baumgartner	
Fujitsu 616	AIR		Fujitsu 616	X.10.12.7	255.255.255.0	Static	Baumgartner	
W0020	AIR		ITFSF-LD1GWS20	X.10.12.20	255.255.255.0	Static	Baumgartner	
W0021	AIR		ITFSF-LD1GWS21	X.10.12.21	255.255.255.0	Static	Baumgartner	