Individualized I.S. Activity

Router
Maintenance

My I.S. Individualized Activity

As part of the duties of an Info. Sys. Manager, it is likely that you will be asked to audit network connections for the corporation that you work for. In preparing myself for such work, I conducted an audit of my own, in-home, network router.

Definition

In performing a network audit, the criteria that would define such action includes reviewing the number of currently connected devices, blocking unknown connections, assigning devices with unique IP addresses and performing a review of the router logs for suspicious/unauthorized actions.

Perform and Documentation of Router Evaluation

Within this evaluation, the first thing I conducted was a review of what devices are currently connected and if they are permitted. Such review was conducted and is shown below.

	technicolor	Connection / Devices Technicolor Wireless Cable Voice Gateway					

Status	Connection	Security	Application	Administration				
Devices	LAN	WAN	Routing	MoCA	Modem	Network Time	MTA	

Private Network

Host Name	DHCP/Reserved	MAC Address	IPv4 Address	Connection	Status	Opera
eero	DHCP	f8:bc:0e:04:93:20	192.168.0.87	Ethernet	🖥	✕ ✎
ESP_A263C6	DHCP	dc:4f:22:a2:63:c6	192.168.0.93	Wi-Fi 2.4G	📶	✕ ✎
290e9b66f8dd52f636945bb6900c341e	DHCP	6c:21:a2:68:97:ed	192.168.0.234	Wi-Fi 2.4G	📶	✕ ✎
nixplay_W10F-06	DHCP	80:9f:9b:c0:31:ed	192.168.0.24	Wi-Fi 2.4G	📶	✕ ✎
LAPTOP-RP7F67CU	DHCP	04:ed:33:55:55:c8	192.168.0.146	Wi-Fi 5G	📶	✕ ✎
WSG9035M8	DHCP	F4:D1:08:51:30:24	192.168.0.59	Unknown	🚫	✕ ✎
RokuPremiere-501	DHCP	d8:31:34:d1:3f:8a	192.168.0.25	Unknown	🚫	✕ ✎

c8:3d:d4:08:47:f8	DHCP	c8:3d:d4:08:47:f8	192.168.0.100	Wi-Fi 5G		✕	✎
38:9D:92:C7:60:2D	DHCP	38:9D:92:C7:60:2D	192.168.0.250	Wi-Fi 2.4G		✕	✎
1c:fe:2b:ec:9f:66	DHCP	1c:fe:2b:ec:9f:66	192.168.0.202	Wi-Fi 5G		✕	✎
Cliftons-iPad	DHCP	88:cb:87:a0:5a:bc	192.168.0.137	Wi-Fi 5G		✕	✎
amazon-470ad4dd3	DHCP	fc:65:de:7f:af:bc	192.168.0.14	Wi-Fi 5G		✕	✎
E2:C5:BC:25:78:96	DHCP	E2:C5:BC:25:78:96	192.168.0.127	Unknown		✕	✎
BattleCat-Line	DHCP	9E:C3:17:FC:1A:72	192.168.0.12	Unknown		✕	✎
CliftonpleWatch	DHCP	F2:55:16:9D:01:F3	192.168.0.163	Wi-Fi 2.4G		✕	✎
Candaces-Phone	DHCP	16:BD:F6:68:12:D9	192.168.0.66	Unknown		✕	✎
m-givsgo	DHCP	70:BC:10:6E:CC:9F	192.168.0.236	Unknown		✕	✎
CGFamily-PC	DHCP	00:25:56:30:f9:03	192.168.0.52	Unknown		✕	✎
Candaces-iPad	DHCP	5e:5a:87:55:de:18	192.168.0.27	Unknown		✕	✎

Snapshot of network connected devices and their current connection status

After reviewing these devices, it was clear that there were several devices that connected to the network that were not originally accounted for; however, after conducting an internal audit of devices – 20 devices in total – it was confirmed that all connections were accurately accounted for. These devices include the following:

- 1 wired Eero Device

- 1 wireless printer

- 1 Desktop Computer

- 3 laptops

- 3 iPads

- 4 wireless WOW Set tops for television

- 1 apple watch

- 1 Blu-ray Player

- 1 Xbox 360

- 2 Apple phones

- 1 Smart TV

- 1 Roku Device

Out of all the devices mention, only 4 devices were active on the network and obtaining network connections. The next thing in the audit is to ensure that DHCP reservations are set and functioning properly.

To ensure that printing is always static to one address, a DHCP reservation was performed ensure that this information does not change. Below is an example of setting such a reservation.
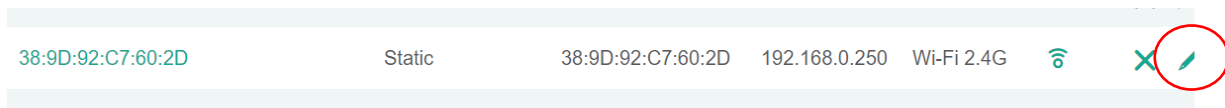
By hitting the edit button to the right of this online device, I am able to access the reservation feature. This allows me to set this device's IP to static position on the network. What this means that, no matter what happens with the network connections, this device will always have the same assigned IP. Below is a view of how that process is performed.
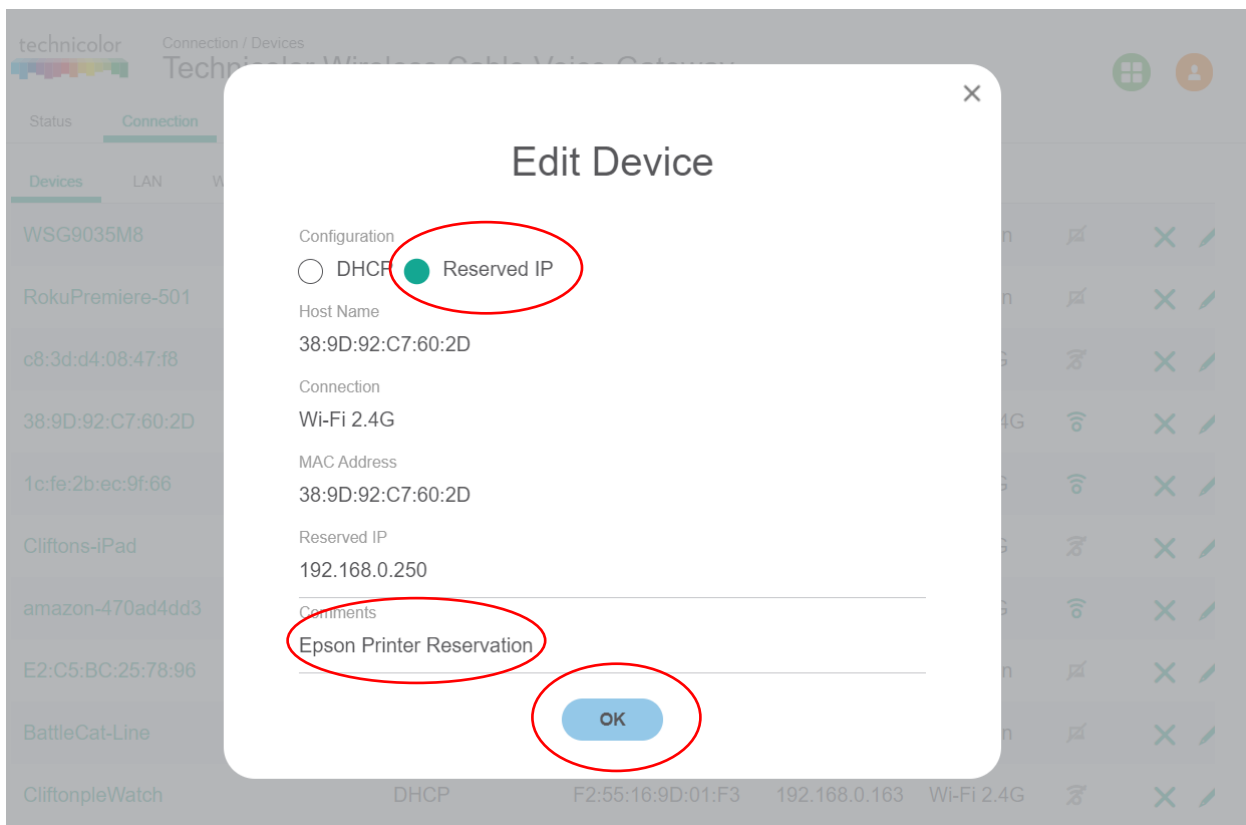
Now that I have conducted the DHCP reservation, it is time to conduct a network audit of router changes and/or updates. This process is unique for each router; however, such reports can either be online only, printed only or a hybrid of the two options. Below is an example of this router's logs.

Fri Apr 16 01:34:00 2021	74010100	Notice (6)	CM-STATUS message sent. Event Type Code: 24; Chan ID: 32; DSID: N/A; MAC Addr: N/A; OFDM/OFDMA Profile ID: 2.;CM-MAC=a0:ff:70:98:dd:33;CMTS-MAC=00:01:5c:6a:4c:56;CM-QOS=1.1;CM-VER=3.1;
Fri Apr 16 06:20:29 2021	68010300	Error (4)	DHCP RENEW WARNING - Field invalid in response v4 option;CM-MAC=a0:ff:70:98:dd:33;CMTS-MAC=00:01:5c:6a:4c:56;CM-QOS=1.1;CM-VER=3.1;
Fri Apr 16 11:24:17 2021	74010100	Notice (6)	CM-STATUS message sent. Event Type Code: 16; Chan ID: 32; DSID: N/A; MAC Addr: N/A; OFDM/OFDMA Profile ID: 2.;CM-MAC=a0:ff:70:98:dd:33;CMTS-MAC=00:01:5c:6a:4c:56;CM-QOS=1.1;CM-VER=3.1;
Fri Apr 16 11:24:43 2021	74010100	Notice (6)	CM-STATUS message sent. Event Type Code: 24; Chan ID: 32; DSID: N/A; MAC Addr: N/A; OFDM/OFDMA Profile ID: 2.;CM-MAC=a0:ff:70:98:dd:33;CMTS-MAC=00:01:5c:6a:4c:56;CM-QOS=1.1;CM-VER=3.1;
Sat Apr 17 18:20:29 2021	68010300	Error (4)	DHCP RENEW WARNING - Field invalid in response v4 option;CM-MAC=a0:ff:70:98:dd:33;CMTS-MAC=00:01:5c:6a:4c:56;CM-QOS=1.1;CM-VER=3.1;
Sun Apr 18 08:08:58 2021	74010100	Notice (6)	CM-STATUS message sent. Event Type Code: 16; Chan ID: 32; DSID: N/A; MAC Addr: N/A; OFDM/OFDMA Profile ID: 2.;CM-MAC=a0:ff:70:98:dd:33;CMTS-MAC=00:01:5c:6a:4c:56;CM-QOS=1.1;CM-VER=3.1;
Sun Apr 18 08:09:34 2021	74010100	Notice (6)	CM-STATUS message sent. Event Type Code: 24; Chan ID: 32; DSID: N/A; MAC Addr: N/A; OFDM/OFDMA Profile ID: 2.;CM-MAC=a0:ff:70:98:dd:33;CMTS-MAC=00:01:5c:6a:4c:56;CM-QOS=1.1;CM-VER=3.1;

What is unique about this log is that I see some DHCP renewal warnings. This lets me know that some devices are attempting renewal, but there is either a software concern with those devices or a firmware update may be needed soon. Since the device belongs to our cable provider, I will be scheduling a call for firmware updates; however, this is not necessary as all devices are successfully connected for network service.

Conclusion

The need to know how to look for, perform and implement these simple IT services can be invaluable to a company when it comes to network management. A strong Info. Sys. Management candidate must be able to manage his/her own network services successfully before they can better support professional services. While home routers are not, typically, as advanced as professional network routers, the basic concepts will remain the same and are beneficial for every degree recipient to know and perform.