9 practice exercises to become a professional network administrator

The series of 9 exercises allotted to the 3 basic, intermediate and advanced levels mentioned below will cover different network topics, from basic to advanced.

With network management profession, experience is above all, followed by qualifications. Basically, IT training certificates such as Network + or CCNA are the passport for you to start the day of searching for a network administrator, but new experience is everything.

When faced with a problem, if you do not have experience, it is difficult to catch the eye of the employer, especially in the first years of entering the system administration industry.

The question is, have you ever configured or hacked a network? Even if you have been an administrator or a network technician, it is difficult for you to touch every aspect of this field.

The series of 9 exercises allotted to the 3 basic, intermediate and advanced levels mentioned below will cover different network topics, from basic to advanced.

Some exercises will take a few minutes to complete, but some will take you away from the weekends. You may also need to invest a little in hardware equipment, particularly networking equipment, but there are ways that do not need them.

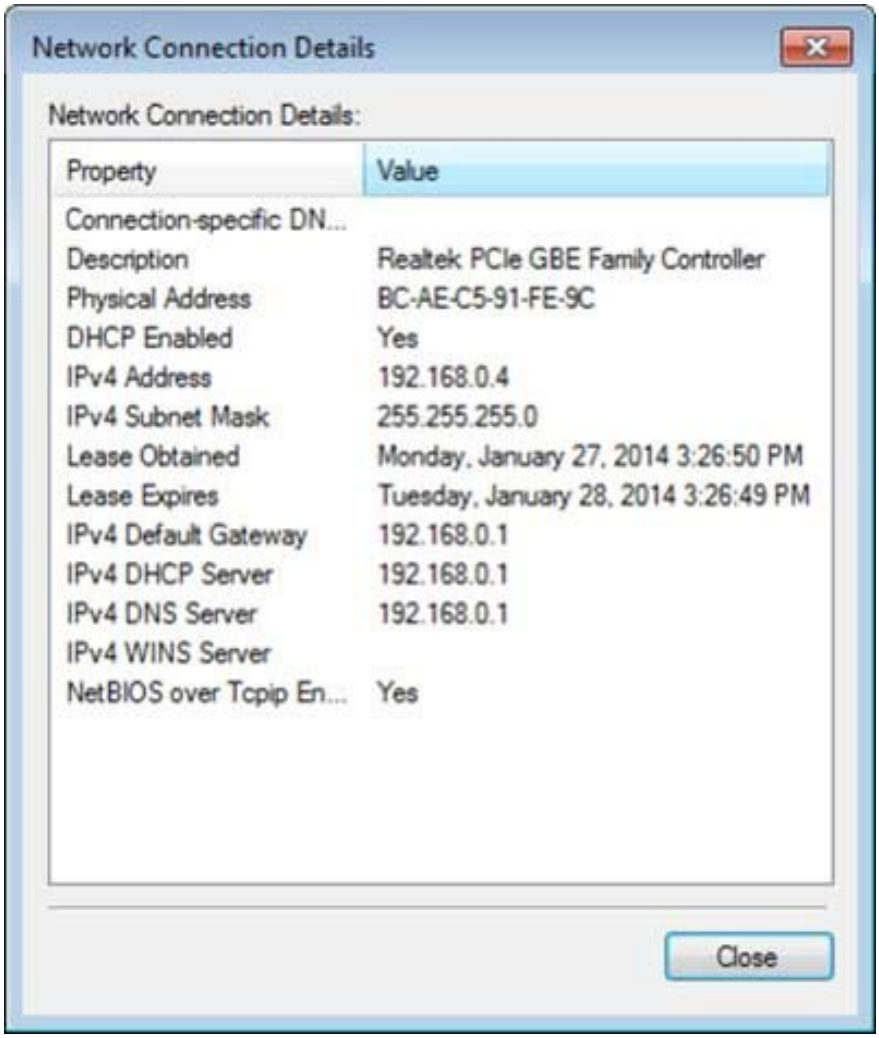
Part 1 - Basic level

Exercise 1: Configuring TCP / IP

One of the most basic tasks of a network administrator is to configure TCP / IP settings. If a network does not use the Dynamic Host Configuration Protocol (DHCP), which automatically manages the IP address when the client connects, you must manually set a static IP and a DNS address for each client. Your system may require you to set static IP information at the beginning of the router setup and configuration steps or other components on the network.

To set a static IP, you must know the router's IP address and IP address range so that you can set it for the client. You can find this information in the Settings of the computer that successfully connects to the network.

You will need the IP address, the Subnet Mask address, the IP address of the router (as well as the Default Gateway) and the DNS server address (Domain Name System).

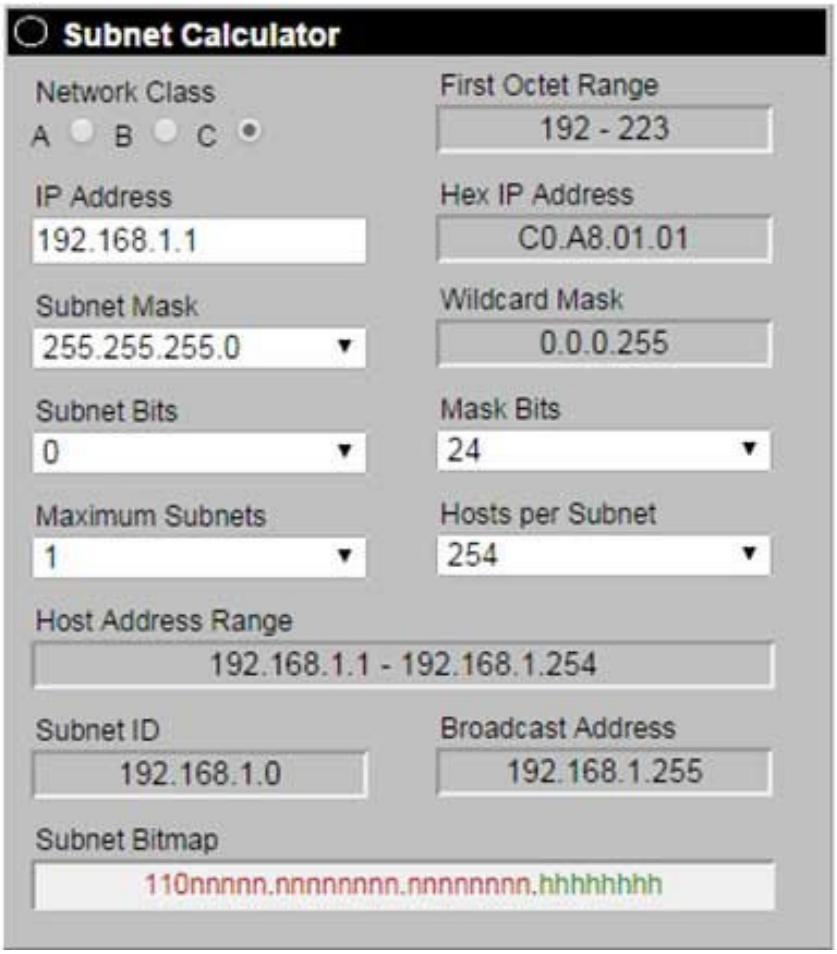


The Network Connection Details window gives you information about the IP address, the Subnet Mask, the Default Gateway and the DNS server.
In Windows : In Network Connections via Control Panel, or Network and Sharing Center. Next, open the active connection and click the Details button.

In Mac OS X : In System Preferences, click the Network icon, then select an active connection, such as AirPort (wireless) or Ethernet (wired). With a wired connection, you'll see information right above the fold; For wireless connections, click the Advanced button and look under the TCP / IP tab and DNS.

Write these numbers down on paper or copy them to a text file, then close the window.

To see the range of IP addresses for the network, you can enter the IP address and Subnet Mask into a subnet calculator application called the Subnet Calculator. For example, entering IP 192.168.1.1 and Subnet Mask 255.255.255.0 will give you the address range from 192.168.1.1 to 192.168.1.254.

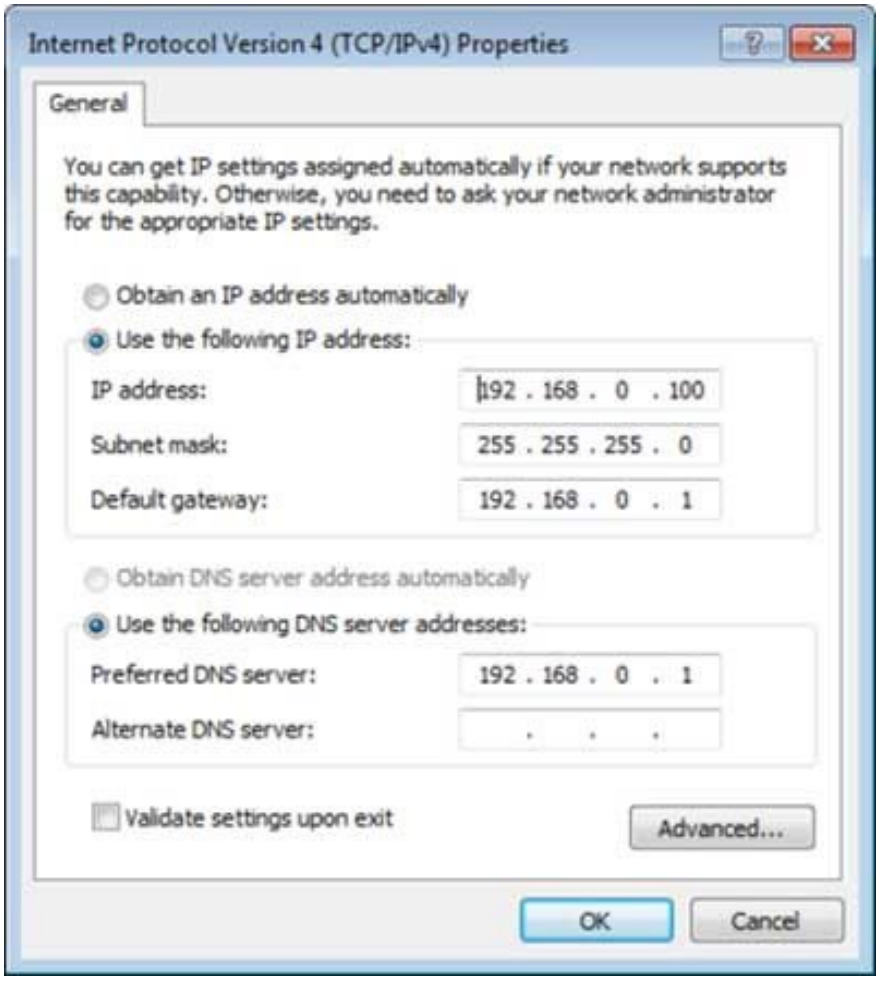


The Subnet Calculator tells you which IP is valid.
By now, you already know the range of IP addresses, but remember that each device must have a unique IP address. The best way to check the IP address is to log into the router, but you can either guess or simply pick a random address in the range. If that address is already used by a device, Windows or OS X will warn of an IP address conflict and you can choose a different one. Once successfully set the IP address, then you write down that address or save it in a text file. This is the best way to record any static IP address along with the serial number of the computer using that IP address.

Now let's set up a static IP:

In Windows : Open the Network Connection Status window, click the Properties button and open TCP / IPv4 settings (Internet Protocol Version 4). Select 'Use the following IP address' and type in the settings: an IP address must be within the allowed IP range, plus Subnet Mask, Default Gateway and DNS server in the Network Connection Details window.

In Mac OS X : Open the Network window and click the Advanced button. On the TCP / IP tab, click the drop-down button next to Configure IPv4, select Manually and type in a valid IP address in the range, plus the Subnet Mask and router address that you copied earlier. Go to the DNS tab and type in the DNS server address.

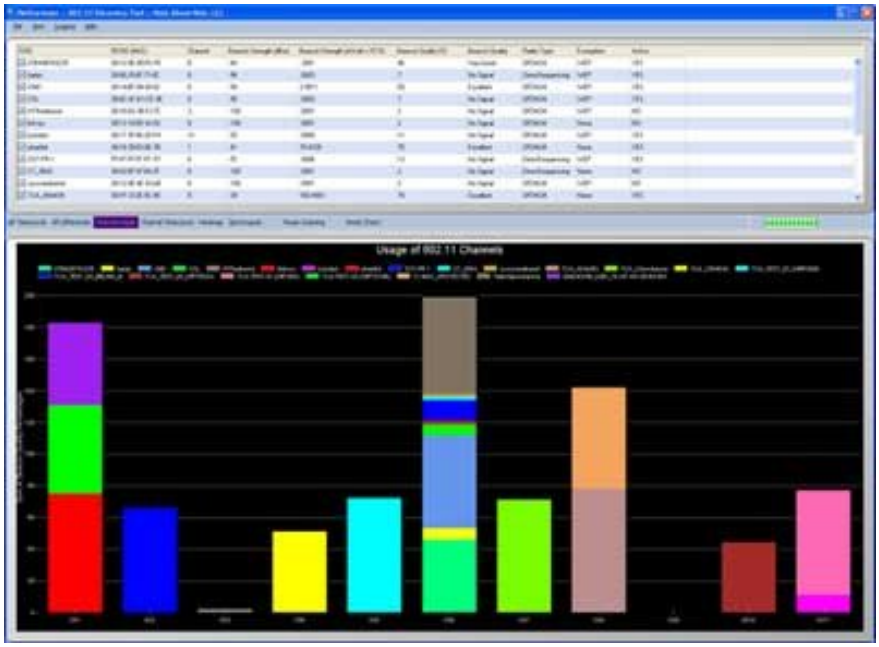


You type manually set IP.
Click OK to finish.

Exercise 2: Analyzing Wi-Fi

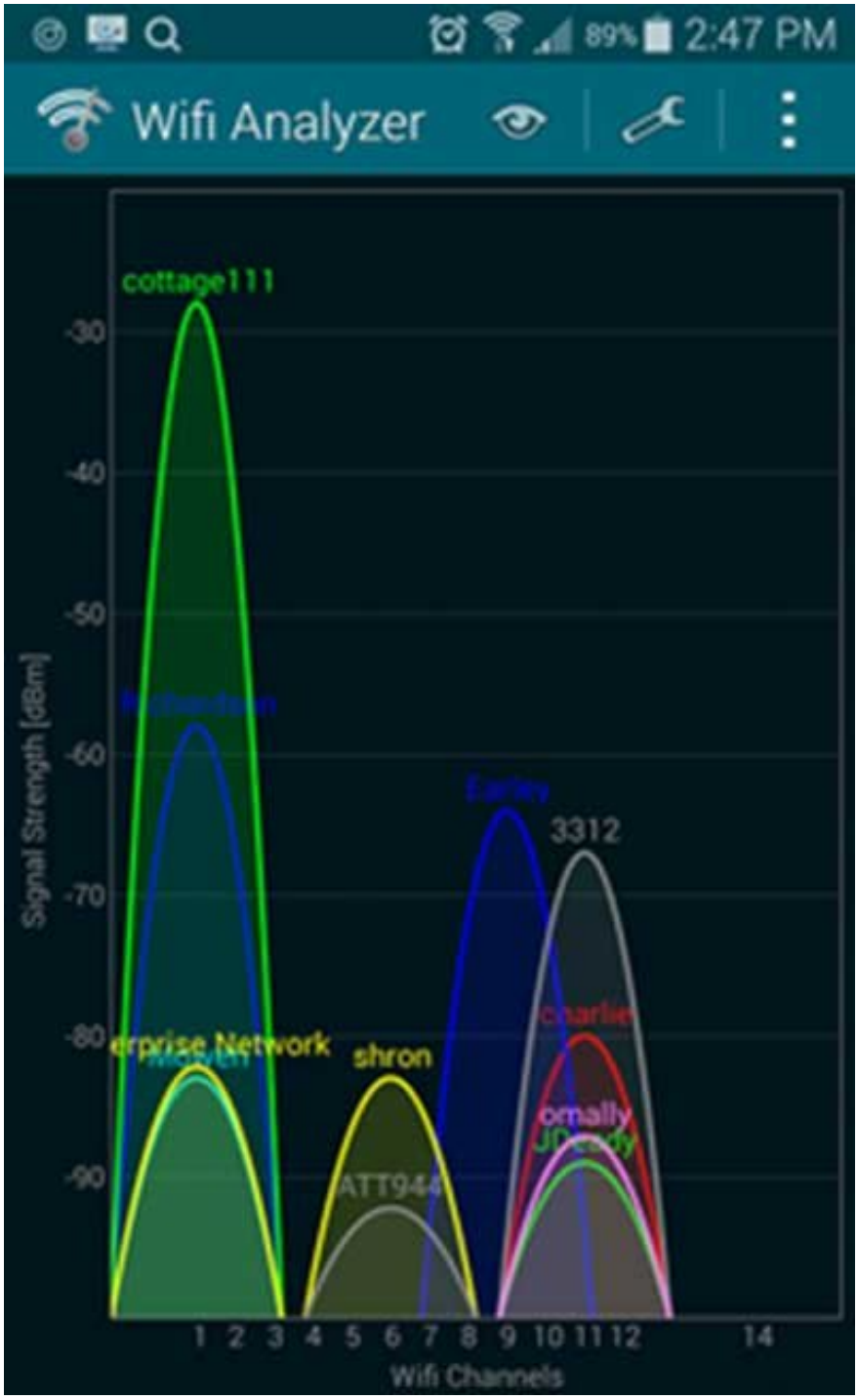
As a network administrator, you will want to set up, fine-tune, and maintain a wireless network on the network. One of the most basic tools you need is a Wi-Fi analyzer (Wi-Fi stumbler). These tools can scan and list basic information about wireless networks, including nearby routers and Access Points (APs), including the service set identifier (SSID), also known as the network name. wireless; MAC address of the router / AP; channels; signal level; and security status.

You can use a Wi-Fi detector to check your home network. For example, you can check which channel your neighbor is using on Wi-Fi so you can switch to another channel for noise reduction. You also need to make sure the router's security mode is at least WPA or WPA2.



NetSurveyor gives you details about surrounding Wi-Fi networks in words as well as graphs.
Windows has Vistumbler and NetSurveyor tools; Mac OS X has KisMac; or Kismet for both operating systems, plus Linux. All four tools are free, allowing you to view text or histogram information about the channel and Wi-Fi signal level.

If you use an Android smartphone or tablet, you can use Wifi Analyzer or Meraki WiFi Stumbler, both of which are free.



WiFi Analyzer presents the Wi-Fi channel graphically with visualization.

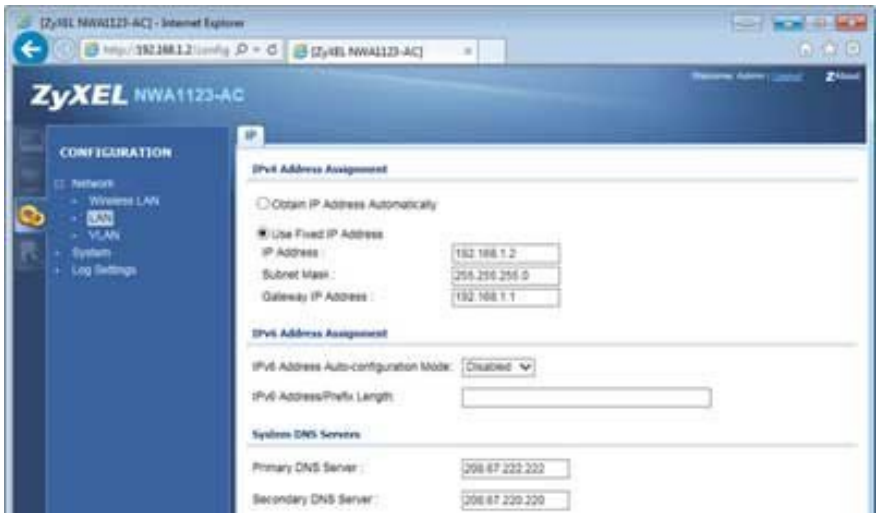
Exercise 3: Configuring wireless routers and APs

For more experience setting up and configuring wireless, you should work with your wireless router at home. Or better yet, you should be exposed to an AP that is manufactured for business. It's best to borrow from someone in your company's IT department, or try to find out if there are routers or APs for low-cost businesses, such as Ubiquiti Networks APs that are quite soft (about $ 70 USD). on eBay).

To access the wireless router configuration interface, type the IP address in the browser. Refer back to Practice 1, the router's IP address is the same as the Default Gateway address that Windows lists in the Details window for wireless connectivity.

Access AP configuration interface is quite different. If you have a wireless controller, there is a common interface that you can configure for every AP. For systems without this wireless controller, you must access each AP individually through its IP address.

Once you have access to the router or AP configuration interface, look at all the settings and try to understand them. See enabling wireless separation (or layer 2) if the device supports it and see how it blocks user-users. You can also change the router / AP's IP address in LAN settings, turn off DHCP and assign specific IP addresses for each device / computer. You also see static DNS addresses (like OpenDNS) in WAN settings; Set up Quality of Service (QoS) to prioritize data flow. Once you have mastered those parameters, set the highest security level for the network as WPA2.



Assign IP addresses and DNS addresses to the router.
In case you are unable to earn an enterprise level AP, take a look at the interface emulation tools or demos of some manufacturers, such as Cisco.

Part 2 - Intermediate level

Exercise 4: Installing DD-WRT on a wireless router

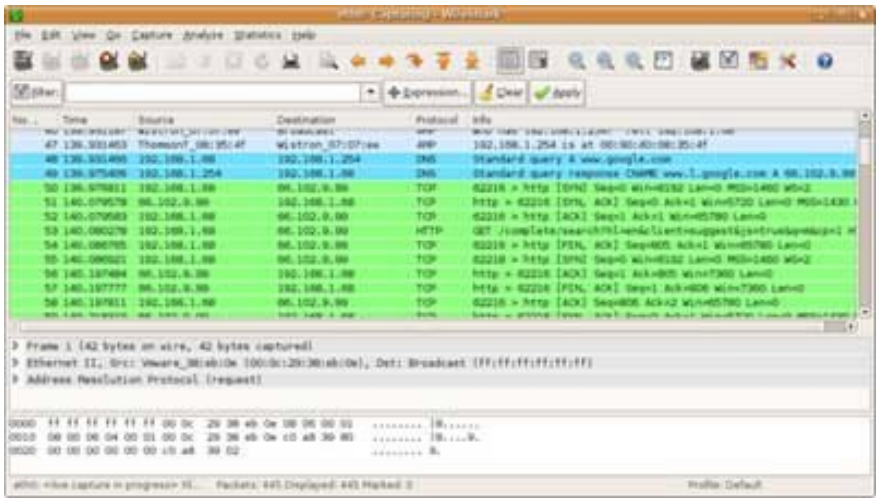
To "play around" more than wireless networks, you can install open source firmware for DD-WRT wireless routers. This firmware has many advanced features only available at the enterprise level, and can be customized very well. But before downloading and updating the firmware, you need to check the list of routers compatible with this firmware.

For example, it supports virtual LANs and multiple SSIDs, so you can divide a network into multiple virtual networks. It also supports a client and a VPN server for remote access, or even site-to-site direct connection. Moreover, it allows you to customize the firewall, run launch and shutdown scripts, and support various hotspot solutions.

DD-WRT has many advanced new features for you to "dab".

Exercise 5: Analyzing networks and data flows on the network

As a system administrator, you will need to handle the problems associated with tracking data packets that are transmitted on the network. Although network protocol analysis tools can cost a lot of money, Wireshark is a free, open source option that works on all operating systems. It has many features and supports real-time monitoring and offline analysis for hundreds of different network protocols, decrypts for many types of encryption and has strong filters, capable of reading / writing through many captured file format (file) online.



Wireshark captures packets on the network.
Once you have installed Wireshark, try capturing the packet and seeing what it has in it. In other words, go around the web or locate online shares to see how data flows on the network. Remember, you can stop capturing data to take a closer look. Although Wireshark can capture all traffic flowing through the network, you may only see the incoming / outgoing data flow of a client if the "mixed" packet capture mode is not enabled by the operating system you are currently running. User or network adapter (network adapter) supported. For more information, you can refer to the website of Wireshark.

Note: even when packet capture is usually run in the passive mode, it means not interfering or interfering with the network, but some people view this type of surveillance as a violation of privacy and personal policies. So you should note that it should only be applied to a home personal network, or require the rights of the system administrator or company CTO before implementation.

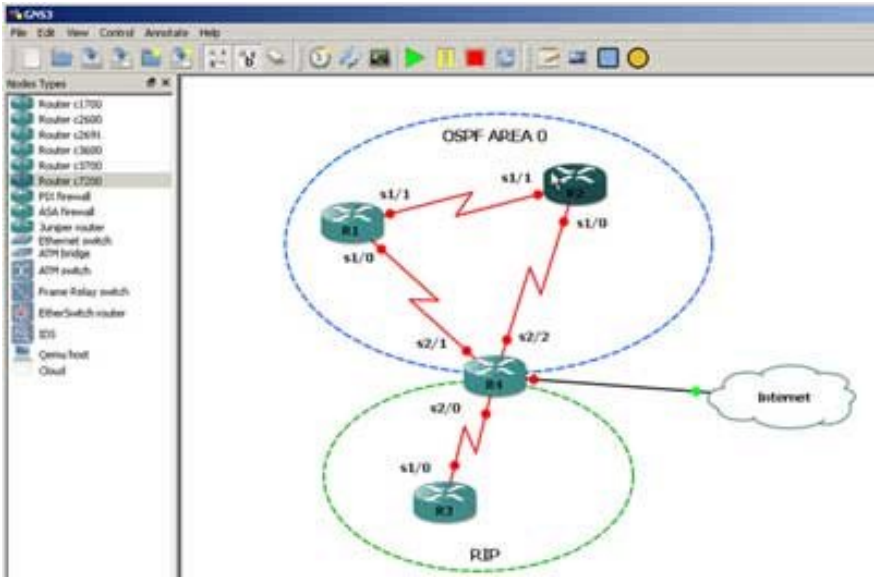
In addition, there are a few other free network analysis tools that you may want to try. For example, EffeTech HTTP Sniffer can assemble HTTP packets and display them on a web page so that they can be clearly displayed graphically for easier tracking, instead of looking at heaps of raw data packets. Or as Password Sniffer just "listens" for passwords on the Internet and lists them out, showing us that alphanumeric passwords are very insecure. And to analyze mobile data via Android phones or tablets, there are free tools like Shark for Root.

Exercise 6: Try the network simulator

Although it is difficult to directly use the corporate network for internships, we have another way, which is to use emulators to virtualize network configuration and configuration. They are invaluable tools to prepare for IT exams, including Cisco and Juniper certifications. Once you create a virtual network with full components and clients, you can configure and administer them using the settings and emulator commands. You can even run network analysis tools like Wireshark with several emulators to see where the network data stream is going.

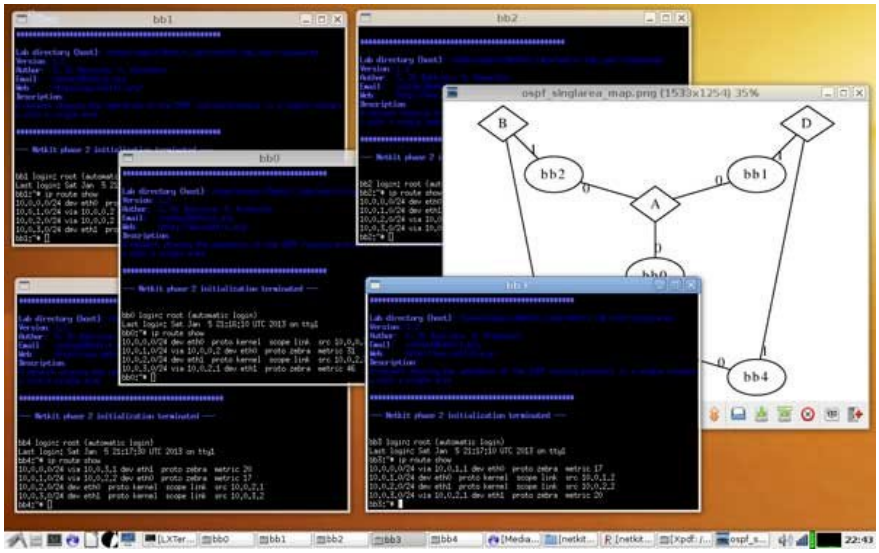
Here are some emulators you should check out:

1. GNS3 Graphical Network Simulator is a free, open source option. It requires you to run the corresponding operating system, like Cisco IOS or Juniper OS Juniper, and you need to register.



GNS3 Graphical Network Simulator supports Cisco IOS / IPS / PIX / ASA and Juniper JunOS.

1. Netkit is another free, open source option. It does not require specific functions associated with the manufacturer and is limited in network components. The good news is that Netkit doesn't have the same operating system requirements as GNS3.



Netkit network simulator running the pre-configured single-area OSPF lab

1. Boson NetSim Network Simulator is a paid simulator, priced at 99 USD; Its main purpose is for you to learn about Cisco IOS. It has free demo but very limited functionality.

There are also websites like SharonTools and Open Network Laboratory that give you remote access to network components and simulate the web platform for you to execute commands. You should also try out free Cisco emulators.

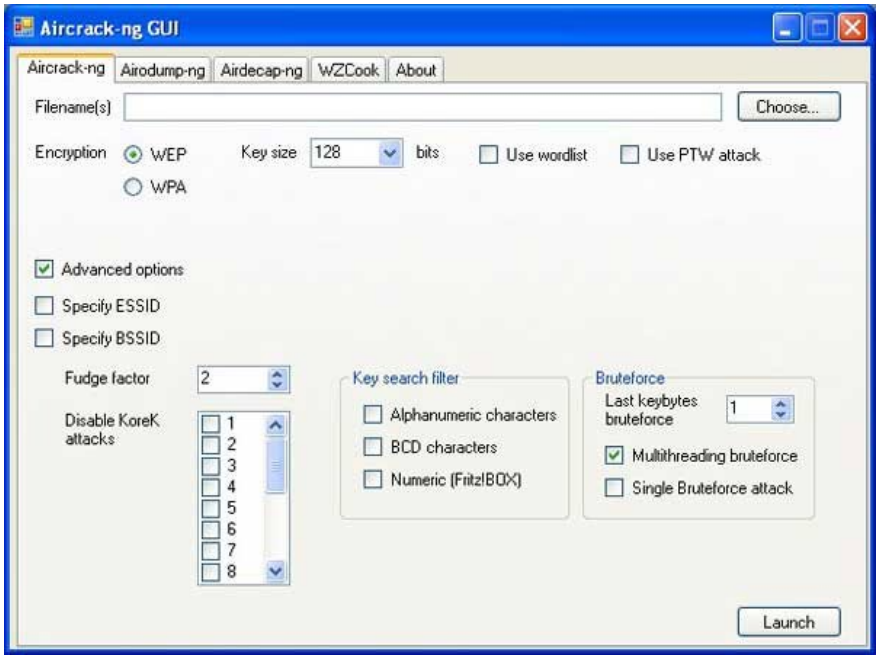
Part 3 - Advanced level

Exercise 7: Self-attack the system

You can read a lot about network security, but the best way is to learn how to assess the security level of the network by testing its own network attacks.

Here are a few attack methods you can try:

1. Wi-Fi cracking. WEP encryption is the easiest way to hack using Aircrack-ng. Wi-Fi Protected Setup (WPS) cracking with a PIN using Reaver-WPS can also access a wireless router.



Aircrack-ng's multimedia gallery.

WPSCrackGUI - WPS (WiFi Protected Setup).

1. Hacking online accounts via Wi-Fi using Firefox add-on Firesheep or Android DroidSheep application.

Firesheep.

1. Capturing data packets and cracking login information on 802.11X networks using FreeRadius-WPE.

WEAKERTH4N: FreeRadius-WPE.
As you study, you'll find instructions on how each tool works. Another popular tool that integrates hundreds of available tools is the CD BackTrack, but this project has now stopped working.

However, Kali Linux is a similar tool, currently very popular, can be installed directly into computers or virtual machines, or run on USB, CD.

If you want to find ways to test your network, you can refer to Ethical Hacker at the link below.

`https://www.pcworld.com/article/250045/how_to_become_an_ethical_hacker.html`

Ethical Hacker.

Exercise 8: Setting up a RADIUS security server

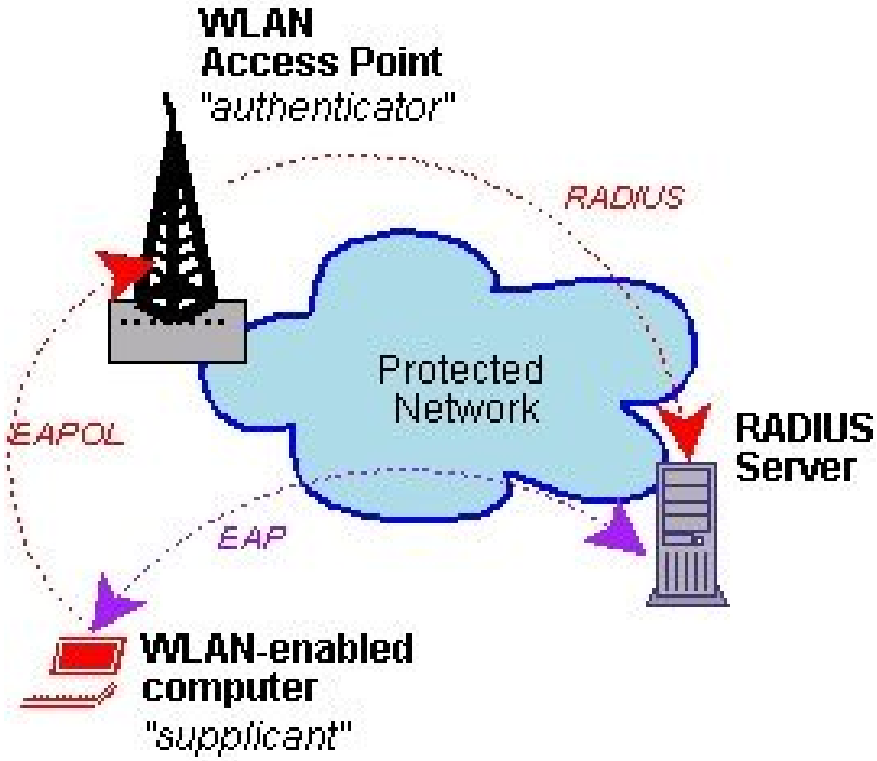
At home, you often encrypt your wireless router with Personal or Pre-shared Key (PSK) mode for WPA or WPA2 security to help keep your wireless network from being snooped on. Personal mode is the simplest way to encrypt Wi-Fi: set a password on the router and simply enter this password into the connected device and computer.

However, for businesses, the Enterprise mode of WPA or WPA2 is preferred by security experts, because of its combination with 802.11x authentication.

Instead of using a Wi-Fi password, each user will receive a unique login information; This encryption protects against data theft between users. Moreover, you can change or delete an account to protect the network when an employee does not work anymore or some device is lost or stolen.

To use enterprise mode, you must have a separate RADIUS (Remote Authentication Dial-In User Service) server to handle the user's 802.11x login. As a system administrator, you will have to configure and configure the client with 802.11x authentication and help maintain the RADIUS server. For an internship, see setting up a server for you at home and using enterprise-class Wi-Fi security at home.

If you are running a Windows-based network, the Network Policy Server (NPS) or Internet Authentication Service (IAS) can be used as a RADIUS server. If not, you have several free options. If you're familiar with Linux, check out the FreeRADIUS open source software. Some options are easier to use, have a GUI interface and are free like TekRADIUS, or the 30-day ClearBox trial tool.



RADIUS Server.
Once you have installed the RADIUS server, you create user accounts and enter the shared secrets for the AP. Then, configure your wireless router or AP with WPA / WPA2-Enterprise: type in the IP address and port of the RADIUS server, then the shared secret that you set on the RADIUS server. You can then connect the device by typing in the login information that you specify on the RADIUS server.

Exercise 9: Installing Windows Server and setting up the domain name

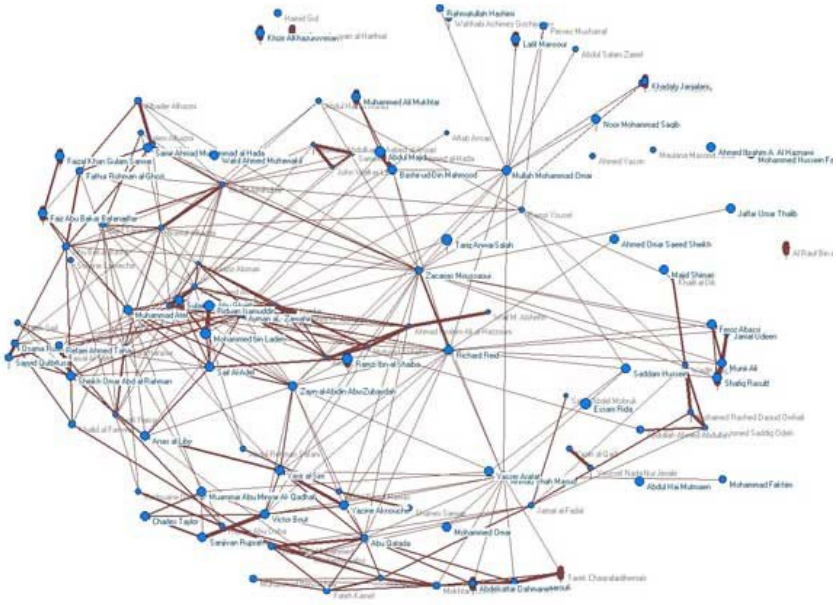
Administrators also need to manage Windows-based network systems running with Windows Server. For more experience, try running a copy of Windows Server at home.

Although buying a server operating system version is not cheap, you have a few free options. Microsoft gives you a 180-day free trial of the downloaded ISO version to install on a physical server, a virtual hard disk (VHD) for the virtual server and access to an unconfigured virtual machine in the Azure cloud. Moreover, Microsoft also offers Virtual Labs, there are instructions for you in a virtualized environment, you can try it.

Once you have access to a server, explore it and practice. Perhaps you should try configuring Active Directory and trying with Group Policies, setting up Exchange and configuring an Outlook client, or setting up NPS for 802.11x authentication.

Next step: Study, study more, learn forever

If these exercises are really useful and need more management experience, there are still many online courses that you can take. Find and choose a training course according to specific management qualifications.



The complexity of Networking.

You finished reading the article "**9 practice exercises to become a professional network administrator**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
