



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at <http://www.giac.org/registration/gsec>

Look who's listening

Rogue Access Point Detection with Nortel's 2200 Series Wireless System

Richard Sillito
08/17/04

© SANS Institute 2004, Author retains full rights.

Table of Contents

Abstract	3
Introduction	4
How does WiFi work?.....	4
Under the hood of an access point.....	5
Introduction to some wireless standards	6
802.11.....	6
802.11b.....	6
802.11g.....	6
802.11a.....	6
ISM and U-NII.....	7
Are Wireless Access Points great because they're so easy to install?.....	7
What is a Rouge/Free Agent Access Point?	8
Wait a minute, what is an Access Port and why is it different than an Access Point?	8
Nortel 2200 WiFi System.....	9
Installation of Equipment	11
Configuration and Mapping.....	12
Installation of the Rogue Access Point	22
Detection of the Rogue AP	22
Results.....	25
Conclusion	26
References.....	27

Abstract

Wireless communications continues to show more and more penetration into our everyday lives. We continue to see wireless networks showing up at hospitals, schools and business. The nature of wireless communications, reaching out beyond the physical boundaries, means that the deployment and administration of Access Points is critical to the security of the network as a whole.

The Access Point has long been considered the gateway which brings wireless devices such as computers, laptops, PDAs, etc. on the network. Being the gateway, network designers use these devices to allow access and protect the network from unauthorized access. With only weak standards and having never been built with security in mind, the Access Point has very much failed. This forced network designers to look elsewhere for devices to place between the Access Points and the network, devices such as firewalls, VPN, etc. These devices were designed with security in mind, but not wireless. Is it any wonder securing wireless networks is such a challenge? One such challenge is Rogue Access Point detection. Listening in on your network, even joining in, these Rogue Access Point can attach themselves to legitimate Access Points or wireless devices and start controlling communications.

As always, there is hope, two new technologies have arrived on the scene Wireless Security Switches and Access Ports. Access Ports are gateways designed with security in mind and Wireless Security Switches are firewalls designed with wireless in mind. Finally defense in depth is possible even in the WiFi world. Also the combination of Wire Security Switches and Access Ports now allows for Access Ports to work together, as a team of devices, allowing for the strategic identification and possible containment of Rogue Access Points.

© SANS Institute

Introduction

When Nortel first approached me to look at their Nortel 2270 Wireless Security Switch and their Nortel 2230 Access Ports, I was very interested to try them out. My background as a Technology Analyst and now Security Analyst caused me to cross paths with WiFi technologies on several occasions in my 11 year career in IT. During these brushes with the WiFi world, I was always left with the feeling that technology had failed in establishing a balance between manageability, security, and usability. It was refreshing to see how new WiFi technologies such as Wireless Security Switches and Access Ports, have made huge advances towards this balance.

In order to fully understand these advances I take you through some of the more technical aspects of WiFi but don't worry I'll keep it light. I start with a simple description of how WiFi works and move on to traditional Access Points. From there I cover off some of the standards that apply in the WiFi world (don't worry it will be quick and painless I promise). Then I cover some of the dangers around Access Points and WiFi in general, at this point I define Rogue and Free Agent Access Points. After completing that I talk about Access Ports and their advantages. Finally, I take you through my test of the Rogue Access Point detection feature of the Nortel 2200 series WiFi system.

How does WiFi work?

WiFi as it is often referred to, is technically referred to as 802.11 network or simply wireless networking. It is a network that is established between two or more computers that uses wireless signals traveling through the air. Here is a simple example that will help you understand how wireless networks work. [1] Think about the wireless radios that the average family buys for the ski trip to the mountains. These radios have a couple of hardware components inside, an antenna (to send and receive the signals) an encoder (which converts voice to radio signals) and a decoder (which converts radio signals back to voice). When you use your radio you click the talk button, this tells the device to listen to your voice, encode your voice into radio signals, and transmit the radio signals using the antenna. Then the signals are sent into the air, where the other radio uses its antenna to pickup the signals, decode the signals and convert them back to voice. It then plays the voice on a speaker built into the radio. Once the message is heard in its entirety, the operator then clicks their talk button and starts to the whole process again. Thus responding to the message received.

As kids we quickly realized that these signals where sent out into the air without any thought as to where they should be going. As a result we were able to listen in on other people's conversations. Of course the next step was to interrupt the

conversation, maybe even pretend to be the person they were talking to. Little did we know we were forming the basis for hacking wireless networks.

But enough reminiscing, let's get back to the subject at hand. How does all this wireless radio talk apply to the WiFi computing of today? Well surprisingly enough, it is quite similar. The computers are equipped with a card called a wireless network adapter. This adapter combined with the driver, takes the data streams (1's and 0's) and converts them into radio signals, then transmits these radio signals into the air via an antenna. The other device, usually a wireless access point (wireless routers are simply an access point and a router combined) receives the signals via its antenna, then converts the radio signals back to a data stream (1's and 0's). Once the signals are back to a data stream, the data stream is then placed on the regular network where it is handled the same as any other network traffic.

Looking back to tricks that we played as a kid, we can see how wireless networks are not without their risks. Simply adding another wireless workstation, or wireless Access Point, we can listen to the radio signals floating in the air. We can also interrupt the conversations with our own signals; even pretend to be someone we are not! Scared yet, well maybe you should be. This is why it is so important to detect unauthorized wireless equipment on our network.

Under the hood of an access point

All of this makes sense for two people who are talking on a couple of radios, but what about many computers perhaps hundreds of computers all trying to maintain conversations. Obviously we can't have that kind of mayhem or a message would never get sent or received. As was the case of earlier networks, networking equipment needs to play a part in the game. To do this WiFi had to become simply an extension of the current Local Area Network or LAN. In order to provide this extension to many WiFi users the concept of an Access Point was invented. To put it simply an Access Point or AP is the point at which many wireless users can gain access to the LAN.

The early AP's were layer 2 devices, this meant that the device understood little to nothing about the packets it sent or received. The AP simply converted the medium from air to wire. The WiFi world found it important that the traffic being sent through the air be on the public band frequencies as their objective was to make WiFi simple and relatively inexpensive. Of course to ensure interoperability with different WiFi vendors it was important to develop some standards (one is never enough). Although there are many WiFi standards today, 4 stand out as the most common: 802.11, 802.11b, 802.11g, and 802.11a.

Introduction to some wireless standards

Although there are many components of the 802.11 standards we will keep it simple with information such as the radio band, date of introduction and data rates:

802.11

First introduced as a standard by the IEEE in 1997, it had three physical layers: Frequency Hopping Spread Spectrum (FHSS) at 2.4 GHz, Direct Sequence Spread Spectrum (DSSS) at 2.4 GHz or Infrared. It had relatively low data rates of 1 or 2 Mbps and interestingly enough the FHSS equipment is still compatible with the more current 802.11b and 802.11g.

802.11b

First introduced as a standard by the IEEE in 1999, it used DSSS at 2.4 GHz. This protocol was able to automatically select a data rate of (1, 2, 5.5 or 11 Mbps) based on signal strength. 802.11b is often referred to as the de facto standard as millions of devices have been produced to this standard and affordable pricing will likely help to keep it in the market place for the near future. Because of its good coverage and reasonable data rates it is considered the “good enough” network protocol for wireless networks.

802.11g

First introduced as a standard by the IEEE in 2003, this standard is much like its predecessor 802.11b only faster. The physical layer of the protocol uses Orthogonal Frequency Division Multiplexing (OFDM) at the 2.4 GHz but can also fall back to DSSS to maintain backwards compatibility with 802.11b. OFDM at 2.4GHz allows 802.11g users the 54 Mbps with same great range that 802.11b offered. The higher data rates and backwards compatibility lead many to believe this standard has a great future ahead of itself.

802.11a

First introduced as a standard by the IEEE in 1999, this standard is sometime referred to as the Betamax of the wireless world. Although it is technically sound its lack of backward compatibility has led it to have little acceptance in the wireless world. This protocol uses Coded Orthogonal Frequency Division Multiplexing (COFDM) at 5 GHz for its physical layer. COFDM at 5 GHz meant

that sending data could be done in a massively parallel fashion. This made it the first 802.11 standard to achieve 54Mbps, unfortunately because it used the 5 GHz band it was incompatible with everything and ran a shorter distance than the more traditional 2.4 GHz devices. Many say that this will be its downfall. All that said if you're looking for short range, high throughput with little frequency contention and noise, 802.11a provides a cost effective solution.

For a list of these standards and some others you may not be aware of, you can visit <http://www.computerhope.com/jargon/num/80211.htm> [2].

ISM and U-NII

When looking at the 802.11 standards, listed above, you will see that they operate in either the 2.4 GHz or 5 GHz band range. This is no coincidence! These frequency ranges are governed in North America by both the Canadian Radio-television and Telecommunications Commission (CRTC) and the Federal Communications Commission (FCC). These organizations list these bands as Industrial Scientific and Medical (ISM) and Unlicensed National Information Infrastructure (U-NII), both of these bands are unlicensed radio bands.

For more detailed information about these standards and physical media used in 802.11 standards visit <http://www.informit.com/articles/article.asp?p=31731&seqNum=4> [3].

Are Wireless Access Points great because they're so easy to install?

Unlicensed radio bands were used in WiFi equipment to make the establishment of WiFi networks easy. If WiFi was to be adopted by the masses it had to be free of the process and cost of licensing a frequency in a given area. Of course the frequency was just one issue, the hardware had to be easy to install. Manufacturers did everything they could to make WiFi equipment easy to install, turning off security, allowing any client to connect, they even went so far as to self configure the clients to get onto your network. Even today many people are installing WiFi in their own home without understanding the security impact. Luckily the average home is not an attractive target for hackers. However, here comes a very real threat, the same person who unwittingly installs an unsecured WiFi network in their house can also install an Unauthorized Access Point on your network. I know what your thinking, does this really happen? Not only does it really happen but it happened in the very company I work for. Luckily it was discovered before incident. Like our network, most networks are not equipped with the proper port security or possess the required equipment to detect such activity, so this may be happening to you today and you may be totally unaware.

What is a Rouge/Free Agent Access Point?

An Unauthorized AP on your network is referred to as a “Free Agent Access Point”. These AP’s, having not been installed by your network team, are often installed without the appropriate security precautions. Because they are behind the firewall and not properly secured they become a hackers dream. Now the hacker “midnight parkers” can pull up in your parking lot, at night when life is quiet, and slowly work on the AP and once they’re in they’re right into your network!

This is not the only type of Unauthorized AP you have to be concerned about. Injection and man in the middle attacks are becoming more and more popular in the WiFi hacking world. Often these are performed from an AP that is within the WiFi range but not connected to your wired network. These AP are referred to as “Rogue Access Points”. The objective here is for the attacker to get their AP accepted into the wireless infrastructure, thus allowing them to either see or inject traffic.

It is interesting to note that most discussions around wireless security are focused on authentication and confidentiality. As an IT community we appear to be concerned about who is accessing our wireless network and ensuring people don’t know what we are sending. But we are perfectly willing to let them listen. Perhaps this is due to the continuation of the wired world mentality where physical boundaries lead us to a false sense of security. We must never forget wireless is about breaking the physical boundaries!

For a more detailed article on Rogue Access Points and alternate ways to identify them check out this article <http://www.wi-fiplanet.com/tutorials/article.php/1564431> [4].

Wait a minute, what is an Access Port and why is it different than an Access Point?

We have kept the discussion of an AP to a fairly simple level, discussing only its radio qualities. However, most APs have more “smarts” than just a simple radio. Apart from handling the WiFi network it also handles any WiFi security that has been enabled. The fact that these devices work independently of each other introduces possible security problems. The incorrect deployment of an AP can be difficult to detect and therefore security could be compromised. Also the administration of many APs can become daunting. Image an implementation where 100’s of APs need to have the WEP key updated. The WiFi world was looking for something simpler that would help enforce security. Hence was born

the Access Port, basically they took everything out of the AP except the radio and a little network smarts and gave the Access Ports a common device that they could share, one that held all the smarts they were missing. These new devices are referred to as Wireless Security Switches. The beauty of this is two fold, from an administration perspective when an Access Port is installed on the network it won't work until it talks with the Security Switch. Typically once it has established this connection it is self configured before the device accepts traffic. From a security perspective the advantage is the Access Ports are usually forced to adhere to the security policies enforced by the Security Switch. On top of this, since all Access Ports are reporting to one device, now there is the opportunity to watch for malicious traffic, much like a firewall gave us a central point to perform security operations.

Nortel 2200 WiFi System

Let's look at how all this ties into the Nortel 2200 WiFi system. The system that I used for this demonstration used a Nortel 2270 Security Switch with the Nortel 2230 Access Ports, managed by a Dell 1650 server loaded with Nortel's Adaptive Solution software.

To view Nortel's product literature visit

<http://a752.g.akamai.net/7/752/5107/20040712180955/www.nortelnetworks.com/products/01/wlan/collateral/nn103962-022704.pdf> [5].

What Nortel has done is made a Security Switch that works with VLANs using 802.1q tags. This allows the network administrators the ability to create their Wireless infrastructure either on an independent network or a VLAN contained within their existing network. It works with either Layer 2 or Layer 3 VLANs, although the self discovery isn't as cool when using Layer 3. The system was easy to install, you simply setup the VLANs on your network, then configure the Nortel 2270 with the appropriate VLANs and then connect it via the Fiber Connection. At this point it is integrated with your network. Then you configure your wireless settings, SSIDs (which are then associated with VLANs), Security Settings, Radios, etc, this can be done via https directly to the Security Switch or through Nortel's Adaptive Solution software loaded on a server on your network. The next step is to configure the switch port in your existing network, where the Access Port will be connected, with the correct wireless infrastructure VLAN and plug in the Access Port. The Access Port will then discover the Security Switch and register itself. At this point the Security Switch checks the flash and updates it if required. The next step the Security Switch configures any required settings on the Access Port and finally the Access Port comes alive and starts to accept traffic. I was concerned that Nortel had made it too easy. Nortel was quick to note the answer is in the administration of the VLAN, an Access Port can only discover the Security Switch if it is on the same VLAN. Therefore as long as network administrators are controlling which ports on the network are assigned to

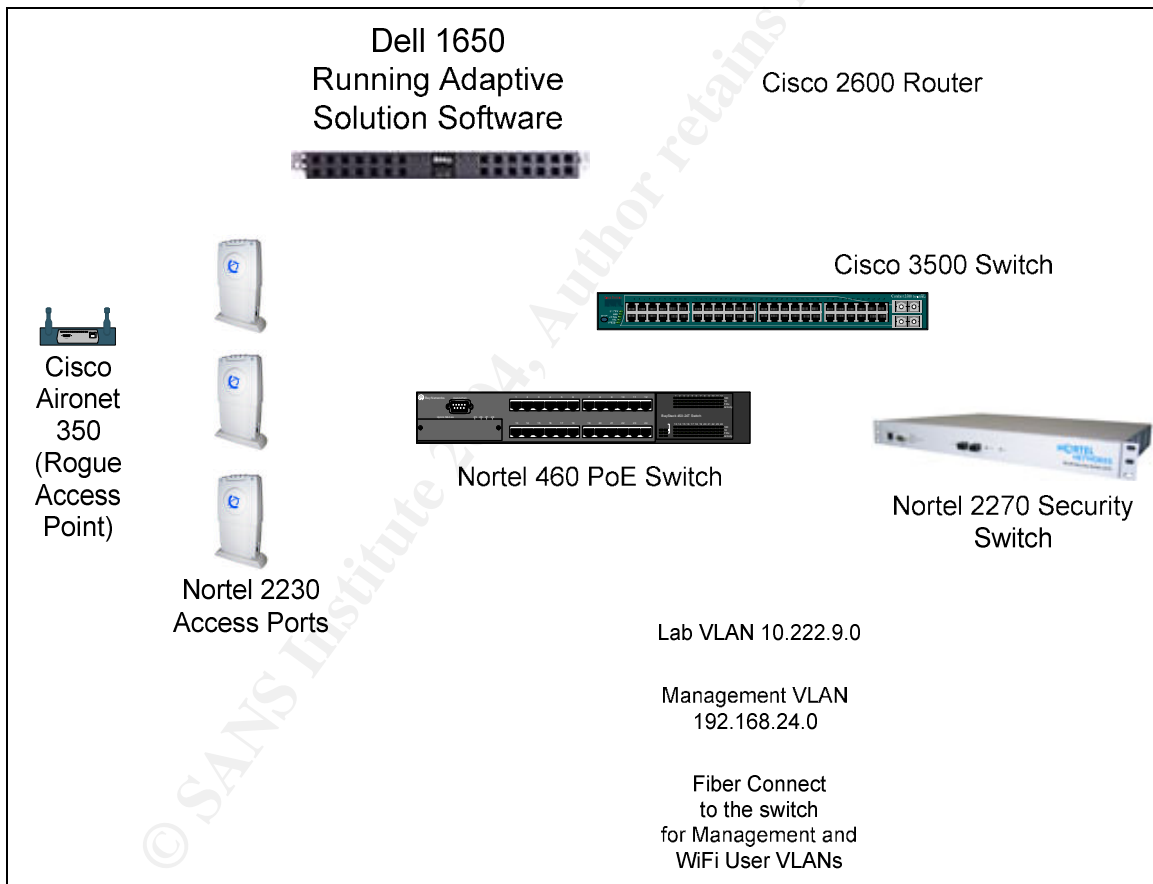
the VLAN for the wireless infrastructure (typical practice for network administrators) then ease of installation reaches a balance with security.

The next step is to teach the system where in the building your Access Ports are using the Adaptive Solution software. To be honest Nortel recommends that you do the following step before you install the Access Ports, as the software has the ability to do site planning. As this was not a requirement of the paper, I simply installed the Access Ports and told the software where they were. Now the system is set to detect the Rogue AP's.

© SANS Institute 2004, Author retains full rights.

Installation of Equipment

- Cisco 2600 Router (Not really require in this exercise but was part of the lab configuration)
- Cisco 3500 Switch with 2 VLAN configured
- Nortel 2270 Wireless Security Switch
- Nortel 460 PoE Switch (This was only included because our Switch did not support Power over Ethernet, otherwise we could have used the Cisco Switch)
- Nortel 2230 Access Ports
- Cisco Aironet 350 Access Point (Rogue Access Point)
- Dell 1650 Running the Adaptive Solution Software



Configuration and Mapping

Before getting started I requested our network team confirm the Cisco 2600 Router was configured for my lab network. This was the configuration that was in the router:

```
interface FastEthernet0/0.850
description ** HG LAB Primary Server LAN **
encapsulation dot1Q 850
ip address 10.222.9.1 255.255.255.0
```

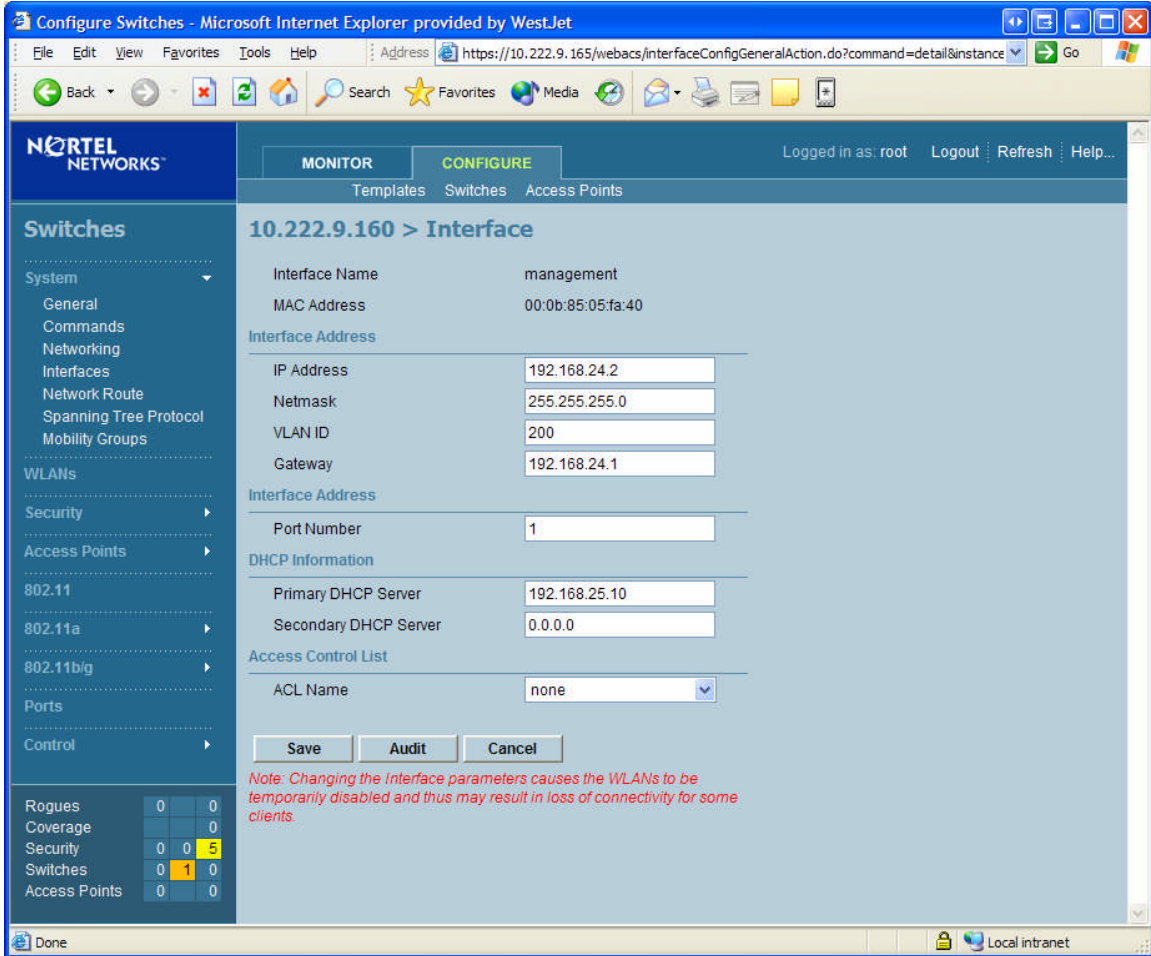
Then I requested setup of the interface connecting the lab router to the Cisco 3500 switch. Also I requested two VLANs in the Cisco 3500 Switch. The following is what was configured:

```
interface VLAN850
ip address 10.222.9.3 255.255.255.0
no ip directed-broadcast
no ip route-cache
```

```
200 VLAN0200          active Fa0/9, Fa0/24
300 VLAN0300          active Fa0/10
```

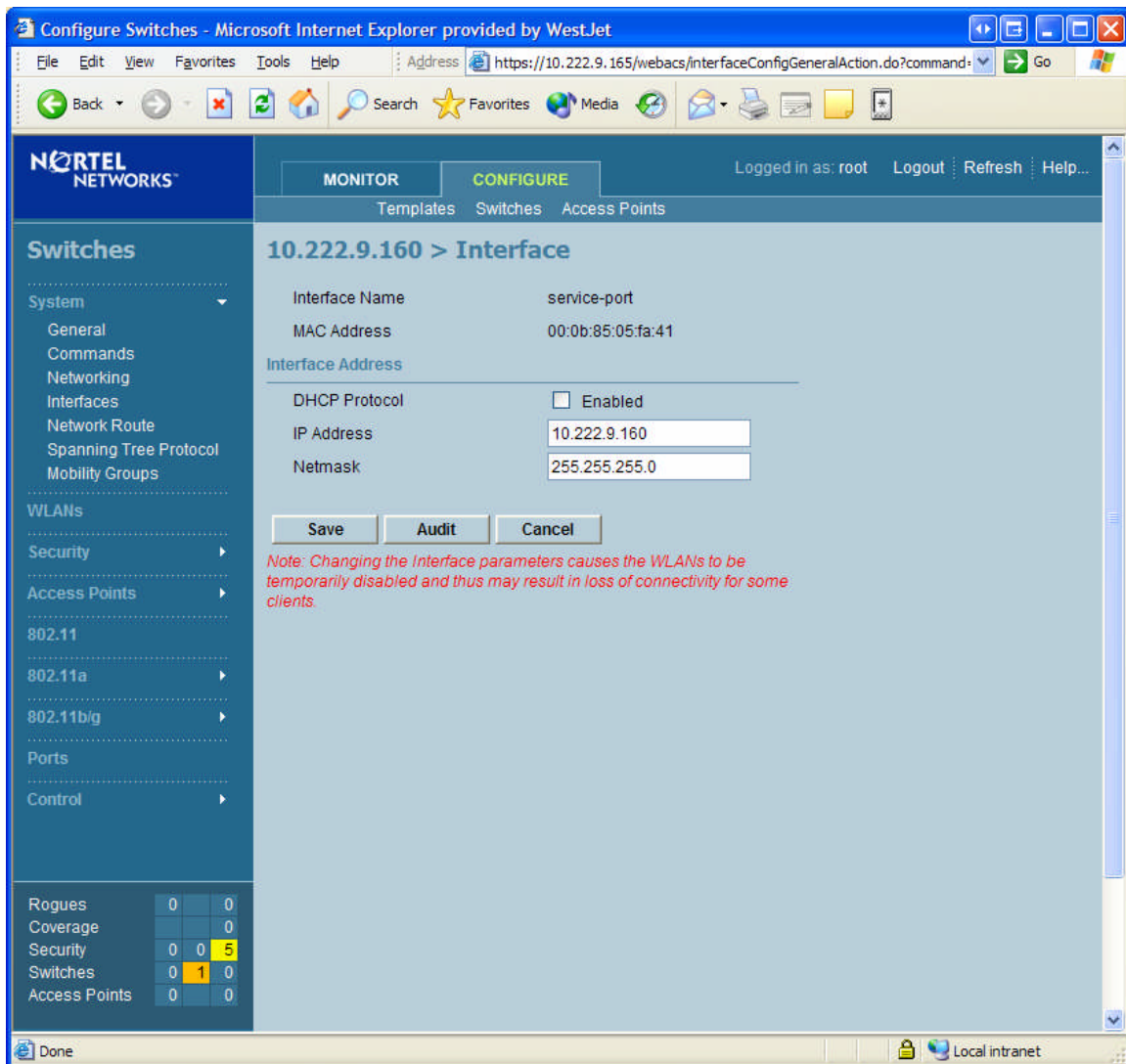
© SANS Institute 2004, Author retains full rights.

This covered the configuration of the existing infrastructure, next I moved on to configuring the Nortel 2270. I started by configuring the following Management interface. This interface is used for layer 2 communications between the Security Switch (Nortel 2270) and the Access Ports (Nortel 2230).



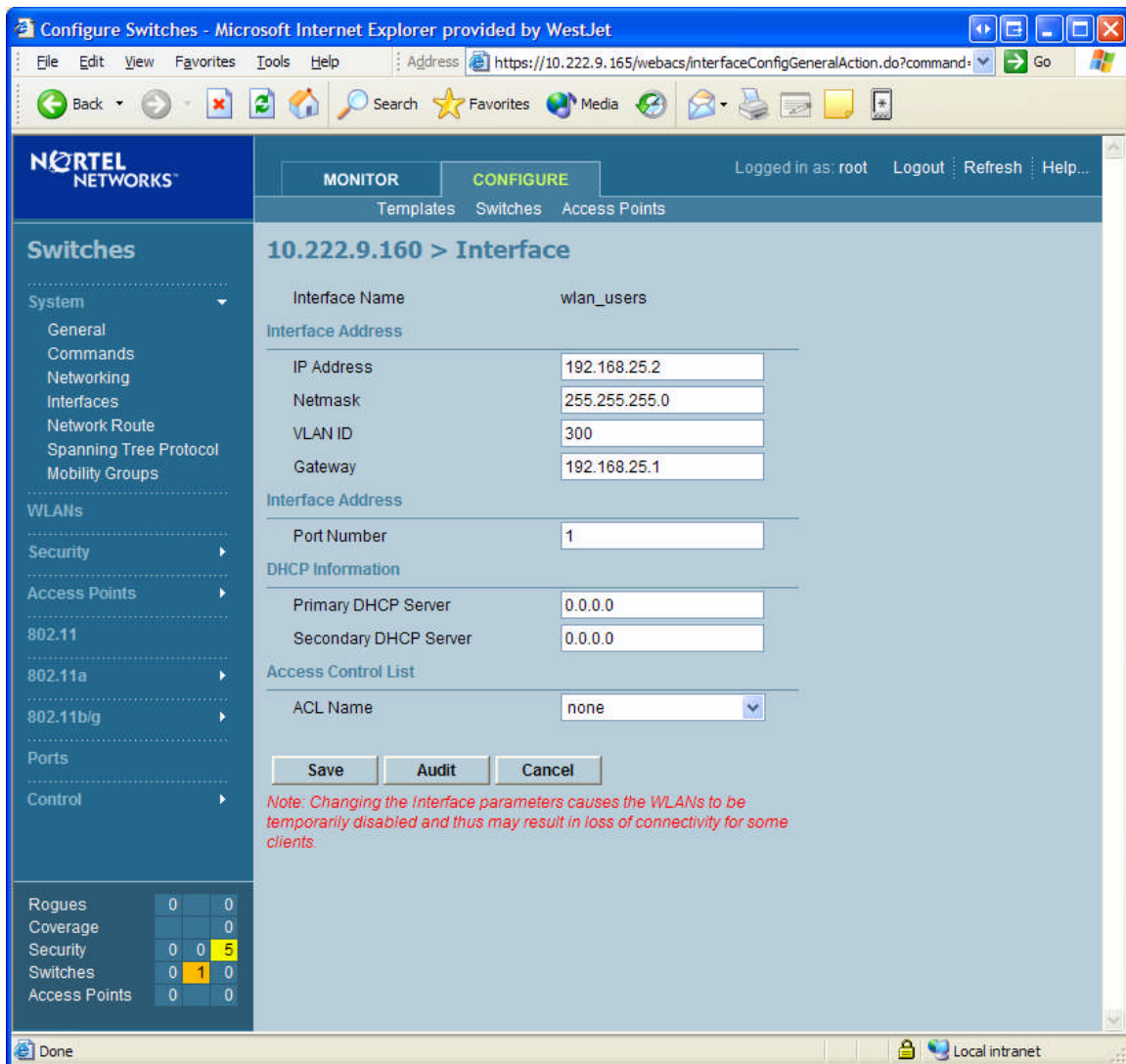
© SANS Institute

Next I configured the Service Port. The Service Port is a separate physical port on the front of the Security Switch and is used to configure and manage the Nortel 2270.



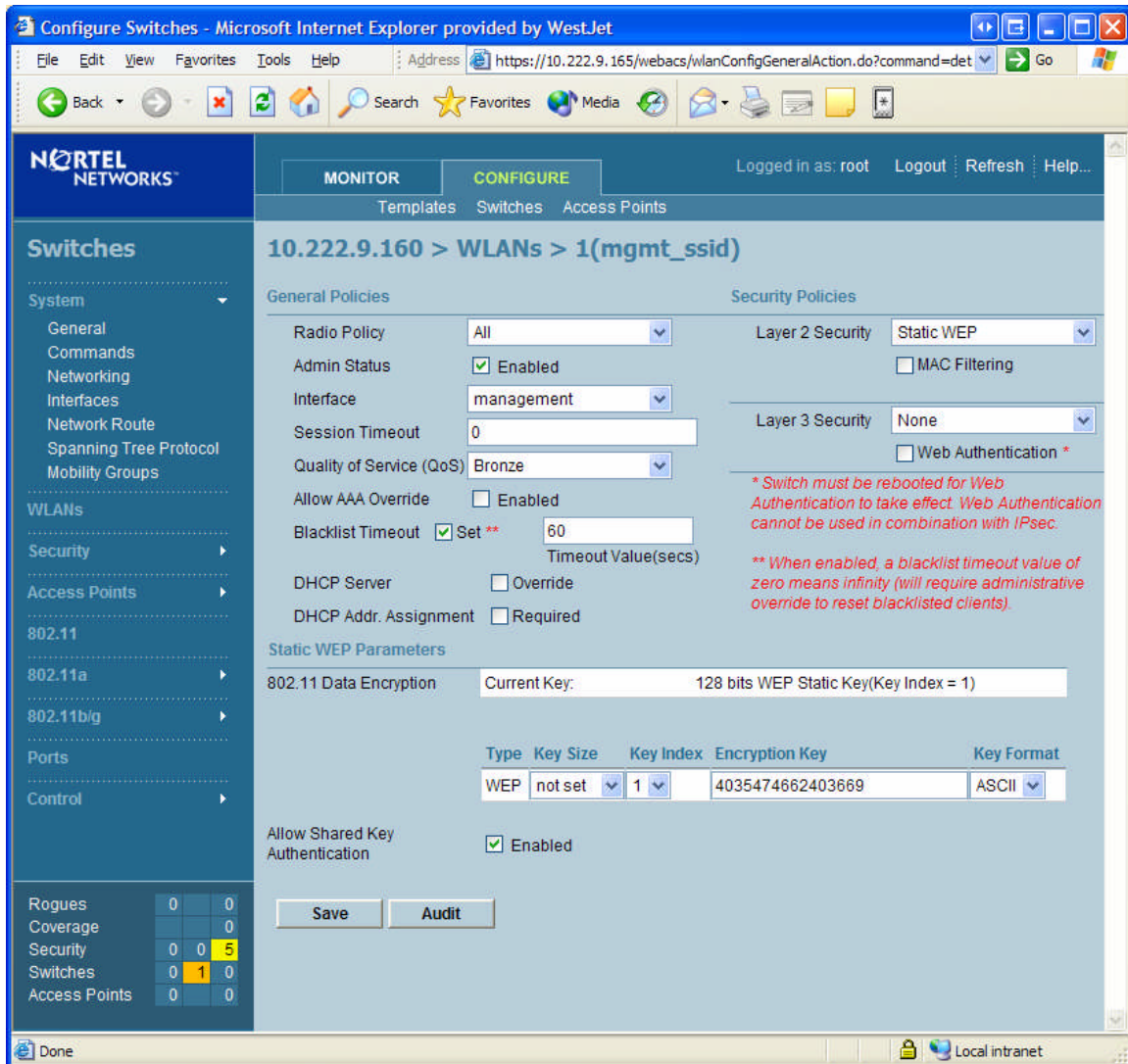
© SANS

Next I setup a wireless user's interface. The wlan_users is an interface configured for the WiFi communications. This would be the network that WiFi devices would exist in.



© SANS

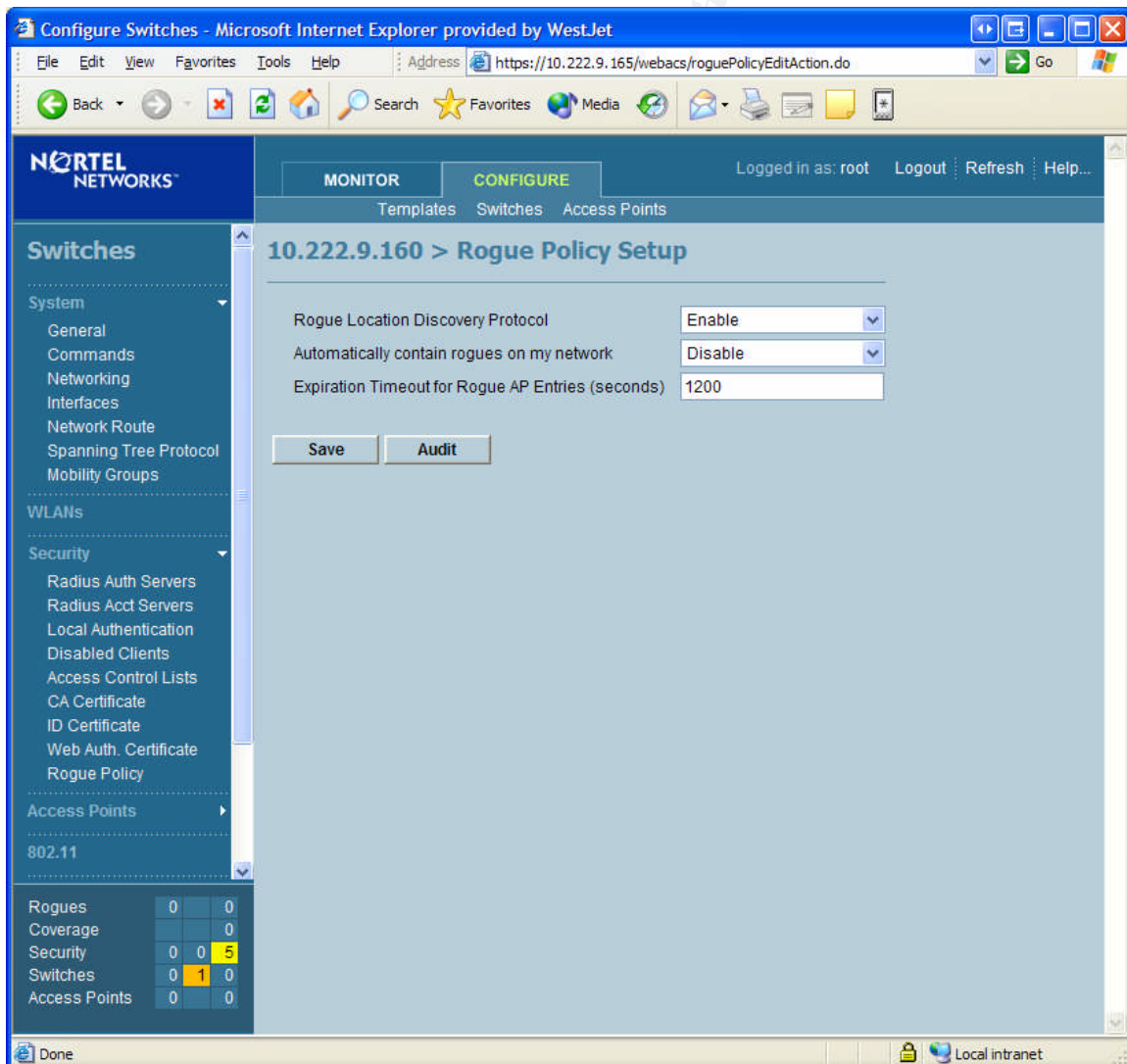
Next I setup the Service Set Identifier (SSID), simply put, the name of the wireless network. I chose the name mgmt_ssid, then configured it with WEP 128 bit, and assigned a WEP Key.



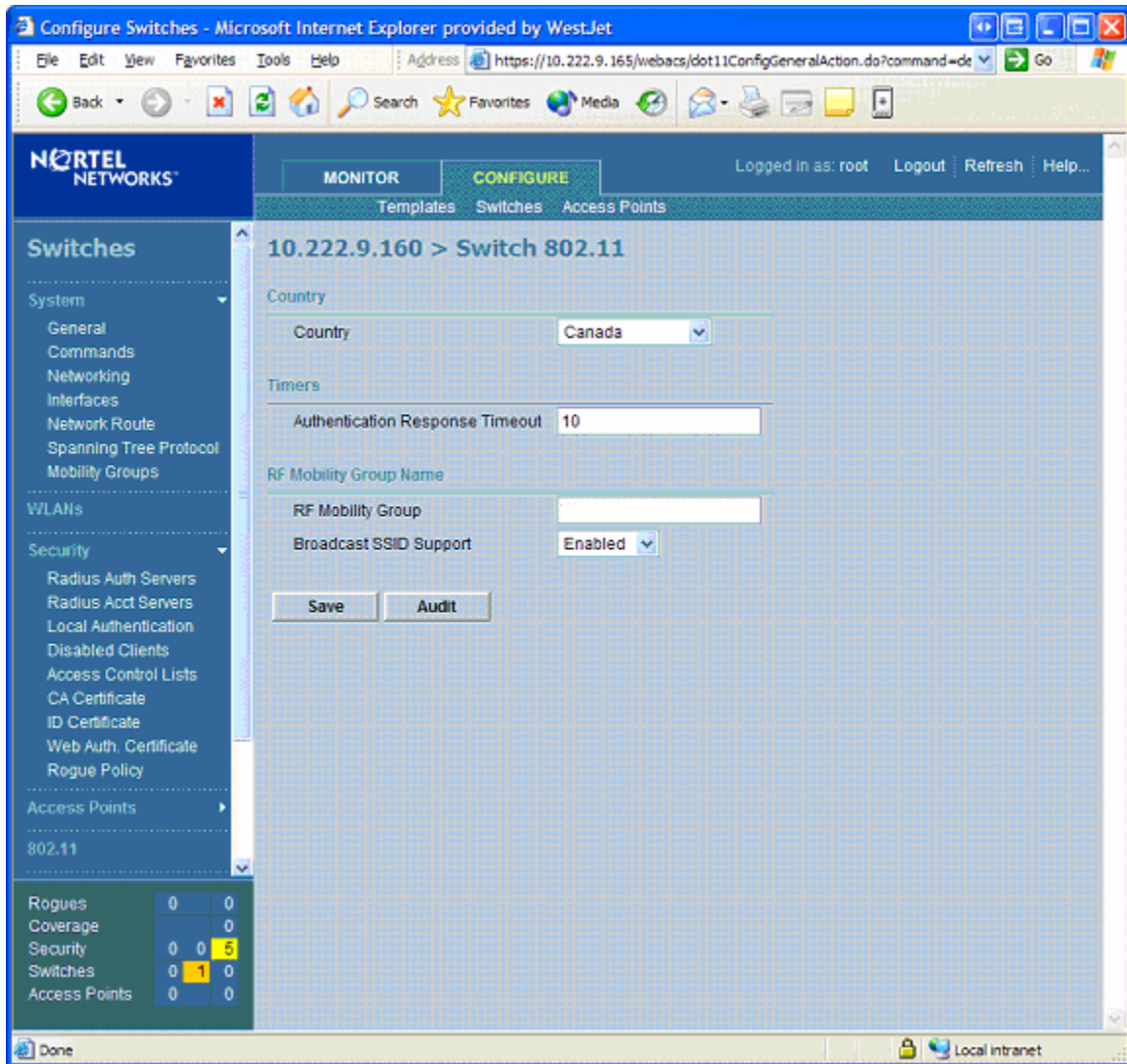
© SANS

Next I set the Rogue Policy. Here I enabled Rogue Location Discovery Protocol, although this it was not required by this particular test. This option tells the Access Ports to attempt to acquire an address on the Rogue AP and then attempt to find that address on the management interface. If it finds the address then the alert level is raised as this Rogue AP has been identified as a Free Agent.

I chose to shut off automatic containment for two reasons. Firstly, because it was not required by this test, secondly this feature can be risky. When a Rogue AP is contained the Nortel 2230 Access Port steals the Rogue AP's MAC address. It then sends out a broadcast disassociate command, using the Rogue AP's MAC address. This causes any clients connected to the Rogue AP to disconnect themselves. If this sounds like a sort of denial of service attack, that's because it is. If you were to detect an unidentified Access Point that was servicing a nearby business and then contain the AP, it could be misconstrued as an attempted DoS attack.



Next I configured the radio setting. We enabled all four physical access protocol's 802.11, 802.11b/g, 802.11a.



© SANS

Configure Switches - Microsoft Internet Explorer provided by WestJet

Address: https://10.222.9.165/webacs/dot11aConfigGeneralAction.do?command=c

MONITOR CONFIGURE

Templates Switches Access Points

Logged in as: root Logout Refresh Help...

Switches

System

- General
- Commands
- Networking
- Interfaces
- Network Route
- Spanning Tree Protocol
- Mobility Groups

WLANs

Security

- Radius Auth Servers
- Radius Acct Servers
- Local Authentication
- Disabled Clients
- Access Control Lists
- CA Certificate
- ID Certificate
- Web Auth. Certificate
- Rogue Policy

Access Points

802.11

Rogues	0	0
Coverage		0
Security	0	0 5
Switches	0	1 0
Access Points	0	0 0

10.222.9.160 > 802.11a Parameters

General

802.11 a Network Status Enabled

Beacon Period (millisec)

Template Applied 802.11aConfig_1

802.11a Band Status

Low Band Enable

Medium Band Enable

High Band Enable

802.11a Power Status

Dynamic Assignment

Current Tx Level

Control Interval (sec) 600

802.11a Channel Status

Assignment Mode

Update Interval (sec) 600

Avoid Foreign AP Interference Enabled

Avoid Nortel Networks WLAN AP Load Enabled

Avoid non 802.11 Noise Enabled

Signal Strength Contribution Enabled

Data Rates

6 Mbps	Mandatory
9 Mbps	Supported
12 Mbps	Mandatory
18 Mbps	Supported
24 Mbps	Mandatory
36 Mbps	Supported
48 Mbps	Supported
54 Mbps	Supported

Save Audit

Done Local intranet

© SANS Ins

Configure Switches - Microsoft Internet Explorer provided by WestJet

Address: https://10.222.9.165/webacs/dot11bConfigGeneralAction.do?command=c

MONITOR CONFIGURE

Templates Switches Access Points

Logged in as: root Logout Refresh Help...

Switches

System

- General
- Commands
- Networking
- Interfaces
- Network Route
- Spanning Tree Protocol
- Mobility Groups

WLANs

Security

- Radius Auth Servers
- Radius Acct Servers
- Local Authentication
- Disabled Clients
- Access Control Lists
- CA Certificate
- ID Certificate
- Web Auth. Certificate
- Rogue Policy

Access Points

802.11

802.11a

Parameters

Rogues	0	0
Coverage	0	0
Security	0	0
Switches	0	1
Access Points	0	0

10.222.9.160 > 802.11b/g Parameters

General

802.11 b/g Network Status Enabled

802.11g Support Enabled

Beacon Period (millisec)

Short Preamble * Enabled

Template Applied 802.11bConfig_1

Data Rates

1 Mbps	Mandatory
2 Mbps	Mandatory
5.5 Mbps	Mandatory
6 Mbps	Supported
9 Mbps	Supported
11 Mbps	Mandatory
12 Mbps	Supported
18 Mbps	Supported
24 Mbps	Supported
36 Mbps	Supported
48 Mbps	Supported
54 Mbps	Supported

802.11b/g Power Status

Dynamic Assignment

Current Tx Level

Control Interval (sec) 600

802.11b/g Channel Status

Assignment Mode

Update Interval (sec) 600

Avoid Foreign AP Interference Enabled

Avoid Nortel Networks WLAN AP Load Enabled

Avoid non 802.11 Noise Enabled

Signal Strength Contribution Enabled

* Switch must be rebooted for new value to take an effect

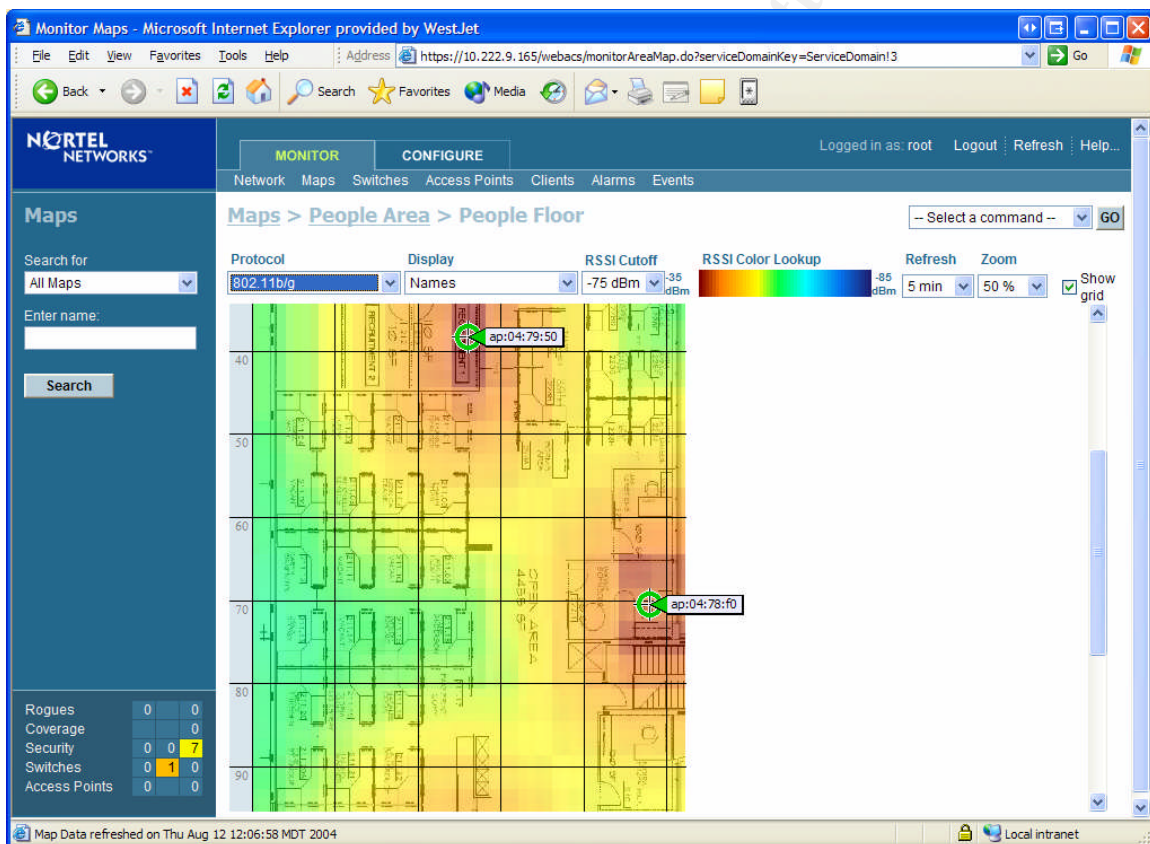
Save Audit

Done Local intranet

© SANS Ins

At this point I plugged in the Access Ports (Nortel 2230). This was the truly an enjoyable part, because all of the settings are enforced from the Security Switch (Nortel 2270) I simply had to plug in the Access Ports and watch them. First it discovered the Security Switch, then it automatically installed the latest firmware, next it downloaded any configuration settings that were required and presto it was configured and working. Hats off to Nortel for making life easy while still maintaining security.

Then I assigned these Access Ports a location on the floor. This step could have been done before placing the Access Ports as the Nortel software does predictive coverage calculations that would be useful in planning wireless installation. It also closely follows a concept called minimal site survey installations, which I don't go into in this paper but is well worth researching.



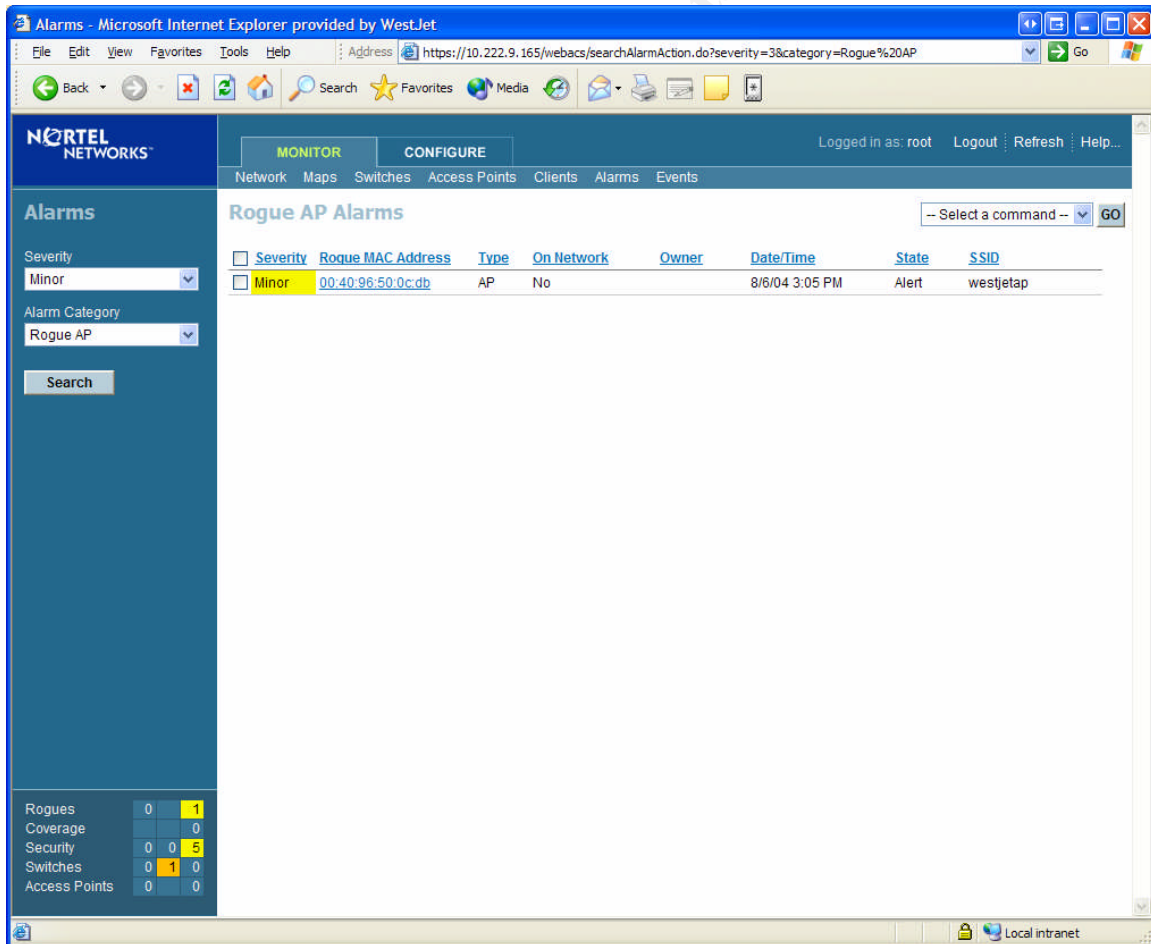
Installation of the Rogue Access Point

Once the Access Ports were up and working I moved onto installing a Rogue AP. A Cisco Aironet 350 was selected for the test. I configured it with WEP 128 bit security and plugged it in as a true Rogue AP (not connected to the test network).

Detection of the Rogue AP

Looking at the figure below, a “1” appeared in the bottom left hand corner beside the rogue section. Clicking on the “1” brought us to the Rogue AP Alarms list.

At this point I clicked on the Rogue MAC address which brought me to the next window.



The screenshot shows the Nortel Networks Alarms interface in a Microsoft Internet Explorer browser window. The browser address bar shows the URL: <https://10.222.9.165/webacs/searchAlarmAction.do?severity=3&category=Rogue%20AP>. The interface is titled "Alarms" and includes a navigation menu with "MONITOR" and "CONFIGURE" tabs. The "MONITOR" tab is active, and the "Alarms" section is selected. The "Rogue AP Alarms" table is displayed, showing a single alarm entry with the following details:

<input type="checkbox"/>	Severity	Rogue MAC Address	Type	On Network	Owner	Date/Time	State	SSID
<input type="checkbox"/>	Minor	00:40:96:50:0c:db	AP	No		8/6/04 3:05 PM	Alert	westjetap

On the left side of the interface, there is a "Severity" dropdown menu set to "Minor" and an "Alarm Category" dropdown menu set to "Rogue AP". Below these is a "Search" button. In the bottom left corner, there is a summary table for various network components:

Rogues	0	1
Coverage	0	0
Security	0	5
Switches	0	1
Access Points	0	0

Here we can see it found the Rogue AP and provided such information as the MAC address, SSID, channel, it even tells us that it is not connected to our network.

The screenshot shows a web browser window displaying the Nortel Networks Alarms interface. The page title is "Alarms - Microsoft Internet Explorer provided by WestJet". The address bar shows the URL: <https://10.222.9.165/webacs/alarmDetailAction.do?alarmKey=RogueAp%2100%3A40%3A96%3A50%3A0c%3Adb>. The page is logged in as "root" and has a "Logout" and "Refresh" option.

The main content area is titled "Alarms > Rogue AP 00:40:96:50:0c:db". It features a "General" section with the following details:

Rogue MAC Address	00:40:96:50:0c:db
Rogue Type	AP
On Network	No
Owner	
State	Alert
Channel Number	3
SSID	[REDACTED]
Containment Level	Unassigned
Created	Aug 6, 2004 3:05:40 PM
Modified	Aug 6, 2004 3:05:40 PM
Severity	Minor
Previous Severity	Minor

There is also a "Message" section with the text: "Rogue AP '00:40:96:50:0c:db' with SSID 'westjetap' and channel number '3' is detected by AP MAC address '00:0b:35:04:80:50' Slot '1' with RSSI '-72' and SNR '18'." Below this is a "Help" section with the text: "Rogue AP '00:40:96:50:0c:db' with SSID 'westjetap' and channel number '3' is detected by AP MAC address '00:0b:35:04:80:50' Slot '1' with RSSI '-72' and SNR '18'." There are also links for "Event History" and "Annotations".

At the bottom left, there is a summary table:

Rogues	0	1
Coverage	0	0
Security	0	5
Switches	0	1
Access Points	0	0

The page also includes a "Search" button and an "Add" button. The status bar at the bottom shows "Done" and "Local intranet".

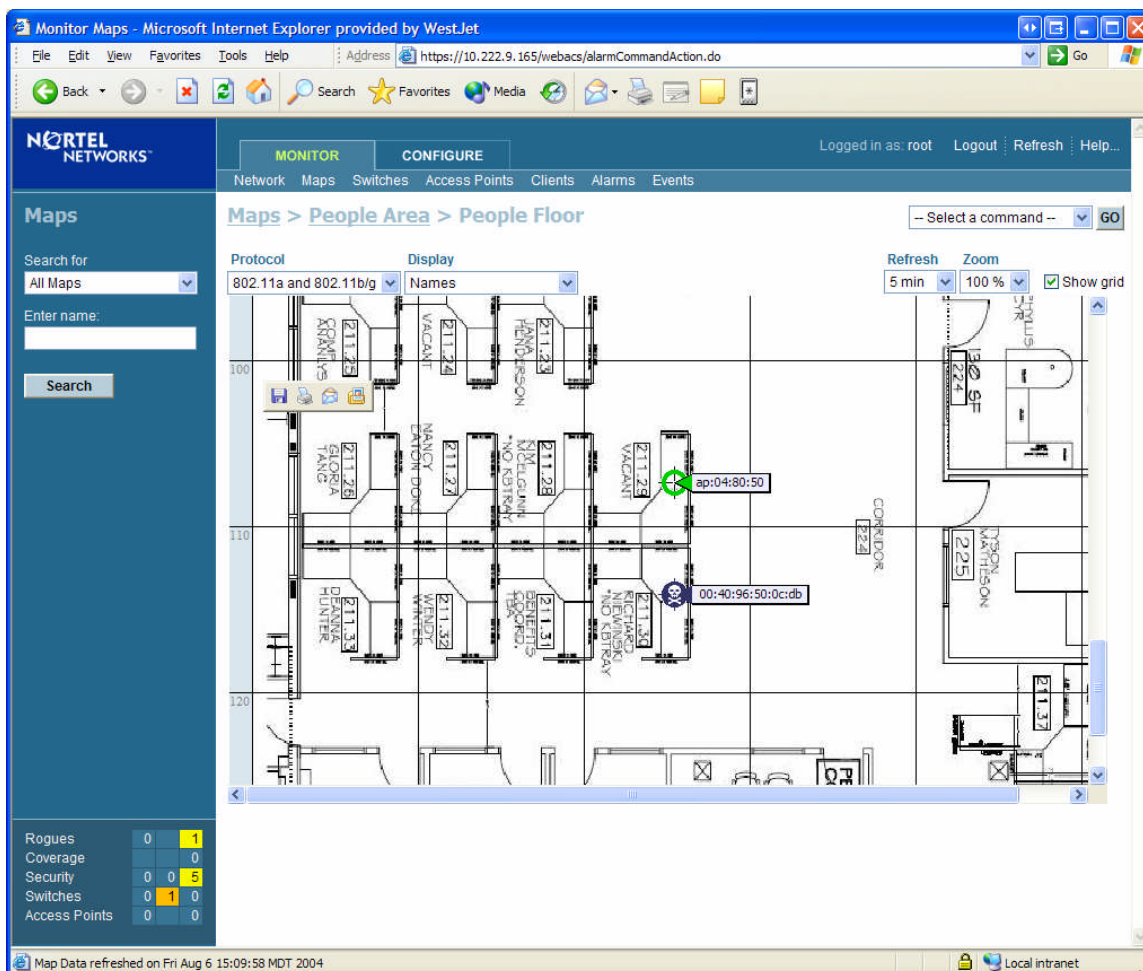
© SANS Institute

Next I selected the Map command from the drop down list.

The screenshot shows the Nortel Networks Alarms web interface in Microsoft Internet Explorer. The browser address bar shows a URL for a specific alarm. The interface is divided into a left sidebar and a main content area. The sidebar contains navigation tabs for 'MONITOR' and 'CONFIGURE', and a list of network components: Network, Maps, Switches, Access Points, Clients, Alarms, and Events. The 'Alarms' section is active, displaying a list of alarms with columns for Severity, Alarm Category, and a Search button. The main content area shows details for a specific alarm: 'Rogue AP 00:40:96:50:0c:db'. The details are organized into sections: General (Rogue MAC Address, Rogue Type, On Network, Owner, State, Channel Number, SSID, Containment Level, Created, Modified, Severity, Previous Severity), Message (Rogue AP '00:40:96:50:0c:db' with SSID 'W channel number 3' is detected by AP MAC '00:0b:85:04:80:50' Slot '1' with RSSI '-72'), Help (Rogue AP '00:40:96:50:0c:db' with SSID 'W channel number 3' is detected by AP MAC '00:0b:85:04:80:50' Slot '1' with RSSI '-72'), Event History, and Annotations. A dropdown menu is open over the 'Map' link in the 'Event History' section, showing options: Assign to me, Unassign, Delete, Event History, Detecting APs, Map (highlighted), Trend, Set State to 'Unknown', Set State to 'Known - Internal', Set State to 'Known - External', Level 1 Containment, Level 2 Containment, Level 3 Containment, and Level 4 Containment. The bottom status bar shows 'Done' and 'Local intranet'.

© SANS Institute

Then presto it mapped the Rogue AP, unfortunately it didn't exactly pin point it, but it was within 10 meters. This is Nortel's claim to accuracy with this version of software; but still well within what an average security analyst needs.



Results

As you can see from the outcome of the test, it was a success. The Nortel 2270 was able to quickly detect the Rogue AP, map it within 10 Meters and provided some detailed information about the AP.

It is worth mentioning a couple of notes here:

When speaking with Nortel regarding the discrepancy in the mapping of the Rogue AP, Nortel informed me that although 10 Meters is considered reasonably accurate, the next version of software, that includes RF Fingerprinting, will reduce that distance to about half. So you can look forward to even better mapping in the future.

To keep the scope of this paper focused I purposely avoid testing other functionality, notably two, the determination if the Rogue AP was connected to the wired network or not, and the containment feature. However, our company is planning completing this testing.

Conclusion

This paper was not intended to be a complete guide to securing your wireless environment. However, with so much emphasis being on what I like to call “information security” it is important to remind people building WiFi networks to remember the “network security” side of the equation. Network security is all about timing. The quicker you are aware of an incident, the quicker you can shut down an attacker’s access, resulting in less damage if any. Simply put, it’s all about reducing the risk.

For those of us struggling to find sanity in the chaotic world of WiFi, it’s easy to see why systems like the Nortel 2200 series are truly a breath of fresh air, real time Rogue AP detection is something that is here now and should be a “must have” requirement for anyone looking to engineer an Enterprise Level WiFi network.

We covered a lot of ground in a short time here, we started with an introduction to WiFi networks, we talked about the “wave space” or frequencies that WiFi operates in. We covered what an Access Point/Port does and how it works, then introduced the concept of a Rogue/Free Agent AP and how it is a threat to your wireless network. We worked through a demonstration of how Nortel’s 2200 series wireless equipment can help in the endeavor to thwart such attacks. We have also seen how the combination of Wireless Security Switches and Access Ports has improved the landscape of WiFi giving us the ability to look at who’s listening.

© SANS Institute
Author retains full rights.

References

[1] Brain, Marshall. "How WiFi Works", [howstuffworks](http://computer.howstuffworks.com/wireless-network1.htm).
URL:<http://computer.howstuffworks.com/wireless-network1.htm> (7/18/04)

[2] Computer Hope.com. "IEEE 802.11", [Computer Hope.com](http://www.computerhope.com/jargon/num/80211.htm).
URL:<http://www.computerhope.com/jargon/num/80211.htm> (8/02/04)

[3] Unger, Jack. "Deploying License-Free Wireless Wide-Area Networks", [informIT](http://www.informit.com/articles/article.asp?p=31731&seqNum=4). 5/16/03.
URL:<http://www.informit.com/articles/article.asp?p=31731&seqNum=4> (8/24/04)

[4] Geirer, Jim. "Identifying Rogue Access Points", [internet.com](http://www.wi-fiplanet.com/tutorials/article.php/1564431). 1/6/03.
URL:<http://www.wi-fiplanet.com/tutorials/article.php/1564431> (7/18/04)

[5] Nortel. "Wireless LAN-moving into the mainstream", [Nortel](http://a752.g.akamai.net/7/752/5107/20040712180955/www.nortelnetworks.com/products/01/wlan/collateral/nn103962-022704.pdf). 2003.
<http://a752.g.akamai.net/7/752/5107/20040712180955/www.nortelnetworks.com/products/01/wlan/collateral/nn103962-022704.pdf> (8/16/04)

Flickenger, Rob. "Wireless Hacks" 1005 Gravenstein Highway North, Sebastopol, CA 95472: O'Reilly, 2003. Pages 1-6, 43-54, 56-62, 68-70, 76-79, 94-100, 128-135.

© SANS Institute 2004, All rights reserved.