DIR-878

FAQ _ Ver.1.1

HW Version	Firmware Version
A1	1.00

Written By

Customer Service Department I of DHQ on July 24th, 2017

Contents

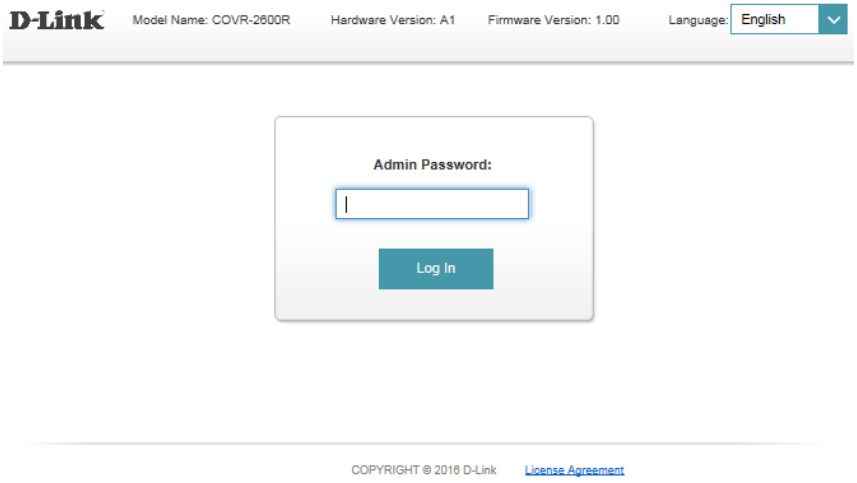
Device Setup/Installation

Q1: How do I login to my router?

Verify that your computer is connected to the router either via an Ethernet cable or wireless connection, then follow the steps below:

Step 1: Open your web browser and enter the IP address of the router into the address bar (not in google). The default IP is 192.168.0.1, or using the link: **http://dlinkrouter.local**.

Step 2: You should be taken to a D-Link login page. By default, the username is admin and no password is required.



Note: Administering a Router over Wi-Fi:

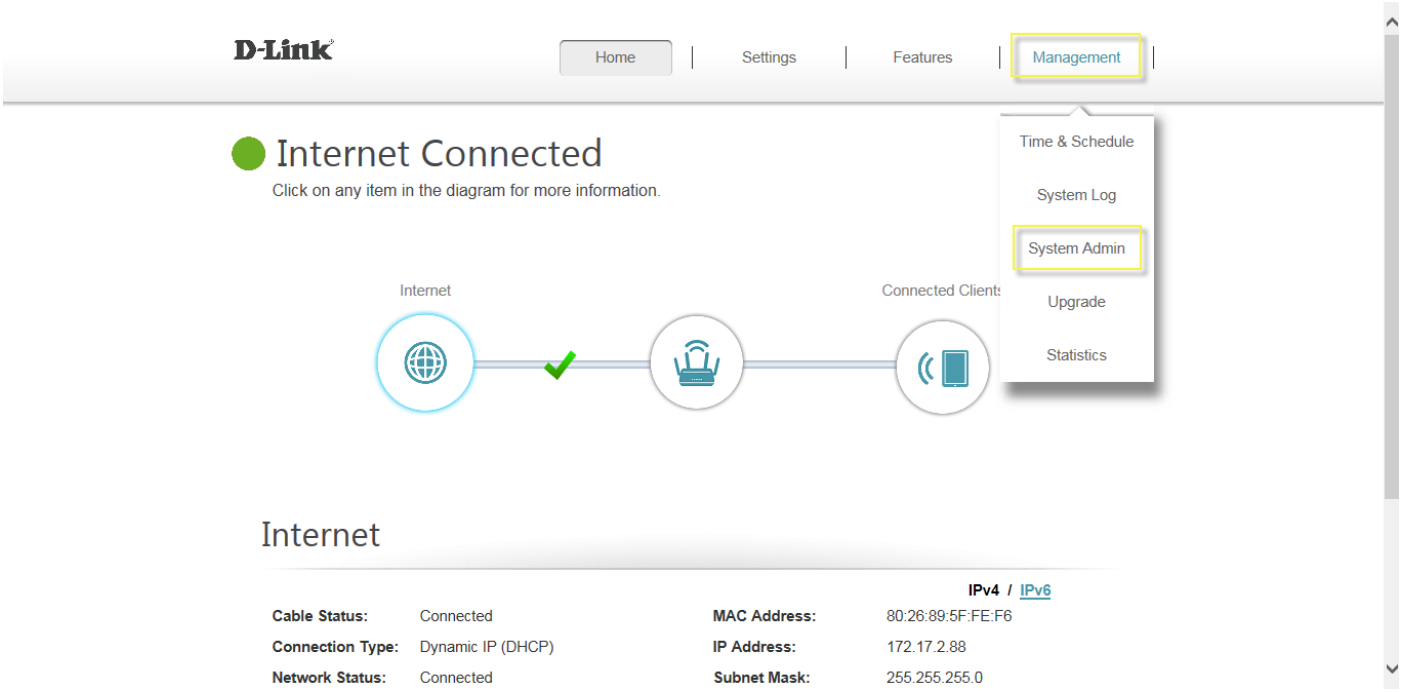
Setting up a router for the first time is best done over a wired connection so that your connection isn't dropped if the security or wireless settings are changed the process. However, it can be done over wireless too.

When connecting to a router via Wi-Fi, keep the computer close to the router - in the same room if necessary - to avoid connection drops due to interference or weak wireless signals.

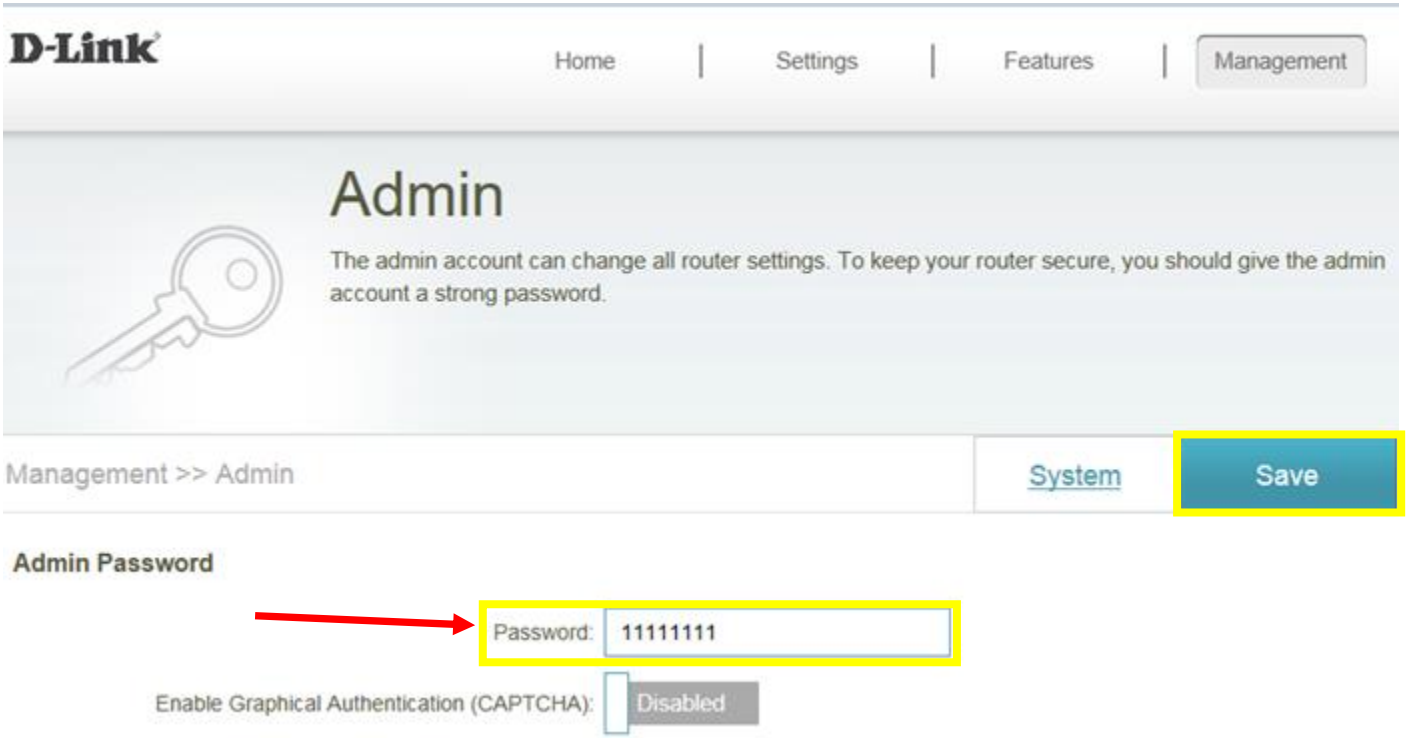
Q2: How do I change the login password?

Please launch your browser and enter http://dlinkrouter.local or http://192.168.0.1 into the address bar. Then login and follow the steps below:

Step 1: Click **Management** -> **System Admin**



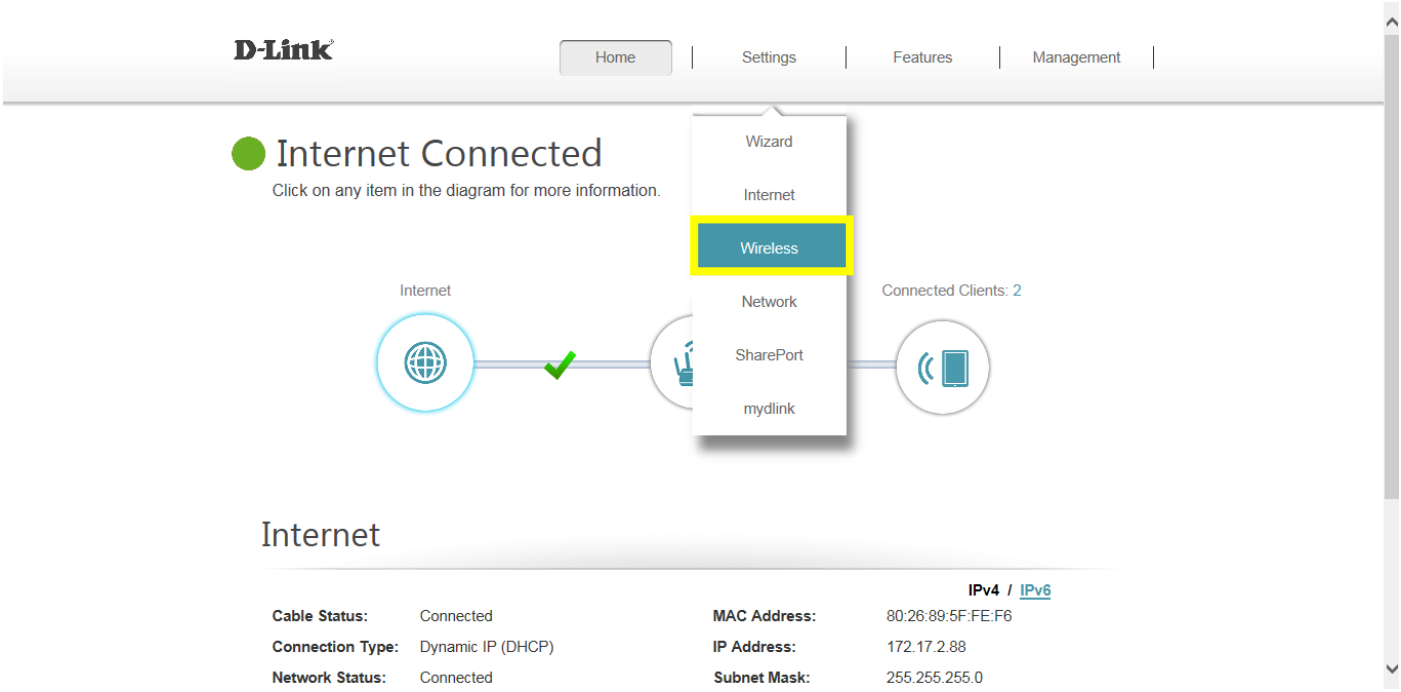
Step 2: Fill in the password you'd like to set and click **Save**:



Q3: How do I set up and secure my wireless connection?

Please launch your browser and enter http://dlinkrouter.local or http://192.168.0.1 into the address bar. Then login and follow the steps below:

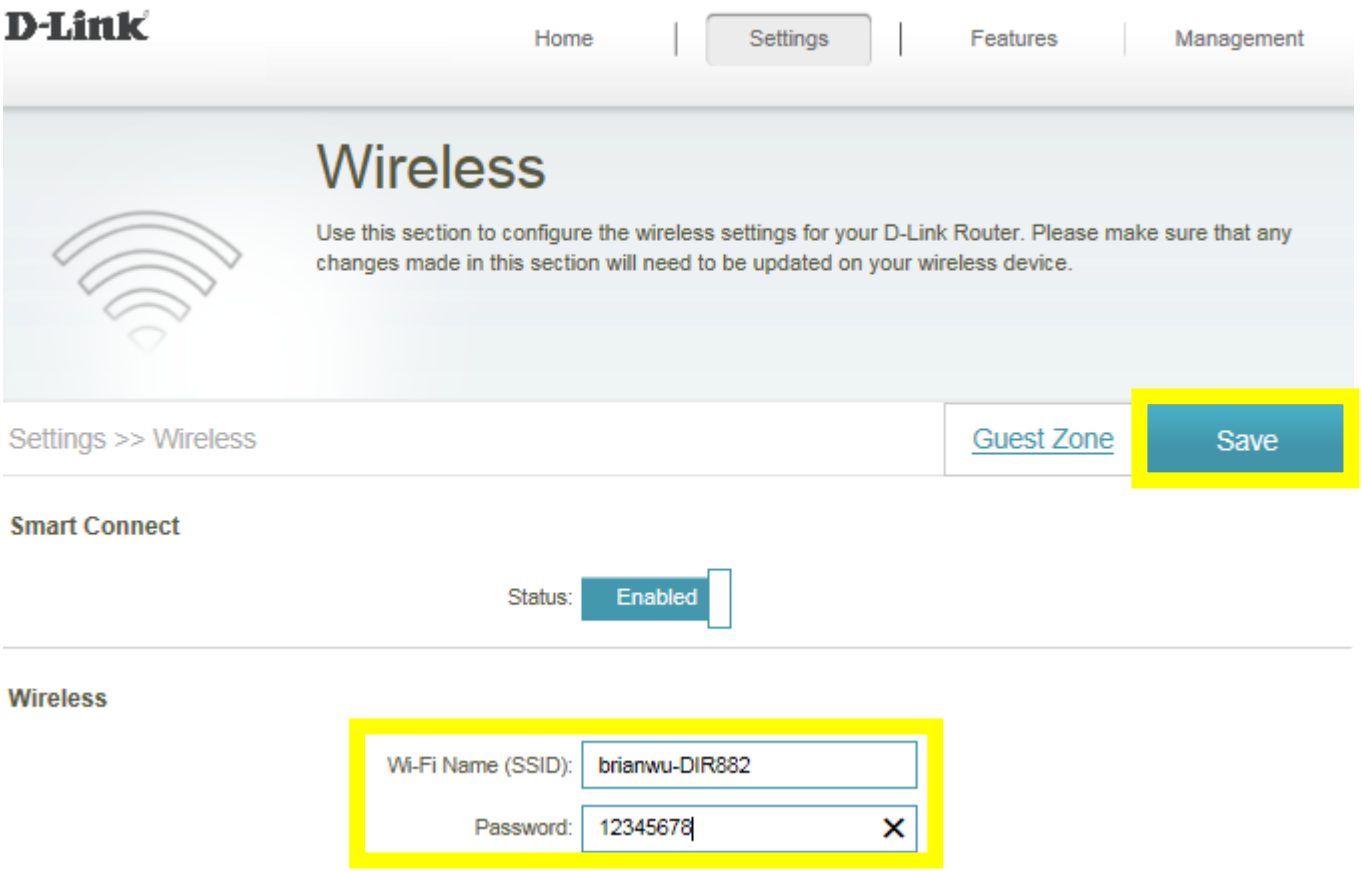
Step 1: Click **Settings** -> **Wireless**



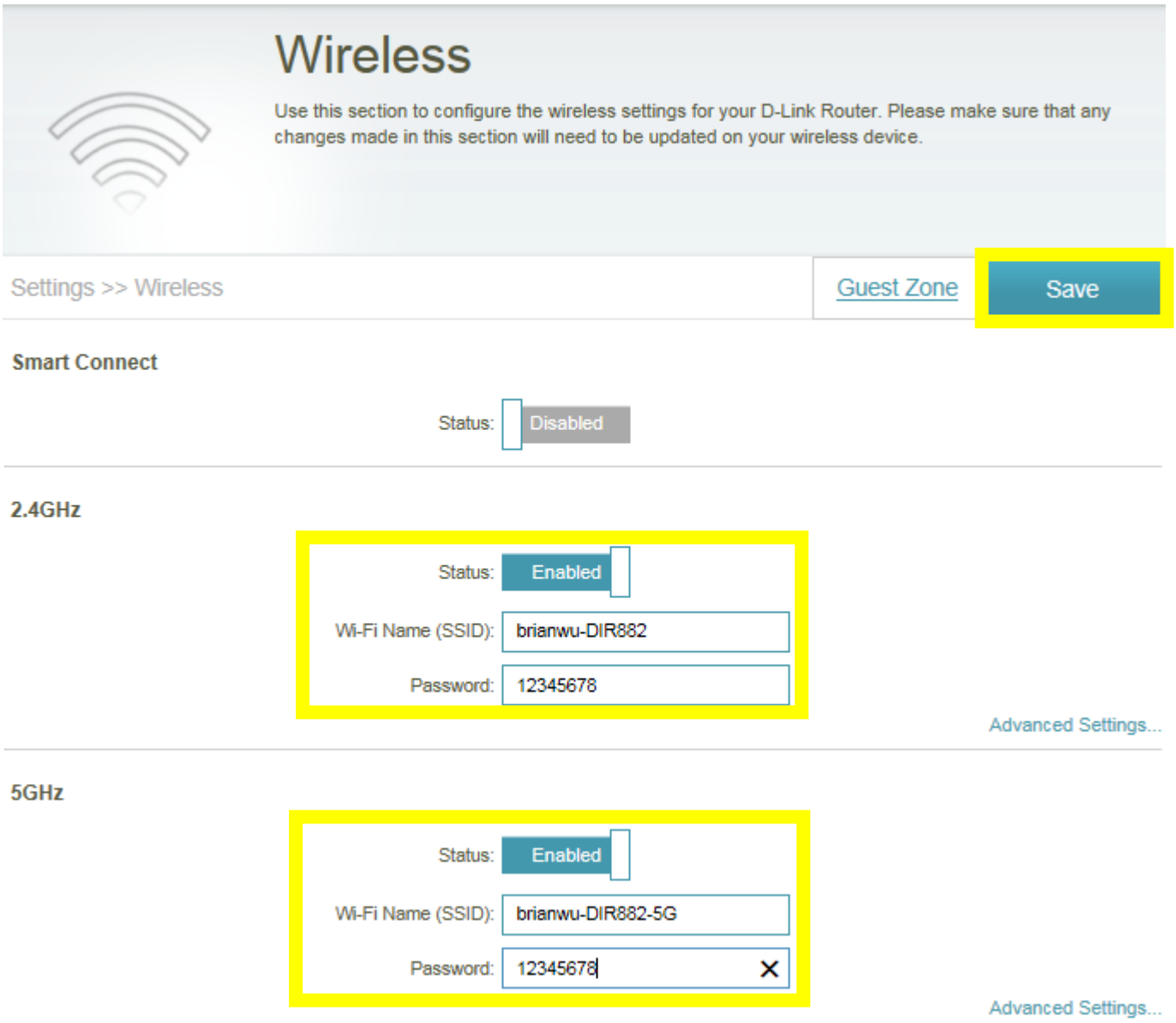
Step 2: In the wireless **Wi-Fi name (SSID)** field (for both the 2.4 and 5GHz sections), erase the default name (dlink-xxxxx) and enter a unique wireless network name (This is the name you will see when scanning for wireless networks on your computer/wireless device).

In the password field, remove the default password and enter a new one of your choice. (Must be a minimum of 8 characters), then click **Save.**

(1) Smart Connect enabled:



(2) Smart Connect disabled:



Note: Please check Q3 as the link below about the detailed information about Smart Connect:

What is smart connect?

General Settings

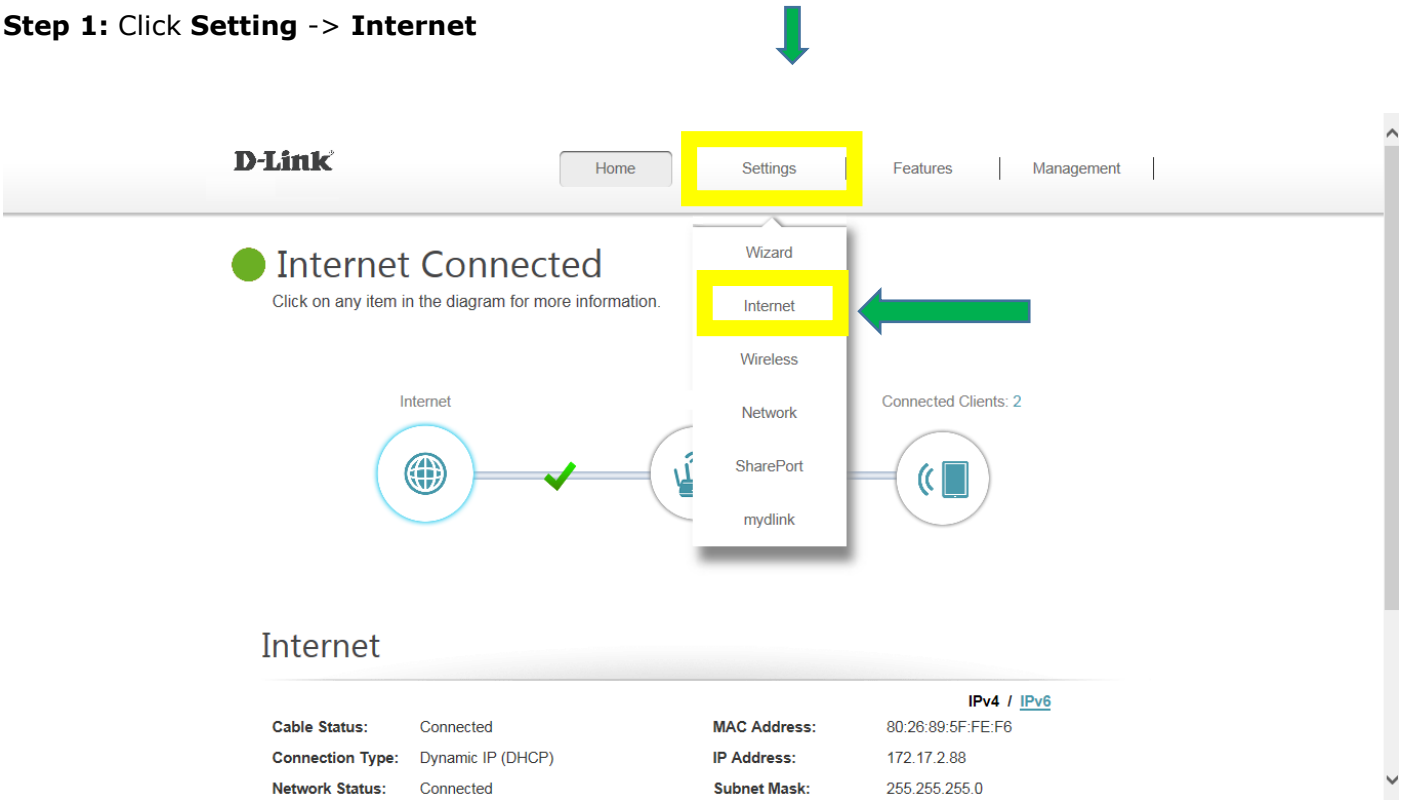
Q4: How to clone my PC MAC address to the router?

Few cable internet providers requires you to clone PC Mac address in order to go online through the router.

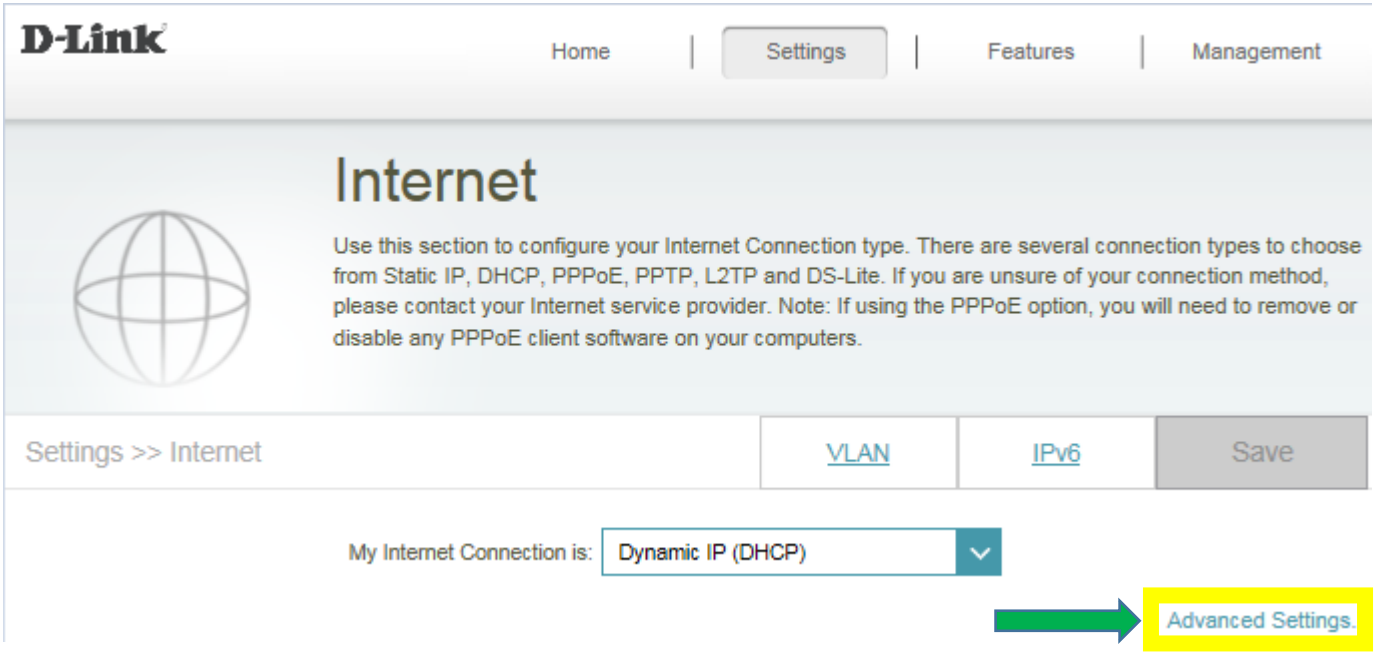
Note: It is recommended to clone MAC address from last computer which was able to go online when connected to modem.

Please launch your browser and enter http://dlinkrouter.local or http://192.168.0.1 into the address bar. Then login and follow the steps below:

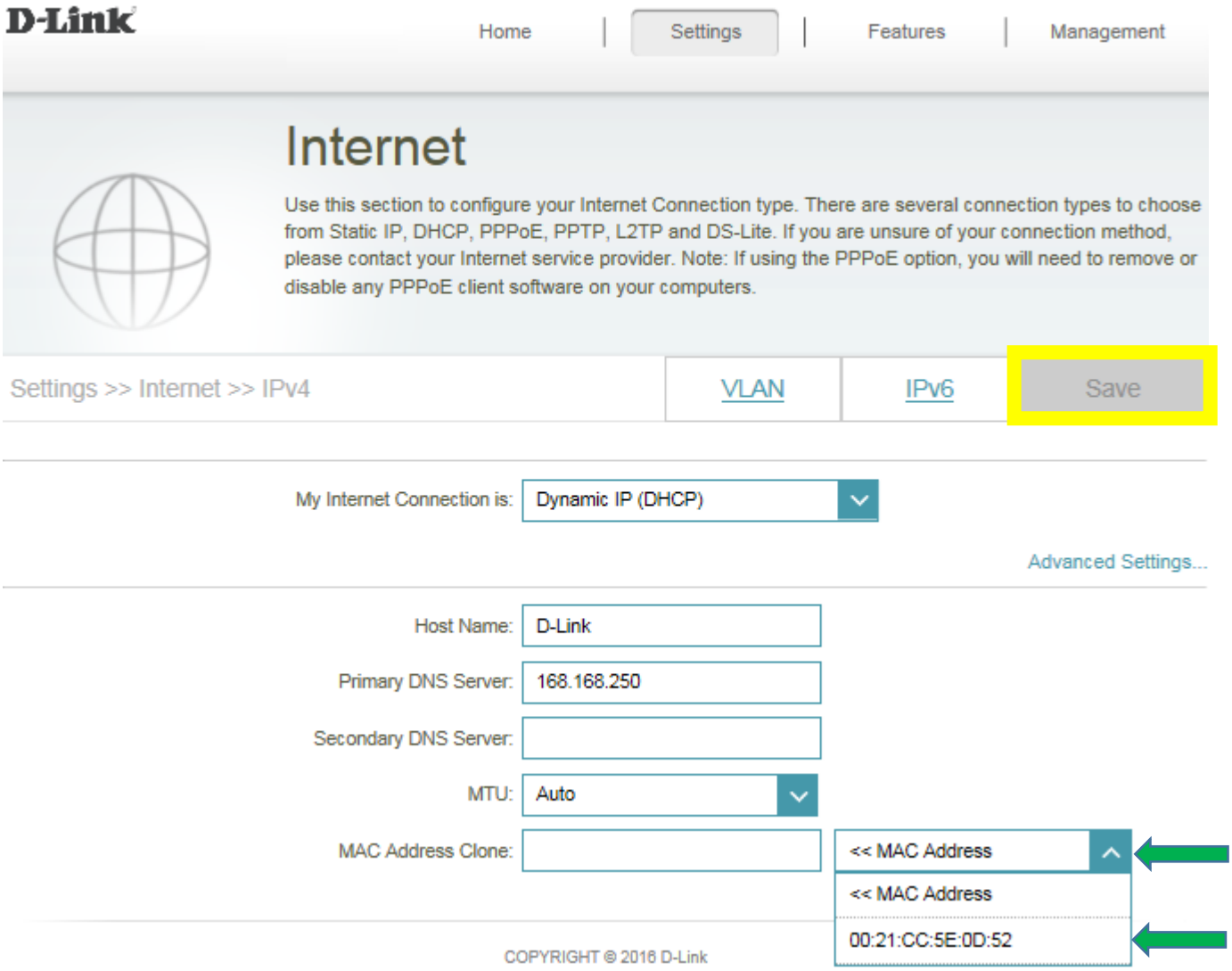
Step 1: Click **Setting** -> **Internet**



Step 2: Click **Advanced Setting**



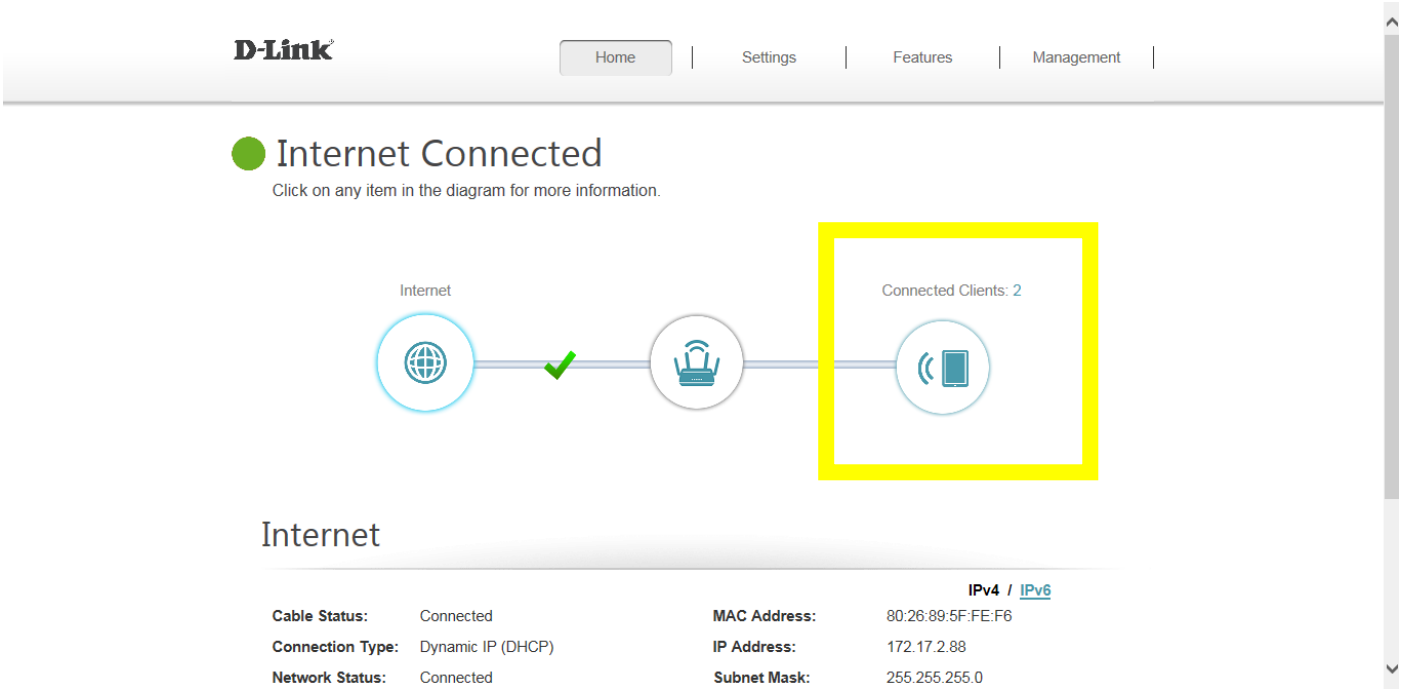
Step 3: Find **Mac address clone** field, then select one Mac address from the drop-down menu and click **Save**



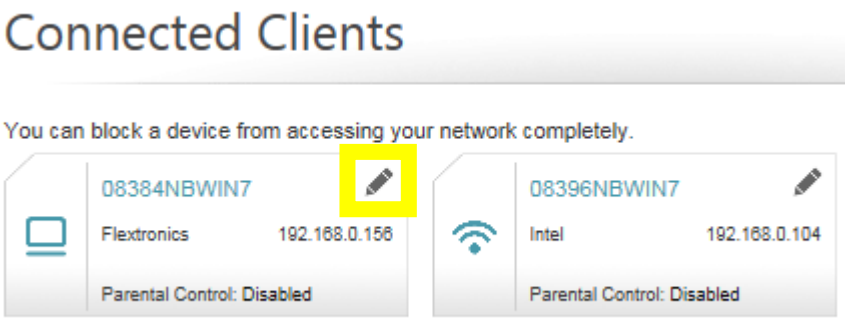
Q5: How do I configure DHCP reservation?

Please launch your browser and enter http://dlinkrouter.local or http://192.168.0.1 into the address bar. Then login and follow the steps below:

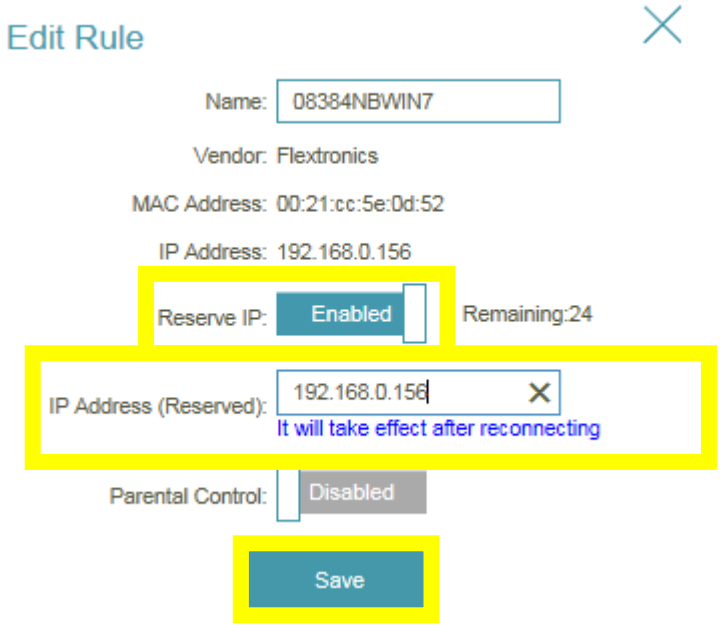
Step 1: Click **Connected Clients** from the Home Tab:



Step 2: Click the **Pencil Icon** next to your client you'd like to adjust:



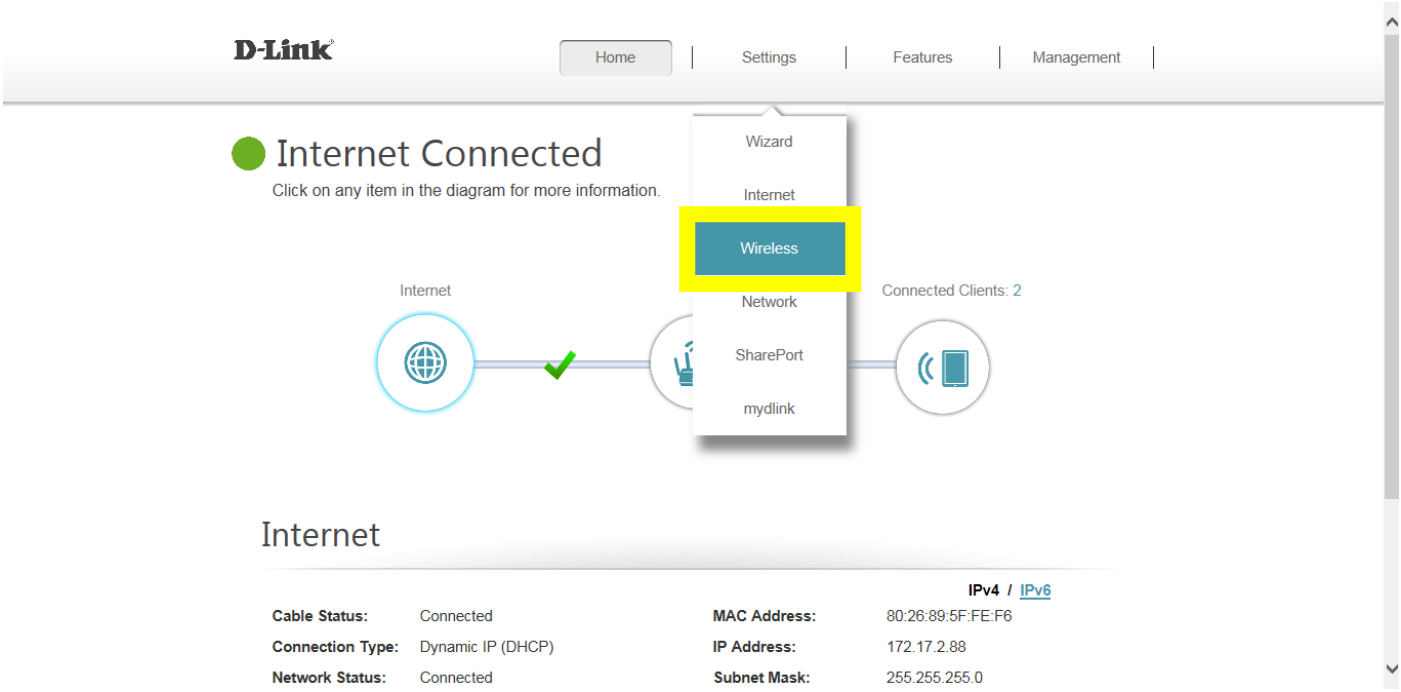
Step 3: Click **Reserve IP** to Enable, and fill in the reserved IP address, then click **Save**.



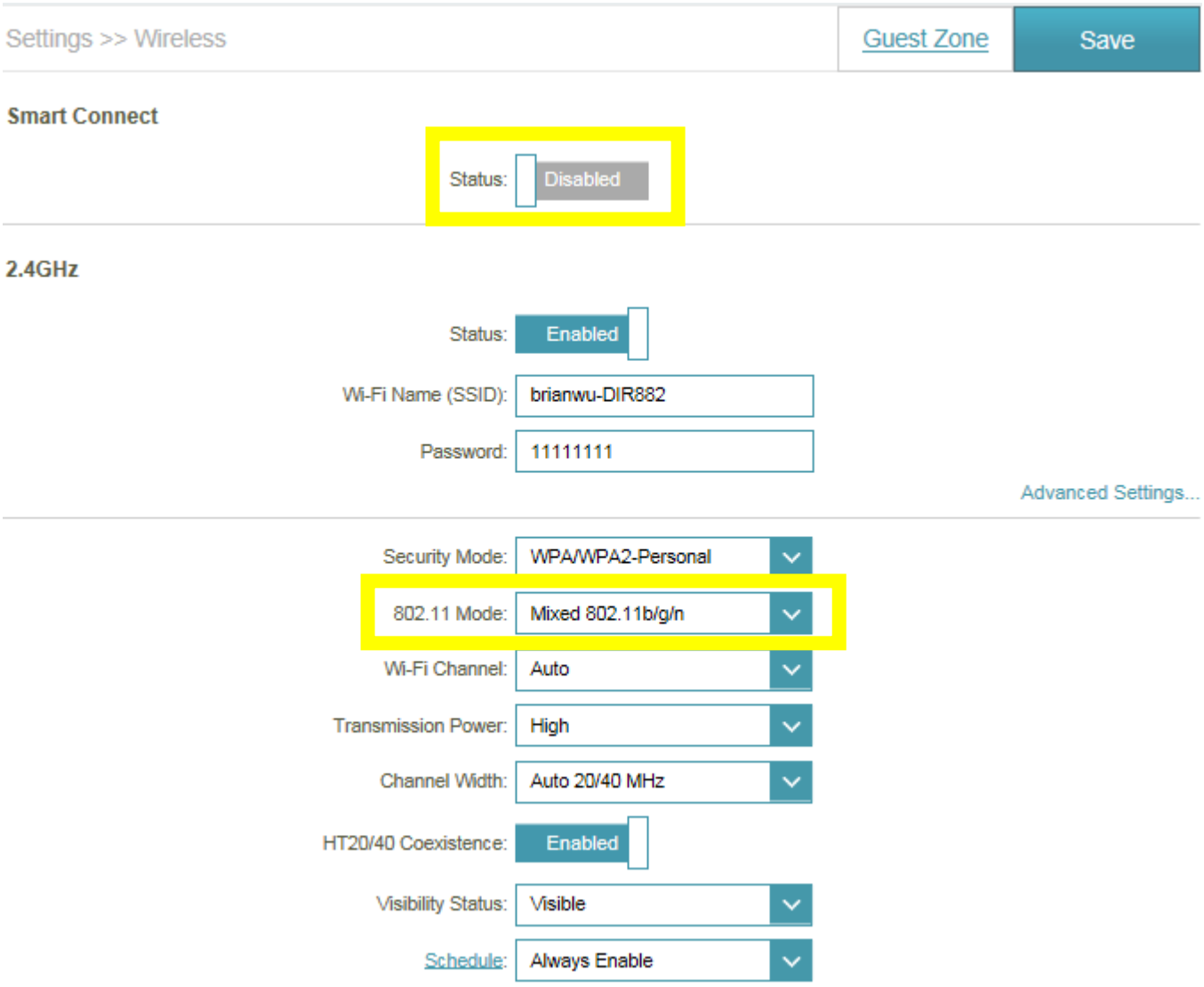
Q6: How do I configure 802.11 mode on my router?

Please launch your browser and enter http://dlinkrouter.local or http://192.168.0.1 into the address bar. Then login and follow the steps below:

Step 1: Click **Settings** -> **Wireless**



Step 2: Disable **Smart Connect**, and select the 802.11 mode for 2.4G/5G band:



5GHz

Status: Enabled

Wi-Fi Name (SSID): brianwu-DIR882

Password: 11111111

Advanced Settings...

Security Mode: WPA/WPA2-Personal

802.11 Mode: Mixed 802.11a/n/ac

Wi-Fi Channel: Auto

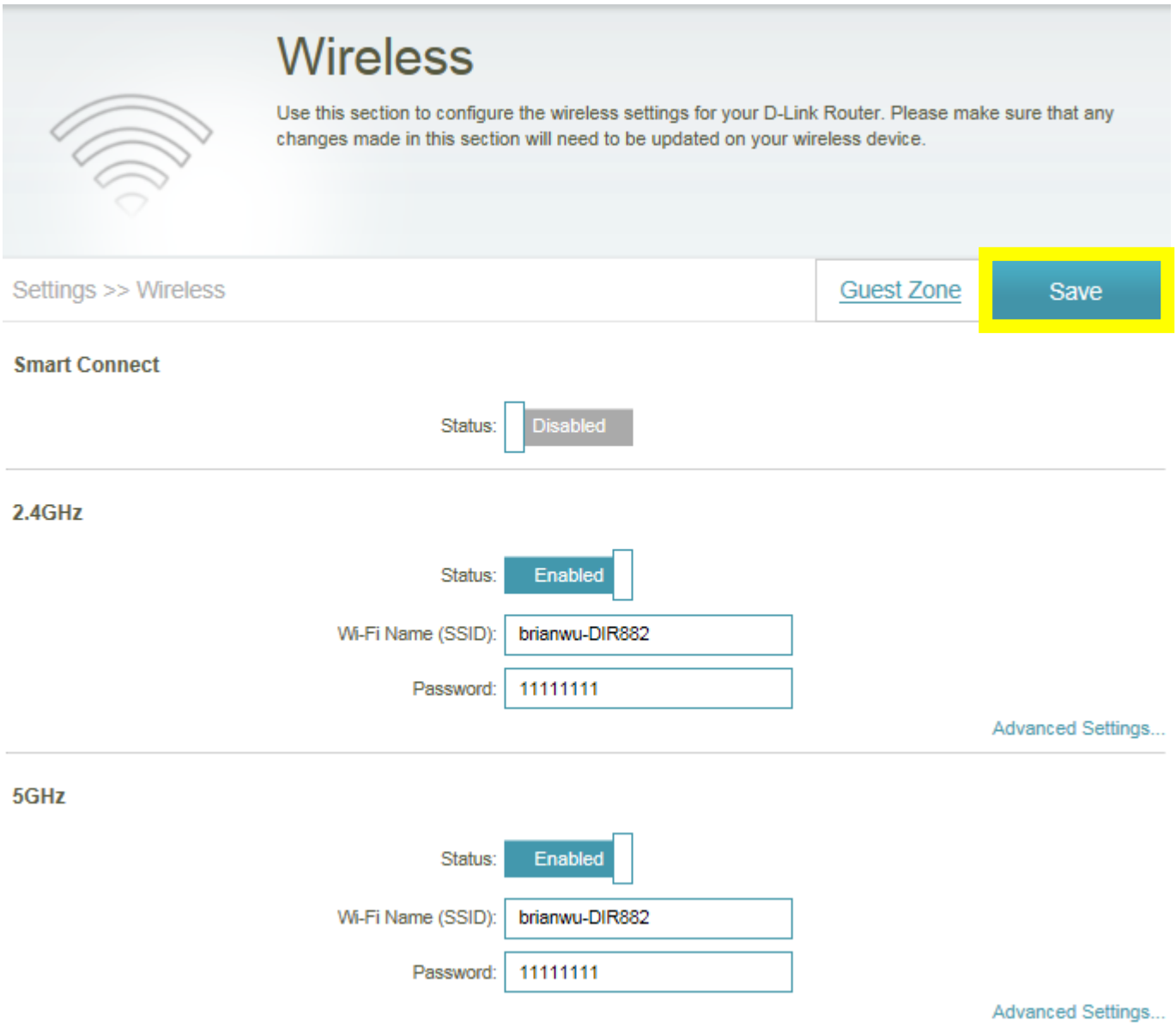
Transmission Power: High

Channel Width: Auto 20/40/80 MHz

Visibility Status: Visible

Schedule: Always Enable

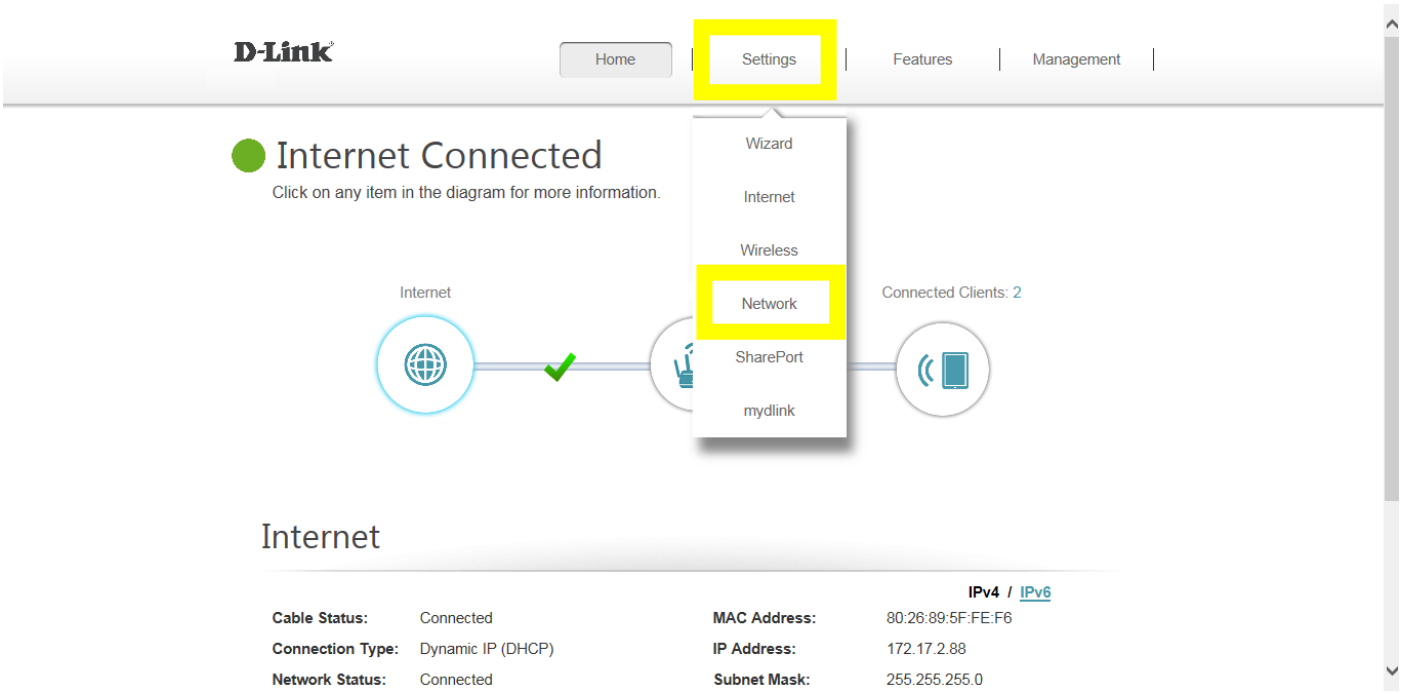
Step 3: Click **Save** to save your configuration.



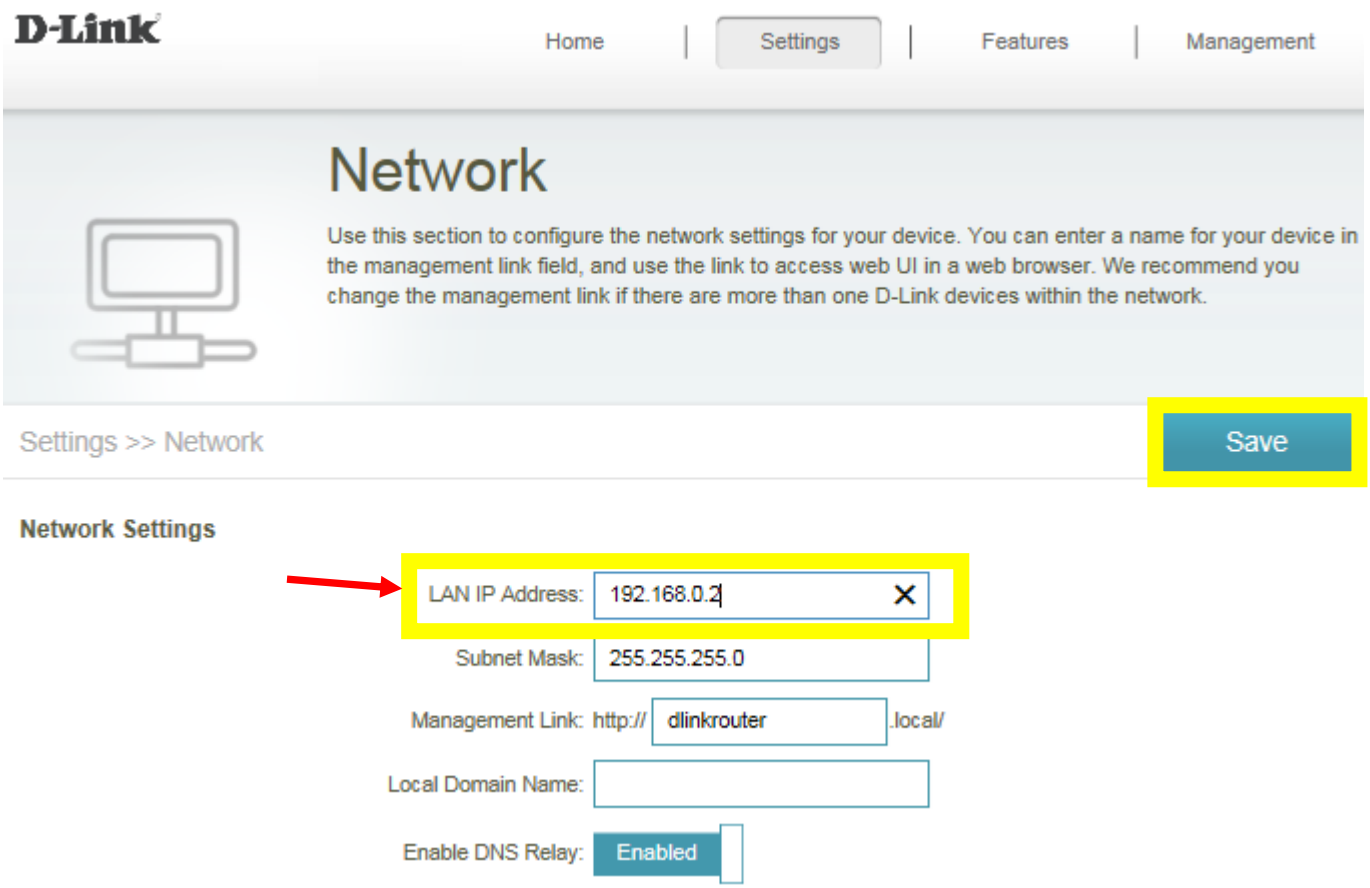
Q7: How do I change the router's IP address?

Please launch your browser and enter http://dlinkrouter.local or http://192.168.0.1 into the address bar. Then login and follow the steps below:

Step 1: Click **Settings** -> **Network**



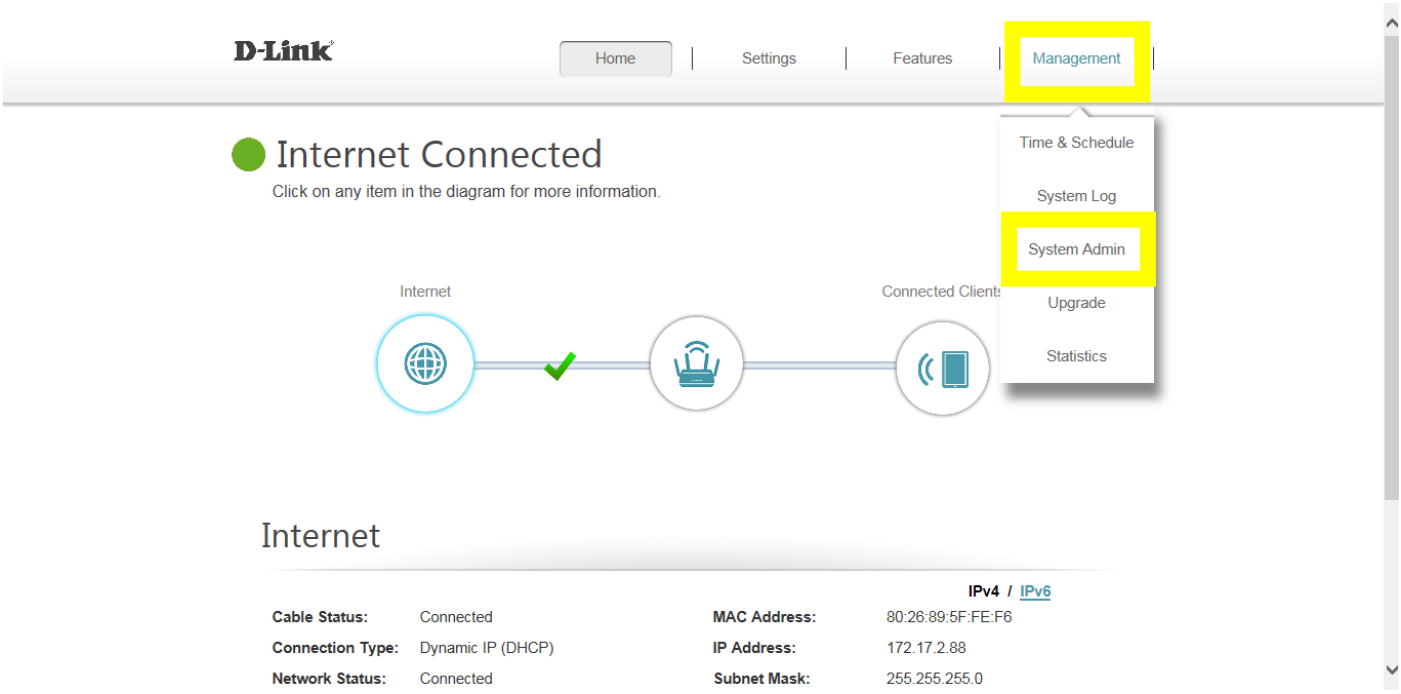
Step 2: Change the IP address as needed under **Network Setting**, and click **Save**



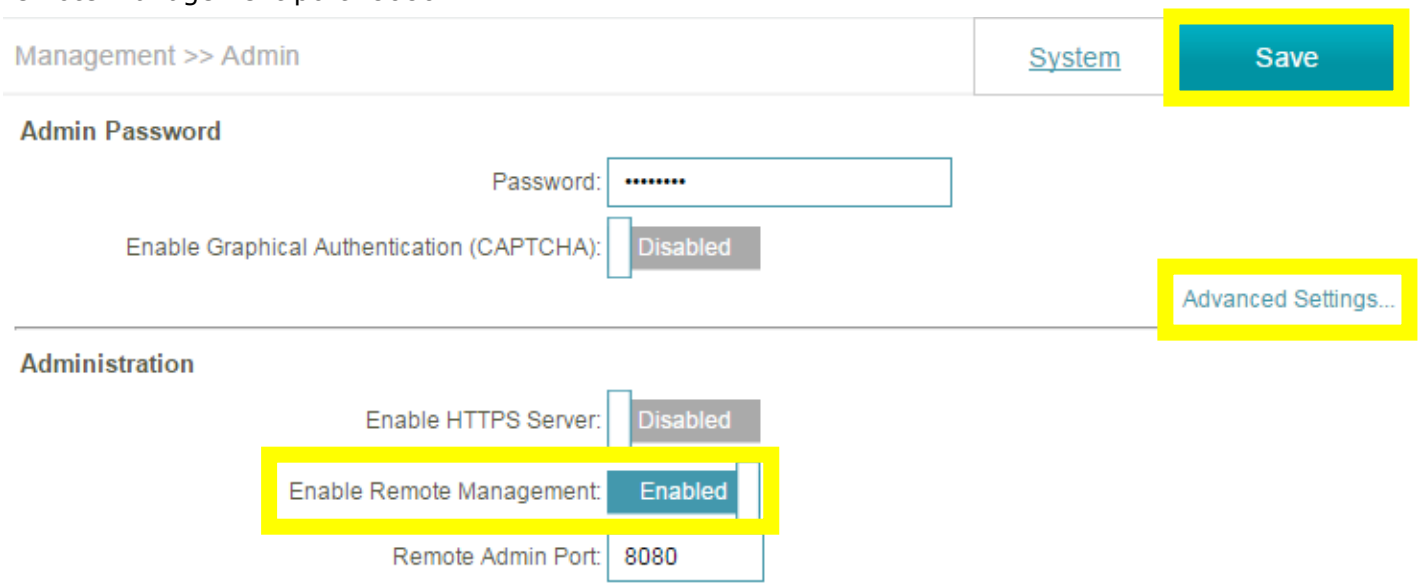
Q8: How do I enable remote management for my router?

Please launch your browser and enter http://dlinkrouter.local or http://192.168.0.1 into the address bar. Then login and follow the steps below:

Step 1: Click **Management -> System Admin**

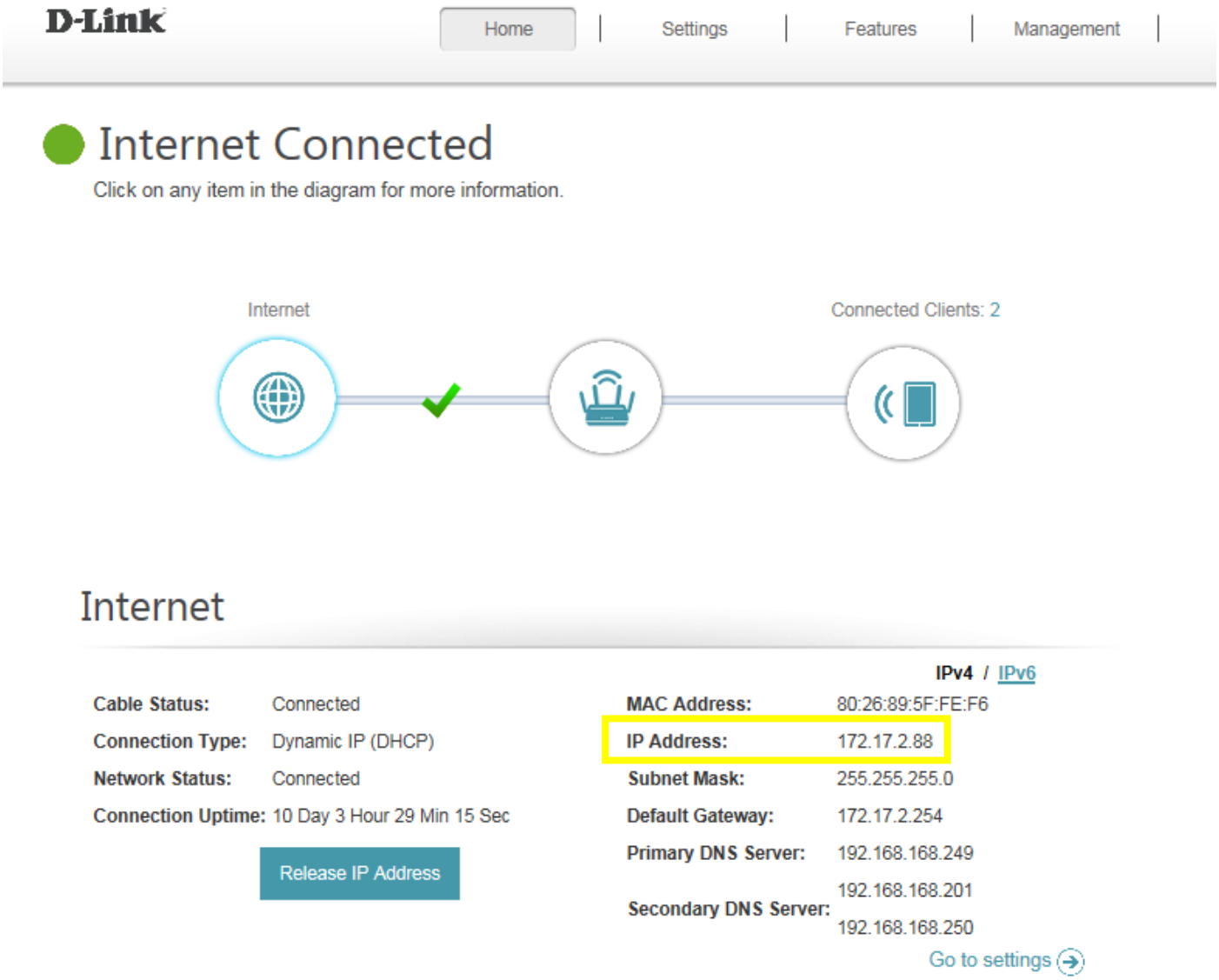


Step 2: Click **Advanced Settings**, and enable Remote Management, then click **Save**. The default remote management port: 8080.



Note: To access your router remotely, from a web browser enter: http://<your WAN IP>:8080.
e.g. http://172.17.2.74:8080

You can find your WAN IP by clicking on the Home tab. It will be displayed under the Internet Section



Q9: What model support bridge mode?

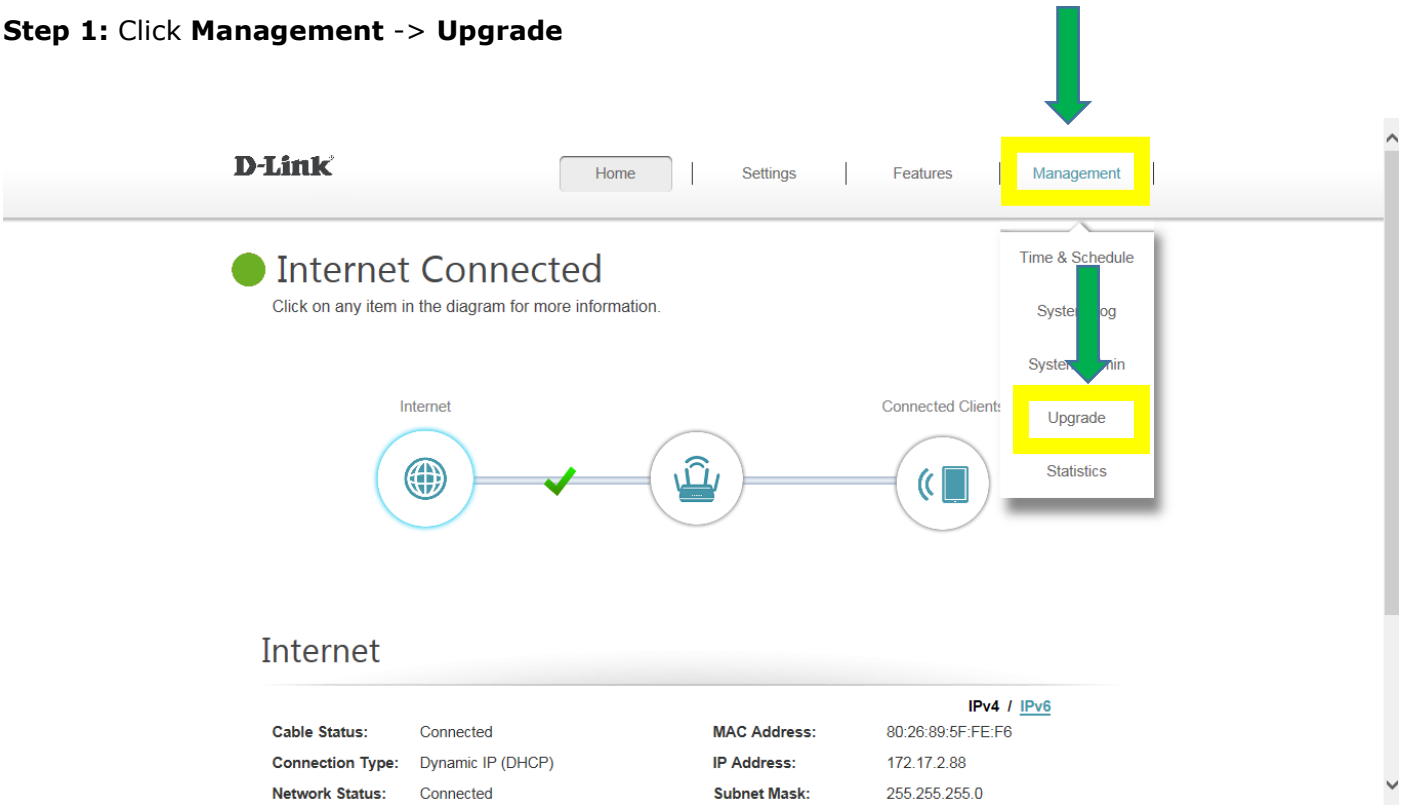
Currently, the models support bridge model are: DIR-895L, DIR-885L, DIR-880L, DIR-868L, DIR-865L, DIR-605L.

Firmware Upgrade/Checking

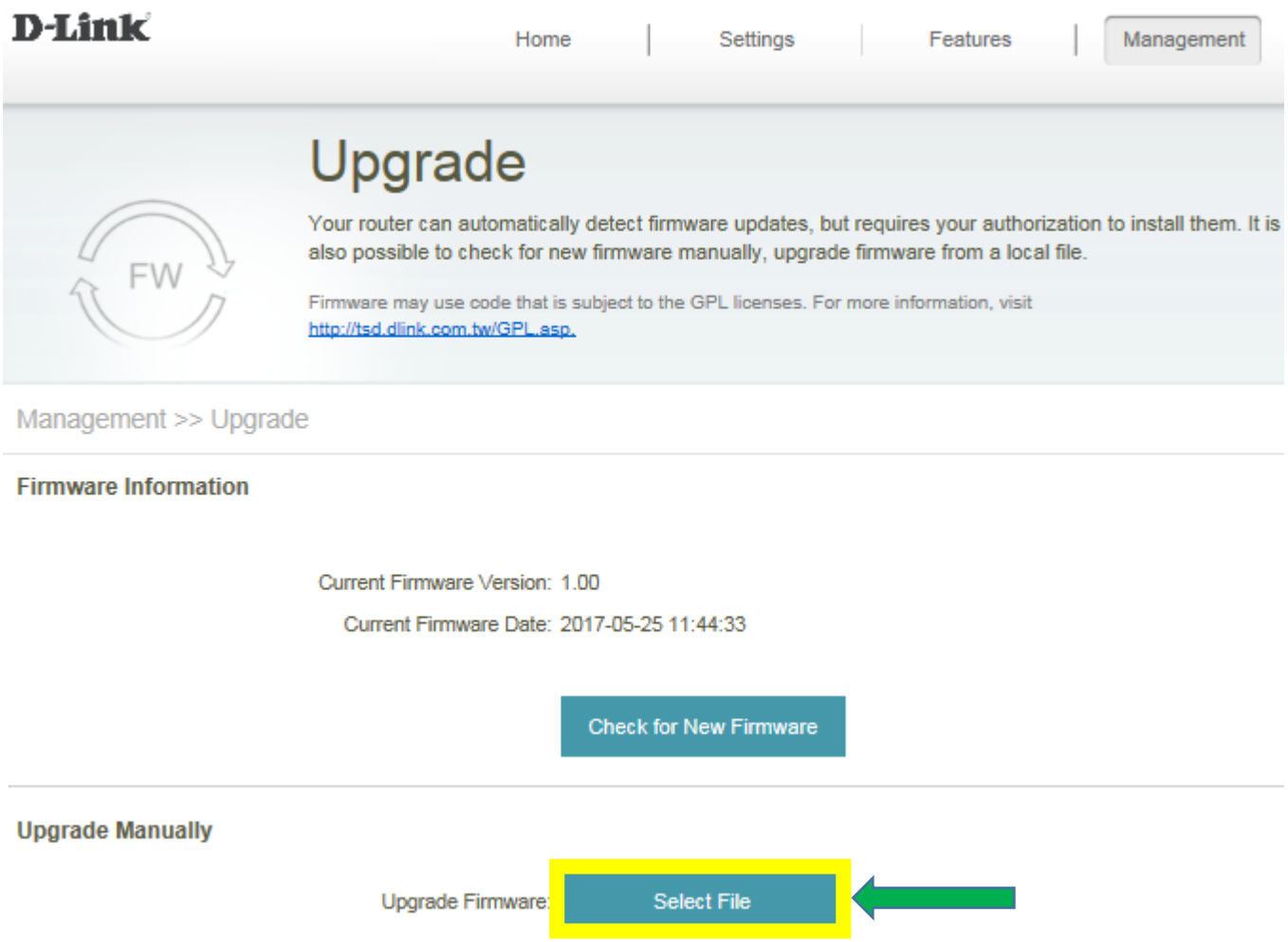
Q10: How to upgrade firmware for router?

Please launch your browser and enter http://dlinkrouter.local or http://192.168.0.1 into the address bar. Then login and follow the steps below:

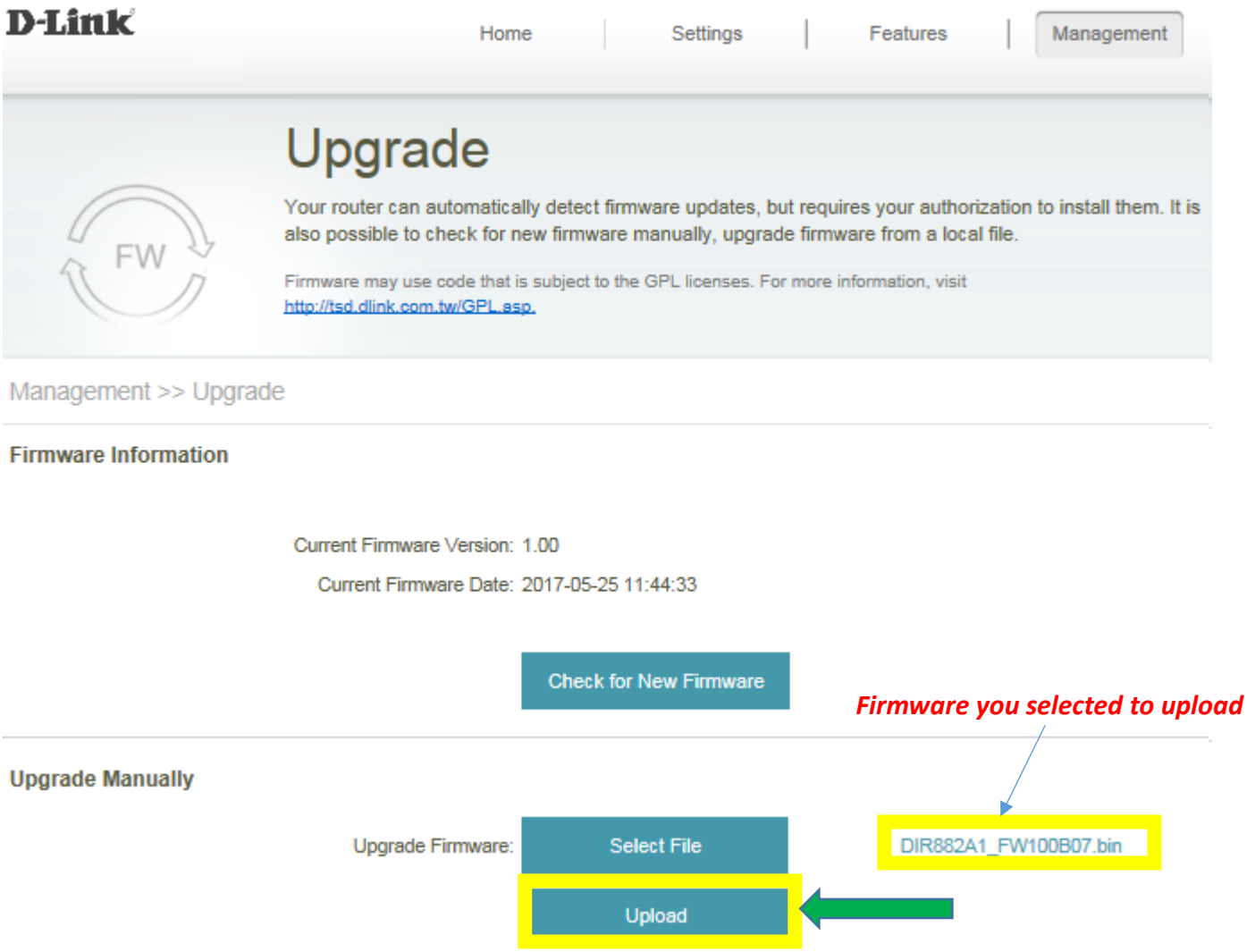
Step 1: Click **Management** -> **Upgrade**



Step 2: Click **Select File** to browse for the firmware

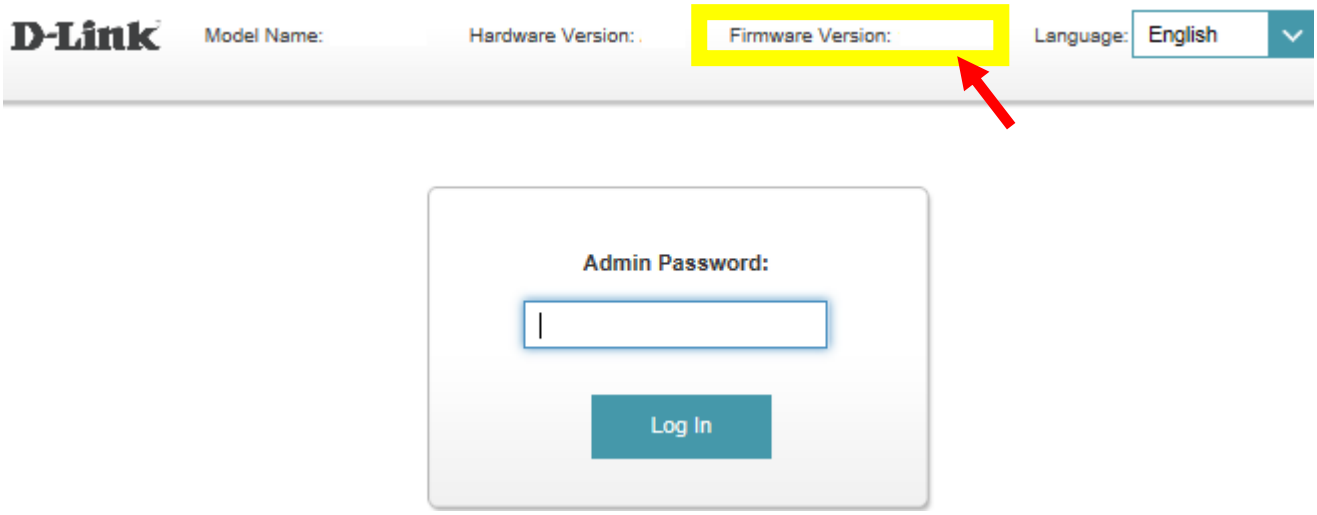


Step 3: Click **Upload**



Q11: How to check firmware version of router?

Please launch your browser and enter http://dlinkrouter.local or http://192.168.0.1 into the address bar. The firmware version can be found at the top right hand corner of the page.



Factory Reset

Q12: How to reset my router to factory default setting?

Example: If you forget the password of your router's configuration interface, you can do a factory reset to return the settings to the factory defaults.

Note: Performing a factory reset will erase all current settings, and this action cannot be undone.

Step 1: With the unit on, use the end of a paperclip to press the reset button for seven seconds, which is located inside a small hole on the base of the unit. The power light on the front of the router will turn orange to indicate that the unit is restarting.

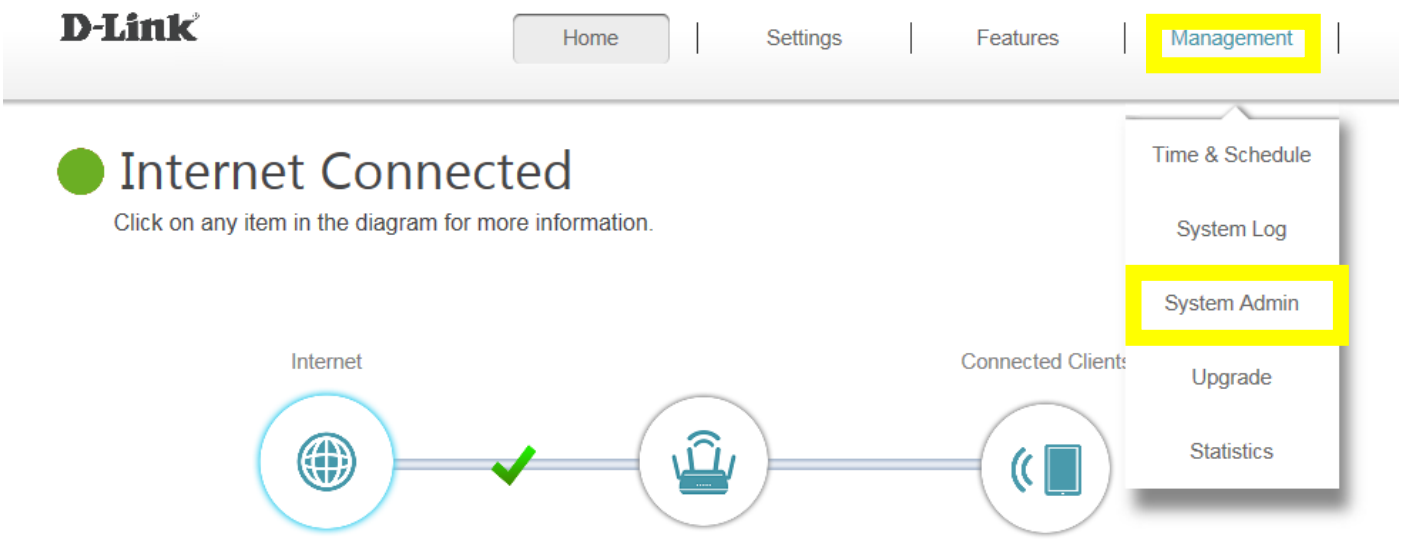
Step 2: The unit will reboot automatically. Once the power light stops blinking, the unit has been reset and is ready to use. **Resetting the router does not reset the firmware to the previous version, but it will change all settings back to factory defaults**.

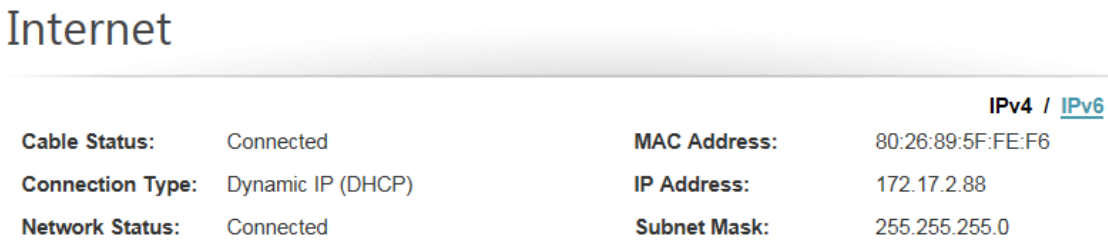
Note: The password for the Administrator (Admin) account will be reset to the default. When logging in for the first time after resetting your router, leave the Password field blank and click Log In.

Q13: How do I backup/restore the configuration on my router?

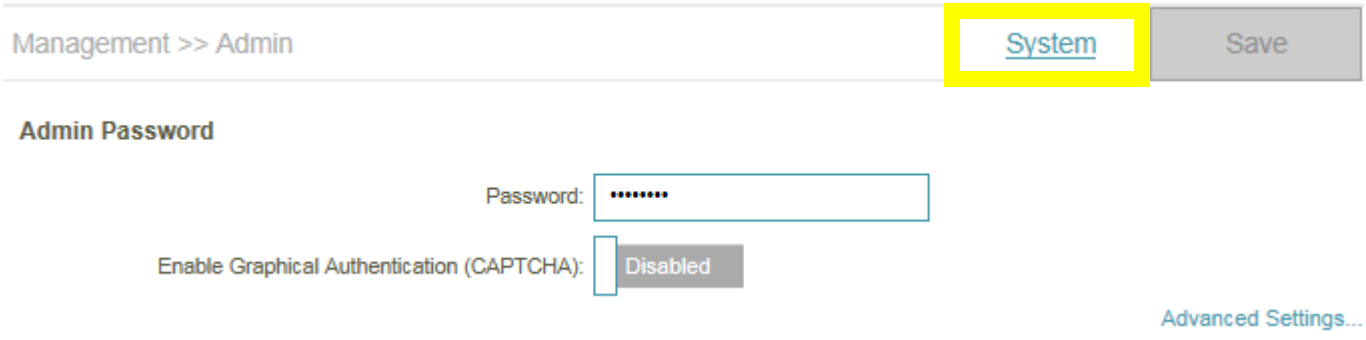
Please launch your browser and enter http://dlinkrouter.local or http://192.168.0.1 into the address bar. Then login and follow the steps below:

Step 1: Click **Management -> System Admin**

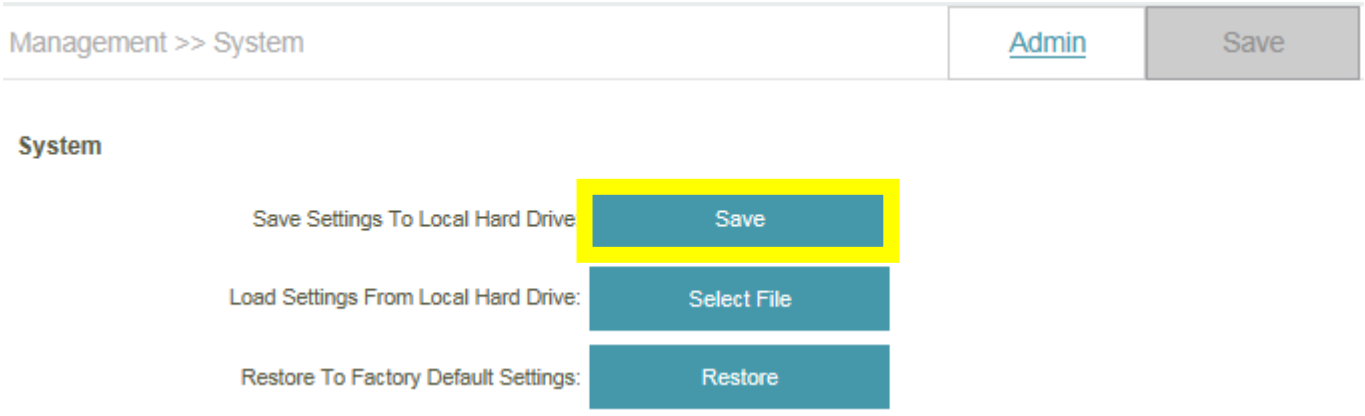




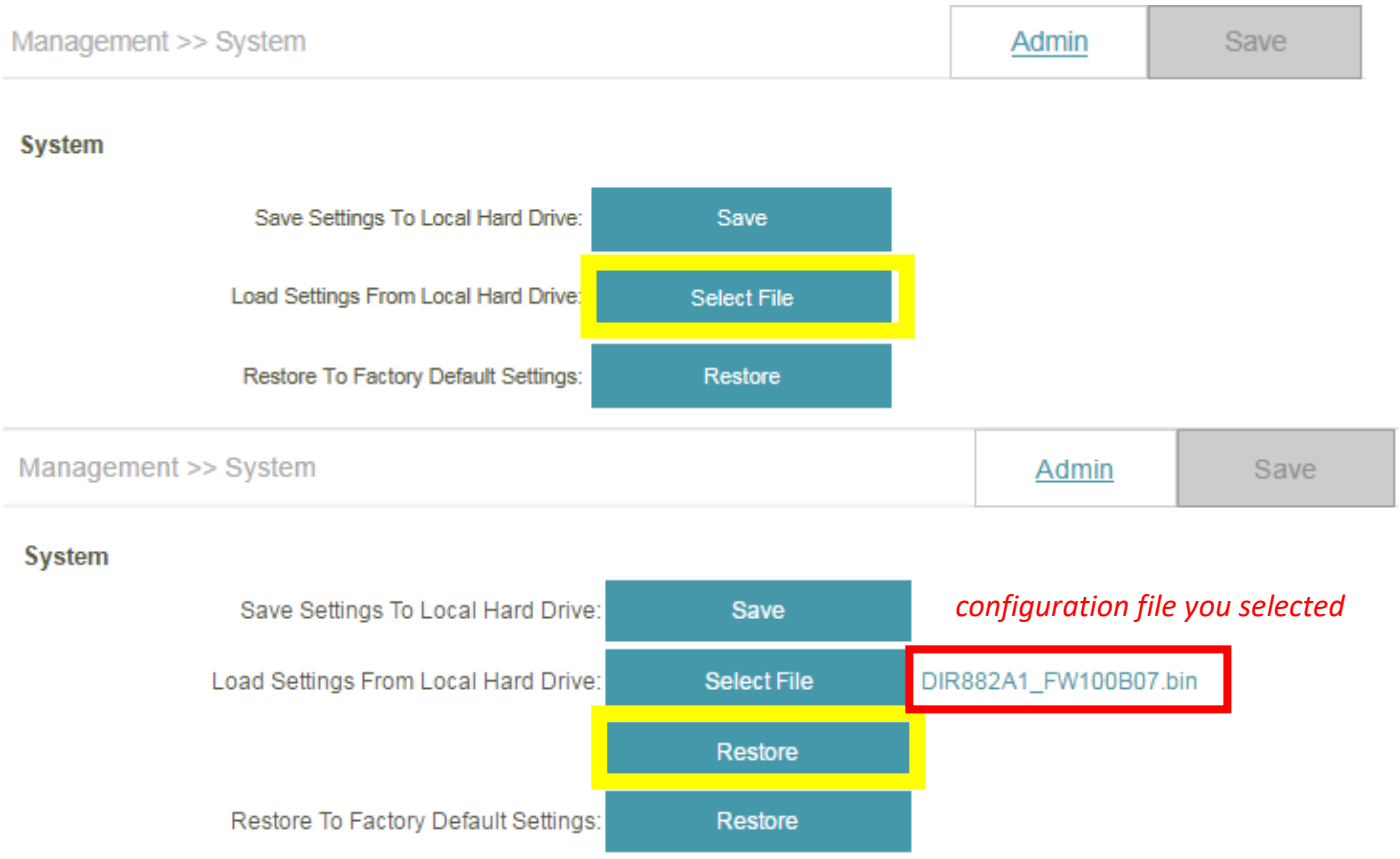
Step 2: Click **System**



Step 3: Click **Save** to save the configuration:



Step 4: To restore your configuration, click the **Select File** button and select your configuration backup file. Once selected, click **Restore**.

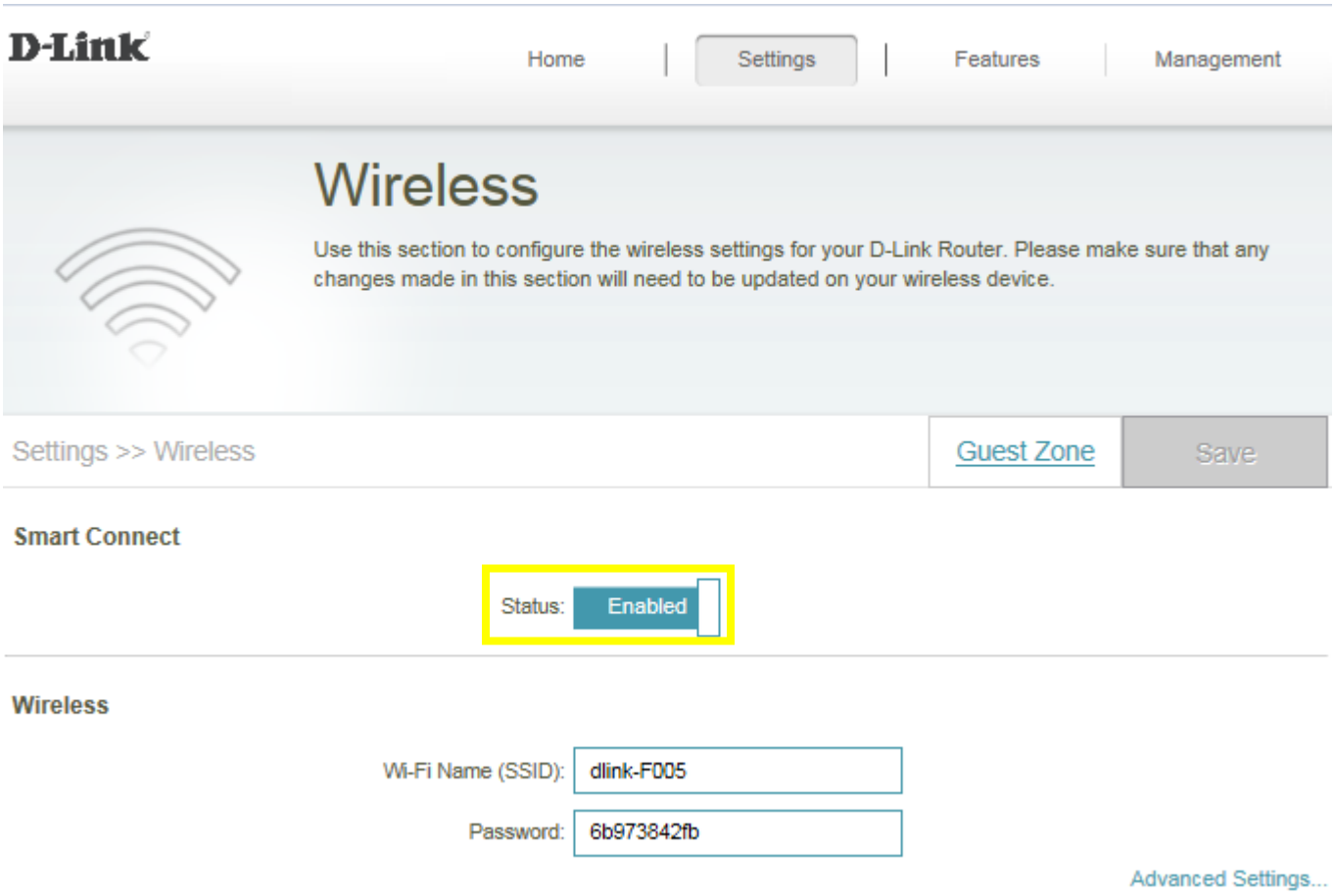


Definitions

Q14: What is smart connect?

Smart Connect - Creates a 'single' wireless network for your devices to connect to. Behind the scenes, the router automatically determines whether to connect a device to the 2.4 or 5 GHz band, thereby providing the best speed and range for each device and optimally distributing devices to each network.

Smart connect is enabled by default in **Setting** -> **Wireless**:



If disable smart connect, you'll need to configure 2.4G/5G band individually.

Q15: What is WPS?

Wi-Fi Protected Setup (WPS) is a standard to connect wireless devices together easily and secure. To use WPS, your product must support WPS and be compatible with WPA/WPA2 security.

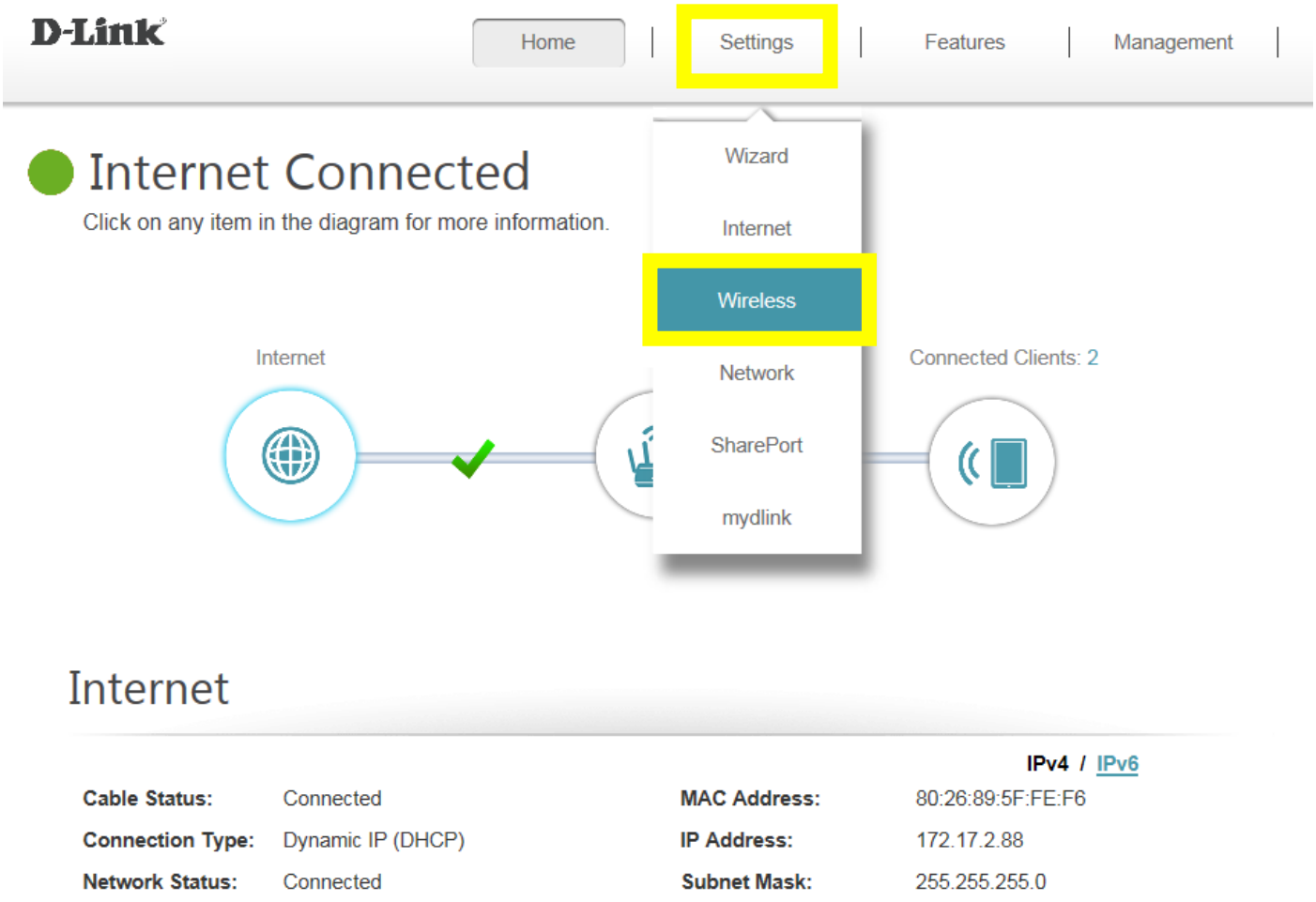
To use, simply press the WPS button on your router or access point, and then press the WPS button on your wireless client (sometimes may be enabled by software) within 2 minutes. The router/access point will automatically configure your client with your Wi-Fi name (SSID) and Wi-Fi password.

Guest Zone Setting

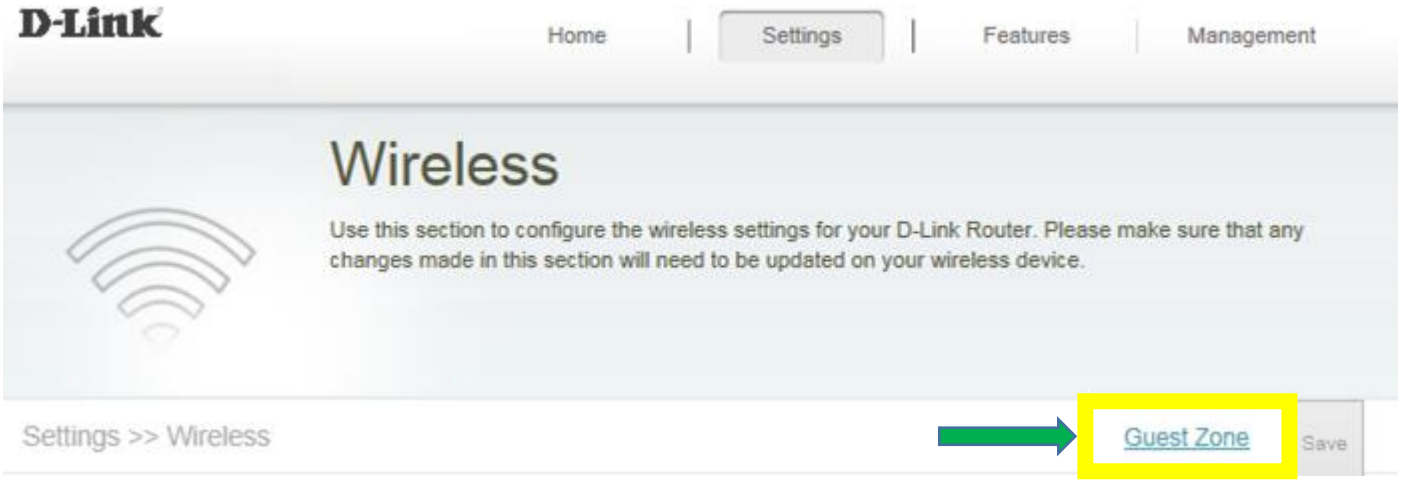
Q16: How do I enable Guest Zone/Guest Access on my router?

Please launch your browser and enter http://dlinkrouter.local or http://192.168.0.1 into the address bar. Then login and follow the steps below:

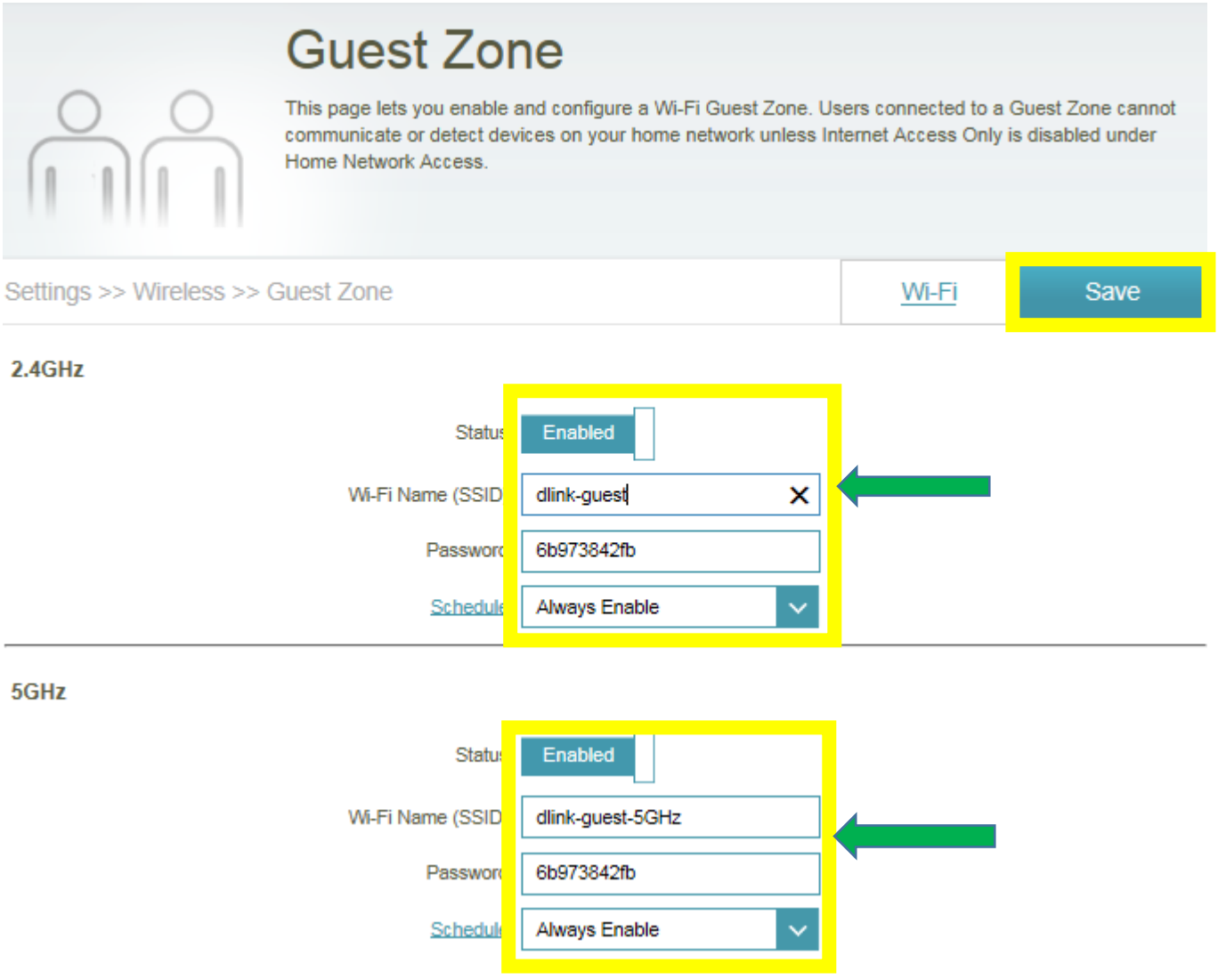
Step 1: Click **Settings** -> **Wireless**



Step 2: Click the **Guest Zone** tab:



Step 3: Configure Guest Zone and click **Save**:



Connection Checking/Troubleshooting

Q17: How many simultaneous users can my Wi-Fi network handle?

The more devices that are simultaneously connected to your device, the slower the transfer speed will be for each device. D-Link recommends **15 simultaneously connected users** as the maximum number.

Q18: My router is dropping connections, how to fix this?

If your router is not performing properly (freezing, automatically rebooting, disconnecting…etc.), this could be happening for a number of reasons.

Please check the following:

1. Ensure the router is in a well ventilated area. If the router does not get adequate airflow, it could overheat.
2. Ensure the firmware is up to date.
   Firmware is the "brain" of the router, it is the programming that tells it how to work. D-Link will release new firmware versions when bugs are reported and fixed. Upgrading the firmware may correct issues you are experiencing.
   Please follow this link for instructions of how to upgrade the firmware- How to upgrade firmware for router?
3. Perform a factory reset on the router. Please follow this link for instructions: Reset your router to factory default setting?

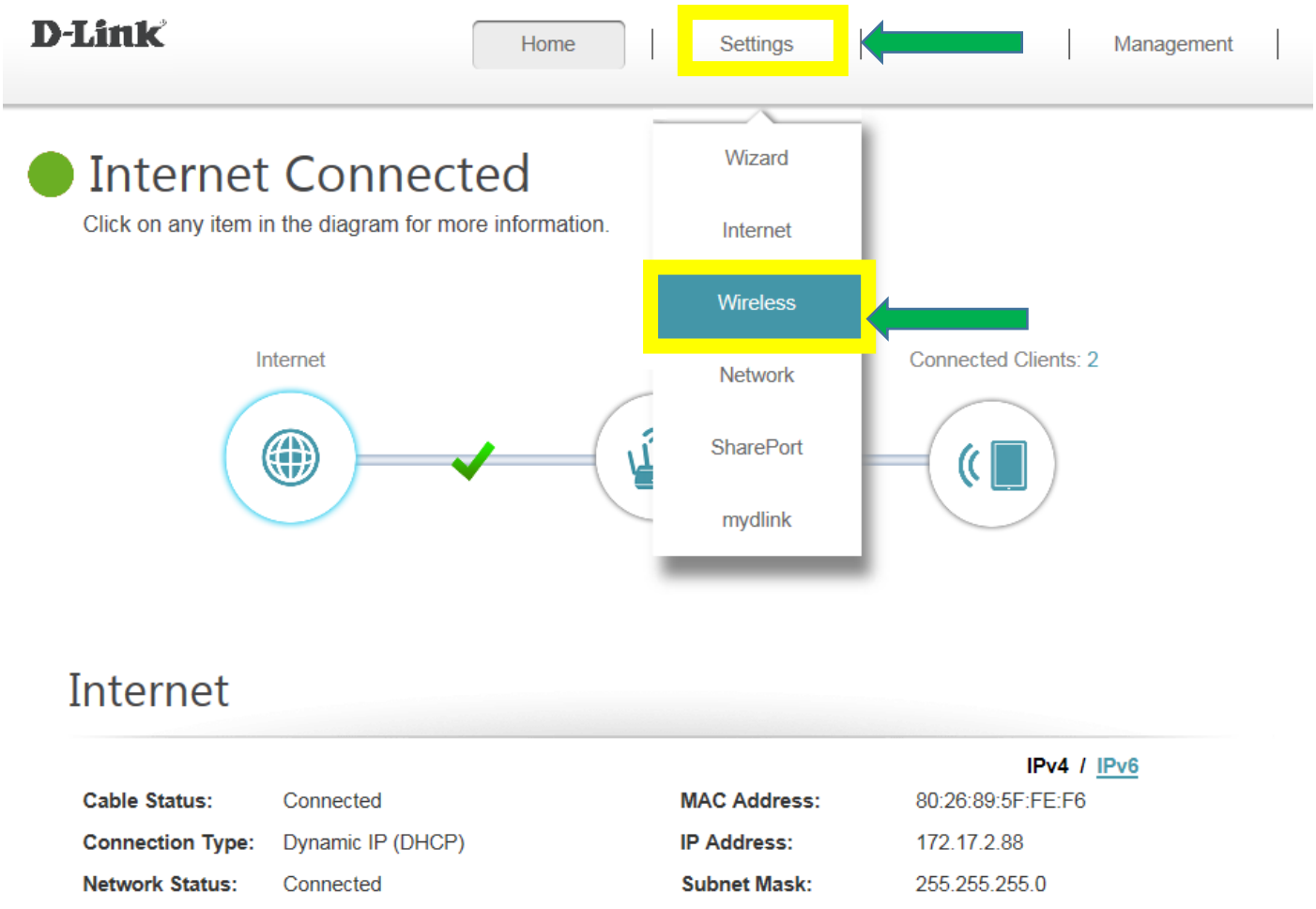
Q19: What can I do if I'm having wireless connection problems?

If you are experiencing any of the below wireless problems:

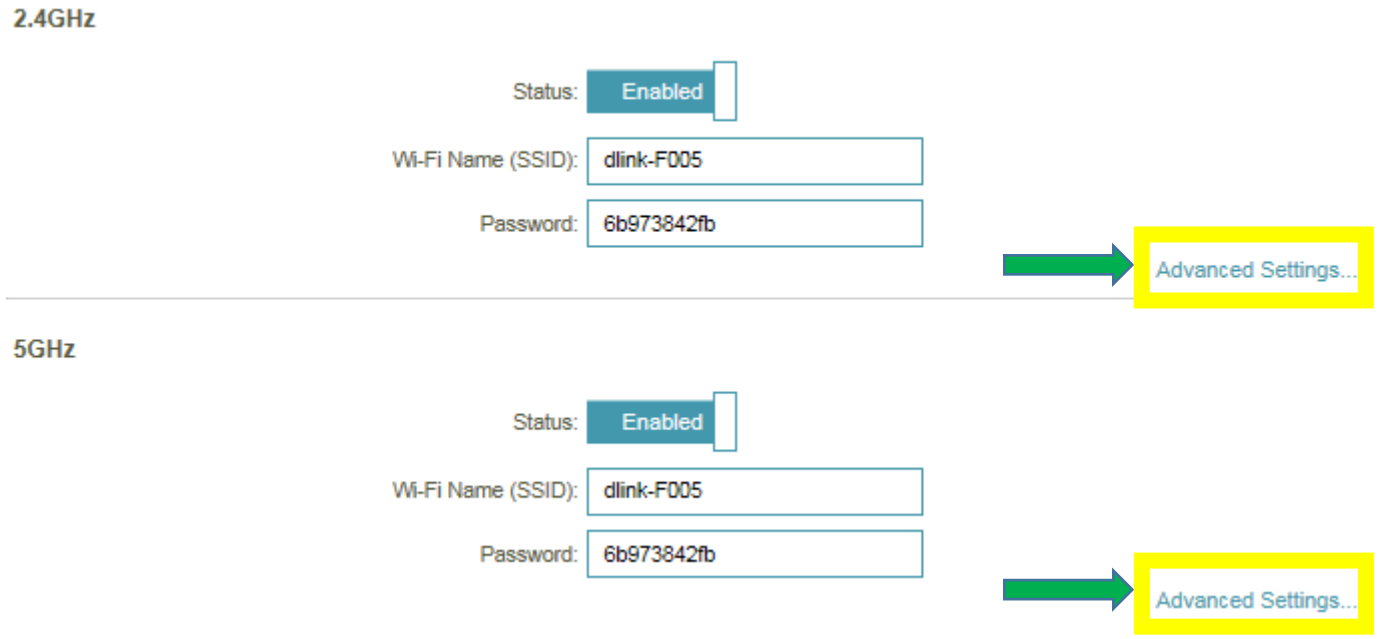
- Slow Wireless Speeds
- Wireless Connection Drops
- Low Wireless Signal

Note: An easy way to determine if the issue is with the router or with the wireless device is to see if the issue exists on multiple devices. If you internet is slow or is only dropping on one of multiple devices/computers, then the issue is probably not with the router. If the router is the cause, all devices connected will be affected.

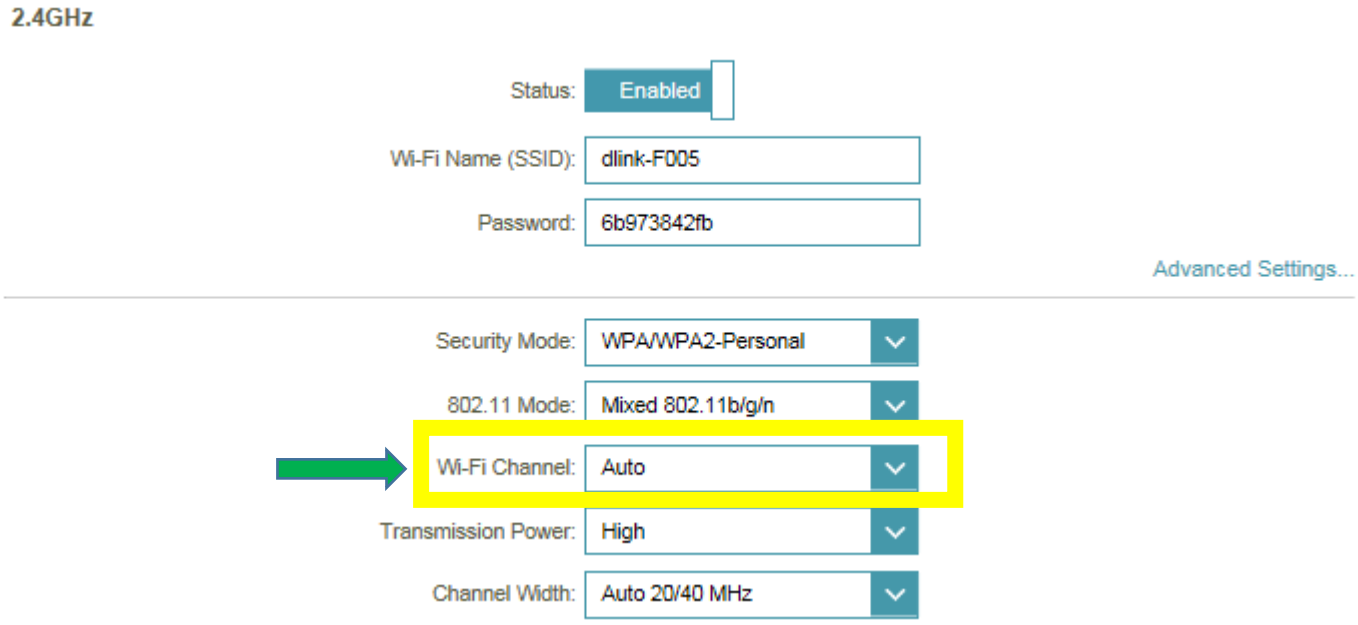
1. **Change the wireless channel:**
   Please launch your browser and enter http://dlinkrouter.local or http://192.168.0.1 into the address bar. Then login and follow the steps below:
   Step 1: Click **Settings** -> **Wireless**



Step 2: Click **Advanced Settings** for both 2.4G and 5G bands:



Step 3: Click **Wi-Fi Channel** box, select your desired Channel and click **Save**



2. **Check or change the location of your router**-- even a subtle changes (2-3 feet) can make a big difference.
   - Ensure the router is in a well ventilated and open area (Do not put the router in a cabinet or enclosed area)

   - Other devices that use the 2.4Ghz/5Ghz wireless band will interfere with your wireless network, these include- (Microwaves, wireless cameras, baby monitors). If needed, place the router or the other devices in a different area if they are close to each other.

- Wireless signals will degrade (or die completely) when going through brick (fireplace), metal (file cabinet), steel, lead, mirrors, water (fish tank), large appliances, glass, etc.

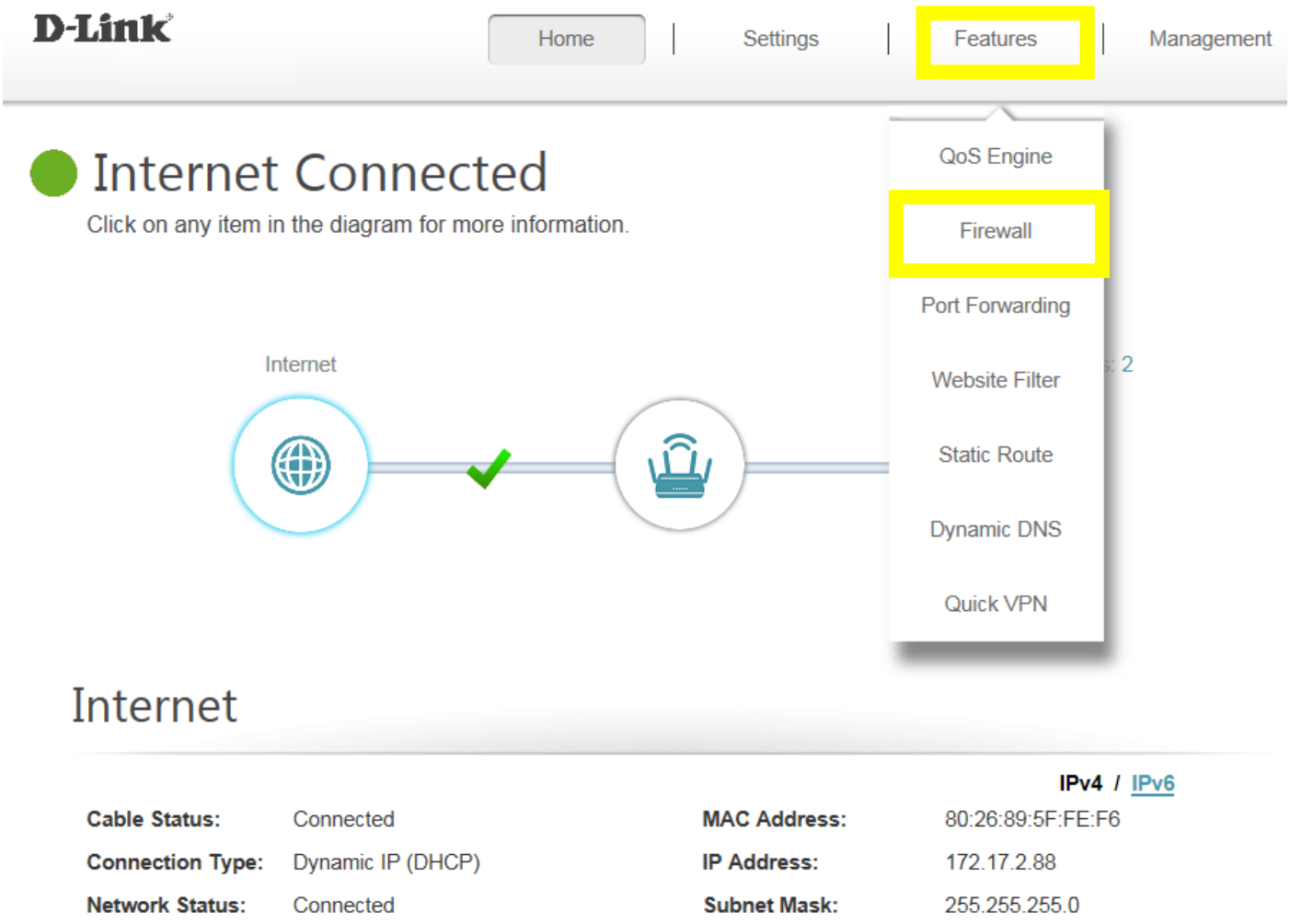
3. **Ensure that your router is running the latest firmware version.** Please follow this link for instructions of how to upgrade the firmware- How to upgrade firmware for router?

Q20: Why won't my VoIP device work with my router?

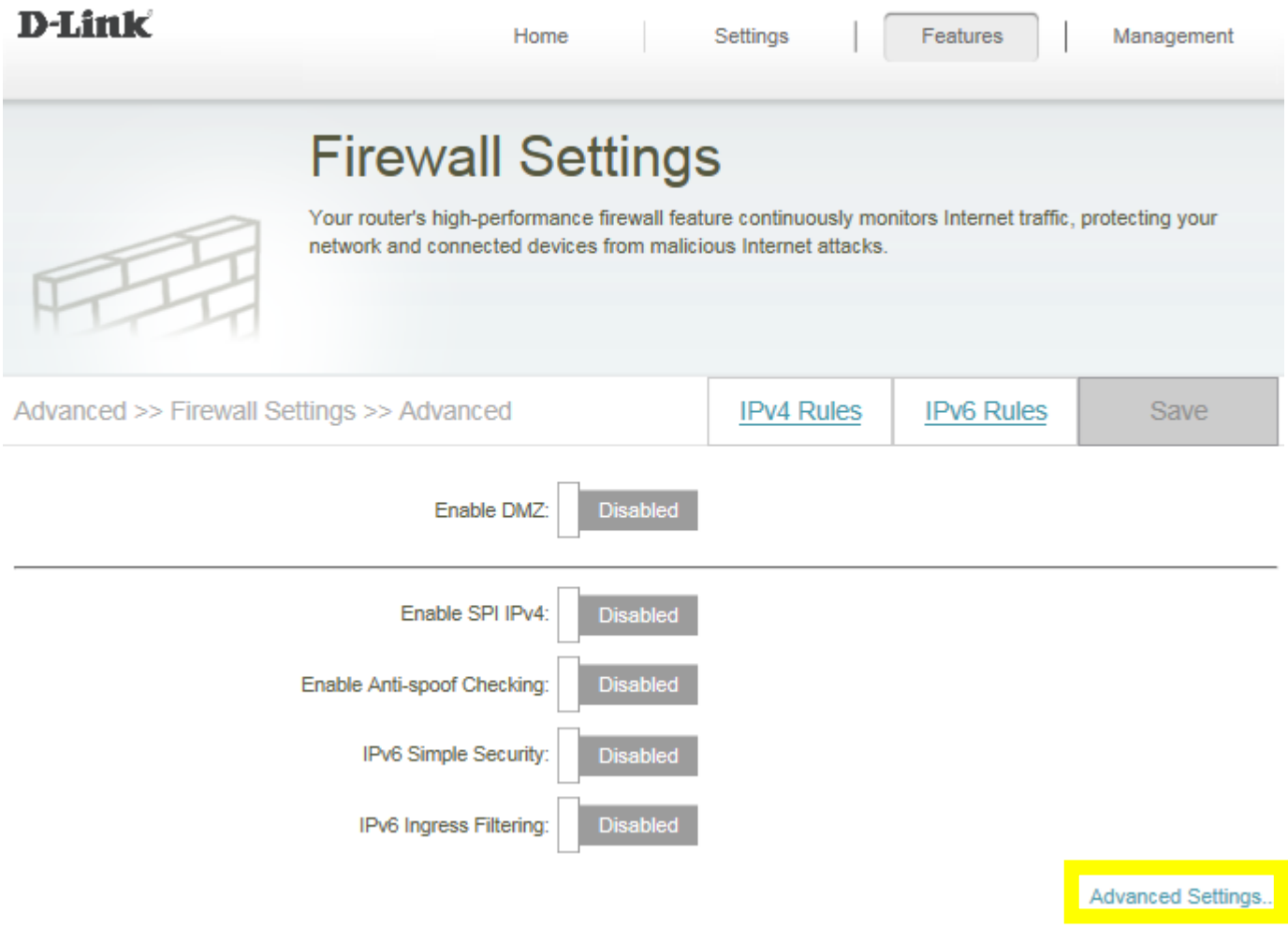
1. Please confirm if you load the latest firmware in your router. You can review the process of firmware version checking and upgrading process below:
   (1) Firmware version checking: How to check firmware version for your router?
   (2) Firmware upgrade process: How to upgrade firmware for your router?

2. **Disable the SIP ALG feature on your router**
   SIP ALG allows devices and applications using VoIP (Voice over IP) to communicate across NAT. Some VoIP applications and devices have the ability to discover NAT devices and work around them. This ALG may interfere with the operation of such devices. If you are having trouble making VoIP calls, try turning this ALG off.

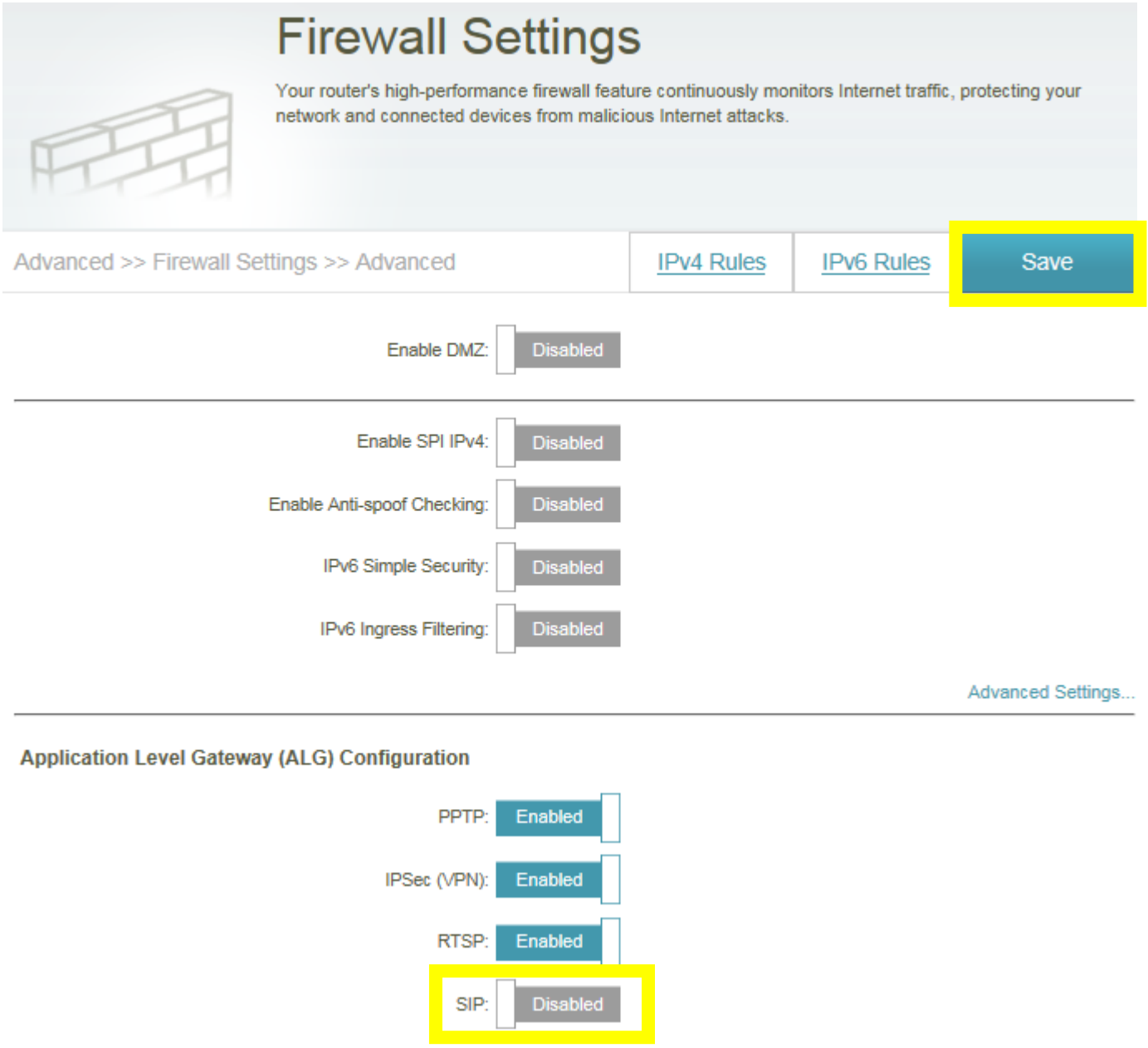
   Please launch your browser and enter http://dlinkrouter.local or http://192.168.0.1 into the address bar. Then login and follow the steps below:
   Step 1: First, click **Feature** -> **Firewall**:



Step 2: Then, click **Advanced Settings**:



Step 3: Click **SIP** to disable SIP ALG, then click **Save**:



Port Forwarding/Virtual Server Setting

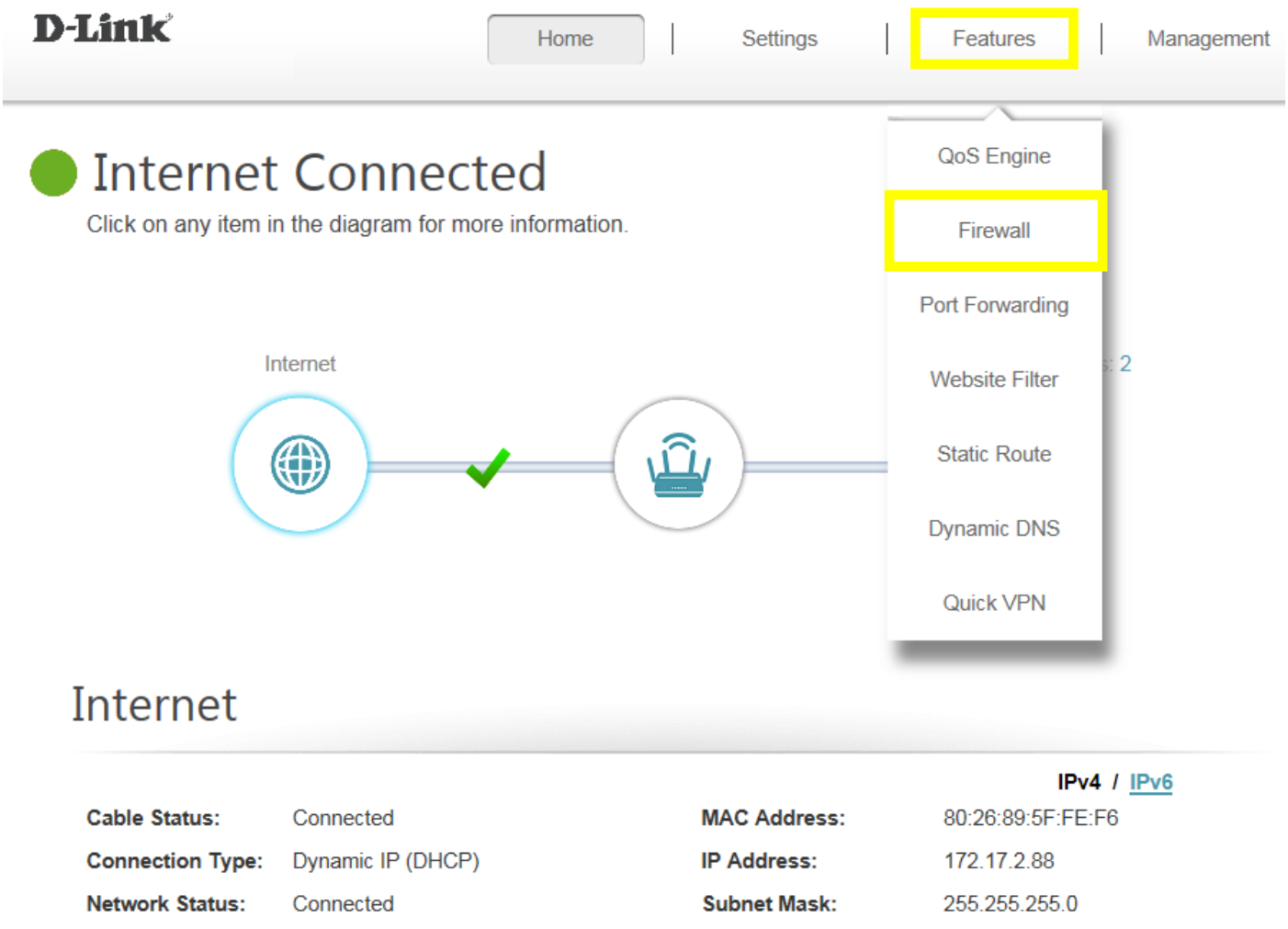
Q21: How do I enable DMZ on my router?

DMZ should only be used if you have a computer/device that cannot run Internet applications properly from behind the router.

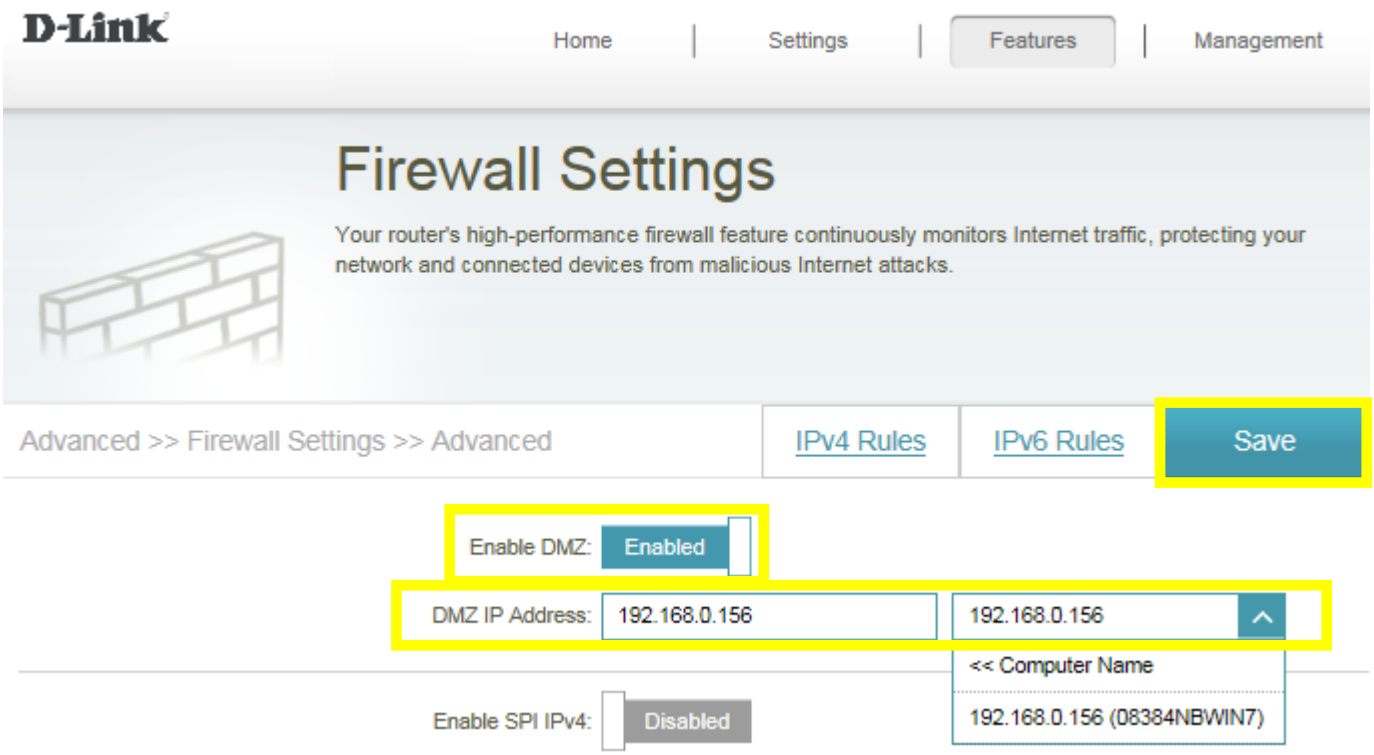
Note: By enabling the DMZ (Demilitarized Zone) feature, you are allowing the router to forward all incoming traffic from the internet to the device specified, virtually disabling the routers "firewall protection". This may expose the device to a variety of security risks, so only use this option as a last resort.

Please launch your browser and enter http://dlinkrouter.local or http://192.168.0.1 into the address bar. Then login and follow the steps below:

Step 1: Click **Features** -> **Firewall**



Step 2: Click **Enable DMZ** to toggle the DMZ state, and fill in the IP address of the specified device (**One device only**), then click **Save**.



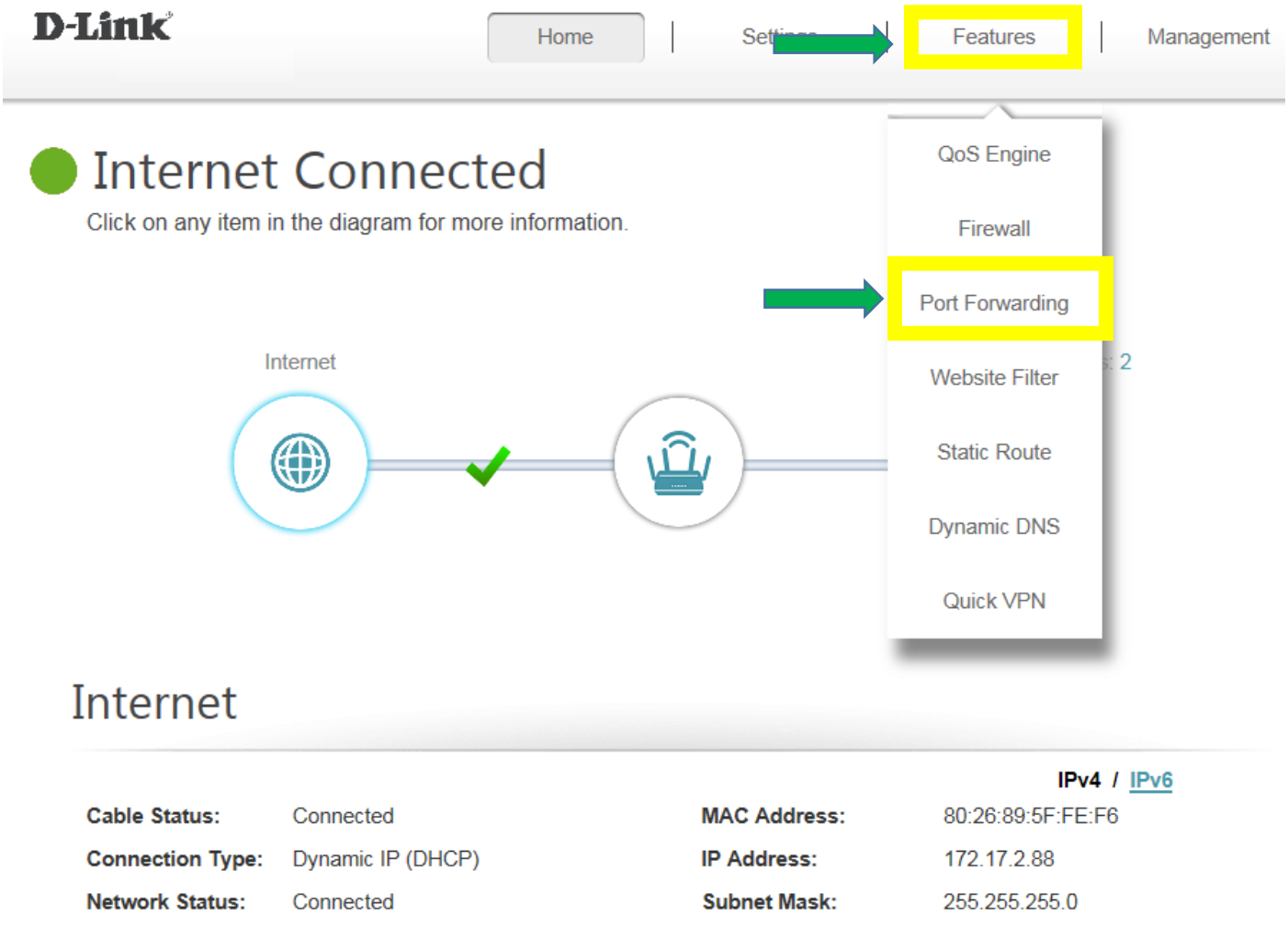
Q22: How do I open ports for routers?

Scenario 1: Single Port:

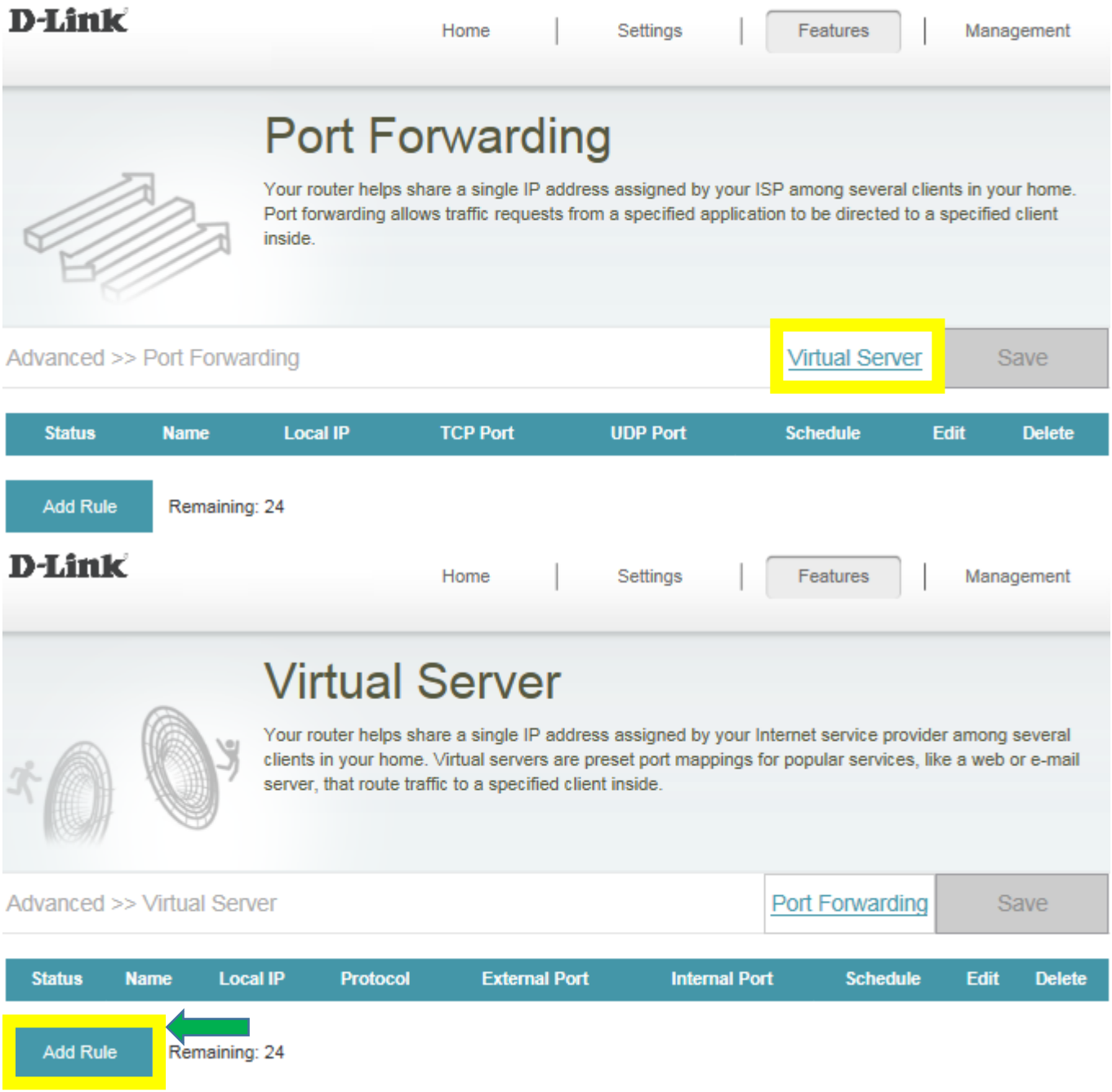
By default, your router will block all incoming connections (into your network) and allow all Outgoing connections to the Internet. In some cases, you may need to allow some connections into your network (for Example: Using the Remote Desktop Application). To do this, you must open ports on your router.

Please launch your browser and enter http://dlinkrouter.local or http://192.168.0.1 into the address bar. Then login and follow the steps below:

Step 1: Click **Feature** -> **Port Forwarding**

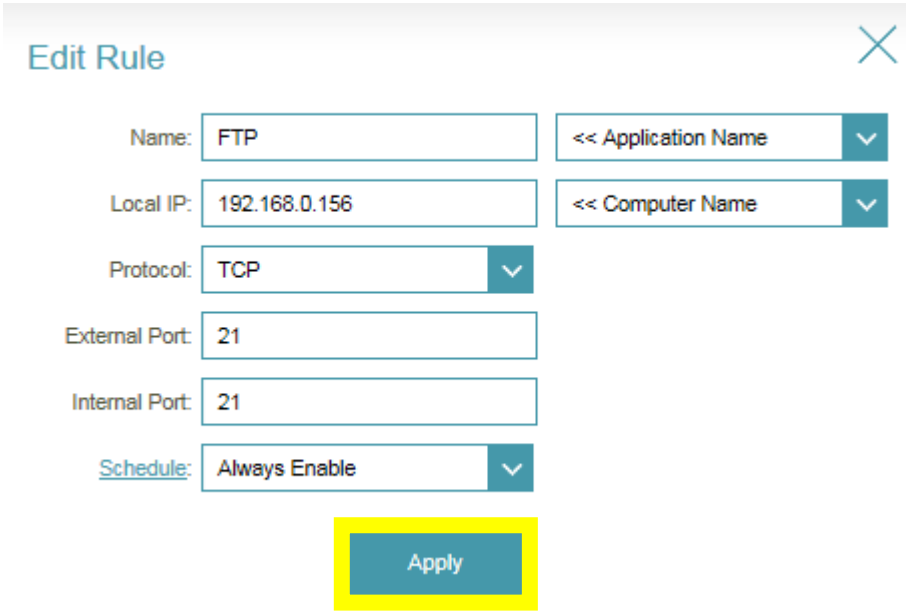


Step 2: Click **Virtual Server** and **Add Rule**

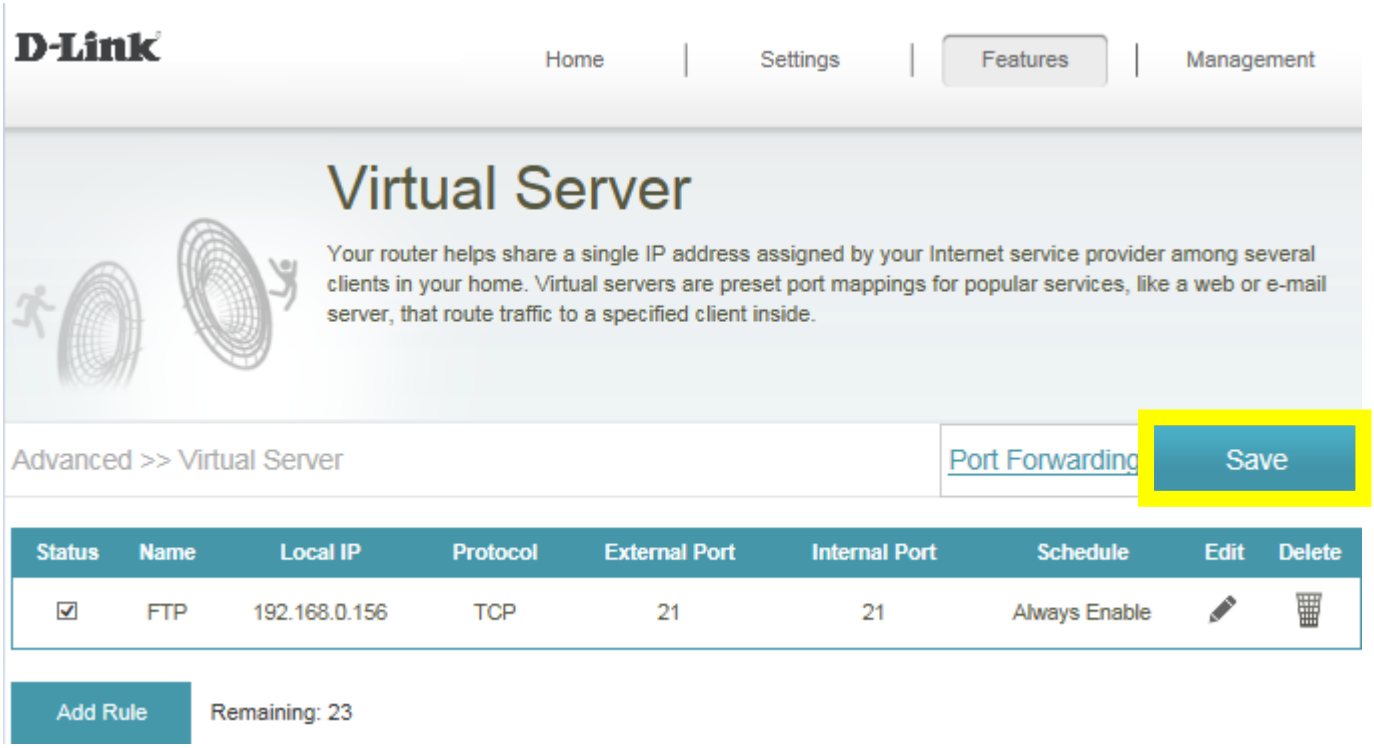


Step 3: Create your rule (FTP server as example), then **apply**

- **Name-** Enter a name for the rule (i.e. Web Server 1)
- **Local IP:** Specify the IP address of the device you are opening the port for
- **Protocol:** Specify the traffic type (TCP or UDP) - **Note:** If you are not sure, choose **BOTH**
- **External/Internal Port:** Enter the port number you want to open (i.e. 21, for FTP)



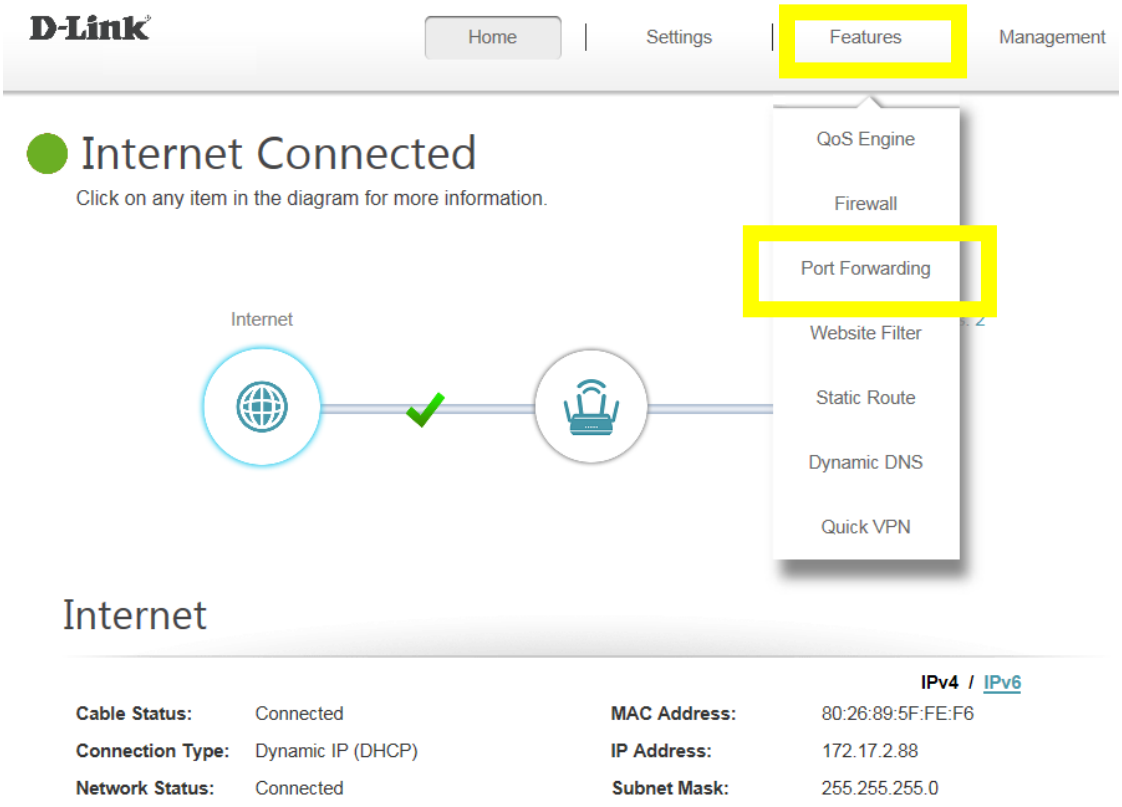
Step 4: Click **Save** After finish adding your rule.



Scenario 2: Multiple Ports:

Please launch your browser and enter http://dlinkrouter.local or http://192.168.0.1 into the address bar. Then login and follow the steps below:

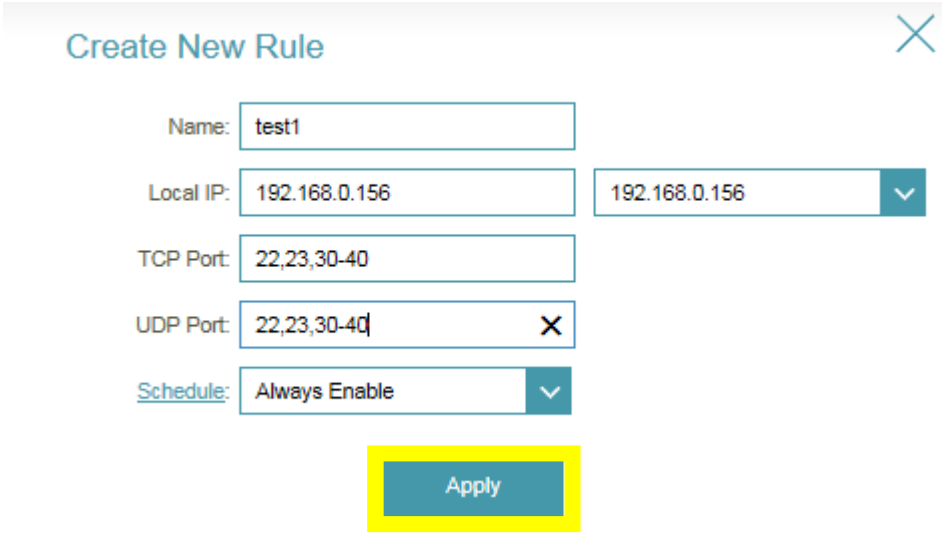
Step 1: Click **Feature** -> **Port Forwarding**



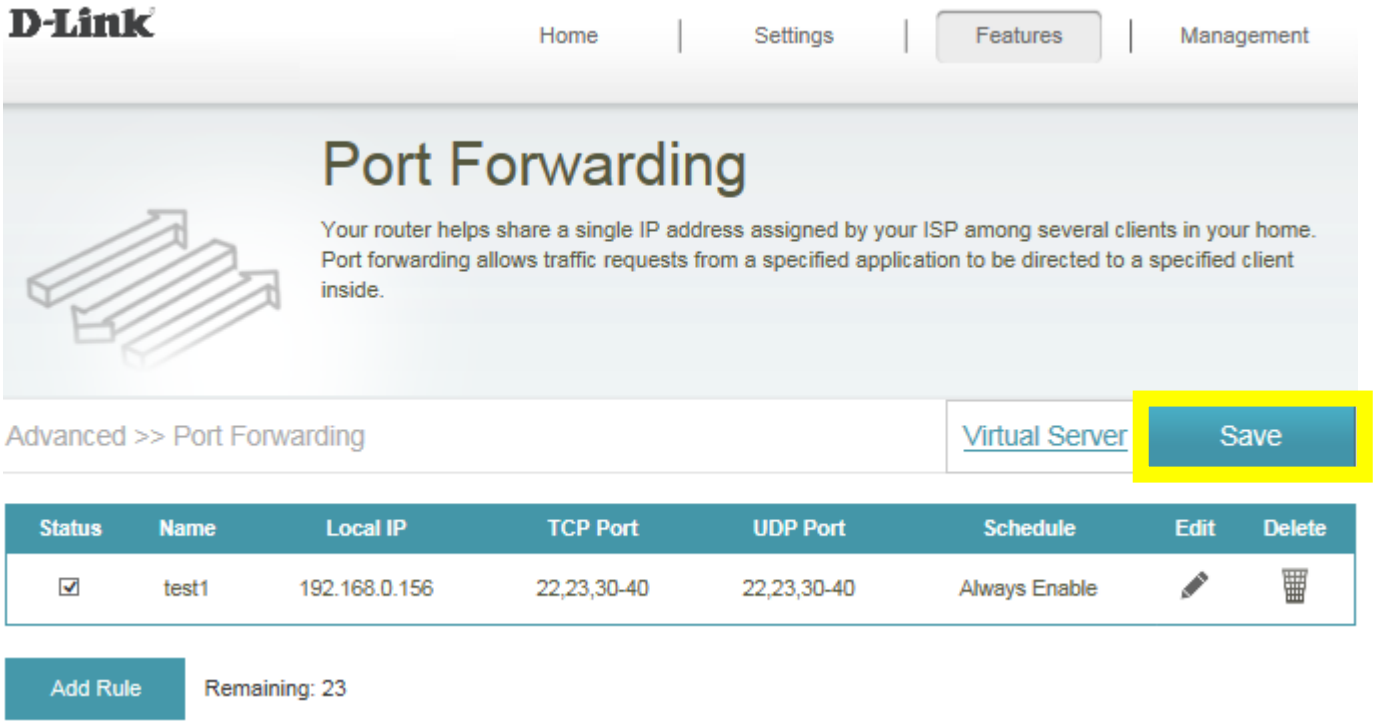
Step 2: Enter the TCP port numbers you want to open:

- **Name-** Enter a name for the rule (i.e. Web Server 1)
- **Local IP:** Specify the IP address of the device you are opening the port for
- **TCP Port:** Enter the TCP port numbers you want to open
- **UDP Port-** Enter the UDP port numbers you want to open

Note: You can enter the ports in multiple different ways- Range (50-100) Individual (80, 68, 888) Mixed (1020-5000, 689)



Step 3: Click **Save** After finish adding your rule.



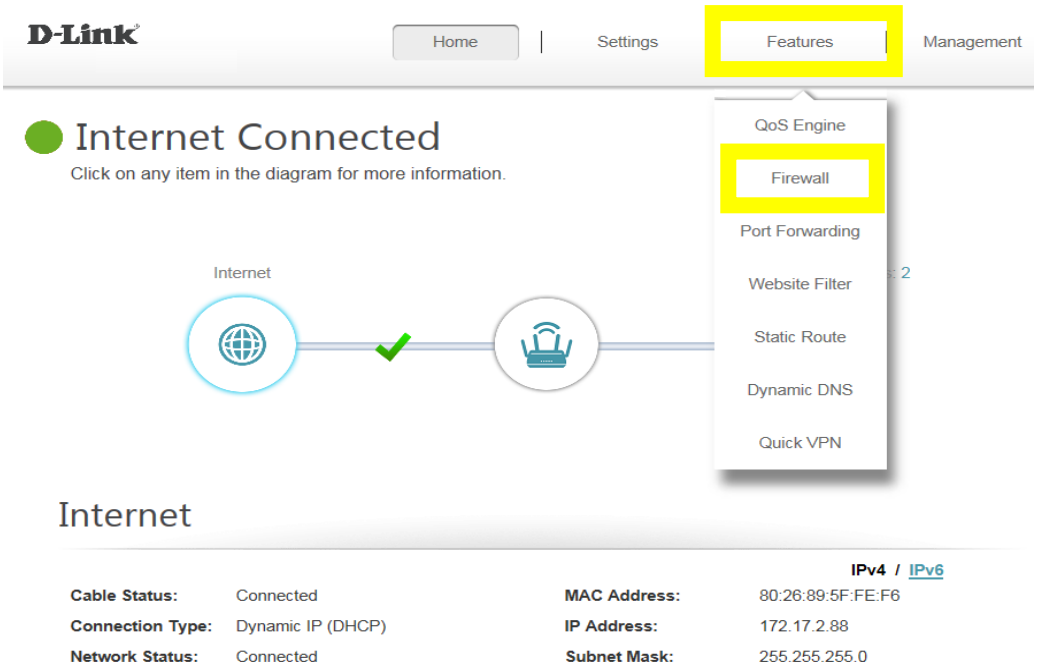
Q23: How do I configure inbound filter?

When you use the Virtual Server, Port Forwarding, or Remote Administration features to open specific ports to traffic from the Internet, you could be increasing the exposure of your LAN to cyberattacks from the Internet.

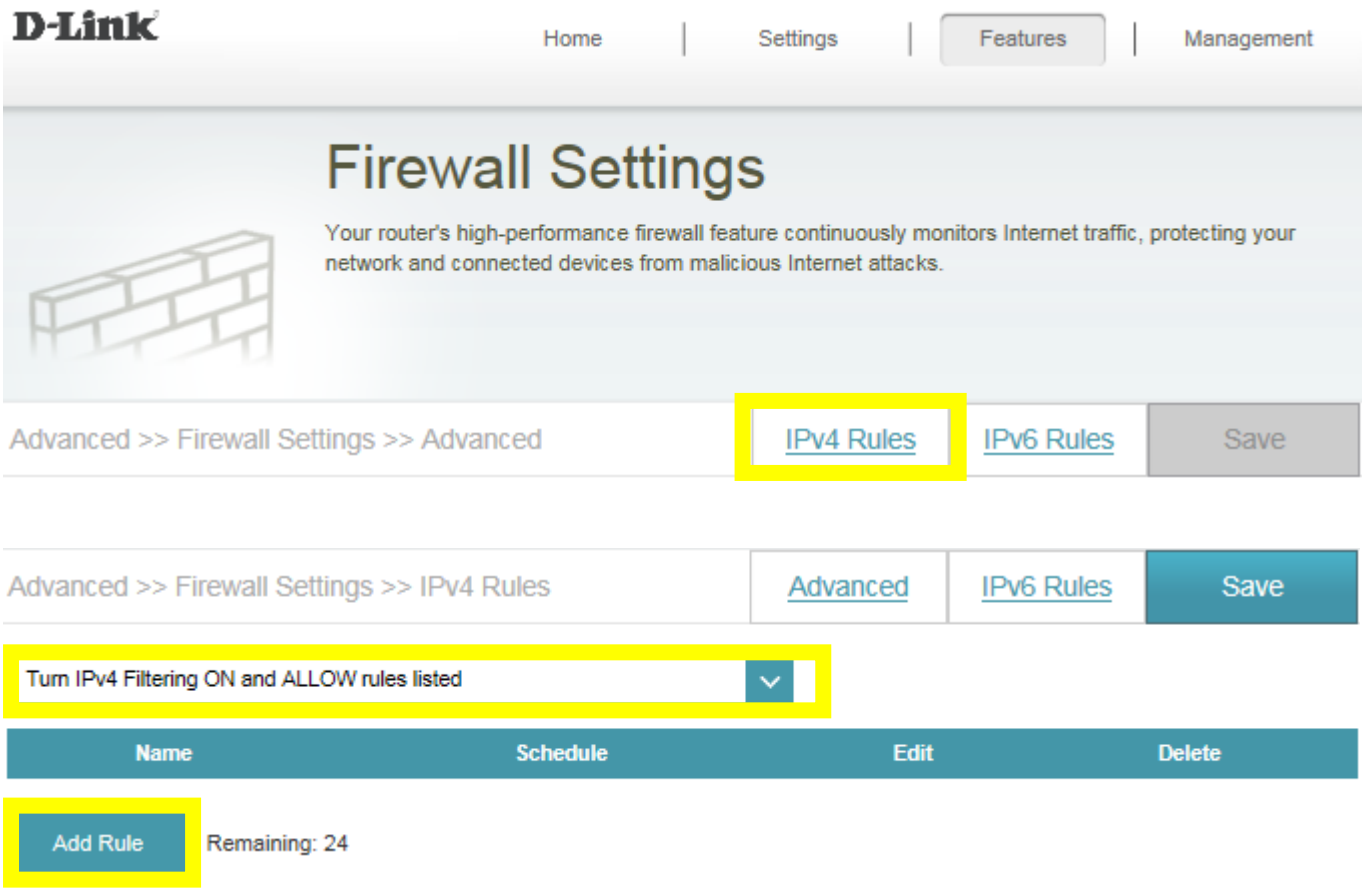
In these cases, you can use **Inbound Filters** to limit that exposure by specifying the IP addresses of internet hosts that you trust to access your LAN through the ports that you have opened. You might, for example, only allow access to a game server on your home LAN from the computers of friends whom you have invited to play the games on that server.

Inbound Filters can be used for limiting access to a server on your network to a system or group of systems. Filter rules can be used with Virtual Server, Gaming, or Remote Administration features. Each filter can be used for several functions; for example a "Game Clan" filter might allow all of the members of a particular gaming group to play several different games for which gaming entries have been created. At the same time, an "Admin" filter might only allow systems from your office network to access the WAN admin pages and an FTP server you use at home. If you add an IP address to a filter, the change is effected in all of the places where the filter is used.

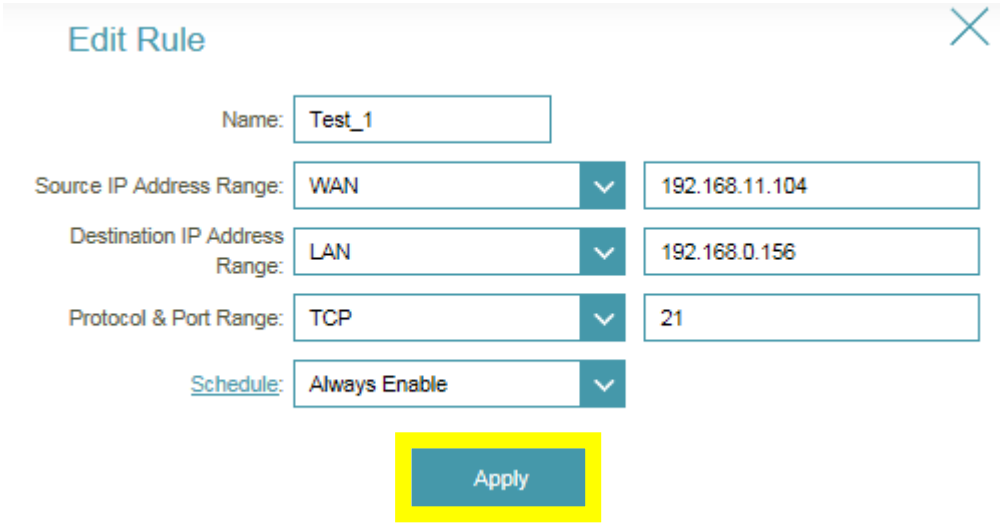
Please launch your browser and enter http://dlinkrouter.local or http://192.168.0.1 into the address bar. Then login and follow the steps below:
Step 1: Click on **Features** on the top and then **Firewall**



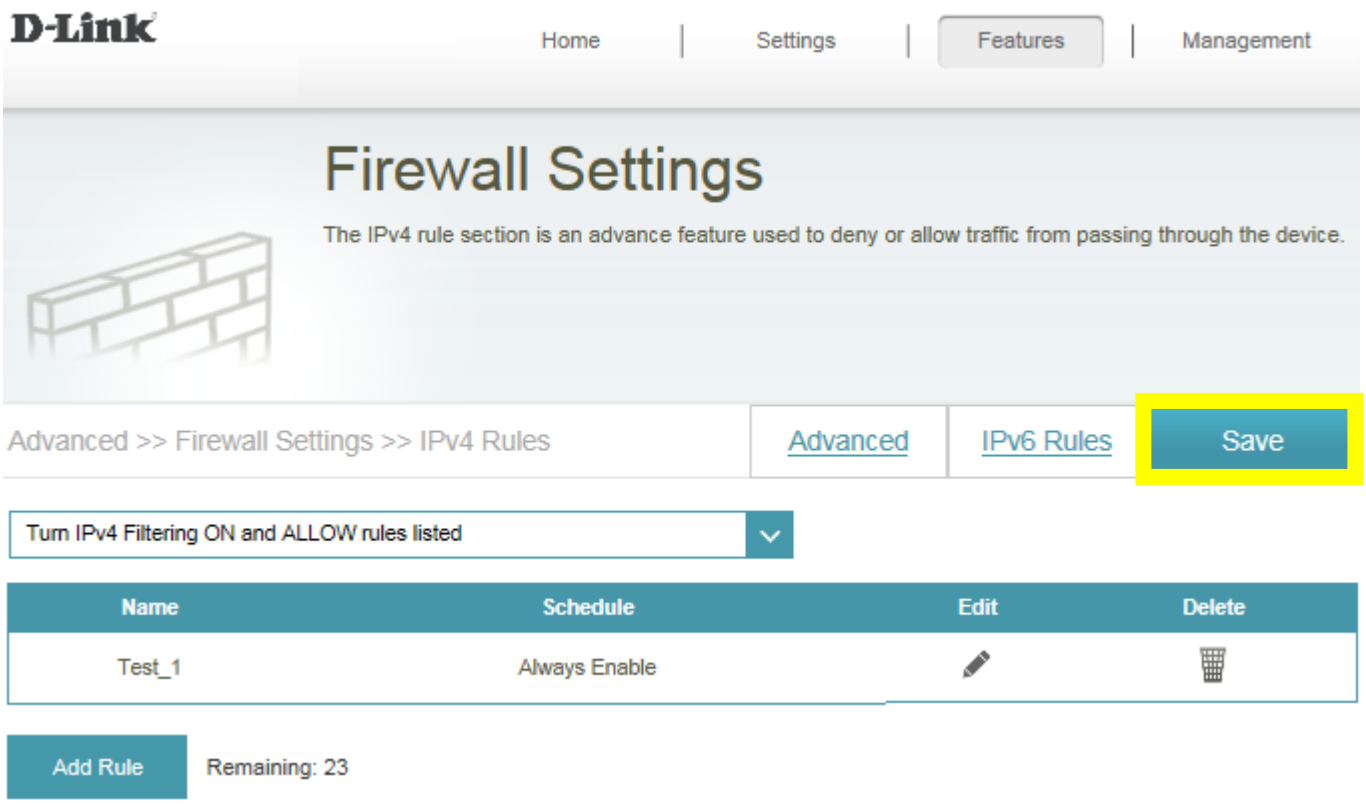
Step 2: Click on **IPV4 Rules**, then select **Turn IPV4 Filtering ON and ALLOW rules listed**, then click **Add Rule**



Step 3: Create your rule



Step 4: Click **Save** after adding your rule.



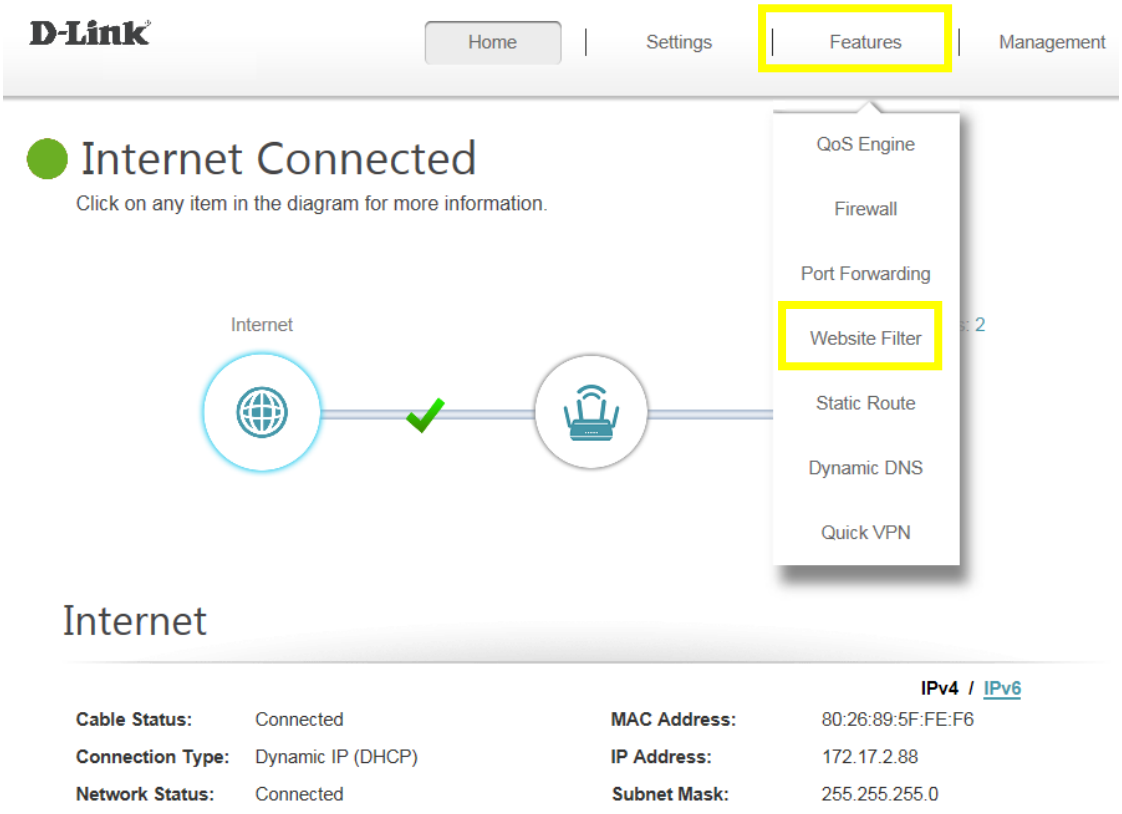
Note: If you'd like to block specific IP addresses accessing your router, please select "**Turn IPV4 Filtering ON and ALLOW rules listed**" from the drop-down menu.

Website Filter Setting

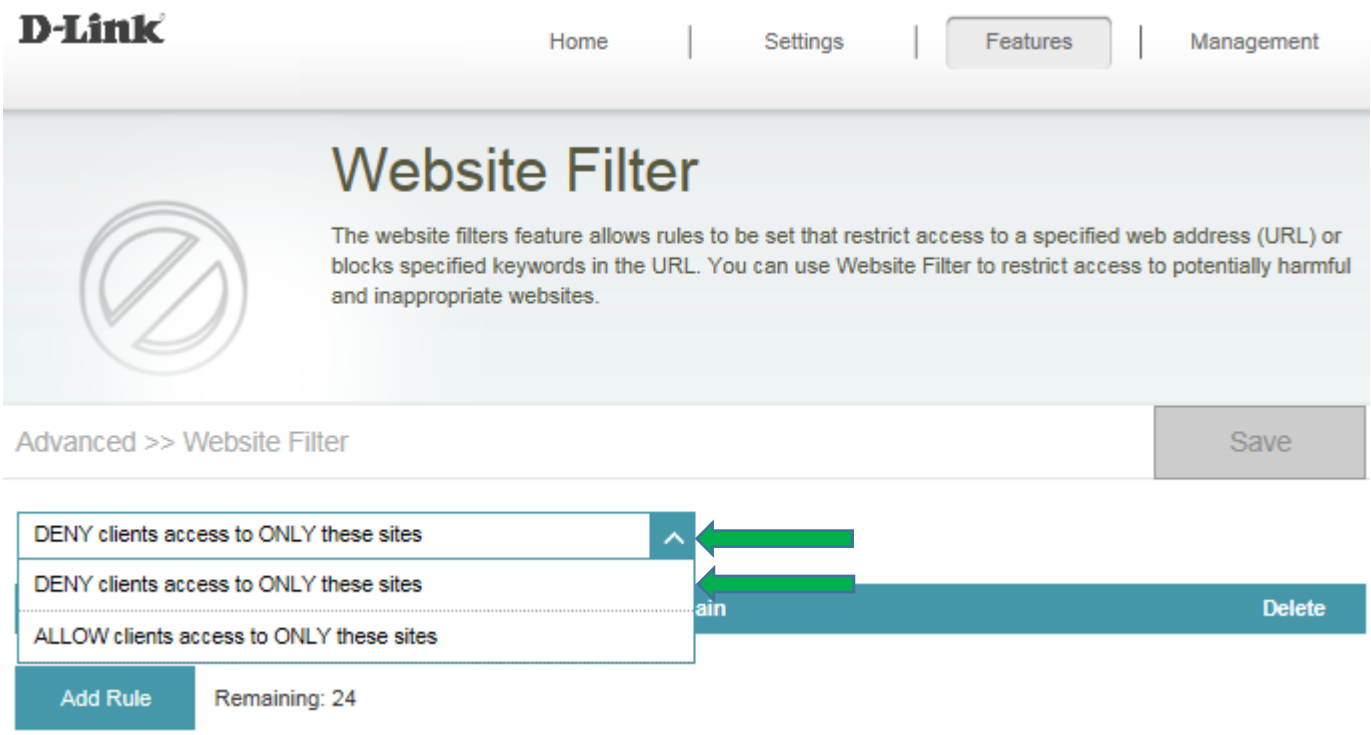
Q24: How do I set up website filter on my router?

Please launch your browser and enter http://dlinkrouter.local or http://192.168.0.1 into the address bar. Then login and follow the steps below:

Step 1: Click **Features** -> **Website Filter**

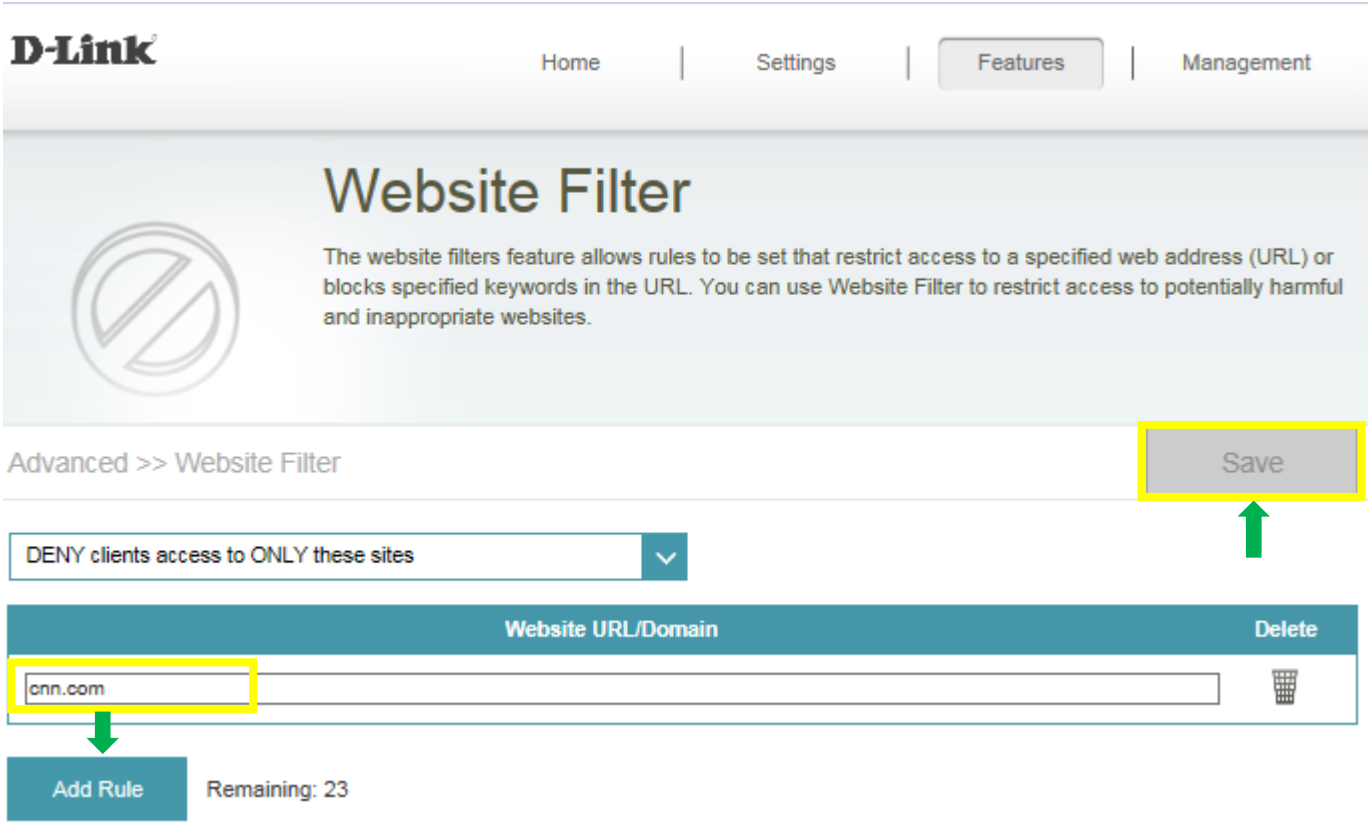


Step 2: If you want to create a list of sites to block, **select DENY computers access to ONLY these sites** from the drop-down menu. All other sites will be accessible.



If you want to specify a list of sites to allow, select **ALLOW computers access to ONLY these sites** from the drop menu. All other sites will be blocked.

Step 3: You may specify a maximum of fifteen web sites. To add a new site to the list, click **Add Rule**, and enter the URL or domain you wish to deny or allow access to in the Website URL/Domain column, and click **save**.



Note:

1. If you wish to delete a rule, click on its trash can icon in the Delete column. If you wish to edit a rule, simply replace the URL or domain.
2. **The https website can't be blocked by website filter. For example: Facebook, YouTube, Amazon...etc. If necessary, please apply OpenDNS paid service to fulfill your requirement.**

   The service website is as below: https://www.opendns.com/setupguide/. There are 15 days for free trial. Sign up for new account, follow the setup guide to establish the service, and start enjoy the stunning service provided by Cisco.

   Note: Please confirm if DNS relay is enabled. (It's enabled by default)

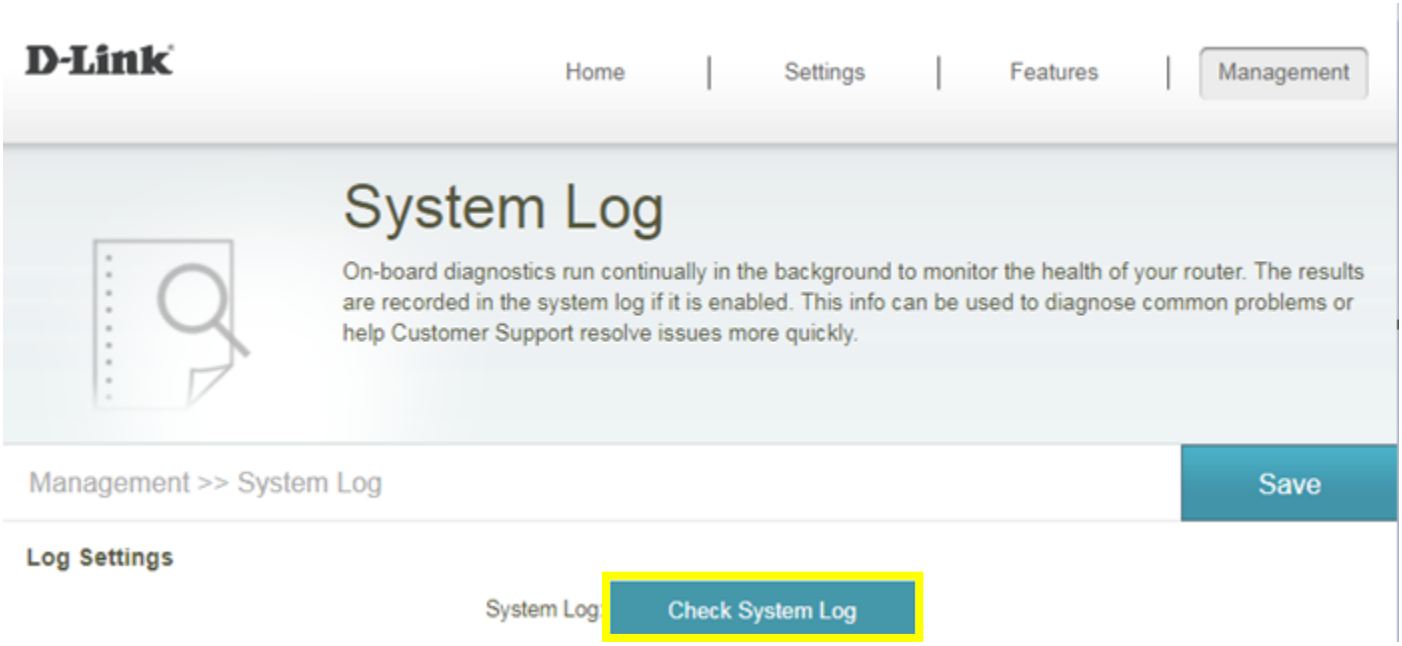
System Log

Q25: How to check system log for router?

There are 3 methods to check system log of router. Select **Management** -> **System Log**, and follow the methods as below:

Method 1: Log Settings

Step 1: Click Check System Log button, and download the file "**messages**" to your folder.



Step 2: Open the messages via WordPad/NotePad, then you can check system log.

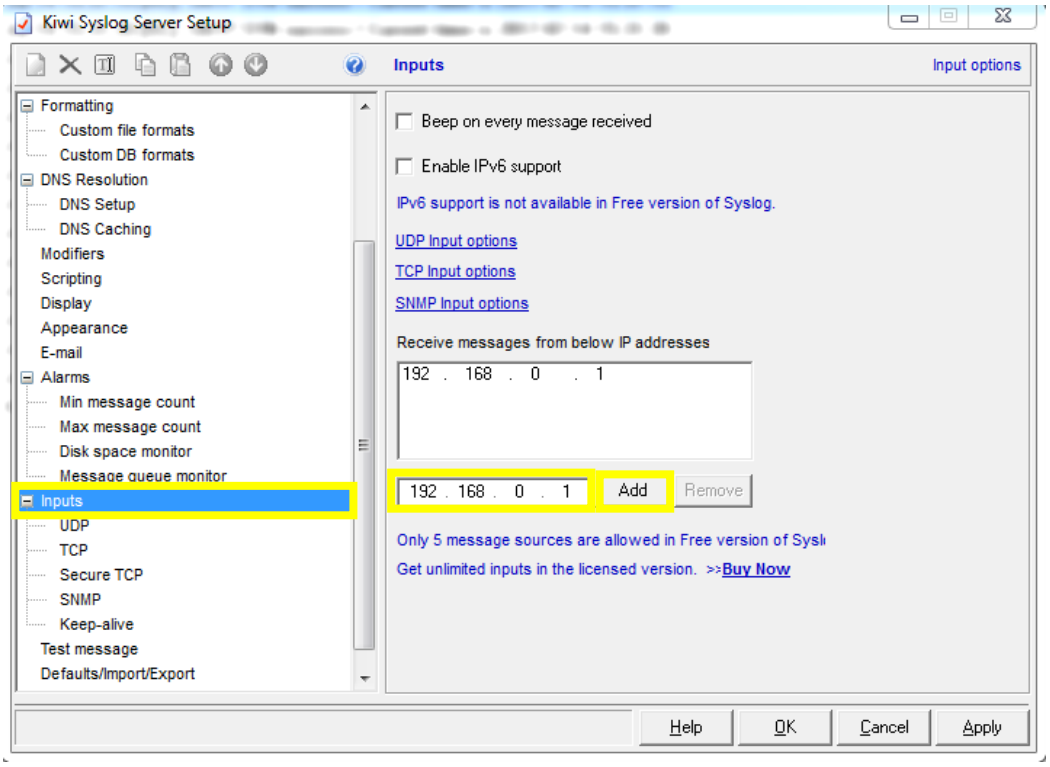
```
2017-05-25 11:44:40 [SYSLOG]: start BusyBox v1.12.1
2017-05-25 11:45:20 [RC]: Wan(ppp0) Disconnect
2017-05-25 11:45:20 ipsec_setup: ...Openswan IPsec stopped
2017-05-25 11:45:20 [DHCPS-6]: dhcp6_ctl_authinit: failed to
open /var/etc/dhcp6sctlkey: No such file or directory
2017-05-25 11:45:20 [RC]: Current Wan interface is eth3 , mode
is pppoe
2017-05-25 11:45:38 [RC]: Wan(ppp0) connect Success , Current
Wan ip is 220.137.10.136
2017-05-25 11:45:38 [UPNP]: WPS listening on port 8888
2017-05-25 11:45:41 [UPNP]: addSubscriber(/event,
http://192.168.0.2:2869/upnp/eventing/jldkzxeqsi, 1800)
2017-05-25 11:45:42 ipsec_setup: ...Openswan IPsec stopped
2017-07-12 03:19:14 [RC]: SNTP SYN success ! Current timer is
2017-07-12 03:19:14
2017-07-12 03:19:14 [MDNS]: mDNSCoreReceive: mDNSPlatformRawTime
went backwards by 79350006 ticks; setting correction factor to -
1610415401
2017-07-12 06:12:15 [UPNP]: addSubscriber(/event,
http://192.168.0.2:2869/upnp/eventing/nizkldsuia, 1800)
2017-07-12 06:12:16 [UPNP]: addSubscriber(/evt/L3F,
http://192.168.0.2:2869/upnp/eventing/vadwoqkleo, 1800)
2017-07-12 06:12:16 [UPNP]: addSubscriber(/evt/CmnIfCfg,
http://192.168.0.2:2869/upnp/eventing/lzeipjapnq, 1800)
2017-07-12 06:12:16 [UPNP]: addSubscriber(/evt/IPConn,
http://192.168.0.2:2869/upnp/eventing/zjauwwprtx, 1800)
2017-07-12 06:16:42 [UPNP]: addSubscriber(/evt/CmnIfCfg,
http://192.168.0.2:2869/upnp/eventing/qjthsaxtua, 1800)
2017-07-12 06:16:42 [UPNP]: addSubscriber(/evt/CmnIfCfg,
http://192.168.0.2:2869/upnp/eventing/pzxdjayxaf, 1800)
```

Method 2: Syslog Settings

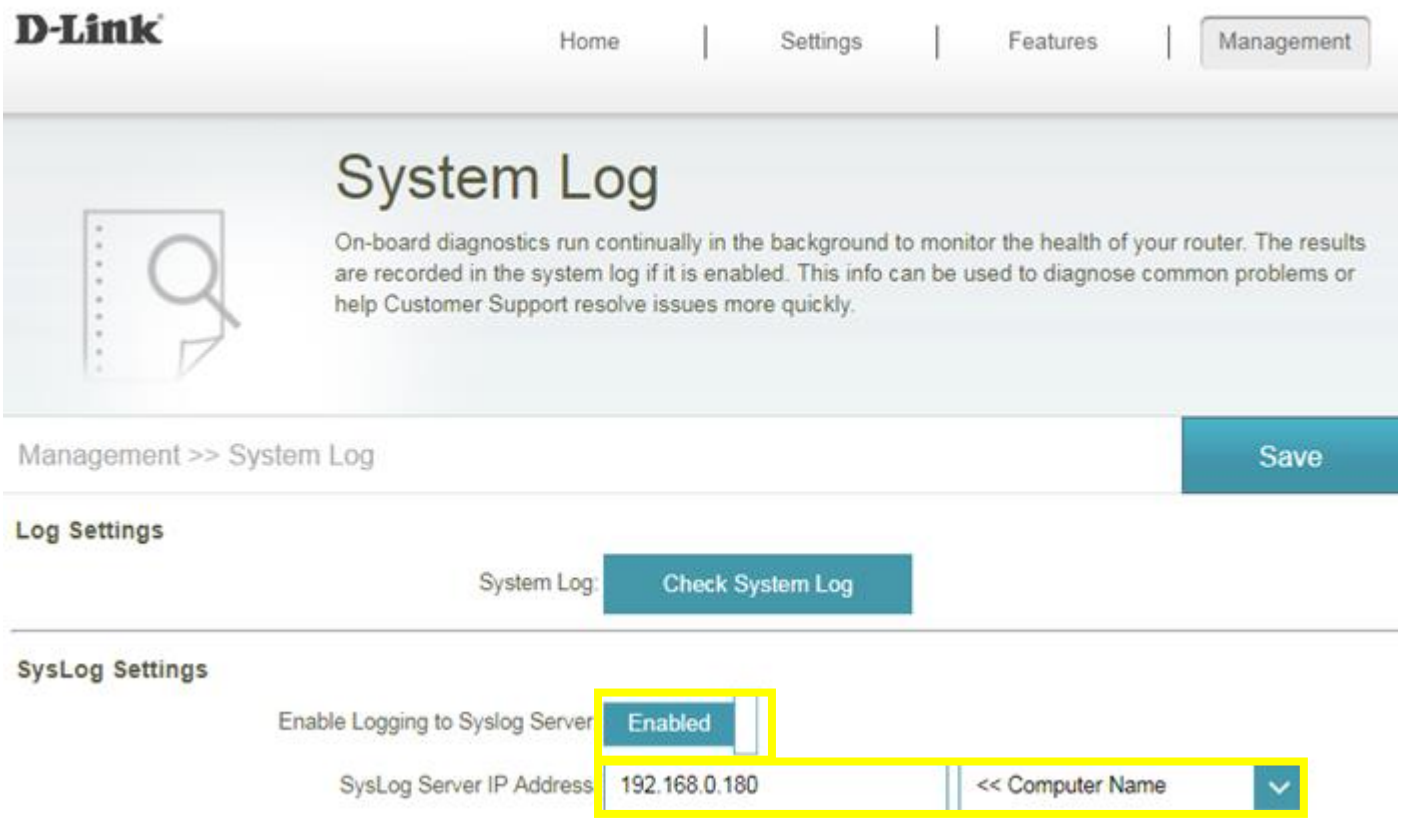
Step 1: Download system log server application, ex: Kiwi Syslog Server:

http://www.kiwisyslog.com/free-tools/kiwi-free-syslog-server

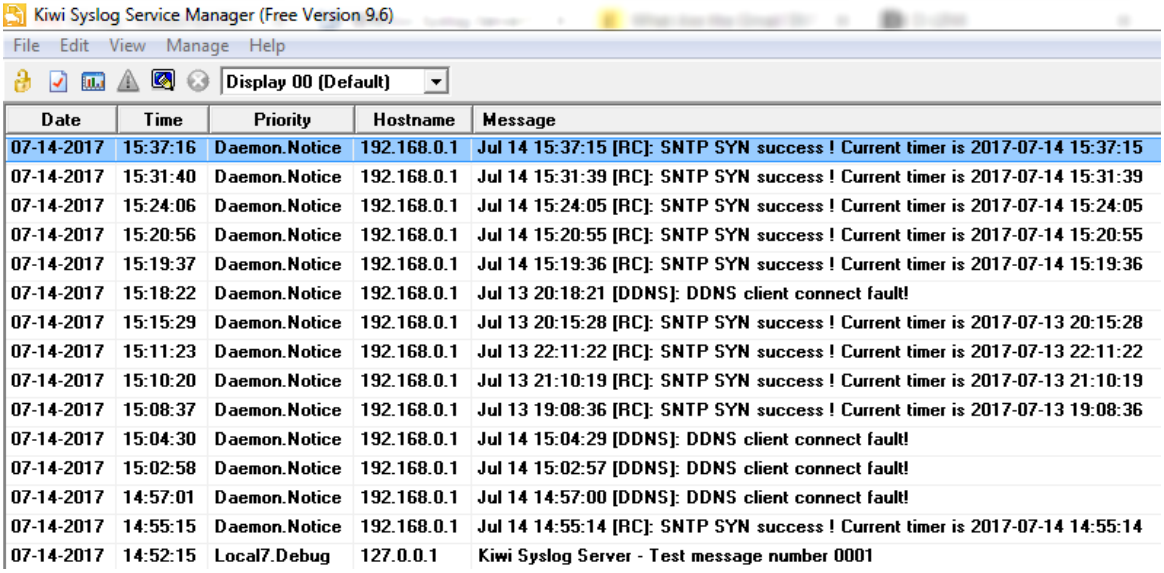
Step 2: Click **File** -> **Setup**, and fill in the IP address of your network device, then click **Add**:



Step 3: Enable "Enable Logging to Syslog Server", and fill in the IP address of the PC installing Kiwi Syslog Server:



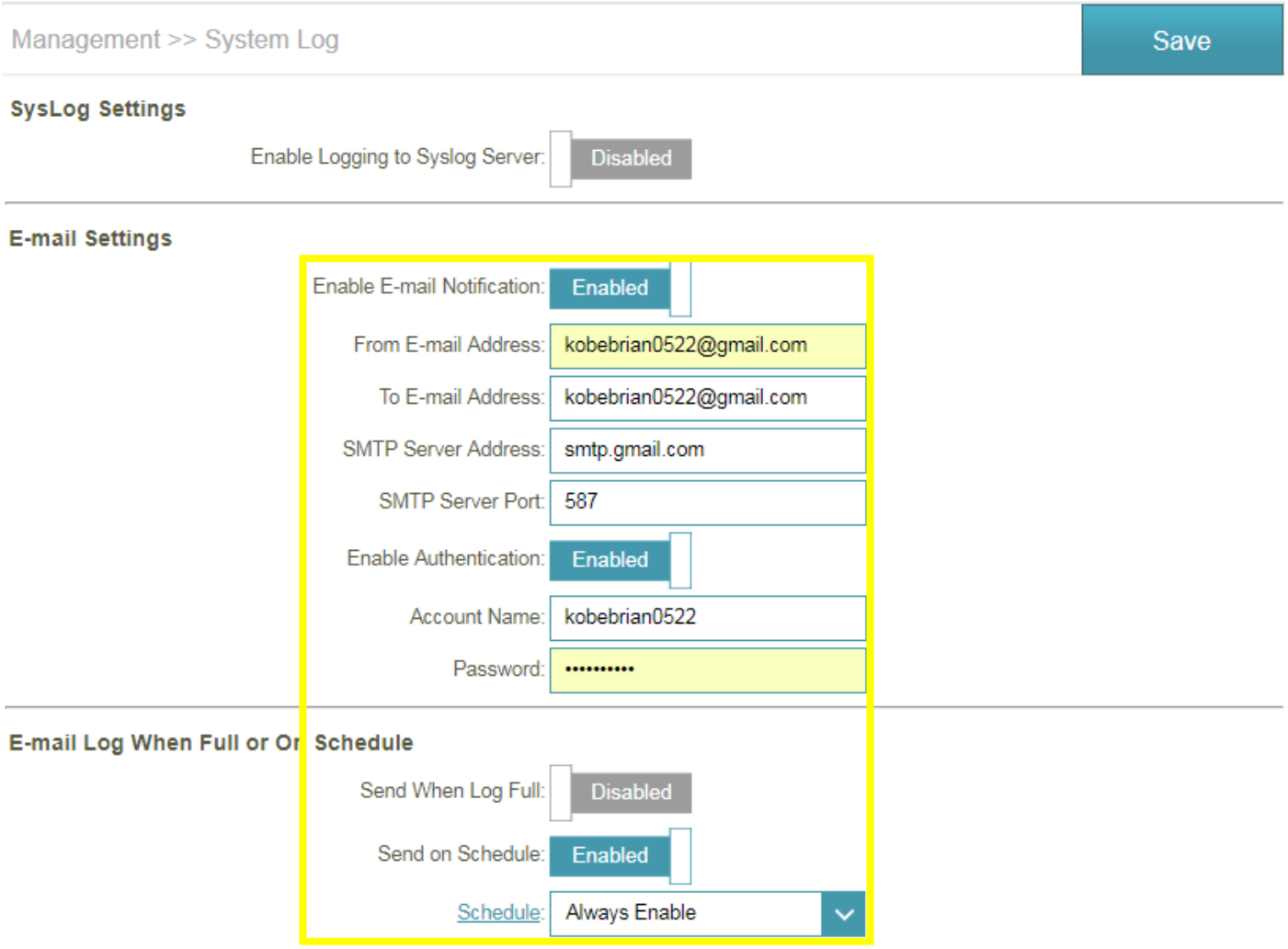
Step 4: You'll be able to check the log in Kiwi Syslog Service Manager as below:



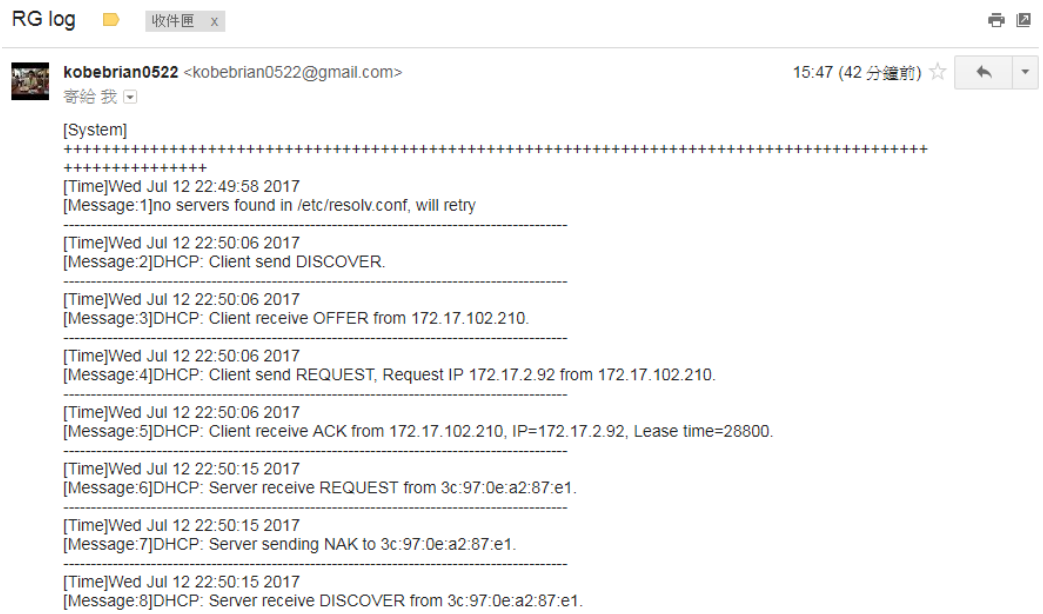
Date	Time	Priority	Hostname	Message
07-14-2017	15:37:16	Daemon.Notice	192.168.0.1	Jul 14 15:37:15 [RC]: SNTP SYN success ! Current timer is 2017-07-14 15:37:15
07-14-2017	15:31:40	Daemon.Notice	192.168.0.1	Jul 14 15:31:39 [RC]: SNTP SYN success ! Current timer is 2017-07-14 15:31:39
07-14-2017	15:24:06	Daemon.Notice	192.168.0.1	Jul 14 15:24:05 [RC]: SNTP SYN success ! Current timer is 2017-07-14 15:24:05
07-14-2017	15:20:56	Daemon.Notice	192.168.0.1	Jul 14 15:20:55 [RC]: SNTP SYN success ! Current timer is 2017-07-14 15:20:55
07-14-2017	15:19:37	Daemon.Notice	192.168.0.1	Jul 14 15:19:36 [RC]: SNTP SYN success ! Current timer is 2017-07-14 15:19:36
07-14-2017	15:18:22	Daemon.Notice	192.168.0.1	Jul 13 20:18:21 [DDNS]: DDNS client connect fault!
07-14-2017	15:15:29	Daemon.Notice	192.168.0.1	Jul 13 20:15:28 [RC]: SNTP SYN success ! Current timer is 2017-07-13 20:15:28
07-14-2017	15:11:23	Daemon.Notice	192.168.0.1	Jul 13 22:11:22 [RC]: SNTP SYN success ! Current timer is 2017-07-13 22:11:22
07-14-2017	15:10:20	Daemon.Notice	192.168.0.1	Jul 13 21:10:19 [RC]: SNTP SYN success ! Current timer is 2017-07-13 21:10:19
07-14-2017	15:08:37	Daemon.Notice	192.168.0.1	Jul 13 19:08:36 [RC]: SNTP SYN success ! Current timer is 2017-07-13 19:08:36
07-14-2017	15:04:30	Daemon.Notice	192.168.0.1	Jul 14 15:04:29 [DDNS]: DDNS client connect fault!
07-14-2017	15:02:58	Daemon.Notice	192.168.0.1	Jul 14 15:02:57 [DDNS]: DDNS client connect fault!
07-14-2017	14:57:01	Daemon.Notice	192.168.0.1	Jul 14 14:57:00 [DDNS]: DDNS client connect fault!
07-14-2017	14:55:15	Daemon.Notice	192.168.0.1	Jul 14 14:55:14 [RC]: SNTP SYN success ! Current timer is 2017-07-14 14:55:14
07-14-2017	14:52:15	Local7.Debug	127.0.0.1	Kiwi Syslog Server - Test message number 0001

Method 3: E-mail Settings

Step 1: Setup the e-mail information as below:



Step 2: You will receive the log email:

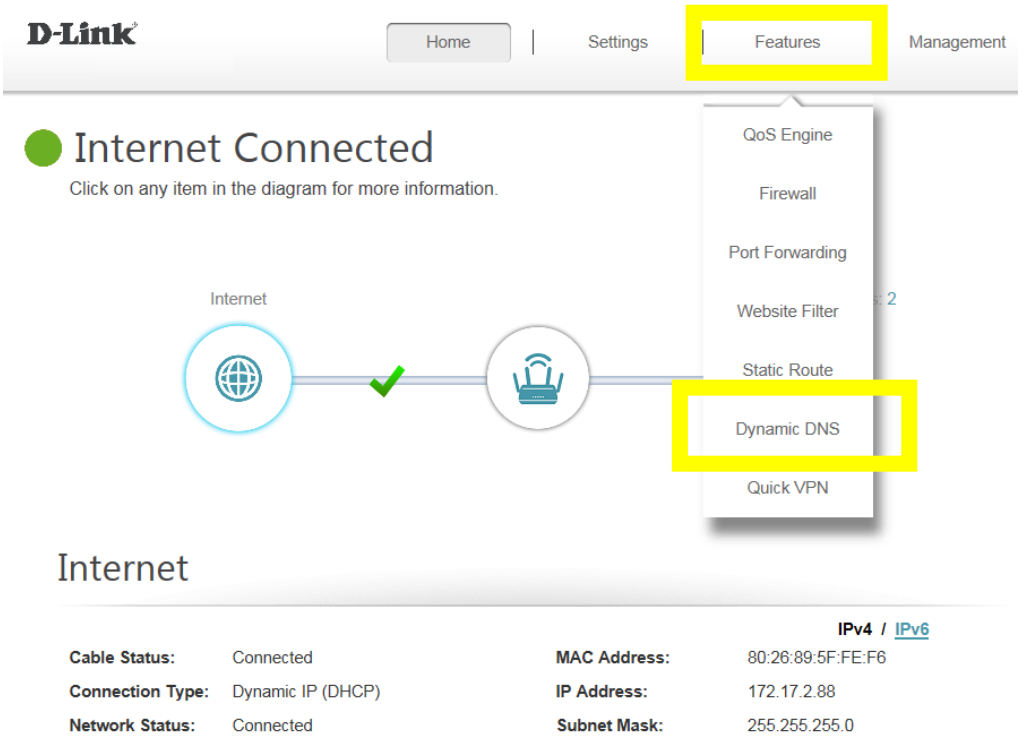


DNS/DDNS

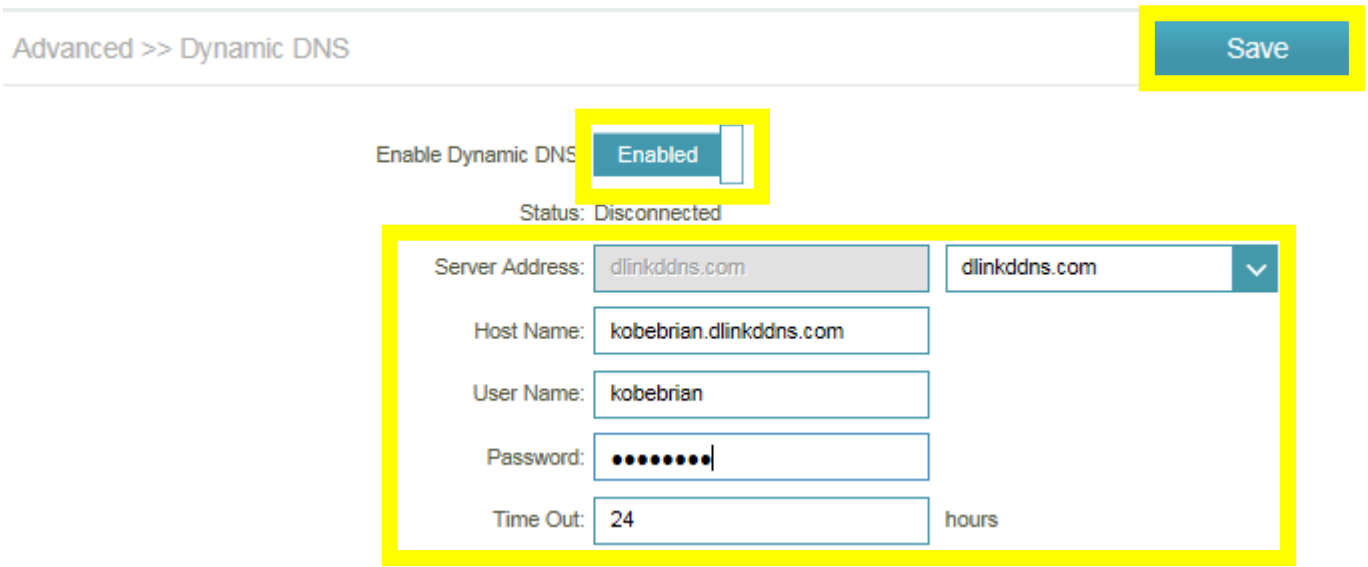
Q26: How do I configure Dynamic DNS on my router?

Please launch your browser and enter http://dlinkrouter.local or http://192.168.0.1 into the address bar. Then login and follow the steps below:

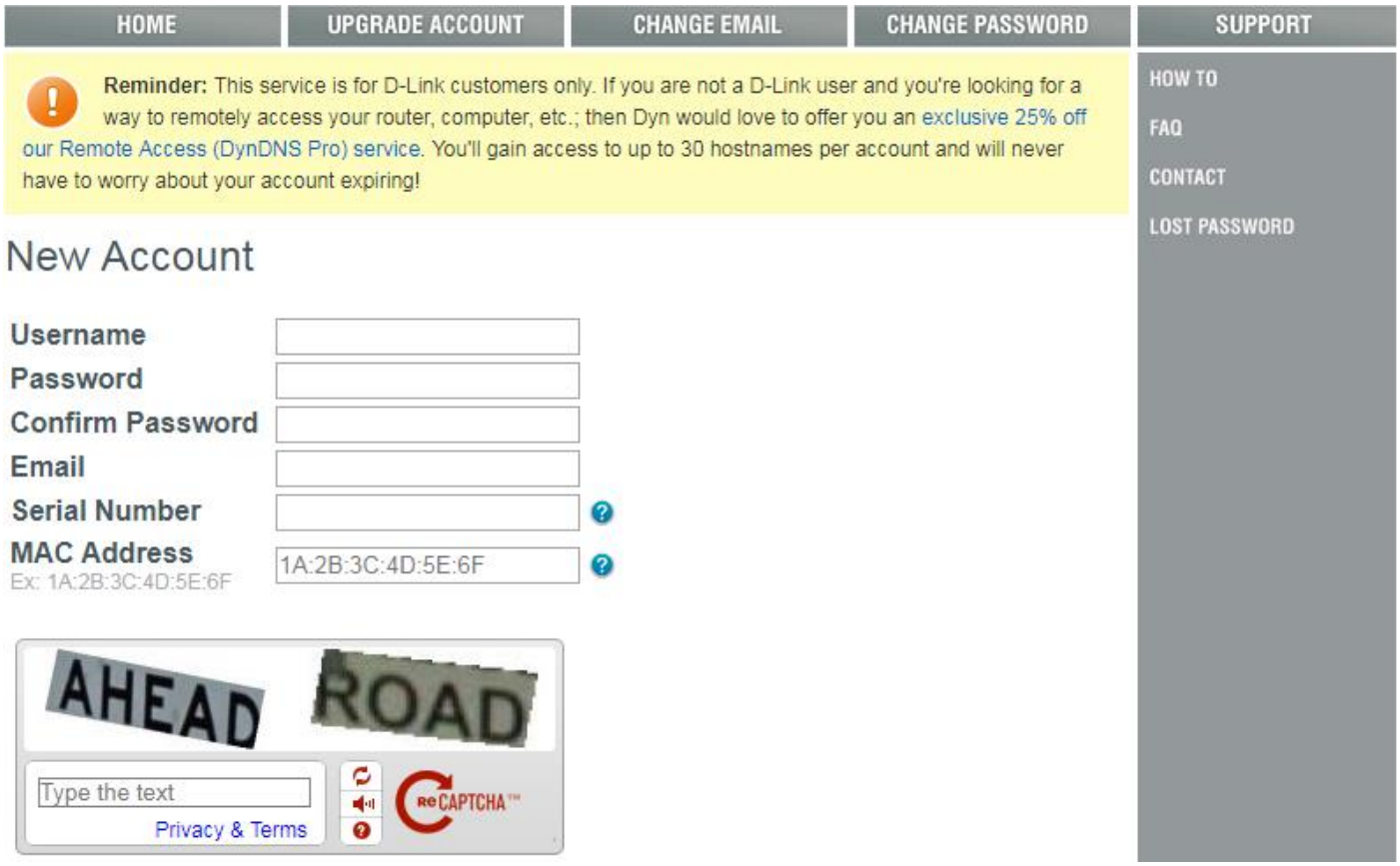
Step 1: Click **Features** -> **Dynamic DNS**



Step 2: Enable Dynamic DNS, and **enter your Dynamic DNS account information**, then **save**:



Note: To register to get the dlinkddns service, Please enter the website: https://www.dlinkddns.com/signin/, then fill in the required information.



Q27: Why am I unable to register my device with dlinkddns?

When validating your D-Link device with dlinkddns, you may receive an "**Unknown Serial Number/Unknown MAC Address**" error.

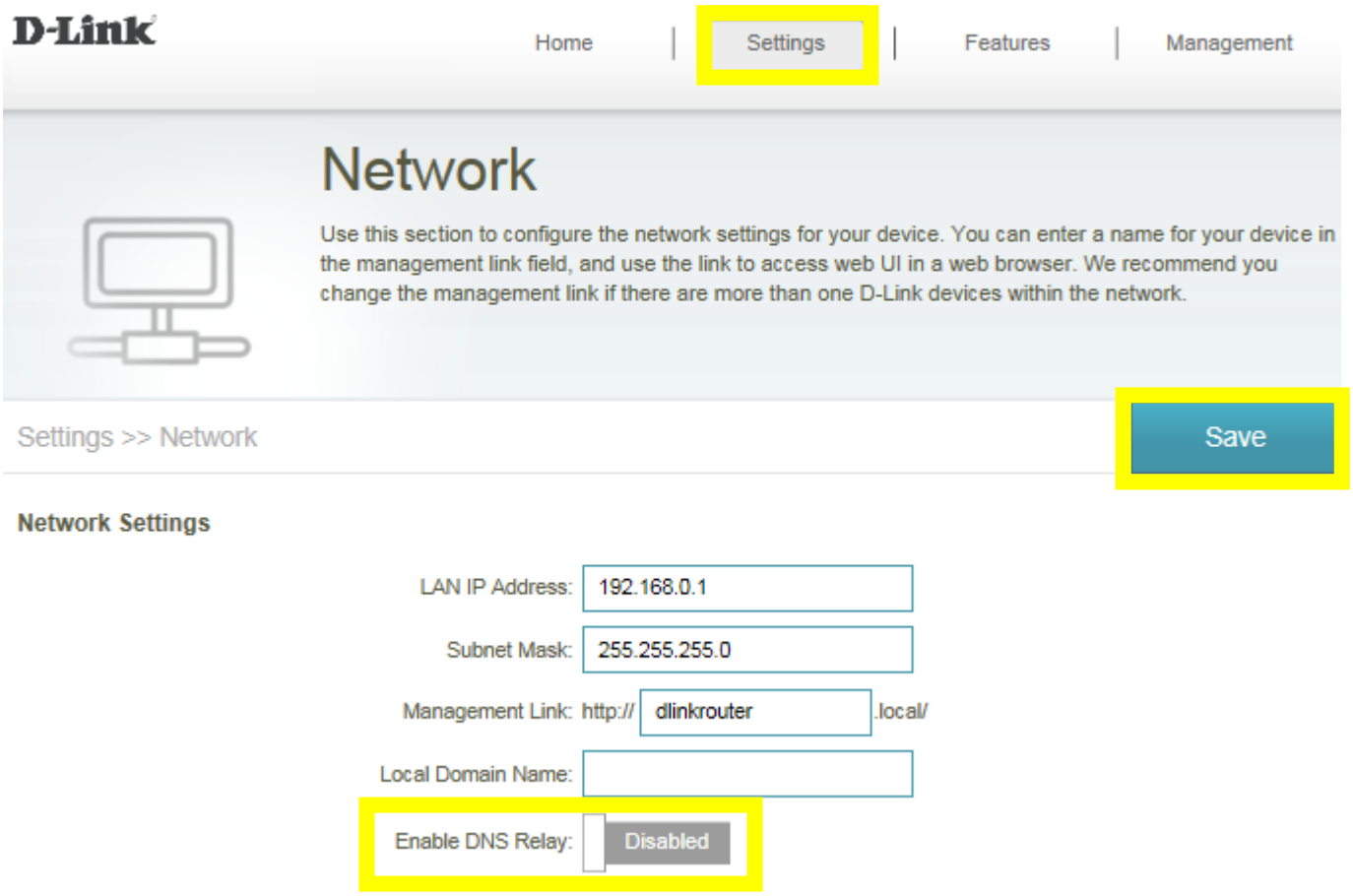
Please confirm the information you are entering is correct. You can find the needed information on the product label of the back/bottom of the router/device.
Note: When entering the MAC address, you **MUST** enter it in the following format, including colons, **e.g. 12:34:56:78:91:01**

Q28: How do I disable DNS relay?

If enabling DNS relay, your computers will use the router for a DNS server.

Please launch your browser and enter http://dlinkrouter.local or http://192.168.0.1 into the address bar. Then login and follow the steps below:

Step 1: Click **Settings ->** **Network**, and click to disable DNS Relay, then click **Save.**

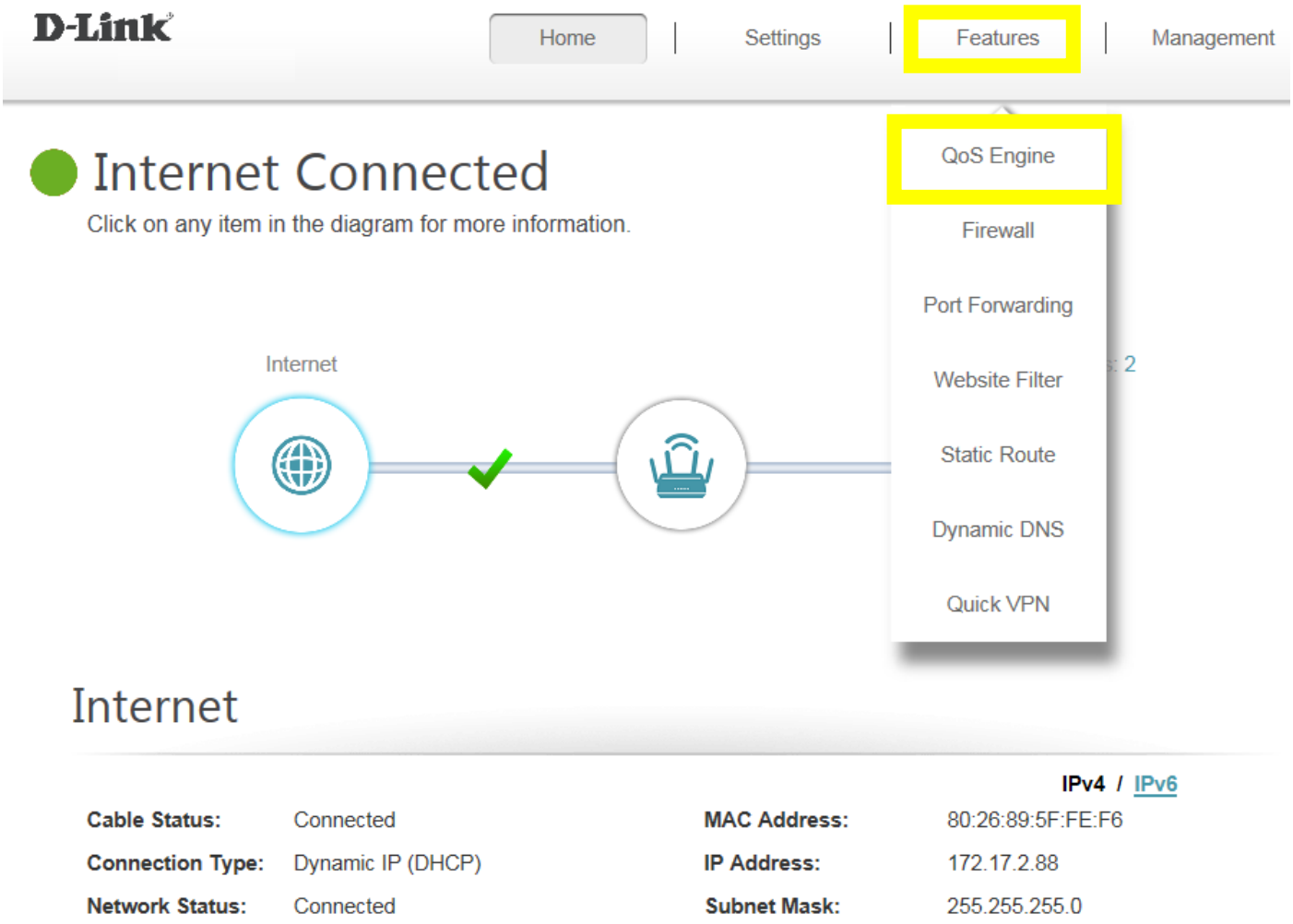


QoS Setting

Q29: How do I configure QoS on my router?

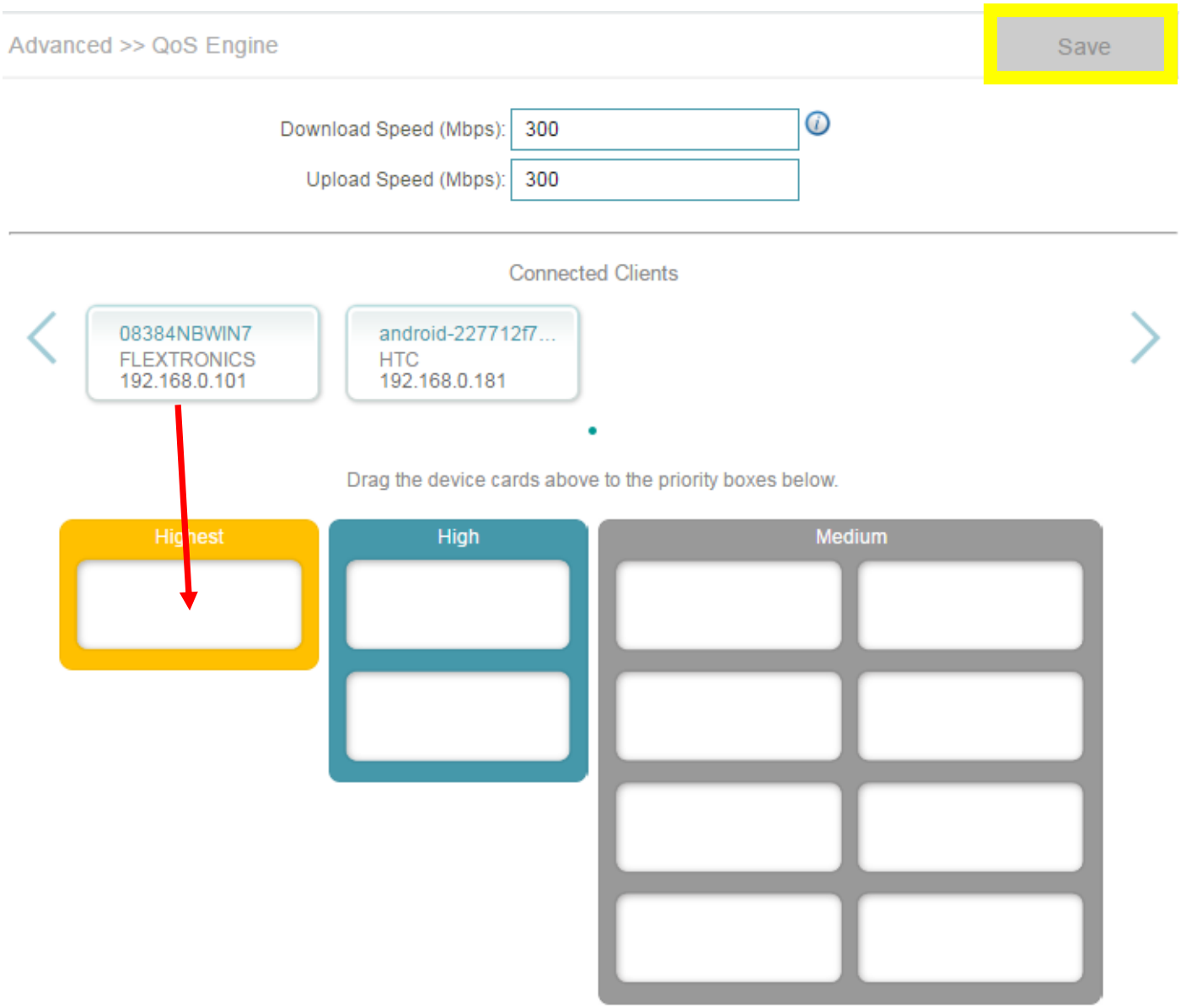
Please launch your browser and enter http://dlinkrouter.local or http://192.168.0.1 into the address bar. Then login and follow the steps below:

Step 1: Click **Features** -> **QoS Engine**



Step 2: To assign a priority level to a device, drag the device card from the **Connected Clients** list to an empty slot and release the mouse button. The card will move to the priority slot. If you want to remove a priority assignment from a device and return it to the All Devices list, click the cross icon in the top right of the device card.

- A maximum of one device can be assigned **Highest** priority.
- A maximum of two devices can be assigned **High** priority.
- A maximum of eight devices can be assigned **Medium** priority.

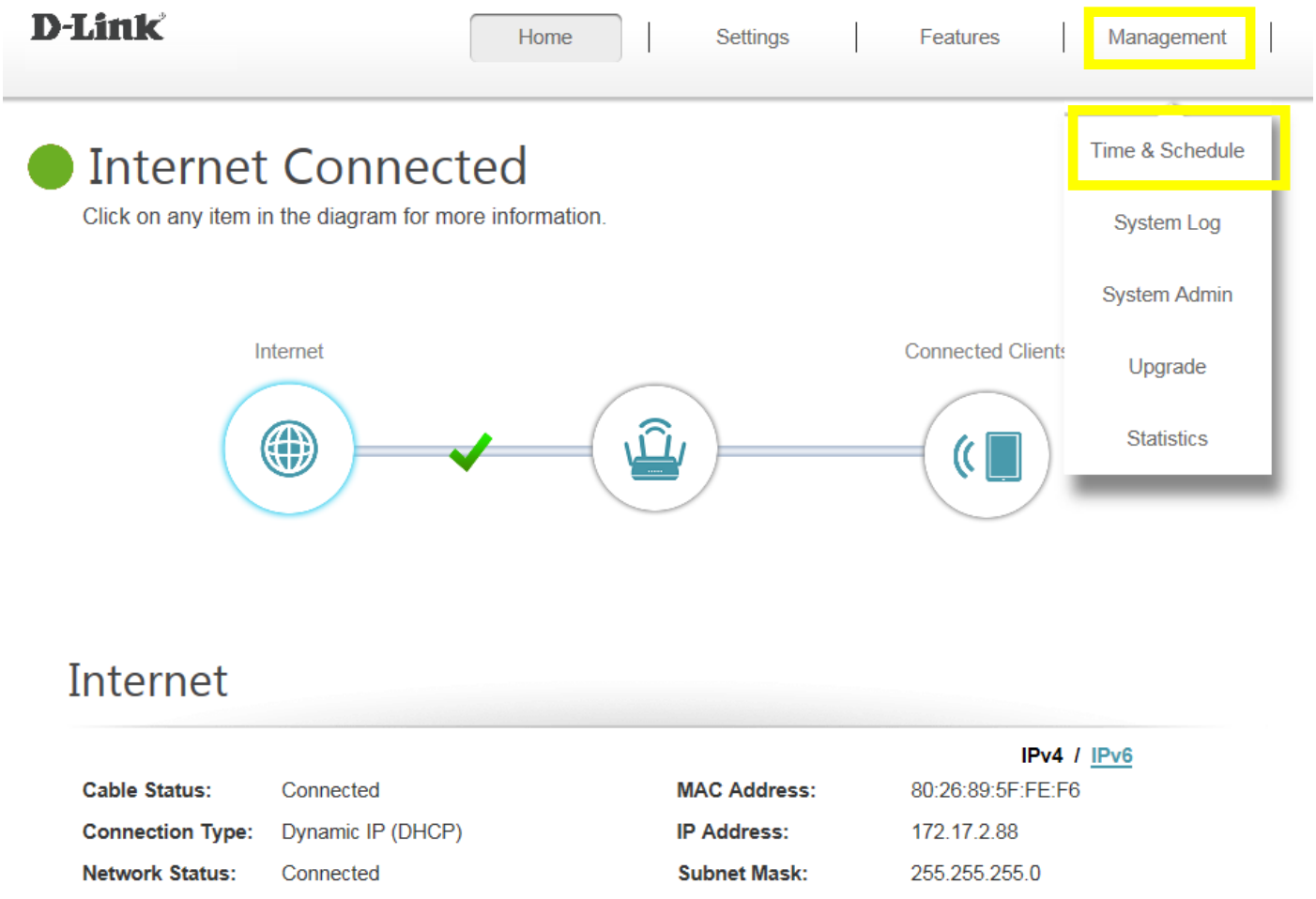


Time/Schedule

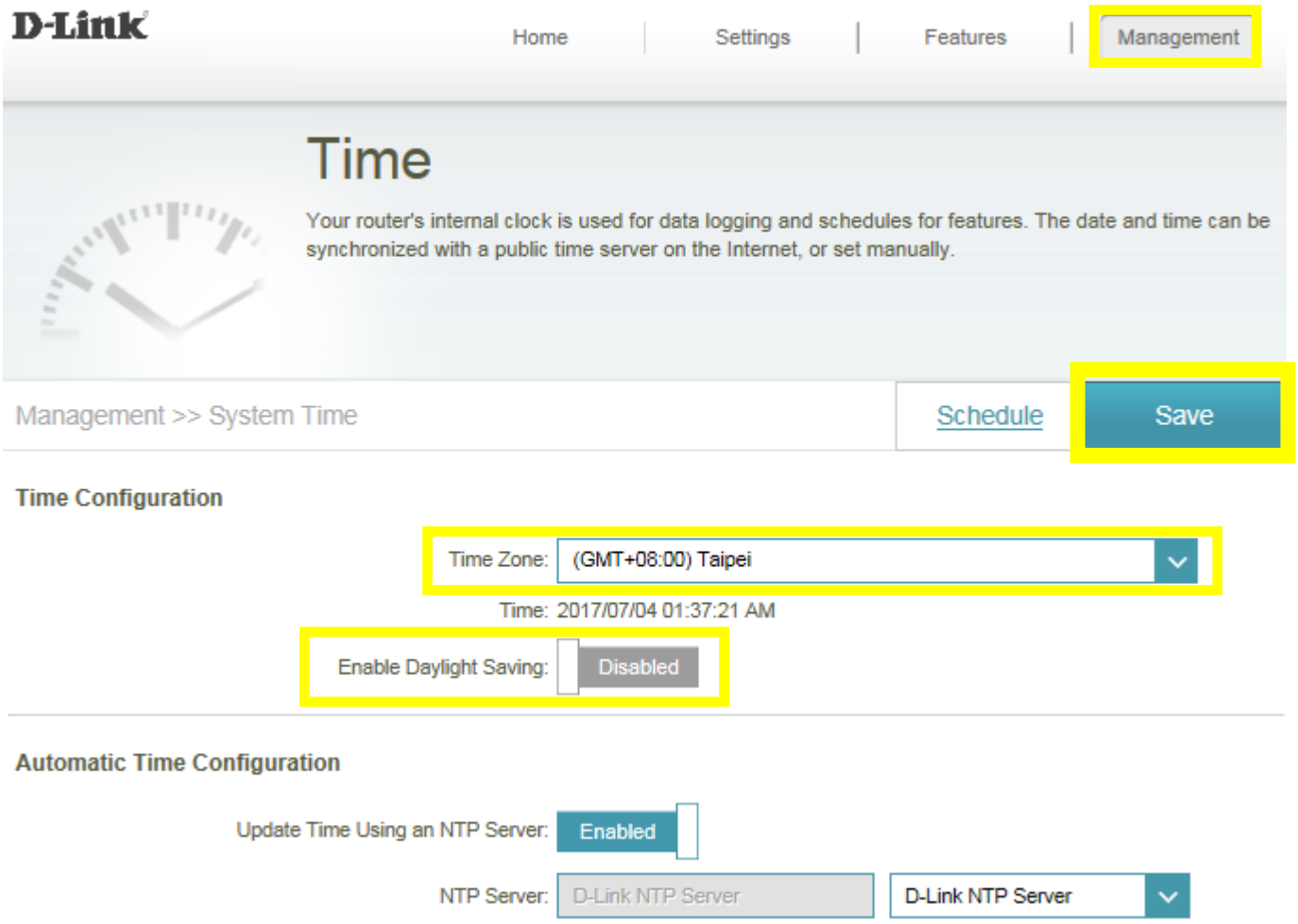
Q30: How do I configure the time on my router?

Please launch your browser and enter http://dlinkrouter.local or http://192.168.0.1 into the address bar. Then login and follow the steps below:

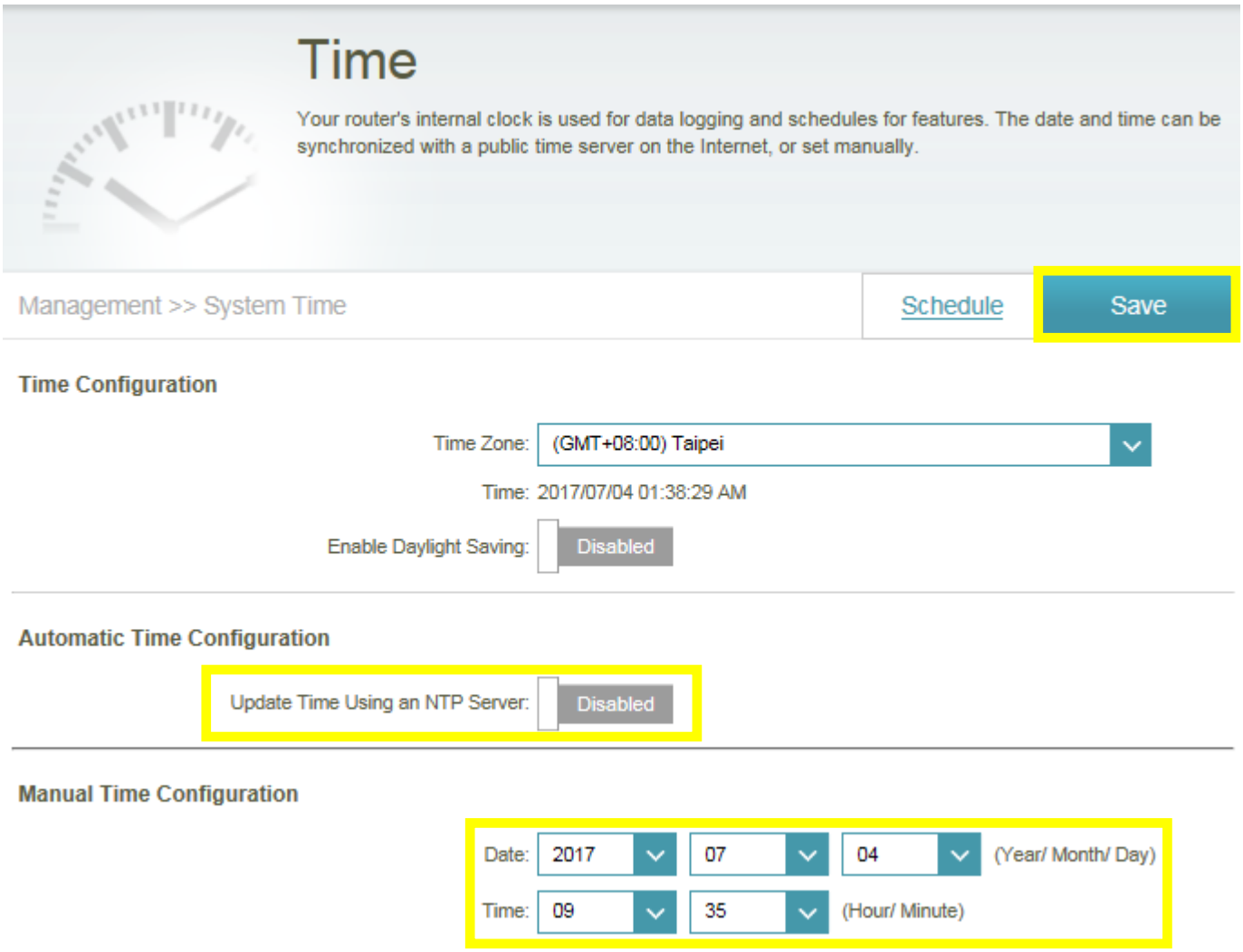
Step 1: Click on the **Maintenance** -> **Time & Schedule**



Step 2: By default, the D-Link NTP server is enabled. Specify the Time Zone if you need to synchronize the time with the specific region, and enable daylight saving if required, and click **Save**.



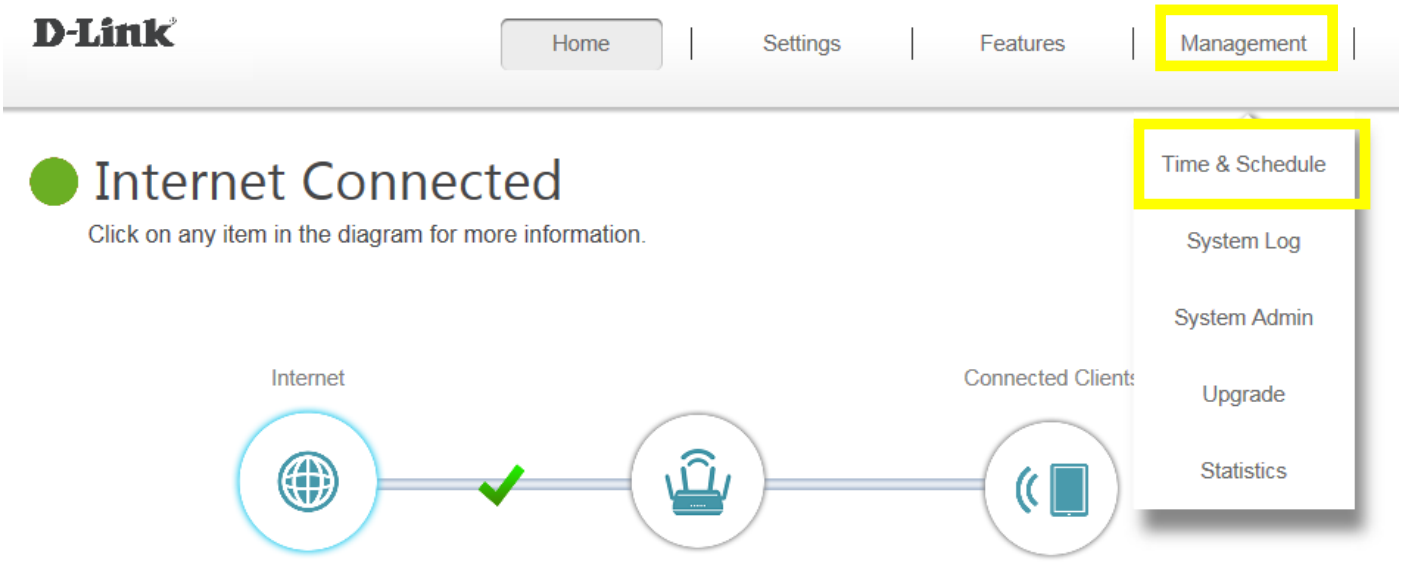
Note: To manually specify the time, change the automatic time configuration to **Disabled**, then adjust time as needed and click **Save.**



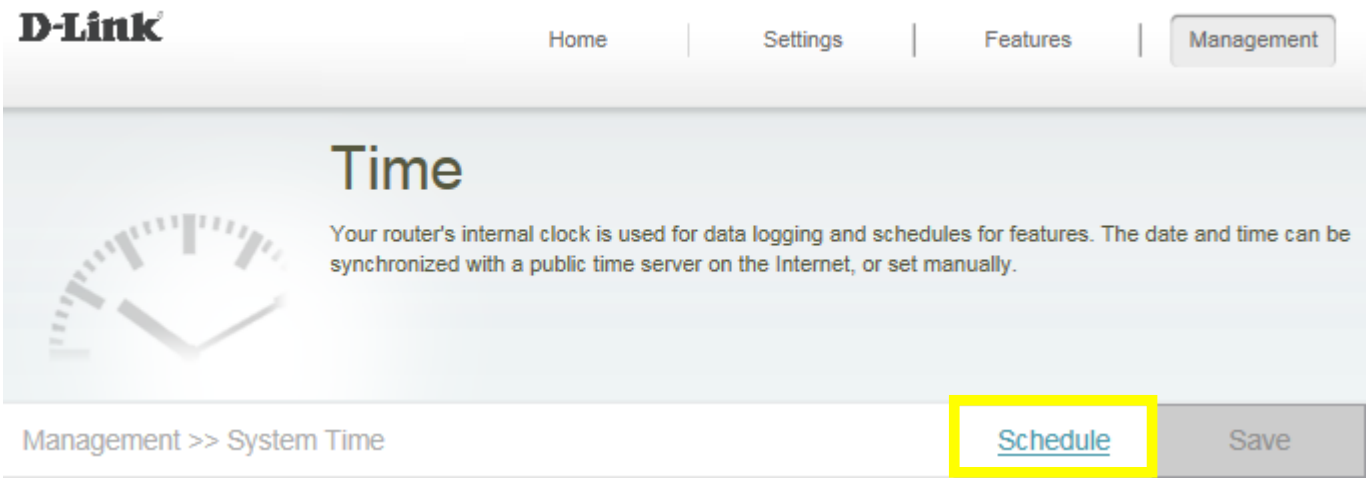
Q31: How do I create schedule on my router?

Please launch your browser and enter http://dlinkrouter.local or http://192.168.0.1 into the address bar. Then login and follow the steps below:

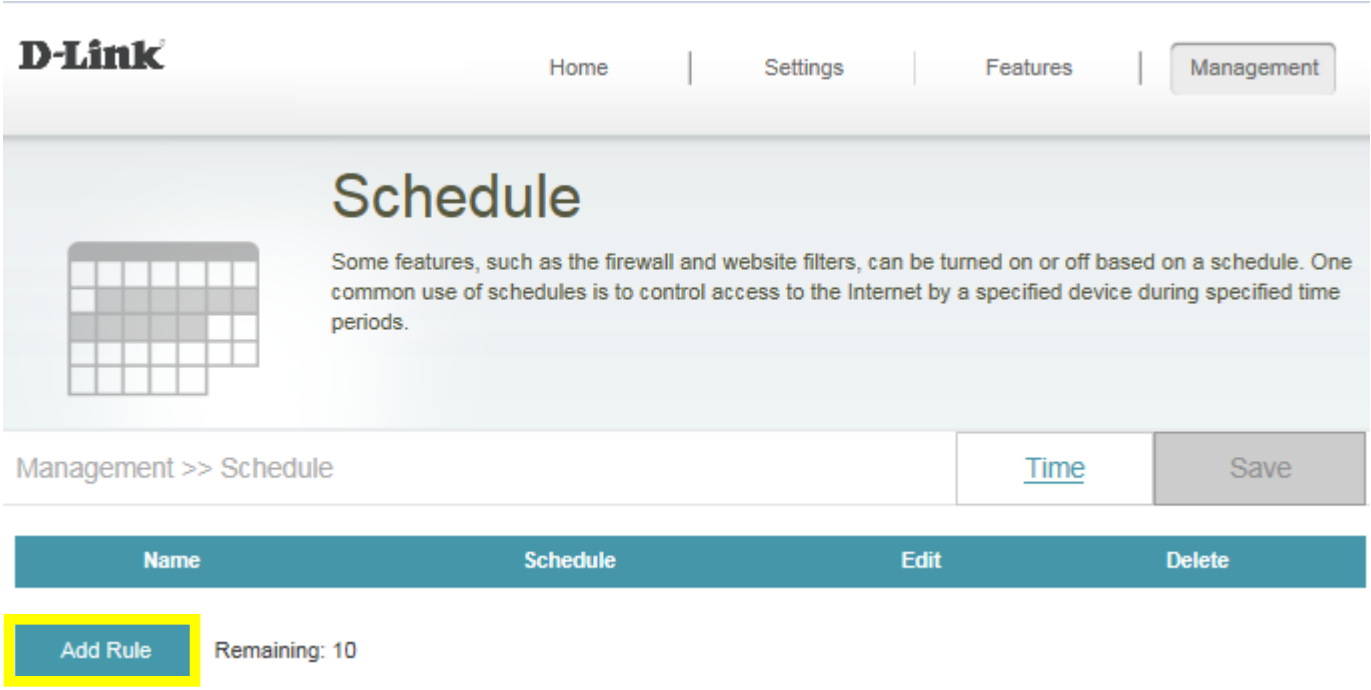
Step 1: Click on the **Maintenance** -> **Time & Schedule**



Step 2: Click **Schedule**:



Step 3: Click **Add Rule:**

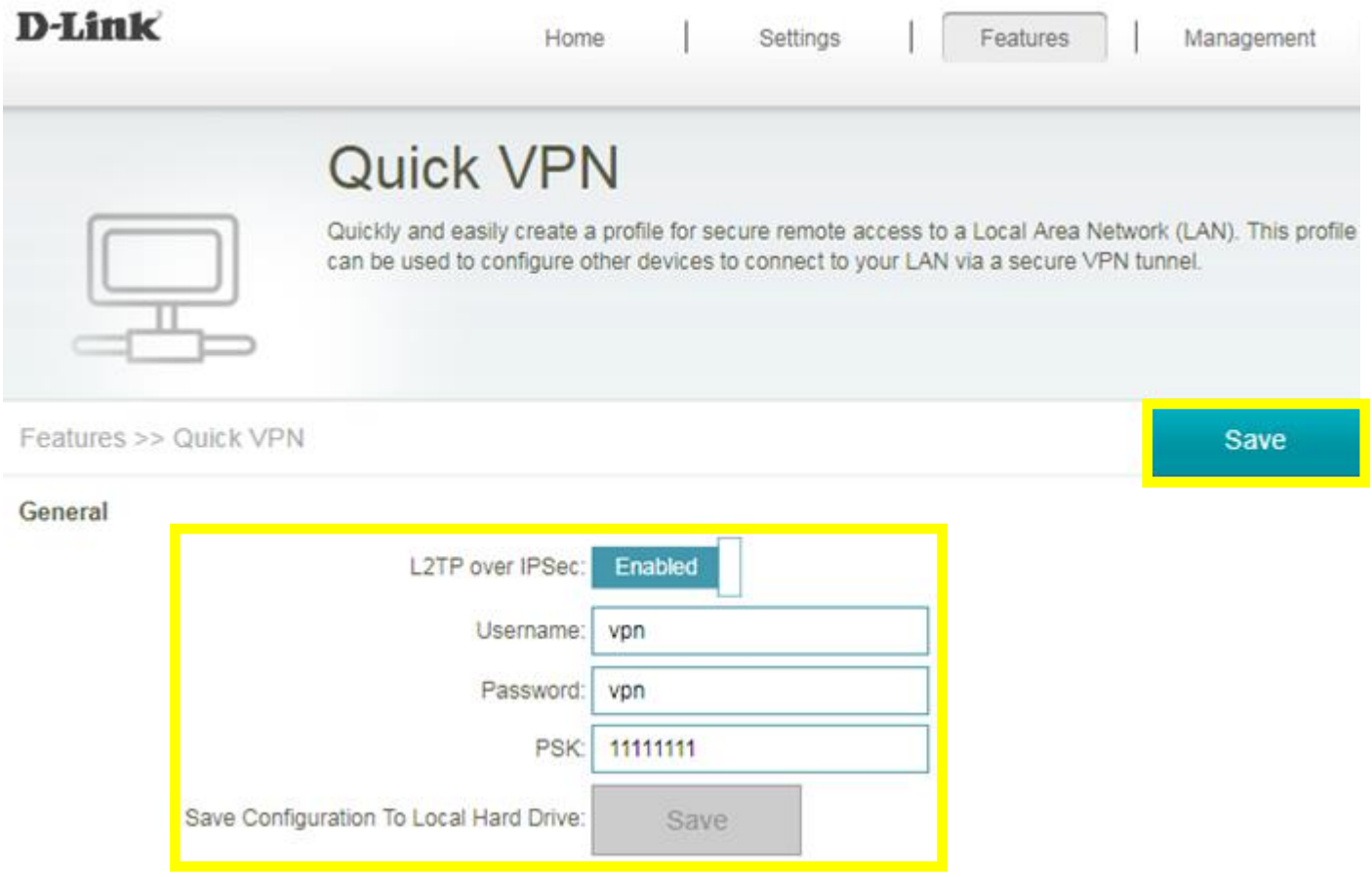


Step 4: Create your Schedule and click **Apply.** The example below shows the scheduled time from 8:00-19:00.

VPN Setting

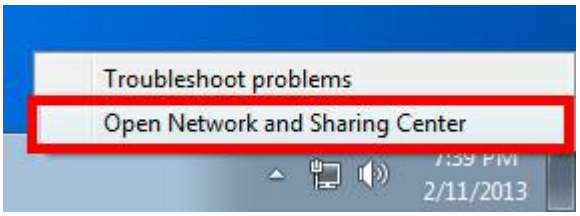
Q32: How to setup VPN connection?

First and foremost, please enable L2TP over IPSec, and setup Username/password/PSK to vpn/vpn/11111111, respectively:

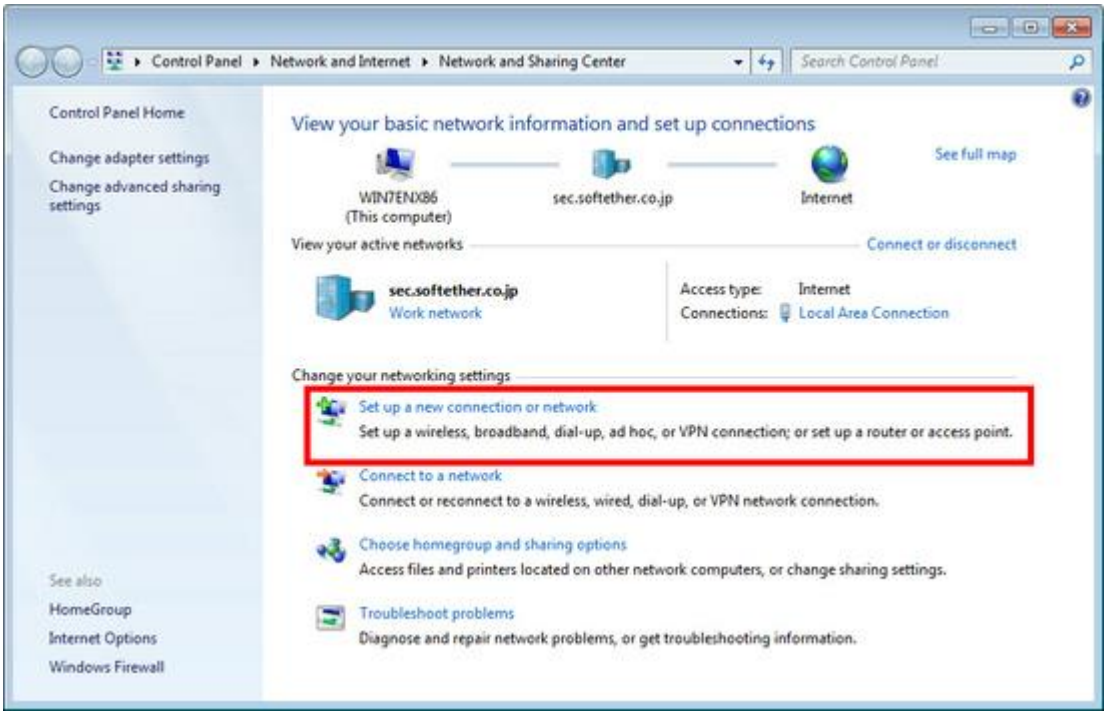


1. Windows client:

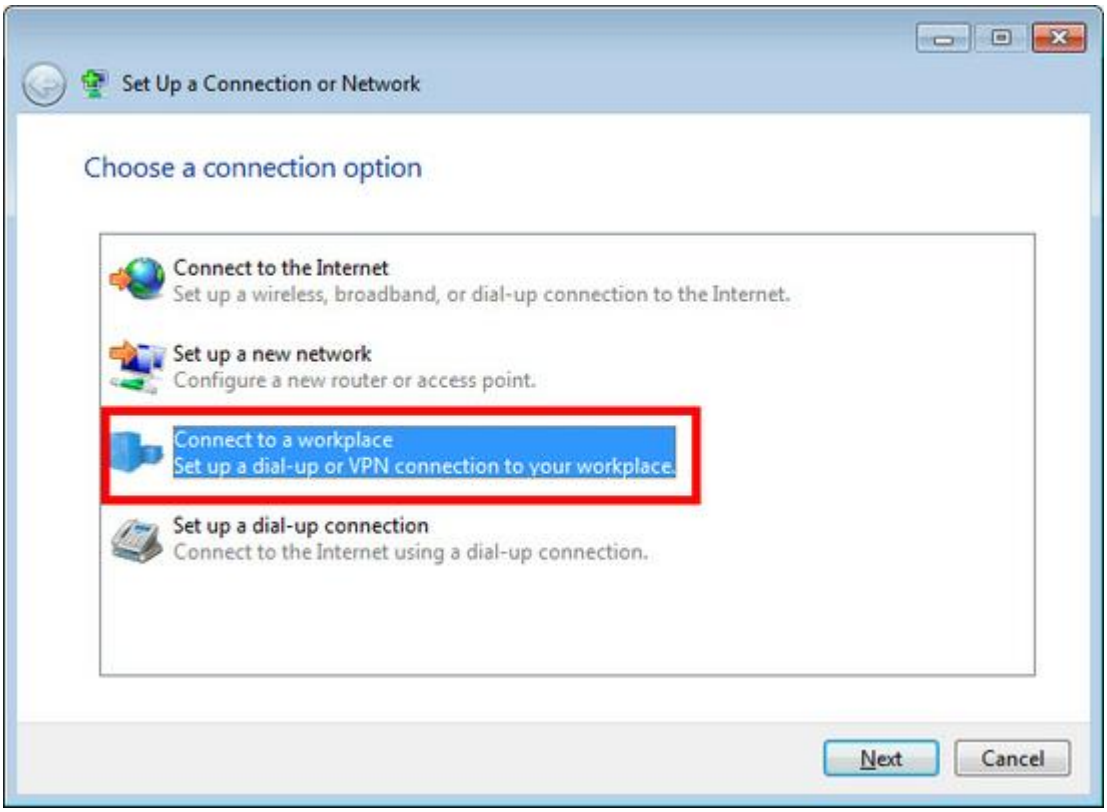
Step 1: Initial configurations (only once at the first time): Right-click the network icon on the bottom-right side of Windows screen, and click "Open Network and Sharing Center".



Step 2: Click "Set up a new connection or network" on the "Network Sharing Center":



Step 3: Select "Connect to a workplace":



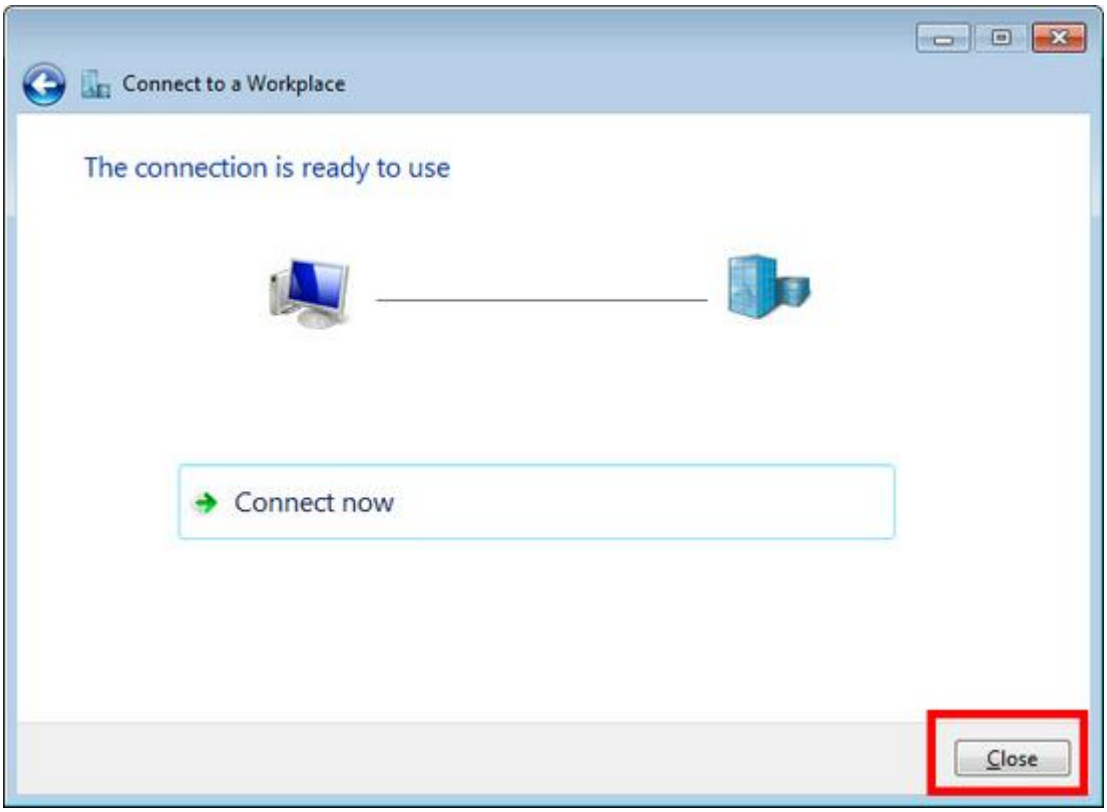
Step 4: Select "Use my Internet connection (VPN)":

Step 5: You have to input the destination SoftEther VPN Server's IP address or hostname here:

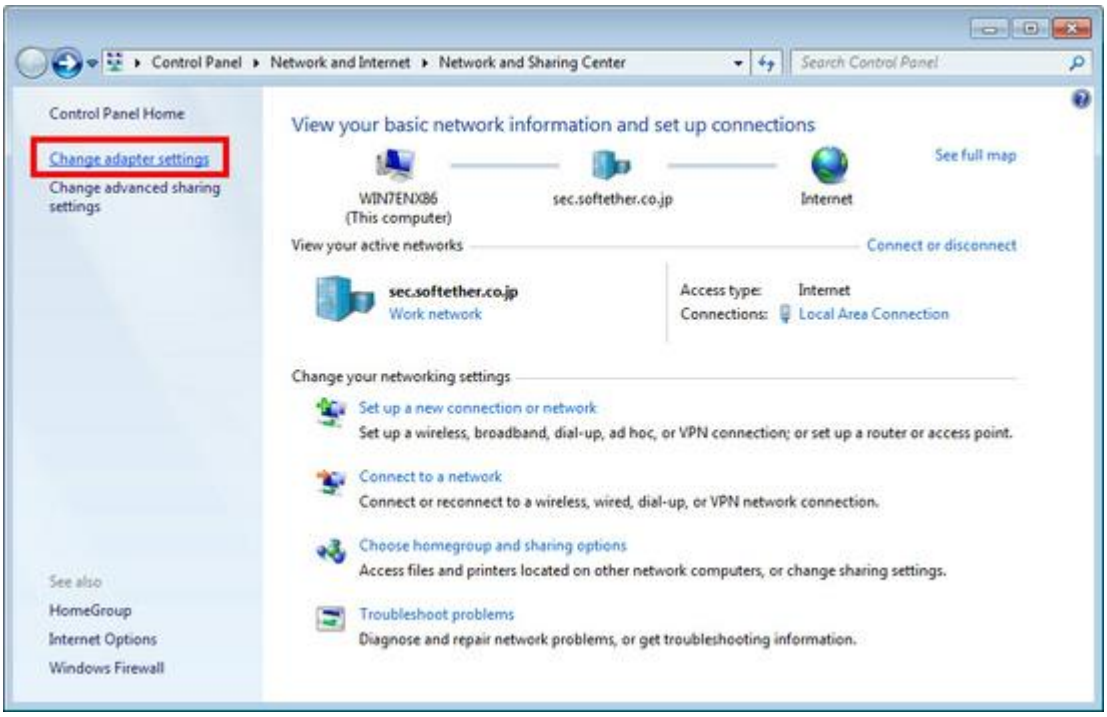
Enter either hostname or IP address on the "Internet address" field on the configuration wizard.

Step 6: Type your username and password you set on the router:

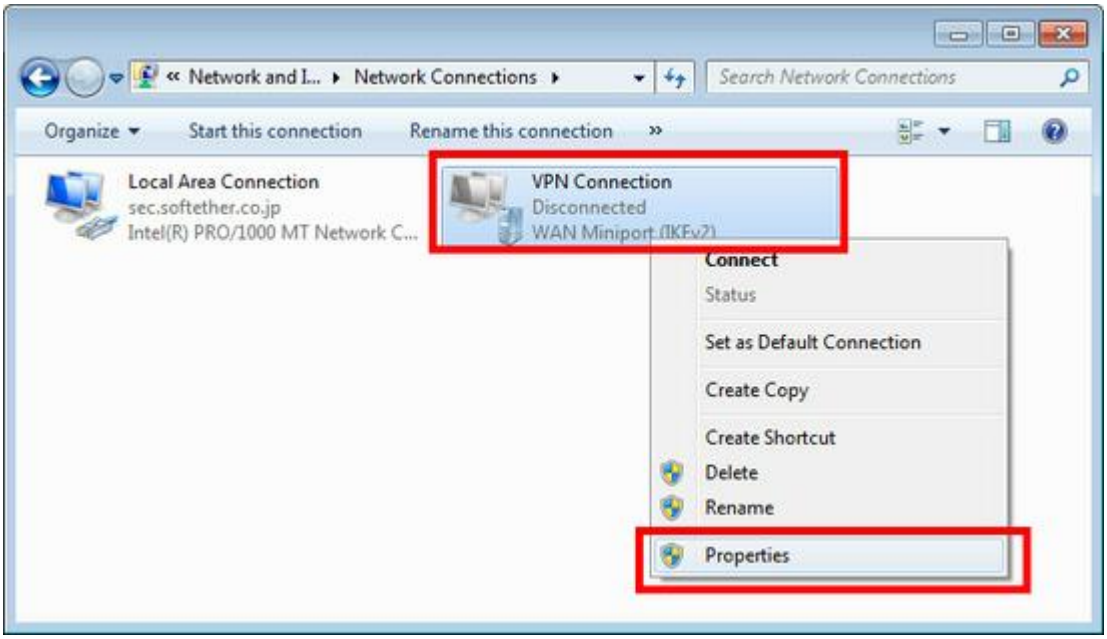
Step 7: When "The connection is ready to use" message appears, click the "**Close**" button. Do not click the "Connect now" button.



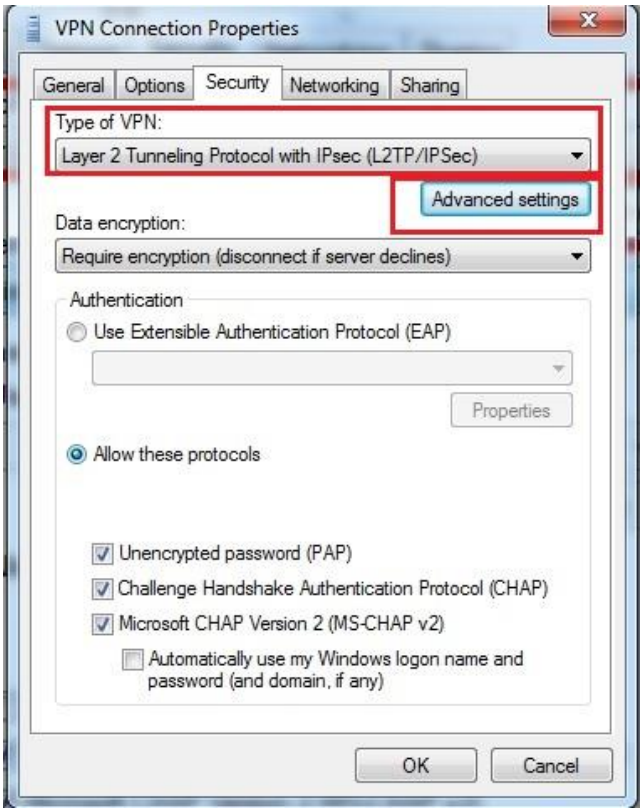
Step 8: Go to "Network and Sharing Center" and click "Change adapter settings":



Step 9: The currently defined VPN connection settings are listed. Right click the icon you created in the previous step, and click "Properties":



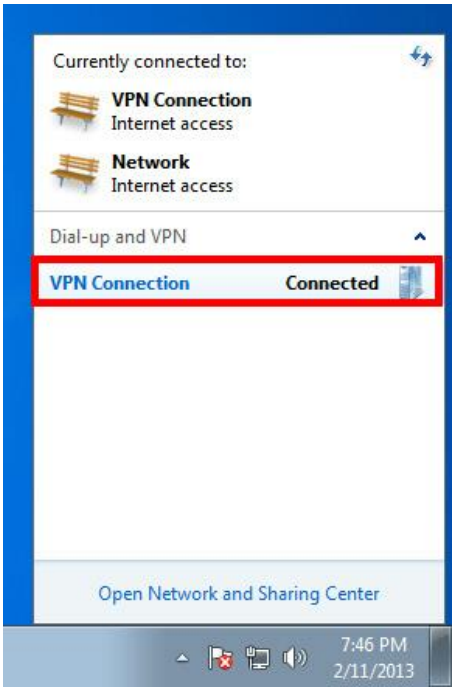
Step 10: On the Properties screen, switch to the "Security" tab. (In Windows XP, switch to the "Network" tab.) Choose "Layer 2 Tunneling Protocol with IPsec (L2TP/IPSec)" on the "Type of VPN" drop-down list.



The following screen will appear. Click "Use preshared key for authentication" and input the pre-shared key on the "Key" field.

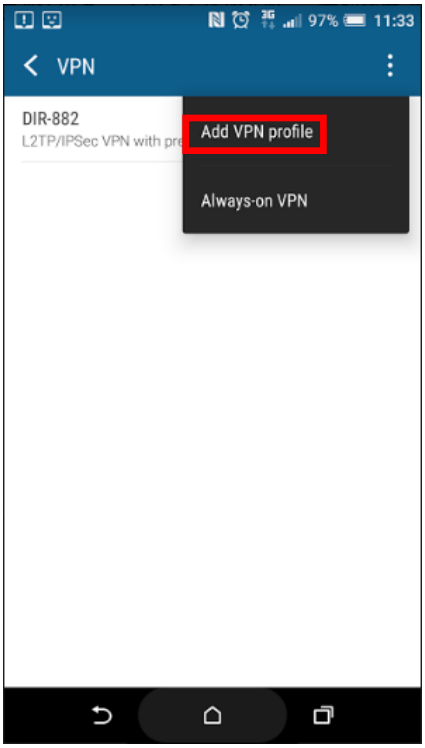
Step 11: Connect to the VPN Server: Double-click the created VPN connection setting, the below screen will appear. "User name" and "Password" fields should be filled automatically if you enable password-saving options in previous steps. If not, input both "User name" and "Password" fields. Click the "Connect" button to start the VPN connecting attempts.

Step 12: If the VPN connection is successfully established, a VPN connection icon will be listed on the screen which appears when you click the network icon on the bottom-right of Windows screen. The status of the VPN connection icon should be "Connected".

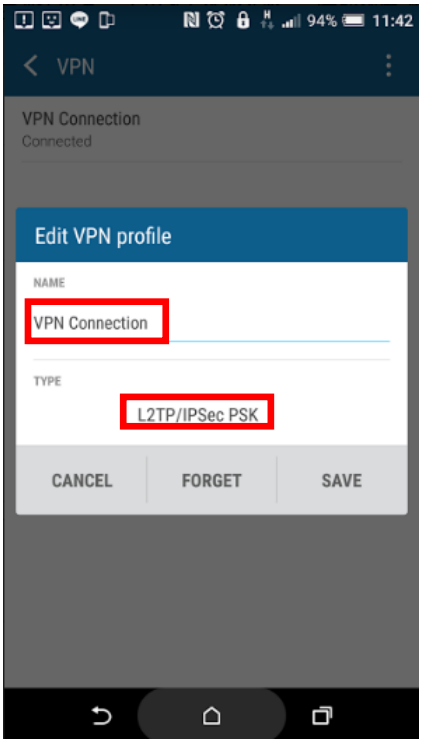


2. Mobile client (Android):

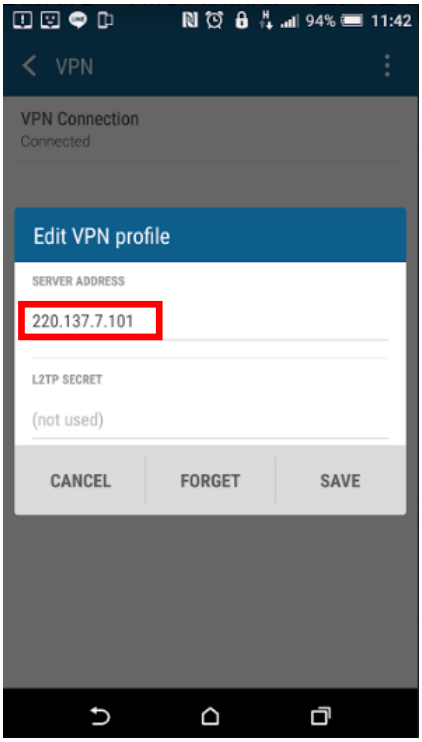
Step 1: Add new VPN profile:



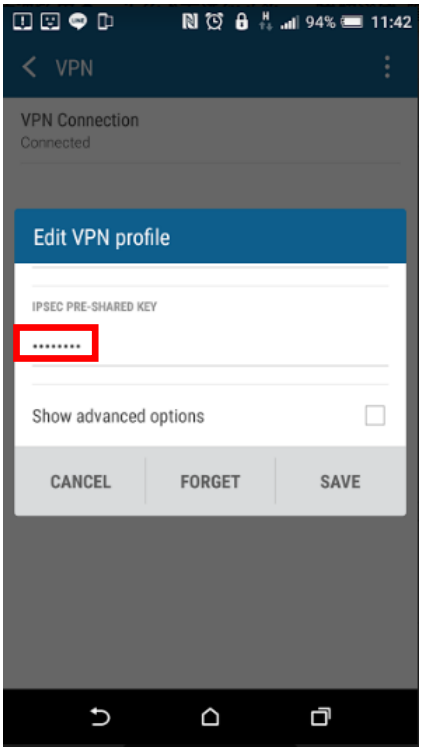
Step 2: Edit the name of VPN connection and select VPN type as **L2TP/IPSec PSK**:



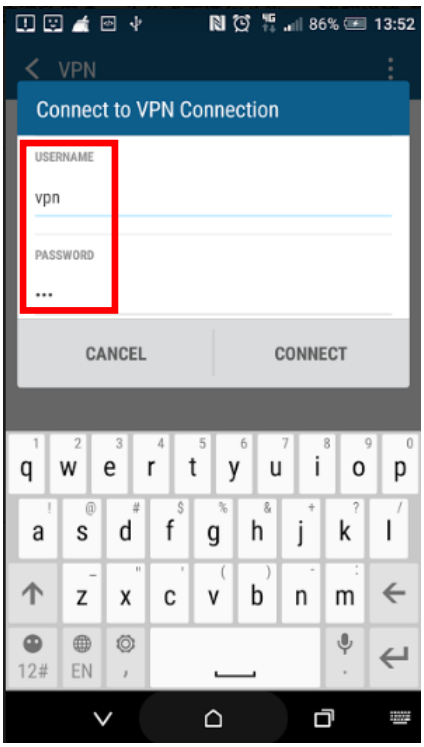
Step 3: Fill in the WAN IP address:

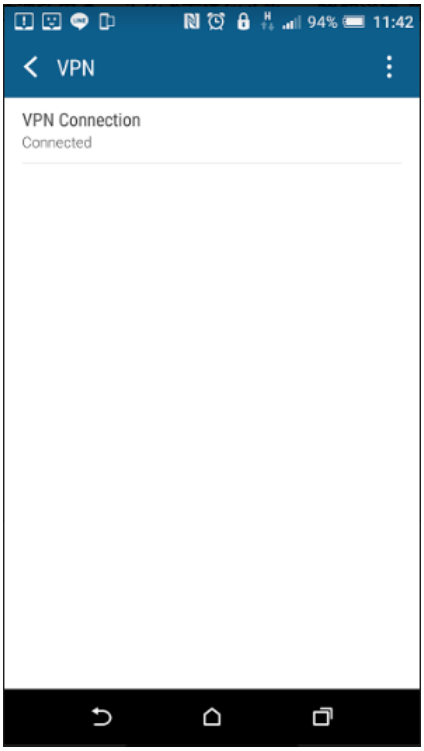


Step 4: Fill in the Pre-shared key:

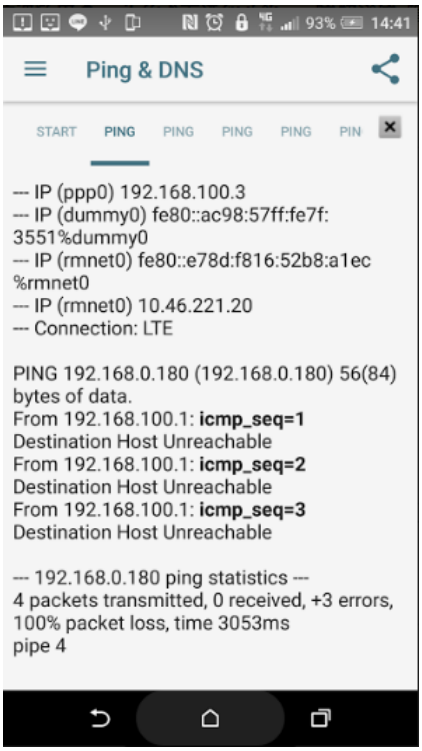


Step 5: Connect to your VPN server:





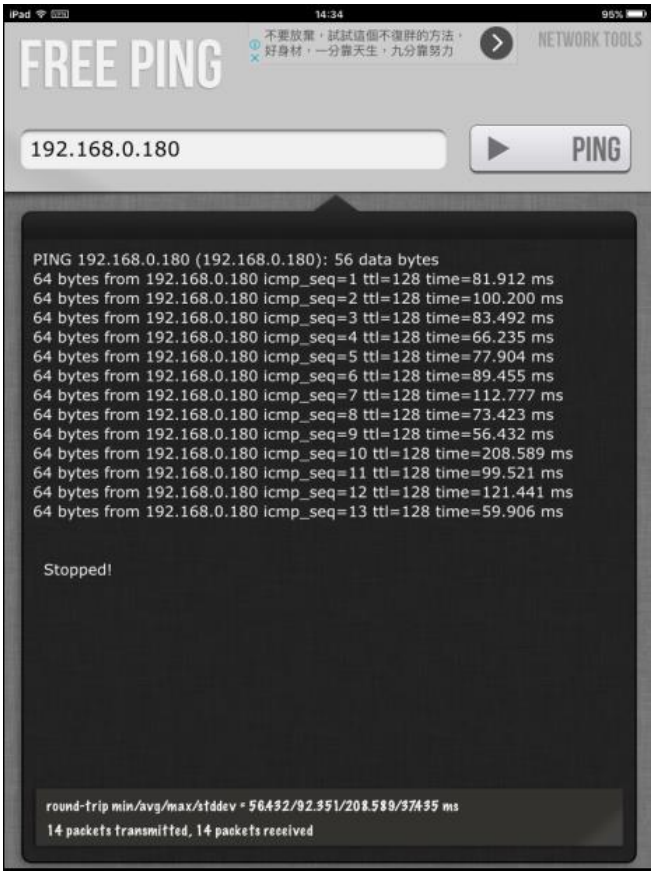
Step 6: Make sure if you can ping your client under DUT:



3. Mobile client (iOS):

Step 1: Setup the required information for VPN connection:

Step 2: Setup the required information for VPN connection:

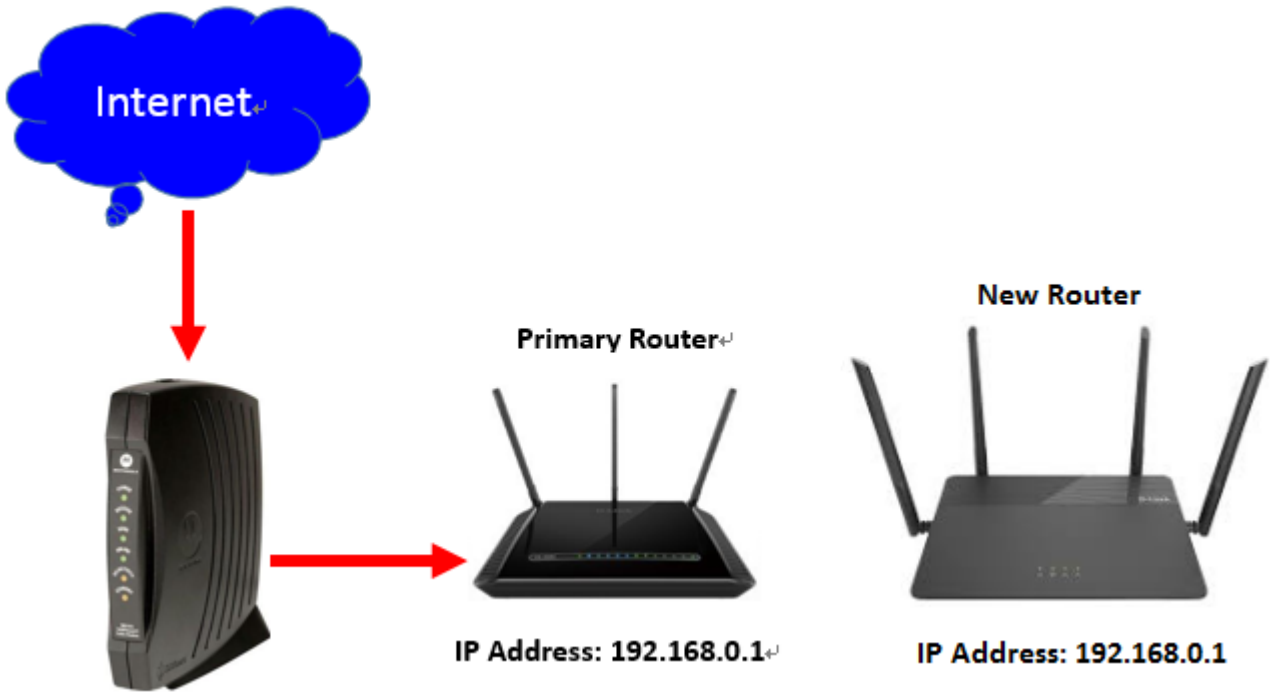


Advanced Application

Q33: How do I connect two routers together?

Connecting multiple routers together may be necessary if you have one of the following issues:

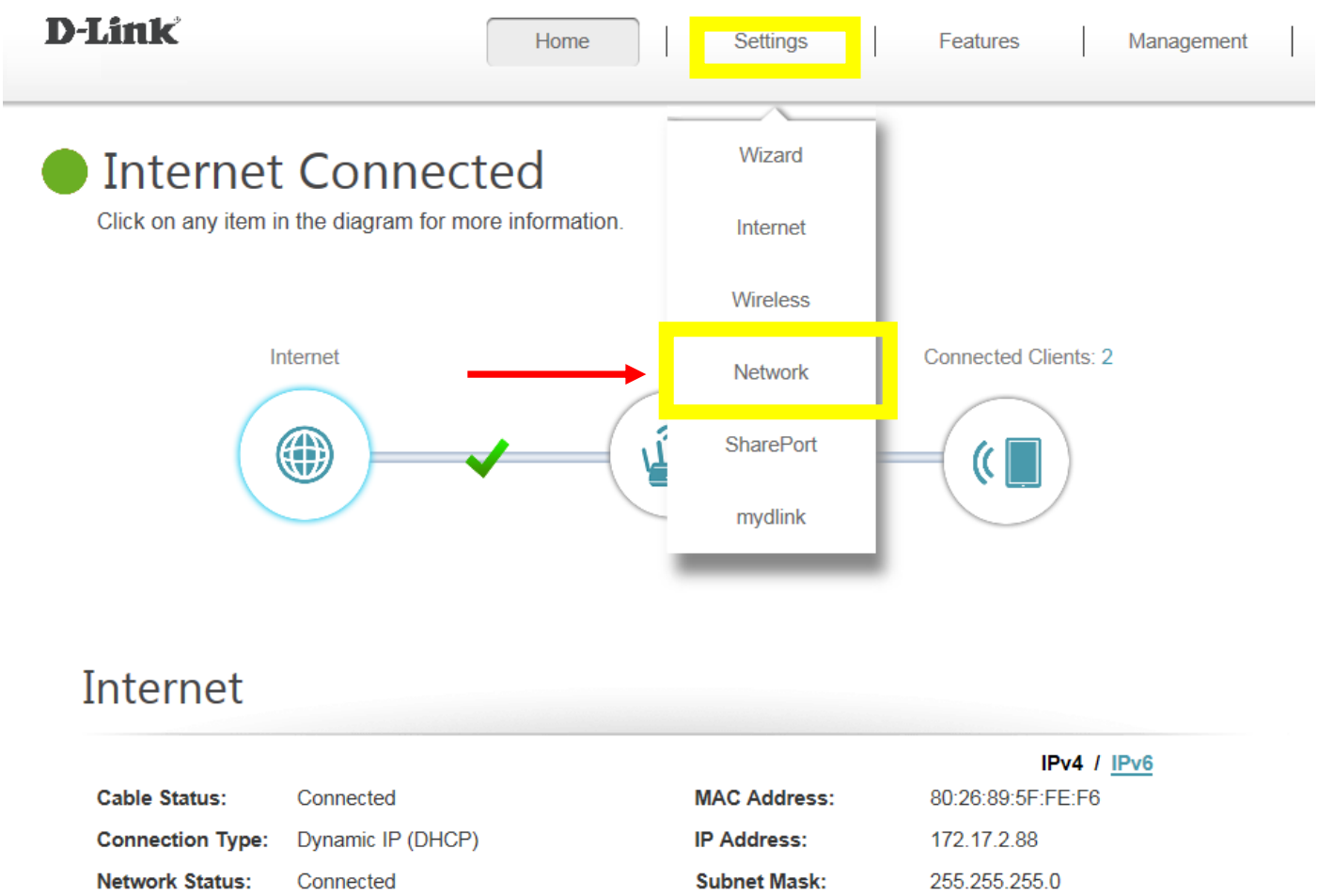
-Your Internet provider has provided you a Modem/Router (two in one) and you want to connect a new router to it.
-You want to expand the amount of Ethernet ports in your network (without a switch)
-You want to extend the range of the wireless signal in your home (by using the 2nd router as an access point)



Note: DO NOT Connect the routers together until these settings have been changed.

Please launch your browser and enter http://dlinkrouter.local or http://192.168.0.1 into the address bar. Then login and follow the steps below:

Step 1: Change the IP address to 192.168.0.2. Then, click advanced settings on the bottom right, and **Disable the DHCP Server**.



Settings >> Network

Save

Network Settings

LAN IP Address: 192.168.0.2

Subnet Mask: 255.255.255.0

Management Link: http:// dlinkrouter .local/

Local Domain Name:

Enable DNS Relay: Enabled

Advanced Settings...

DHCP Server

Status: Disabled

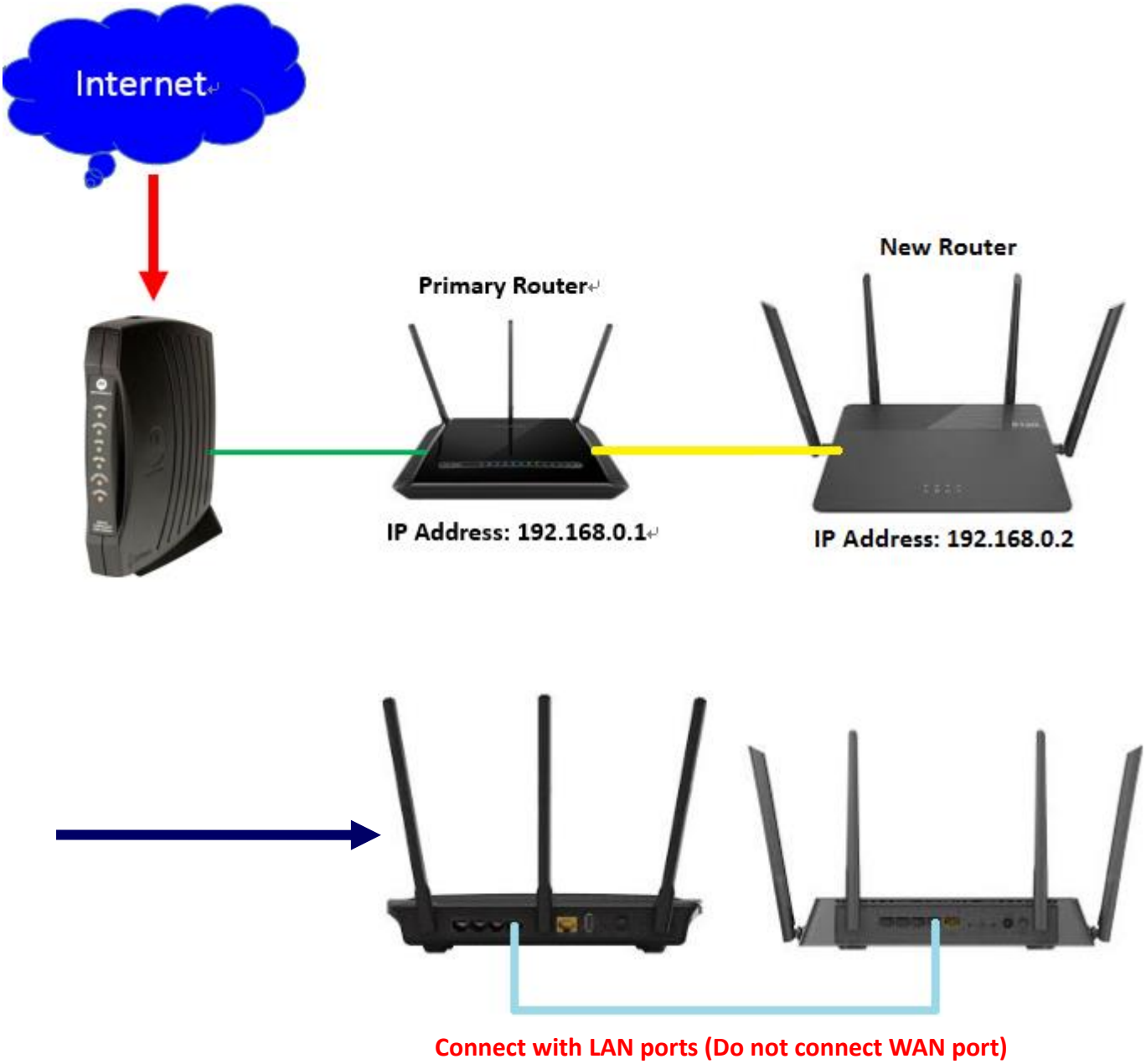
DHCP IP Address Range: 192.168.0. 100 to 192.168.0. 199

DHCP Lease Time: 10080 minutes

Always Broadcast: Disabled

(compatibility for some DHCP Clients)

Step 2: Connect a cable from a LAN port (1,2,3,4) on your Primary Router to a LAN port (1,2,3,4) on your new router.



The Setup is now complete. If you now want to configure the wireless settings on your "new" router, go to this address: http://192.168.0.2.

Note: NAT, defined in RFC 3022, allows a host that does not have a valid, registered, globally unique IP address to communicate with other hosts through the Internet. The hosts might be using private addresses or addresses assigned to another organization. In either case, NAT allows these addresses that are not Internet-ready to continue to be used and still allows communication with hosts across the Internet.