



# **Pharmacy Information System (PhIS) and Clinic Pharmacy System (CPS)**

---

## **Training Manual Facility Network Module**

<b>Version</b>	<b>: 1.4</b>
<b>Document ID</b>	<b>: H_T.MANUAL_Network_Facility</b>



© 2011-2019 Pharmaniaga Logistics Sdn Bhd (PLSB)

**CONFIDENTIAL COPYRIGHTED MATERIAL** – *The information includes all concepts, comments, recommendations, and material, contained herein shall remain the property of Pharmaniaga Logistics Sdn Bhd (PLSB). No portion of this document shall be disclosed, duplicated or used in whole or in part of any purpose other than the purpose of the Pharmacy Information System & Clinic Pharmacy System (PhIS& CPS) Project execution only.*

### Revision History

Version No	Date of Release	Prepared by	Reviewed / Verified by	List of changes from Previous Version
1.0	20.09.2013	Suzieana	Sophian	Initial Document
1.1	13.11.2014	Amiera N.	Ken Wong / Sophian	Amended Introduction section -Add Cisco Aironet 1602i -Add Wireless Bridge
1.2	09.09.2015	Helmi	Ken Wong / Ikhwal	Added Appendix A & Appendix B
1.3	15.11.2016	Amiera N. Helmi	Ken Wong	Added DLINK AP Added reference for DLINK Added Appendix C – Wireless Bridge Operation
1.4	4.1.2019	Helmi	Amiera	Amend Table of Content Amend Introduction Added Common Issue & Resolution heading Added Network Equipment Configuration Amend Commonly Used CLI

### Peer Review

Version No	Reviewer	List of changes from Previous Version
1.0	(QA) Maxine Wong	Initial Document (overall review)
1.1	(QA) Juridah Ayob	Review on Introduction section
1.2	(QA) Michelle Foo	Review on Appendix A and Appendix B
1.3	(QA) Michelle Foo	Added DLINK AP Added reference for DLINK Added Appendix C – Wireless Bridge Operation
1.4		



## Table of Contents

1	Introduction .....	1
2	Switch - Cisco SG500-28 & SG300-28 .....	2
2.1	Overview of Cisco SG300-28 & SG500-28 .....	2
2.2	Features of the Cisco SG500-28 & SG300-28 .....	2
2.2.1	Cisco SG500-28 front view .....	2
2.2.2	Cisco SG300-28 front view .....	3
2.3	Key and LED status of Cisco SG500-28 & SG300-28.....	4
2.3.1	Cisco SG500-28 Key & LED status .....	4
2.3.2	Cisco SG300-28 Key & LED status .....	6
2.4	Network Equipment Configuration .....	8
2.4.1	Cisco SG500-28 .....	8
2.4.2	Cisco SG300-28 .....	11
2.5	Troubleshooting .....	13
3	Access Point - Cisco Aironet 1141 & Aironet 1602i & Dlink DWL-6600AP1 .....	14
3.1	Overview of Cisco Aironet 1141 & Cisco Aironet 1602i .....	14
3.2	Features of the Cisco Aironet 1141 & Cisco Aironet 1602i .....	15
3.2.1	Cisco Aironet 1141 Front View .....	15
3.2.2	Cisco Aironet 1141 Rear View .....	15
3.2.3	Cisco Aironet 1602i Front View.....	16
3.2.4	Cisco Aironet 1602i Rear View .....	16
3.3	LED Status of Cisco Aironet 1141 & Cisco Aironet 1602i .....	17
3.4	Overview of Dlink DWL-6600APA1 .....	18
3.5	Features of Dlink DWL-6600APA1 .....	19
3.5.1	Dlink DWL-6600APA1 Front View .....	19
3.5.2	Dlink DWL-6600APA1 Rear View .....	19
3.5.3	Dlink DWL-6600APA1 Side View.....	19
3.6	LED Status of Dlink DWL-6600APA1 .....	20
3.7	Network Equipment Configuration .....	21
3.7.1	Cisco Aironet 1141 & Cisco Aironet 1602i .....	21
3.7.2	Dlink DWL-6600APA1.....	26
3.8	Troubleshooting .....	30
4	Wireless Bridge NanoStation M5 .....	31
4.1	NanoStation M5 Hardware Overview.....	31
4.2	NanoStation M5 Specifications .....	32
4.3	Wireless Bridge AirOS Status .....	33
4.4	Network Equipment Configuration .....	34
5	<b>Common Issue &amp; Resolution .....</b>	<b>38</b>
6	<b>References.....</b>	<b>47</b>
7	<b>Acronyms .....</b>	<b>48</b>
	<b>Appendix A - Switch Operation Guideline .....</b>	<b>49</b>
1	Remote Access to Switch .....	49



1.1	Console Cable .....	49
1.2	Secure Socket Shell (SSH).....	50
1.3	Graphical Web Interface (GUI).....	51
1.4	Commonly Used CLI.....	52
2	Switch Monitoring.....	53
2.1	Check switch availability (PING) .....	53
2.2	Check Switch CPU Utilization (Switch CLI).....	53
2.3	Monitor Switch Ports Status and Errors (Web GUI) .....	54
3	Backup and Restore Switch Configuration File .....	55
3.1	Backup Switch Configuration File .....	55
3.2	Restore Switch Configuration File.....	55
4	Switch Logs.....	56
4.1	View logs through Web Interface .....	56
4.2	Log Message Format .....	56
4.3	Severity Table .....	57
<b>Appendix B – Access Point Operation Guideline.....</b>		<b>58</b>
1	Remote Access to Access Point .....	58
1.1	Console Cable .....	58
1.2	Secure Socket Shell (SSH).....	59
1.3	Graphical Web Interface (GUI).....	60
1.4	Commonly Used CLI* .....	60
2	Access Point Monitoring.....	61
2.1	Check access point availability (PING) .....	61
2.2	Check access point radio status (GUI).....	61
2.3	Check access point SSID & signal strength (Wifi Analyzer).....	62
3	Access Point Logs.....	63
3.1	View the access point logs (GUI) .....	63
4	Backup and Restore Access Point Configuration File (GUI) .....	64
4.1	Cisco Aironet - Backup Access Point Configuration File (GUI) .....	64
4.2	D-Link AP - Backup Access Point Configuration File (GUI) .....	65
4.3	Cisco Aironet - Restore Access Point Configuration File (GUI).....	66
4.4	D-Link AP - Restore Access Point Configuration File (GUI).....	67
<b>Appendix C – Wireless Bridge Operation Guidelines .....</b>		<b>68</b>
1	Access with Graphical User Interface .....	68
2	View Wireless Bridge status.....	69
3	Backup Bridge Configuration File (GUI).....	70
4	Restore Bridge Configuration File (GUI) .....	70

## 1 Introduction

This document consists the Network Equipment module for PhIS/CPS Project of all Hospital and Clinic. Scope of this document cover the following areas:

- **Switch - Cisco SG500-28 & SG300-28**
  - ✓ Overview of Cisco SG500-28 & SG300-28
  - ✓ Features of the Cisco SG500-28 & SG300-28
  - ✓ Key and LED status of Cisco SG500-28 & SG300-28
  - ✓ Network Equipment Configuration
  - ✓ Troubleshooting
- **Access Point - Cisco Aironet 1141, Cisco Aironet 1602i, and Dlink DWL-6600APA1**
  - ✓ Overview of Cisco Aironet 1141 & Cisco Aironet 1602i
  - ✓ Features of the Cisco Aironet 1141 & Cisco Aironet 1602i
  - ✓ LED Status of Cisco Aironet 1141 & Cisco Aironet 1602i
  - ✓ Overview of Dlink DWL-6600APA1
  - ✓ Features of the Dlink DWL-6600APA1
  - ✓ LED Status of Cisco Aironet 1141 & Cisco Aironet 1602i
  - ✓ Network Equipment Configuration
  - ✓ Troubleshooting
- **Wireless Bridge**
  - ✓ NanoStation M5 Hardware Overview
  - ✓ NanoStation M5 Specifications
  - ✓ Wireless Bridge AirOS Status
  - ✓ Network Equipment Configuration
- **Common Issue & Resolution**

## 2 Switch - Cisco SG500-28 & SG300-28

### 2.1 Overview of Cisco SG300-28 & SG500-28

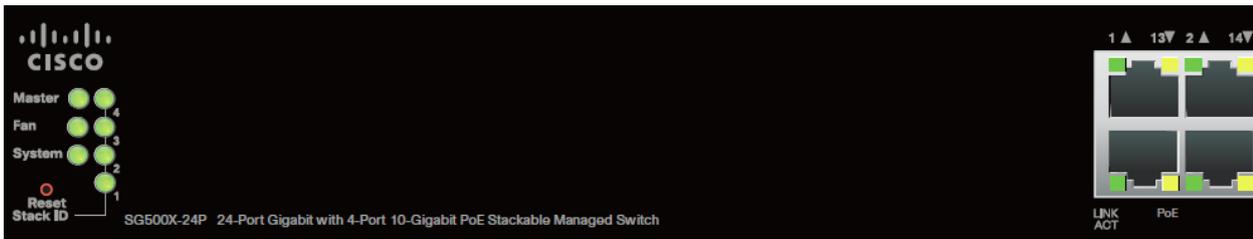
Specification		
 <p style="text-align: center;"><b>SG500-28</b></p>	 <p style="text-align: center;"><b>SG300-28</b></p>	
Basic Layer 3	<b>Switch Layer</b>	Basic Layer 3
Manage	<b>Switch Type</b>	Manage
192.168.1.254/24	<b>Default IP Address</b>	192.168.1.254/24
Yes	<b>Web-based management</b>	Yes
10/100/1000Base-T	<b>Network Technology</b>	10/100/1000Base-T
24	<b>Number of Ethernet Port</b>	26
2 Combo port + 2 SFP	<b>Number of SFP Port</b>	2 Gigabit Ethernet Combo
Yes	<b>Stack Port</b>	No
Supported Gigabit Ethernet SX Mini –GBIC SFP Transceiver	<b>SFP Module</b>	Gigabit Ethernet SX Mini –GBIC SFP Transceiver

### 2.2 Features of the Cisco SG500-28 & SG300-28

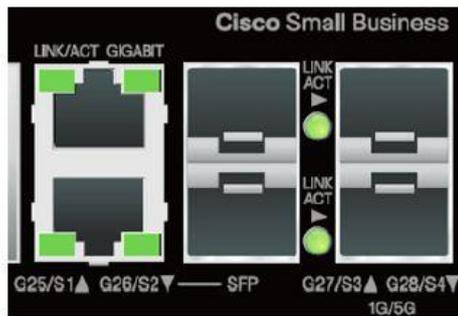
#### 2.2.1 Cisco SG500-28 front view



The following image illustrate the right side of switch.



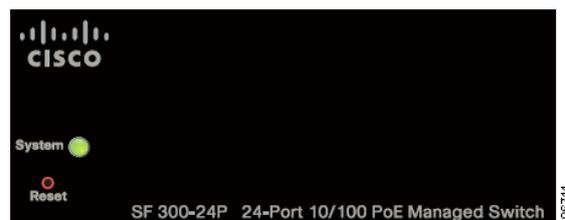
The following image illustrate the left side of switch.



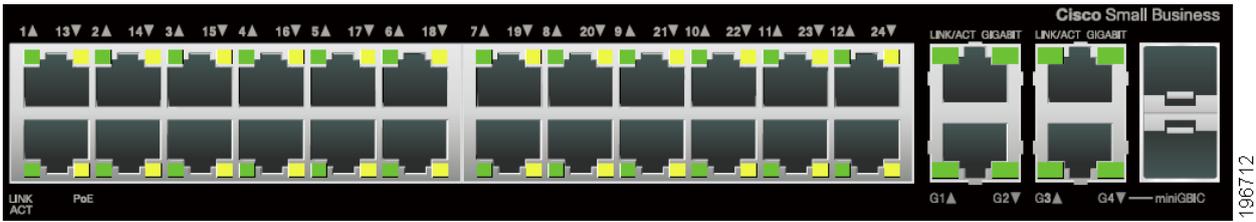
### 2.2.2 Cisco SG300-28 front view



The following image illustration shows the right side of switch.

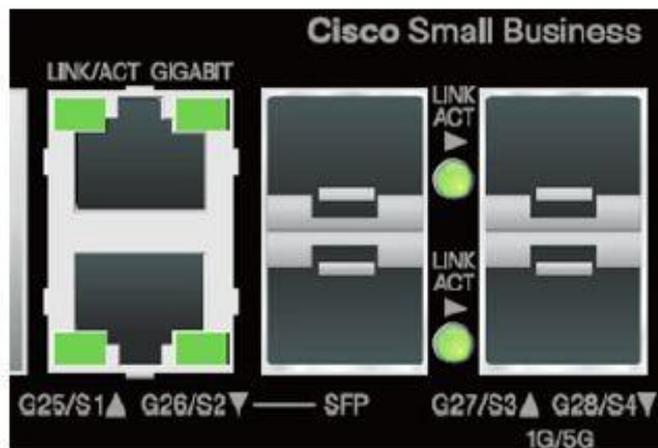
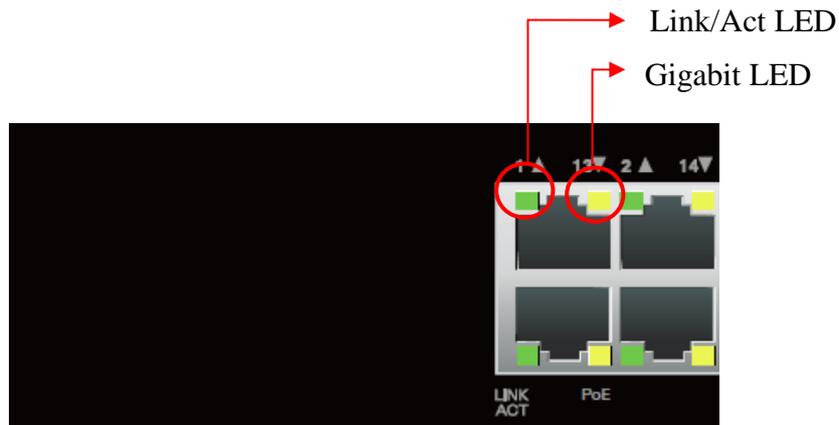
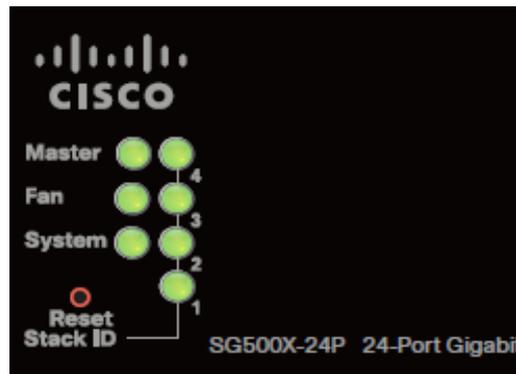


The following image illustrate the left front panel port.



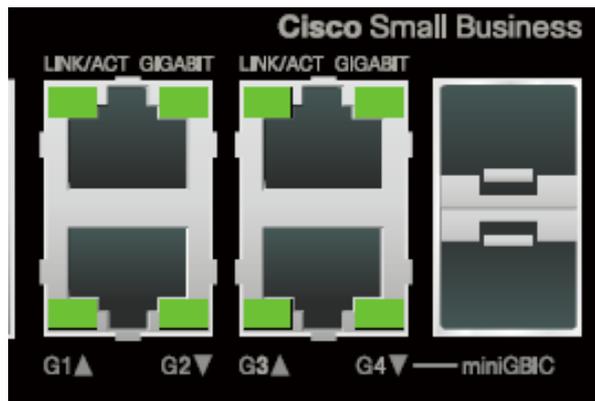
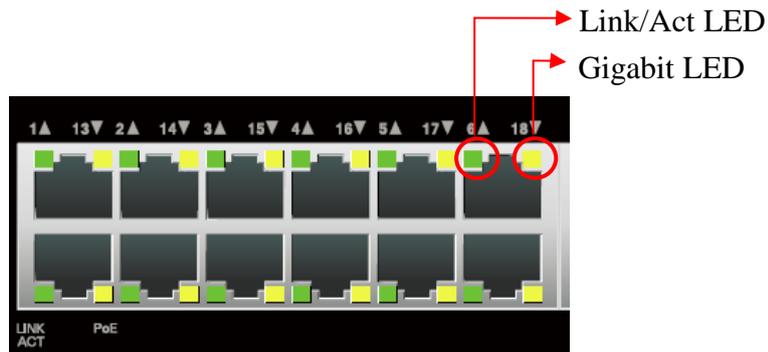
### 2.3 Key and LED status of Cisco SG500-28 & SG300-28

#### 2.3.1 Cisco SG500-28 Key & LED status



Part	LED Status	Meaning
Master LED	Green (Lights steady)	Switch is a stack master
Fan LED	Green (Lights steady)	Cooling fan is operational
	Green (Blinks)	Fan in failure
System LED	Green (Lights steady)	Switch is powered on
	LED flashes	Booting, performing self-tests, or acquiring an IP address
	LED flashes Amber	Switch has detected a hardware failure
Stack ID LED	Green (Lights steady)	This switch is stacked and the corresponding number indicates its stack ID
Link/Act LED	Green (Lights steady)	A link between the corresponding port and another device is detected
	Green (Flashes)	The port is passing traffic.
Gigabit LED	Green (Lights steady)	Connected and is powered on
	LED Off	Nothing is cabled to the port
SFP LED	Green (Lights steady)	Connection is made through the shared port.
	Green (Flashes)	The port is passing traffic.

### 2.3.2 Cisco SG300-28 Key & LED status



Part	LED Status	Meaning
Master LED	Green (Lights steady)	Switch is a stack master
Fan LED	Green (Lights steady)	Cooling fan is operational
	Green (Blinks)	Fan in failure
System LED	Green (Lights steady)	Switch is powered on
	LED flashes	Booting, performing self-tests, or acquiring an IP address
	LED flashes Amber	Switch has detected a hardware failure
Link/Act LED	Green (Lights steady)	A link between the corresponding port and another device is detected
	Green (Flashes)	The port is passing traffic.
Gigabit LED	Green (Lights steady)	Connected and is powered on
	LED Off	Nothing is cabled to the port
MiniGBIC	Green (Lights steady)	Connection is made through the shared RJ-45 port
	Green (Flashes)	The port is passing traffic.

## 2.4 Network Equipment Configuration

### 2.4.1 Cisco SG500-28

The following table show Standard Configuration for SG500 (Flat VLAN) using CLI command.

```
stack standalone reboot
wr me
set system mode router queues-mode 8

config t
hostname CSW-XXX-DNXXXXXXXXXX
username phisadmin password XXXXXXXXX privilege 15

clock timezone " " +8
clock source sntp
sntp unicast client enable
sntp unicast client poll
sntp server 10.41.28.10 poll

ip dhcp snooping
ip dhcp snooping vlan 1
ip ssh server
spanning-tree priority 24576

int range GE 1/1/1-23
switchport mode access
switchport access vlan 1

int range GE 1/1/24-28
switchport mode trunk
ip dhcp snooping trust
spanning-tree cost 10000
spanning-tree port-priority 112

int GE 1/24
description "Uplink To Facility Core Switch"

int vlan 1
ip address X.X.X.X Y.Y.Y.Y

ip default-gateway X.X.X.X
wr me
```



The following table show Standard Configuration for SG500 (VLAN) using CLI command.

```
stack standalone reboot
wr me
set system mode router queues-mode 8

config t
hostname CSW-XXX-DNIXXXXXXXXXX
username phisadmin password XXXXXXXXX privilege 15
vlan 10,20,30

clock timezone " " +8
clock source sntp
sntp unicast client enable
sntp unicast client poll
sntp server 10.41.28.10 poll

ip dhcp snooping
ip dhcp snooping vlan 20
ip dhcp snooping vlan 30

ip ssh server
spanning-tree priority 24576

int range GE 1/1/1-3
switchport mode access
switchport access vlan 20

int range GE 1/1/13-15
switchport mode access
switchport access vlan 20

int range GE 1/1/4-12
switchport mode access
switchport access vlan 30

int range GE 1/1/16-23
switchport mode access
switchport access vlan 30

int range GE 1/1/24-28
switchport mode trunk
switchport trunk allowed vlan add 10,20,30
ip dhcp snooping trust
spanning-tree cost 10000
spanning-tree port-priority 112
```



```
int GE 1/24  
description "Uplink To Facility Core Switch"
```

```
int vlan 10  
ip address X.X.X.X Y.Y.Y.Y  
name management
```

```
int vlan 20  
name server
```

```
int vlan 30  
name user
```

```
ip default-gateway X.X.X.X  
wr me
```

## 2.4.2 Cisco SG300-28

The following table show Standard Configuration for SG300 (Flat VLAN) using CLI command.

```
config t
hostname DSW-XXX-DNIXXXXXXXXXX
username phisadmin password XXXXXXXXX privilege 15

clock timezone " " +8
clock source sntp
sntp unicast client enable
sntp unicast client poll
sntp server 10.41.28.10 poll

ip dhcp snooping
ip dhcp snooping vlan 1
ip ssh server

int range GE 1-24
switchport mode access

int range GE 25-28
switchport mode trunk
ip dhcp snooping trust
spanning-tree cost 10000
spanning-tree port-priority 112

int vlan 1
ip address X.X.X.X Y.Y.Y.Y

ip default-gateway X.X.X.X
wr me
```

The following table show Standard Configuration for SG300 (VLAN) using CLI command.

```
config t
hostname DSW-XXX-DNIXXXXXXXXXX
username phisadmin password XXXXXXXXXXXX privilege 15
vlan 10,20,30

clock timezone " " +8
clock source sntp
sntp unicast client enable
sntp unicast client poll
sntp server 10.41.28.10 poll

ip dhcp snooping
ip dhcp snooping vlan 20
ip dhcp snooping vlan 30
ip ssh server

int range GE 1-3
switchport mode access
switchport access vlan 20

int range GE 13-15
switchport mode access
switchport access vlan 20

int range GE 4-12
switchport mode access
switchport access vlan 30

int range GE 16-24
switchport mode access
switchport access vlan 30

int range GE 25-28
switchport mode trunk
ip dhcp snooping trust
spanning-tree cost 10000
spanning-tree port-priority 112

int vlan 10
ip address X.X.X.X Y.Y.Y.Y
name management

int vlan 20
name server

int vlan 30
name user

ip default-gateway X.X.X.X
wr me
```

## 2.5 Troubleshooting

Part	LED Status	Possible Cause	Recovery Procedure
Master LED (SG500-28 Only)	Green (Lights steady)	N/A	<b>No action necessary.</b> to use
	LED Off	- Stacking not using - Not Function	<ul style="list-style-type: none"> <li>• <b>If the stacking function not use, No action necessary to use</b></li> <li>• Try to check Cable or Switch that been configured as slave.</li> </ul>
Fan LED	Green (Lights steady)	N/A	<b>No action necessary.</b> to use
	Green (Blinks)	Fan Failure	Swap with new switch and the old one sent to vendor for repairing.
System LED	Green (Lights steady)	N/A	<b>No action necessary.</b> to use
	LED flashes	N/A	<b>No action necessary.</b> to use
	LED flashes Amber	hardware failure	Swap with new switch and the old one sent to vendor for repairing.
Stack ID LED (SG500-28 Only)	Green (Lights steady)	N/A	<b>No action necessary.</b> to use
	LED off	- Not Using - Link Down / Switch Down	<ul style="list-style-type: none"> <li>• <b>If it is “Not Using”, no action should be taken.</b></li> <li>• <b>Try to check connected Cable</b></li> </ul>
Link/Act LED	Green (Lights steady)	N/A	<b>No action necessary.</b> to use
	Green (Flashes)	N/A	<b>No action necessary.</b> to use
	LED off	- Not Using - Link Down / Switch Down	<ul style="list-style-type: none"> <li>• <b>If not using, No action necessary to use</b></li> <li>• Try to check Cable or Switch that connected into that port.</li> </ul>
Gigabit LED	Green (Lights steady)	N/A	<b>No action necessary.</b> to use
	LED Off	- Not Using - Connection Down	<ul style="list-style-type: none"> <li>• <b>If not using, No action necessary to use</b></li> <li>• Try to check Cable or Switch that connected into that port.</li> </ul>
SFP LED (SG500-28 Only)	Green (Lights steady)	N/A	<b>No action necessary.</b> to use
	Green (Flashes)	N/A	<b>No action necessary.</b> to use
	LED Off	- Not Using - Connection Down	<ul style="list-style-type: none"> <li>• <b>If not using, No action necessary to use</b></li> <li>• Try to check Cable or Switch that connected into that port.</li> </ul>
MiniGBIC (SG300-28 Only)	Green (Lights steady)	N/A	<b>No action necessary.</b> to use
	Green (Flashes)	N/A	<b>No action necessary.</b> to use

### 3 Access Point - Cisco Aironet 1141 & Aironet 1602i & Dlink DWL-6600AP1

#### 3.1 Overview of Cisco Aironet 1141 & Cisco Aironet 1602i

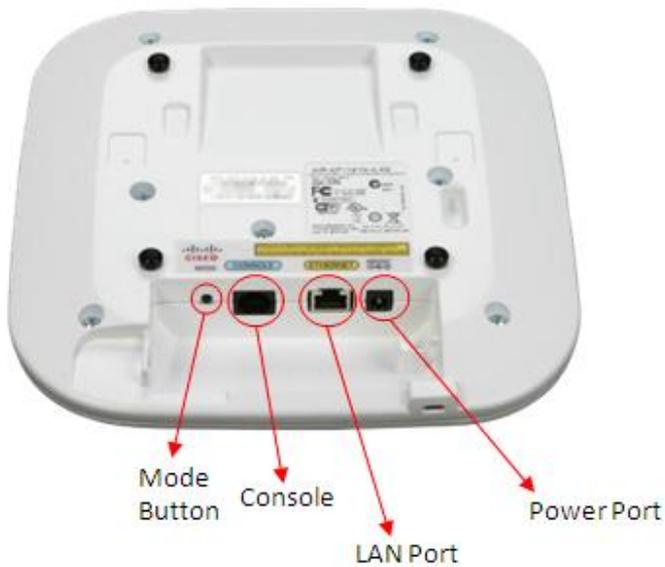
Category	Specification
Antenna	Internal
Connectivity Technology	Wireless
Data Link/Wireless Protocol	IEEE 802.11b, IEEE 802.11g, IEEE 802.11n
Frequency Band	2.4 GHz
Security Support	WPA, TKIP, WPA2, PEAP, AES, TLS, TTLS
Data Transfer Rate	802.11b: 1, 2, 5.5, 11Mbps 802.11g: up to 54Mbps 802.11n: up to 150Mbps

### 3.2 Features of the Cisco Aironet 1141 & Cisco Aironet 1602i

#### 3.2.1 Cisco Aironet 1141 Front View



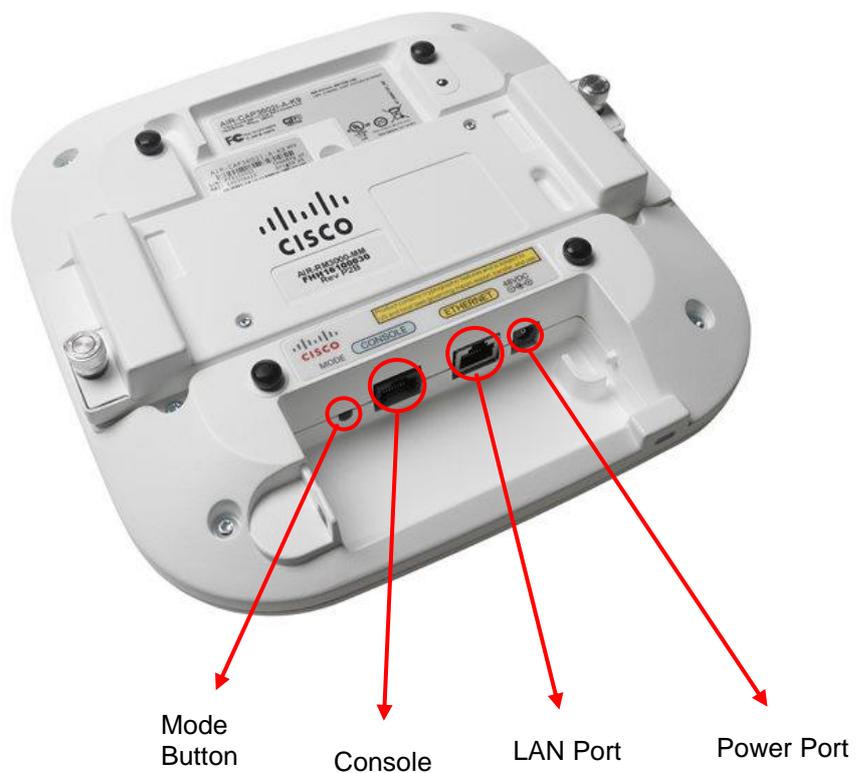
#### 3.2.2 Cisco Aironet 1141 Rear View



### 3.2.3 Cisco Aironet 1602i Front View



### 3.2.4 Cisco Aironet 1602i Rear View



### 3.3 LED Status of Cisco Aironet 1141 & Cisco Aironet 1602i

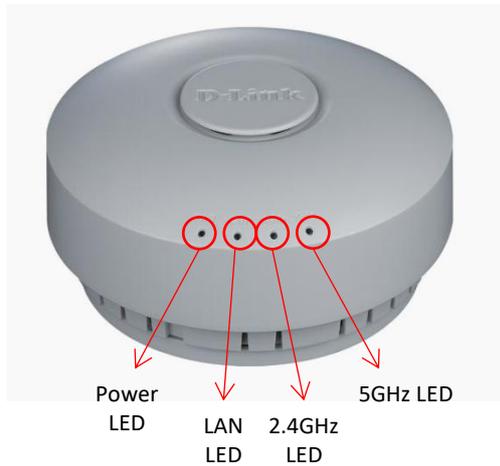
Message type	Status LED	Message Meaning
Boot Loader Status Sequence	Blinking green	<ul style="list-style-type: none"> <li>• DRAM memory test in progress</li> <li>• DRAM memory test OK</li> <li>• Board initialization in progress</li> <li>• Initialization FLASH file system</li> <li>• Flash memory OK test</li> <li>• initialization Ethernet</li> <li>• Ethernet OK</li> <li>• Starting Cisco IOS</li> <li>• Initialization Successful</li> </ul>
Association Status	Green	Normal operating condition, but no wireless client associated
	Blue	Normal operating condition, at least one wireless client association
Operating Status	Blinking blue	Software upgrade in progress
	Cycling through green, red, and amber	Discovery/join process in progress
	Rapidly cycling through blue, green and red	Access Point location command invoked
	Blinking red	Ethernet link not operational
Boot loader errors	Red	DRAM memory test failure
	Blinking red and blue	FLASH file system failure
	Blinking red and off	<ul style="list-style-type: none"> <li>• Environment variable failure</li> <li>• BAD MAC address</li> <li>• Ethernet failure during image recovery</li> <li>• Boot environment failure</li> <li>• No Cisco image file</li> <li>• Boot failure</li> </ul>
Cisco IOS failure	Red	Software failure; try disconnecting and reconnecting power unit
	Cycling through blue, green, red and off	General Warning; insufficient inline power

### 3.4 Overview of Dlink DWL-6600APA1

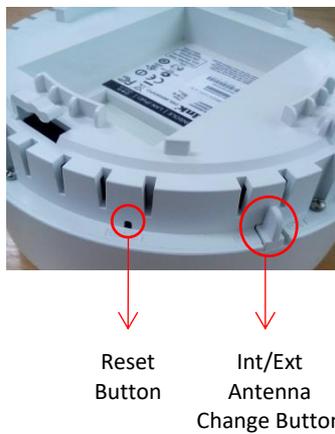
Category	Specification
Wi-Fi Interface	802.11a/b/g/n 2.4/5.0 GHz
LAN Interface	10/100/1000 Gigabit Ethernet
Console	RJ-45
Antenna	2x2 MIMO embedded antenna with 4 external antenna connectors
Power Method	IEEE 802.3af Power Over Ethernet or external power adapter
Wireless Frequency	802.11n: 2.4 to 2.497 GHz and 4.9 to 5.85 GHz 802.11b/g: 2.4 to 2.4835 GHz 802.11a: 5.15 to 5.35 GHz and 5.725 to 5.825 GHz
Data Transfer Rate	802.11n: 6.5 Mbps-130 Mbps (20 MHz), 6.5 MHz-300 Mbps (40 Mbps) 802.11a/g: 54, 48, 36, 24, 18, 12, 9, and 6 Mbps 802.11b: 11, 5.5, 2 and 1 Mbps
Wireless Security	WEP Dynamic WEP WPA Personal/ Enterprise WPA2 Personal/ Enterprise

### 3.5 Features of Dlink DWL-6600APA1

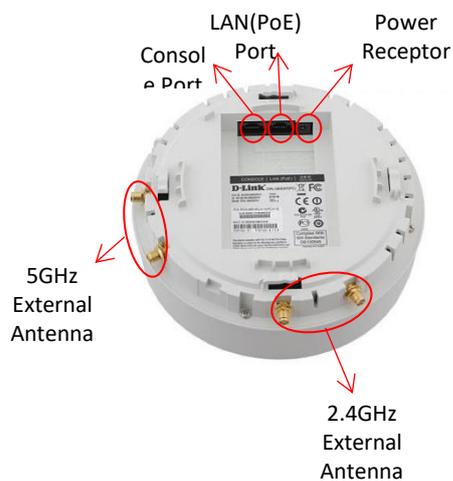
#### 3.5.1 Dlink DWL-6600APA1 Front View



#### 3.5.2 Dlink DWL-6600APA1 Rear View



#### 3.5.3 Dlink DWL-6600APA1 Side View





### 3.6 LED Status of Dlink DWL-6600APA1

LED Name	LED Color/Status	Message
POWER	Red	access point is boot-up
	Green	access point is ready
LAN	Lit	device's ethernet port is connected to an active router or switch
	Blink	there is traffic going through the port
2.4 GHz	Lit	access point is operating at 2.4GHz
	Blink	there is wireless traffic
5 GHz	Lit	access point is operating at 5GHz
	Blink	there is wireless traffic



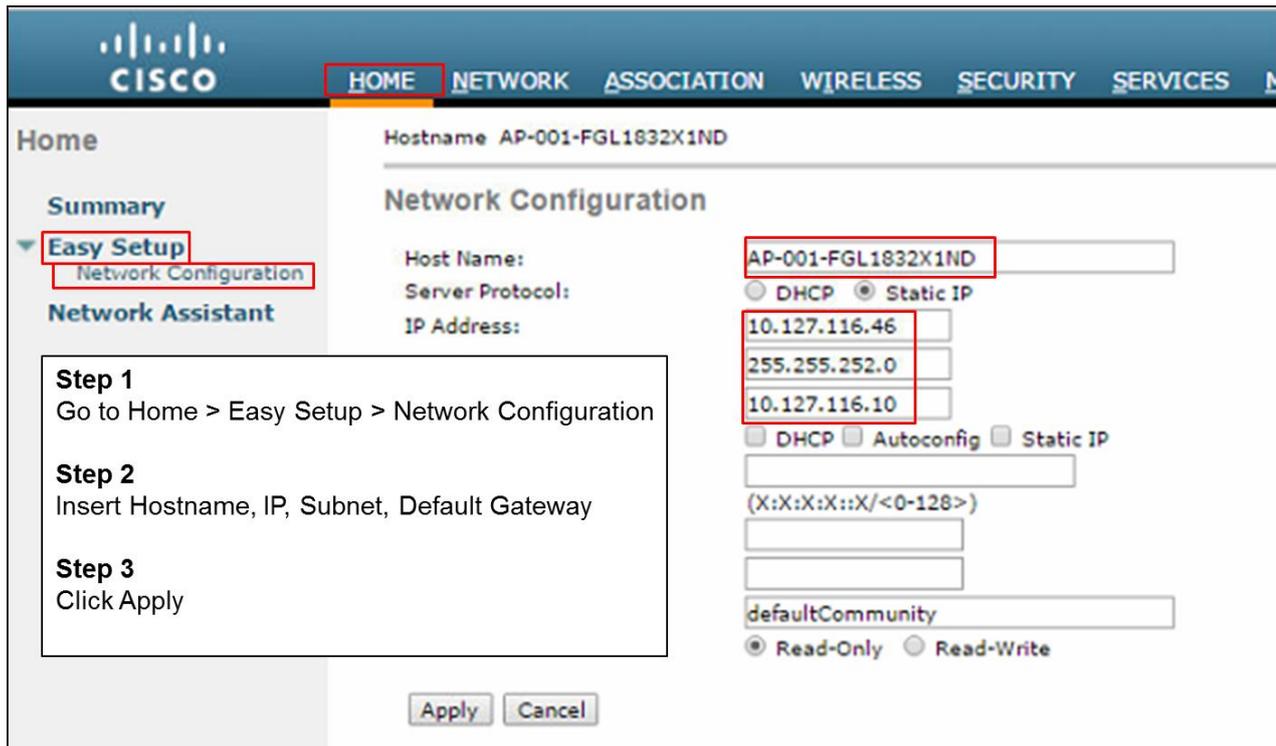
### 3.7 Network Equipment Configuration

#### 3.7.1 Cisco Aironet 1141 & Cisco Aironet 1602i

The following table show summary of Cisco AP configuration

No.	Configuration
1	IP, Subnet, Gateway & Hostname
2	Vlan
3	Encryption Mode
4	SSID & Password Key
5	Username & Password (Management Access)
6	Radio

## Part 1: Configure IP, Subnet, Gateway & Hostname



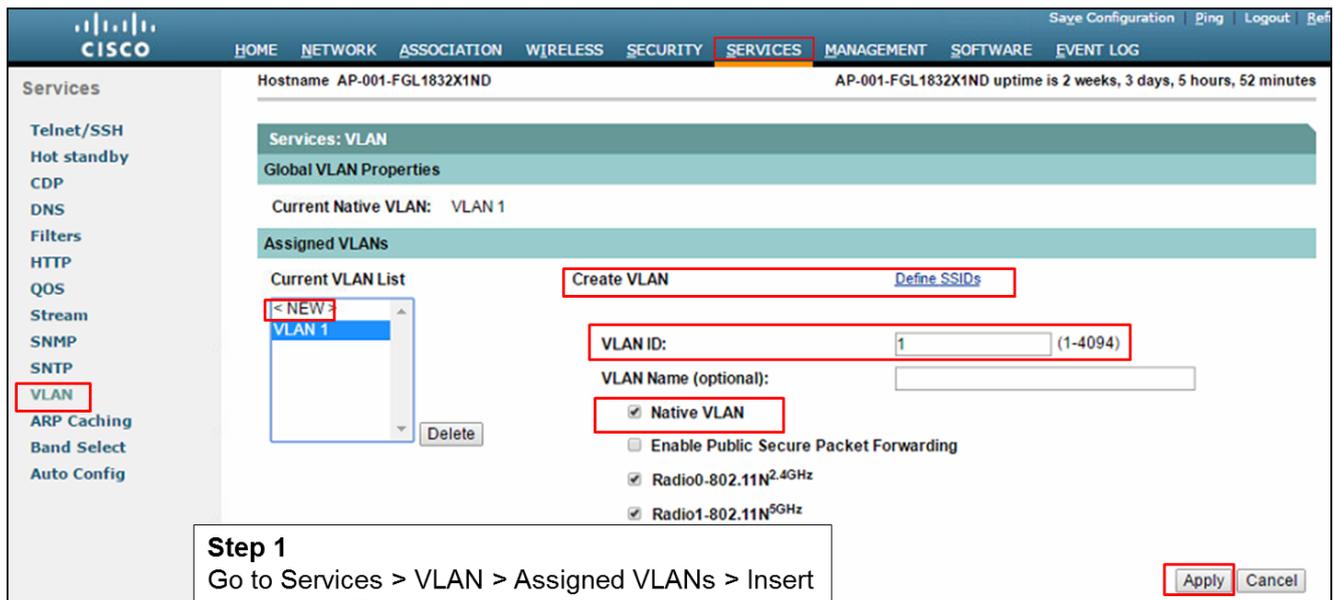
The screenshot shows the Cisco Easy Setup Network Configuration page for device AP-001-FGL1832X1ND. The 'HOME' tab is selected. The 'Easy Setup' section is expanded to 'Network Configuration'. The 'Host Name' field is set to 'AP-001-FGL1832X1ND'. The 'Server Protocol' is set to 'Static IP'. The 'IP Address' field is set to '10.127.116.46', the 'Subnet Mask' is '255.255.252.0', and the 'Default Gateway' is '10.127.116.10'. The 'DHCP' and 'Static IP' radio buttons are both present, with 'Static IP' selected. The 'Autoconfig' and 'Static IP' checkboxes are also present. The 'Read-Only' radio button is selected. The 'Apply' and 'Cancel' buttons are at the bottom.

**Step 1**  
Go to Home > Easy Setup > Network Configuration

**Step 2**  
Insert Hostname, IP, Subnet, Default Gateway

**Step 3**  
Click Apply

## Part 2: Configure VLAN



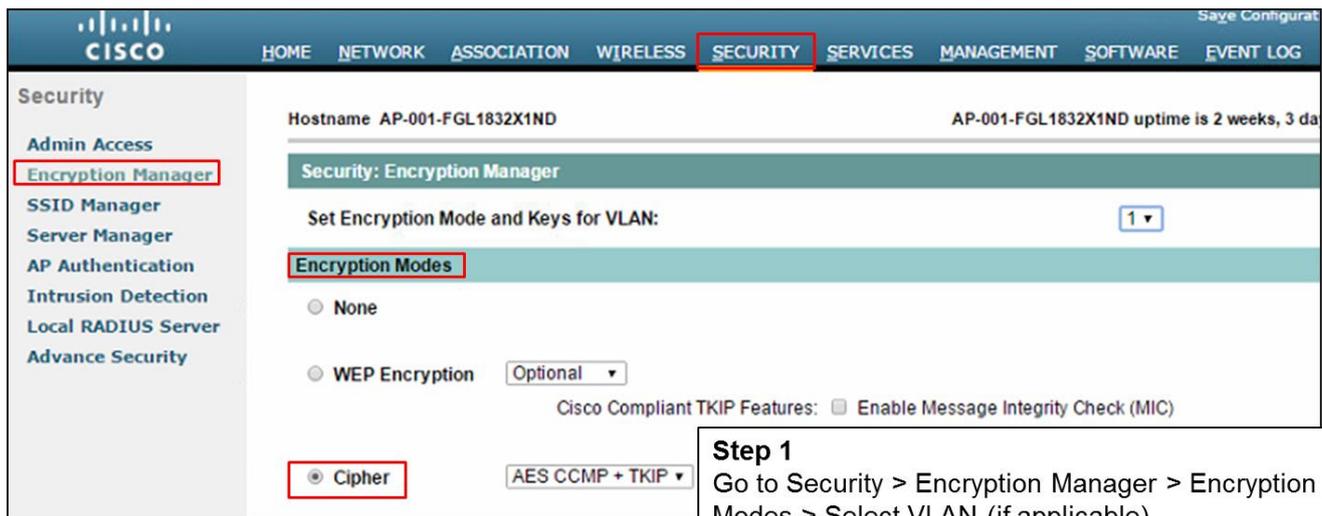
The screenshot shows the Cisco Services VLAN configuration page for device AP-001-FGL1832X1ND. The 'SERVICES' tab is selected. The 'Assigned VLANs' section is expanded. The 'Current VLAN List' shows 'VLAN 1'. The 'Create VLAN' button is highlighted. The 'VLAN ID' field is set to '1'. The 'VLAN Name (optional)' field is empty. The 'Native VLAN' checkbox is checked. The 'Radio0-802.11N 2.4GHz' and 'Radio1-802.11N 5GHz' checkboxes are also checked. The 'Apply' and 'Cancel' buttons are at the bottom.

**Step 1**  
Go to Services > VLAN > Assigned VLANs > Insert New VLAN ID (if applicable)

**Step 2**  
Select Native VLAN & both 2.4, 5 Ghz radio.

**Step 3**  
Click Apply

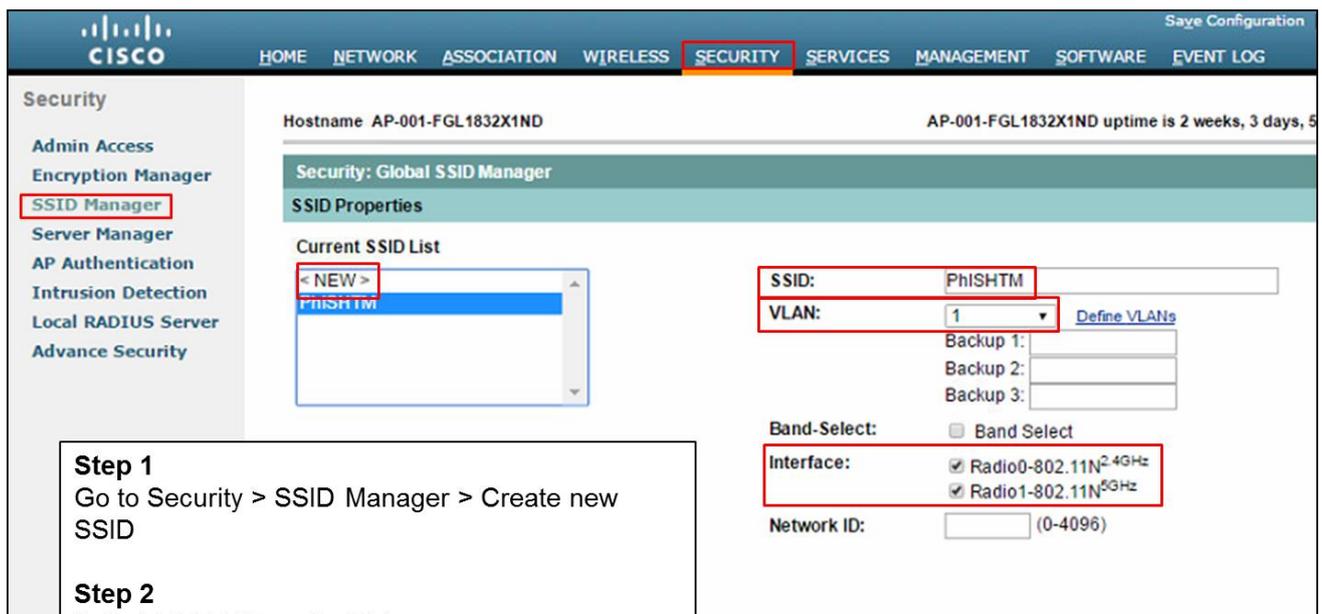
Part 3: Configure Encryption Mode



The screenshot shows the Cisco configuration interface for an AP. The 'SECURITY' tab is active. In the left sidebar, 'Encryption Manager' is selected. The main content area shows 'Security: Encryption Manager' for VLAN 1. Under 'Encryption Modes', the 'CIPHER' radio button is selected, and 'AES CCMP + TKIP' is selected from the dropdown menu. Other options like 'None' and 'WEP Encryption' are visible but not selected.

- Step 1**  
Go to Security > Encryption Manager > Encryption Modes > Select VLAN (if applicable)
- Step 2**  
Select Cipher - AES CCMP + TKIP
- Step 3**  
Click Apply

Part 4: Configure SSID



The screenshot shows the Cisco configuration interface for an AP. The 'SECURITY' tab is active. In the left sidebar, 'SSID Manager' is selected. The main content area shows 'Security: Global SSID Manager' for SSID Properties. Under 'Current SSID List', a new entry '<NEW>' is highlighted. In the configuration fields, 'SSID' is 'PhISHTM', 'VLAN' is '1', and 'Interface' has both 'Radio0-802.11N 2.4GHz' and 'Radio1-802.11N 5GHz' checked. 'Band-Select' is unchecked.

- Step 1**  
Go to Security > SSID Manager > Create new SSID
- Step 2**  
Select VLAN (if applicable)
- Step 3**  
Select Interface - Both 2.4 & 5 Ghz

**Client Authenticated Key Management**

Key Management:   CCKM  Enable WPA

WPA Pre-shared Key:   ASCII  Hexadecimal

**Guest Mode/Infrastructure SSID Settings**

**Radio0-802.11N<sup>2.4GHz</sup>:**  
Set Beacon Mode:  Single BSSID Set Single Guest Mode SSID:   
 Multiple BSSID  
Set Infrastructure SSID:   Force Infrastructure Devices to associate only to this SSID

**Radio1-802.11N<sup>5GHz</sup>:**  
Set Beacon Mode:  Single BSSID Set Single Guest Mode SSID:   
 Multiple BSSID  
Set Infrastructure SSID:   Force Infrastructure Devices to associate only to this SSID

**Step 4**

Select Key Management - Mandatory, Enable WPA with WPAv2

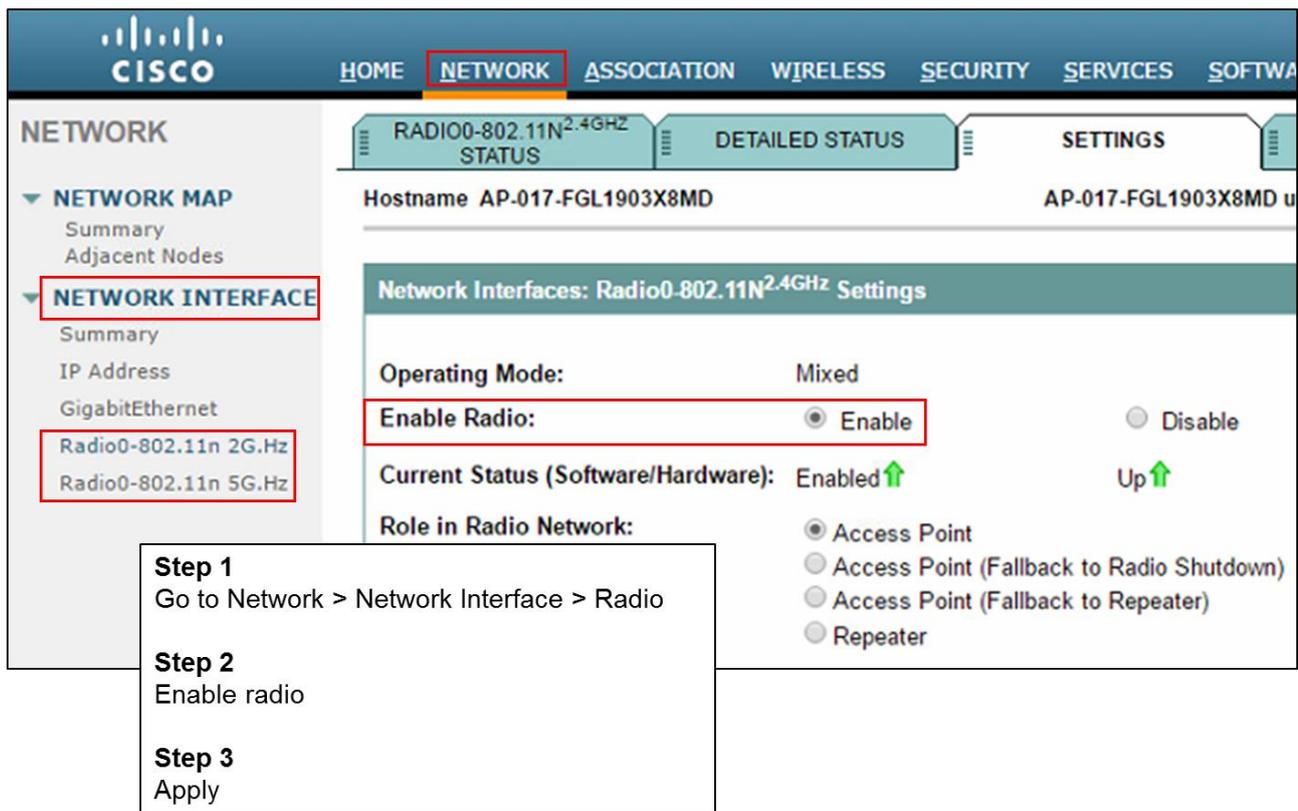
**Step 5**

Insert SSID pass key

**Step 6**

Click Apply

Part 5: Enable radio

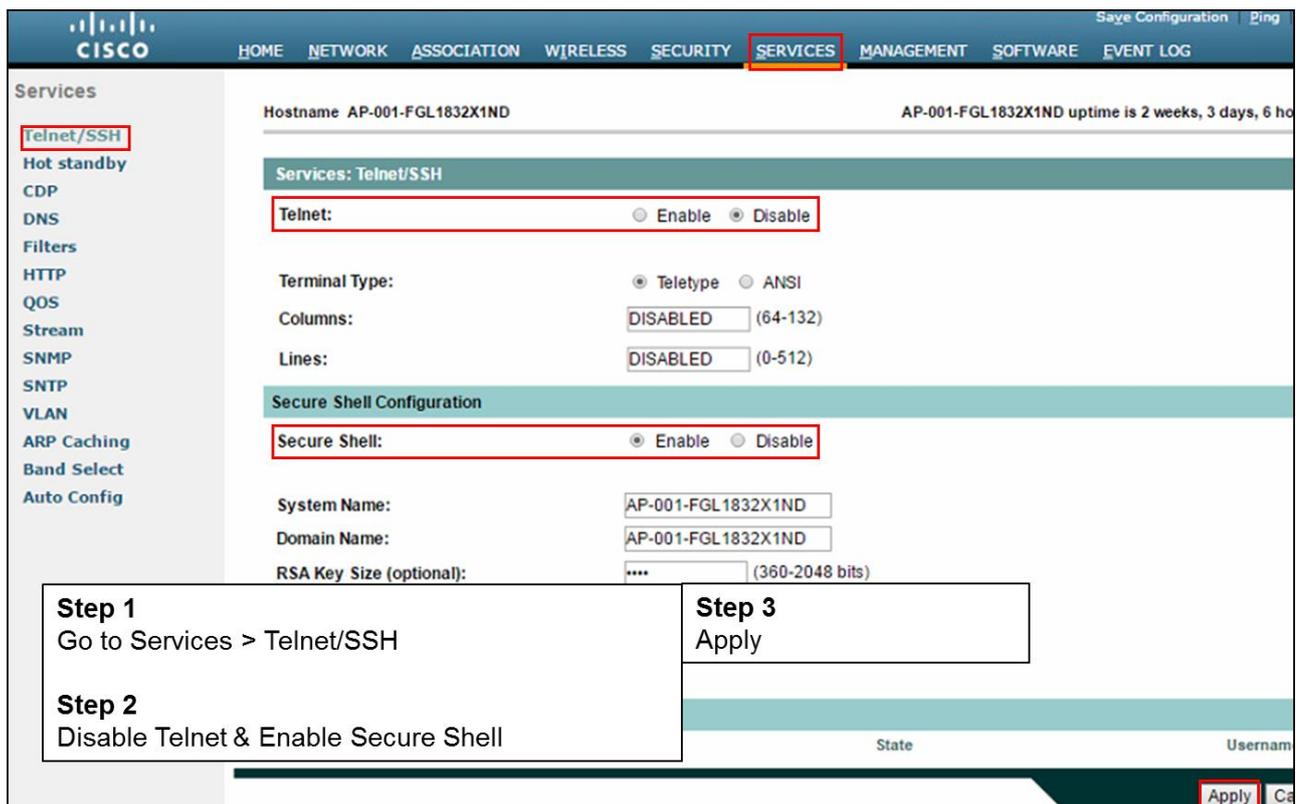


**Step 1**  
Go to Network > Network Interface > Radio

**Step 2**  
Enable radio

**Step 3**  
Apply

Part 6: Enable SSH



**Step 1**  
Go to Services > Telnet/SSH

**Step 2**  
Disable Telnet & Enable Secure Shell

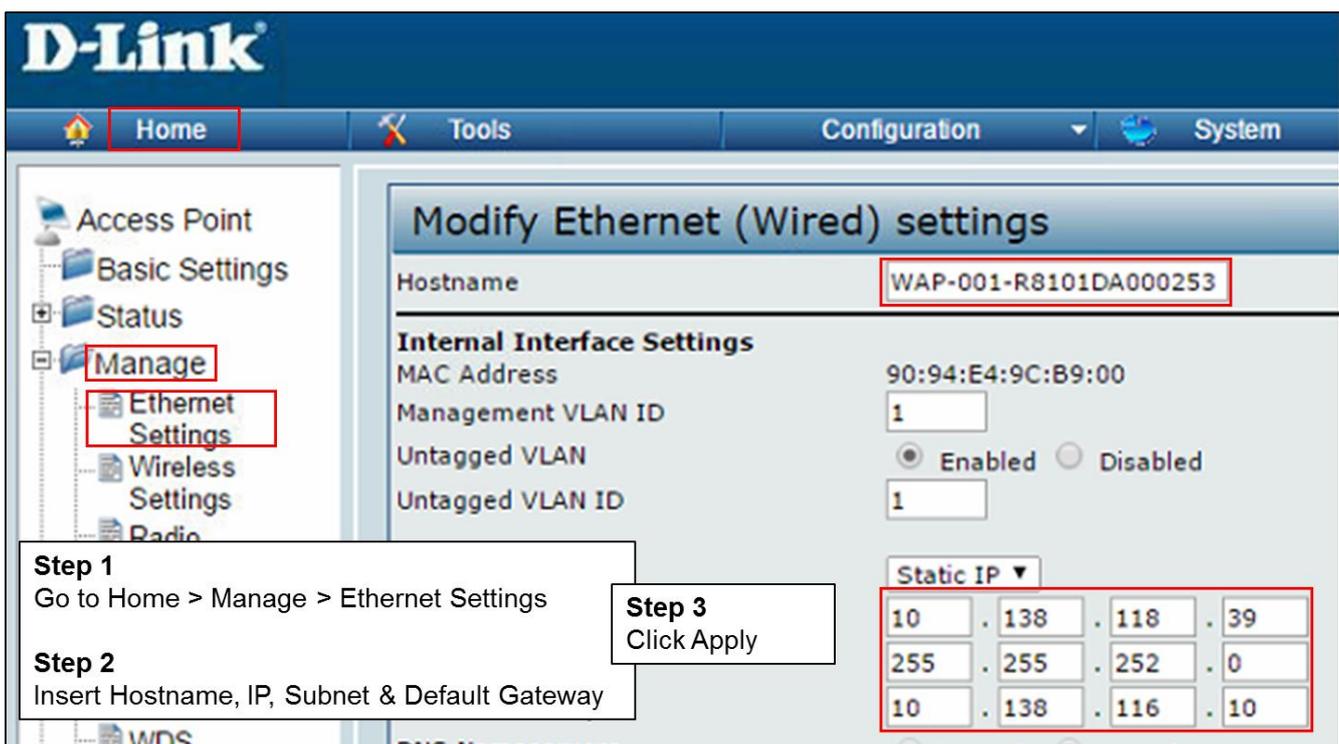
**Step 3**  
Apply

### 3.7.2 Dlink DWL-6600APA1

The following table show summary of Dlink AP configuration

No.	Configuration
1	IP, Subnet, Gateway & Hostname
2	NTP
3	Configure VAP (SSID)
4	Configure Cluster

Part 1: Configure IP, Subnet, Gateway & Hostname



The screenshot shows the D-Link web interface for configuring an Access Point. The navigation menu on the left includes 'Home', 'Tools', 'Configuration', and 'System'. Under 'Configuration', the 'Manage' folder is expanded to show 'Ethernet Settings', which is highlighted with a red box. The main content area is titled 'Modify Ethernet (Wired) settings'. The 'Hostname' field is set to 'WAP-001-R8101DA000253' and is highlighted with a red box. Under 'Internal Interface Settings', the 'Management VLAN ID' and 'Untagged VLAN ID' are both set to '1'. The 'Static IP' dropdown is set to 'Static IP', and the IP address '10.138.118.39' is entered in the first row of the IP configuration table. The second row shows '255.255.252.0' and the third row shows '10.138.116.10'. A 'Step 3' callout box points to the 'Apply' button.

**Step 1**  
Go to Home > Manage > Ethernet Settings

**Step 2**  
Insert Hostname, IP, Subnet & Default Gateway

**Step 3**  
Click Apply

## Part 2: Configure NTP

### Modify to discover the time for access point

System Time (24 HR) Fri Dec 31 1999 12:21:02 MST

Set System Time  Using Network Time Protocol (NTP)  Manually

NTP Server

Time Zone

Adjust Time for Daylight Savings

Click "Apply" to save the new settings.

**Step 1**  
Go to Home > Services > Time Settings (NTP)

**Step 2**  
Select Using Network Time Protocol (NTP)

**Step 3**  
Insert '10.41.28.10' in NTP Server

## Part 3: Configure VAP (SSID)

### Modify Virtual Access Point settings

Global RADIUS server settings

RADIUS IP Address Type:  IPv4  IPv6

RADIUS IP Address:

RADIUS IP Address-1:

RADIUS IP Address-2:

RADIUS IP Address-3:

RADIUS Key:

RADIUS Key-1:

RADIUS Key-2:

RADIUS Key-3:

Enable RADIUS accounting

Enable RADIUS Failthrough

Radio

VAP	Enabled	VLAN ID	SSID	Broadcast SSID	Security	MAC Auth Type	Redirect Mode
0	<input checked="" type="checkbox"/>	<input type="text" value="1"/>	<input type="text" value="PhISHSM-C3"/>	<input checked="" type="checkbox"/>	<input type="text" value="WPA Personal"/>	<input type="text" value="Disabled"/>	<input type="text" value="None"/>

WPA Versions:  WPA  WPA2

Cipher Suites:  TKIP  CCMP (AES)

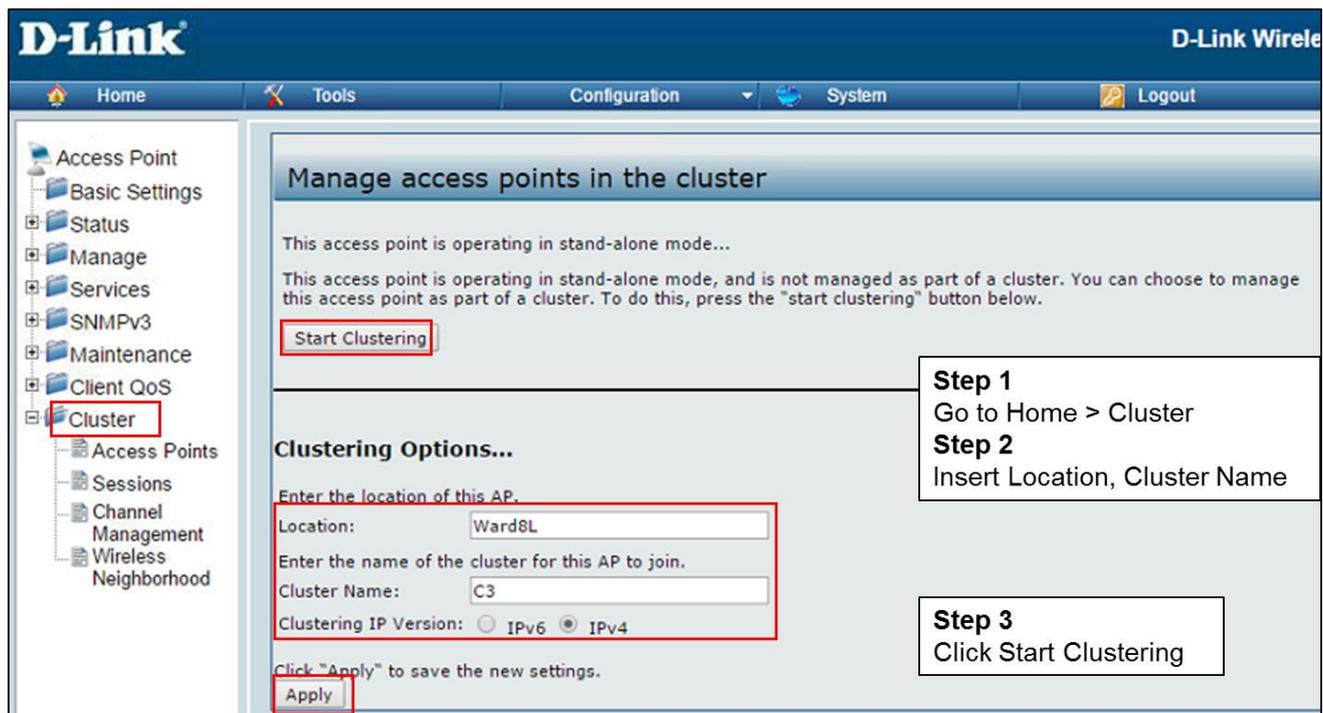
Key:

Broadcast Key Refresh Rate (Range: 0-86400)

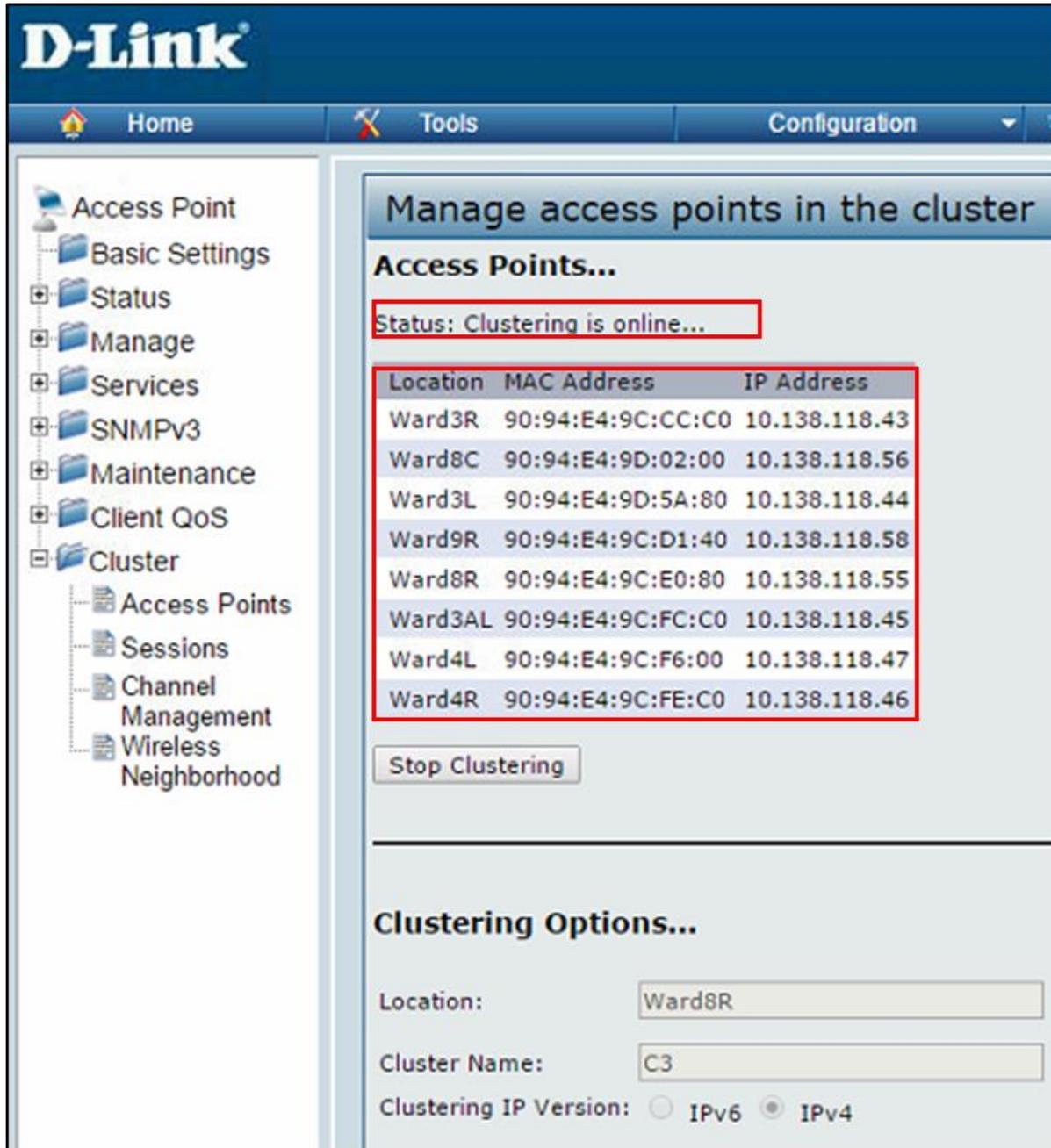
**Step 1**  
Go to Home > Manage > VAP

**Step 2**  
Insert VLAN ID, SSID, Security, WPA Version, Cipher Suites

## Part 4: Configure Cluster



The screenshot shows the D-Link Wireless configuration interface. The left sidebar contains a tree view with 'Cluster' selected. The main content area is titled 'Manage access points in the cluster' and contains the following text: 'This access point is operating in stand-alone mode...' and 'This access point is operating in stand-alone mode, and is not managed as part of a cluster. You can choose to manage this access point as part of a cluster. To do this, press the "start clustering" button below.' A red box highlights the 'Start Clustering' button. Below this is the 'Clustering Options...' section, which includes: 'Enter the location of this AP.' with a text box containing 'Ward8L'; 'Enter the name of the cluster for this AP to join.' with a text box containing 'C3'; and 'Clustering IP Version:' with radio buttons for 'IPv6' and 'IPv4' (selected). A red box highlights the 'Apply' button at the bottom. Three callout boxes provide instructions: 'Step 1: Go to Home > Cluster', 'Step 2: Insert Location, Cluster Name', and 'Step 3: Click Start Clustering'.

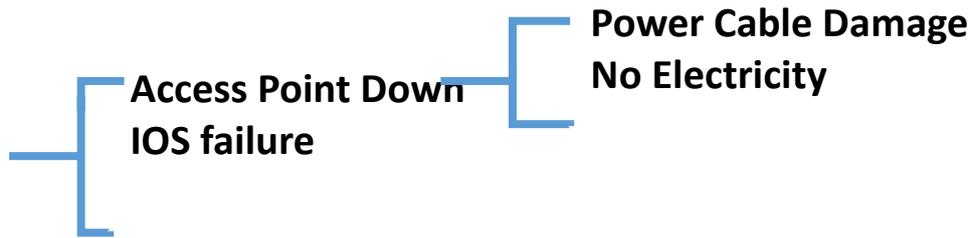


The screenshot shows the D-Link web interface for managing access points in a cluster. The left sidebar contains a navigation menu with categories like Access Point, Basic Settings, Status, Manage, Services, SNMPv3, Maintenance, Client QoS, and Cluster. The main content area is titled "Manage access points in the cluster" and includes a "Status: Clustering is online..." message. Below this is a table listing access points with columns for Location, MAC Address, and IP Address. A "Stop Clustering" button is visible below the table. The "Clustering Options..." section includes input fields for "Location" (Ward8R) and "Cluster Name" (C3), and radio buttons for "Clustering IP Version" (IPv6 and IPv4, with IPv4 selected).

Location	MAC Address	IP Address
Ward3R	90:94:E4:9C:CC:C0	10.138.118.43
Ward8C	90:94:E4:9D:02:00	10.138.118.56
Ward3L	90:94:E4:9D:5A:80	10.138.118.44
Ward9R	90:94:E4:9C:D1:40	10.138.118.58
Ward8R	90:94:E4:9C:E0:80	10.138.118.55
Ward3AL	90:94:E4:9C:FC:C0	10.138.118.45
Ward4L	90:94:E4:9C:F6:00	10.138.118.47
Ward4R	90:94:E4:9C:FE:C0	10.138.118.46

### 3.8 Troubleshooting

#### Access Point



#### \*\*Reminder

If there is Red color on LED, it means that the Access Point is having problems. The easiest way is to reboot the access point.

From user site, it is compulsory to re-check entered password and SSID; make sure the password and SSID is correct. Alert if the password is case sensitive.

Problems	Causes	Solution
Accessing Wi-Fi is denied	Wrong password	Enter correct password
Cannot access Wi-Fi	Wireless disable	Enable wireless option
Wireless icon:  OR 	Static or DHCP issue AP not up/problem	<ul style="list-style-type: none"> <li>• Please Enter the correct IP Address (Static IP issue)</li> <li>• Reboot PC or laptop /</li> <li>• Power on AP / check PoE injector (AP not up)</li> </ul>
iPad received an unknown IP (e.g. 169.x.x.x)	The 169.xx address range is usually self-assigned by the device when it fails to receive a DHCP address	Test by using static IP. If using static IP success, check on DHCP server (DHCP issue, etc)

## 4 Wireless Bridge NanoStation M5

### 4.1 NanoStation M5 Hardware Overview



NanoStation



24V PoE  
Adapter



Power Cord



Mounting Ties  
(Qty. 2)

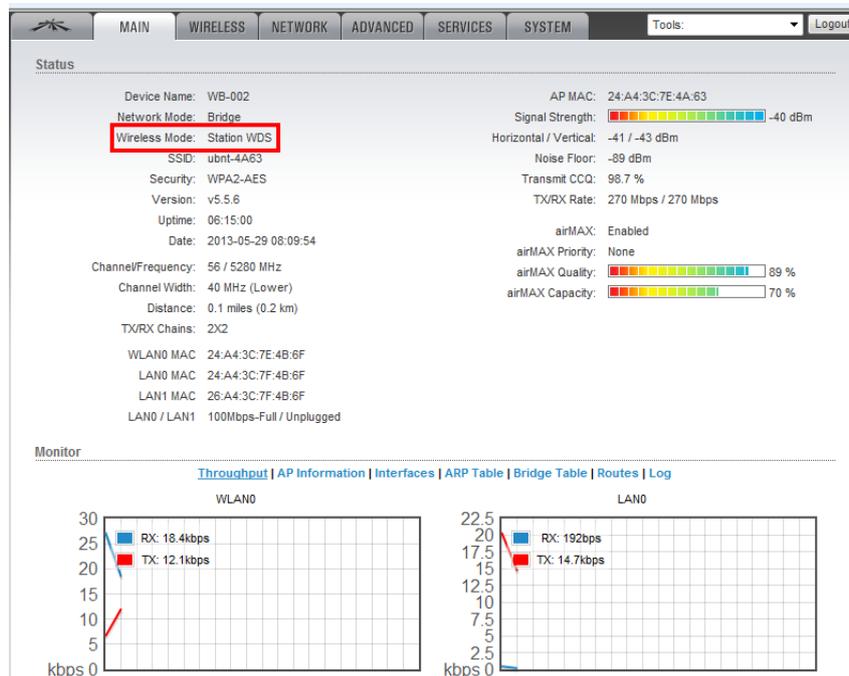
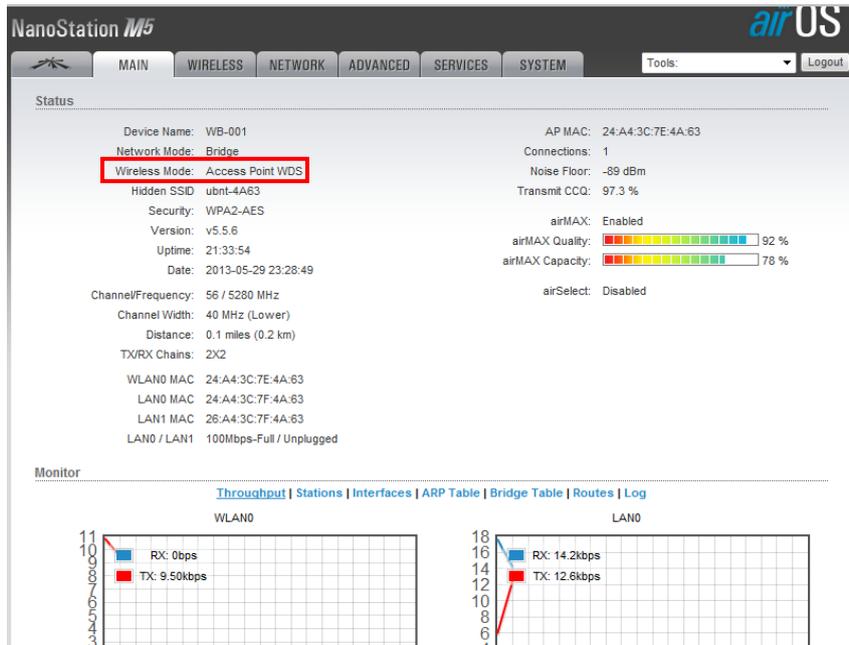


**Note:** The *Secondary Ethernet Port* is included on NanoStation M5. It is capable of 24V Power over Ethernet (PoE) output, which can provide power to a secondary device. It can be enabled using the airOS Configuration Interface.

## 4.2 NanoStation M5 Specifications

NanoStation M5	
Dimensions	294 x 30 x 80 mm
Weight	0.4 kg
Operating Frequency	5170 – 5875 MHz
Gain	16 dBi
Maximum Power Consumption	8 W
Power Supply	24V, 0.5A PoE Adapter Included
Power Method	Passive PoE (Pairs 4, 5+; 7, 8 Return)
Mounting	Pole-Mounting Kit included
Networking Interface	TWO (2) 10/100 Ethernet Ports
Operating Temperature	-30 to 75 DC
Operating Humidity	4 95% Condensing

## 4.3 Wireless Bridge AirOS Status

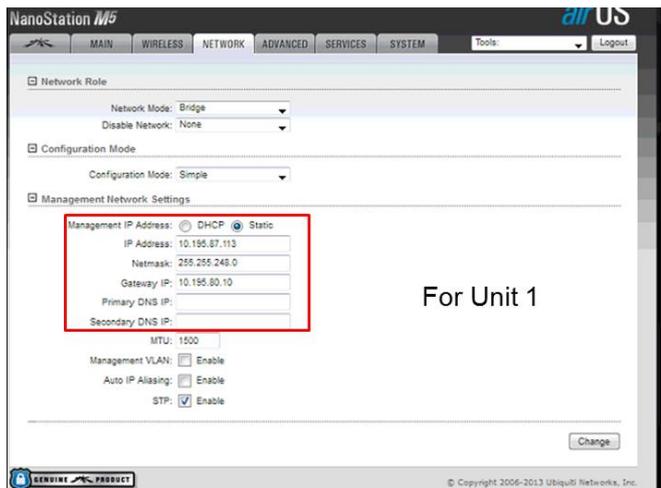


## 4.4 Network Equipment Configuration

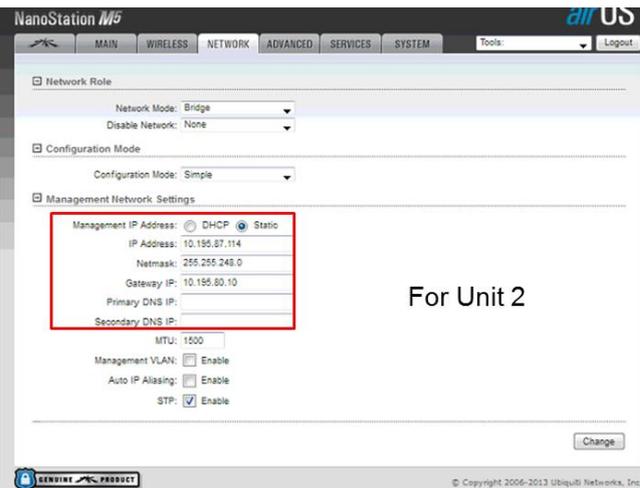
The following table show summary of Wireless Bridge configuration

No.	Task
1	IP, Subnet & Gateway
2	Wireless Mode
3	NTP
4	Hostname

### Part 1: Configure IP, Subnet & Gateway



For Unit 1



For Unit 2

#### Step 1

Go to Network > Management Network Settings

#### Step 2

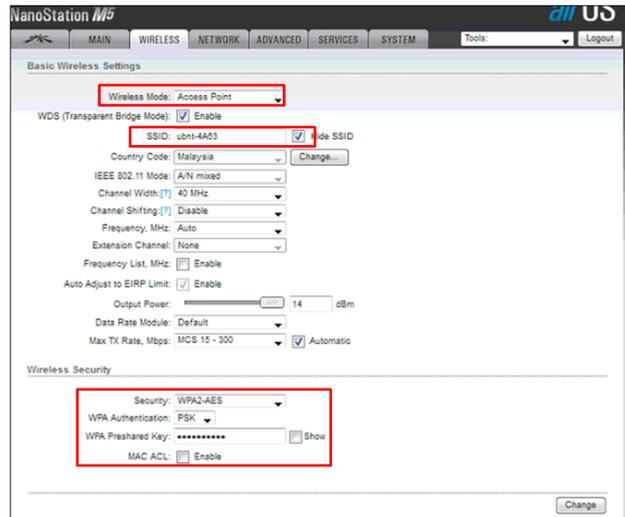
Select Static and Insert Hostname, IP, Subnet, Default Gateway

#### Step 3

Click Change

## Part 2: Configure Wireless Mode

For Unit 1:  
Access Point



### Step 1

Go to Wireless > Basic Wireless Settings

### Step 2

Go to Wireless Mode > Select Access Point

### Step 3

Go to SSID > Insert SSID.

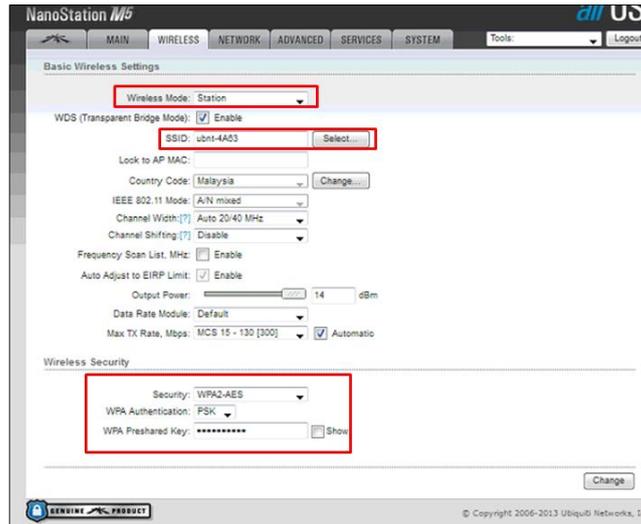
### Step 4

Go to Wireless Security > Security. Select WPA2-AES. Then go to WPAAuthentication > Select PSK. Then go to WPA Preshared Key > Insert password key.

### Step 5

Click Change

For Unit 2:  
Station



### Step 1

Go to Wireless > Basic Wireless Settings

### Step 2

Go to Wireless Mode > Select Station

### Step 3

Go to SSID > Select SSID configured in Unit 1

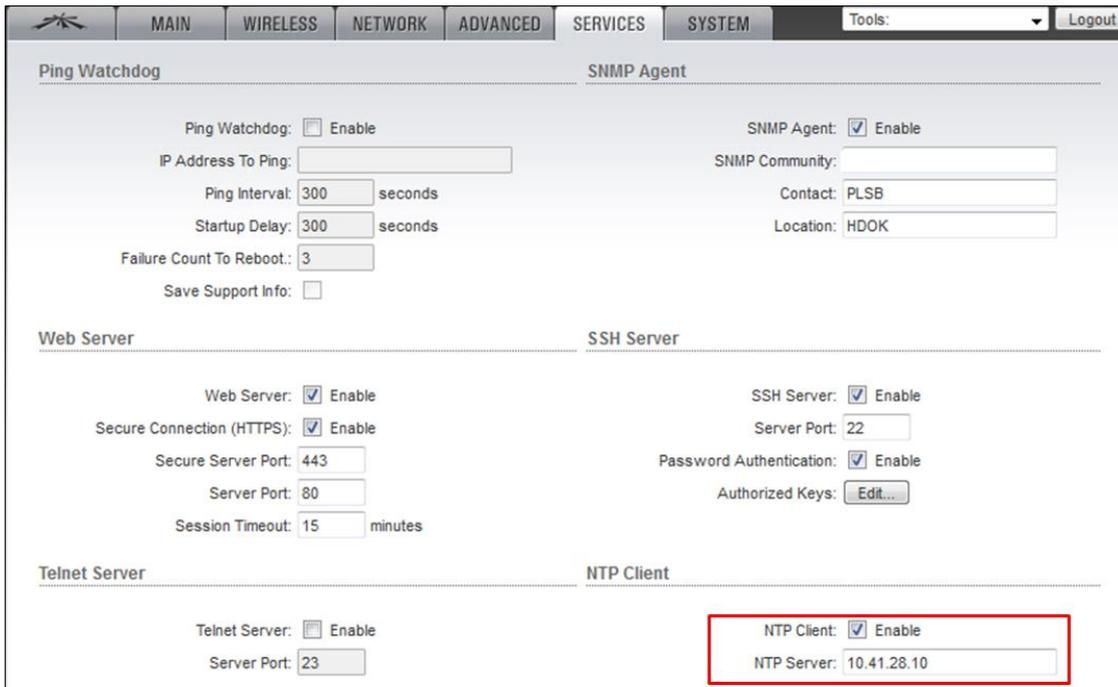
### Step 4

Go to Wireless Security > Security. Select WPA2-AES. Then go to WPAAuthentication > Select PSK. Then go to WPA Preshared Key > Insert password key.

### Step 5

Click Change

### Part 3: Configure NTP



The screenshot shows a web-based configuration interface with a navigation menu at the top: MAIN, WIRELESS, NETWORK, ADVANCED, SERVICES, SYSTEM, Tools, and Logout. The main content area is divided into several sections:

- Ping Watchdog:** Includes checkboxes for 'Enable', input fields for 'IP Address To Ping', 'Ping Interval: 300 seconds', 'Startup Delay: 300 seconds', 'Failure Count To Reboot: 3', and a 'Save Support Info' checkbox.
- SNMP Agent:** Includes checkboxes for 'Enable', input fields for 'SNMP Community', 'Contact: PLSB', and 'Location: HDOK'.
- Web Server:** Includes checkboxes for 'Enable' and 'Secure Connection (HTTPS): Enable', and input fields for 'Secure Server Port: 443', 'Server Port: 80', and 'Session Timeout: 15 minutes'.
- SSH Server:** Includes checkboxes for 'Enable', 'Password Authentication: Enable', and an 'Authorized Keys' button.
- Telnet Server:** Includes checkboxes for 'Enable' and an input field for 'Server Port: 23'.
- NTP Client:** This section is highlighted with a red box. It includes a checked 'Enable' checkbox and an input field for 'NTP Server: 10.41.28.10'.

#### Step 1

Go to Services > NTP Client

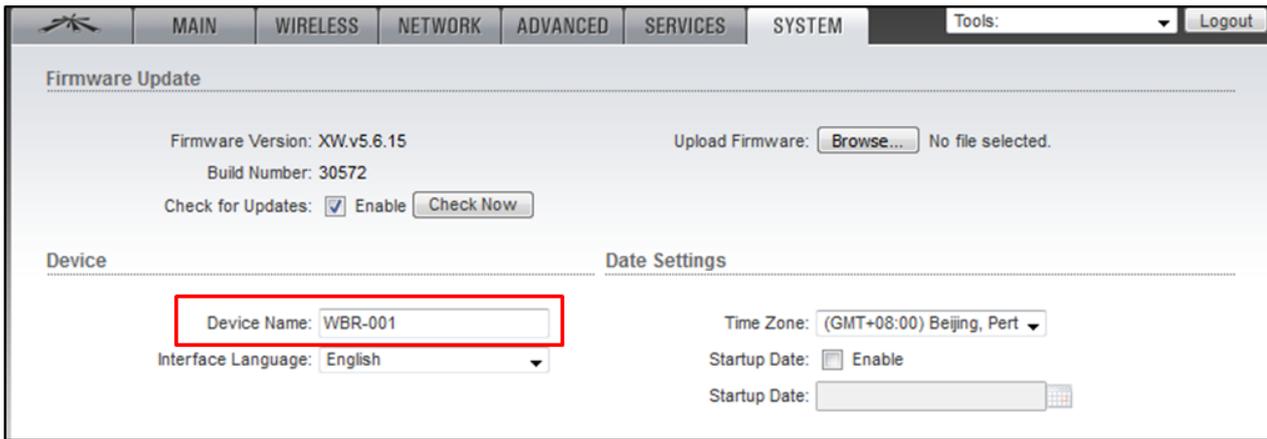
#### Step 2

Click Enable and Insert '10.41.28.10' in NTP Server

#### Step 3

Click Change

## Part 4: Configure Hostname



MAIN WIRELESS NETWORK ADVANCED SERVICES SYSTEM Tools: Logout

Firmware Update

Firmware Version: XW.v5.6.15 Upload Firmware:  No file selected.

Build Number: 30572

Check for Updates:  Enable

Device Date Settings

Device Name:

Interface Language:

Time Zone:

Startup Date:  Enable

Startup Date:

### Step 1

Go to System > Device. Insert Hostname.

### Step 2

Click Change

## 5 Common Issue & Resolution

The following table show summary of common issue encountered in PhIS and how to resolve it.

No	Common Issue
1	PC received IP 169.254.x.x
2	Switch/Port Faulty
3	Network Looping
4	IP Conflict
5	Rogue DHCP Server
6	Network Flood
7	STP Issue

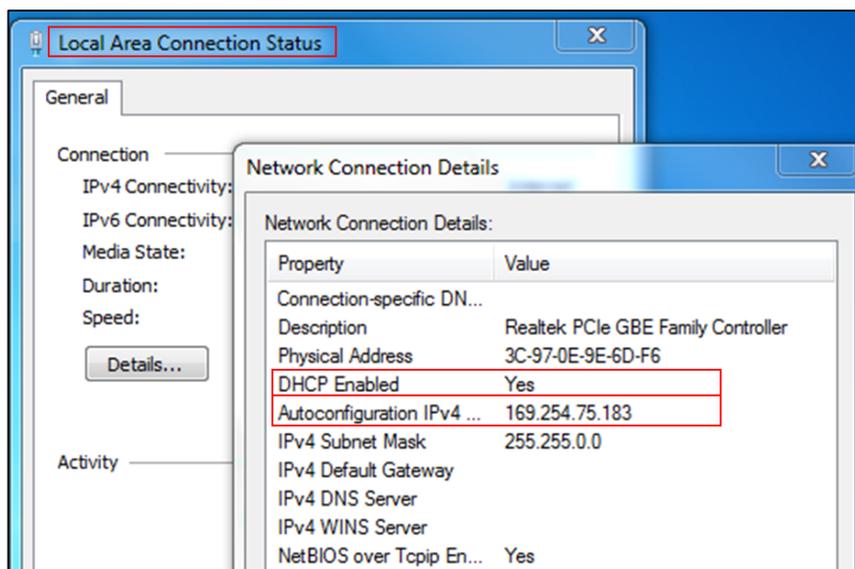
Issue 1: PC received IP 169.254.x.xx IP

**Description:**

PC received DHCP IP from APIPA when there is no DHCP server available. May due to DHCP Server is down or switch BB/Uplink issue.

**Resolution:**

Get DHCP Server to be online/up, change BB/Uplink switchport, replace switch, repair BB cable.



## Issue 2: Switch/Port Faulty

### Description:

Physical scenario of faulty switch/port based on switch LED.

### Resolution:

Replace switch or change switchport.



System LED OFF  
Port LED ON



System LED OFF  
Port LED OFF



System LED OFF  
Port LED ON



System LED ON  
Port LED ON

### Issue 3: Network Looping

**Description:**

Loop (multiple links between two endpoints). Endpoints can be between two network switches or two ports on same switch connected to each other. Caused broadcast storm in every switchport.

**Resolution:**

Trace offended port in switch log or check physically cable at switch & disconnect it.



```
C:\PuttyLog\10.195.95.116-20181017-141343.txt (4 hits)
Line 16: DSW-007-DNI192607SH#sh system17-Oct-2018 14:10:21 %STP-W-PORSTATUS: gi26: STP status Blocking
Line 215: 17-Oct-2018 14:10:21 :%STP-W-PORSTATUS: gi26: STP status Blocking
Line 2549: 12-Oct-2018 11:59:19 :%STP-W-PORSTATUS: gi26: STP status Blocking
Line 2557: 12-Oct-2018 11:39:03 :%STP-W-PORSTATUS: gi26: STP status Blocking
```

## Issue 4: IP Conflict

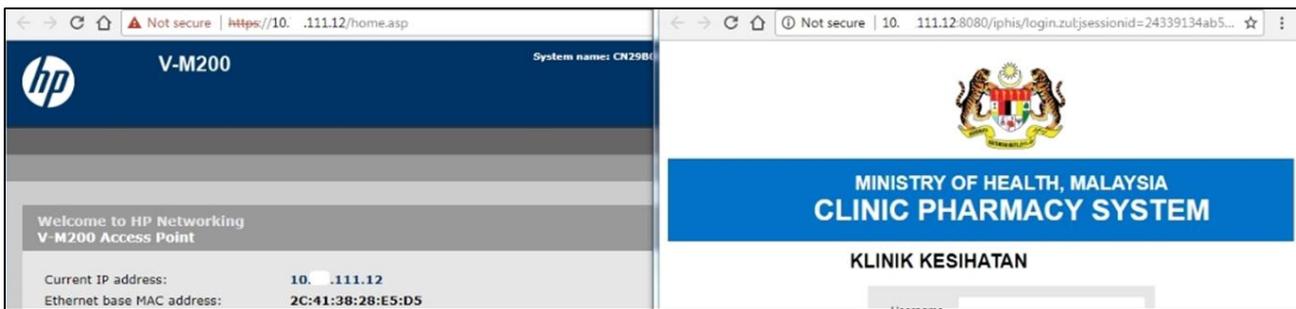
### Description:

PhIS Server IP is used by existing/unknown device. Caused PhIS inaccessible or intermittent access.

### Resolution:

Trace & isolate conflicted device from network or change device IP.

```
:~ # arping 10. .88.12
ARPING 10. .88.12 from 10. .88.14 eth0
Unicast reply from 10. .88.12 [08:94:EF:05:EA:F0] 0.755ms
Unicast reply from 10. .88.12 [94:0C:6D:A6:72:B3] 28.565ms
Unicast reply from 10. .88.12 [94:0C:6D:A6:72:B3] 1.541ms
Unicast reply from 10. .88.12 [94:0C:6D:A6:72:B3] 8.007ms
Unicast reply from 10. .88.12 [94:0C:6D:A6:72:B3] 517.971ms
Unicast reply from 10. .88.12 [94:0C:6D:A6:72:B3] 457.422ms
Unicast reply from 10. .88.12 [94:0C:6D:A6:72:B3] 27.795ms
```



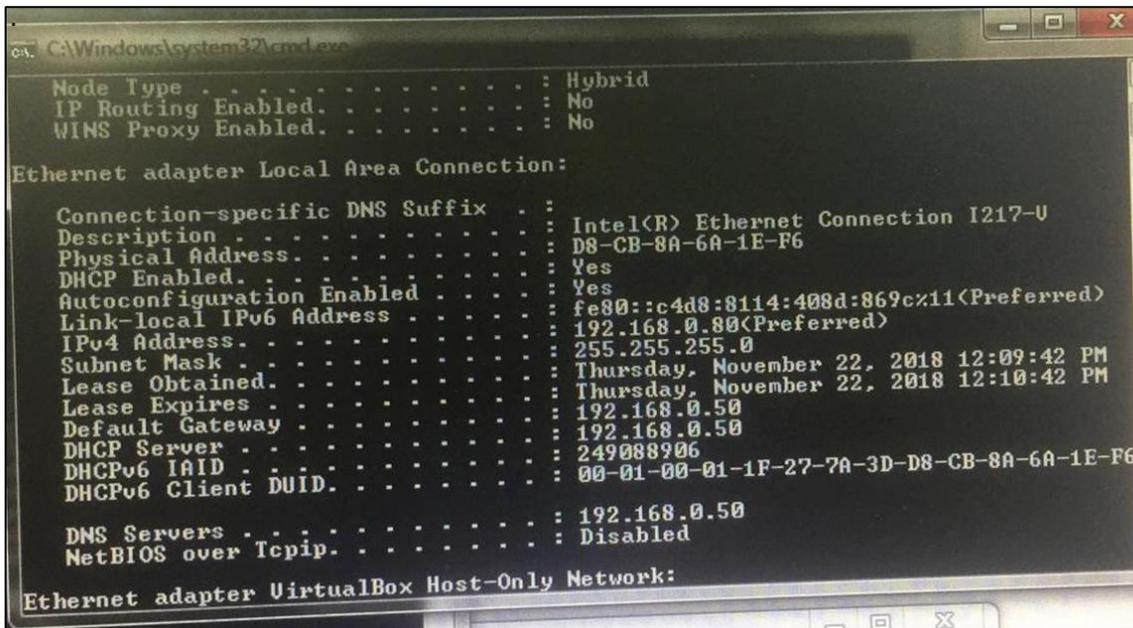
## Issue 5: Rogue/Unauthorized DHCP Server

### Description:

Rogues DHCP Server is unauthorized/illegitimate DHCP server connected to network. PhIS PC will received unknown DHCP pool from Rogue DHCP Server. Caused PhIS inaccessible

### Resolution:

Identify & isolate rogue device from network or disable dhcp server in device configuration.



```
ca. C:\Windows\system32\cmd.exe
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . . . : 
Description . . . . . : Intel(R) Ethernet Connection I217-U
Physical Address. . . . . : D8-CB-8A-6A-1E-F6
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::c4d8:8114:408d:869c%11(Preferred)
IPv4 Address. . . . . : 192.168.0.80(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Thursday, November 22, 2018 12:09:42 PM
Lease Expires . . . . . : Thursday, November 22, 2018 12:10:42 PM
Default Gateway . . . . . : 192.168.0.50
DHCP Server . . . . . : 249088906
DHCPv6 IAD . . . . . : 00-01-00-01-1F-27-7A-3D-D8-CB-8A-6A-1E-F6
DHCPv6 Client DUID. . . . . : 

DNS Servers . . . . . : 192.168.0.50
NetBIOS over Tcpip. . . . . : Disabled

Ethernet adapter VirtualBox Host-Only Network:
```

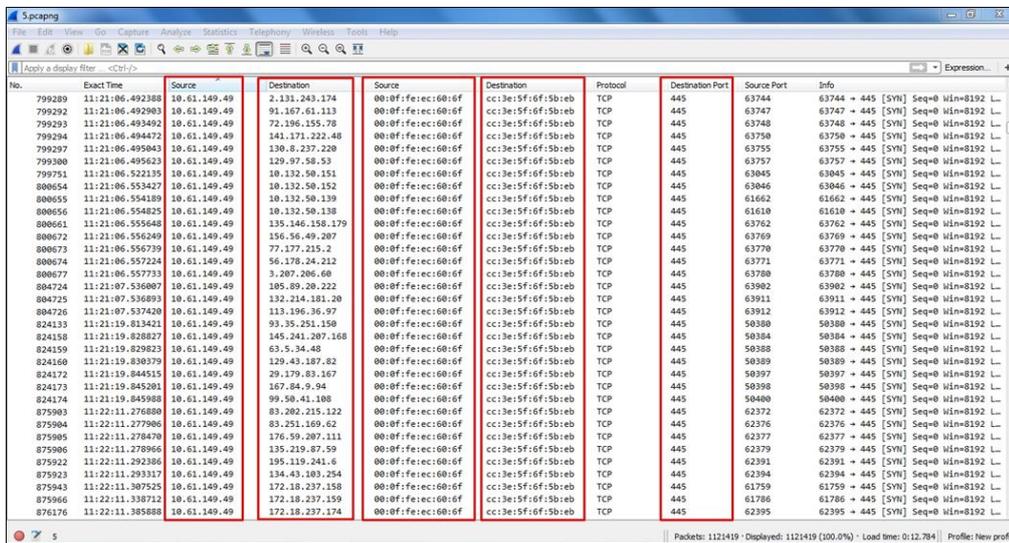
## Issue 6: Network Flood - Scenario 1

### Description:

Network flooded with SYN(TCP 445) Packets that may caused traffic congestion. TCP 445 is used for Server Message Block(SMB) protocol to provide shared access to files, printers, etc. Ransomware(Wannacry) is using same port.

### Resolution:

Identify & isolate offended machine from network.



No.	Exact Time	Source	Destination	Source	Destination	Protocol	Destination Port	Source Port	Info
799289	11:21:06.492388	10.61.149.49	2.131.243.174	00:0f:fec6:00:0f	cc:3e:5f:6f:5b:eb	TCP	445	63744	63744 → 445 [SYN] Seq=0 Win=8192 L...
799292	11:21:06.492903	10.61.149.49	91.167.61.113	00:0f:fec6:00:0f	cc:3e:5f:6f:5b:eb	TCP	445	63747	63747 → 445 [SYN] Seq=0 Win=8192 L...
799293	11:21:06.493492	10.61.149.49	72.196.155.78	00:0f:fec6:00:0f	cc:3e:5f:6f:5b:eb	TCP	445	63748	63748 → 445 [SYN] Seq=0 Win=8192 L...
799294	11:21:06.494472	10.61.149.49	141.171.222.48	00:0f:fec6:00:0f	cc:3e:5f:6f:5b:eb	TCP	445	63750	63750 → 445 [SYN] Seq=0 Win=8192 L...
799297	11:21:06.495843	10.61.149.49	130.8.237.220	00:0f:fec6:00:0f	cc:3e:5f:6f:5b:eb	TCP	445	63755	63755 → 445 [SYN] Seq=0 Win=8192 L...
799300	11:21:06.495623	10.61.149.49	129.97.56.53	00:0f:fec6:00:0f	cc:3e:5f:6f:5b:eb	TCP	445	63757	63757 → 445 [SYN] Seq=0 Win=8192 L...
799751	11:21:06.522135	10.61.149.49	10.132.50.151	00:0f:fec6:00:0f	cc:3e:5f:6f:5b:eb	TCP	445	63845	63845 → 445 [SYN] Seq=0 Win=8192 L...
800654	11:21:06.553427	10.61.149.49	10.132.50.152	00:0f:fec6:00:0f	cc:3e:5f:6f:5b:eb	TCP	445	63846	63846 → 445 [SYN] Seq=0 Win=8192 L...
800655	11:21:06.554189	10.61.149.49	10.132.50.139	00:0f:fec6:00:0f	cc:3e:5f:6f:5b:eb	TCP	445	61662	61662 → 445 [SYN] Seq=0 Win=8192 L...
800656	11:21:06.554825	10.61.149.49	10.132.50.138	00:0f:fec6:00:0f	cc:3e:5f:6f:5b:eb	TCP	445	61610	61610 → 445 [SYN] Seq=0 Win=8192 L...
800661	11:21:06.555648	10.61.149.49	135.146.150.179	00:0f:fec6:00:0f	cc:3e:5f:6f:5b:eb	TCP	445	63762	63762 → 445 [SYN] Seq=0 Win=8192 L...
800672	11:21:06.556249	10.61.149.49	156.56.49.207	00:0f:fec6:00:0f	cc:3e:5f:6f:5b:eb	TCP	445	63769	63769 → 445 [SYN] Seq=0 Win=8192 L...
800673	11:21:06.556739	10.61.149.49	77.177.215.2	00:0f:fec6:00:0f	cc:3e:5f:6f:5b:eb	TCP	445	63770	63770 → 445 [SYN] Seq=0 Win=8192 L...
800674	11:21:06.557224	10.61.149.49	56.170.24.212	00:0f:fec6:00:0f	cc:3e:5f:6f:5b:eb	TCP	445	63771	63771 → 445 [SYN] Seq=0 Win=8192 L...
800677	11:21:06.557733	10.61.149.49	3.207.206.60	00:0f:fec6:00:0f	cc:3e:5f:6f:5b:eb	TCP	445	63780	63780 → 445 [SYN] Seq=0 Win=8192 L...
804724	11:21:07.536007	10.61.149.49	105.89.20.222	00:0f:fec6:00:0f	cc:3e:5f:6f:5b:eb	TCP	445	63902	63902 → 445 [SYN] Seq=0 Win=8192 L...
804725	11:21:07.536893	10.61.149.49	132.214.181.20	00:0f:fec6:00:0f	cc:3e:5f:6f:5b:eb	TCP	445	63911	63911 → 445 [SYN] Seq=0 Win=8192 L...
804726	11:21:07.537420	10.61.149.49	113.196.36.97	00:0f:fec6:00:0f	cc:3e:5f:6f:5b:eb	TCP	445	63912	63912 → 445 [SYN] Seq=0 Win=8192 L...
824133	11:21:19.813421	10.61.149.49	93.35.251.150	00:0f:fec6:00:0f	cc:3e:5f:6f:5b:eb	TCP	445	50380	50380 → 445 [SYN] Seq=0 Win=8192 L...
824150	11:21:19.820827	10.61.149.49	145.241.207.168	00:0f:fec6:00:0f	cc:3e:5f:6f:5b:eb	TCP	445	50384	50384 → 445 [SYN] Seq=0 Win=8192 L...
824159	11:21:19.829823	10.61.149.49	63.5.34.48	00:0f:fec6:00:0f	cc:3e:5f:6f:5b:eb	TCP	445	50388	50388 → 445 [SYN] Seq=0 Win=8192 L...
824160	11:21:19.830379	10.61.149.49	129.43.187.82	00:0f:fec6:00:0f	cc:3e:5f:6f:5b:eb	TCP	445	50389	50389 → 445 [SYN] Seq=0 Win=8192 L...
824172	11:21:19.844515	10.61.149.49	29.179.83.167	00:0f:fec6:00:0f	cc:3e:5f:6f:5b:eb	TCP	445	50397	50397 → 445 [SYN] Seq=0 Win=8192 L...
824173	11:21:19.845201	10.61.149.49	167.84.9.94	00:0f:fec6:00:0f	cc:3e:5f:6f:5b:eb	TCP	445	50398	50398 → 445 [SYN] Seq=0 Win=8192 L...
824174	11:21:19.845988	10.61.149.49	99.50.41.108	00:0f:fec6:00:0f	cc:3e:5f:6f:5b:eb	TCP	445	50400	50400 → 445 [SYN] Seq=0 Win=8192 L...
875903	11:22:11.276800	10.61.149.49	83.202.215.122	00:0f:fec6:00:0f	cc:3e:5f:6f:5b:eb	TCP	445	62372	62372 → 445 [SYN] Seq=0 Win=8192 L...
875904	11:22:11.277906	10.61.149.49	83.251.169.62	00:0f:fec6:00:0f	cc:3e:5f:6f:5b:eb	TCP	445	62376	62376 → 445 [SYN] Seq=0 Win=8192 L...
875905	11:22:11.278470	10.61.149.49	176.59.207.111	00:0f:fec6:00:0f	cc:3e:5f:6f:5b:eb	TCP	445	62377	62377 → 445 [SYN] Seq=0 Win=8192 L...
875906	11:22:11.278966	10.61.149.49	135.219.67.59	00:0f:fec6:00:0f	cc:3e:5f:6f:5b:eb	TCP	445	62379	62379 → 445 [SYN] Seq=0 Win=8192 L...
875922	11:22:11.292306	10.61.149.49	195.119.243.6	00:0f:fec6:00:0f	cc:3e:5f:6f:5b:eb	TCP	445	62391	62391 → 445 [SYN] Seq=0 Win=8192 L...
875923	11:22:11.293317	10.61.149.49	134.43.103.254	00:0f:fec6:00:0f	cc:3e:5f:6f:5b:eb	TCP	445	62394	62394 → 445 [SYN] Seq=0 Win=8192 L...
875943	11:22:11.307525	10.61.149.49	172.18.237.158	00:0f:fec6:00:0f	cc:3e:5f:6f:5b:eb	TCP	445	61759	61759 → 445 [SYN] Seq=0 Win=8192 L...
875966	11:22:11.338712	10.61.149.49	172.18.237.159	00:0f:fec6:00:0f	cc:3e:5f:6f:5b:eb	TCP	445	61786	61786 → 445 [SYN] Seq=0 Win=8192 L...
876176	11:22:11.385808	10.61.149.49	172.18.237.174	00:0f:fec6:00:0f	cc:3e:5f:6f:5b:eb	TCP	445	62395	62395 → 445 [SYN] Seq=0 Win=8192 L...

Note: captured packets using third party software (Wireshark)

Issue 6: Network Flood - Scenario 2

**Description:**

Network flooded with ICMPv6 Packets (Multicast Listener Report) that may caused traffic congestion.

**Resolution:**

Identify & isolate offended machine from network.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	fe80::c23f:d5ff:febc:297e	ff02::1:ff6d:2933	ICMPv6	86	Multicast Listener Report
2	0.000009	fe80::c23f:d5ff:febc:290f	ff02::1:ff6d:2933	ICMPv6	86	Multicast Listener Report
3	0.000013	fe80::c23f:d5ff:febc:28af	ff02::1:ff6d:2933	ICMPv6	86	Multicast Listener Report
4	0.000016	fe80::c23f:d5ff:febc:297e	ff02::1:ff6d:2933	ICMPv6	86	Multicast Listener Report
5	0.000020	fe80::c23f:d5ff:febc:290f	ff02::1:ff6d:2933	ICMPv6	86	Multicast Listener Report
6	0.000023	fe80::c23f:d5ff:febc:28af	ff02::1:ff6d:2933	ICMPv6	86	Multicast Listener Report
7	0.000029	fe80::c23f:d5ff:febc:297e	ff02::1:ff6d:2933	ICMPv6	86	Multicast Listener Report
8	0.000033	fe80::c23f:d5ff:febc:290f	ff02::1:ff6d:2933	ICMPv6	86	Multicast Listener Report
9	0.000358	fe80::c23f:d5ff:febc:28af	ff02::1:ff6d:2933	ICMPv6	86	Multicast Listener Report
10	0.000367	fe80::c23f:d5ff:febc:297e	ff02::1:ff6d:2933	ICMPv6	86	Multicast Listener Report
11	0.000371	fe80::c23f:d5ff:febc:290f	ff02::1:ff6d:2933	ICMPv6	86	Multicast Listener Report
12	0.000375	fe80::c23f:d5ff:febc:28af	ff02::1:ff6d:2933	ICMPv6	86	Multicast Listener Report
13	0.000378	fe80::c23f:d5ff:febc:297e	ff02::1:ff6d:2933	ICMPv6	86	Multicast Listener Report
14	0.000381	fe80::c23f:d5ff:febc:290f	ff02::1:ff6d:2933	ICMPv6	86	Multicast Listener Report
15	0.000385	fe80::c23f:d5ff:febc:28af	ff02::1:ff6d:2933	ICMPv6	86	Multicast Listener Report
16	0.001020	fe80::c23f:d5ff:febc:297e	ff02::1:ff6d:2933	ICMPv6	86	Multicast Listener Report
17	0.001030	fe80::c23f:d5ff:febc:290f	ff02::1:ff6d:2933	ICMPv6	86	Multicast Listener Report
18	0.001034	fe80::c23f:d5ff:febc:28af	ff02::1:ff6d:2933	ICMPv6	86	Multicast Listener Report
19	0.001037	fe80::c23f:d5ff:febc:297e	ff02::1:ff6d:2933	ICMPv6	86	Multicast Listener Report
20	0.001041	fe80::c23f:d5ff:febc:290f	ff02::1:ff6d:2933	ICMPv6	86	Multicast Listener Report
21	0.001044	fe80::c23f:d5ff:febc:28af	ff02::1:ff6d:2933	ICMPv6	86	Multicast Listener Report
22	0.001047	fe80::c23f:d5ff:febc:297e	ff02::1:ff6d:2933	ICMPv6	86	Multicast Listener Report
23	0.001053	fe80::c23f:d5ff:febc:290f	ff02::1:ff6d:2933	ICMPv6	86	Multicast Listener Report
24	0.001057	fe80::c23f:d5ff:febc:28af	ff02::1:ff6d:2933	ICMPv6	86	Multicast Listener Report
25	0.001541	fe80::c23f:d5ff:febc:297e	ff02::1:ff6d:2933	ICMPv6	86	Multicast Listener Report
26	0.001551	fe80::c23f:d5ff:febc:290f	ff02::1:ff6d:2933	ICMPv6	86	Multicast Listener Report
27	0.001555	fe80::c23f:d5ff:febc:28af	ff02::1:ff6d:2933	ICMPv6	86	Multicast Listener Report
28	0.001559	HewlettP_0f:70:53	Broadcast	ARP	60	Who has 10.195.80.10? Tell 10
29	0.001564	fe80::c23f:d5ff:febc:297e	ff02::1:ff6d:2933	ICMPv6	86	Multicast Listener Report
30	0.001567	fe80::c23f:d5ff:febc:290f	ff02::1:ff6d:2933	ICMPv6	86	Multicast Listener Report
31	0.001571	fe80::c23f:d5ff:febc:28af	ff02::1:ff6d:2933	ICMPv6	86	Multicast Listener Report
32	0.001574	fe80::c23f:d5ff:febc:297e	ff02::1:ff6d:2933	ICMPv6	86	Multicast Listener Report
33	0.001577	fe80::c23f:d5ff:febc:290f	ff02::1:ff6d:2933	ICMPv6	86	Multicast Listener Report
34	0.001581	fe80::c23f:d5ff:febc:28af	ff02::1:ff6d:2933	ICMPv6	86	Multicast Listener Report

Name: C:\Users\Network Team\Desktop\New folder\Captu...  
 Length: 29 MB  
 Format: Wireshark/... - pcapng  
 Encapsulation: Ethernet

**Time**  
 First packet: 2017-08-21 15:25:52  
 Last packet: 2017-08-21 15:26:06  
 Elapsed: 00:00:13

**Capture**  
 Hardware: Intel(R) Core(TM) i3-4150T CPU @ 3.00GHz (with S...  
 OS: 64-bit Windows 7 Service Pack 1, build 7601  
 Application: Dumpcap (Wireshark) 2.4.0 (v2.4.0-g9be0fa500d)

**Interfaces**  
 Interface: WPP\_ (82EDC2C8-1A97-4580-951A-6E77E0C6328) Dropped packets: 0 (0%)  
 Device: Captured: 248158

**Statistics**  
 Measurement: Captured: 248158  
 Packets: Time span, s: 13.134

Capture file comments

Refresh

Packets: 248158 | Displayed: 248158 (100.0%) | Load time: 0:3.721

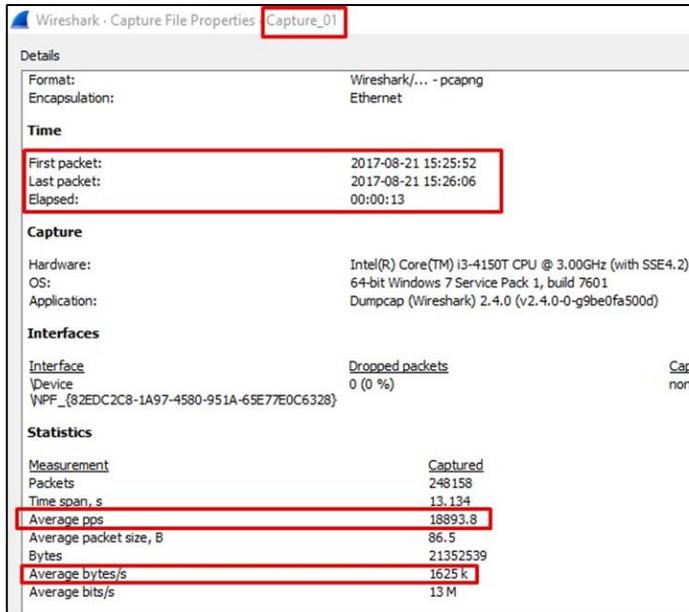
Note: captured packets using third party software (Wireshark)

### Description:

Network flooded with ICMPv6 Packets (Multicast Listener Report) that may caused traffic congestion. Flooded with 18000 packets per second.

### Resolution:

Identify & isolate offended machine from network.



Wireshark - Capture File Properties: Capture\_01

Details

Format: Wireshark/... - pcapng  
Encapsulation: Ethernet

**Time**

First packet: 2017-08-21 15:25:52  
Last packet: 2017-08-21 15:26:06  
Elapsed: 00:00:13

**Capture**

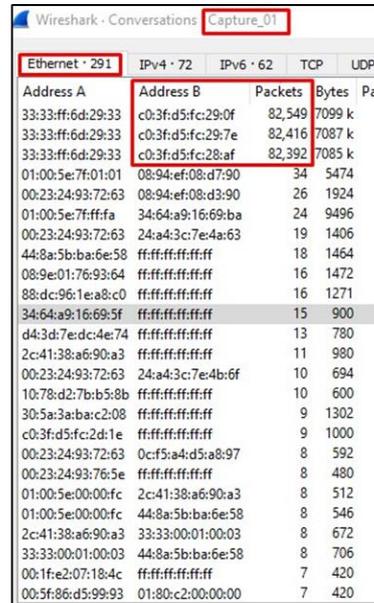
Hardware: Intel(R) Core(TM) i3-4150T CPU @ 3.00GHz (with SSE4.2)  
OS: 64-bit Windows 7 Service Pack 1, build 7601  
Application: Dumpcap (Wireshark) 2.4.0 (v2.4.0-0-g9be0fa500d)

**Interfaces**

Interface	Dropped packets	Capt
\Device\NPF_{82EDC2C8-1A97-4580-951A-65E77E0C6328}	0 (0 %)	none

**Statistics**

Measurement	Captured
Packets	248158
Time span, s	13.134
Average pps	18893.8
Average packet size, B	86.5
Bytes	21352539
Average bytes/s	1625 k
Average bits/s	13 M



Wireshark - Conversations: Capture\_01

Ethernet · 291	IPv4 · 72	IPv6 · 62	TCP	UDP
Address A	Address B	Packets	Bytes	Pac
33:33:ff:6d:29:33	c0:3f:d5:fc:29:0f	82,549	7099 k	
33:33:ff:6d:29:33	c0:3f:d5:fc:29:7e	82,416	7087 k	
33:33:ff:6d:29:33	c0:3f:d5:fc:28:af	82,392	7085 k	
01:00:5e:7f:01:01	08:94:ef:08:d7:90	34	5474	
00:23:24:93:72:63	08:94:ef:08:d3:90	26	1924	
01:00:5e:7f:ff:fa	34:64:a9:16:69:ba	24	9496	
00:23:24:93:72:63	24:a4:3c:7e:4a:63	19	1406	
44:8a:5b:ba:6e:58	ffff:ffff:ffff	18	1464	
08:9e:01:76:93:64	ffff:ffff:ffff	16	1472	
88:dc:96:1e:a8:c0	ffff:ffff:ffff	16	1271	
34:64:a9:16:69:5f	ffff:ffff:ffff	15	900	
d4:3d:7e:dc:4e:74	ffff:ffff:ffff	13	780	
2c:41:38:a6:90:a3	ffff:ffff:ffff	11	980	
00:23:24:93:72:63	24:a4:3c:7e:4b:6f	10	694	
10:78:d2:7b:b5:8b	ffff:ffff:ffff	10	600	
30:5a:3a:ba:c2:08	ffff:ffff:ffff	9	1302	
c0:3f:d5:fc:2d:1e	ffff:ffff:ffff	9	1000	
00:23:24:93:72:63	0c:f5:a4:d5:a8:97	8	592	
00:23:24:93:76:5e	ffff:ffff:ffff	8	480	
01:00:5e:00:00:fc	2c:41:38:a6:90:a3	8	512	
01:00:5e:00:00:fc	44:8a:5b:ba:6e:58	8	546	
2c:41:38:a6:90:a3	33:33:00:01:00:03	8	672	
33:33:00:01:00:03	44:8a:5b:ba:6e:58	8	706	
00:1f:e2:07:18:4c	ffff:ffff:ffff	7	420	
00:5f:86:d5:99:93	01:80:c2:00:00:00	7	420	

Note: captured packets using third party software (Wireshark)

Issue 7: STP

**Description:**

PhIS Switch is using RSTP(default) which may not compatible with facility network design. Caused BB/Uplink connection issue.

**Resolution:**

Current solution is to disable STP at PhIS Switch that having issue.

```
DSW-009-DNI214202L0#sh spanning-tree active
Spanning tree enabled mode RSTP
Default port cost method: long
Loopback guard: Disabled

Root ID    Priority    32768
Address    70:1f:53:e4:89:c5
This switch is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Number of topology changes 0 last change occurred 26:08:57 ago
Times: hold 1, topology change 35, notification 2
hello 2, max age 20, forward delay 15

Interfaces
-----
Name      State Prio.Nbr   Cost   Sts  Role PortFast      Type
-----
gi2       enabled 128.50    20000  Frw  Desg  Yes      P2P (RSTP)
gi25      enabled 112.73    10000  Frw  Desg  Yes      P2P (RSTP)
```

```
<B7-AS2>dis stp
-----[CIST Global Info] [Mode MSTP]-----
CIST Bridge      :32768.001a-c143-1080
Bridge Times     :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC  :32768.0016-e011-0ec0 / 120
CIST RegRoot/IRPC :32768.001a-c143-1080 / 0
CIST RootPortId :128.24
BPDU-Protection :disabled
TC-Protection    :enabled / Threshold=6
Bridge Config
Digest Snooping  :disabled
TC or TCN received :62719
Time since last TC :0 days 0h:1m:21s
```

## 6 References

### Cisco Aironet 1141

- [http://www.cisco.com/en/US/docs/wireless/access\\_point/1140/autonomous/getting\\_started/guide/ap1140aut\\_getstart.html](http://www.cisco.com/en/US/docs/wireless/access_point/1140/autonomous/getting_started/guide/ap1140aut_getstart.html)
- [http://www.cisco.com/en/US/docs/wireless/access\\_point/mounting/guide/apmount.html#wp46770](http://www.cisco.com/en/US/docs/wireless/access_point/mounting/guide/apmount.html#wp46770)
- [http://www.cisco.com/en/US/docs/wireless/access\\_point/1140/autonomous/getting\\_started/guide/ap1140aut\\_getstart.html#wp35993](http://www.cisco.com/en/US/docs/wireless/access_point/1140/autonomous/getting_started/guide/ap1140aut_getstart.html#wp35993)

### Cisco Aironet 1602i

- [https://www.cisco.com/c/en/us/td/docs/wireless/access\\_point/1600/quick/guide/ap1600getstart.html](https://www.cisco.com/c/en/us/td/docs/wireless/access_point/1600/quick/guide/ap1600getstart.html)
- [http://www.cisco.com/en/US/docs/wireless/access\\_point/mounting/guide/apmount.html#wp46770](http://www.cisco.com/en/US/docs/wireless/access_point/mounting/guide/apmount.html#wp46770)
- [https://www.cisco.com/c/en/us/td/docs/wireless/access\\_point/1600/quick/guide/ap1600getstart.html#39770](https://www.cisco.com/c/en/us/td/docs/wireless/access_point/1600/quick/guide/ap1600getstart.html#39770)

### SG500-28

- [http://www.cisco.com/en/US/docs/switches/lan/csbms/Sx500/administration\\_guide/500\\_Series\\_Admin\\_Guide.pdf](http://www.cisco.com/en/US/docs/switches/lan/csbms/Sx500/administration_guide/500_Series_Admin_Guide.pdf)
- [http://www.cisco.com/en/US/docs/switches/lan/csbms/Sx500/cli\\_guide/CLI\\_500.pdf](http://www.cisco.com/en/US/docs/switches/lan/csbms/Sx500/cli_guide/CLI_500.pdf)

### SG300-28

- [http://www.cisco.com/en/US/docs/switches/lan/csbms/sf30x\\_sg30x/quick\\_start/78-19252-01.pdf](http://www.cisco.com/en/US/docs/switches/lan/csbms/sf30x_sg30x/quick_start/78-19252-01.pdf)
- [http://www.cisco.com/en/US/docs/switches/lan/csbms/sf30x\\_sg30x/administration\\_guide/78-19308-01.pdf](http://www.cisco.com/en/US/docs/switches/lan/csbms/sf30x_sg30x/administration_guide/78-19308-01.pdf)

### Dlink DWL-6600APA1

- [http://www.dlink.com/uk/en/-/media/business\\_products/dwl/dwl-6600ap/manual/dwl\\_2600ap\\_3600ap\\_6600ap\\_8600ap\\_8610ap\\_a1\\_manual\\_v5\\_00\\_ww.pdf](http://www.dlink.com/uk/en/-/media/business_products/dwl/dwl-6600ap/manual/dwl_2600ap_3600ap_6600ap_8600ap_8610ap_a1_manual_v5_00_ww.pdf)
- [http://www.dlink.com/uk/en/-/media/business\\_products/dwl/dwl-6600ap/manual/dwl-6600ap-cli-guide-v20.pdf](http://www.dlink.com/uk/en/-/media/business_products/dwl/dwl-6600ap/manual/dwl-6600ap-cli-guide-v20.pdf)
- [http://www.dlink.com/uk/en/-/media/business\\_products/dwl/dwl-6600ap/qig/dwl\\_6600ap\\_a1\\_qig\\_v110.pdf](http://www.dlink.com/uk/en/-/media/business_products/dwl/dwl-6600ap/qig/dwl_6600ap_a1_qig_v110.pdf)

## 7 Acronyms

### Cisco Aironet 1141 & 1602i

Abbreviations	Description
LED	Lights Emitting Diodes
GUI	Graphics User Interface
CLI	Command Line
AP	Access Point

### SG500-28 & SG300-28

Abbreviations	Description
LED	Lights Emitting Diodes
GUI	Graphics User Interface
CLI	Command Line
IP	Internet Protocol
VLAN	Virtual LAN
SSH	Secure Shell
SFP	Small Form-Factor Pluggable

## Appendix A - Switch Operation Guideline

This section describes Switch Operation Guidelines.

Scope of this section covers the following topics:

- Remote access to switch
- Switch monitoring
- Backup and restore switch configuration
- Switch logs

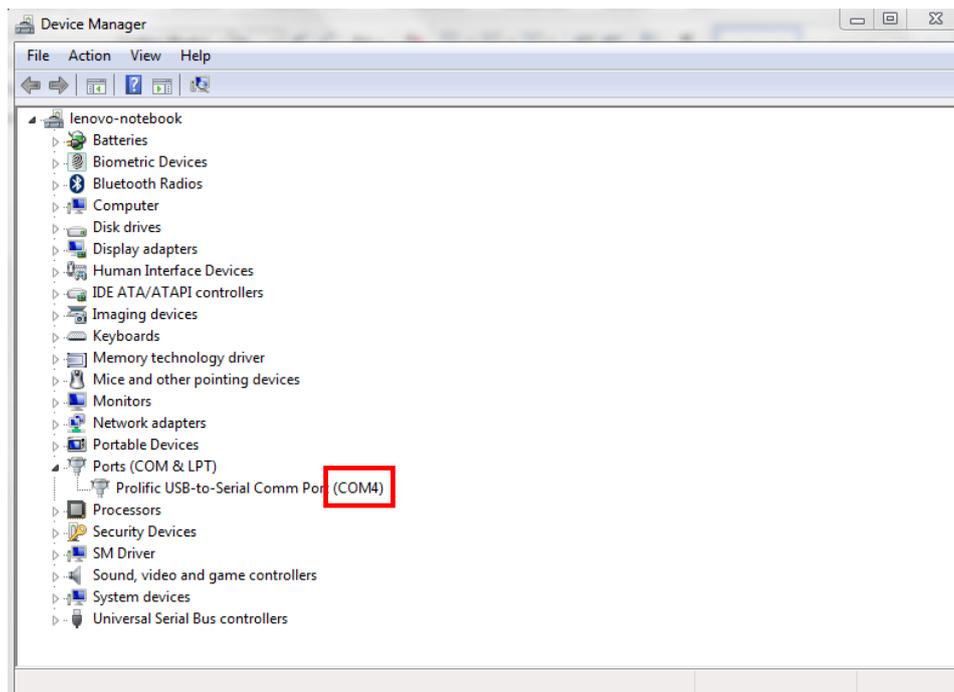
### 1 Remote Access to Switch

There are 3 ways to access the switch through the following method

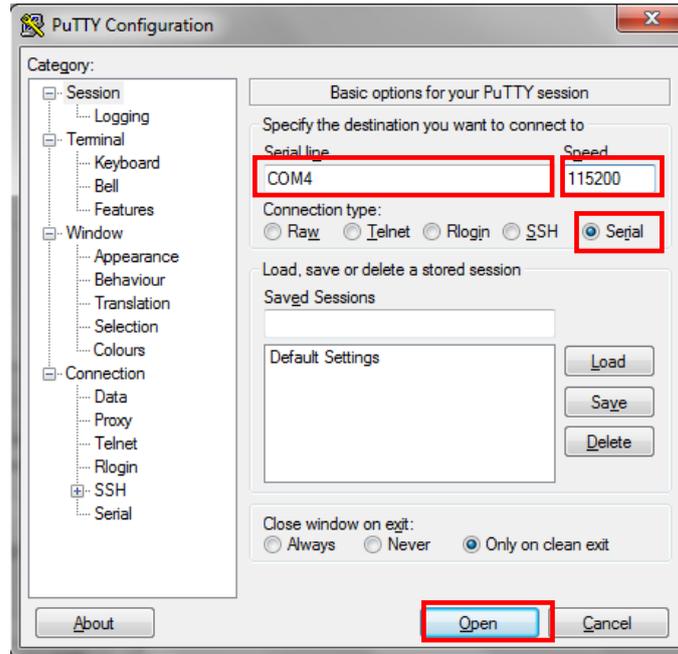
- Console Cable
- Secure Socket Shell (SSH)
- Graphical Web Interface (GUI)

#### 1.1 Console Cable

- Connect USB-to-Serial and console cable to PC / Laptop and plug it PhIS switch **Comm port**. To find out what is the name of your Comm Port, open **Device Manager** and go to Ports (**COM & LPT**)



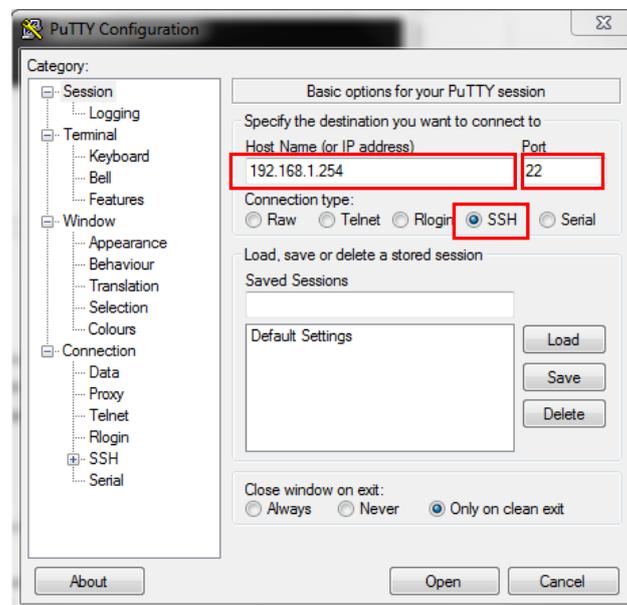
- Open **PuTTY**, under **Connection type** select **Serial** and then fill up the following value and click **Open**
  - **Serial line:** Your Comm port name
  - **Speed:** 115200



- iii. Press **Enter** 2 times and the switch will prompt for enter **User Name** and **Password**. Key in switch user name and password

## 1.2 Secure Socket Shell (SSH)

- i. Open **PuTTY**, select **SSH** and then fill up the following value and click **Open**
- **Host Name (or IP address)**: switch default IP address
  - **Port**: 22



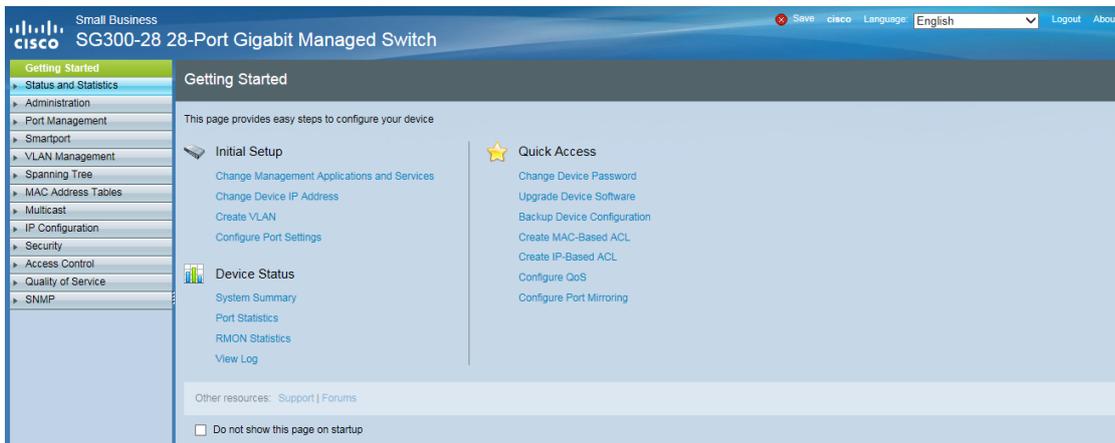
- ii. Switch will prompt for User Name and Password. Key in switch user name and password

### 1.3 Graphical Web Interface (GUI)

- i. Open web browser and key in switch IP address and you will get the following switch login screen



- ii. Key in **Username, Password** and click **Log In**
- iii. The following page will appear once you have successfully login



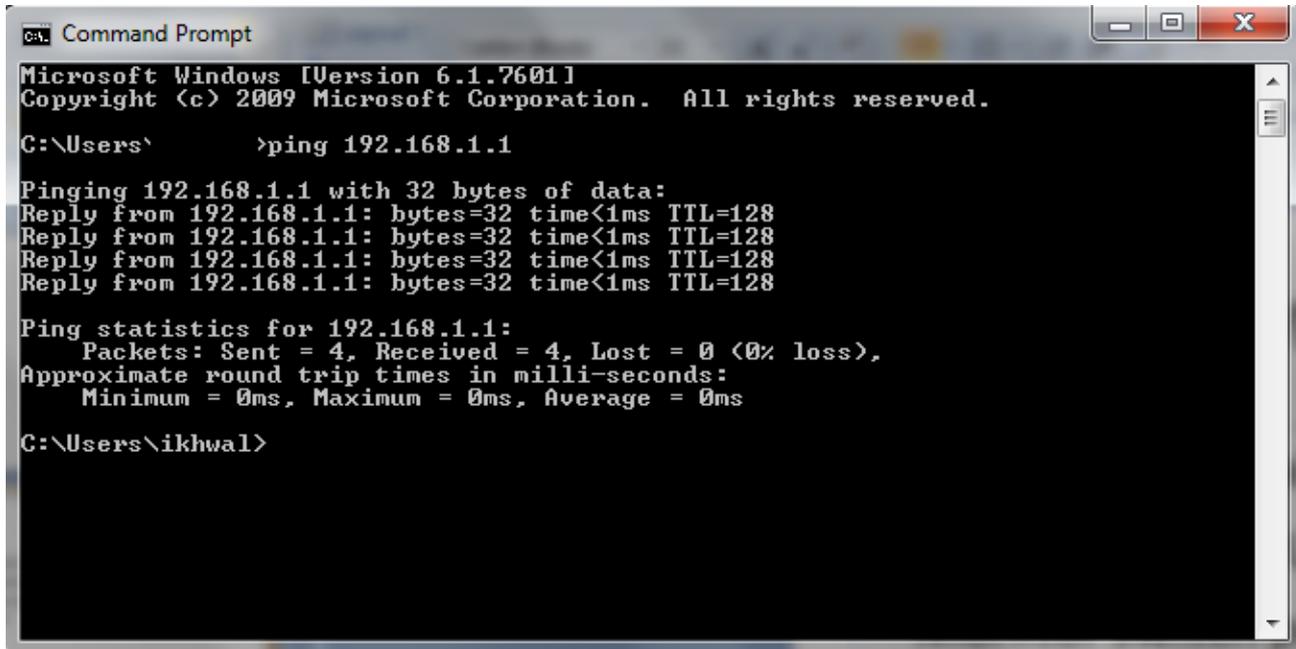
## 1.4 Commonly Used CLI

No.	Command	Description
1	sh run	Display running configuration
2	sh start	Display startup configuration
3	sh system	Display switch information (uptime, MAC, model)
4	sh clock	Display switch time
5	sh system id	Display switch serial number
6	sh system mode	Display switch layer mode
7	sh int status	Display port status information (duplex mode, speed, link state)
8	sh vlan	Display VLAN information
9	sh cdp neighbors detail	Display information about a neighbor (or neighbors) from main cache including network address, enabled protocols, hold time, and software version
10	sh lldp neighbors	Displays information about neighboring devices discovered using LLDP on all ports on which LLDP is enabled and who are up
11	sh spanning-tree active	Display spanning-tree configuration on active port
12	sh spanning-tree blockedports	Display spanning-tree configuration on block port
13	ping x.x.x.x	Send ICMP echo request packets to another node on the network
14	sh arp	Display ARP table entries
15	sh mac address-table address H:H:H:H:H:H	Display address table entries based on specified MAC
16	sh int counter ge x	Display packets and errors statistic on port
17	sh rmon statistics ge x	Display RMON Ethernet statistics on port
18	sh log	Display switch log
19	wr	Save running configuration to startup configuration file

## 2 Switch Monitoring

### 2.1 Check switch availability (PING)

- i. From Desktop, open command prompt and type ping x.x.x.x (where x.x.x.x is switch IP address)
- ii. If the switch is online, you should get reply message from the switch



```
GA. Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\>ping 192.168.1.1

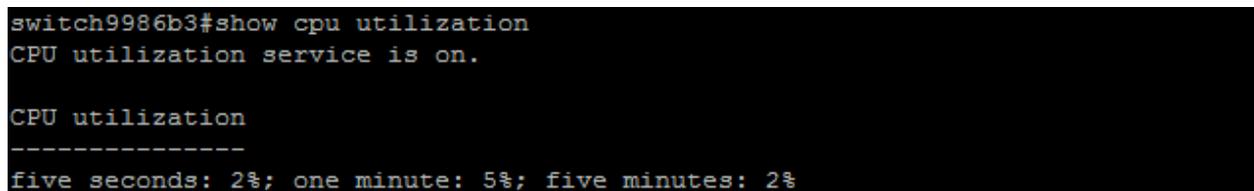
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\ikhwal>
```

### 2.2 Check Switch CPU Utilization (Switch CLI)

- i. Login to switch through console or SSH
- ii. From switch console type show cpu utilization
- iii. The CPU utilization in percentage will be display as below

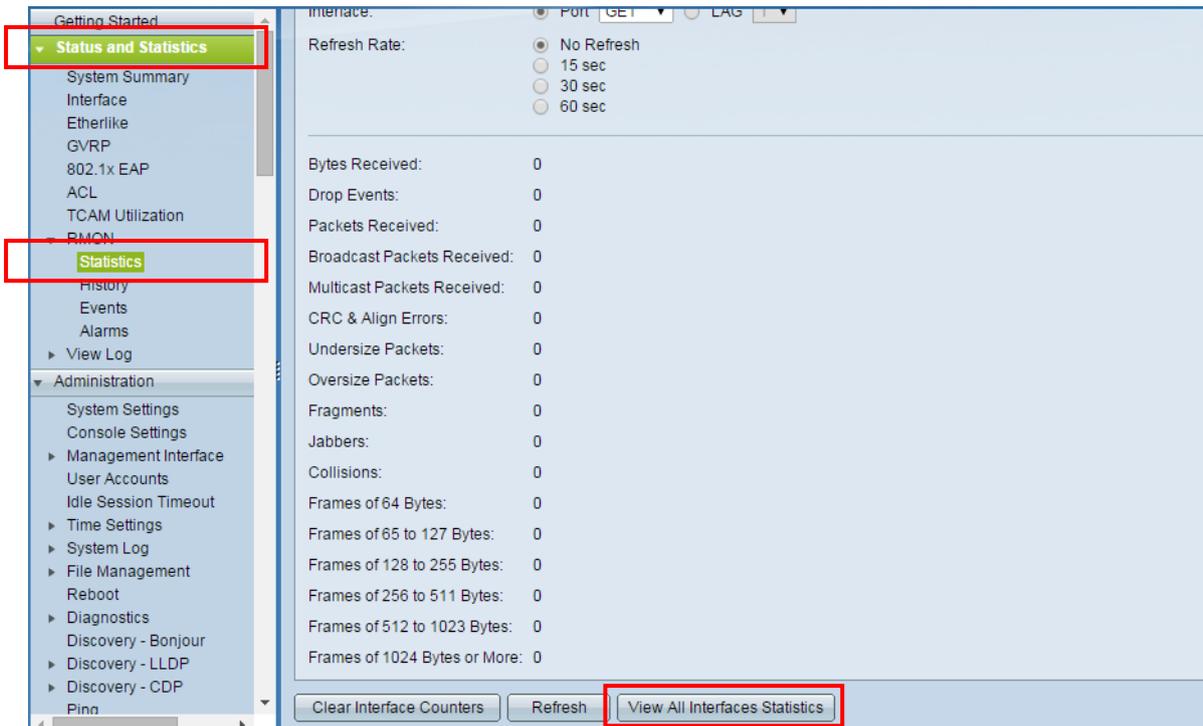


```
switch9986b3#show cpu utilization
CPU utilization service is on.

CPU utilization
-----
five seconds: 2%; one minute: 5%; five minutes: 2%
```

### 2.3 Monitor Switch Ports Status and Errors (Web GUI)

- i. Go to **Status and Statistics -> RMON -> Statistics**
- ii. Click on **View All Interfaces Statistics** button



- i. A table with all switch ports status with CRC errors will be displayed.

RMON Statistics Table														
Filter: Interface Type equals to <span>Port</span> <input type="button" value="Go"/>														
Interface	Bytes Received	Drop Events	Packets Received	Broadcast Packets Received	Multicast Packets Received	CRC & Align Errors	Undersize Packets	Oversize Packets	Fragments	Jabbers	Collisions	Frames of 64 Bytes	Frames of 65 to 127 Bytes	Frames of 128 to 255 Bytes
<input type="radio"/> GE1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<input type="radio"/> GE2	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<input type="radio"/> GE3	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<input type="radio"/> GE4	214797	0	1880	747	319	0	0	0	0	0	0	965	432	0
<input type="radio"/> GE5	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<input type="radio"/> GE6	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<input type="radio"/> GE7	757019	0	5351	951	881	0	0	0	0	0	0	2794	1085	0
<input type="radio"/> GE8	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<input type="radio"/> GE9	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<input type="radio"/> GE10	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<input type="radio"/> GE11	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<input type="radio"/> GE12	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<input type="radio"/> GE13	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<input type="radio"/> GE14	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<input type="radio"/> GE15	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<input type="radio"/> GE16	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<input type="radio"/> GE17	0	0	0	0	0	0	0	0	0	0	0	0	0	0

### 3 Backup and Restore Switch Configuration File

#### 3.1 Backup Switch Configuration File

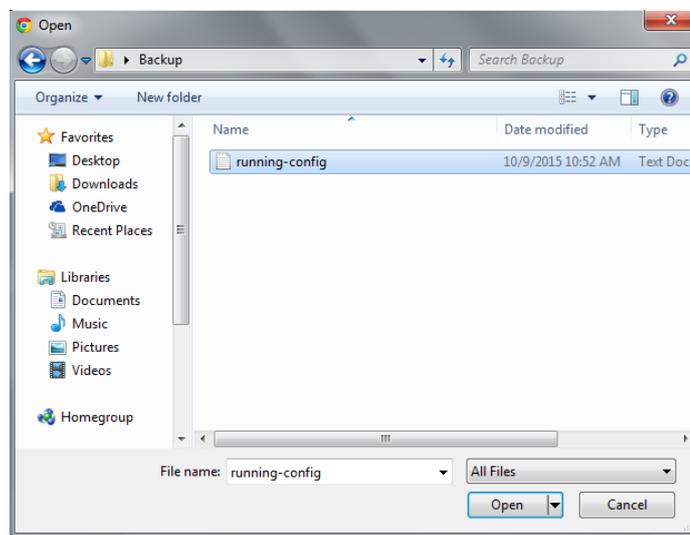
- i. Login to switch through Web
- ii. Go to **Administration -> File Management -> Download/Backup Configuration/Log**



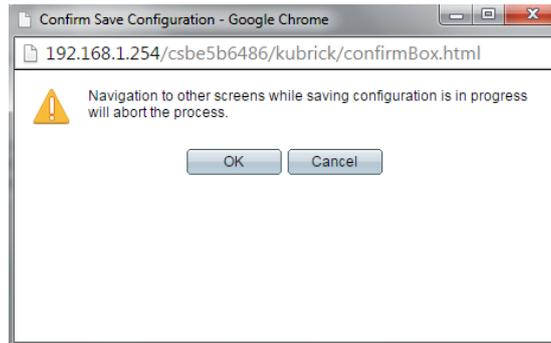
- iii. In **Transfer Method**, select **via HTTP/HTTPS**
- iv. In **Save Action**, select **Backup**
- v. In **Source File Type**, select **Running configuration file**
- vi. In **Sensitive Data**, select **Encrypted**
- vii. Then click **Apply**. The running configuration file will be downloaded into PC.

#### 3.2 Restore Switch Configuration File

- i. Login to switch through Web
- ii. Go to **Administration -> File Management -> Download/Backup Configuration/Log**
- iii. In **Transfer Method**, select **via HTTP/HTTPS**
- iv. In **Save Action**, select **Download**
- v. In **Source File Name**, click **Choose File**. A windows **Open dialog box** will appear. Select which backup file you want to restore and click **Open**.



- vi. In **Destination File Type**, select **Running configuration** then click **Apply**.
- vii. A **Confirm Save Configuration** message box will appear. Click **OK** to proceed



## 4 Switch Logs

### 4.1 View logs through Web Interface

- i. To view the logs, login to switch web interface.
- ii. Go to **Status and Statistics > View Log -> RAM Memory** and the following log screen will be display

Log Index	Log Time	Severity	Description
2147483602	2014-Aug-06 17:48:09	Informational	%AAA-I-CONNECT: New http connection for user cisco, source 192.168.1.1 destination 192.168.1.254 ACCEPTED
2147483603	2014-Aug-06 17:33:55	Informational	%AAA-I-DISCONNECT: http connection for user cisco, source 192.168.1.1 destination 192.168.1.254 TERMINATED
2147483604	2014-Aug-06 17:23:36	Informational	%AAA-I-CONNECT: New http connection for user cisco, source 192.168.1.1 destination 192.168.1.254 ACCEPTED
2147483605	2014-Aug-06 17:20:38	Informational	%AAA-I-DISCONNECT: http connection for user cisco, source 192.168.1.1 destination 192.168.1.254 TERMINATED
2147483606	2014-Aug-06 17:12:51	Notice	%COPY-N-TRAP: The copy operation was completed successfully
2147483607	2014-Aug-06 17:12:48	Informational	%COPY-I-FILECPY: Files Copy - source URL HTTP://192.168.1.1/ destination URL running-config
2147483608	2014-Aug-06 17:04:49	Notice	%COPY-N-TRAP: The copy operation was completed successfully
2147483609	2014-Aug-06 17:04:41	Informational	%COPY-I-FILECPY: Files Copy - source URL running-config destination URL HTTP://192.168.1.1/
2147483610	2014-Aug-06 16:58:39	Informational	%INIT-I-Startup: Cold Startup
2147483611	2014-Aug-06 16:57:59	Informational	%AAA-I-CONNECT: New http connection for user cisco, source 192.168.1.1 destination 192.168.1.254 ACCEPTED
2147483612	2014-Aug-06 16:57:16	Notice	%SYSLOG-N-LOGGING: Logging started.
2147483613	2014-Aug-06 16:56:43	Warning	%STP-W-PORTSTATUS: gi12: STP status Forwarding
2147483614	2014-Aug-06 16:56:38	Informational	%LINK-I-Up: Vlan 1
2147483615	2014-Aug-06 16:56:38	Informational	%LINK-I-Up: gi12
2147483616	2014-Aug-06 16:56:32	Informational	%LINK-I-Up: loopback1
2147483617	2014-Aug-06 16:56:32	Warning	%LINK-W-Down: gi28
2147483618	2014-Aug-06 16:56:32	Warning	%LINK-W-Down: gi27
2147483619	2014-Aug-06 16:56:32	Warning	%LINK-W-Down: gi26
2147483620	2014-Aug-06 16:56:32	Warning	%LINK-W-Down: gi25

### 4.2 Log Message Format

A

B

C

D

Log Index	Log Time	Severity	Description
2147483602	2014-Aug-06 17:48:09	Informational	%AAA-I-CONNECT: New http connection for user cisco, source 192.168.1.1 destination 192.168.1.254 ACCEPTED
2147483603	2014-Aug-06 17:33:55	Informational	%AAA-I-DISCONNECT: http connection for user cisco, source 192.168.1.1 destination 192.168.1.254 TERMINATED

Format Indicator	Field Name	Description
A	Log Index	Running numbers for log indexing
B	Log Time	Timestamp
C	Severity	Please refer severity levels table
D	Description	Description on log / event

### 4.3 Severity Table

The event severity levels are listed from the highest severity to the lowest severity, as follows:

Severity	Severity Level	Code	Description
Emergency	0 - High	M	System is not usable
Alert	1	A	Action is needed
Critical	2	C	System is in a critical condition
Error	3	E	System is in error condition
Warning	4	W	System warning has occurred
Notice	5	N	System is functioning properly, but a system notice has occurred
Informational	6	I	Device information
Debug	7 - Lowest	D	Detailed information about an event

## Appendix B – Access Point Operation Guideline

This section describes Access Point Operation Guidelines.

Scope of this section covers the following topics:

- Remote access to Access Point
- Access Point monitoring
- Backup and restore Access Point configuration
- Access Point logs

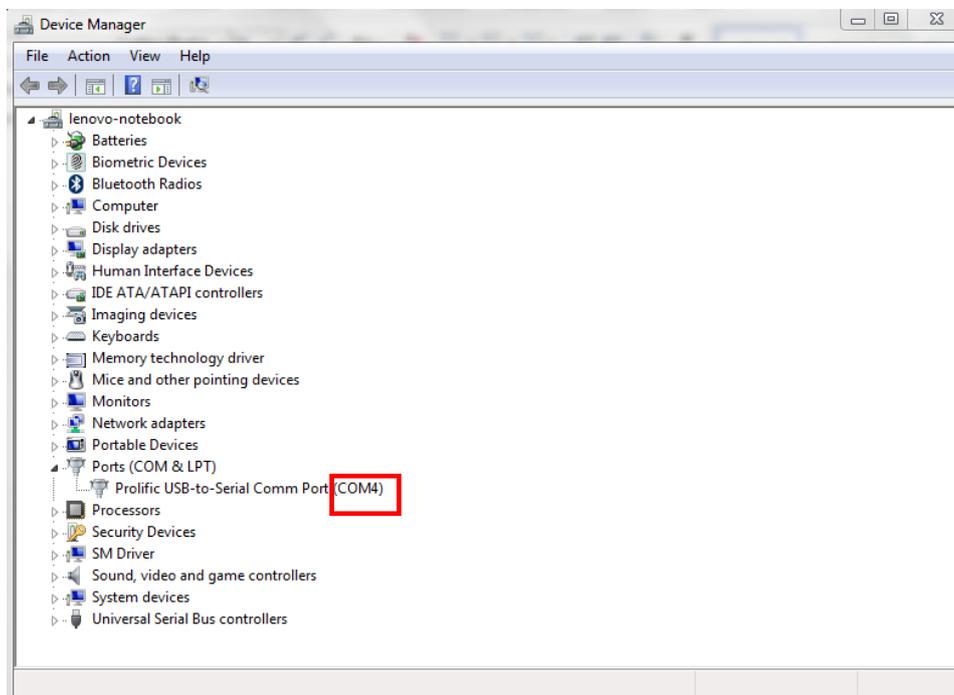
### 1 Remote Access to Access Point

There are 3 ways to access the access point through the following method

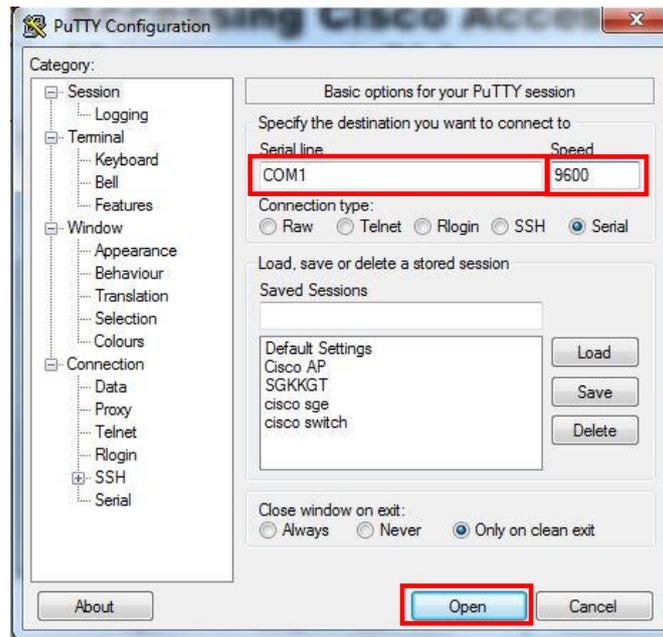
- Console Cable
- Secure Socket Shell (SSH)
- Graphical Web Interface (GUI)

#### 1.1 Console Cable

- i. Connect USB-to-Serial and console cable to PC / Laptop and plug into access point console port.



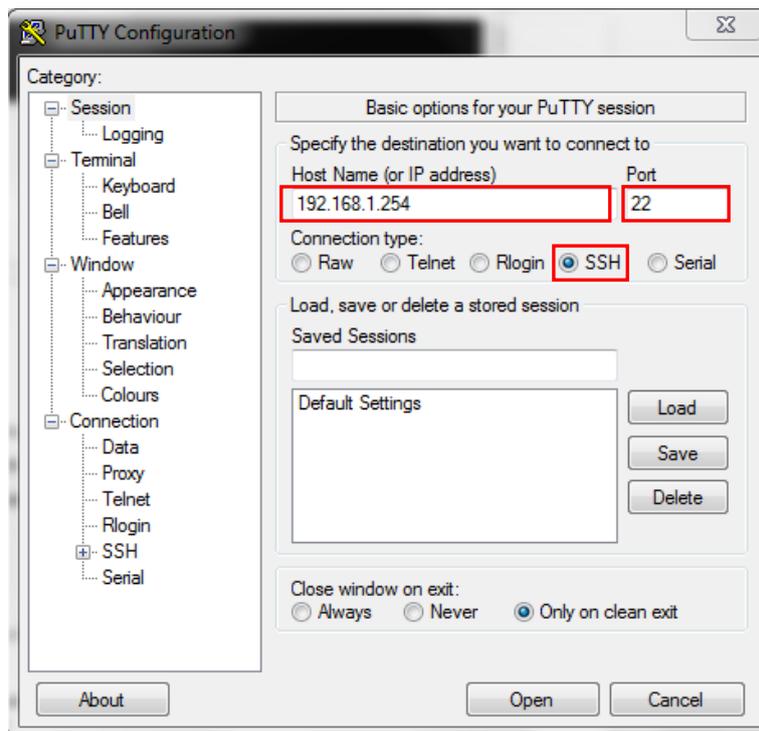
- ii. Open **PuTTY**, under **Connection type** select **Serial** and then fill up the following value and click **Open**
  - **Serial line:** Your Comm port name
  - **Speed:** 9600 (Cisco AP) / 115200 (Dlink AP)



- iii. Press **Enter** 2 times and the switch will prompt for enter **User Name** and **Password**. Key in access point management user name and password

## 1.2 Secure Socket Shell (SSH)

- i. Open **PuTTY**, select **SSH** and then fill up the following value and click **Open**
- **Host Name (or IP address):** access point IP address
  - **Port:** 22



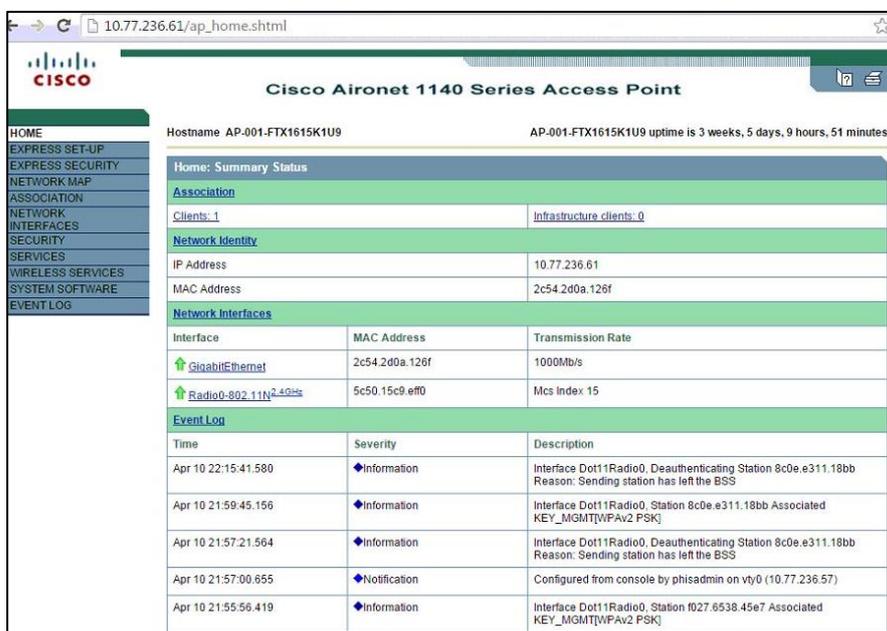
- ii. Access point will prompt for **User Name** and **Password**. Key in access point management user name and password
- iii. Type 'enable' command and key in the management password to go to Priviledge Mode (for Cisco AP only).

```
login as: phisadmin
Using keyboard-interactive authentication.
Password:

AP-001-FTX1615K1U9>enable
Password:
Password:
AP-001-FTX1615K1U9#
```

### 1.3 Graphical Web Interface (GUI)

- i. From Desktop, open browser and type access point IP address
- ii. Key in the management username and password



### 1.4 Commonly Used CLI\*

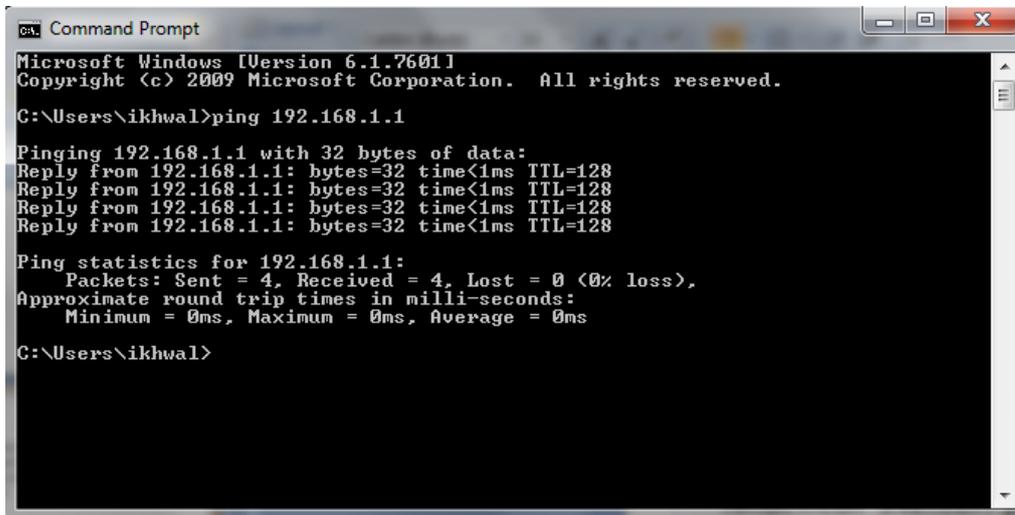
Command Line	Description
show running-config	Show the running configuration
show startup-config	Show the startup configuration
write memory	Save configuration
show vlan	Show configured vlan information
show logging	Show event logs
ping x.x.x.x	Ping to destination IP (where x.x.x.x is destination IP address)

\*for Cisco AP only

## 2 Access Point Monitoring

### 2.1 Check access point availability (PING)

- i. From Desktop, open command prompt and type **ping x.x.x.x** (where x.x.x.x is access point IP address)
- ii. If the access point is online, command prompt should display the ping as below



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\ikhwal>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\ikhwal>
```

### 2.2 Check access point radio status (GUI)

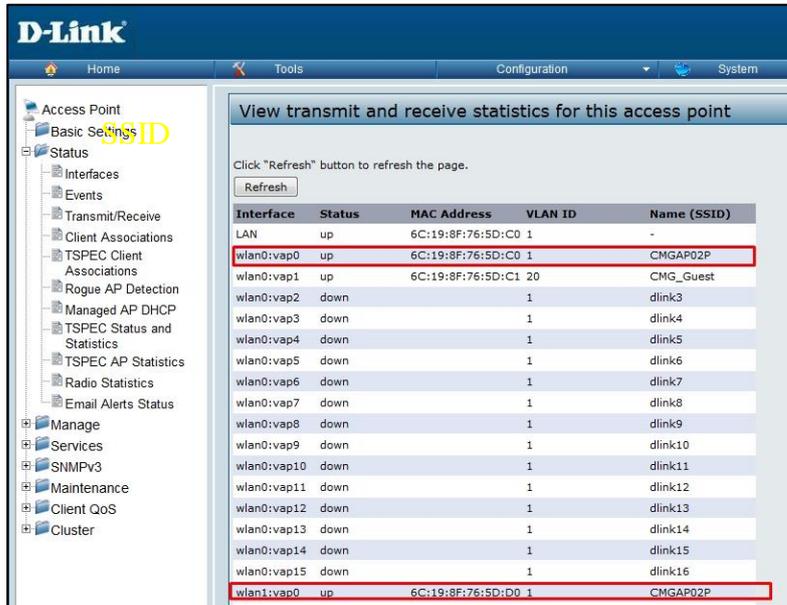
For Cisco AP

- i. From Desktop, open browser and type access point IP address
- ii. In the **Home** menu, go to Network Interfaces
- iii. Check the radio interface. Green arrow indicates that the Radio0-802.11N<sup>2.4GHz</sup> is enabled and the status is UP. Red arrow indicates that either the Radio0-802.11N<sup>2.4GHz</sup> is disabled or the status is down.



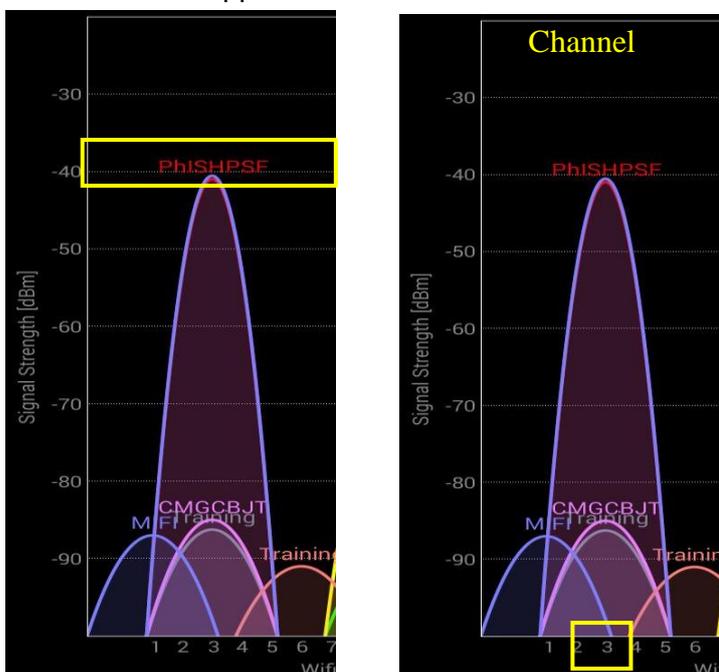
For Dlink AP

- i. From Desktop, open browser and type access point IP address
- ii. In the Home menu, go to Status >> Transmit/Receive
- iii. Check radio interface status. wlan0: vap0 indicate for 5GHz, wlan1: vap0 indicate for 2.4GHz.



### 2.3 Check access point SSID & signal strength (Wifi Analyzer)

- i. From android Wifi Analyzer apps, check the SSID and its signal strength (dBm). It should be more than - 80 dBm within the signal coverage area.
- ii. From android Wifi Analyzer apps, check the access point channel. The access point's channel should be not overlapped with another channel that has strong signal strength (dBm).



### 3 Access Point Logs

#### 3.1 View the access point logs (GUI)

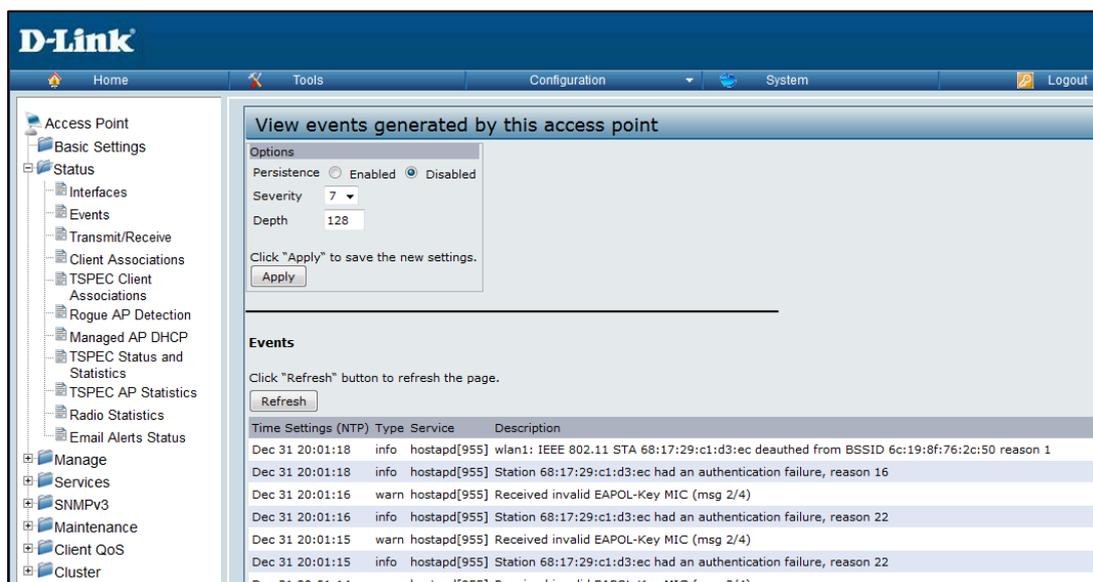
For Cisco AP

- i. From Desktop, open browser and type access point IP address
- ii. Key in the management username and password
- iii. From the main page, go to Event Log >> Configuration options.

Event Log			
Start Display at Index: 1		Max Number of Events to Display: 20	
		<input type="button" value="Previous"/> <input type="button" value="Next"/> <input type="button" value="Refresh"/> <input type="button" value="Clear"/>	
Index	Time	Severity	Description
1	Apr 10 21:02:20.622	Information	Interface Dot11Radio0, Deauthenticating Station 8c0e.e311.18bb Reason: Sending station has left the BSS
2	Apr 10 20:55:18.536	Information	Interface Dot11Radio0, Station 8c0e.e311.18bb Associated KEY_MGMT[WPAv2 PSK]
3	Apr 10 20:52:21.583	Information	Interface Dot11Radio0, Deauthenticating Station 8c0e.e311.18bb Reason: Sending station has left the BSS
4	Apr 10 20:48:14.883	Warning	Packet to client 847a.882c.eb3a reached max retries, removing the client
5	Apr 10 20:48:14.878	Warning	Packet to client 847a.882c.eb3a reached max retries, removing the client
6	Apr 10 20:48:14.857	Warning	Packet to client 847a.882c.eb3a reached max retries, removing the client
7	Apr 10 20:48:14.853	Information	Interface Dot11Radio0, Deauthenticating Station 847a.882c.eb3a Reason: Sending station has left the BSS
8	Apr 10 20:48:11.841	Information	Interface Dot11Radio0, Station 847a.882c.eb3a Associated KEY_MGMT[WPAv2 PSK]
9	Apr 10 20:46:59.467	Information	Interface Dot11Radio0, Station 8c0e.e311.18bb Associated KEY_MGMT[WPAv2 PSK]
10	Apr 10 20:44:23.662	Debugging	Station 503c.c438.4353 Authentication failed
11	Apr 10 20:44:12.645	Debugging	Station 503c.c438.4353 Authentication failed
12	Apr 10 20:44:01.351	Debugging	Station 503c.c438.4353 Authentication failed
13	Apr 10 20:43:50.382	Debugging	Station 503c.c438.4353 Authentication failed

For Dlink DWL-6600APA1

- i. From Desktop, open browser and type access point IP address
- ii. Key in the management username and password
- iii. From the main page, go to Status >> Events.



**View events generated by this access point**

Options

Persistence  Enabled  Disabled

Severity 7

Depth 128

Click "Apply" to save the new settings.

---

**Events**

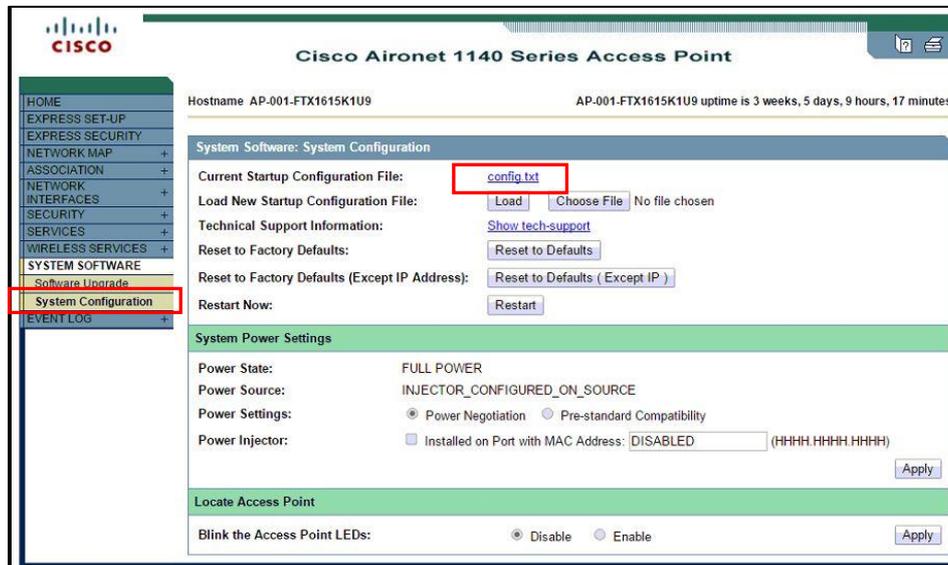
Click "Refresh" button to refresh the page.

Time Settings (NTP)	Type	Service	Description
Dec 31 20:01:18	info	hostapd[955] wlan1: IEEE 802.11 STA 68:17:29:c1:d3:ec deauthed from BSSID 6c:19:8f:76:2c:50 reason 1	
Dec 31 20:01:18	info	hostapd[955]	Station 68:17:29:c1:d3:ec had an authentication failure, reason 16
Dec 31 20:01:16	warn	hostapd[955]	Received invalid EAPOL-Key MIC (msg 2/4)
Dec 31 20:01:16	info	hostapd[955]	Station 68:17:29:c1:d3:ec had an authentication failure, reason 22
Dec 31 20:01:15	warn	hostapd[955]	Received invalid EAPOL-Key MIC (msg 2/4)
Dec 31 20:01:15	info	hostapd[955]	Station 68:17:29:c1:d3:ec had an authentication failure, reason 22
Dec 31 20:01:14	warn	hostapd[955]	Received invalid EAPOL-Key MIC (msg 2/4)

## 4 Backup and Restore Access Point Configuration File (GUI)

### 4.1 Cisco Aironet - Backup Access Point Configuration File (GUI)

- From Desktop, open browser and type access point IP address
- Key in the management username and password
- From the main page, go to **System Software** >> Configuration options
- Click config.txt at Current Startup Configuration File

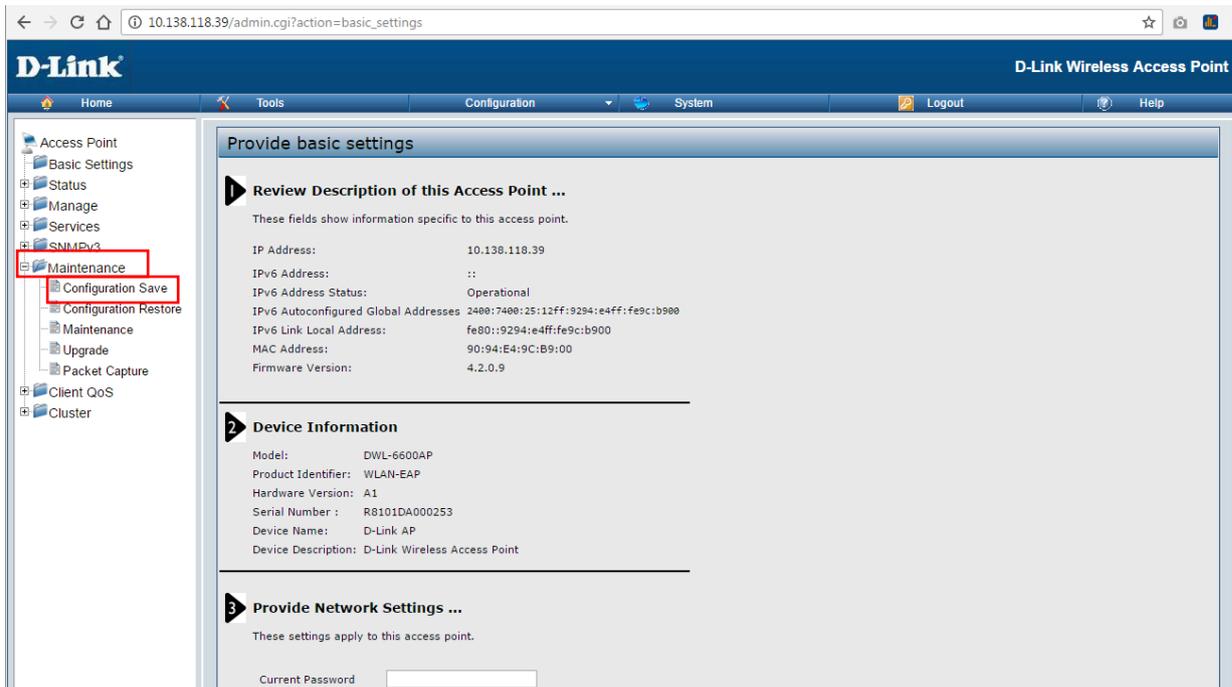


- Select all the text, copy & paste it in the Notepad

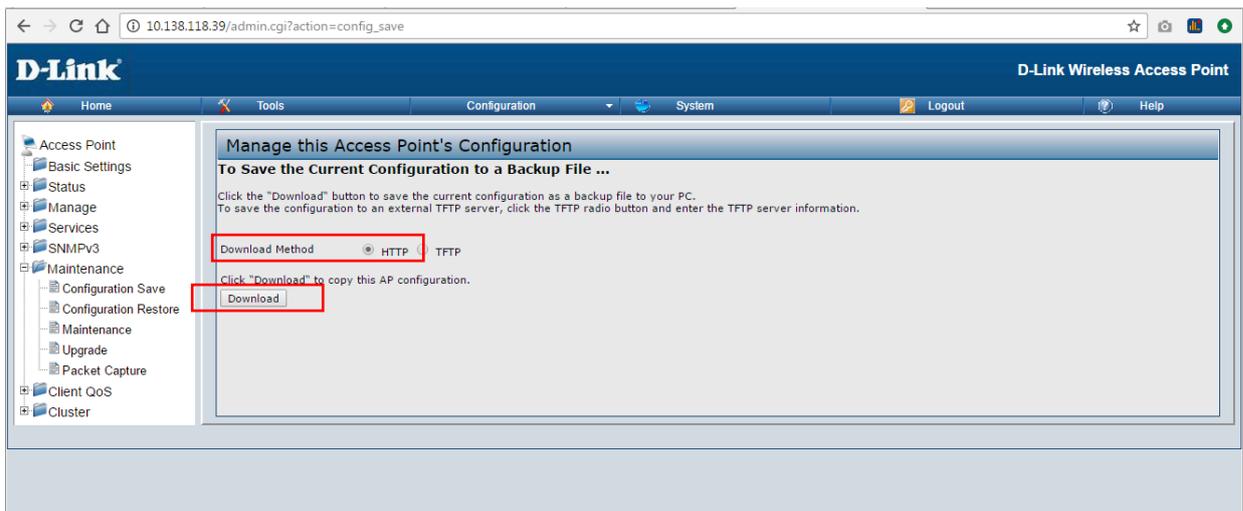
```
!
version 12.4
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname AP-001-FTX1615K1U9
!
enable secret 5 $1$j6Eh$XpTrb
!
no aaa new-model
ip domain name 10.77.236.61
!
dot11 syslog
!
dot11 ssid PHISHPSF
 vlan 999
 authentication open
 authentication key-management wpa version 2
 guest-mode
 infrastructure-ssid optional
 wpa-psk ascii 7 071F291D1821295031
!
!
username phishpsf privilege 15 password 7 001418575173385329
username phisadmin password 7 045A0F9B5E2F647E5C3F
!
!
bridge irb
!
!
interface Dot11Radio0
 no ip address
 no ip route-cache
!
 encryption mode ciphers aes-ccm tkip
!
 encryption vlan 1 mode ciphers aes-ccm tkip
!
 encryption vlan 999 mode ciphers aes-ccm tkip
!
```

## 4.2 D-Link AP - Backup Access Point Configuration File (GUI)

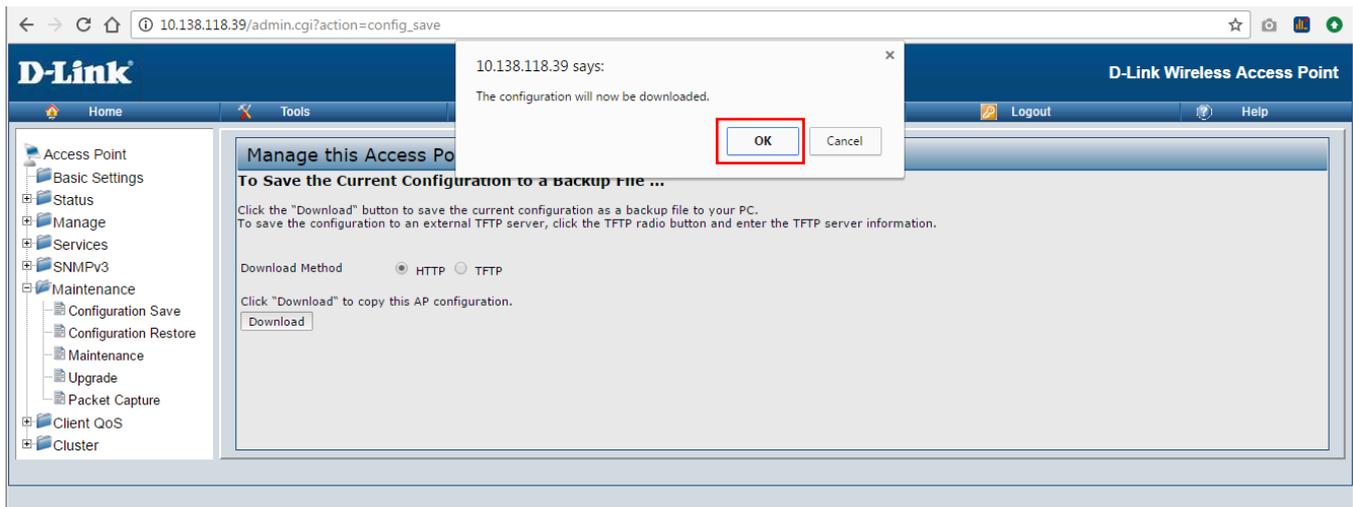
- i. From D-Link main page, expand **Maintenance** and click on **Configuration Save**.



- ii. Choose **HTTP** as download method.
- iii. To save the current configuration to a Backup file, click on **Download** button.

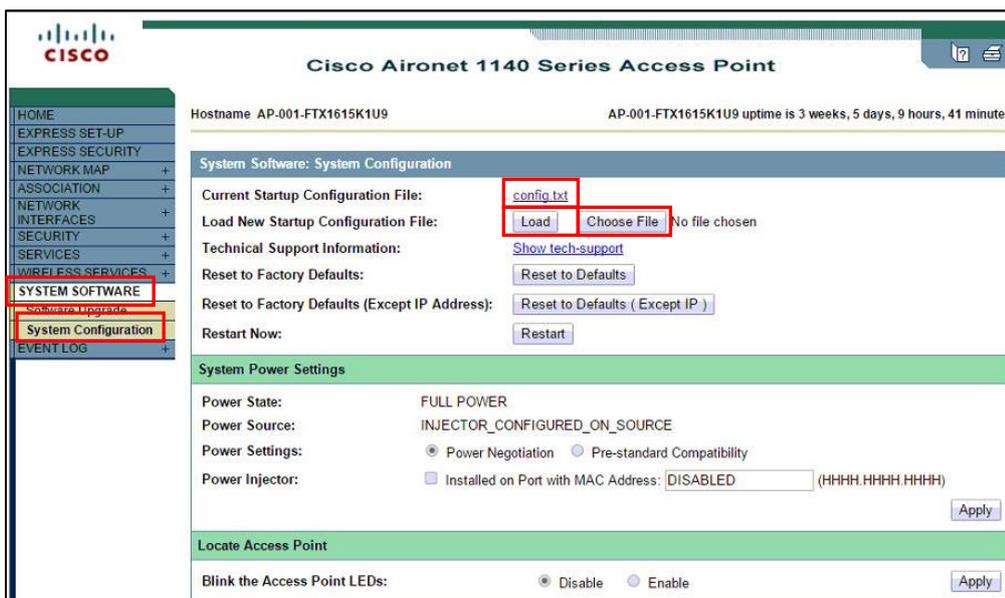


- iv. Click **OK** to download the configuration file in .XML file format.



### 4.3 Cisco Aironet - Restore Access Point Configuration File (GUI)

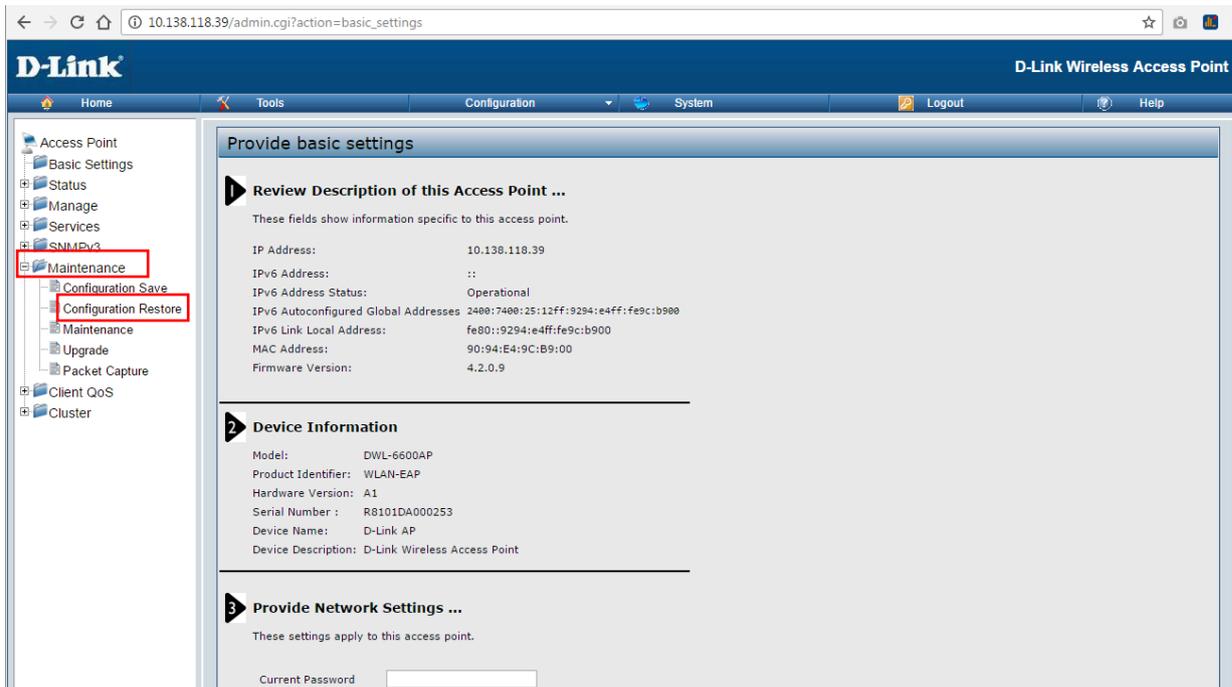
- i. From Desktop, open browser and type access point IP address
- ii. Key in the username and password
- iii. From the main page, go to **System Software** >> System Configuration
- iv. Click the Choose File button to browse the configuration file.
- v. Click Load button to upload the file.



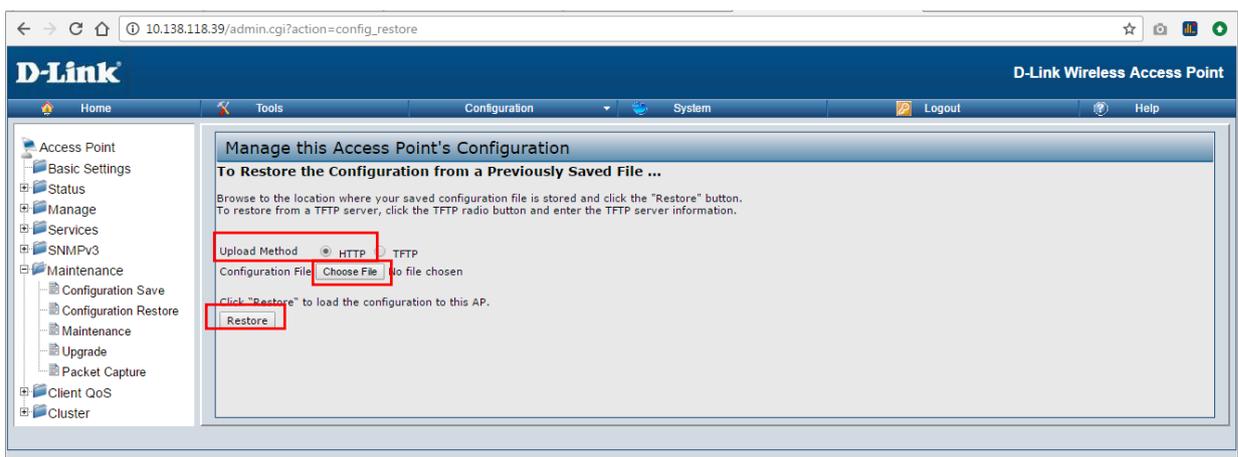
- vi. Then a pop-up will appear. Click OK. After that, the browser will prompt the login credentials. Key in the username and password to proceed. Then click OK. Another pop-up will appear; it indicates that the AP is saving the configuration.

#### 4.4 D-Link AP - Restore Access Point Configuration File (GUI)

- i. From D-Link main page, expand **Maintenance** and click on **Configuration Restore**.



- ii. Choose **HTTP** as upload method.
- iii. Click on **Choose File** button to upload the previously saved file configuration.
- iv. To restore the configuration, click on **Restore** button.



- v. The restoration process shall begin automatically.

## Appendix C – Wireless Bridge Operation Guidelines

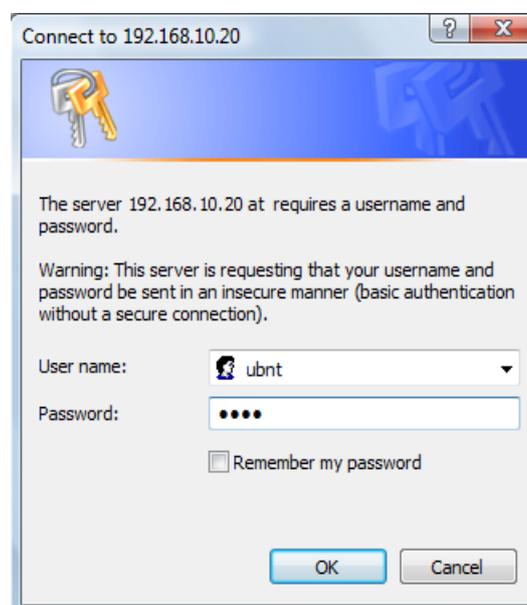
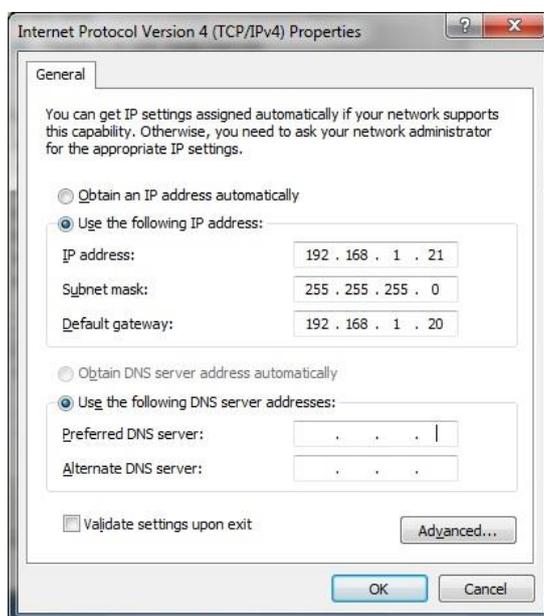
This section describes on Wireless Bridge Operation Guidelines.

Scope of this section covers the following topics:

- Access with Graphical User Interface (GUI)
- Access Point monitoring
- Backup and restore Access Point configuration
- Access Point logs

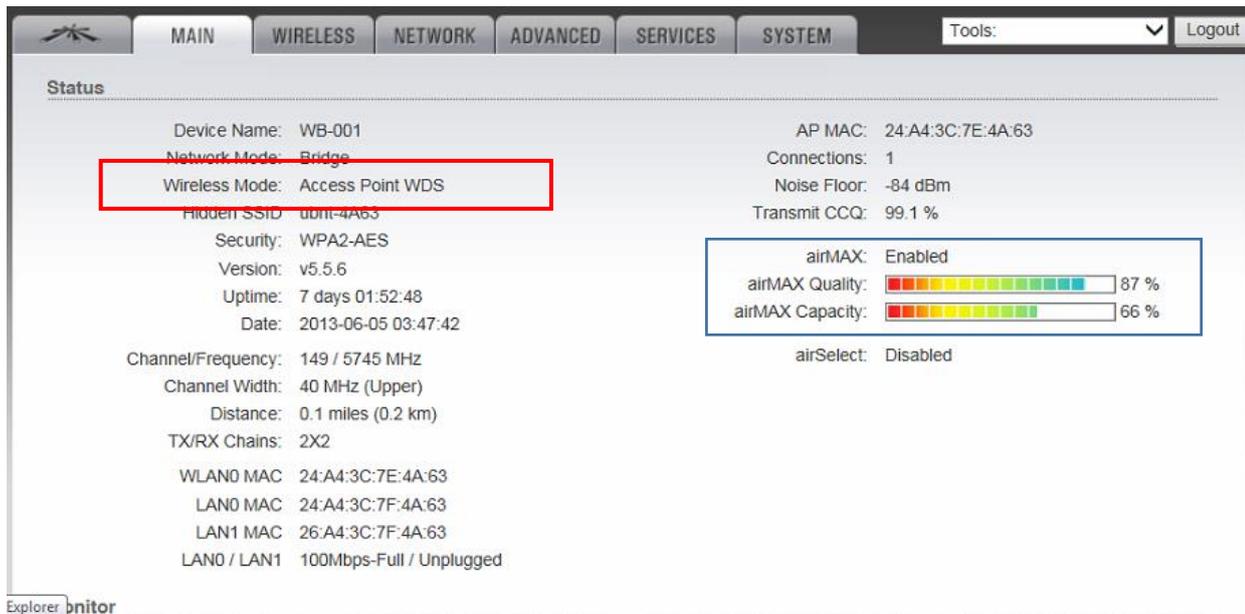
### 1 Access with Graphical User Interface

STEP	DESCRIPTION
1	In your computer, open Control Panel > Network Connections > Local Area Connection.
2	In Local Area Connection Status > General, click <b>Properties</b> .
3	In Local Area Connection Properties > General, select <b>Internet Protocol (TCP/IP)</b> and click <b>Properties</b> .
4	In Internet Protocol (TCP/IP) Properties > General, select <b>Use the following IP address</b> .
5	Enter your <b>IP address</b> and <b>Subnet Mask</b> . The default IP address of the radio is <b>192.168.1.21</b> , which cannot be used here. <b>So type IP address 192.168.1.21 and gateway 192.168.1.20</b>
6	Click <b>OK</b> and <b>Close</b>
7	Open your browser (e.g. Internet Explorer, Firefox, Opera, etc.) and type in address bar: <b>http://192.168.1.20</b> (The default address of the device) then press the Enter key.  Default Username : Password :



## 2 View Wireless Bridge status

- i. On the **Access Point WDS** main page, observe the airMAX Quality to check the effectiveness of wireless bridge connection. The percentage of airMAX Quality must be more than 80%.

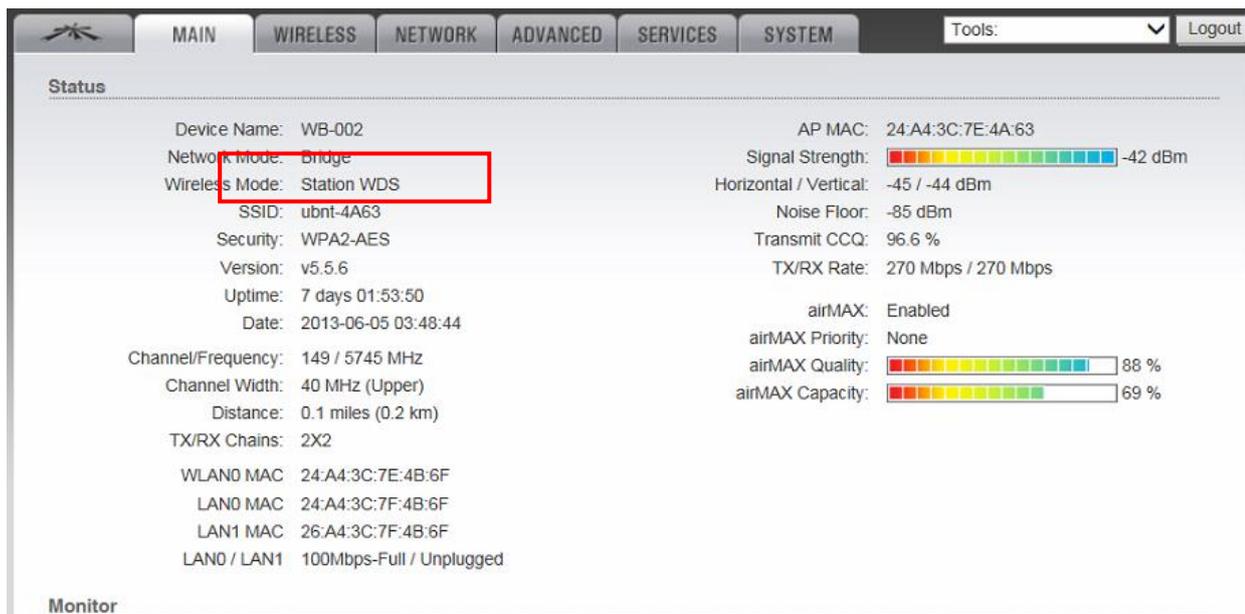


The screenshot shows the main page of a Ubiquiti Nano Station M5. The 'Wireless' tab is selected. The 'Wireless Mode' is set to 'Access Point WDS', which is highlighted with a red box. The 'airMAX Quality' is 87% and 'airMAX Capacity' is 66%, both shown with color-coded progress bars. Other details include Device Name: WB-001, AP MAC: 24:A4:3C:7E:4A:63, and various network parameters.

Device Name:	WB-001	AP MAC:	24:A4:3C:7E:4A:63
Network Mode:	Bridge	Connections:	1
Wireless Mode:	Access Point WDS	Noise Floor:	-84 dBm
Hidden SSID:	ubnt-4A63	Transmit CCQ:	99.1 %
Security:	WPA2-AES	airMAX:	Enabled
Version:	v5.5.6	airMAX Quality:	87 %
Uptime:	7 days 01:52:48	airMAX Capacity:	66 %
Date:	2013-06-05 03:47:42	airSelect:	Disabled
Channel/Frequency:	149 / 5745 MHz		
Channel Width:	40 MHz (Upper)		
Distance:	0.1 miles (0.2 km)		
TX/RX Chains:	2X2		
WLAN0 MAC:	24:A4:3C:7E:4A:63		
LAN0 MAC:	24:A4:3C:7F:4A:63		
LAN1 MAC:	26:A4:3C:7F:4A:63		
LAN0 / LAN1:	100Mbps-Full / Unplugged		

Ubiquiti Nano Station M5 main page

- ii. On the **Station WDS** main page, observe the airMAX Quality to check the effectiveness of wireless bridge connection. The percentage of airMAX Quality must be more than 80%.



The screenshot shows the main page of a Ubiquiti Nano Station M5. The 'Wireless' tab is selected. The 'Wireless Mode' is set to 'Station WDS', which is highlighted with a red box. The 'airMAX Quality' is 88% and 'airMAX Capacity' is 69%, both shown with color-coded progress bars. Other details include Device Name: WB-002, AP MAC: 24:A4:3C:7E:4A:63, and various network parameters.

Device Name:	WB-002	AP MAC:	24:A4:3C:7E:4A:63
Network Mode:	Bridge	Signal Strength:	-42 dBm
Wireless Mode:	Station WDS	Horizontal / Vertical:	-45 / -44 dBm
SSID:	ubnt-4A63	Noise Floor:	-85 dBm
Security:	WPA2-AES	Transmit CCQ:	96.6 %
Version:	v5.5.6	TX/RX Rate:	270 Mbps / 270 Mbps
Uptime:	7 days 01:53:50	airMAX:	Enabled
Date:	2013-06-05 03:48:44	airMAX Priority:	None
Channel/Frequency:	149 / 5745 MHz	airMAX Quality:	88 %
Channel Width:	40 MHz (Upper)	airMAX Capacity:	69 %
Distance:	0.1 miles (0.2 km)		
TX/RX Chains:	2X2		
WLAN0 MAC:	24:A4:3C:7E:4B:6F		
LAN0 MAC:	24:A4:3C:7F:4B:6F		
LAN1 MAC:	26:A4:3C:7F:4B:6F		
LAN0 / LAN1:	100Mbps-Full / Unplugged		

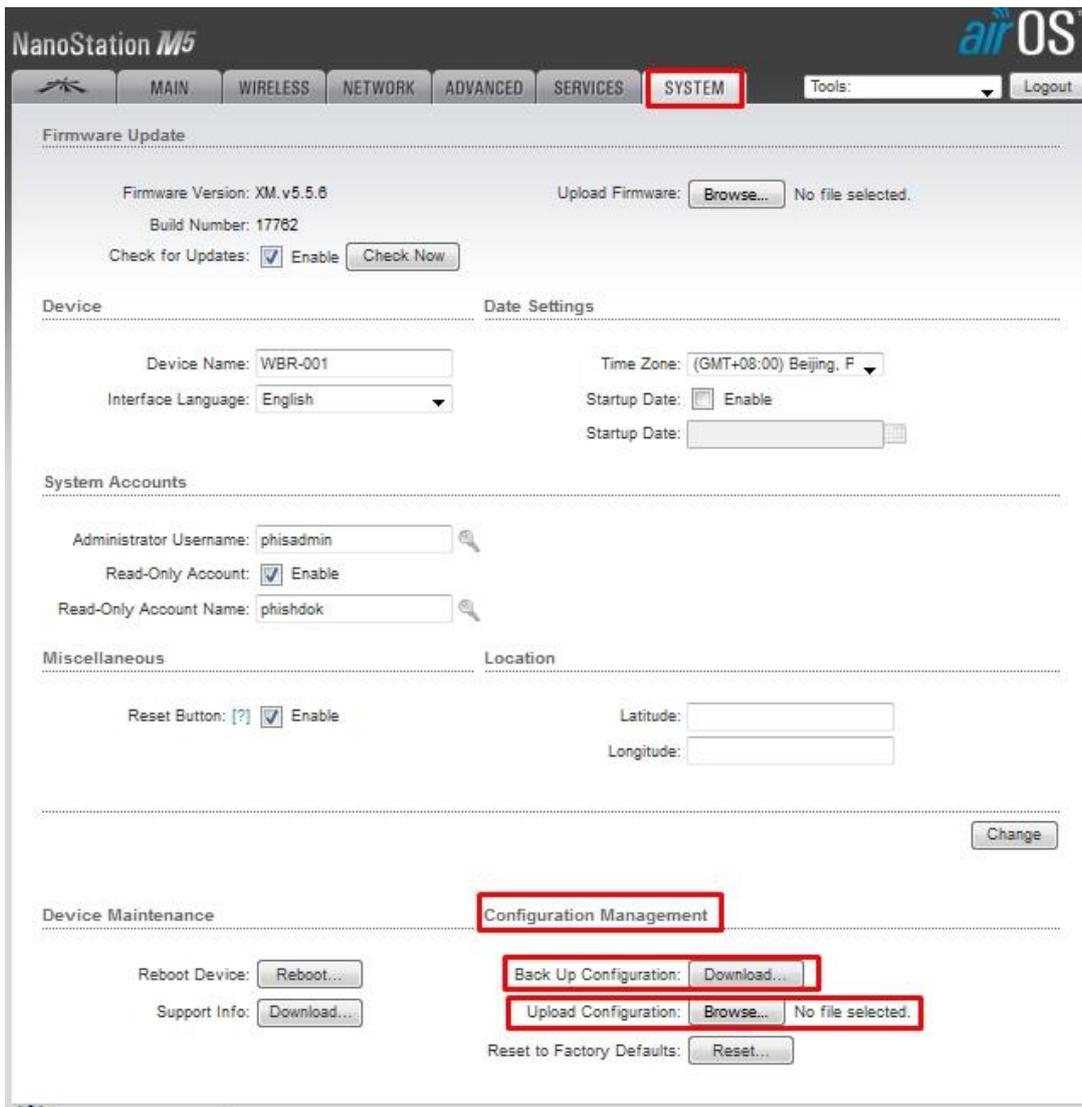
Ubiquiti Nano Station M5 main page

### 3 Backup Bridge Configuration File (GUI)

- i. From Desktop, open browser and type access point IP address
- ii. Key in the management username and password
- iii. From the main page, go to **System** >> Configuration Management
- iv. Click Download

### 4 Restore Bridge Configuration File (GUI)

- i. From Desktop, open browser and type access point IP address
- ii. Key in the management username and password
- iii. From the main page, go to **System** >> Configuration Management
- iv. Click Browse, select the backup configuration file



The screenshot displays the NanoStation M5 web interface. The top navigation bar includes tabs for MAIN, WIRELESS, NETWORK, ADVANCED, SERVICES, and SYSTEM (highlighted with a red box). Below the navigation bar, the 'Firmware Update' section shows the current firmware version (XM.v5.5.6) and build number (17782). The 'Device' section includes fields for Device Name (WBR-001), Interface Language (English), and Time Zone ((GMT+08:00) Beijing, F). The 'System Accounts' section shows the Administrator Username (phisadmin) and Read-Only Account Name (phishdok). The 'Miscellaneous' section includes a Reset Button (Enable) and Latitude/Longitude fields. The 'Device Maintenance' section at the bottom contains buttons for Reboot Device, Support Info, Back Up Configuration (Download...), Upload Configuration (Browse...), and Reset to Factory Defaults (Reset...). The 'Configuration Management' section is highlighted with a red box, and the 'Back Up Configuration: Download...' button is also highlighted with a red box.