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

Training Manual
Facilty
Network Module

Version	**: 1.4**
Document ID	**: H_T.MANUAL_Network_Facility**

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

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

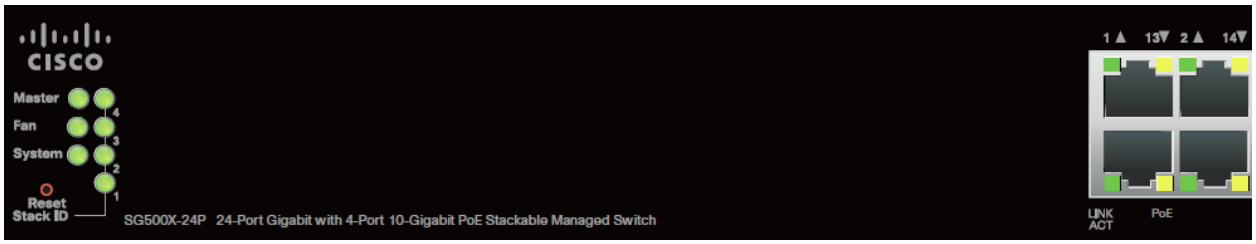
2.1 Overview of Cisco SG300-28 & SG500-28

Specification		
 SG500-28		 SG300-28
Basic Layer 3	**Switch Layer**	Basic Layer 3
Manage	**Switch Type**	Manage
192.168.1.254/24	**Default IP Address**	192.168.1.254/24
Yes	**Web-based management**	Yes
10/100/1000Base-T	**Network Technology**	10/100/1000Base-T
24	**Number of Ethernet Port**	26
2 Combo port + 2 SFP	**Number of SFP Port**	2 Gigabit Ethernet Combo
Yes	**Stack Port**	No
Supported Gigabit Ethernet SX Mini –GBIC SFP Transceiver	**SFP Module**	Gigabit Ethernet SX Mini –GBIC SFP Transceiver

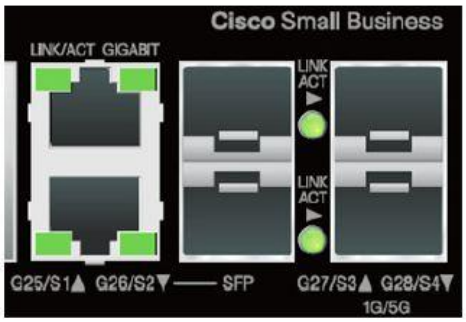
2.2 Features of the Cisco SG500-28 & SG300-28

2.2.1 Cisco SG500-28 front view

The following image illustrate the right side of switch.

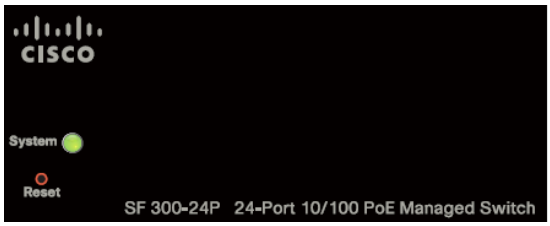


The following image illustrate the left side of switch.

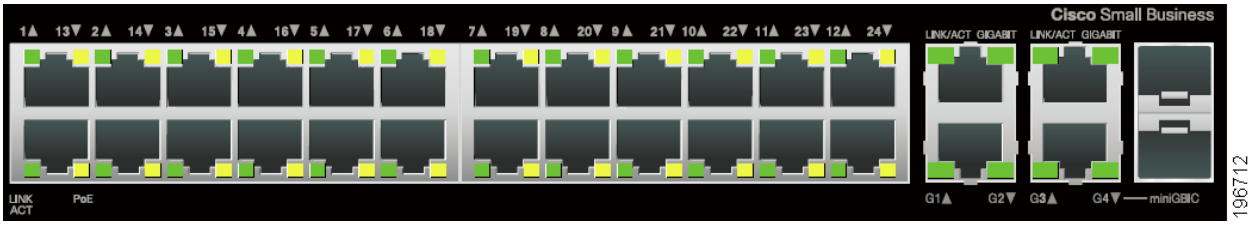


2.2.2 Cisco SG300-28 front view

The following image illustration shows the right side of switch.

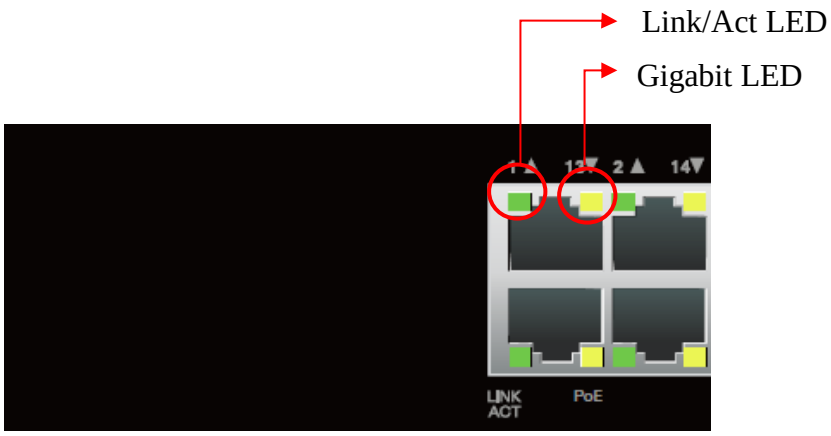


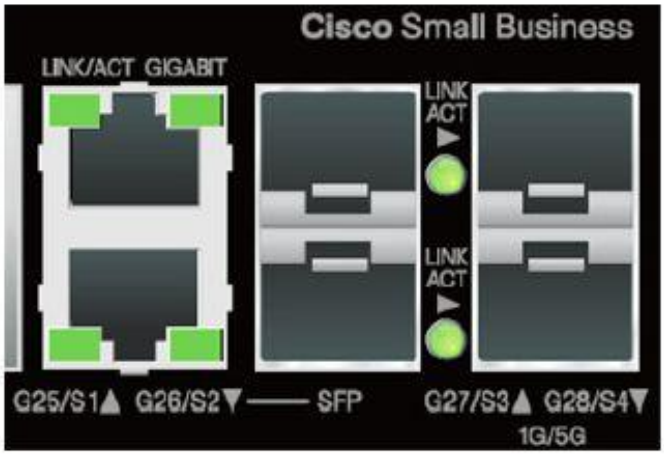
The following image illustrate the left front panel port.



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

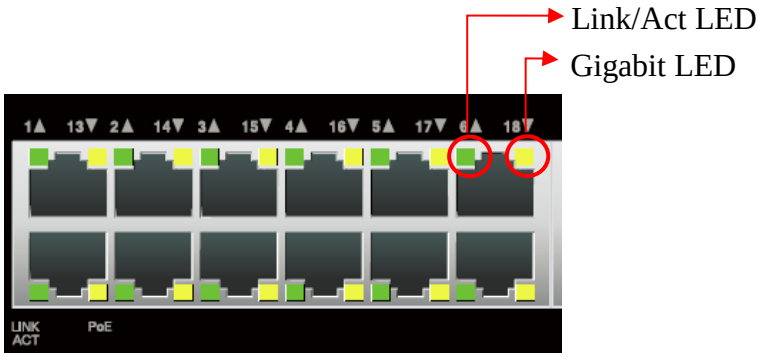
2.3.1 Cisco SG500-28 Key & LED status

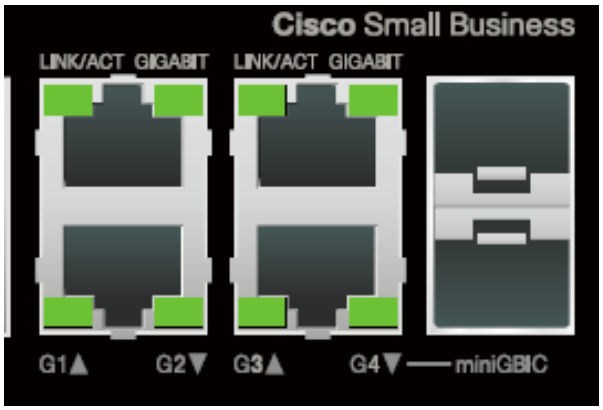




Part	LED Status	Meaning
Master LED	Green (Lights steady)	Switch is a stack master
Fan LED	Green (Lights steady)	Cooling fan is operational
	Green (Blinks)	Fan in failure
System LED	Green (Lights steady)	Switch is powered on
	LED flashes	Booting, performing self-tests, or acquiring an IP address
	LED 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-DNIXXXXXXXXX
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-DNIXXXXXXXXX
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-DNIXXXXXXXXX
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-DNIXXXXXXXXX
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

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	**No action necessary.** to use
	LED Off	- Stacking not using - Not Function	• **If the stacking function not use, No action necessary to use** • Try to check Cable or Switch that been configured as slave.
Fan LED	Green (Lights steady)	N/A	**No action necessary.** 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	**No action necessary.** to use
	LED flashes	N/A	**No action necessary.** 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	**No action necessary.** to use
	LED off	- Not Using - Link Down / Switch Down	• **If it is "Not Using", no action should be taken.** • **Try to check connected Cable**
Link/Act LED	Green (Lights steady)	N/A	**No action necessary.** to use
	Green (Flashes)	N/A	**No action necessary.** to use
	LED off	- Not Using - Link Down / Switch Down	• **If not using, No action necessary to use** • Try to check Cable or Switch that connected into that port.
Gigabit LED	Green (Lights steady)	N/A	**No action necessary.** to use
	LED Off	- Not Using - Connection Down	• **If not using, No action necessary to use** • Try to check Cable or Switch that connected into that port.
SFP LED (**SG500-28 Only**)	Green (Lights steady)	N/A	**No action necessary.** to use
	Green (Flashes)	N/A	**No action necessary.** to use
	LED Off	- Not Using - Connection Down	• **If not using, No action necessary to use** • Try to check Cable or Switch that connected into that port.
MiniGBIC (**SG300-28 Only**)	Green (Lights steady)	N/A	**No action necessary.** to use
	Green (Flashes)	N/A	**No action necessary.** to use

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

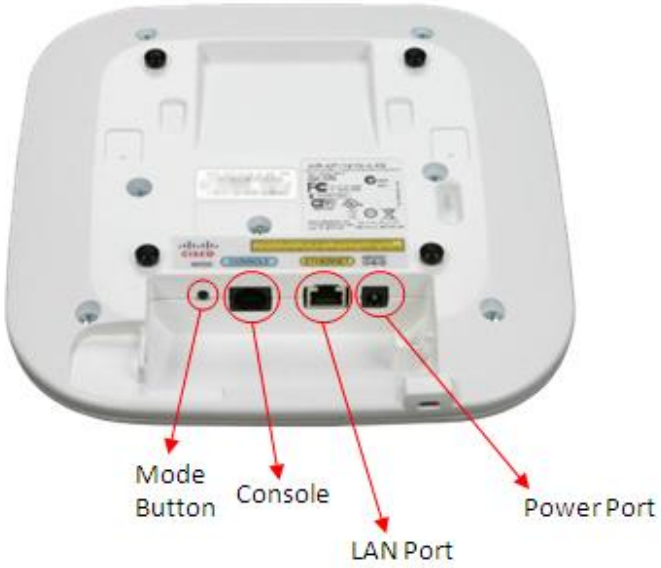
3.1 Overview of Cisco Aironet 1141 & Cisco Aironet 1602i

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

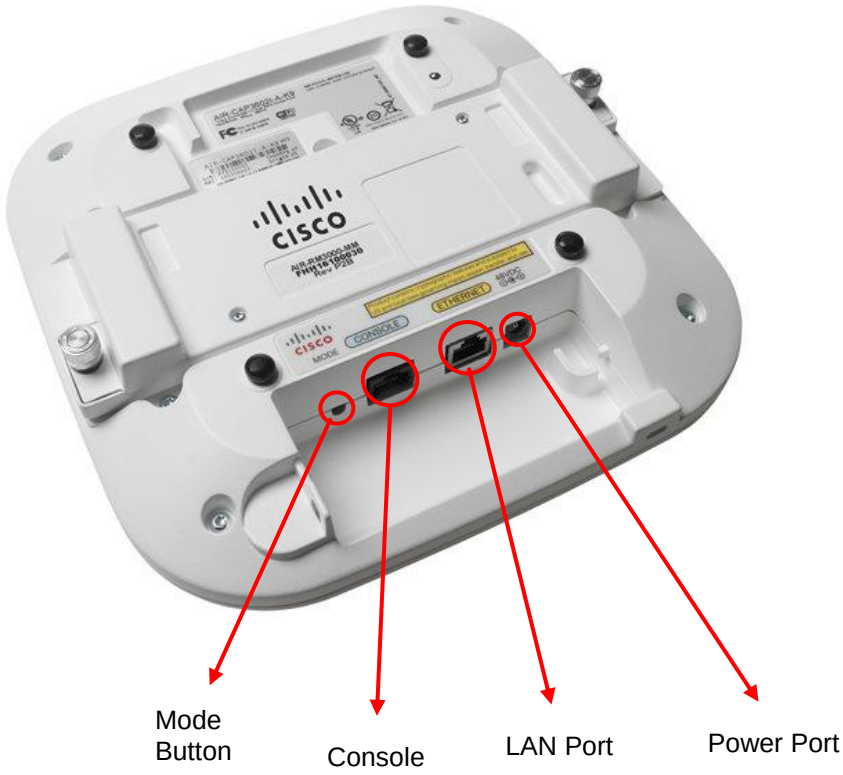
3.2.1 Cisco Aironet 1141 Front View

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

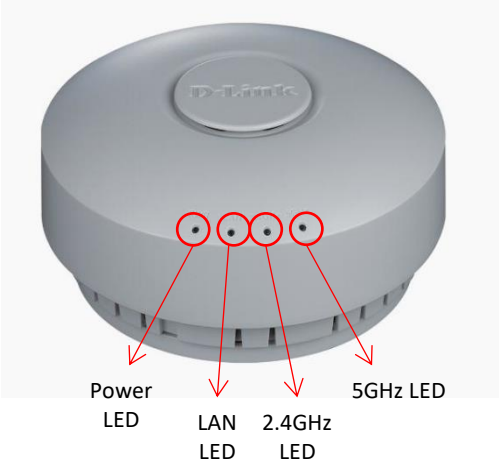
Message type	Status LED	Message Meaning
Boot Loader Status Sequence	Blinking green	• DRAM memory test in progress • DRAM memory test OK • Board initialization in progress • Initialization FLASH file system • Flash memory OK test • initialization Ethernet • Ethernet OK • Starting Cisco IOS • Initialization Successful
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	• Environment variable failure • BAD MAC address • Ethernet failure during image recovery • Boot environment failure • No Cisco image file • Boot failure
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

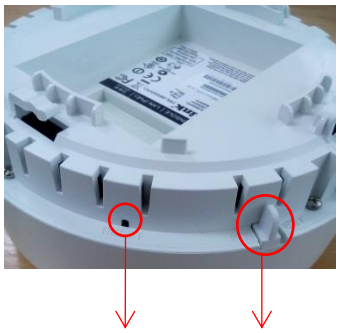
Category	Specification
Wi-Fi Interface	802.11a/b/g/n 2.4/5.0 GHz
LAN Interface	10/100/1000 Gigabit Ethernet
Console	RJ-45
Antenna	2x2 MIMO embedded antenna with 4 external antenna connectors
Power Method	IEEE 802.3af Power Over Ethernet or external power adapter
Wireless Frequency	802.11n: 2.4 to 2.497 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

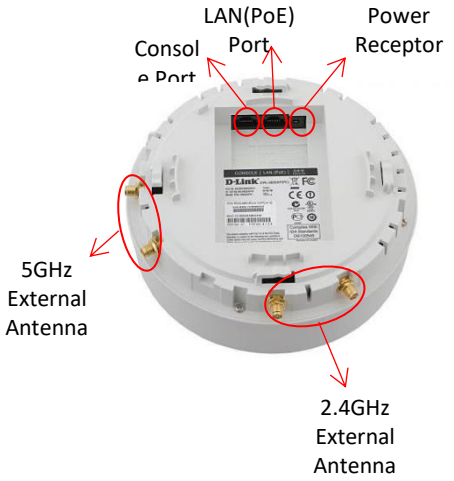
3.5.1 Dlink DWL-6600APA1 Front View



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

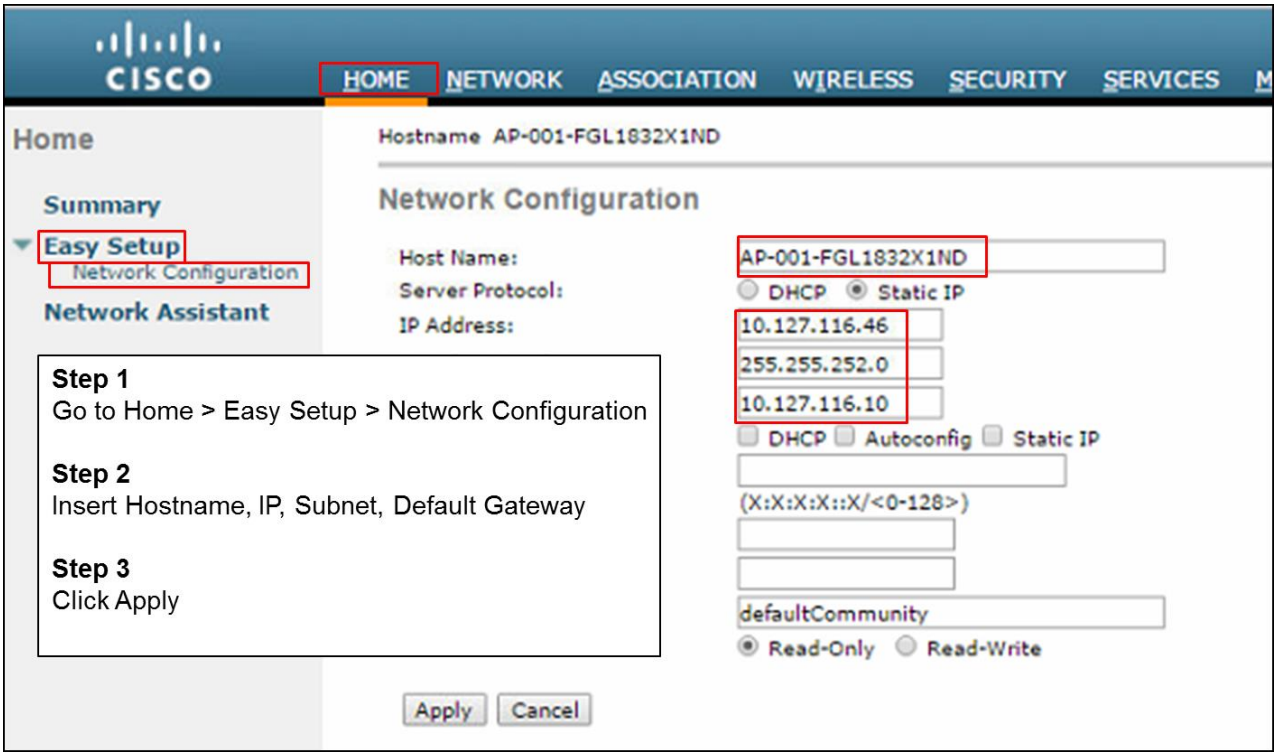
3.7 Network Equipment Configuration

3.7.1 Cisco Aironet 1141 & Cisco Aironet 1602i

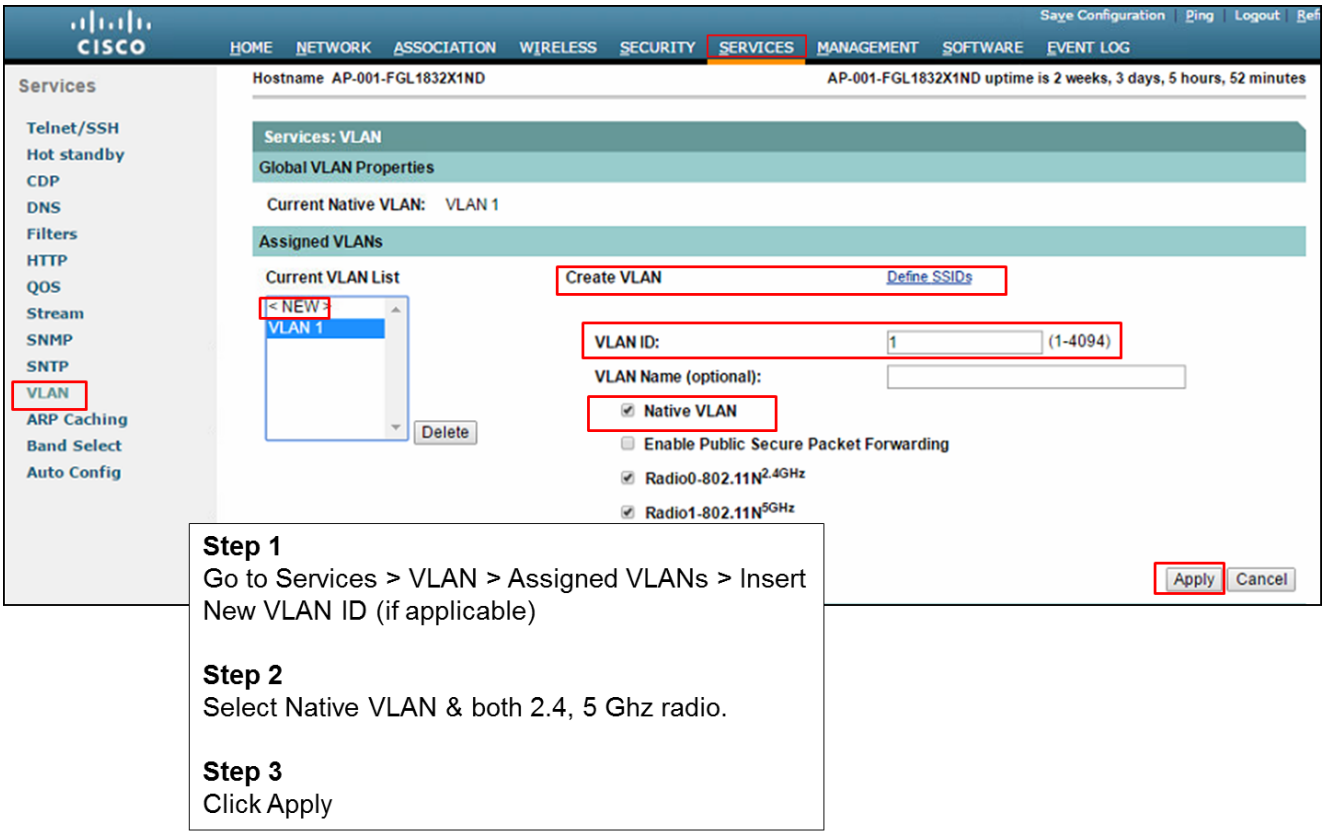
The following table show summary of Cisco AP configuration

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

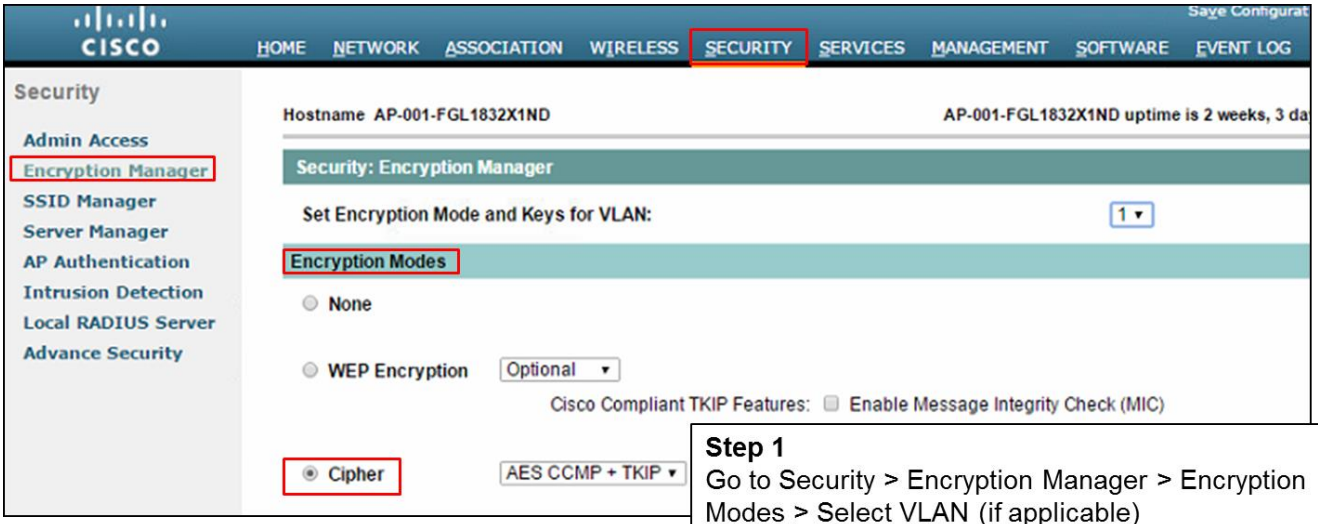
Part 1: Configure IP, Subnet, Gateway & Hostname



Part 2: Configure VLAN



Part 3: Configure Encryption Mode

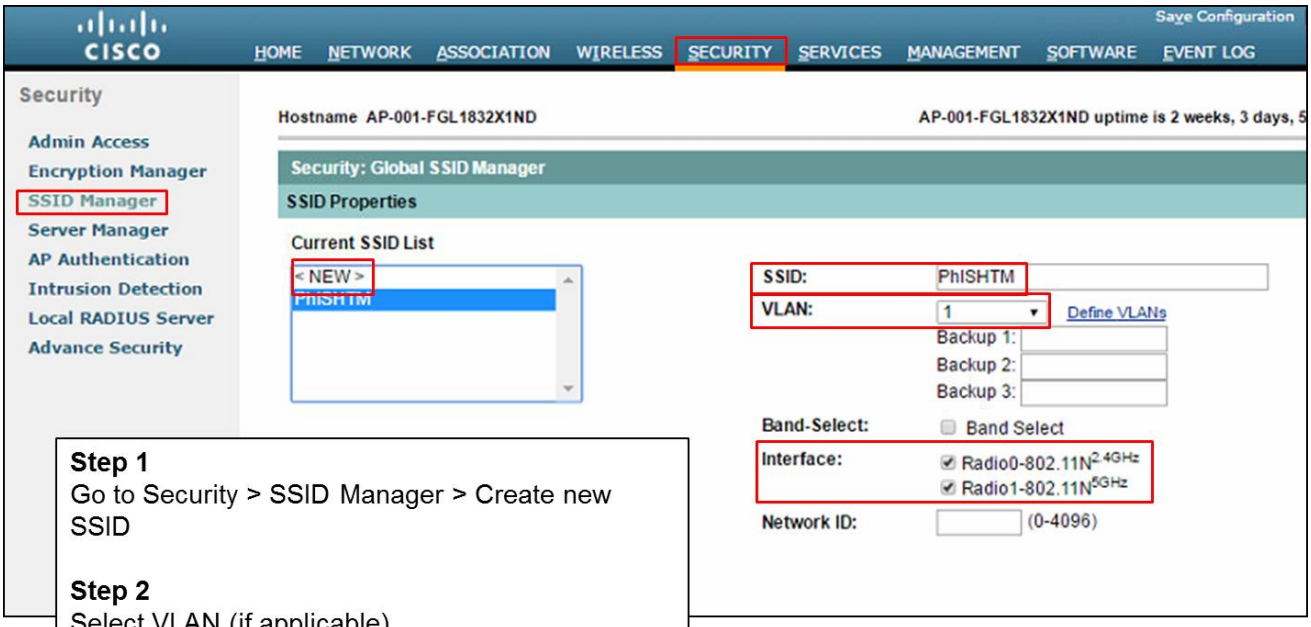


Step 1
Go to Security > Encryption Manager > Encryption Modes > Select VLAN (if applicable)

Step 2
Select Cipher - AES CCMP + TKIP

Step 3
Click Apply

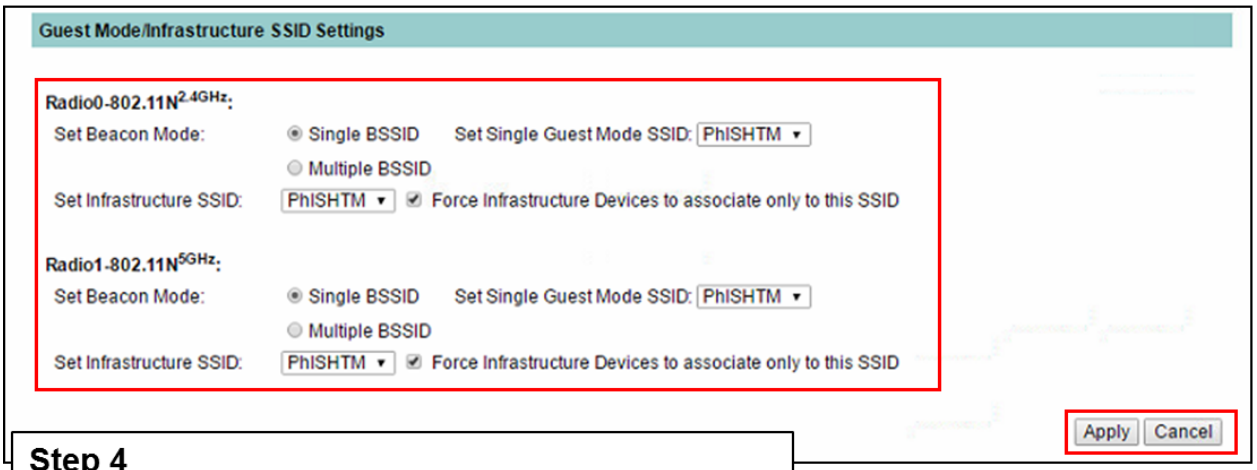
Part 4: Configure SSID



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

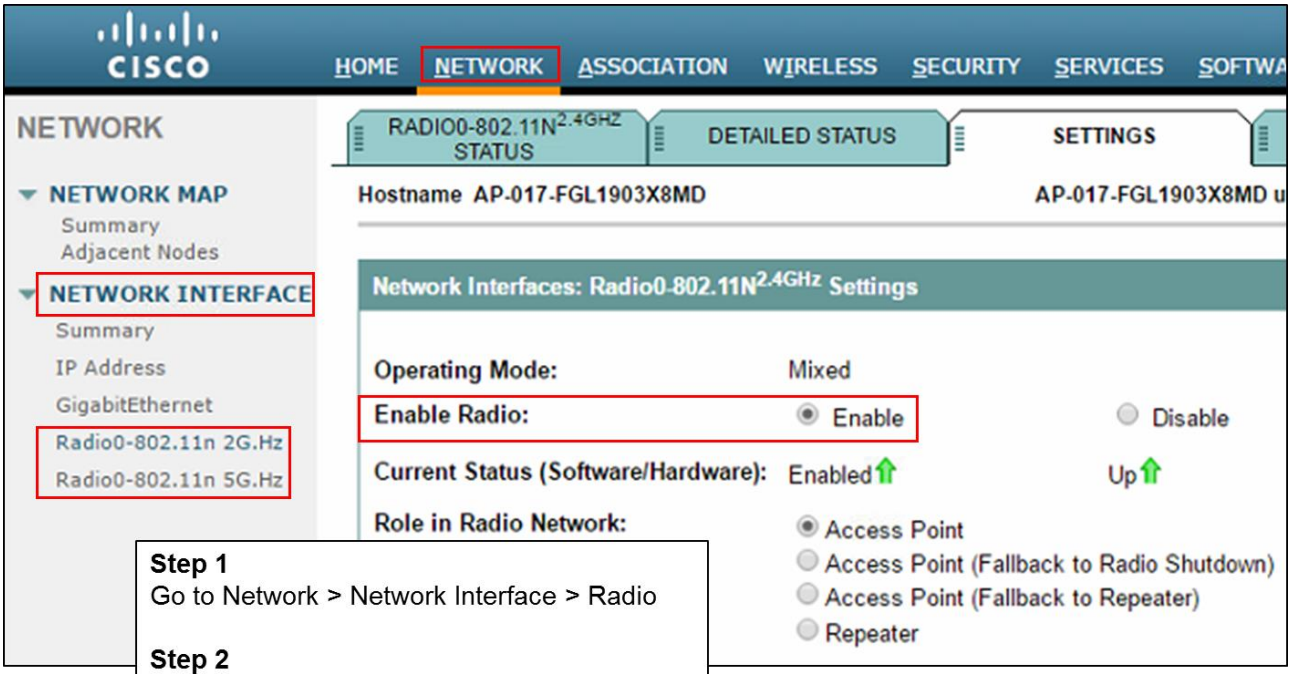


Step 4
Select Key Management - Mandatory, Enable WPA with WPAv2

Step 5
Insert SSID pass key

Step 6
Click Apply

Part 5: Enable radio

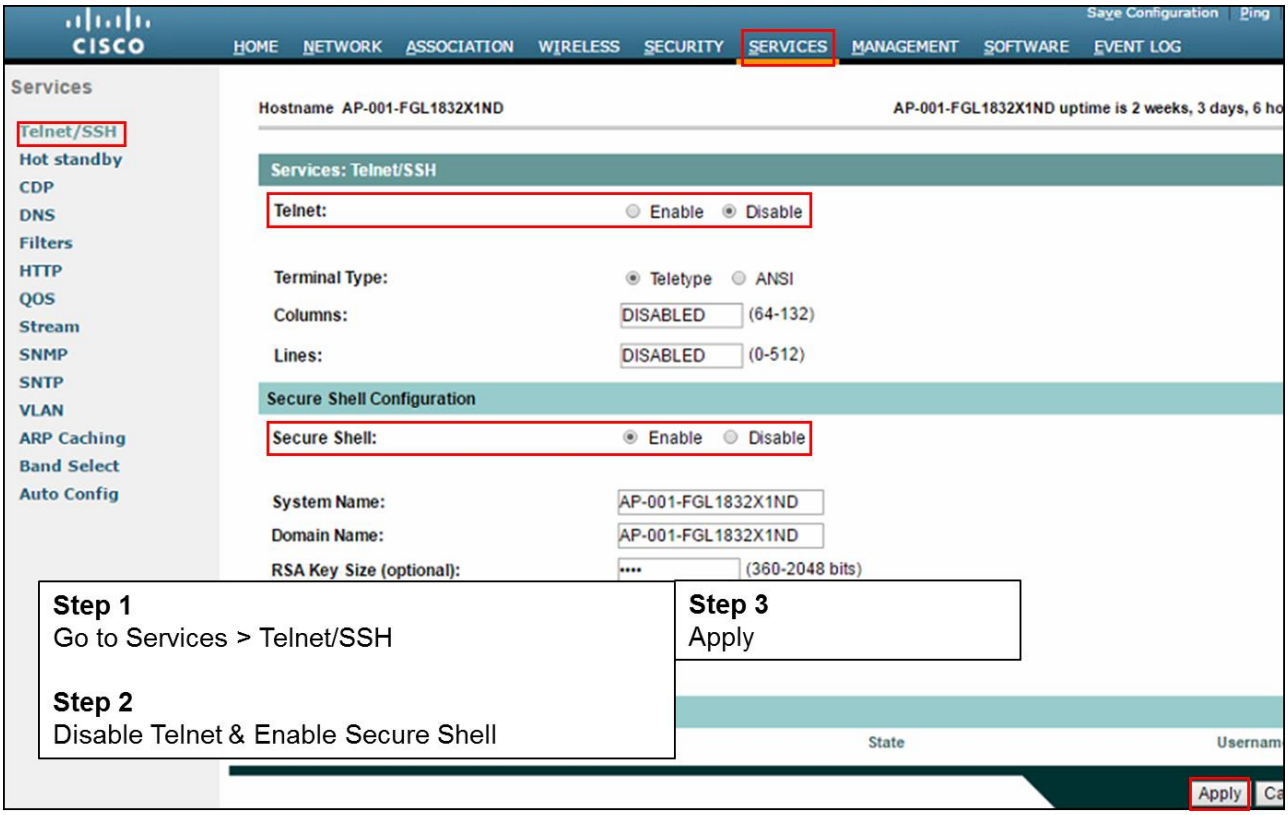


Step 1
Go to Network > Network Interface > Radio

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

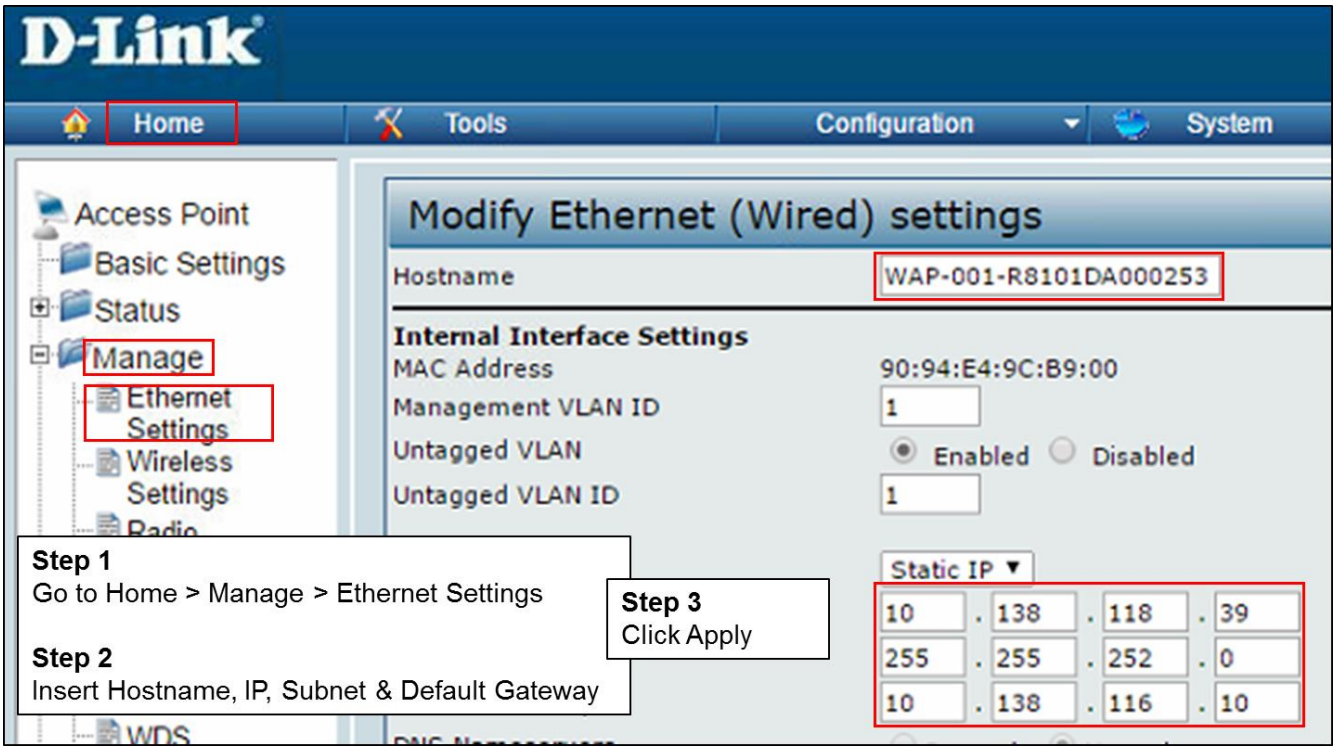
Step 3
Apply

3.7.2 Dlink DWL-6600APA1

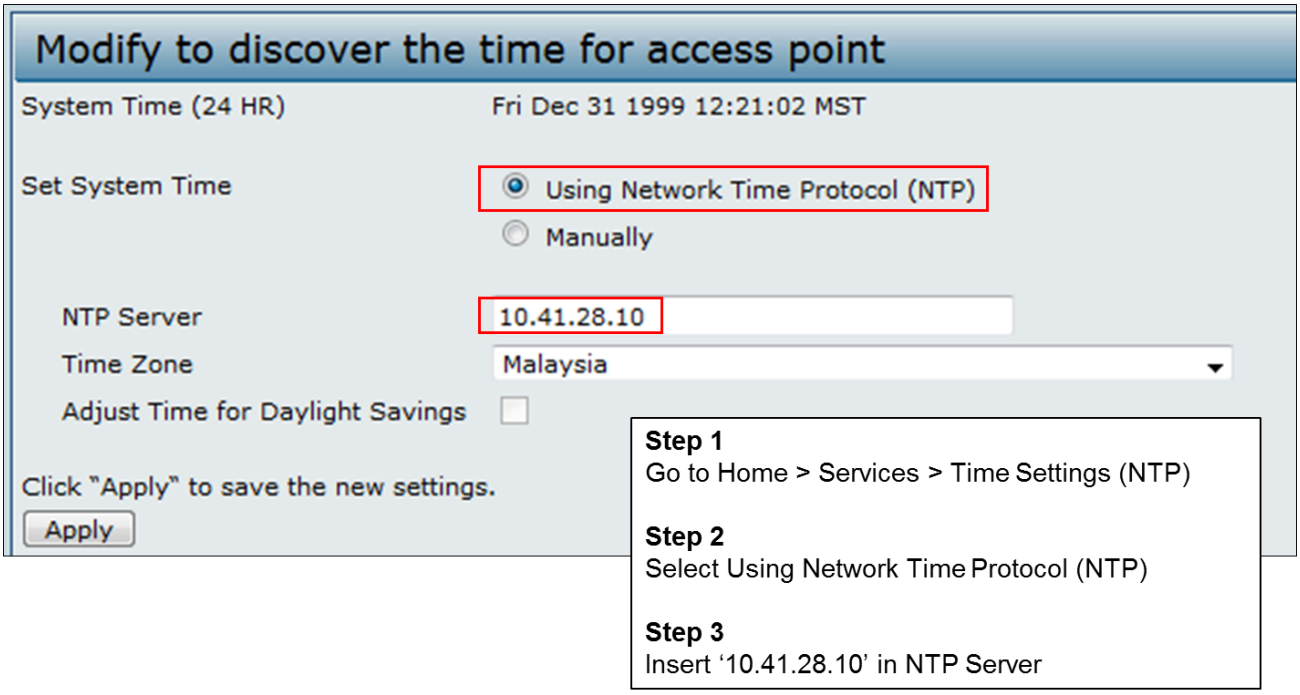
The following table show summary of Dlink AP configuration

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

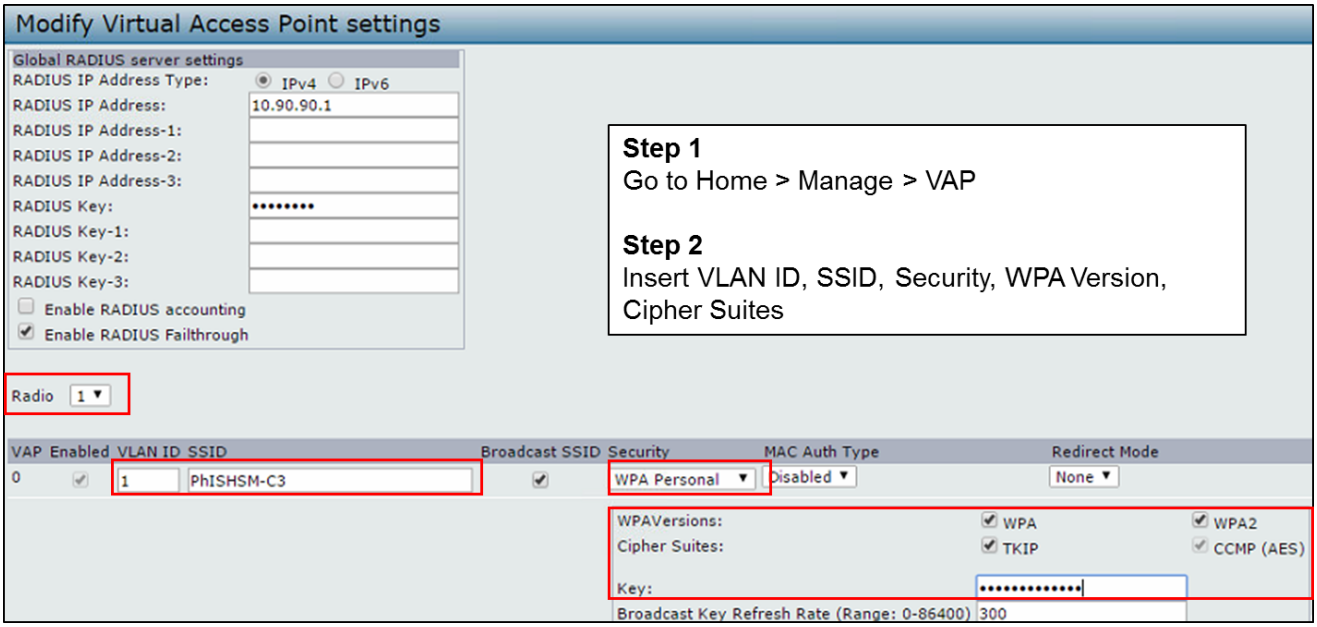
Part 1: Configure IP, Subnet, Gateway & Hostname



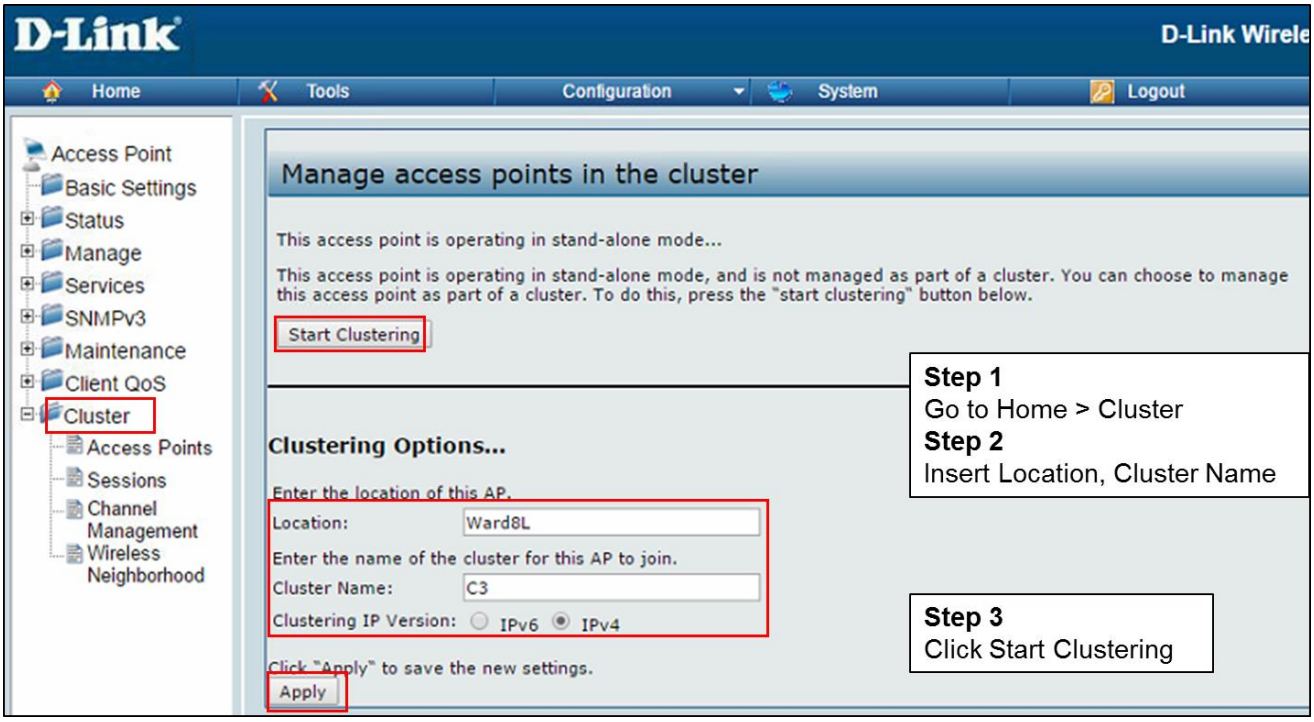
Part 2: Configure NTP

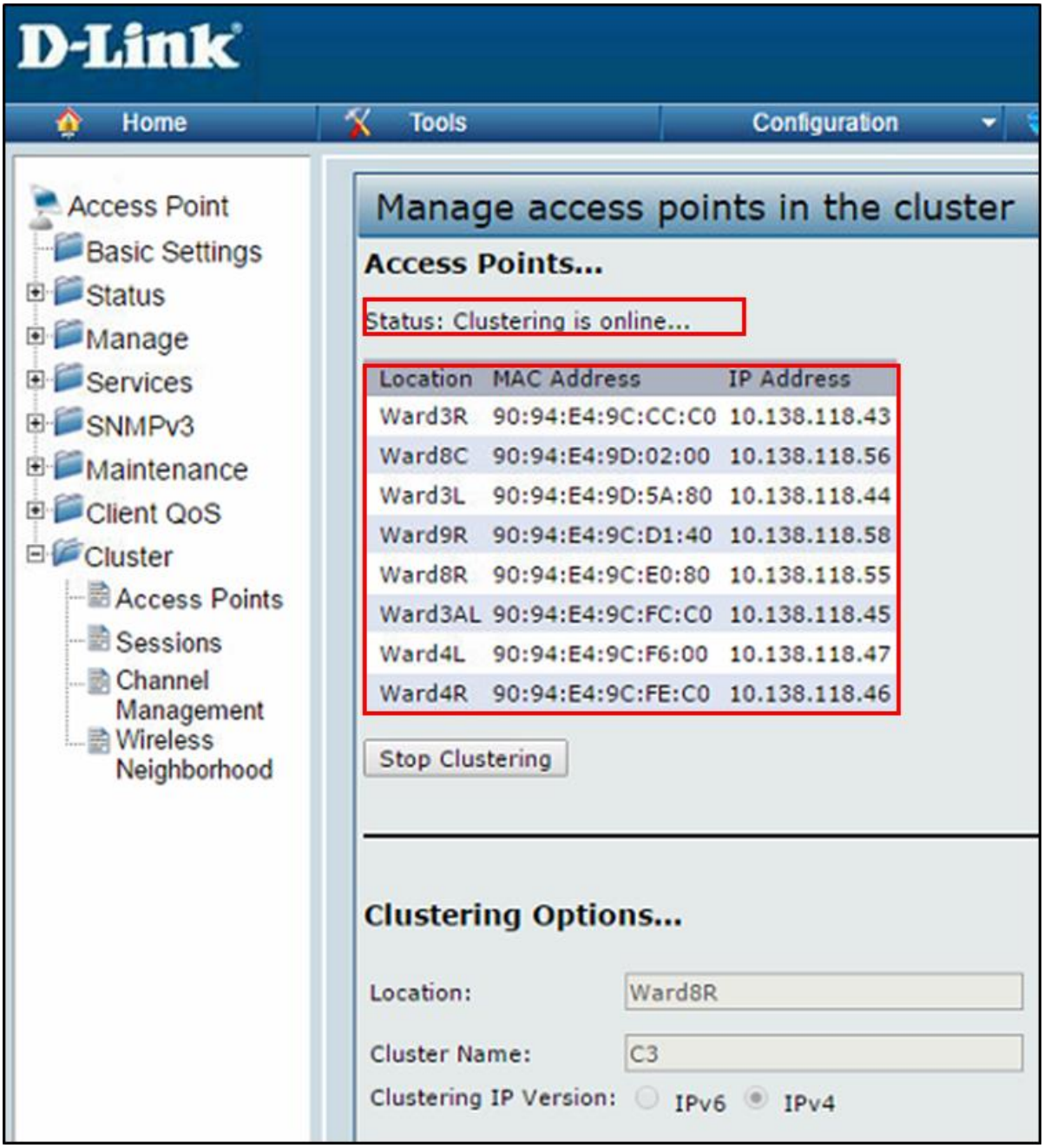


Part 3: Configure VAP (SSID)

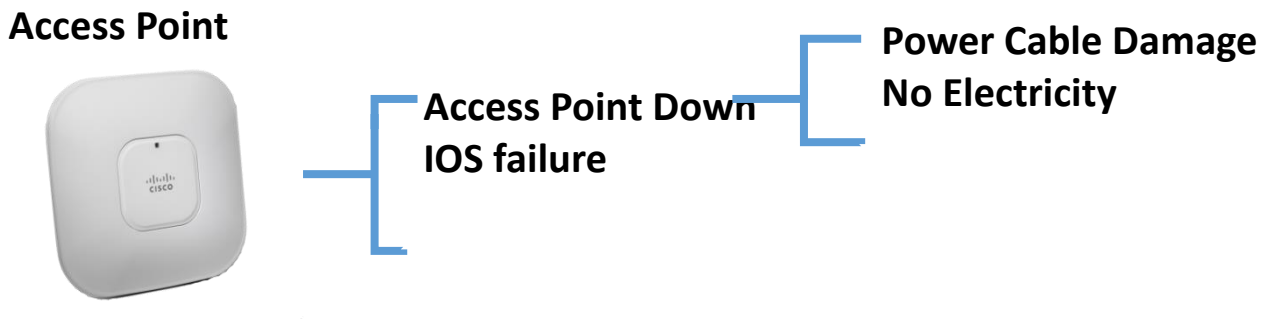


Part 4: Configure Cluster





3.8 Troubleshooting



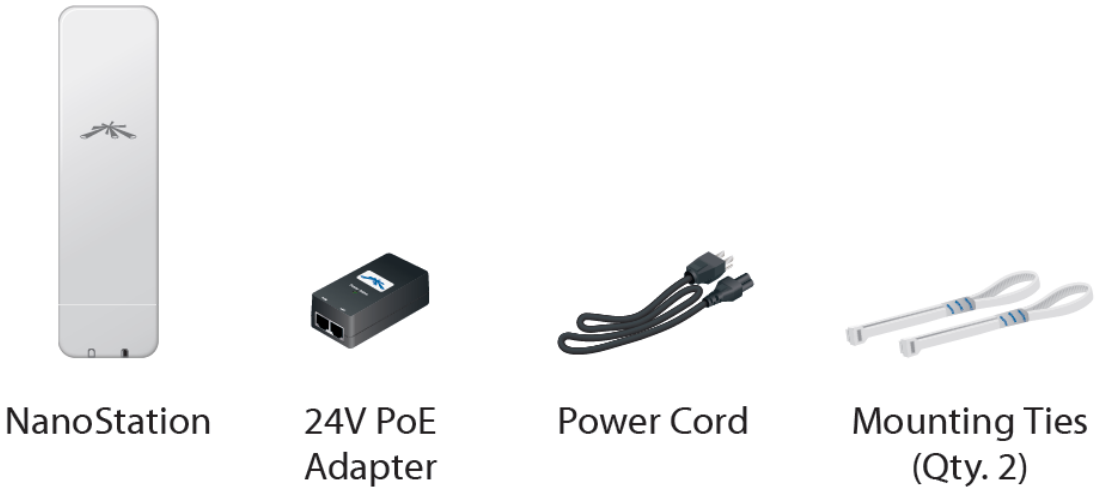
**Reminder
If there is Red color on LED, it means that the Access Point is having problems. The easiest way is to reboot the access point.

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	• Please Enter the correct IP Address (Static IP issue) • Reboot PC or laptop / • Power on AP / check PoE injector (AP not up)
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

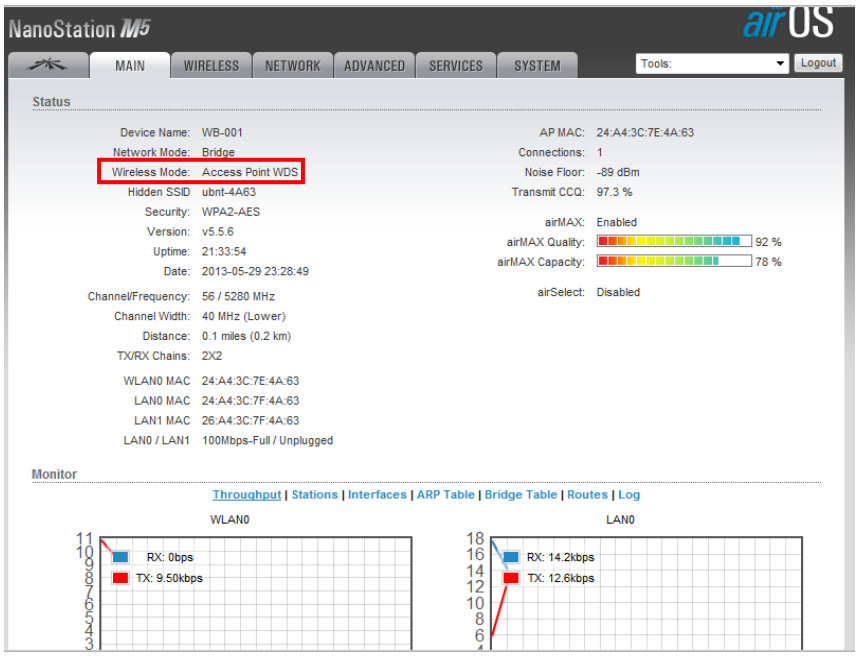


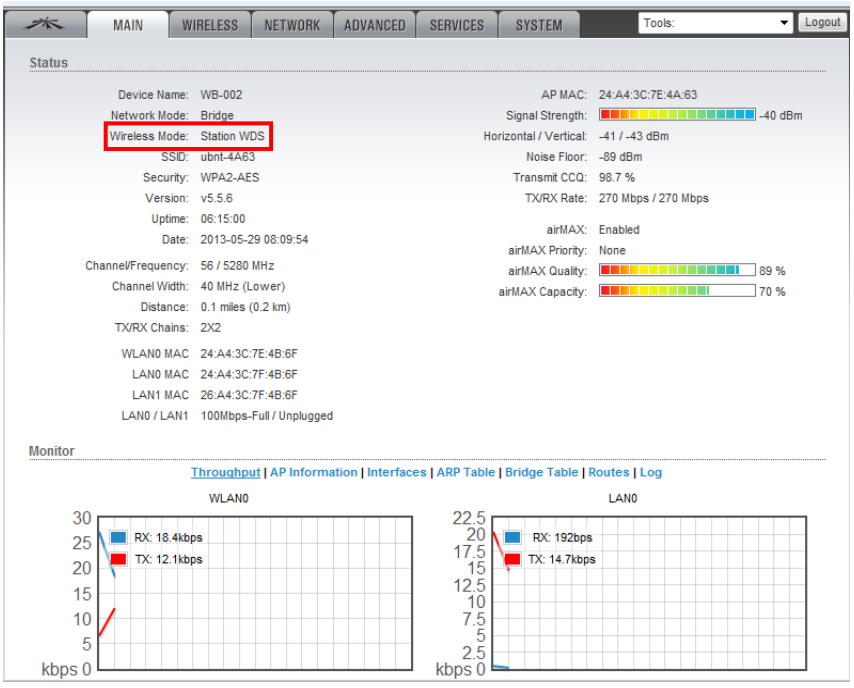
Note: The *Secondary Ethernet Port* is included on NanoStation M5. It is capable of 24V Power over Ethernet (PoE) output, which can provide power to a secondary device. It can be enabled using the airOS Configuration Interface.

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



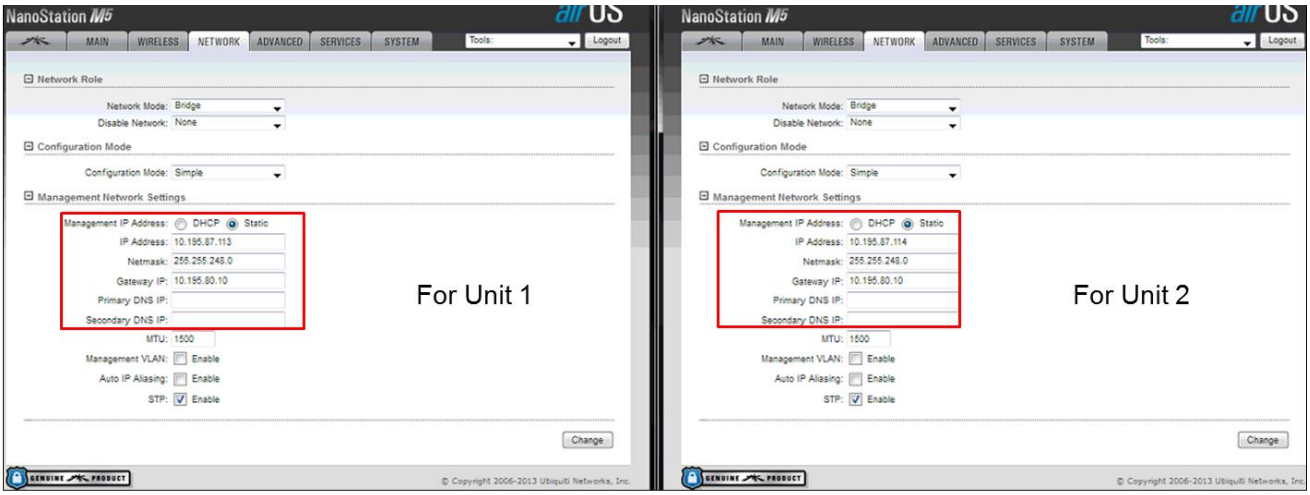


4.4 Network Equipment Configuration

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



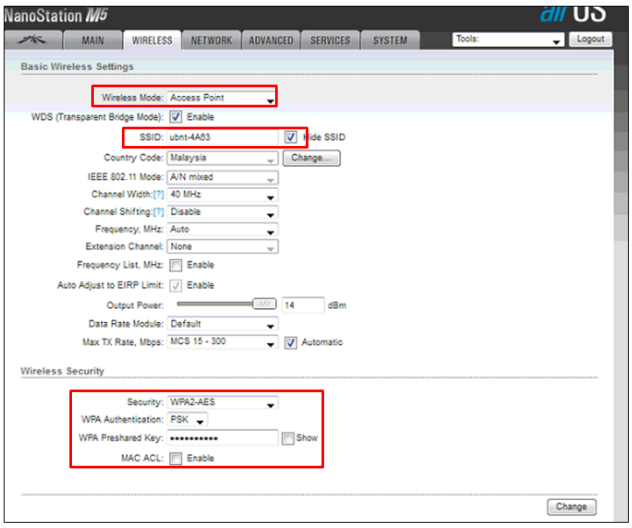
Step 1
Go to Network > Management Network Settings

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

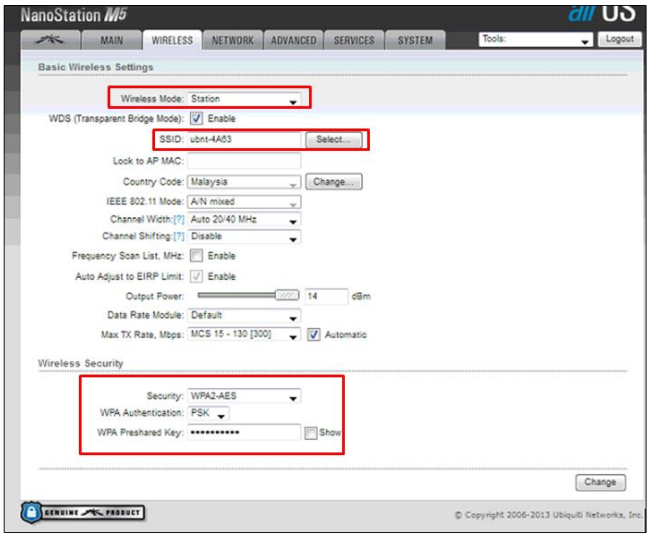
Step 2
Go to Wireless Mode > Select Access Point

Step 3
Go to SSID > Insert SSID.

Step 4
Go to Wireless Security > Security. Select WPA2-AES. Then go to WPA Authentication > 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

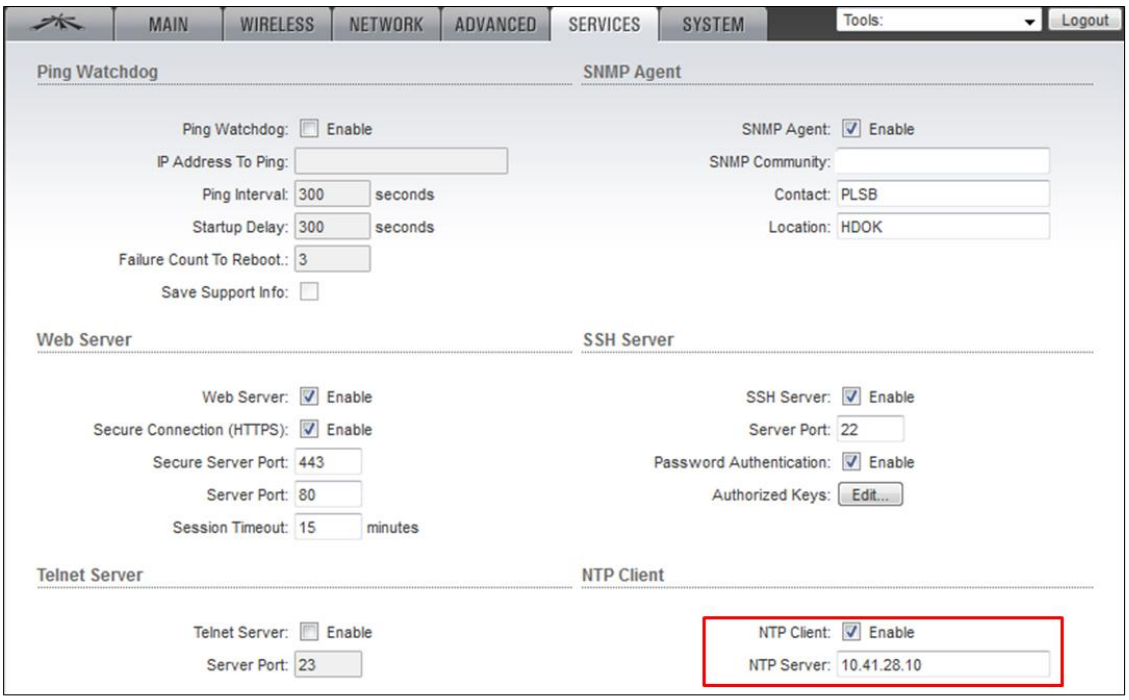
Step 2
Go to Wireless Mode > Select Station

Step 3
Go to SSID > Select SSID configured in Unit 1

Step 4
Go to Wireless Security > Security. Select WPA2-AES. Then go to WPA Authentication > Select PSK. Then go to WPA Preshared Key > Insert password key.

Step 5
Click Change

Part 3: Configure NTP

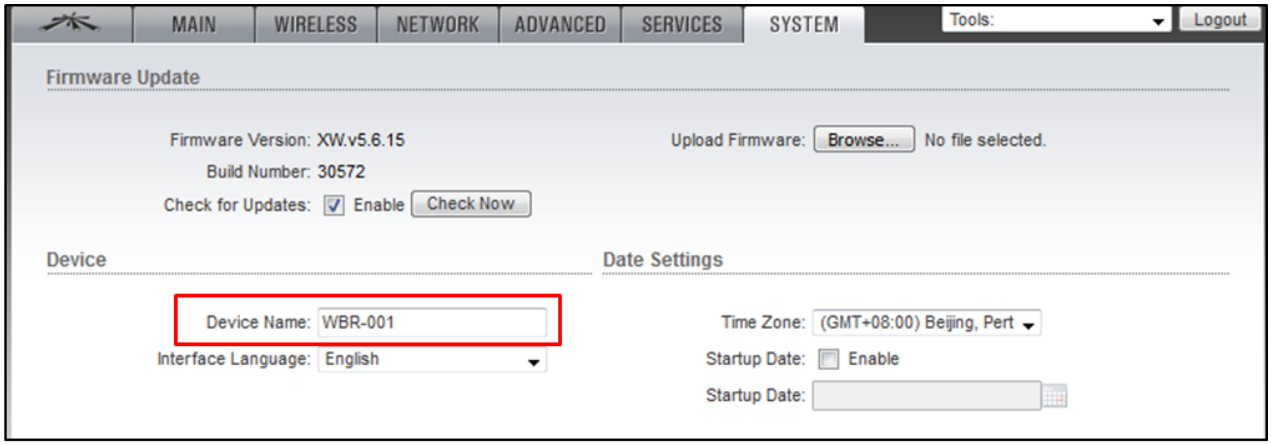


Step 1
Go to Services > NTP Client

Step 2
Click Enable and Insert '10.41.28.10' in NTP Server

Step 3
Click Change

Part 4: Configure Hostname



Step 1
Go to System > Device. Insert Hostname.

Step 2
Click Change

5 Common Issue & Resolution

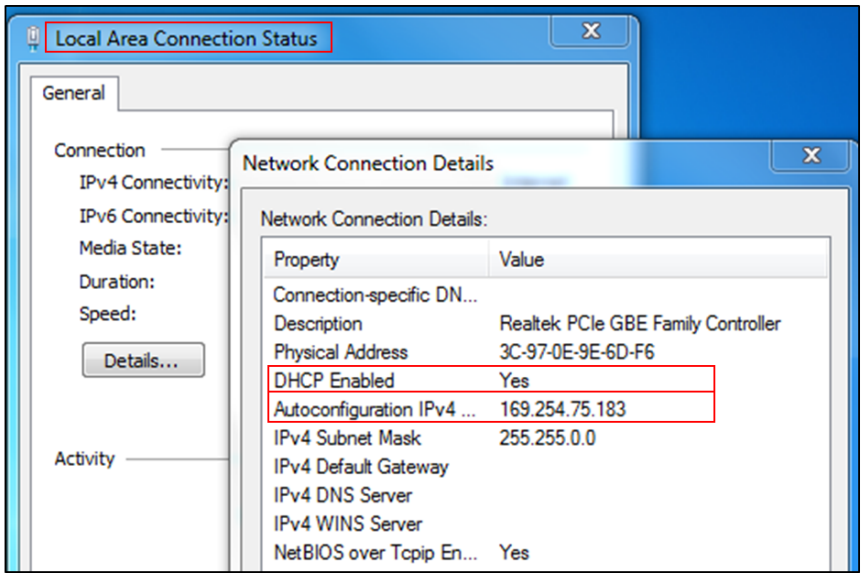
The following table show summary of common issue encountered in PhIS and how to resolve it.

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.

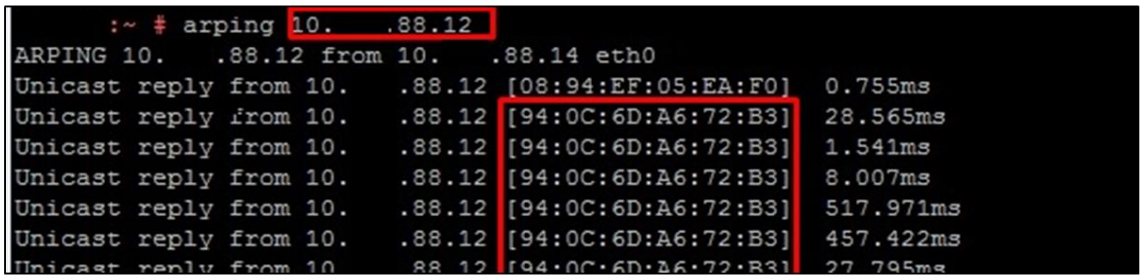
Resolution:
Trace offended port in switch log or check physically cable at switch & disconnect it.

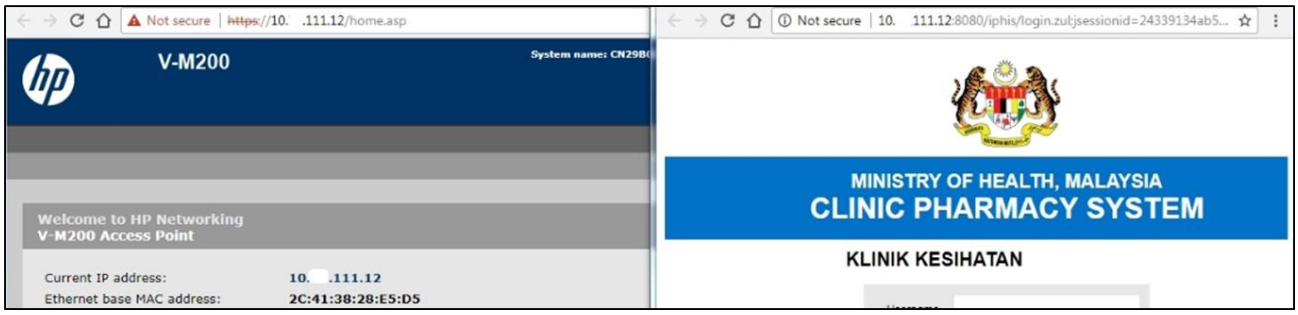
```
C:\PuttyLog\10.195.95.116-20181017-141343.txt (4 hits)
  Line 16: DSW-007-DNI192607SH#sh syste17-Oct-2018 14:10:21 %STP-W-PORTSTATUS: gi26: STP status Blocking
  Line 215: 17-Oct-2018 14:10:21 :%STP-W-PORTSTATUS: gi26: STP status Blocking
  Line 2549: 12-Oct-2018 11:59:19 :%STP-W-PORTSTATUS: gi26: STP status Blocking
  Line 2557: 12-Oct-2018 11:39:03 :%STP-W-PORTSTATUS: 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.

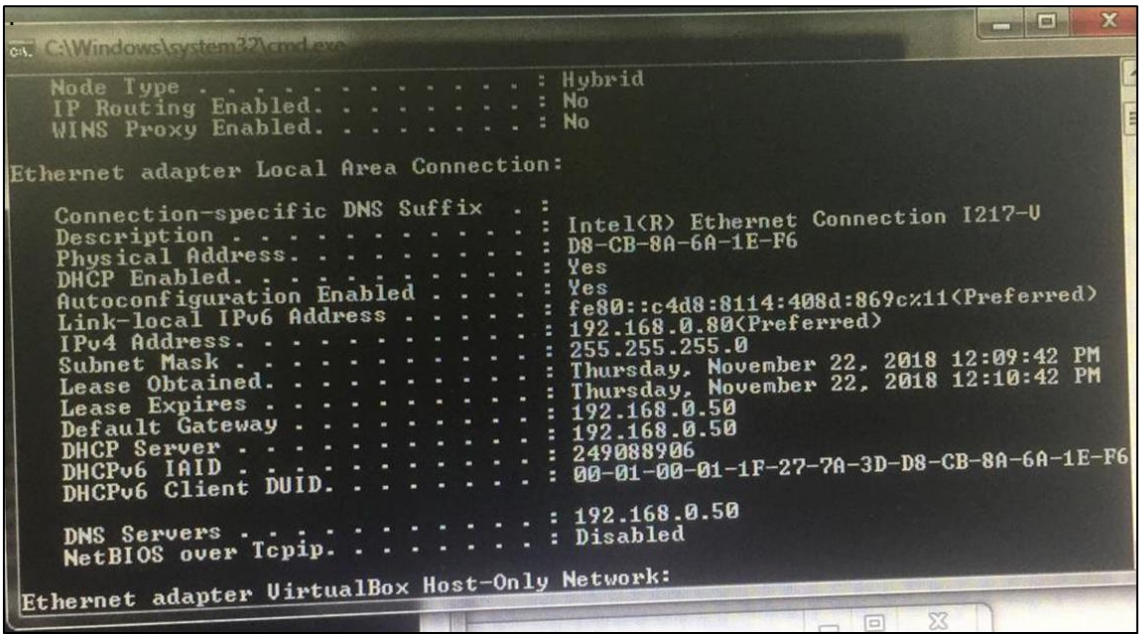




Issue 5: Rogue/Unauthorized DHCP Server

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

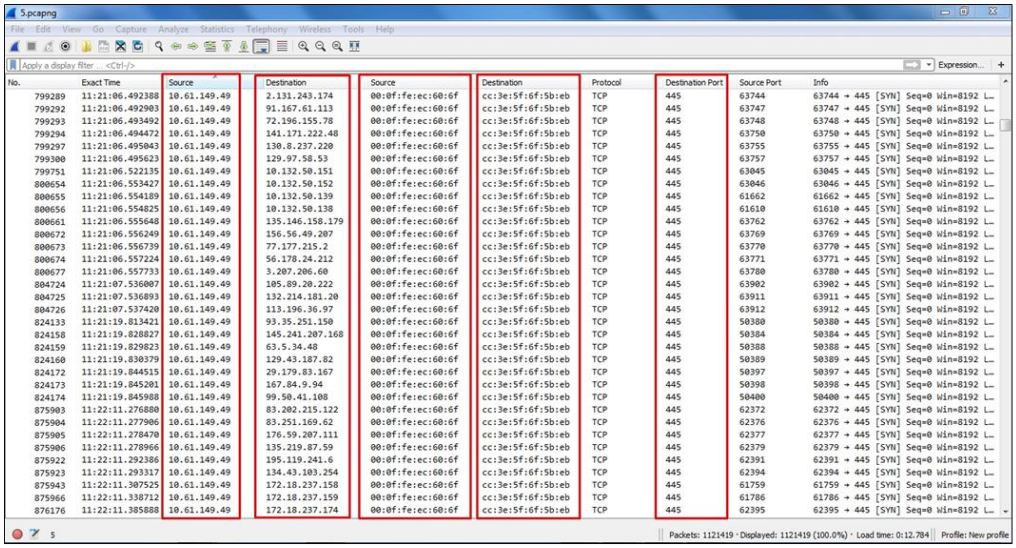
Resolution:
Identify & isolate rogue device from network or disable dhcp server in device configuration.



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.



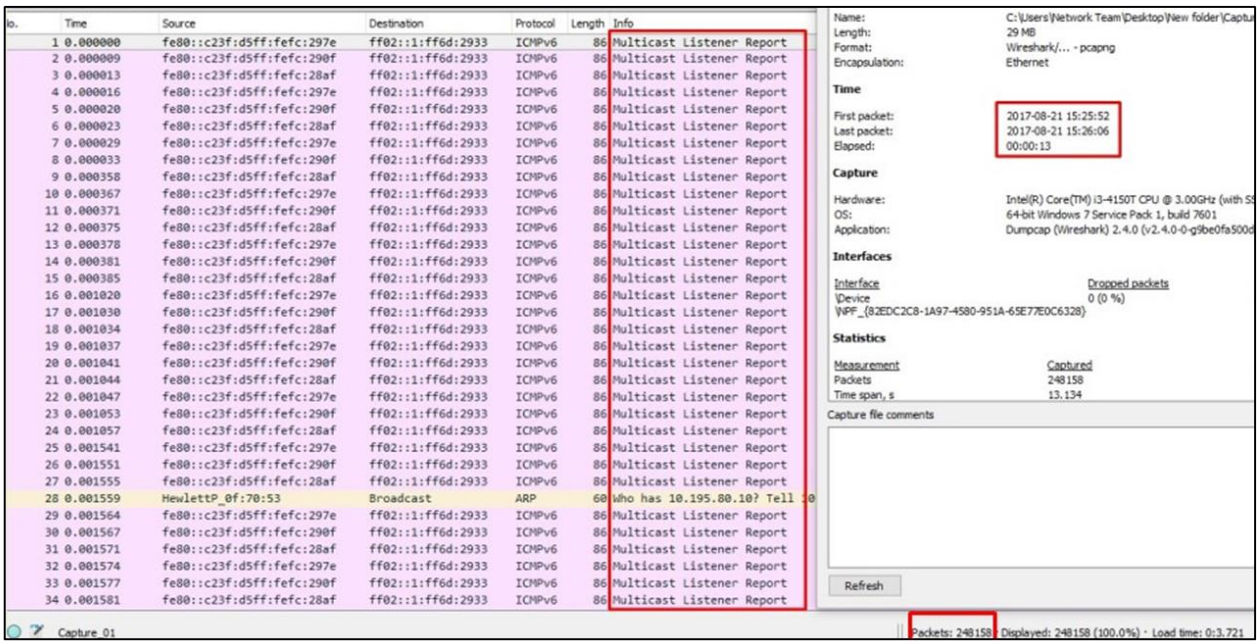
No.	Exact Time	Source	Destination	Source	Destination	Protocol	Destination Port	Source Port	Info
799289	11:21:06.492388	10.61.149.49	2.131.243.174	00:0f:fe:ec:60:6f	cc:3e:5f:6f:5b:eb	TCP	445	63744	63744 → 445 [SYN] Seq=0 Win=8192 L…
799292	11:21:06.492903	10.61.149.49	91.167.61.113	00:0f:fe:ec:60:6f	cc:3e:5f:6f:5b:eb	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:fe:ec:60:6f	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:fe:ec:60:6f	cc:3e:5f:6f:5b:eb	TCP	445	63750	63750 → 445 [SYN] Seq=0 Win=8192 L…
799297	11:21:06.495043	10.61.149.49	130.8.237.220	00:0f:fe:ec:60:6f	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	129.97.58.53	00:0f:fe:ec:60:6f	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:fe:ec:60:6f	cc:3e:5f:6f:5b:eb	TCP	445	63045	63045 → 445 [SYN] Seq=0 Win=8192 L…
800654	11:21:06.553427	10.61.149.49	10.132.50.152	00:0f:fe:ec:60:6f	cc:3e:5f:6f:5b:eb	TCP	445	63046	63046 → 445 [SYN] Seq=0 Win=8192 L…
800655	11:21:06.554189	10.61.149.49	10.132.50.139	00:0f:fe:ec:60:6f	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:fe:ec:60:6f	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	135.146.158.179	00:0f:fe:ec:60:6f	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:fe:ec:60:6f	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:fe:ec:60:6f	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	56.178.24.212	00:0f:fe:ec:60:6f	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:fe:ec:60:6f	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:fe:ec:60:6f	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:fe:ec:60:6f	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:fe:ec:60:6f	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:fe:ec:60:6f	cc:3e:5f:6f:5b:eb	TCP	445	50380	50380 → 445 [SYN] Seq=0 Win=8192 L…
824158	11:21:19.828827	10.61.149.49	145.241.207.168	00:0f:fe:ec:60:6f	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:fe:ec:60:6f	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:fe:ec:60:6f	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:fe:ec:60:6f	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:fe:ec:60:6f	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:fe:ec:60:6f	cc:3e:5f:6f:5b:eb	TCP	445	50400	50400 → 445 [SYN] Seq=0 Win=8192 L…
875903	11:22:11.276880	10.61.149.49	83.202.215.122	00:0f:fe:ec:60:6f	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:fe:ec:60:6f	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:fe:ec:60:6f	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	135.219.87.59	00:0f:fe:ec:60:6f	cc:3e:5f:6f:5b:eb	TCP	445	62379	62379 → 445 [SYN] Seq=0 Win=8192 L…
875922	11:22:11.292386	10.61.149.49	195.119.241.6	00:0f:fe:ec:60:6f	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:fe:ec:60:6f	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:fe:ec:60:6f	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:fe:ec:60:6f	cc:3e:5f:6f:5b:eb	TCP	445	61786	61786 → 445 [SYN] Seq=0 Win=8192 L…
876176	11:22:11.385888	10.61.149.49	172.18.237.174	00:0f:fe:ec:60:6f	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.

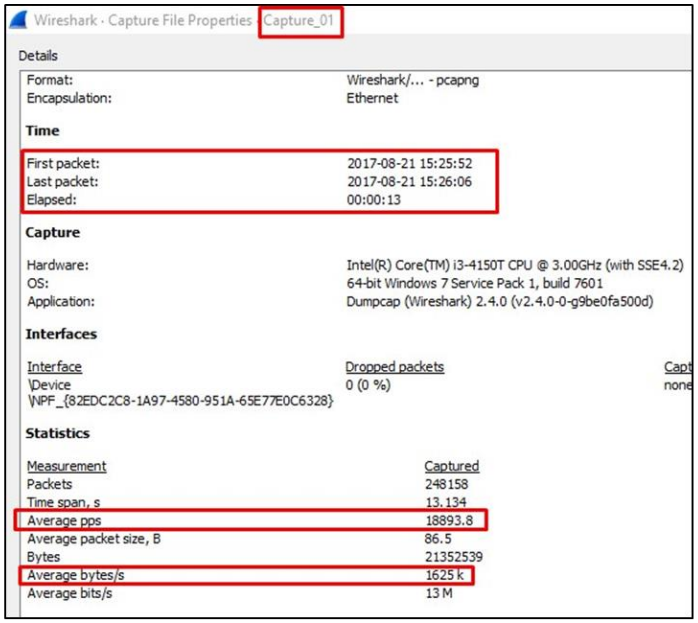
Resolution:
Identify & isolate offended machine from network.

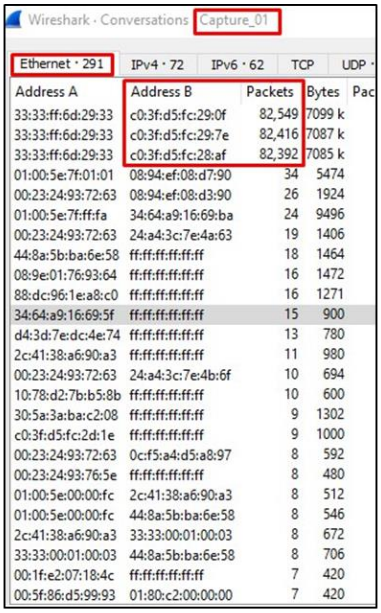


Note: captured packets using third party software (Wireshark)

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.





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-DNI214202LO#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/mounting/guide/apmount.html#wp46770
- 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**
- 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

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/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/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-6600ap-cli-guide-v20.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

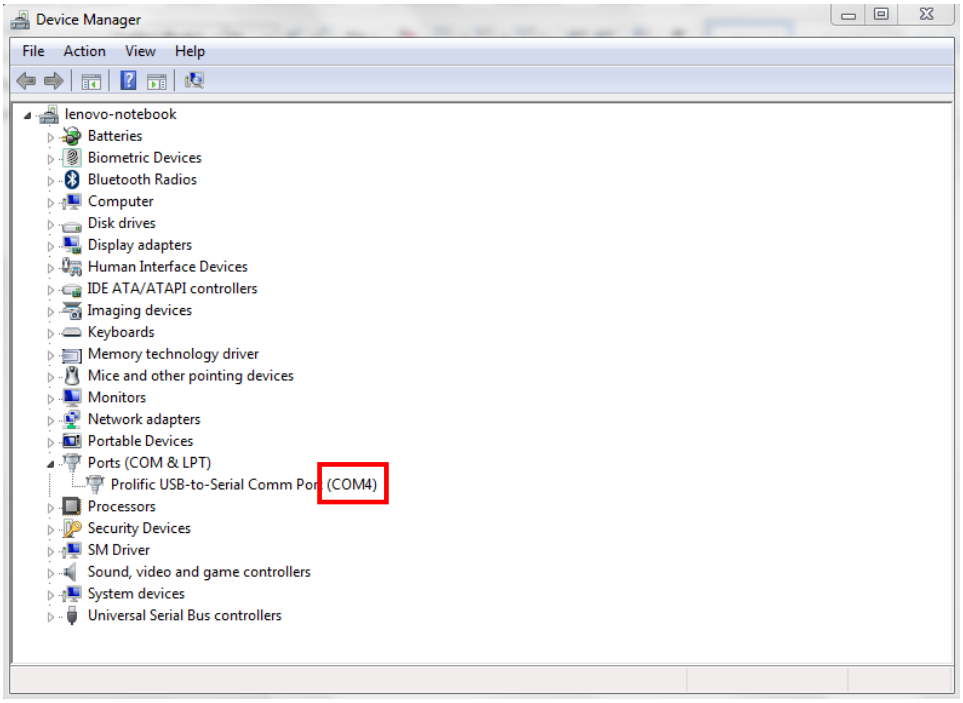
1 Remote Access to Switch

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

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

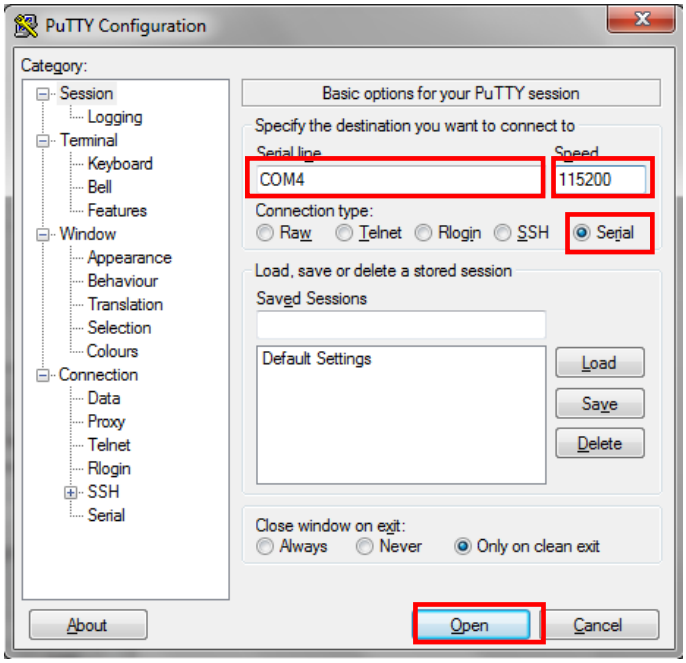
1.1 Console Cable

i. 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)**



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**: 115200

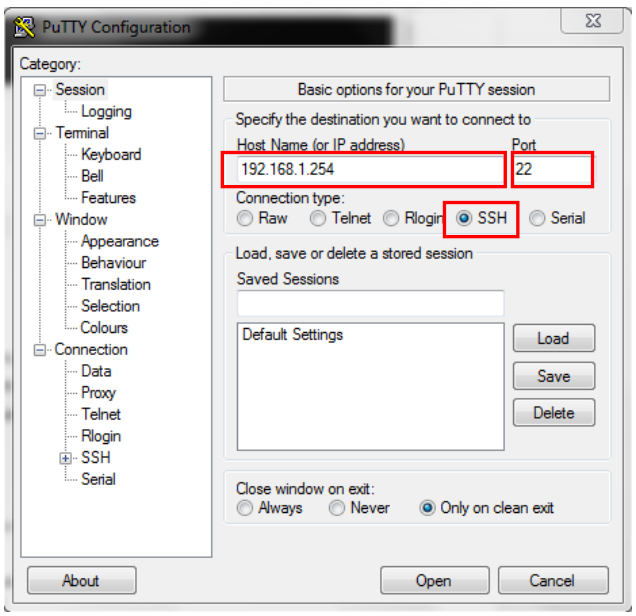


iii. Press **Enter** 2 times and the switch will prompt for enter **User Name** and **Password**. Key in switch user name and password

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

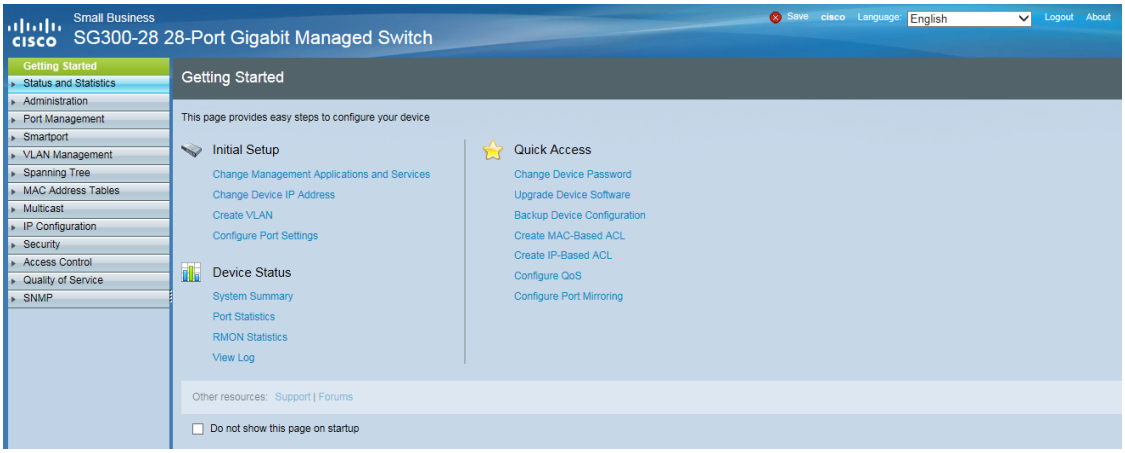


ii. Switch will prompt for User Name and Password. Key in switch user name and password

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

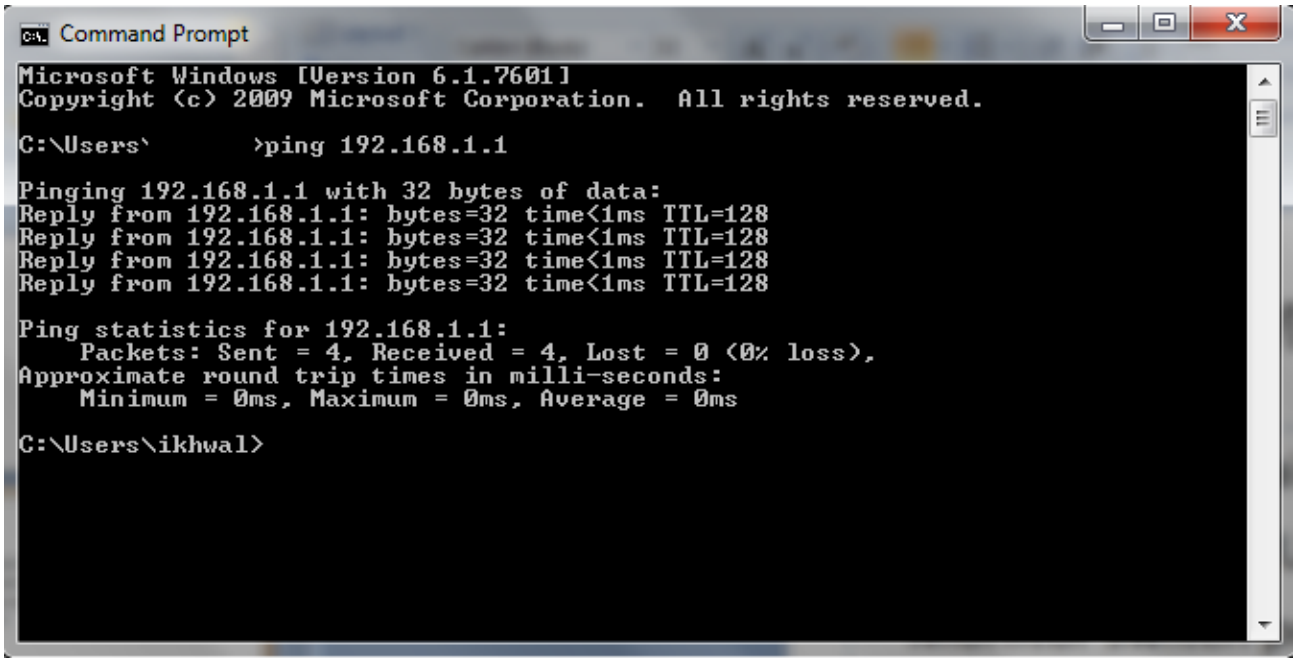
No.	Command	Description
1	sh run	Display running configuration
2	sh start	Display startup configuration
3	sh system	Display switch information (uptime, MAC, model)
4	sh clock	Display switch time
5	sh system id	Display switch serial number
6	sh system mode	Display switch layer mode
7	sh int status	Display 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



2.2 Check Switch CPU Utilization (Switch CLI)

i. Login to switch though console or SSH

ii. From switch console type show cpu utilization

iii. The CPU utilization in percentage will be display as below

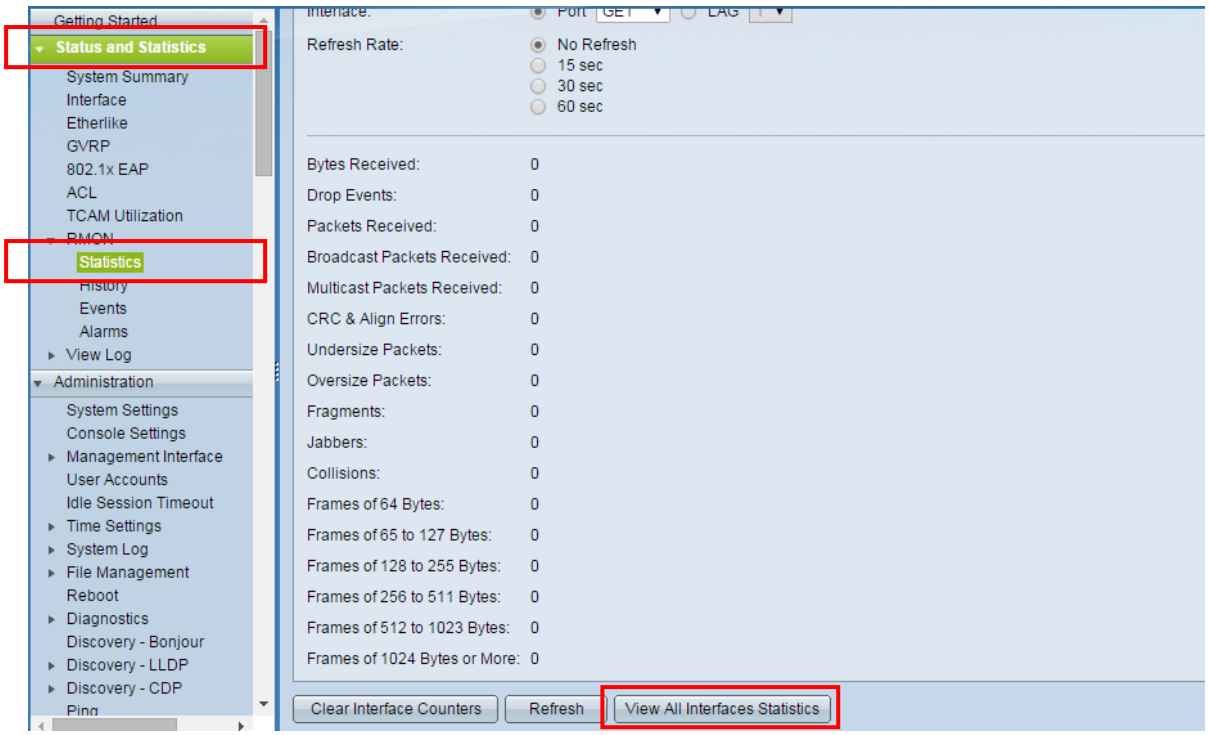
```
switch9986b3#show cpu utilization
CPU utilization service is on.

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 Port 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
GE1	0	0	0	0	0	0	0	0	0	0	0	0	0
GE2	0	0	0	0	0	0	0	0	0	0	0	0	0
GE3	0	0	0	0	0	0	0	0	0	0	0	0	0
GE4	214797	0	1880	747	319	0	0	0	0	0	0	965	432
GE5	0	0	0	0	0	0	0	0	0	0	0	0	0
GE6	0	0	0	0	0	0	0	0	0	0	0	0	0
GE7	757019	0	5351	951	881	0	0	0	0	0	0	2794	1085
GE8	0	0	0	0	0	0	0	0	0	0	0	0	0
GE9	0	0	0	0	0	0	0	0	0	0	0	0	0
GE10	0	0	0	0	0	0	0	0	0	0	0	0	0
GE11	0	0	0	0	0	0	0	0	0	0	0	0	0
GE12	0	0	0	0	0	0	0	0	0	0	0	0	0
GE13	0	0	0	0	0	0	0	0	0	0	0	0	0
GE14	0	0	0	0	0	0	0	0	0	0	0	0	0
GE15	0	0	0	0	0	0	0	0	0	0	0	0	0
GE16	0	0	0	0	0	0	0	0	0	0	0	0	0
GE17	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 though 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

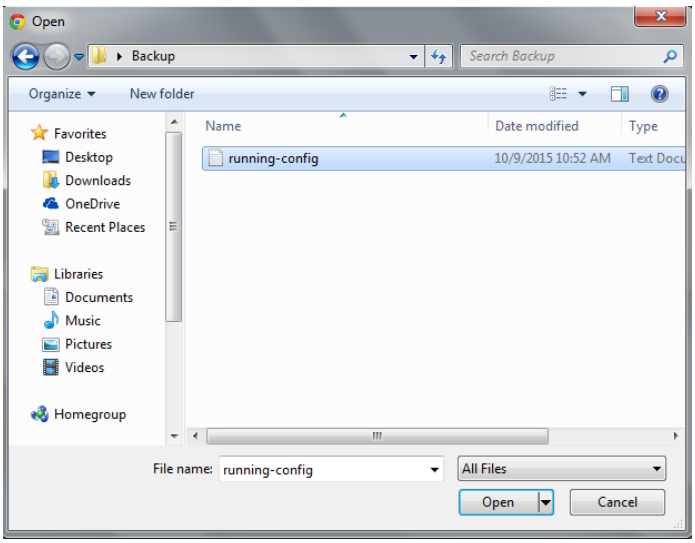
i. Login to switch through Web

ii. Go to **Administration** -> **File Management** -> **Download/Backup Configuration/Log**

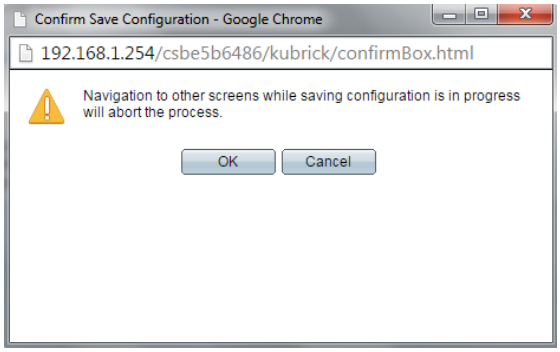
iii. In **Transfer Method**, select **via HTTP/HTTPS**

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**.



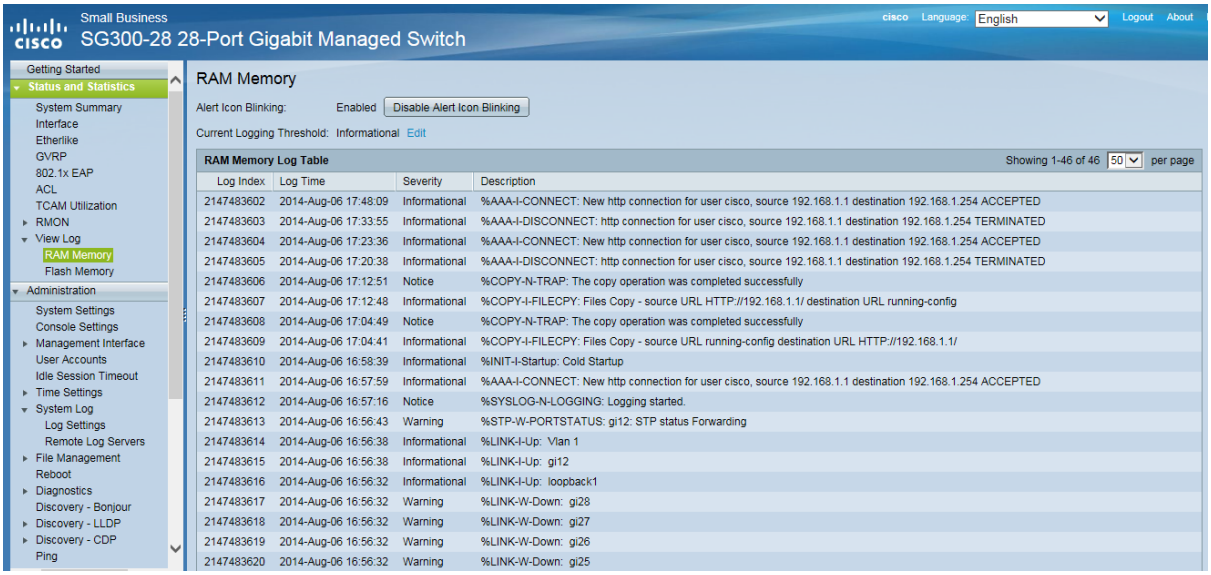
vi. In **Destination File Type**, select **Running configuration** then click **Apply**.
vii. A **Confirm Save Configuration** message box will appear. Click **OK** to proceed



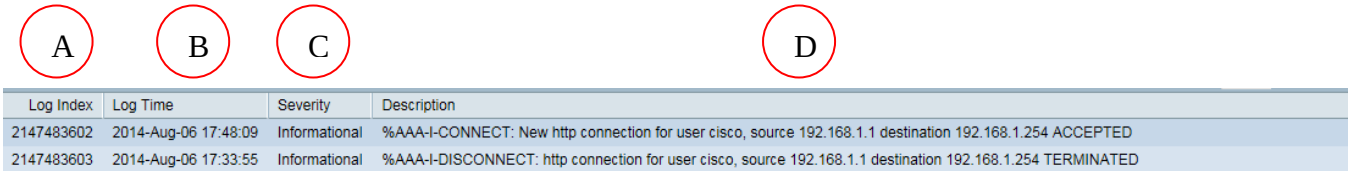
4 Switch Logs

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



4.2 Log Message Format



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

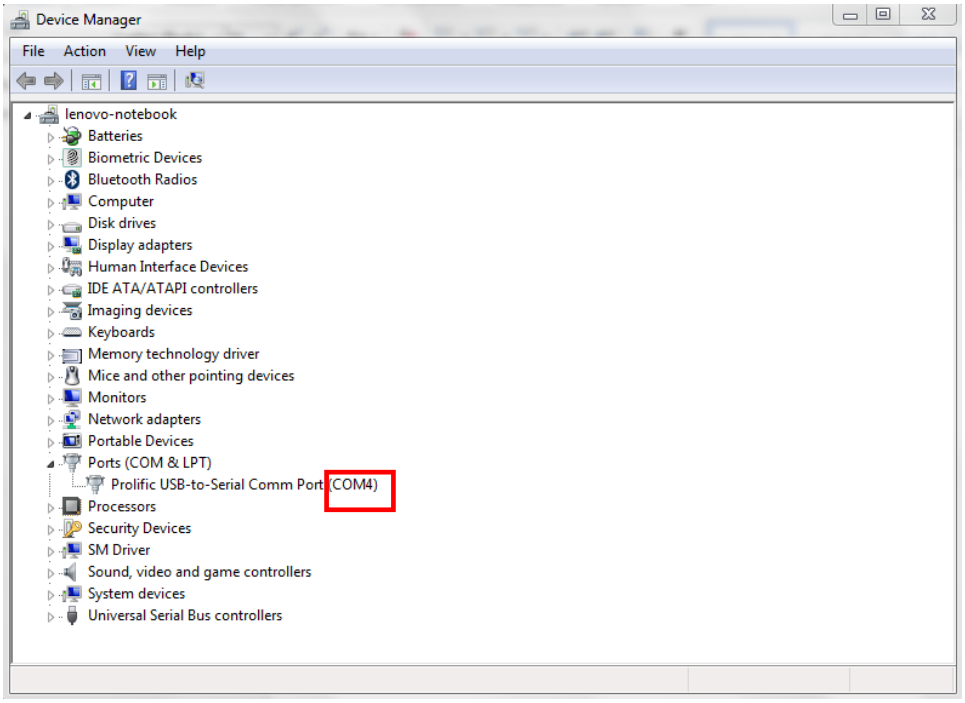
1 Remote Access to Access Point

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

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

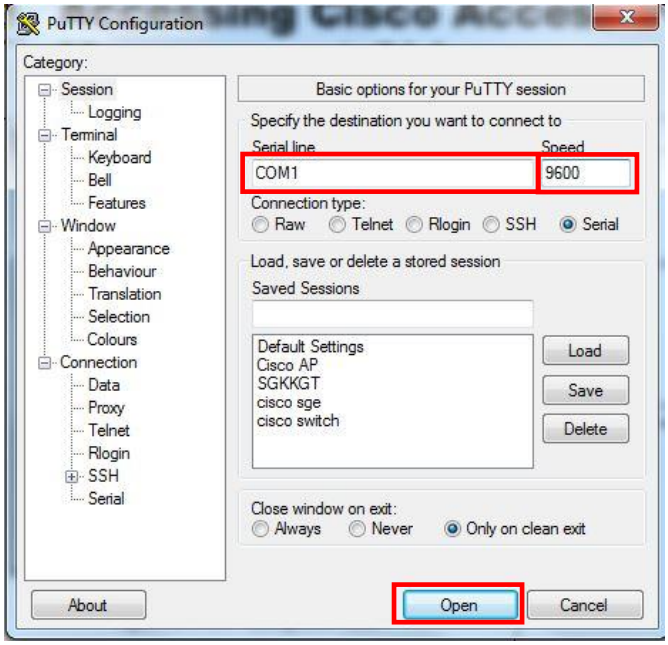
1.1 Console Cable

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**

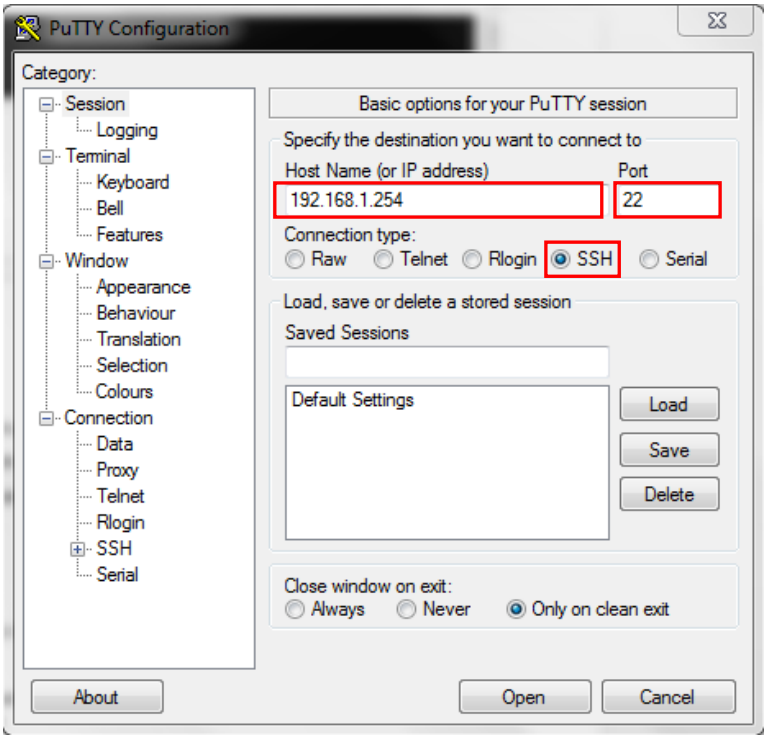
- **Serial line**: Your Comm port name
- **Speed**: 9600 (Cisco AP) / 115200 (Dlink AP)



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

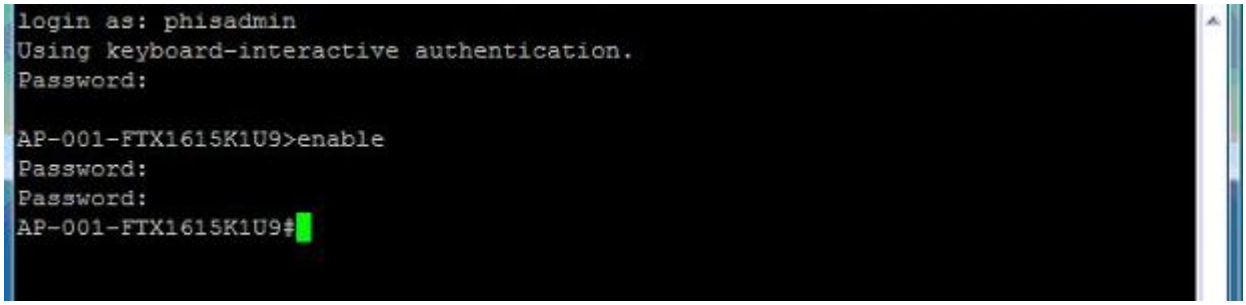
1.2 Secure Socket Shell (SSH)

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

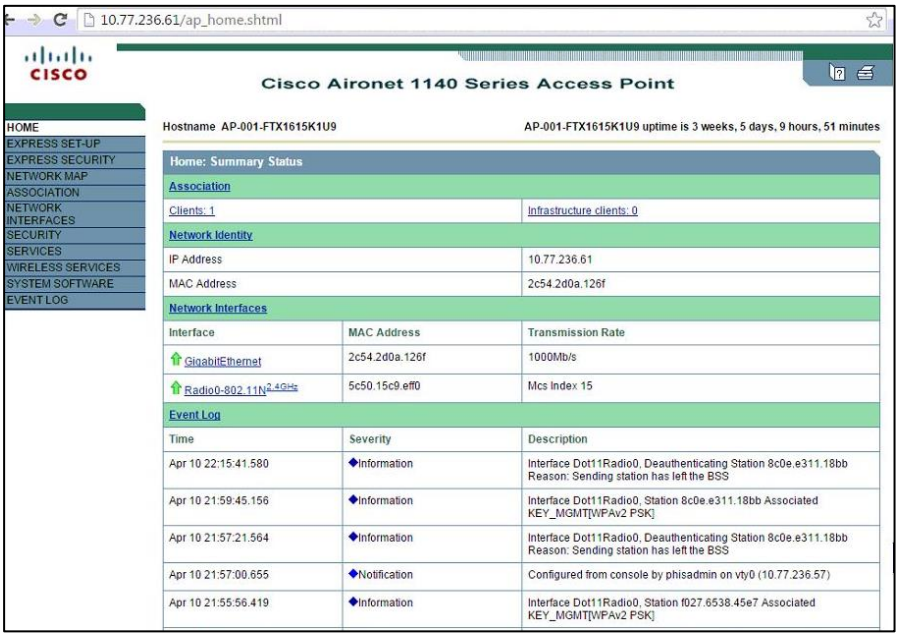
iii. Type 'enable' command and key in the management password to go to Priviledge Mode (for Cisco AP only).



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)

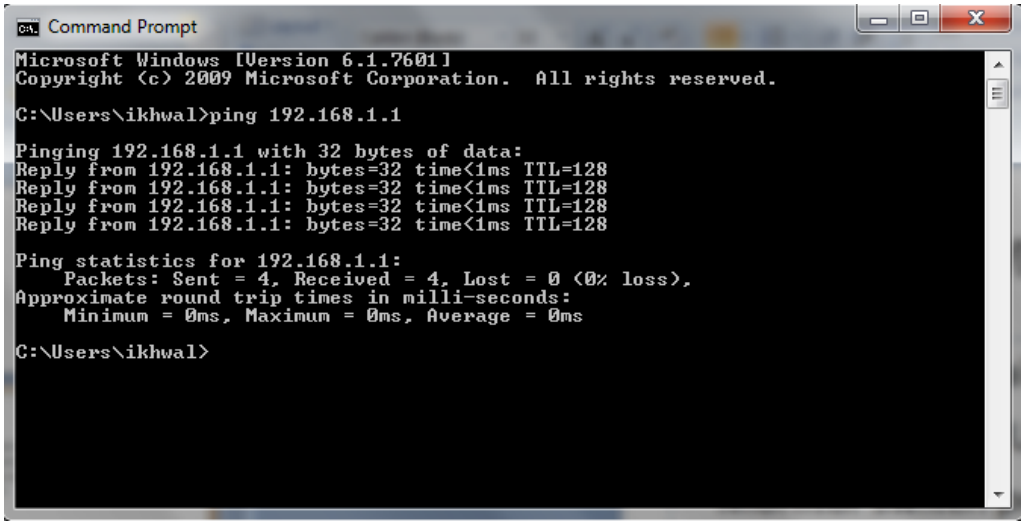
*for Cisco AP only

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



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

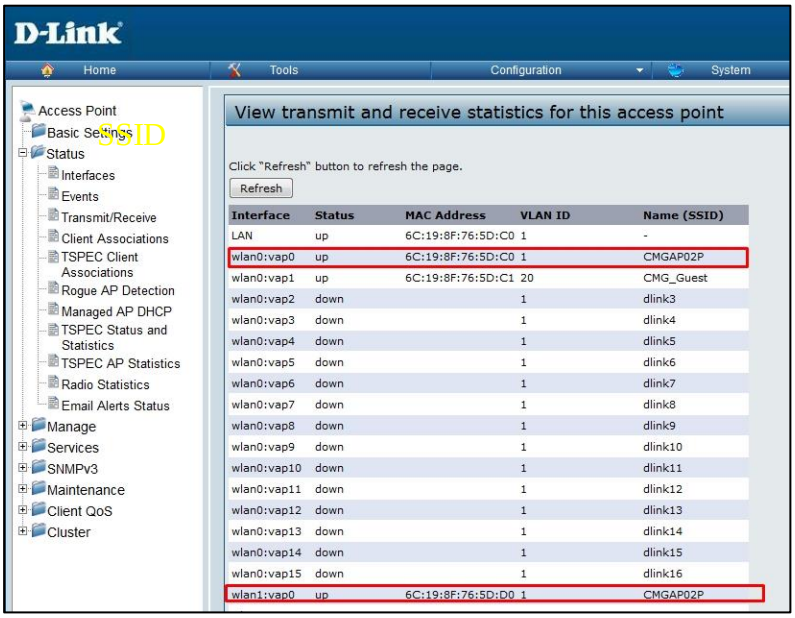
iii. Check the radio interface. Green arrow indicates that the Radio0-802.11N$^{2.4GHz}$ is enabled and the status is UP. Red arrow indicates that either the Radio0-802.11N$^{2.4GHz}$ is disabled or the status is down.

For Dlink AP

i. From Desktop, open browser and type access point IP address

ii. In the Home menu, go to Status >> Transmit/Receive

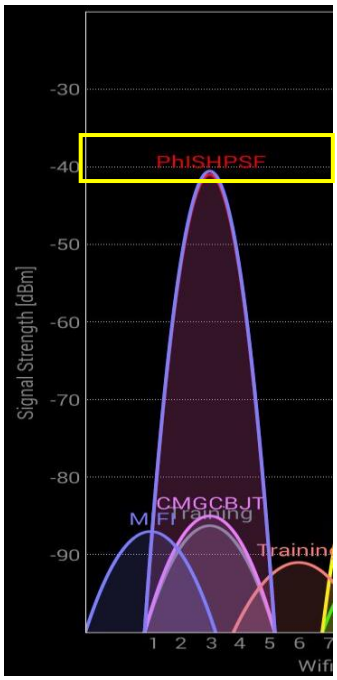
iii. Check radio interface status. wlan0: vap0 indicate for 5GHz, wlan1: vap0 indicate for 2.4GHz.

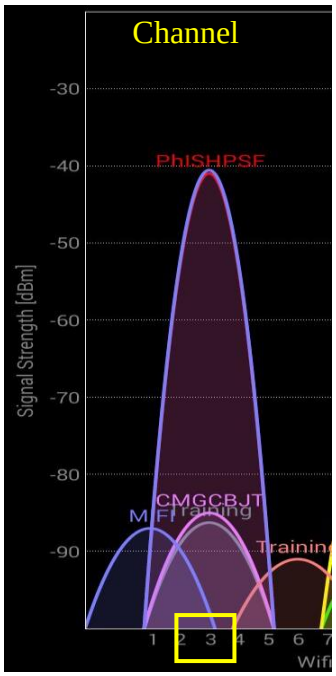


2.3 Check access point SSID & signal strength (Wifi Analyzer)

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).



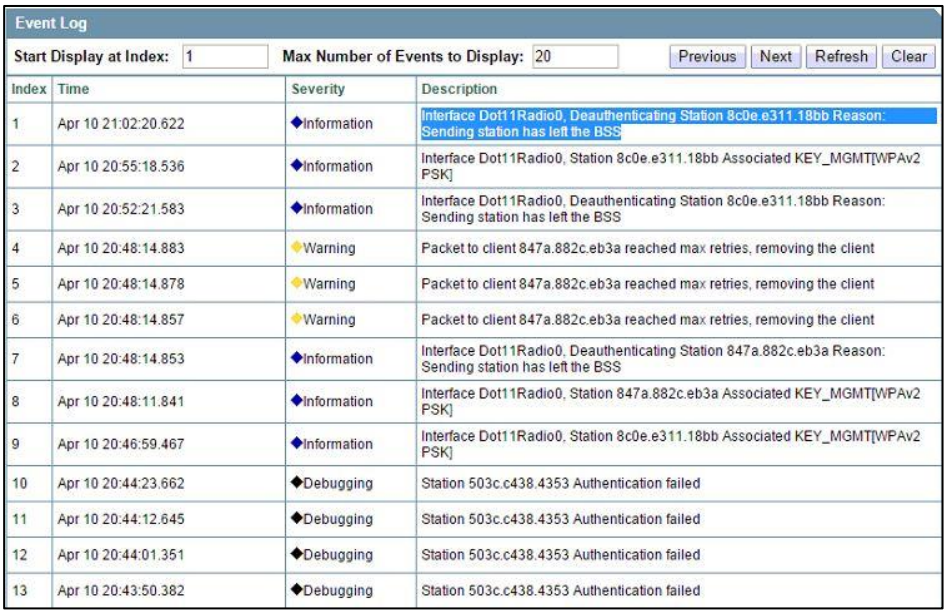


3 Access Point Logs

3.1 View the access point logs (GUI)

For Cisco AP

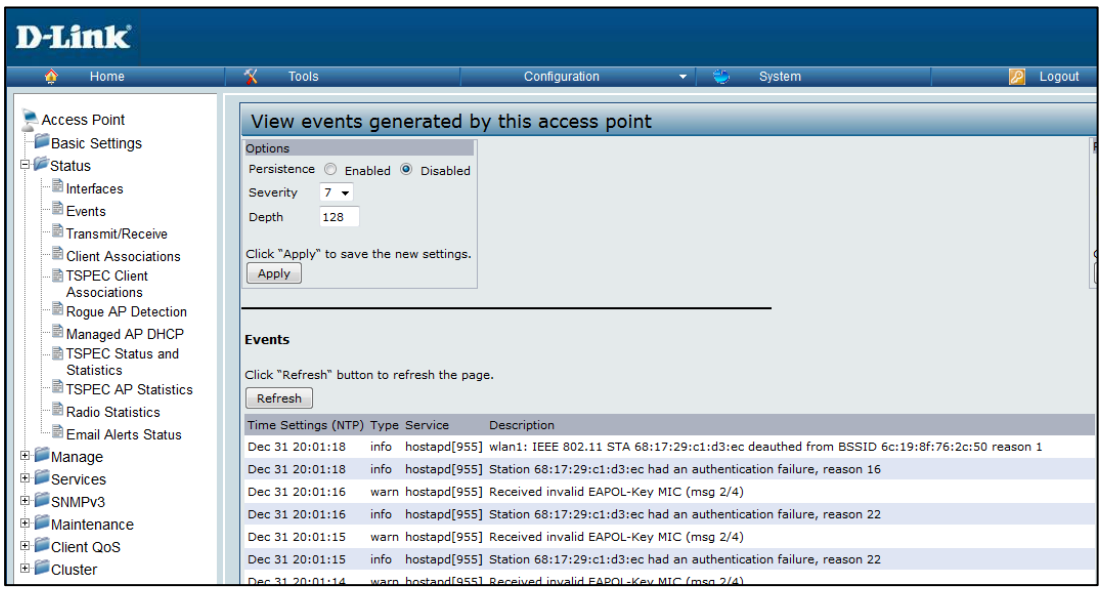
i. From Desktop, open browser and type access point IP address
ii. Key in the management username and password
iii. From the main page, go to Event Log >> Configuration options.



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

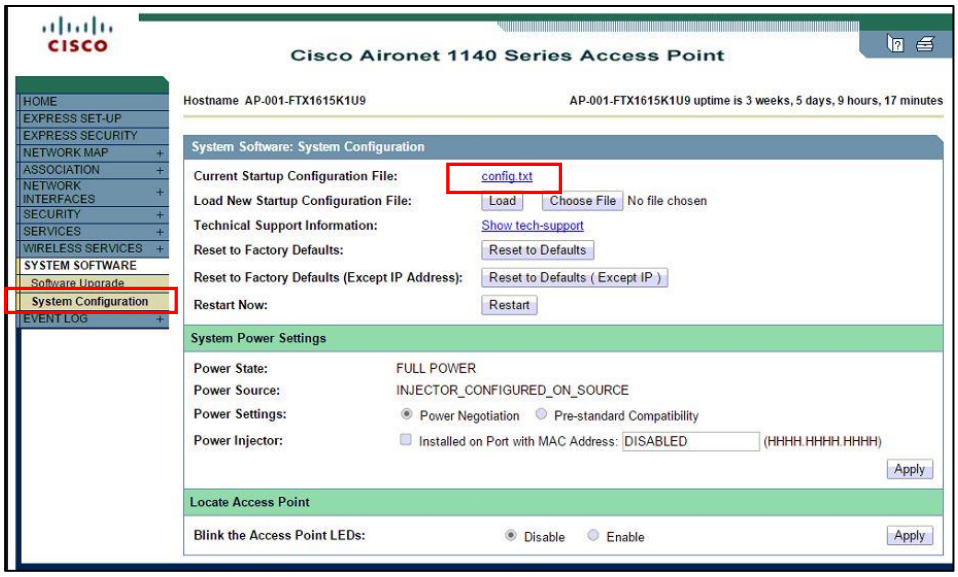
i. From Desktop, open browser and type access point IP address
ii. Key in the management username and password
iii. From the main page, go to Status >> Events.



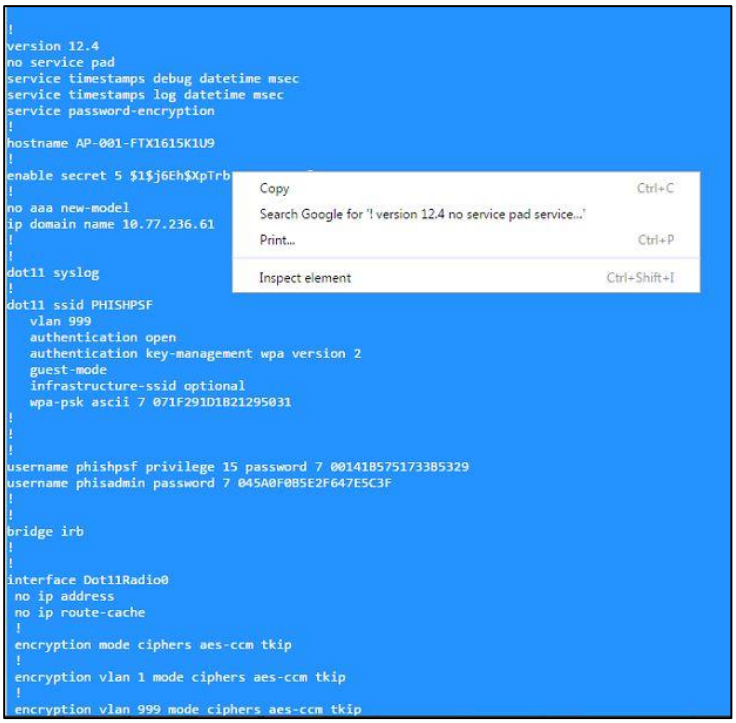
4 Backup and Restore Access Point Configuration File (GUI)

4.1 Cisco Aironet - Backup Access Point 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 Software** >> Configuration options
iv. Click config.txt at Current Startup Configuration File

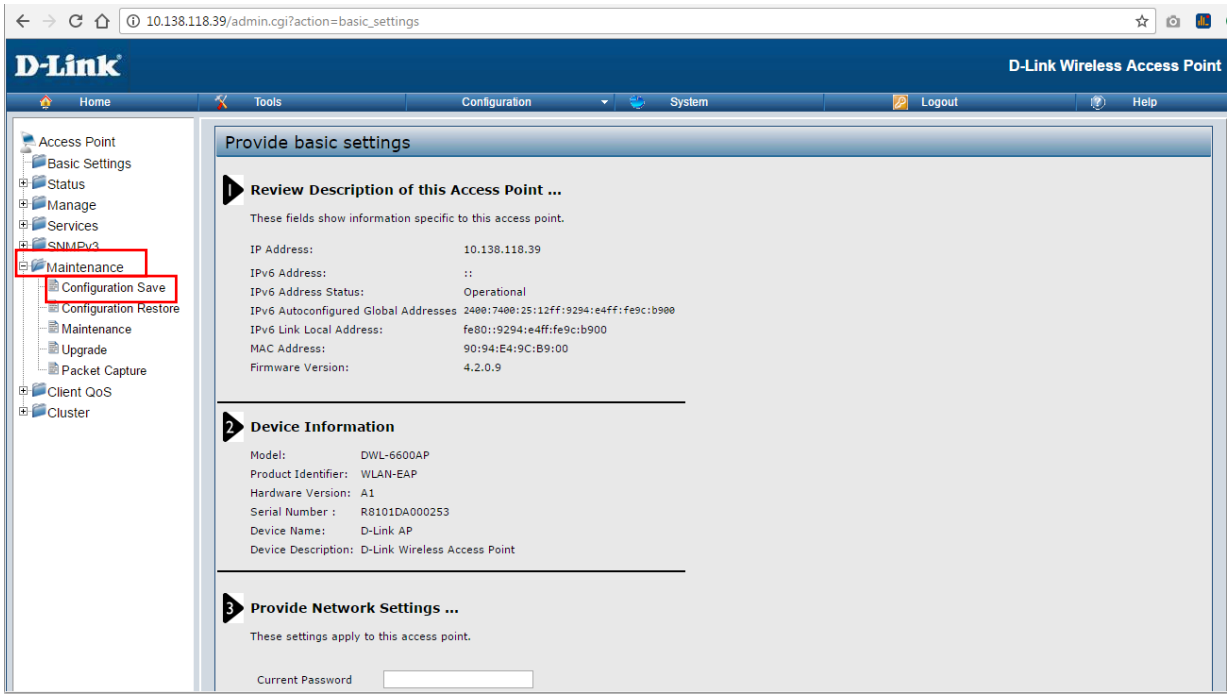


v. Select all the text, copy & paste it in the Notepad



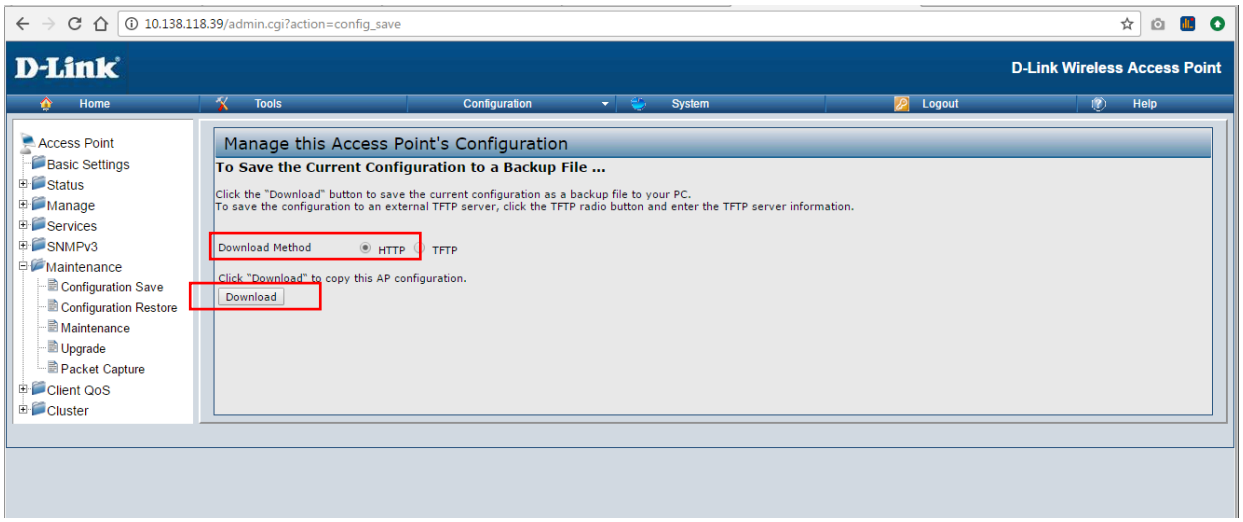
4.2 D-Link AP - Backup Access Point Configuration File (GUI)

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

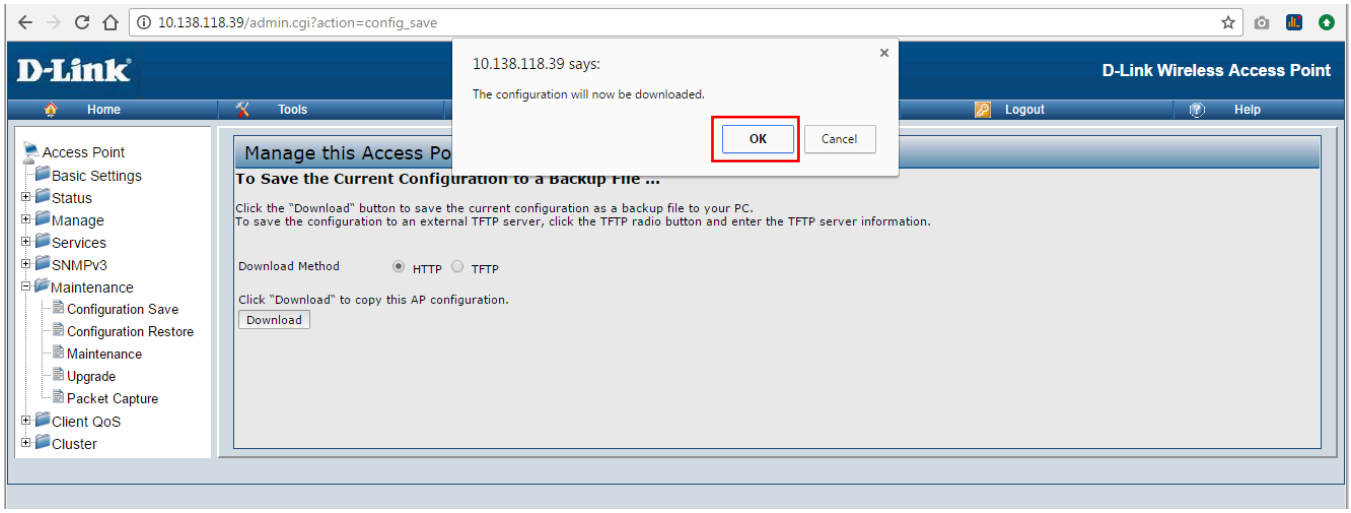


ii. Choose **HTTP** as download method.

iii. To save the current configuration to a Backup file, click on **Download** button.

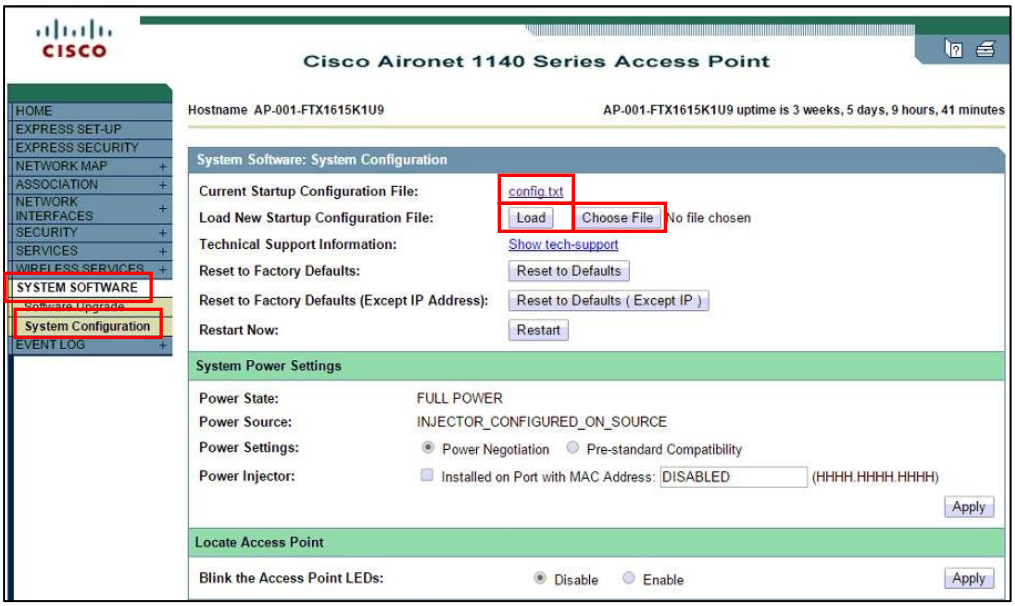


iv. Click **OK** to download the configuration file in .XML file format.



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

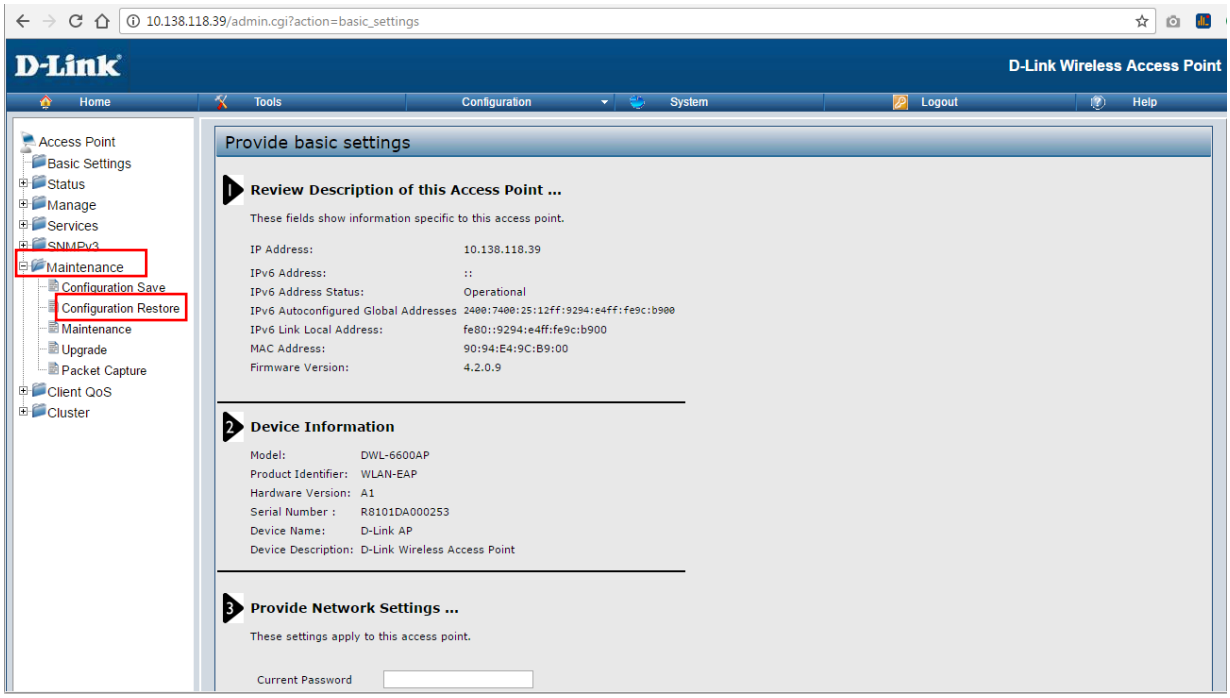
i. From Desktop, open browser and type access point IP address
ii. Key in the username and password
iii. From the main page, go to **System Software** >> System Configuration
iv. Click the Choose File button to browse the configuration file.
v. Click Load button to upload the file.



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)

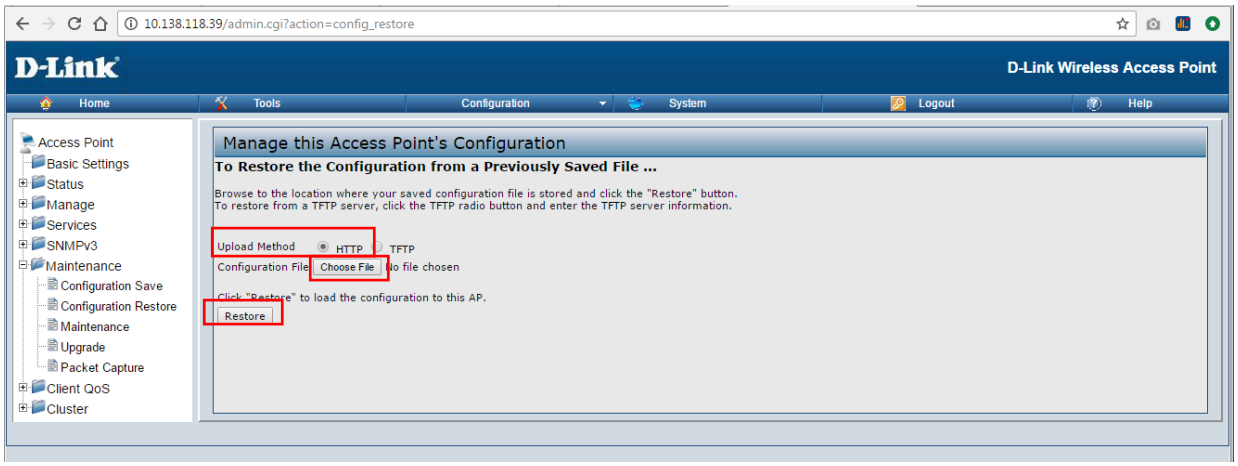
i. From D-Link main page, expand **Maintenance** and click on **Configuration Restore**.



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

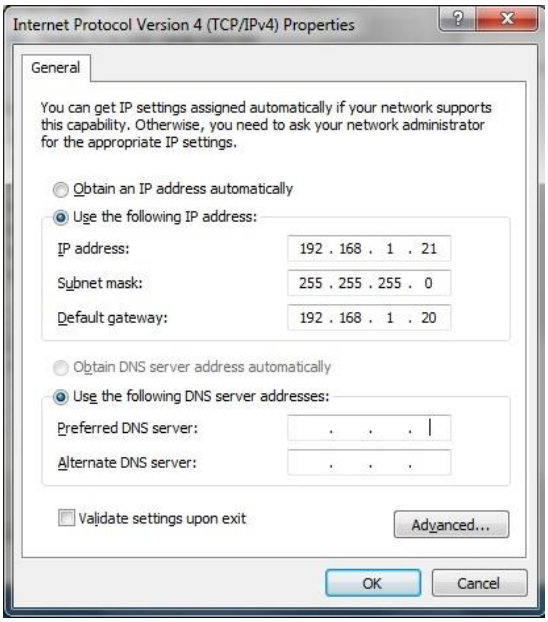
This section describes on Wireless Bridge Operation Guidelines.

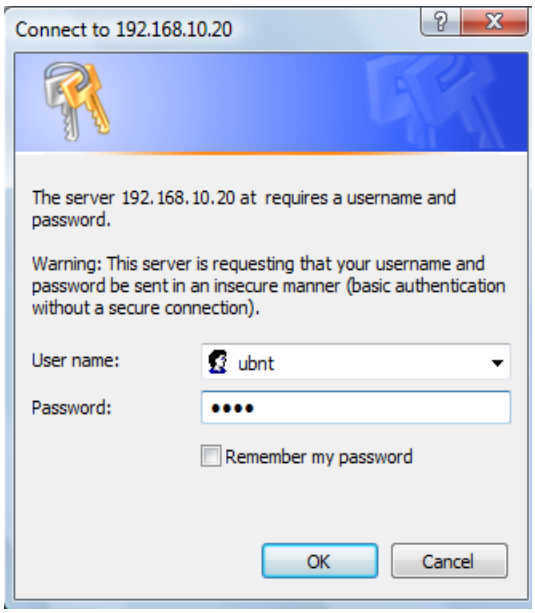
Scope of this section covers the following topics:

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

1 Access with Graphical User Interface

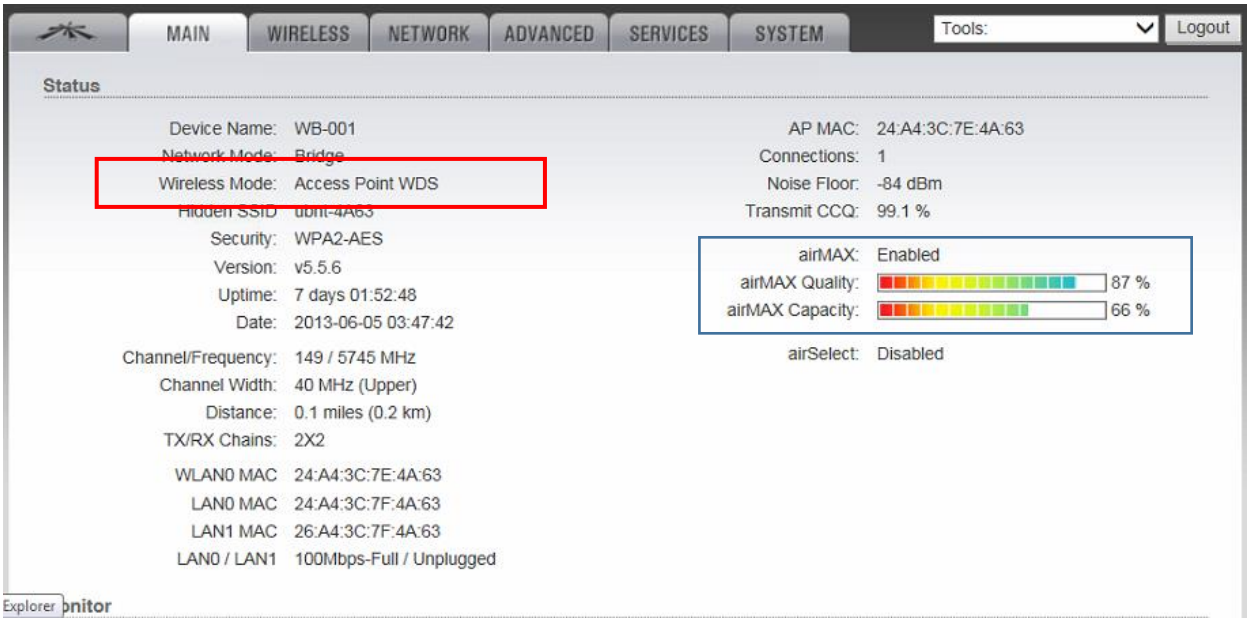
STEP	DESCRIPTION
1	In your computer, open Control Panel > Network Connections > Local Area Connection.
2	In Local Area Connection Status > General, click **Properties**.
3	In Local Area Connection Properties > General, select **Internet Protocol (TCP/IP)** and click **Properties**.
4	In Internet Protocol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





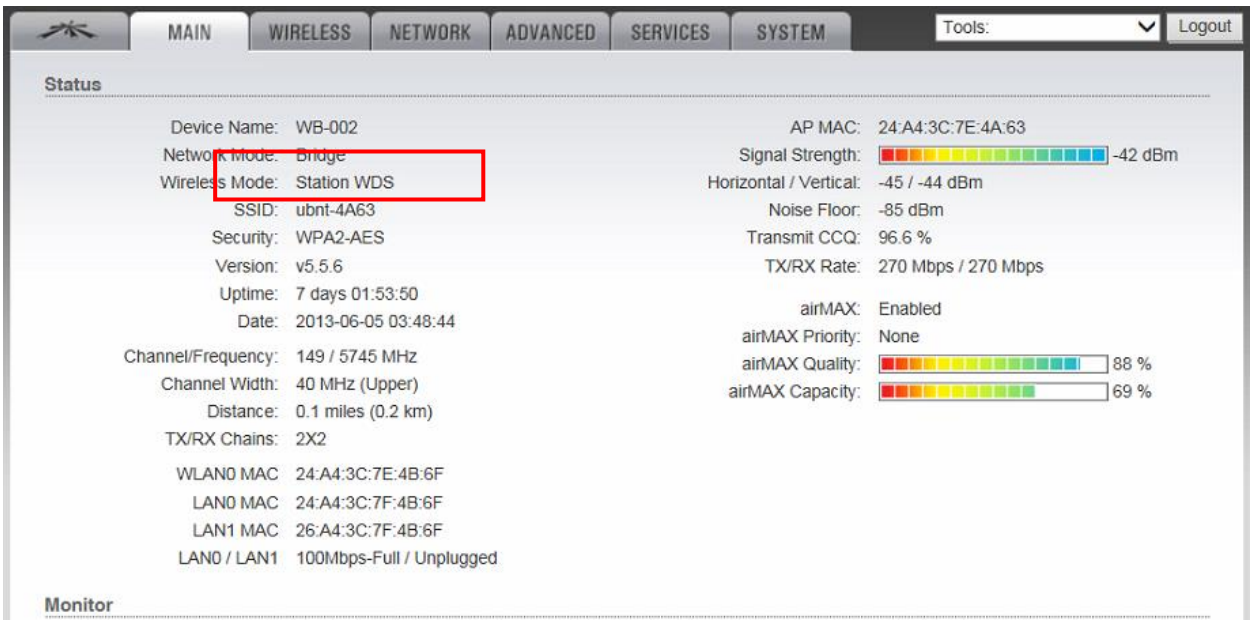
2 View Wireless Bridge status

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%.



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%.



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