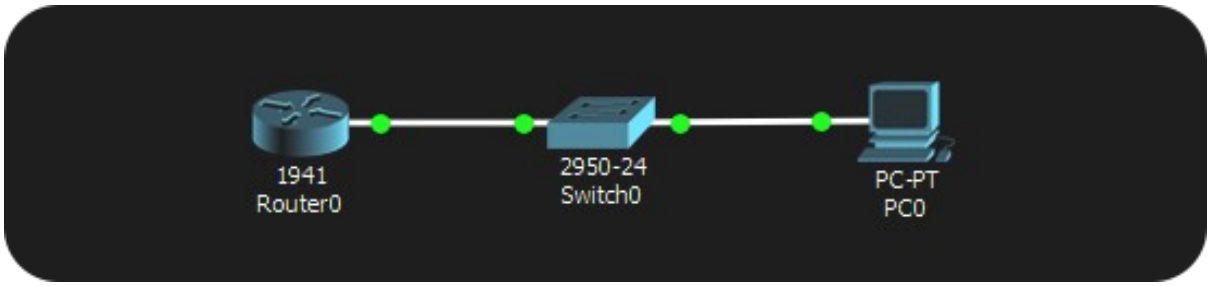
*STATIC IP - NETWORK*




*Configured with information from* (Viktor17GT, 2019).

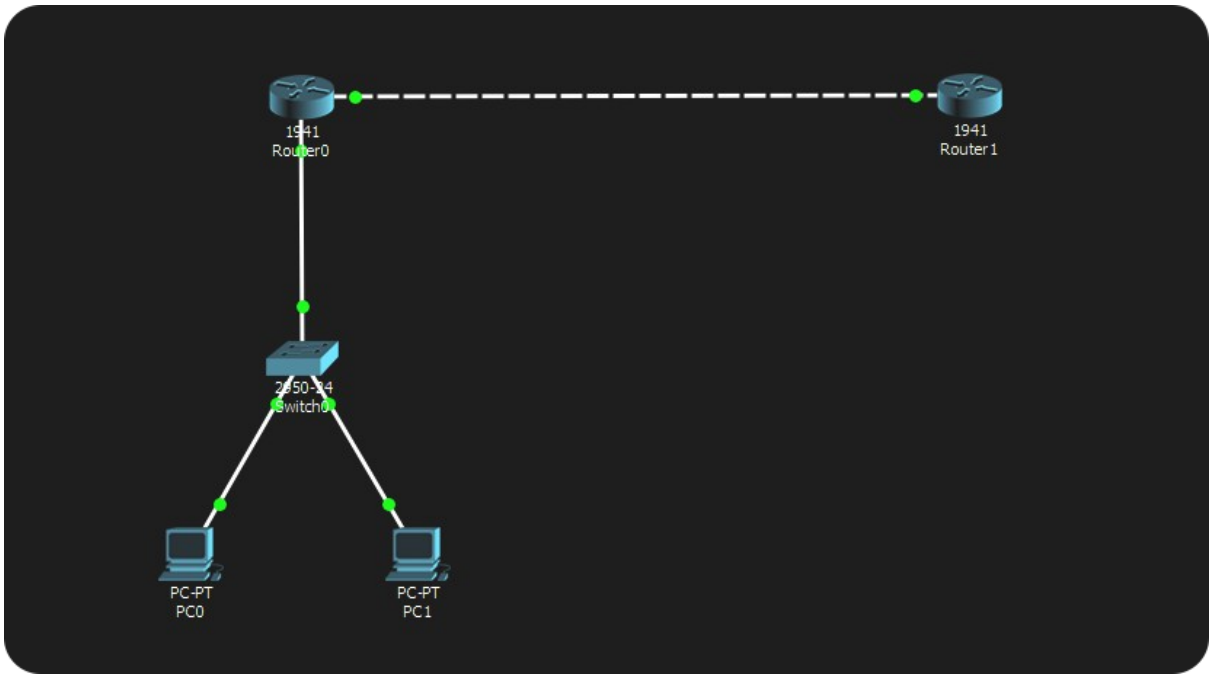
Static IP addresses are easy to set up, relying on configuring the router and/or the end device to use a static IP for the target device, associating a local IP address with a MAC address, which is unique to the hardware in the target device (Fisher, 2019). This utilises DHCP reservations to assign the address to the specific hardware, preventing it from being assigned to any other devices on the network should they require an automatic assignment (PCMag Digital Group, n.d.).

Static addresses are useful for network configuration as they allow you to have a fixed reference to devices on the network. This would be particularly useful with file servers, routers, printers, and specific computers. This is because of how having a fixed reference allows users to skip the address discovery phase of connecting to a device, which involves listing all the IP addresses in use on the network, then finding out which one is the machine they want to target. Instead, they can just reference the fixed address of each machine (Mitchell, 2019).

Additionally, static IP addresses allow for port forwarding. Port forwarding is a feature where the router allows devices on the network to open specific ports, even if those ports are closed on the router itself. This allows for specific firewall rules on each device that's assigned a static IP address, which can be useful for hosting servers and program functionality, should those ports be closed in the first place (Fisher, 2019).

Having specific port forwarding can improve security very much, as it allows for closing ports to the entire network, while retaining essential functionality for specific devices on said network. Having individual devices with a static IP also allows for simpler usage of the network should the usage rely on IP addresses. This means that identifying issues with the network can be much easier and more precise, helping prevent real-time attacks. Static IPs aren't necessarily more secure beyond these factors, as they don't protect from attacks, only making configuration easier and allowing for port forwarding.

*NAT Router - Network*



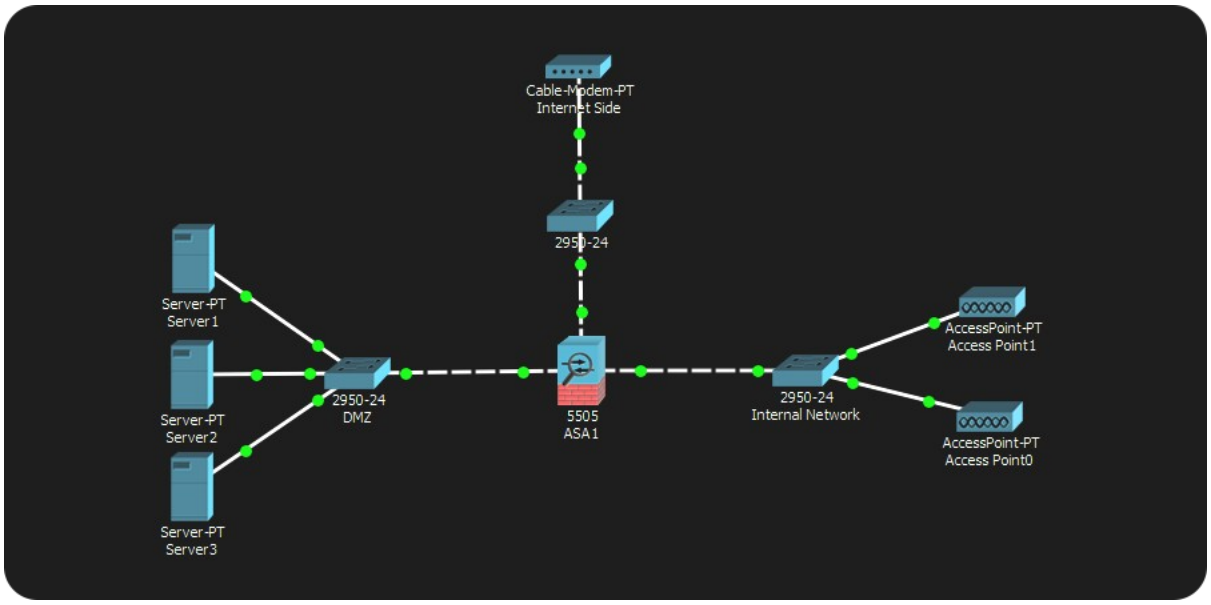

*Configured with information from* (Networks Training, n.d.).

NAT routers involve using Network Address Translation (NAT), which is where the router assigns a public IP address to a private IP address. This means that sending information to the public IP address involves it being forwarded to the private IP address, much like a symbolic link (Javvin Technologies, 2005) (WhatIsMyIPAddress.com, 2019). NAT is usually used to conserve on the amount of public IP addresses that the network utilises (rvigil & mlluis, 2014).

NAT relies on router configuration, specifying IP ranges and configurations for each network interface on said router (ComputerNetworkingNotes, 2018). While NAT has no specified security purpose, it can still be useful for preventing unauthorised traffic involving the LAN, as NAT protects the internal side of the network by assigning them usually fewer numbers of IP addresses than there are devices. The only way the router can identify which device the traffic is meant for is if it also knows which device requested said traffic, otherwise it would end up being dropped (Gibson Research Corporation, 2006).

Because of this, NAT can work like a firewall, blocking traffic that isn't requested. This can be an issue for servers where outside traffic is expected, however for a LAN featuring computers and private file servers, this feature can be incredibly useful.

*Demilitarised Zone (DMZ) - Network*




*Produced with information from* (Cisco, n.d.).

DMZs, or Demilitarised Zones, are isolated areas in a network that are segregated from the rest of the LAN. This segregation allows for the DMZ to have different firewall rules compared to the internal network. This involves having outside-facing servers inside the DMZ with rules allowing for communication with them, like in the case of a public file store or web server, whereas the internal network has rules that restrict those same ports (wiseGEEK, n.d.) (Mitchell, 2019).

DMZs are useful for security as they allow for these group firewall rules that can be tailored for the specific use-case required. As well as this, they protect the internal network from both the DMZ and the external network. Both the DMZ and the external network are considered unsafe compared to the internal network.

DMZs and NAT routers and Static IPs can be merged to combine all the positives that these individual features provide into a single network. A DMZ works well with static IP addresses, as it allows for easy access to the servers from the internal network. Similarly, a NAT router allows for the internal network to be protected from random traffic, which could work alongside the hardware or virtual router that the DMZ requires.

*Bibliography*


Cisco, n.d.. *Configuring DMZ*. [Online]
Available at: https://www.cisco.com/assets/sol/sb/isa500_emulator/help/guide/ad1681599.html

ComputerNetworkingNotes, 2018. *How to Configure Static NAT in Cisco Router*. [Online]
Available at: https://www.computernetworkingnotes.com/ccna-study-guide/how-to-configure-static-nat-in-cisco-router.html

Fisher, T., 2019. *How to Forward Ports on Your Router*. [Online]
Available at: https://www.lifewire.com/how-to-port-forward-4163829

Fisher, T., 2019. *What Is a Static IP Address?*. [Online]
Available at: https://www.lifewire.com/what-is-a-static-ip-address-2626012

Gibson Research Corporation, 2006. *NAT Router Security Solutions*. [Online]
Available at: https://www.grc.com/nat/nat.htm

Javvin Technologies, 2005. In: *Network Protocols Handbook*. s.l.:Javvin Technologies Inc., p. Page 27.

Mitchell, B., 2019. *Demilitarized Zone in Computer Networking*. [Online]
Available at: https://www.lifewire.com/demilitarized-zone-computer-networking-816407

Mitchell, B., 2019. *When to Use a Static IP Address*. [Online]
Available at: https://www.lifewire.com/using-static-ip-address-on-private-computer-818404

Networks Training, n.d.. *Configuring NAT on Cisco Routers Step-by-Step (PAT, Static NAT, Port Redirection)*. [Online]
Available at: https://www.networkstraining.com/configuring-nat-on-cisco-routers/

PCMag Digital Group, n.d.. *Definition of: port forwarding*. [Online]
Available at: https://www.pcmag.com/encyclopedia/term/49509/port-forwarding

rvigil & mlluis, 2014. *Network Address Translation (NAT) FAQ*. [Online]
Available at: https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/26704-nat-faq-00.html

Viktor17GT, 2019. *How to Give a Static IP to Devices in CISCO PACKET TRACER*. [Online]
Available at: https://www.instructables.com/id/How-to-Give-a-Static-IP-to-Devices-in-CISCO-PACKET/

WhatIsMyIPAddress.com, 2019. *What is Network Address Translation?*. [Online]
Available at: https://whatismyipaddress.com/nat

wiseGEEK, n.d.. *In Computer Networking, what is DMZ?*. [Online]
Available at: https://www.wisegeek.com/in-computer-networking-what-is-dmz.htm