BTECH 451A&B

Configuration and Technical Support

Data Communications

With CNZ

Arun Manohar Vejendla

Department of Computer Science

University of Auckland

UPI: avej002

ID: 4866880

JUNE 2011

CAP 501-5D:

WiBorne CAP 501-5D is a high power outdoor wireless bridge, access point, router and CPE (customer premises equipment - generally located at customers end). This bridge acts as a point of connection to wireless networks for service providers that provide last mile services. CAP 501-5D has an option of built-in 5GHz 15dBi dual polarity directional antenna or 2 N-type connectors without antenna (one of the first connectors capable of carrying microwave signals). It consumes 200mW of high power and provides 1 to 54 Mbps of data rates. This bridge connects to Wi-Fi mesh or WDS infrastructure to provide the customers with an Ethernet connection for local access. CAP 501-5D works point to point or in point to multipoint topologies. This device can be used for seven different purposes in four available operation modes. The four operation modes are AP mode (access point mode), WDS mode, CPE mode and Client Bridge + universal repeater mode. CAP 501-5D is a multiple mode system that can be configured as a wireless access point or a gateway. It uses WDS link to expand the range of Ethernet networks. This device supports standards 802.11n and 802.11a and the security is provided using WEP, Wi-Fi protected access (WAP and also WPA2). It has weather proof housing for physical protection. This device also provides quality of service which means proper management of bandwidth and traffic prioritization is taken care of, in other words the most important data is sent first and the least important is sent after the high priority data is sent first.

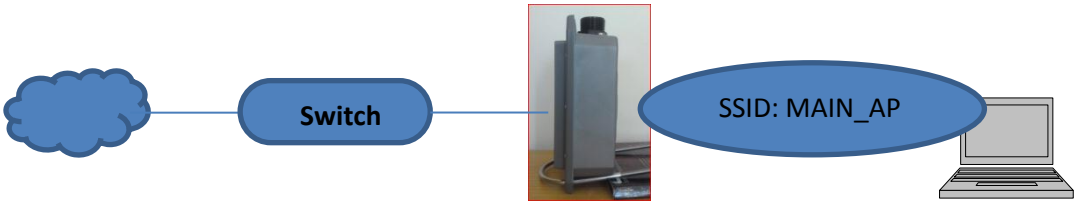
1. This is where the reboot button is located, unscrew the screw to device or reset to default configuration
2. This device has three LEDs, This LED is to check the status of power
3. This LED indicates status of WLAN – green light tells wireless is possible
4. This LED indicates the Ethernet status
5. This is for connecting this device to PSE device for PoE
6. Two N-type connectors for connecting two antennas

Applications of CAP 501-5D:

First of all, the device CAP 501-5D can be used in four different modes such as AP mode (or can be a combination of both AP + WDS), WDS mode, CPE mode and Client Bridge + universal repeater mode. This device can be deployed as a normal access point. The repeater can be used to enlarge/expand the wireless network. WDS can be used to expand the Ethernet network using wireless WDS links. The combination of AP+WDS not only expands the Ethernet network but also provides wireless access to the extended network. CPE is a wireless gateway that uses NAT and DHCP functions in order to connect to wireless internet service providers. Client Bridge + universal repeater is a wireless repeater or a bridge that allows a connection to wireless internet service provider (WISP).

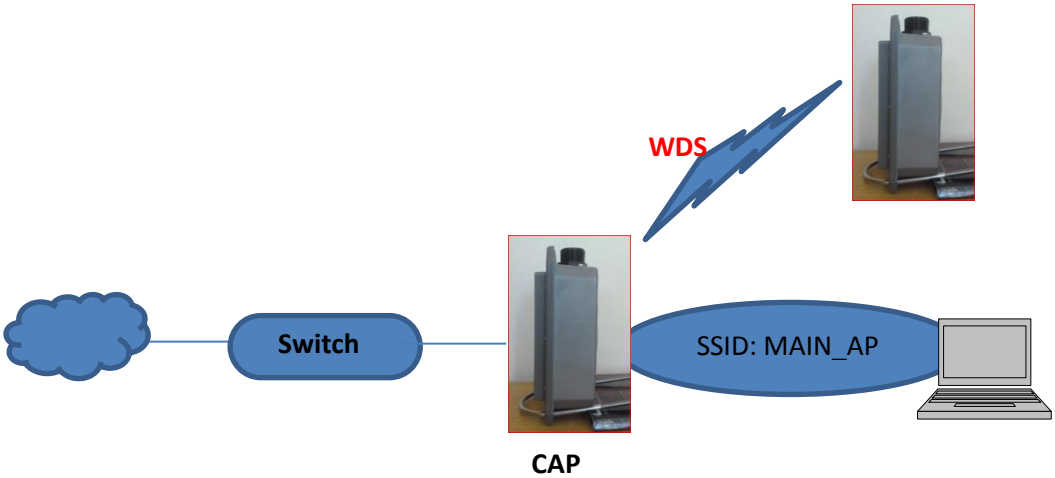
Access point mode (AP mode):

An access point can be either a main, relay or remote base station. The main base station is connected to a wired network. The relay base station is station that relays data between the base, relay and remote stations. The remote base station accepts connections from wireless devices such as laptops. There are two types of AP modes. One is pure AP mode (access point without WDS link) and the other AP/WDS mode. In pure AP mode, generally CAP 501-5D device can be deployed as a fixed access point that connects to a wired network (LAN) that is available and acts as a source of wireless connection point (AP) for other wireless devices so that they could access the internet.



CAP

In AP+WDS mode, an access point can be deployed as a fixed wireless AP that provides a WDS link to expand the network. This mode enables wireless interconnection of several access points in a network and also accepts the wireless connection of clients. In the diagram below, AP+WDS mode is shown and we can see that using a WDS link we can expand the network wirelessly so in this case another wireless AP (CAP 501-5D bridge) is connected so it also accepts many wireless clients to provide wireless access to internet



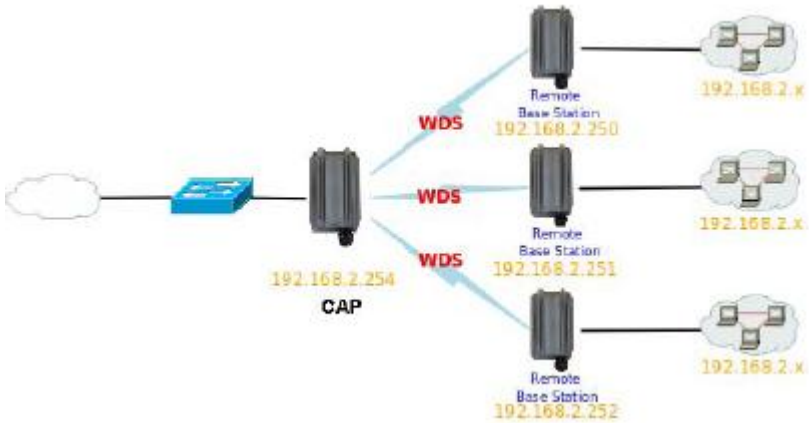
CAP

AP Mode provides single point of control and security for the wireless LANs which helps in keeping the network secure and also controlled.

WDS mode:

WDS mode is also called the repeater mode. Wireless distribution system is a system that provides the wireless interconnection of access points in the network that is using the standard IEEE 802.11. In this case the AP devices are our CAP 501-5D and only they are allowed to communicate with each other but not the clients such as laptops. Because this mode allows the access points to be interconnected, the wireless network will be expanded without the need of physical wiring. It allows one access point to receive data wirelessly from another access point and forward that data to its own wireless clients. The access point allows one or more WDS links but do not allow any wireless clients such as laptops have a direct connection to it. The connections can be point to point, point to multipoint and multi-point as shown in the diagrams below.

Reference: point to point connection - WDS mode: reference – CAP 501-5D pdf compucon, page 3

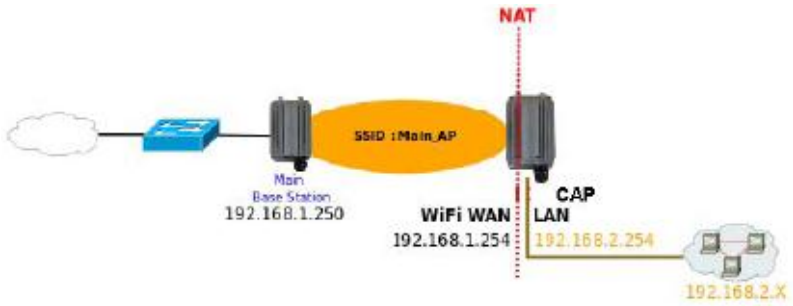


Reference: point to multipoint, WDS mode: reference – CAP 501-5D pdf compucon, page 4

Reference: multi-point, WDS mode – CAP 501-5D pdf compucon, page 4

CPE Mode:

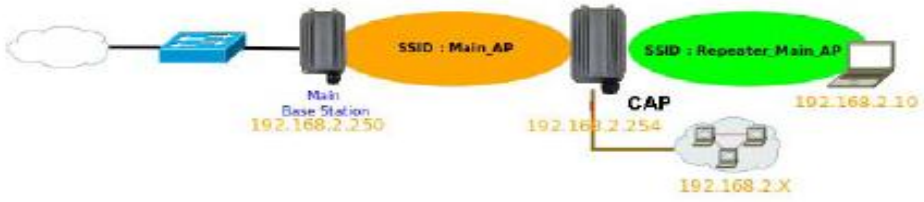
In this CPE (customer premises equipment) mode, the device CAP 501-5D can be used an outdoor CPE device to receive wireless signals over last mile so that wireless internet service providers can provide high speed broadband service to the customers. WAN is used as a Wi-Fi connection. In this mode this device is enabled with NAT and DHCP server functions. 'NAT' is also called network address translation where each IP packet's address information in available in packet headers is modified. In basic NAT, the address and checksum fields are modified and NAT is used when there is a requirement to connect two networks with incompatible addressing. DHCP (dynamic host configuration protocol) on the other hand allows a client to ask the central server for a network address in order to have a source address for that client to send and receive the data. The clients that are connected to CAP 501-5D must be in different subnets from those of main base station. This mode does not allow wireless connections from wireless clients such as laptops



Reference: CPE mode - CAP 501-5D pdf compucon, page 4

Client Bridge + universal repeater mode:

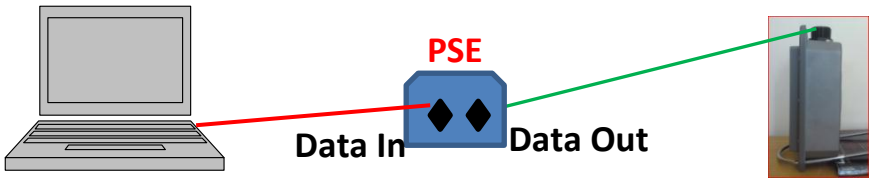
Client bridge + universal repeater mode provides the MAC addresses so that clients that are behind the device CAP 501-5D (one access point) can connect to other access point in this case the main base station without any support of WDS link. In the diagram below, the CAP 501 -5D is supported with DHCP functions and the clients of CAP 501-5D are in the same subnet as the main base station and this device accepts wireless connection from clients such as laptops. In this mode both the access points communicate with each other and also the clients are allowed to communicate.



Reference: Client Bridge + universal repeater mode - CAP 501-5D pdf compucon, page5

Configuration:

Step1: Hardware configuration:

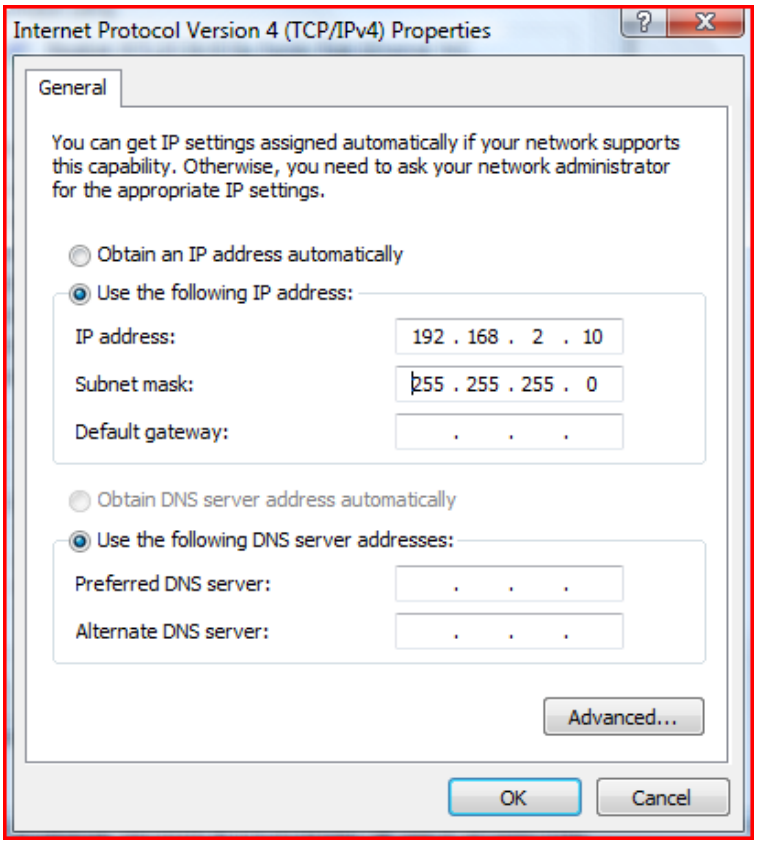


This is the first step – to set up the hardware in an accurate manner. By looking at the above picture we can see that it is important to figure out which cable goes into which slot of the PSE device; other wise the communication won't take place between the two laptops. So, one of the cat5 cables that is connected to the laptop must go into the data in slot of the PSE device and the other cable that is connected to the CAP501-5D bridge must go into the data out slot. Finally, to finish off the hardware setup we must attach the power cable into the PSE injector and connect it to the power outlet.

Step2: Network adaptor configuration:

It is important to assign a static IP address to our laptops network adaptor before configuring the access point (CAP501-5D bridge) in the subnet of 192.168.2.x range; for example 192.168.2.10, 192.168.2.200 etc. The IP address must be in the same range because; the bridges are assigned with a default IP address of 192.168.2.254. To assign a static IP address:

- Go to control panel → network and sharing centre → Manage network connections
- Right click on Local area connection → select properties.
  Note: Under some operating systems e.g. windows7, this local area connection icon is not shown unless the device is physically connected to the laptop and plugged into the main
- Select Internet protocol version 4 (TCP/IPv4) → click properties → change IP address according to the range mentioned above but must be different from default IP address of the bridge (192.168.2.254)

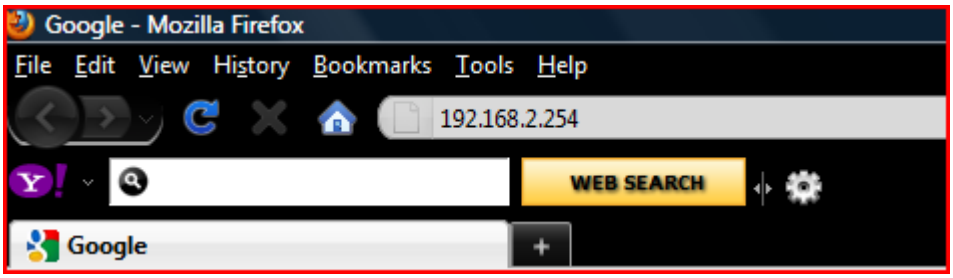


Step 3: Firewalls and antivirus:

These applications must be disabled or removed for configuring the access points (bridges). If the applications are not disabled, they will not let the web interface open up; which is crucial in order to configure the access point.

Step 4: Launching Web Interface:

To open up the web interface, type in the default IP address – 192.168.2.254 into internet explorer or other web browser and press enter.

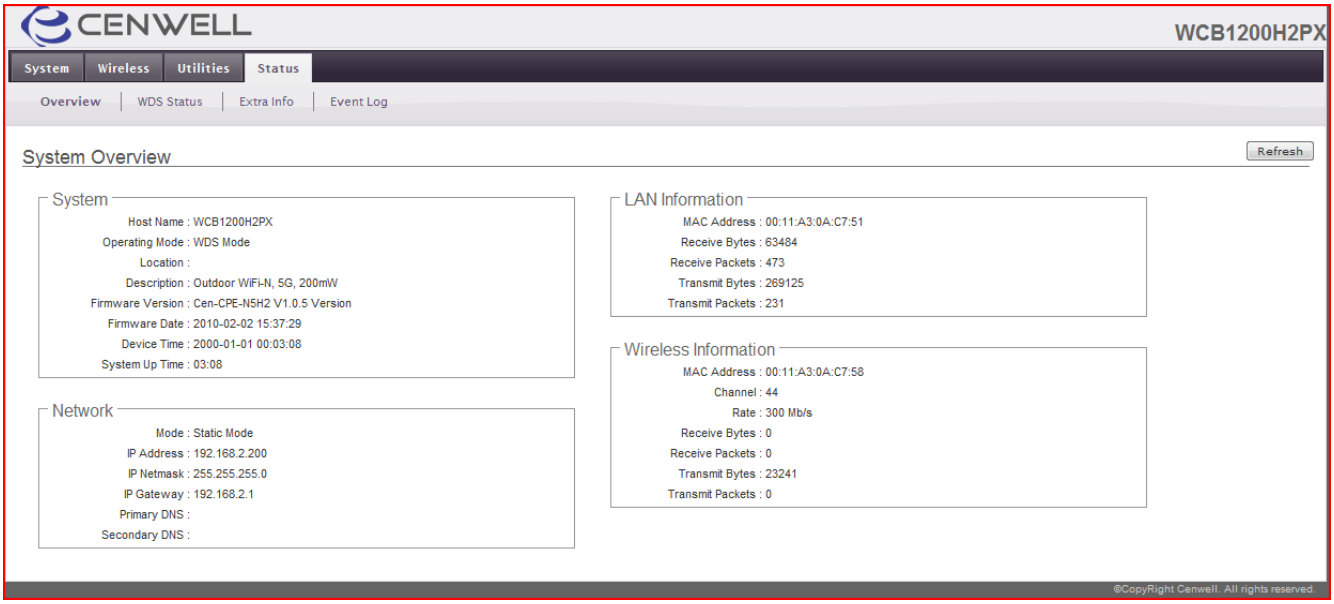


Step 5: Login page

After step4, a login page must appear. If this does not happen, check whether your windows firewall and also antivirus is off. Sometime firewalls are controlled by Norton Internet Security so make sure you turn both off if possible.

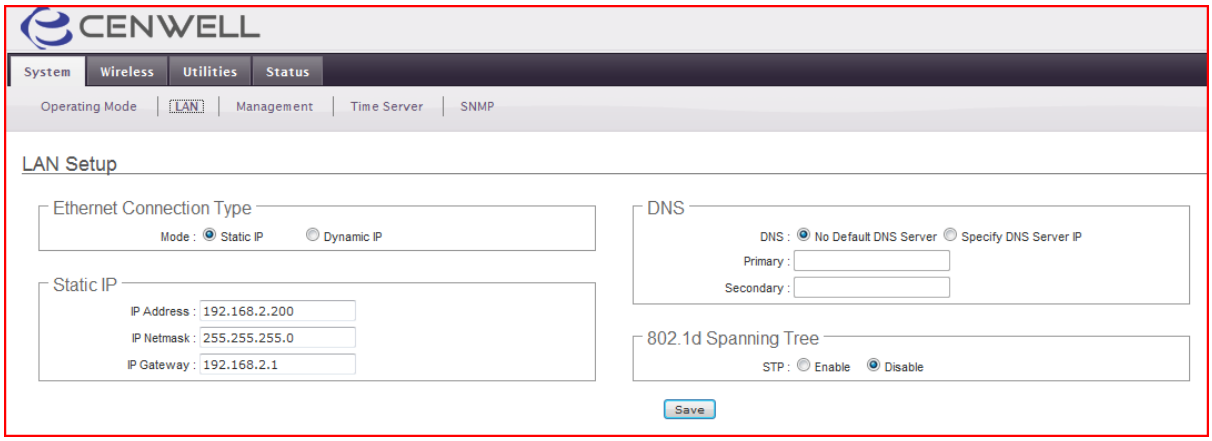
- Once you see this login page, enter:
- Username - “root”
- Password - “default”

Once successfully logged in, the system overview page appears



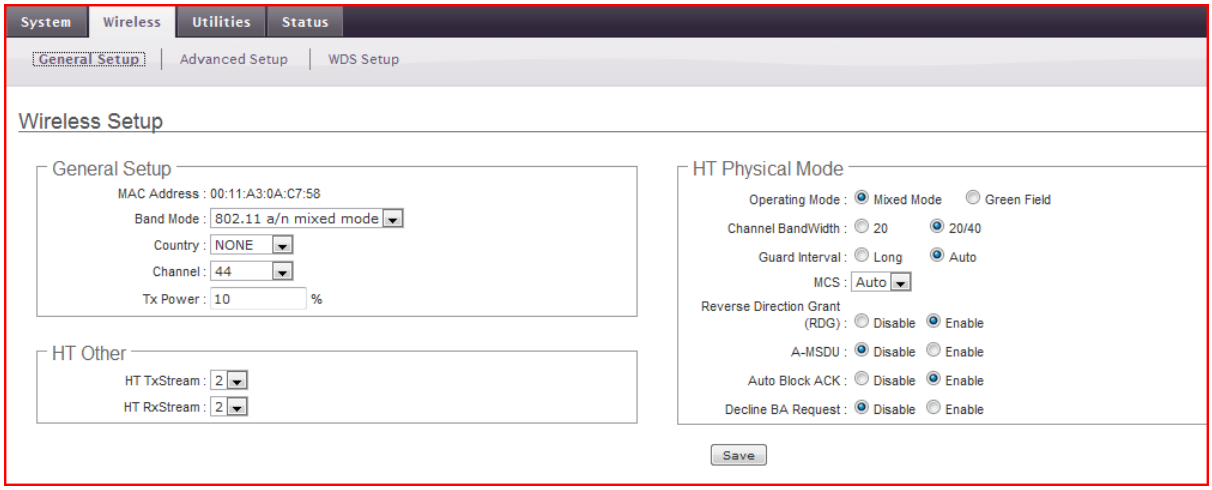
Step 6: System settings

- Click on system → then, click on LAN
- Select static IP → check IP address, IP net mask and gateway (must be: 192.168.2.254, 255.255.255.0, 192.168.2.1) – normally because this device is setup with default IP address, it already displays the static IP address, mask and gateway.
- Select "No default DNS Server"
- Click on save → go to system → click on "save&reboot"

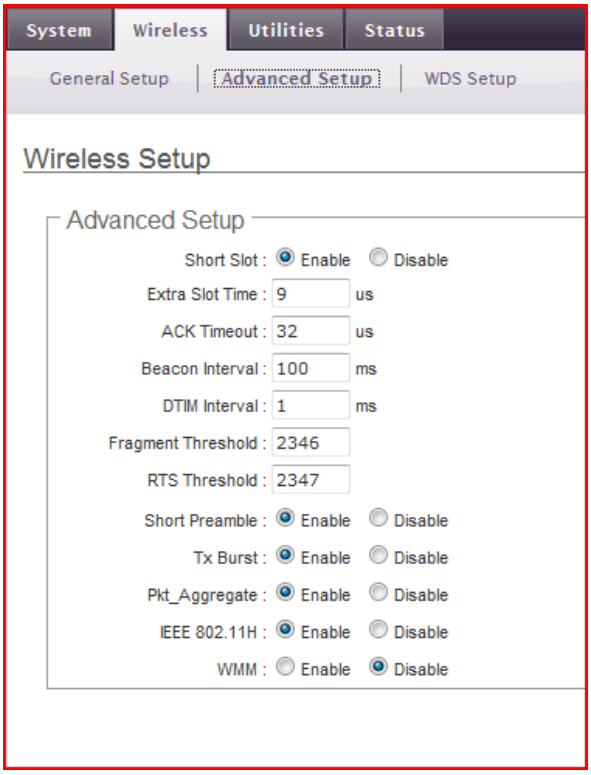


Step 7: Wireless settings

- Click on wireless → General setup and follow the exact format shown below



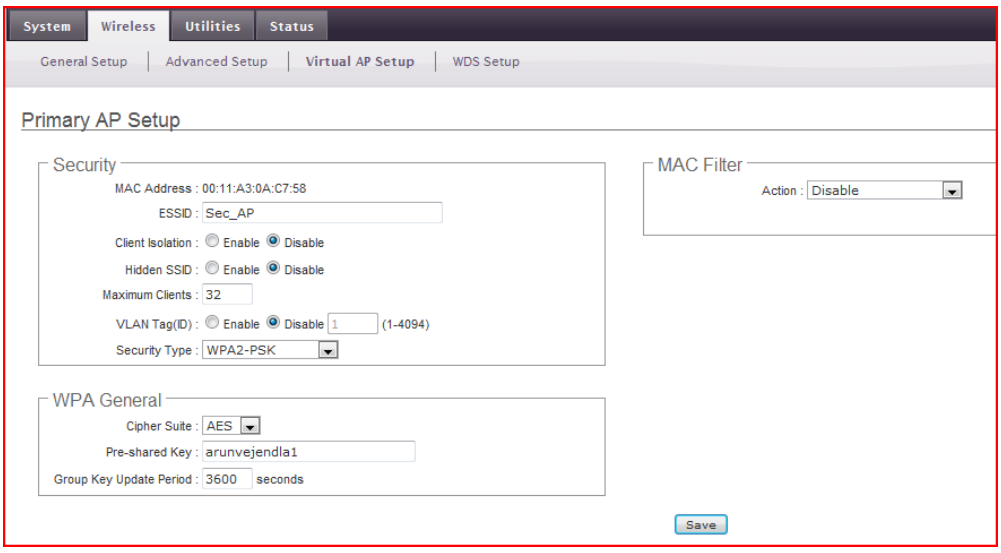
- Click on Advanced Setup → follow the exact format shown below



Step 8: Virtual access point mode

Note: this step is not necessary if communication is required between two bridges - our experiment. This step only allows communication between laptops and the bridge.

- Click system → Click operating mode → select AP mode
- Click wireless →select Virtual AP mode →Click on 'edit' – this brings you to the below interface
- Under security → type your own ESSID (device name), the choose WPA2-PSK security type
- Under WPA general → select AES (advanced security algorithm)→ assign a pre-shared key (passphrase)
- Set MAC Filter as disable
- Rest of the options must be the same as shown below

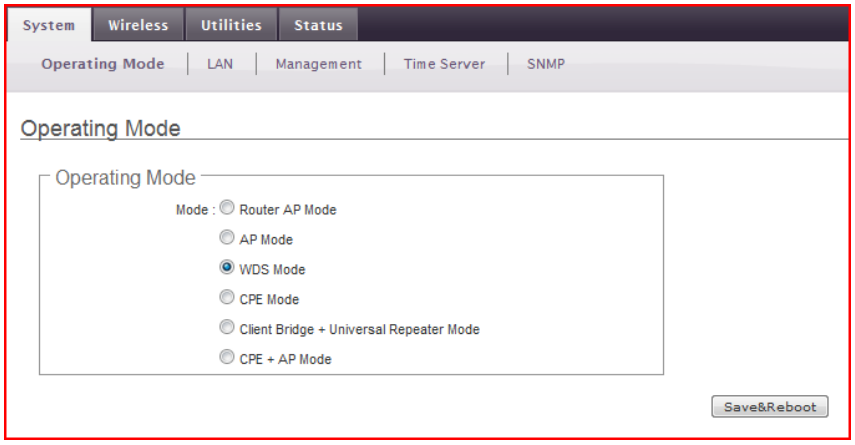


- Save and reboot

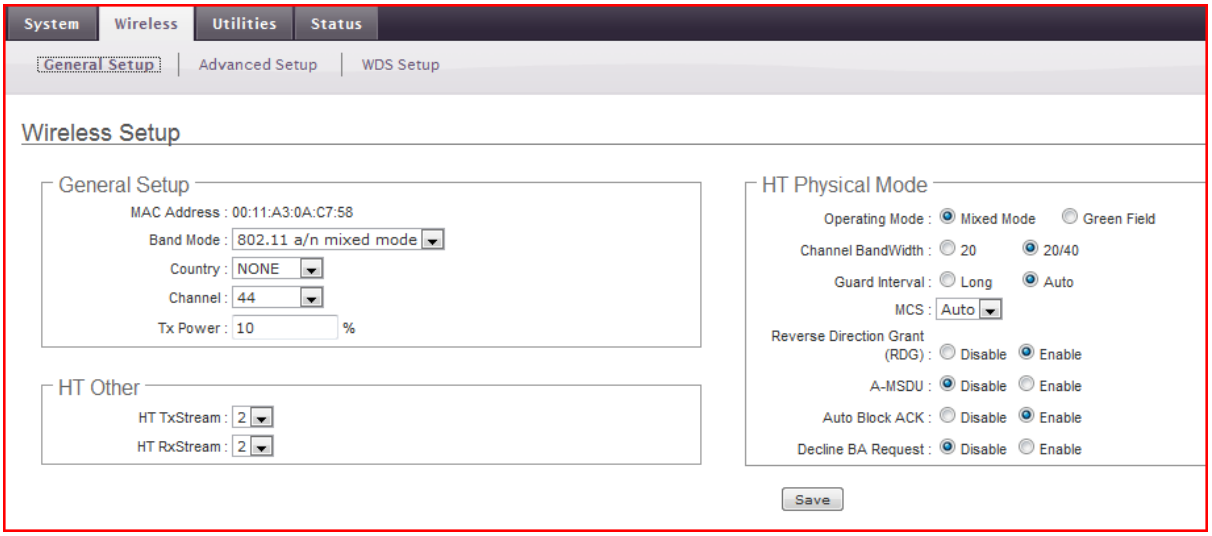
Step 9: Configuring WDS link

This step is crucial for the communication between two laptops

- Make sure you have two bridges for the communication to take place
- Select system → under operating mode → select WDS mode

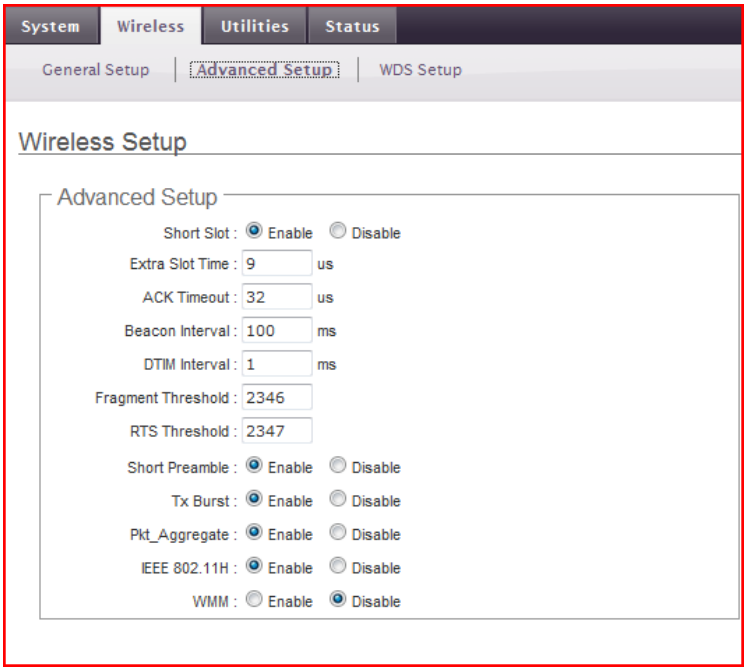


1. Click on wireless → general setup → follow the exact format shown below (the MAC address varies from device to device)

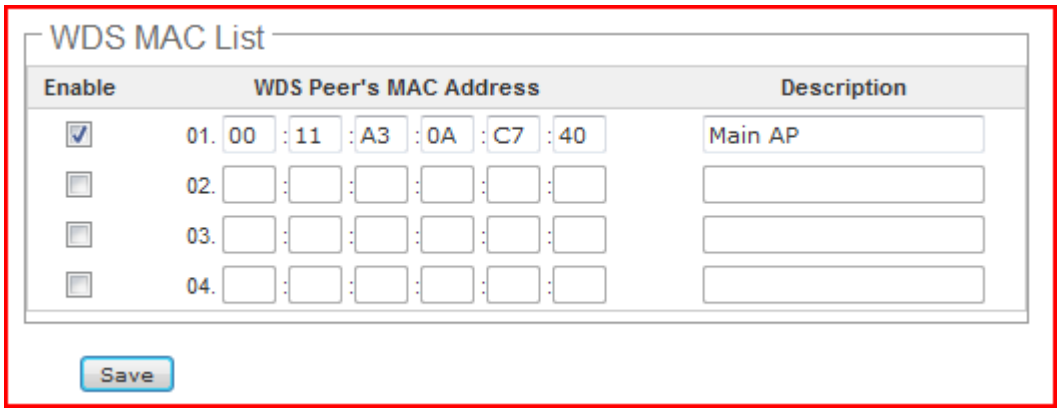


2. Note the MAC address of the remote bridge (present on the device) – not the one you are configuring at the moment

3. Go to Advanced Setup → follow the exact format shown below



4. Click on WDS setup →make sure enable is ticked → Enter remote bridges MAC



5. Click on save → go to system → click on save&reboot button.

Now, the configuration for one access point has been setup, now follow the same procedure with another laptop and remote bridge.

Note: But make sure that this remote bridge's IP address is not the default 192.162.2.254 anymore, we have to change it but within the same range. This is because two devices cannot have the same IP addresses and everything else is the same as shown above.

Trouble Shooting and Technical Support

You may come across many failures while trying to establish the wireless connection between the two bridges (base station and remote station). The below procedures or steps may help you get through most of the obstacles. This trouble shooting notes is written according to my experience. So when you have a poor link or a link does not show up or communication between the two devices is not possible, perform:

1. First, check whether the firewall and antivirus is off. It is possible that the firewall may be blocking the device or the connection. If you can, change the antivirus and the firewall setting to allow the device to connect to your laptop.

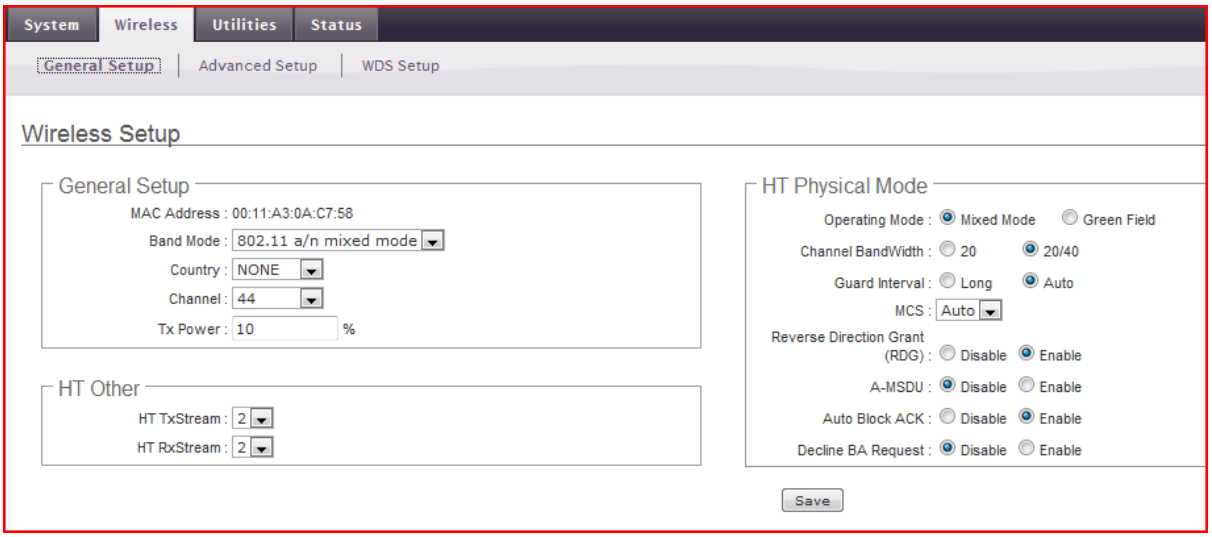
2. Follow the OSI model hierarchy procedure:

    a) First to make sure whether we have a connection in the first place, ping the devices using command prompt. Example, ping base station to the remote using command 'ping *ip address'.* Once the ping fails
    b) Start of by checking the physical layer. So check the connections (cat5 cables) whether they sit in the correct slots (data in goes into laptops Ethernet port, data out plugs into the bridge)
    c) Check physical status of the bridge. The bridge has three lights, check whether the power LED is green, check whether the Ethernet LED is on and finally make that the WLAN led is on. If none of these LED's are green (stationary or flashing time to time), then the WDS connection is not possible. Make sure you do step (a)
    d) Now check the MAC addresses. It is very important that you configure both bridges with the correct MAC address. If the communication has to take place, each bridge must be configured with the remote bridge's MAC address. If the MAC address is not present on the device or if you are not sure what the MAC address is; reset the device and this enables the default MAC address 192.168.2.254. Go to general setup under wireless if connection is present.
    e) If all the above procedures have failed, this step should be enough to bring the connection 'up'. Now check the IP addresses under the TCP/IP setting of LAN; for all the devices, make sure that they have a valid IP address. For example, the laptops – whether they lie in the same range as the 192.168.2.**x**. Then try to ping the laptops. In the worst cases, the static address you assign to a laptop may disappear; in this case go back to the LAN TCP/IP setting and reassign one again.

3. This is the Alignment procedure. To achieve the maximum throughput values, a better signal strength is needed. Make sure that both the devices are facing each other as accurately as possible. This should solve the problem but in worst cases possible interference should also be taken care of if the device is running in the same

frequency band as the other sources. Various procedures can be used to improve the alignment accuracy and to decrease interference; for example, laser pointers, moving away from possible obstructions, station the devices on high grounds.

CAP 501-5D Wireless Setup Terms and Definitions



Wireless → General Setup:

MAC Address: Shows the MAC address of the wireless access point (address of the current device you are configuring)

Band Mode: Shows the available wireless band. 802.11a and 802.11a/n mixed mode bands are available. CAP501-5D uses the standard 802.11n, so use the 802.11a/n band

Country: Select the country code from the list of four options (US, ETSI, JP, NONE)

Channel: The ranges differ from country to country according to the regulations imposed by each of them. The below table shows the countries and their valid channels

Country	Channel
US	36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161
ETSI	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140
JP	36, 40, 44, 48
NONE	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 149, 153, 157, 161

Tx Power: Used to adjust the output power of the device to get appropriate coverage for your wireless network. The default value is 10%; but the range available for selection is between 1 – 100 (unit %)

HT Tx Stream and HT Rx Steam: HT means high throughput and by default the value is 2; when 802.11a standard is selected, these two HT and Rx stream's will be hidden

Operating mode: The default mode is the 'mixed mode', where each packet is sent with a preamble that is compatible with the standards 802.11a/g. This mode allows the receiving system can decode both the mixed mode and legacy packets. In the 'green field' mode, high throughput packets are sent to the destination without the legacy compatible part

Channel Bandwidth: The 20/40 is the better option out of the two because this option increases the throughput and there is more room for transmission; which means you have better quality signal and you can send and receive data at a higher rate(good quality signal = higher bandwidth). The 20 option communicates with 20 MHz bandwidth**.** 20/40 communicates with 40 MHz bandwidth.

Guard Interval: The auto option increases the throughput but also can increase the error rate in some devices and their installation due to the radio frequency reflections

MCS: Represents the transmission rate and as we have talked above, the auto option here allows the fastest transmission rate and the table below shows the MCS indexes

MCS Intex	Modulation	Data Rate (Mb/s)			
		Channel Bandwidth = 20		Channel Bandwidth = 40	
		Long Guard Interval	Short Guard Interval	Long Guard Interval	Short Guard Interval
0	BPSK	6.5	7.2	13.5	15.0
1	QPSK	13.0	14.4	27.0	30.0
2	QPSK	19.5	21.7	40.5	45.0
3	16-QAM	26.0	28.9	54.0	60.0
4	16-QAM	39.0	43.3	81.0	90.0
5	64-QAM	52.0	57.8	108.0	120.0
6	64-QAM	58.5	65.0	121.5	135.0

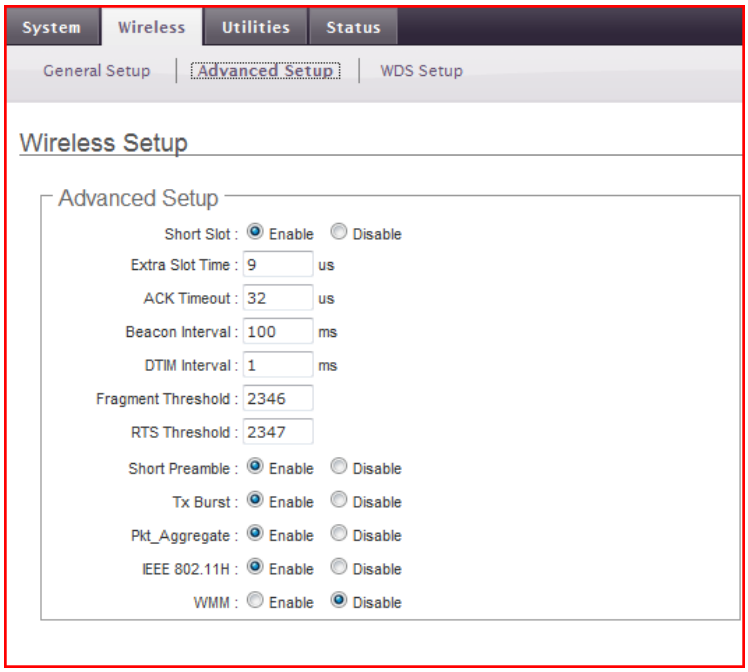
Reverse Direction Grant (RDG): RDG speeds up the data transmission between the sender, receiver and their wireless access point/router by letting the wireless systems to send/receive data simultaneously without contending for shared medium. RDG also allows one wireless system to send/receive burst frames consecutively.

A-MSDU (Aggregated Mac service data unit): enable option allows aggregation for multiple Mac service data units but the disable option disables this aggregation

Auto Block ACK: The default mode is 'enabled'. This is a speed up method for IEEE802.11n standard; which helps not to respond to each sent data (ACK), but only to respond to block unit.

Decline BA Request: enable or disable the BA request

Wireless → Advanced Setup:



Short slot: This tells us that 802.11g network is using a short slot time because there are no legacy (802.11b) stations present.

Extra Slot time: the amount of time the sender waits once a collision occurs before retransmitting the packet to the destination. The smaller the slot time, the smaller the back off period (2x slot time) therefore increases throughput

ACK Timeout: This tell us that the system must receive an acknowledge from the receiver for the data that is sent within the set given; the time set should not be too short because it does takes time for a system to send a packet and also receive an acknowledgement from the receiver. This must be considered carefully

Beacon Interval: available range is between 20 and 1024. Access points send a beacon (50byte frame) and this beacon is broadcasted to every other station and it mentions the AP's SSID, signal strength and data rate to let the others on the network to know about the existence of this AP. Large intervals add latency. Latency is the delay between each packet that is sent to the destination; in this case it means less beacons are sent over some time. The smaller the interval, the more beacons are sent therefore it is good for connecting and roaming

DTM Interval (delivery traffic indication message): available range is between 1 and 255. This tells the wireless devices that support power saving mode to wake up and receive a multicast frame and the interval is the count of number of beacons that must occur before an access point sends the frames. The higher the interval, the more power saving is enabled but decreases the throughput.

Fragment Threshold: available range is between 256 and 2346. Big data packets are divided into smaller packets are sent to the destination and each of these small packets is marked for reassembly at the destination device. The smaller the frame, the collisions and corruptions are much lower so higher threshold increases the throughput

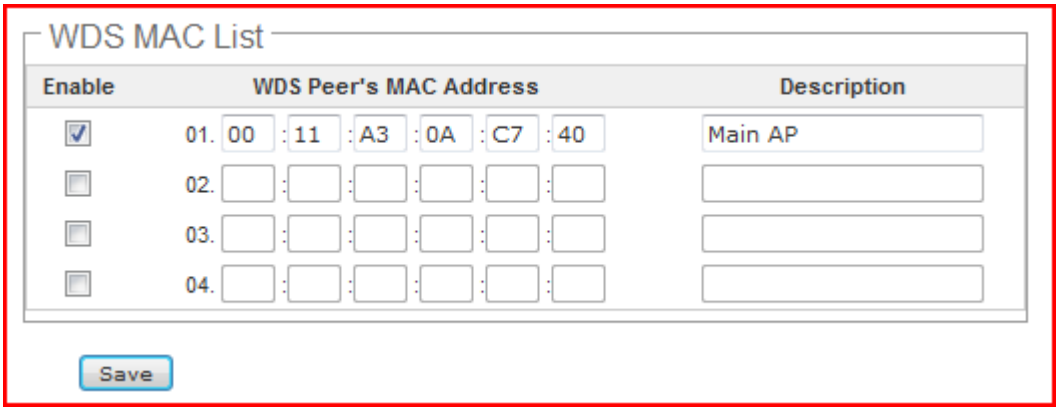
RTS Threshold: available range is between 1 and 2347. This helps up reduce the number of collisions that occur in wireless transmissions especially from the hidden nodes

Short Preamble: by default it is enabled. A preamble is used to signal that sequences of data packets are arriving. Short preamble provides 72bit synchronization field which helps reduce the overhead and hence providing transmission efficiency. The disable option uses the long 128 bit synchronization field

Tx Burst: This is where an access point send frames in bursts (a lot of frames than normal) but collision detection is not involved. You have more throughput because of the burst of data but interference from other devise must be considered

Pkt Aggregate: aggregates multiple packets into a single frame therefore increasing efficiency of transmissions

Wireless → WDS Setup:



Security type (not shown): four security options such as disable, WEP, TKIP and AES are available.

- WEP: enter 5 to 13 ASCII or 10 to 25 HEX format key
- TKIP: enter 8 to 63 ASCII or 64 HEX format key
- AES: enter 8 to 63 ASCII or 64 HEX format key

WDS MAC List:

- Enable: to create a WDS connection or link with another device (another Access point)
- WDS Peer's MAC Address: enter the MAC address of the remote access point (not the access point you are currently configuring)so that this device can talk to the remote device