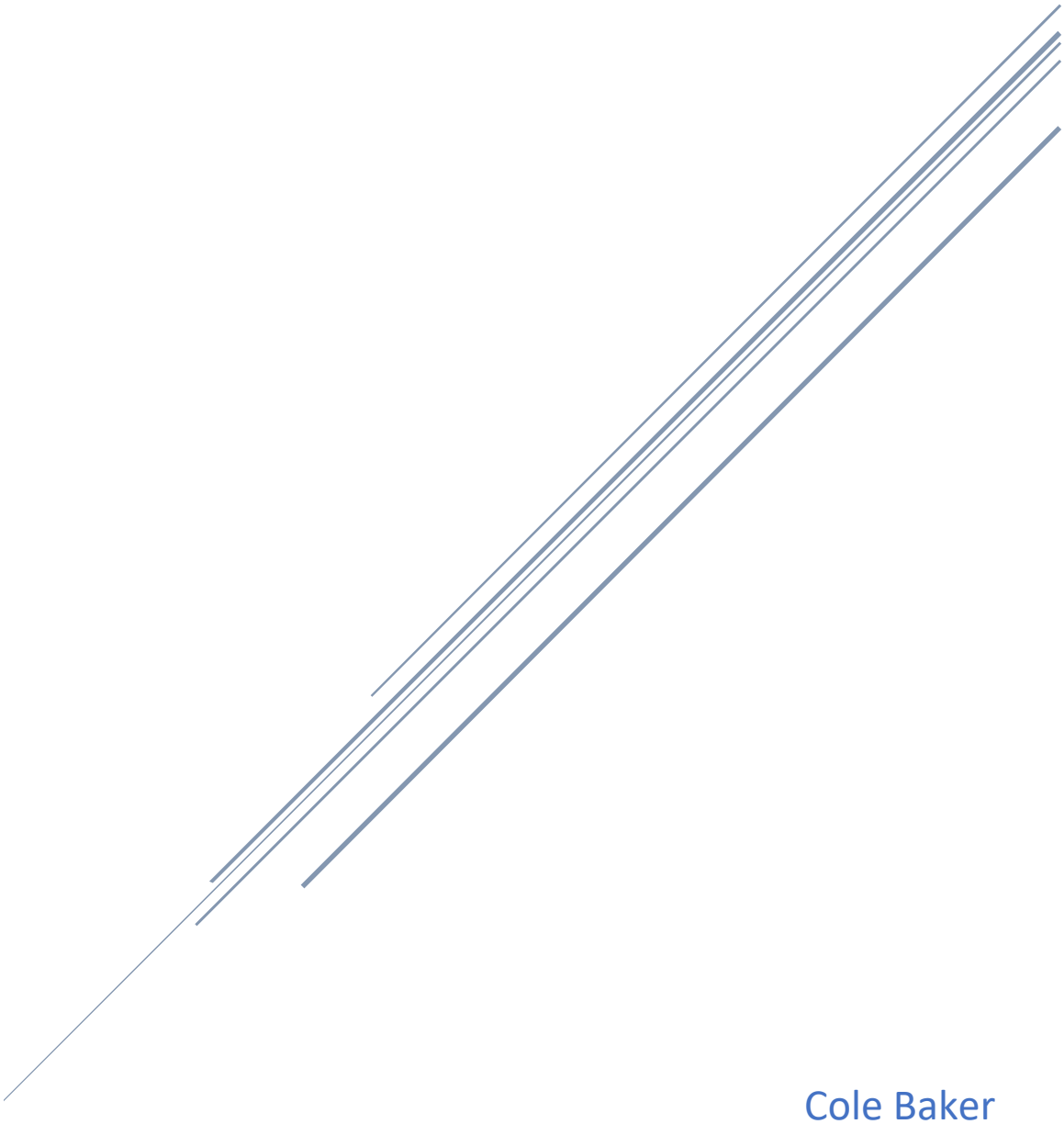
WLAN & APS TESTING PLAN



Cole Baker

Table of Contents

Introduction

This document outlines the steps and procedures needed to complete a full test of the critical systems of the provided Cisco Aironet 3700 AP device. The purpose of this document is to give a real work experience into how a potential employer may request a testing plan to be completed. Completing this assignment should provide insight into how these plans work and how to present one in a professional manner.

Task 1 – WLAN Plan

Section 1 – Initial Plan

The following testing plan laid out in "Task 2" will outline what steps need to be taken to test the features on the Cisco Aironet 3700 AP. The device will initially be configured to accept traffic for the means of testing the features of the Aironet 3700. During the configuration, the following features will be enabled. General Cisco ISO configuration, Wireless communication protocols, and general system settings. These feature together will be used for the successful operation and testing of the Aironet 3700. These features are along with a secure initial configuration (no default passwords), what most external operations would do in a real world production environment.

Section 2 – Planning Stage

The following plan must be approved by the appropriate authority before continuing with testing. The initial configuration must also be completed before any testing can be done. The Cisco Aironet 3700 AP must have the proper physical and environmental setup as defined. The device should be placed on a secure sturdy table with access to a wired ethernet jack and a DC outlet port. This work area should be located in the D wing of the NSCC IT Campus. After the physical AP is setup and running, the initial configuration referred to by "Section 1" above should be implemented. The overall goal of this testing plan is to ensure the correct functionality of the installed Cisco Aironet 3700. All steps have been documented and any changes should be recorded as defined below in the full testing plan located in "Task 2".

Section 3 - Implementation

This final section is implementing the testing plan along with the assistance of "Section 1" and "Section 2" to ensure the testing plan below is implemented correctly. The plan is to be followed step by step, this document must be approved prior to the use of it on the physical Cisco Aironet 3700. This is the most critical step of the initial testing plan due to the fact that this section only occurs when physical access to the Aironet 3700 is granted.

Task 2

Introduction

Setup, configuration and testing of a Cisco Aironet 3700 AP (AP) testing systems. The below will provide an overview of each step in setting up an AP device for proper testing. The goal of the outline is to guide in the configuration of the AP device, such as requirements, testing strategies and any risks associated. No action will be taken towards the physical AP device until the “WLAN & APS Testing Plan” document has been approved the appropriate authority.

Definitions

- “AP”, “AP device” : Cisco Aironet 3700
- “Document” : WLAN & APS Testing Plan Microsoft Word Document “Baker-Cole-ISEC2078-As3

Objectives and Tasks

1. Be granted access to the physical “AP” through approved “WLAN & APS Testing Plan” document.
2. Gather necessary hardware (see section “Hardware Requirements”) and access to production environment (see section “Environment Requirements”)
3. Begin physical setup of “AP device” such as connecting power supply and other physical wiring.
4. Power on “AP device” and begin initial start-up configuration (if approved to procced from task 3)

After completed and approved configuration

1. Refer to the “Document” for initial testing plan guidelines sections “Testing Strategies” & “Features to be Tested” & “Features not to be Tested”.
2. Initiate testing strategies to specifications of the “Document”.
3. Record all results of testing strategies, as well as any errors, warnings or miss configurations noticed from earlier configuration.

Scope

The scope of this document is restricted to the “AP device” as well as the adjoining network traffic going through the “AP device” for the purposes of testing and ensuring proper functionality of the “AP device”. The network traffic will differ based on the network the “AP device” is connected through to receive traffic. The scope of this report does not cover the deep inspection of the traffic through the “AP device” for the purposes of confidentiality. The above tasks will be completed as specified and all results and information received will be recorded into a “Testing Plan Report”

Document. As stated above, no action shall be taken until the “Document” is approved. Any and all changes made to the configuration must be recorded in the “Testing Plan Report”. The “AP device” is to be setup in the appropriate environment with the appropriate hardware and configured to the given or researched specifications.

Test Strategy

The “Document” shall cover the following when performing testing on the “AP device”. The strategy must be approved before any testing can be performed.

- Testing of the range of access and connection signal to the “AP device”.
- Testing of the capacity for users and application traffic passing through the “AP device”).
- Physical testing of the accessibility to the “AP device” (if applicable).
- **Important -** Testing of security protocols and setup of security infostructure for the “AP device” to ensure safe and secure traffic flow. (This testing is to be in depth due to the focus of security of this “Document”)
- Testing of traffic monitoring systems and logging systems for all connections through and from the “AP device”.
- Testing of analytical systems to assess performance of the “AP device”.
- Testing and review of any auditing or general policies in place on the “AP device” to ensure up to date policies.

Hardware Requirements

The physical hardware requirements for this “AP device” are as listed.

- Cisco Aironet 3700 AP
- 44 – 57 VDC DC Power Supply
- An Ethernet LAN Cable
- **For Testing and Configuration Purposes** – A console cable for connections to external device through remote terminal application such as Putty
- Remote device to establish external connection through such as a laptop or desktop pc with the appropriate connections opens

Environment Requirements

The environmental requirements for this “AP device” are as listed.

- A secure and climate controlled area to preserve the condition of the “AP device”
- A well-lit area with sufficient space for “AP device” to securely be placed with minimal chance of damage. As well an accessible DC outlet capable of providing the necessary power output required by the “AP device”
- An area with sufficient internet access to support the “AP device”

Testing Schedule

The “AP device” will use the below schedule to perform testing and reviewing of the “AP device”. This schedule may change or be modified based on access the “AP device” or another unpredictable variable. Additional columns can be added if needed for an extended plan which could occur with the addition of a new feature. The estimated time to complete the testing plan described above: 3 weeks

Test Number	Task	Type	Time
1	Initial Config Test	Test – Testing of the initial config to ensure correct starting config	Week 1
2	Physical Test	Test - Testing to ensure the environment is suitable for the “AP device”	Week 1
3	Starting Report	Report – Report that shows an overview of the two initial test	Week 1 Summary Report
4	Range and Capacity Test	Test – Testing of the range and capacity of the “AP device”	Week 2
5	Security Protocol and Audit System Test	Test – Testing of security protocols and auditing systems active on the “AP device”	Week 2
6	System Performance Test	Test – Testing of system status and system performance to make optimizations.	Week 2
7	System Status Report	Report – Report outlining system status of main features to ensure system functionality	Week 2 Summary Report
8	System Monitoring Test	Test – Testing of the traffic monitoring and logging system of the “AP device”. This will take place over a week to ensure a larger source of data to review	Week 3

9	System Monitoring Report	Report – Report and summary for monitoring system of the “AP device” and traffic monitoring	Week 3 Summary Report

Control Procedures

This section describes the system being used this “Document” to report errors and incidents during the testing process. All change requests must also follow this outline.

If an error, warning or another informational message appears or if information is needed to be reported. The format below will be used to document the following

- Warning, Alerts, Errors, Caution Notices or any error related (shall be marked as **Important** with bold) and should be marked with what the error type is.
- Information messages shall be tagged with INFO. Any messages that do not effect the operation of the “AP device”.

The following example and template must be followed to report any incidents, errors or informational alerts given. Refer to the above points to report incidents.

Template for Incident Reporting

- Date/Time – Incident Type – Incident Title
  Description of Incident

Example for Incident Report

- Oct, 11, 2019/11:30am – System Error – System Configuration Error
  System Configuration Error in initial configuration, system restart required, retry configuration.

Features to be Tested

The following parameters will be the features tested and covered by this “Document”. As each feature of the “AP device” is tested, the results must be recorded, as outlined by the section “Testing Strategy” listed above. As well as all incidents should be handled according to the above section “Control Procedure”. The list of parameters to be tested is as followed.

- Cisco ISO Configuration will be tested to ensure correct configuration.
- Wireless Communications to and from the “AP device” will be tested for range, capacity, and performance.

- All physical features of the “AP device” will be tested to ensure proper operation and functionality.
- All system settings of the “AP device” will be tested to ensure proper setting configuration to the specified requirements.

Features not to be Tested

The features and parameters listed below will not be tested or covered by this “Document”. These features may not be active on the “AP device” so they have no effect on the operation there for they will not be tested. If these features are tested unintentionally, this must be reported in the final testing report as stated above in the section “Testing Schedule”.

- No advanced features of the “AP device” will be tested.

Resources/Roles & Responsibilities

The following section outlines the responsibilities of every member related to this project. It will also outline their roles and any resources required by those said members.

- Cole Baker – Primary Tester/Configuration Lead – Duties include: Following the above “Testing Strategy” and “Testing Schedule” sections and producing a report or results from testing. And configuring the “AP device” from the initial stage to the final deployed configuration.
- To Be Determined – Executive Project Supervisor – Duties include: Reviewing this “Document” for the purposes of granting an approved Testing Plan to the Primary Tester.
- To Be Determined – Peer Reviewer – Duties include: Reviewing this “Document” for the purposes of signing off for pre-approval before submitting to the Executive Project Supervisor.

Dependencies

Due to the availability of the testing environment and the testing hardware, “AP device” testing is limited to approved and supervised use by the above defined Executive Project Supervisor. This “Document” must be approved by the appropriate authority before any testing may be set in place. Approved access to the required hardware and environment is necessary for the successful completion of this “Document. As well as a sufficient internet source with a flow of traffic for testing.

Risks/Assumptions

The following section will outline any risks that may be presented by this testing plan. If any these risks occur, the result, and the incident must be reported to the Executive Project Supervisor.

- Physical risk of damage - to the “AP device” such as fall damage during transportation, or accidental movement that may cause the device to fall from a high place.
- Misconfiguration – to the “AP devices” configuration setup to which could leave the “AP device” vulnerable to cyber attacks or failure of access or proper usage due to incorrectly configured features.
- Ignored Alert Messages – from the “AP device” maybe be accidently ignored, missed or not correctly documented which could point to an issue that may be overlooked.

The following section outlines a contingency plan in the event of a delay or unforeseen shift in scheduling. This will replace the original testing plan specified in the “Testing Schedule” section, only if there is a delay or unforeseen issue with scheduling access to the “AP device”.

Test Number	Task	Type	Time
1	Range and Capacity Test	Test – Testing of the range and capacity of the “AP device”	Week 1
2	Security Protocol and Audit System Test	Test – Testing of security protocols and auditing systems active on the “AP device”	Week 1
3	System Performance Test	Test – Testing of system status and system performance to make optimizations.	Week 1
4	System Monitoring Test	Test – Testing of the traffic monitoring and logging system of the “AP device”. This will take place over a week to ensure a larger source of data to review	Week 1

5	System Monitoring Report	Report – Report and summary for monitoring system of the “AP device” and traffic monitoring as well as range and capacity, security and auditing protocols, and performance	Week 1 Summary Report

The above contingency schedule has been condensed into one week in the event of delay or other unforeseen issues. This schedule has been condensed by eliminating the initial testing sections of the original Testing Plan. Physical and Initial Configuration testing has been moved.

Tools

The below section is a list of tools required to complete the testing plan, these tools can be modified for a similar tools as long as that tool is recorded in the change report as specified in the “Control Procedure” Section.

- Putty SSH Client
- https://fast.com/ Wi-Fi speed testing site
- Desktop PC or Laptop with required IO ports

Approvals

The following section includes information of proof for all approvals provided for this “Document”.

Peer Reviewer Approval (See below Peer Reviewer Feedback)

Printed Name	Signature	Date
_____	_____	_____

Executive Supervisor Approval

Printed Name	Signature	Date
_____	_____	_____

References

Cisco. (2018). *Cisco Aironet 3700 Series Access Points*. Retrieved from Cisco: https://www.cisco.com/c/en/us/products/wireless/aironet-3700-series/index.html