Given a scenario, install and configure SOHO wireless/wired router and apply appropriate settings: CompTIA A+ 220-901 sub-objective 2.6

Detailed (and official) description of CompTIA A+ sub-objective 2.6

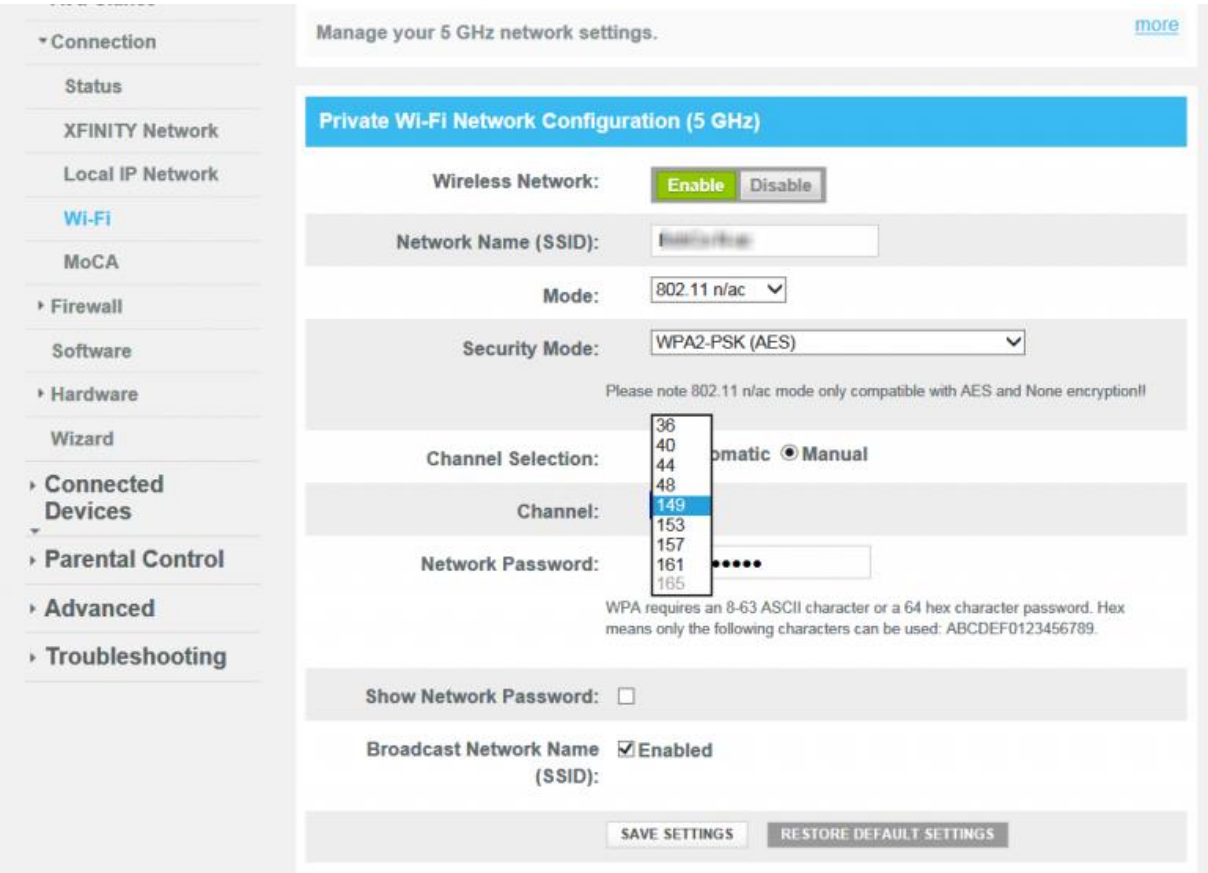
Sub objective 2.6: "Given a scenario, install and configure SOHO wireless/wired router and apply appropriate settings"

> Channels
> Port forwarding, port triggering
> DHCP (on/off)
> DMZ
> NAT / DNAT
> Basic QoS
> Firmware
> UPnP

Welcome to the CertBlaster ExamNotes. Today we'll look at CompTIA 220-901 sub-objective 2.6 which deals with the primary settings you would check and/or adjust on a Wireless router.

Channels

Much as you would set a car radio to your favorite channel the 802.11 family of wireless standards uses one channel to communicate. This channel is chosen by the network administrator in a business environment or the home user in a SOHO environment. As you will see the available channels are plentiful there are only between 1 and 3 channels that you can use in the 2.4 GHz band. We will focus mainly on the SOHO deployment here per the objectives. In the 5GHZ band there can be as many as 8. In the US 5GHZ band is subject to the Federal Communications Commission (FCC) restrictions limiting it to four channels in the lower end of the band (5.250–5.350 GHz) and five in the upper end of the band (5.470–5.725 GHz) .

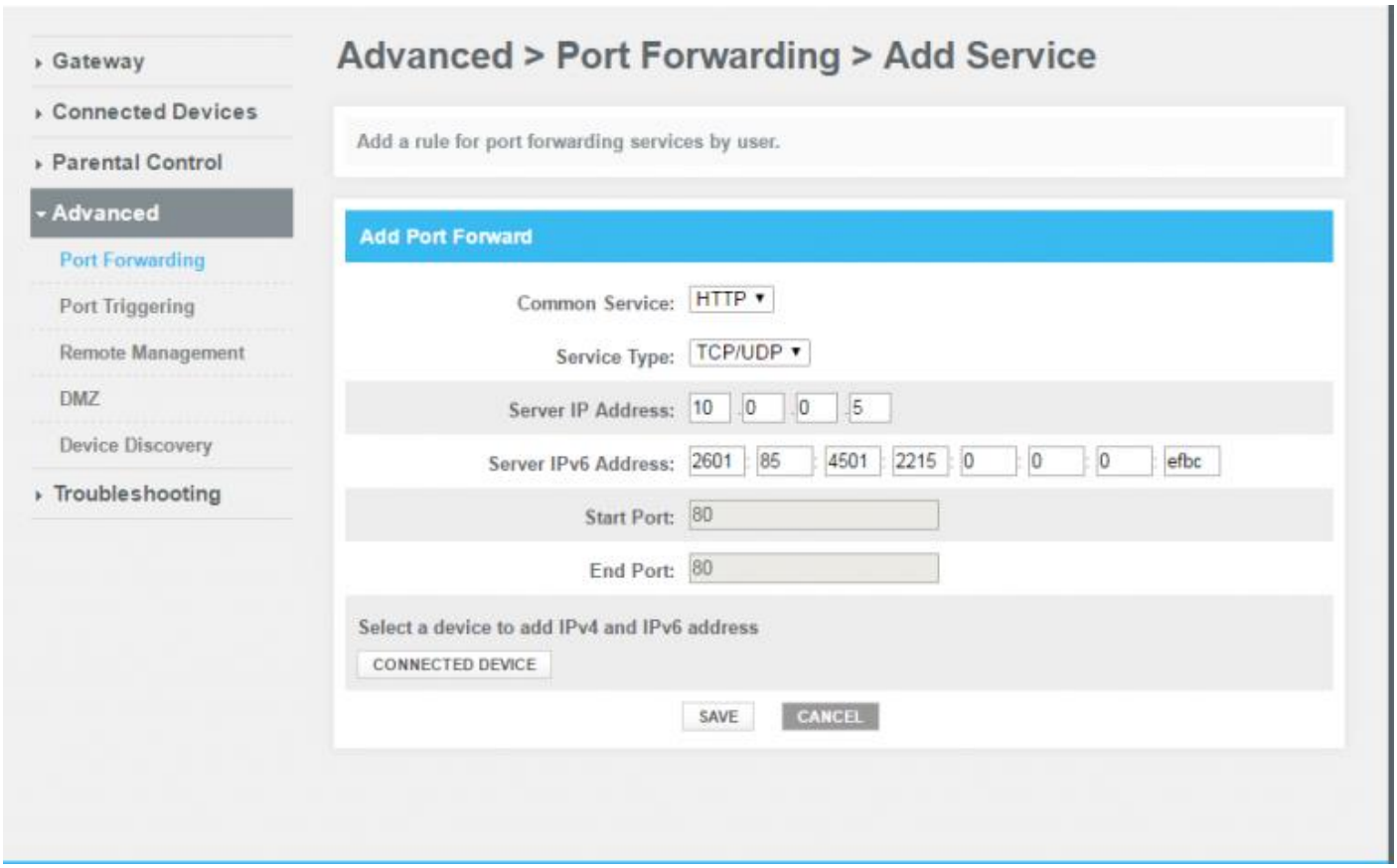


5 GHz Router Configuration Panel

You can see the absence of the reserved channels by reviewing the available channels and noting the gap between Channels 48 and 149. 149 is the default setting here and we'll leave it alone. If there are connection problems you would check the channel and ensure the Mode supports all of your devices and, in our case, switch to another channel possibly in the lower end of the band. You can also choose your encryption type which could prevent connection in the case of a mismatch. Most residential SOHO routers default to WPA/WPA2 (TKIP/AES) allowing most devices to communicate their credentials and start a session. The WPA2 (AES) method is faster if your devices support it.

Port Forwarding, Port Triggering

The port forwarding technique allows incoming connections on a particular port or port range to be delivered to a single specific address or host on the LAN. This is quite useful if you are running a Web server for example, you'd want all new inbound traffic on port 80 to go to that device only. This requires no action on the server's part, it will respond to specific valid requests. Here's how that configuration would look on a SOHO. Your public IP address is inbound port 80 traffic would be directed to the Private IP of the server.



Port Forwarding Configuration Panel

Port Triggering is a variation on this process that requires an outbound communication to "trigger" that port to receive traffic. Now this inbound connection will only be available during a session after which it will timeout.

DHCP (on/off)

Next on our list is the Dynamic Host Configuration Protocol (DHCP). Can't say enough good stuff about this. Imagine having 50 or so users who need to connect to not only the LAN but the internet as well. This is small considering what you will face in the field. Without (DHCP off) or before DHCP you would have to enter each device configuration individually on each device. This includes a complete address (IPv4 and IPv6), the subnet mask the default gateway DNS servers everything that's necessary to connect. DHCP automatically sets up the entire configuration saving you the headache of manual configuration. In some cases for example machines that should not "move" in terms of their addressing like web, DNS and email servers would use static or manual addressing for reliable discovery by all clients. Here is a typical residential/SOHO configuration. Examine the configuration and consider manually adding this to each client along with the DNS settings.

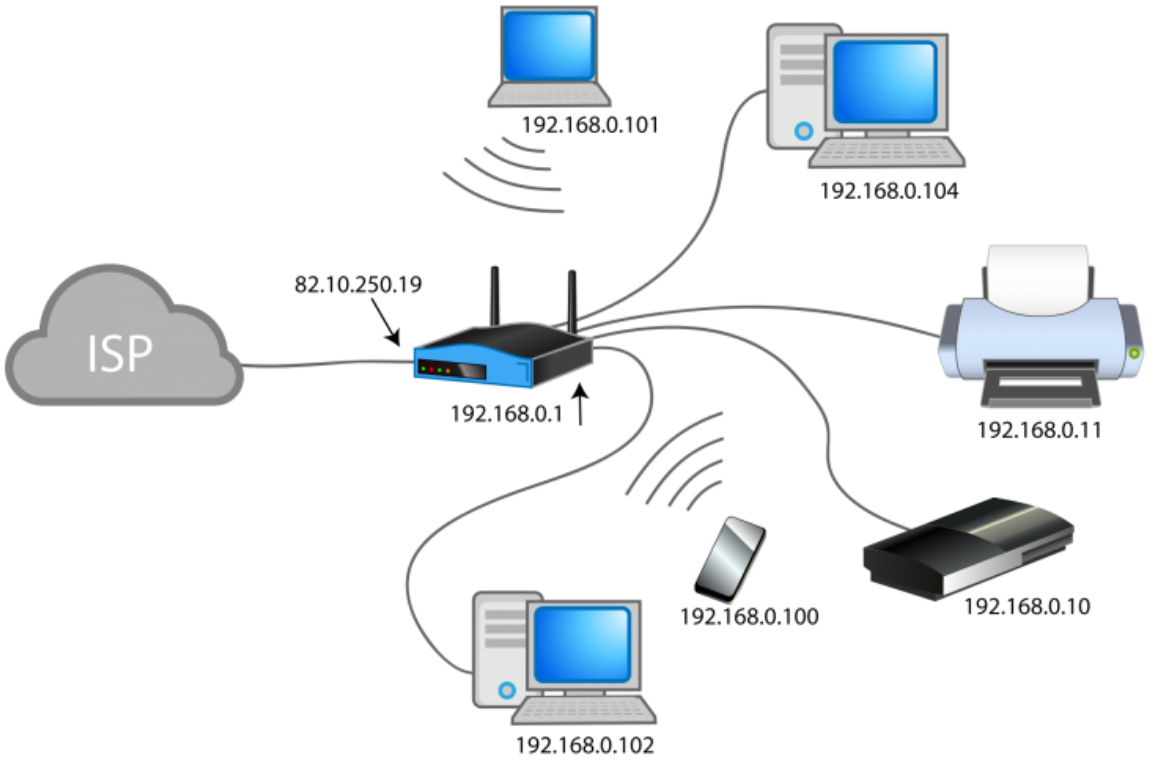
DHCP Configuration Panel

DMZ servers

You know by now that a DMZ (Demilitarized Zone) is a network area outside of your private network that is exposed to any and all traffic on the internet and on the surface it just looks like trouble. However there are good reasons to have this zone, your web server for example is a prime example of effective DMZ utilization. The web server can get hammered with traffic and your LAN will be impervious to it. The services you offer can be deliverable without risk. The concept is to have a **DMZ server** receive the traffic that would normally get dropped by the firewall. The most important point in this configuration is that the hosts in the DMZ cannot connect to the LAN. Now, the LAN on the other hand can connect to anything in the DMZ and the untrusted public network (internet). But the DMZ server has access to everything entirely except your cozy little LAN, relatively speaking.

NAT / DNAT

NAT stands for Network Address Translation. At its simplest is the translation of one network address to another address. This is, in the vast majority of cases, allows the translation of a group of private addresses to communicate externally through a single address the static public address assigned to you by your ISP. This many to one application is a common practice even for large organizations not wishing to expose their networks to the uncontrollable internet.



Network Address Translation – NAT

More often than not and in spite of DHCP, a NAT client will typically get the same address every time it connects unless other circumstances prevent it like a small available pool where addresses are exhausted. This is where the combination of PAT (Port Address Translation) and NAT combine to form DNAT (Destination Network Address Translation). Adding the port to the IP address allows for up to 64,000 addresses from a single IP address.

Basic QoS

Acknowledging that there is always contention for the bandwidth available to you it's easy to envision the need for prioritization of programs and services. The most obvious example of this would be an environment where **basic QoS (**Quality of Service) is not available and you are on a VoIP phone call. Your email automatically checks and receives messages. During the reception of the email your conversation breaks up and is unintelligible. This is because the email program has the same priority on the connection as your phone call. This is easily fixed with Q0S. Each device on the network must have this enabled, most NICs for example have it enabled by default. Routers and both ends of any communication must have it enabled for it to operate properly. The router is one of the main choke points in the service. If you find less than optimal network performance for a particular application, like video conferencing, you can increase its priority on your router. Most routers have built in settings for popular programs, some can be blocked others increased or decreased based on your needs. But think carefully about your choices because setting too many programs to the highest level just moves your problems up a level without resolving them. The priority of the network's use must be carefully evaluated before you make any wholesale changes. Remember that real time A/V communication depends on the packets transmitted and received be uninterrupted and takes precedence over an upload or download.

Firmware

Router firmware can be updated on an as needed basis or from updates provided by the manufacturer. You should check periodically to be sure you have the latest stable version of the firmware. There may be updated security features or functionality. Router firmware deficiencies are often discovered when you bring home a new device and some of its features are not supported because they didn't exist when the router was manufactured.

UPnP

UPnP provides automatic discovery of available hosts and services on the local network. It should be used with caution as it is easily exploitable by hackers. Using UPnP much of your security measures are overridden.