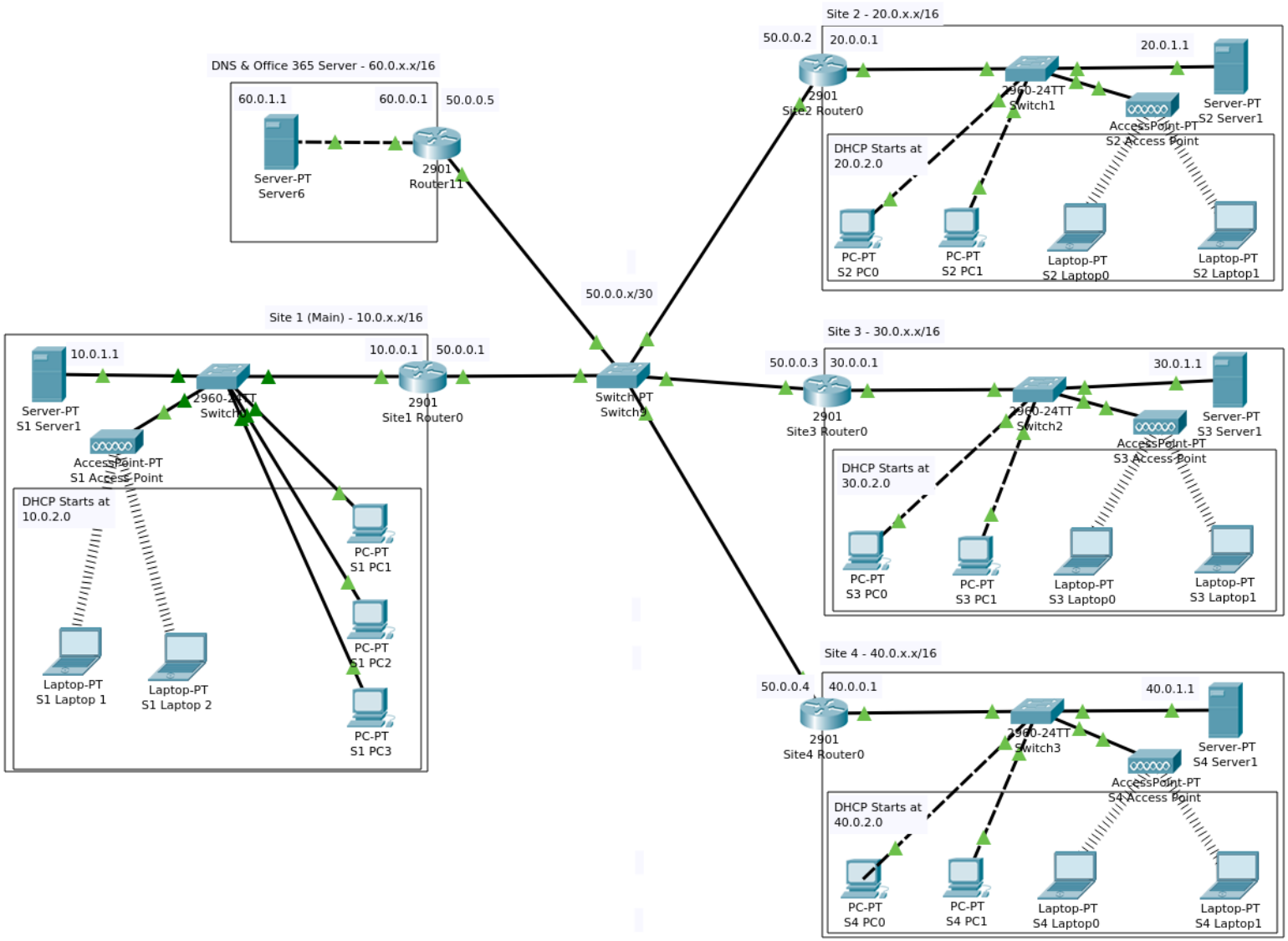
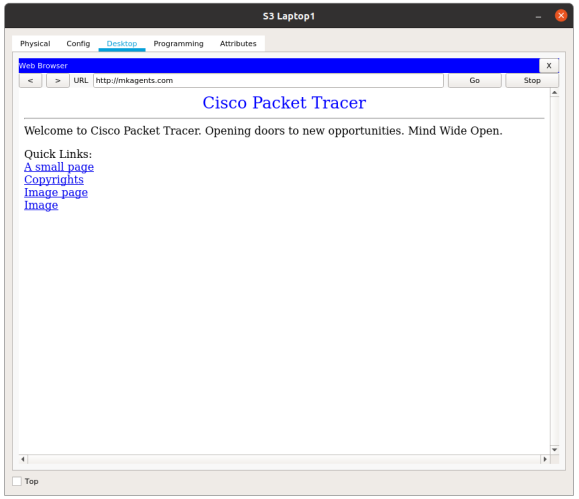
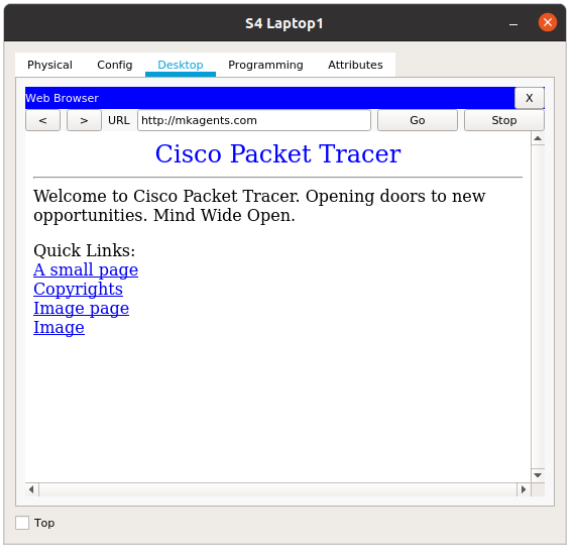
Networking Test Plan



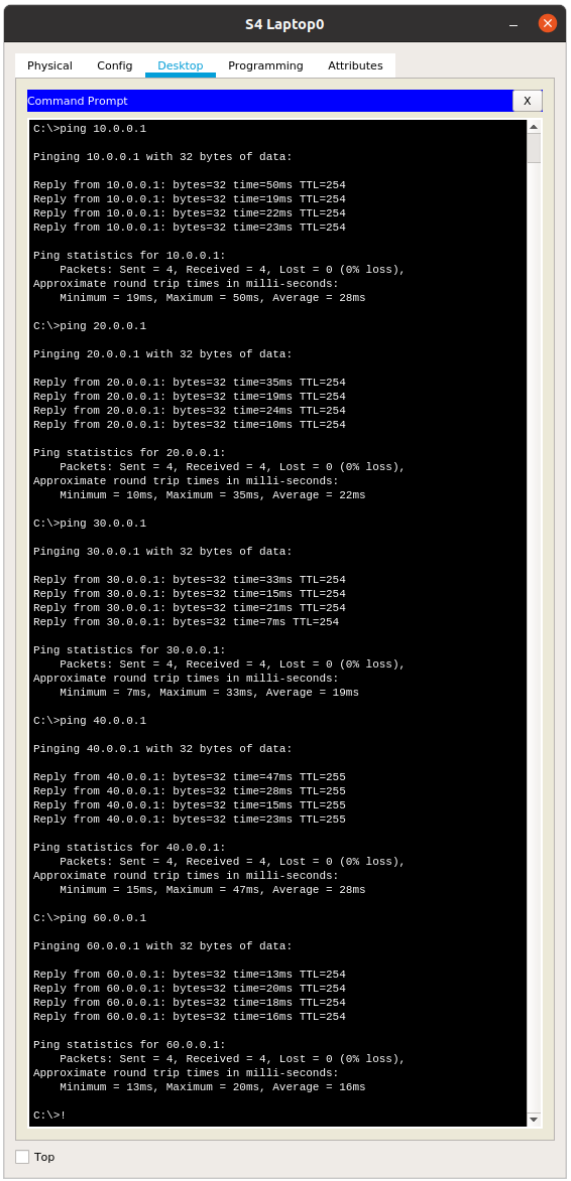
Test Name	Acceptance Criteria	Expected Result	Actual Result	Pass/Fail
`10.0.2.x` device connecting to `mkagents.com`	☑ Client System is assigned DNS settings from DHCP ☑ DNS server is correctly configured to `60.0.1.1` ☐ `60.0.1.1` is reachable from the device ☐ `10.0.1.1` is reachable from the device ☐ In the web browser, `mkagents.com` should load the webpage hosted on `10.0.1.1` server	The DHCP settings are correctly applied, the DNS server is reachable, and the webpage loads normally.	The webpage does not load, because `60.0.1.1` is unreachable for the client.	Fail.
`20.0.2.x` device connecting to `mkagents.com`	☑ Client System is assigned DNS settings from DHCP ☑ DNS server is correctly configured to `60.0.1.1` ☑ `60.0.1.1` is reachable from the device ☐ `10.0.1.1` is reachable from the device ☐ In the web browser, `mkagents.com` should load the webpage hosted on `10.0.1.1` server	The DHCP settings are correctly applied, the DNS server is reachable, and the webpage loads normally.	The webpage does not load. `60.0.1.1` is reachable, however pinging `10.0.1.1` times out.	Fail.

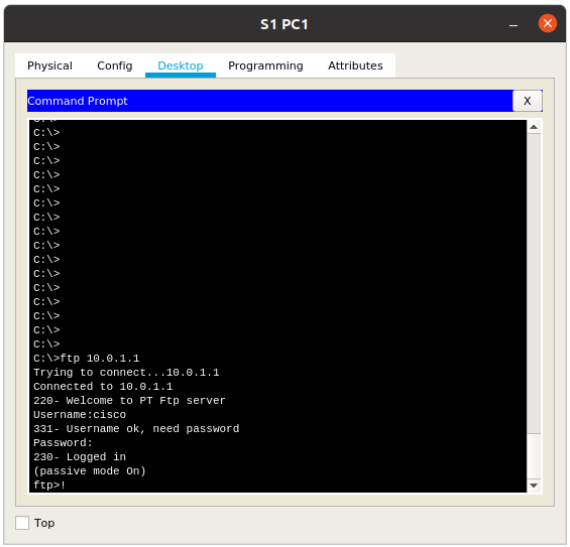
Test Name	Acceptance Criteria	Expected Result	Actual Result	Pass/Fail
`30.0.2.x` device connecting to `mkagents.com`	☑ Client System is assigned DNS settings from DHCP ☑ DNS server is correctly configured to `60.0.1.1` ☑ `60.0.1.1` is reachable from the device ☑ `10.0.1.1` is reachable from the device ☑ In the web browser, `mkagents.com` should load the webpage hosted on `10.0.1.1` server	The DHCP settings are correctly applied, the DNS server is reachable, and the webpage loads normally.	The webpage loads normally. Both `60.0.1.1` and `10.0.1.1` are reachable, DNS is correctly configured, meaning DHCP is configured correctly, and the DNS server resolves the IP correctly. The `10.0.1.1` server then serves the webpage required.	Pass 
`40.0.2.x` device connecting to `mkagents.com`	☑ Client System is assigned DNS settings from DHCP ☑ DNS server is correctly configured to `60.0.1.1` ☑ `60.0.1.1` is reachable from the device ☑ `10.0.1.1` is reachable from the device ☑ In the web browser, `mkagents.com` should load the webpage hosted on `10.0.1.1`	The DHCP settings are correctly applied, the DNS server is reachable, and the webpage loads normally.	The webpage loads normally. Both `60.0.1.1` and `10.0.1.1` are reachable, DNS is correctly configured, meaning DHCP is configured correctly, and the DNS server resolves the IP correctly. The `10.0.1.1` server then serves the webpage required.	Pass 

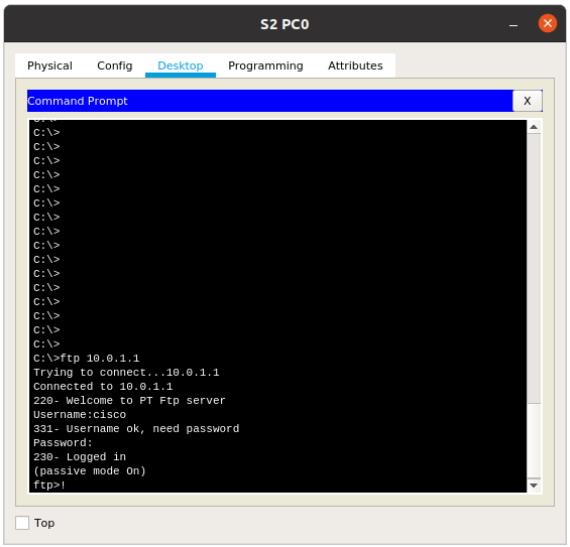
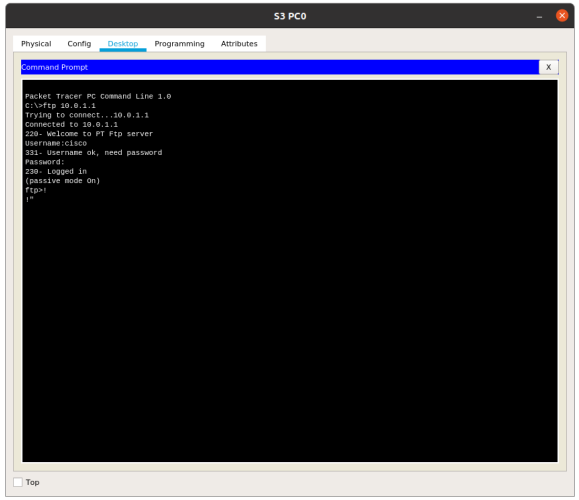
Test Name	Acceptance Criteria	Expected Result	Actual Result	Pass/Fail
`10.0.2.x` device Ping Test	☑ Device can ping to the `10.0.x.x` range ☑ Device can ping to the `20.0.x.x` range ☑ Device can ping to the `30.0.x.x` range ☑ Device can ping to the `40.0.x.x` range ☑ Device can ping to the `60.0.x.x` range	The device can ping to all available address ranges	The device can successfully ping to all available address ranges	Pass 

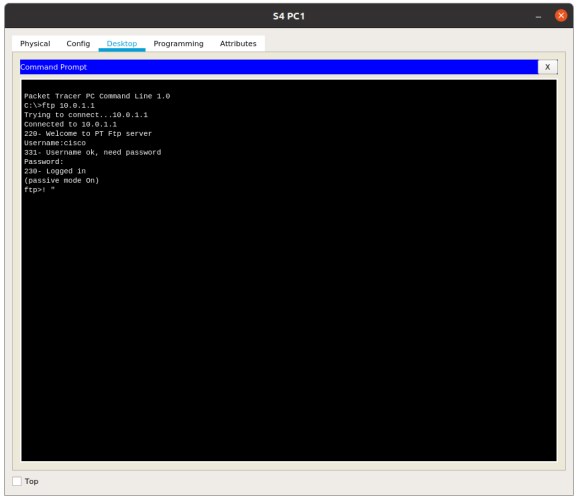
Test Name	Acceptance Criteria	Expected Result	Actual Result	Pass/Fail
`20.0.2.x` device Ping test	☑ Device can ping to the `10.0.x.x` range ☑ Device can ping to the `20.0.x.x` range ☑ Device can ping to the `30.0.x.x` range ☑ Device can ping to the `40.0.x.x` range ☑ Device can ping to the `60.0.x.x` range	The device can ping to all available address ranges	The device can successfully ping to all available address ranges	Pass 

Test Name	Acceptance Criteria	Expected Result	Actual Result	Pass/Fail
`30.0.2.x` device Ping test	☑ Device can ping to the `10.0.x.x` range ☑ Device can ping to the `20.0.x.x` range ☑ Device can ping to the `30.0.x.x` range ☑ Device can ping to the `40.0.x.x` range ☑ Device can ping to the `60.0.x.x` range	The device can ping to all available address ranges	The device can successfully ping to all available address ranges	Pass 

Test Name	Acceptance Criteria	Expected Result	Actual Result	Pass/Fail
`40.0.2.x` device Ping test	☑ Device can ping to the `10.0.x.x` range ☑ Device can ping to the `20.0.x.x` range ☑ Device can ping to the `30.0.x.x` range ☑ Device can ping to the `40.0.x.x` range ☑ Device can ping to the `60.0.x.x` range	The device can ping to all available address ranges	The device can successfully ping to all available address ranges	Pass 

Test Name	Acceptance Criteria	Expected Result	Actual Result	Pass/Fail
`10.0.2.x` device FTP test	☑ Device can reach `10.0.1.1` ☑ Device can utilise `ftp` in the command line to connect and login	The device can use FTP normally	The device can connect with the FTP command	Pass 

Test Name	Acceptance Criteria	Expected Result	Actual Result	Pass/Fail
`20.0.2.x` device FTP test	☑ Device can reach `10.0.1.1` ☑ Device can utilise `ftp` in the command line to connect and login	The device can use FTP normally	The device can connect with the FTP command	Pass 
`30.0.2.x` device FTP test	☑ Device can reach `10.0.1.1` ☑ Device can utilise `ftp` in the command line to connect and login	The device can use FTP normally	The device can connect with the FTP command	Pass 

Test Name	Acceptance Criteria	Expected Result	Actual Result	Pass/Fail
`40.0.2.x` device FTP test	☑ Device can reach `10.0.1.1` ☑ Device can utilise `ftp` in the command line to connect and login	The device can use FTP normally	The device can connect with the FTP command	Pass 

User Feedback

This feedback comes from a screen-sharing session involving the demonstration of systems included in the network design. These features include:

- An allegory for a 'real' DNS server
- Multiple DHCP servers
- Routing tables
- Routers connecting internal site ranges with an external ip range
- Two web servers
- FTP server
- WiFi access points with encryption

> the dhcp ranges seem a little arbitrary, as 10.0.0.0/24 and 10.0.1.0/24 are hardly used at all.

This is true, in another context I would plan the DHCP range to be start at 10.0.0.8 or something, though this requires more knowledge about the quantities of routers, firewalls, other networking equipment, and servers on the network. For the purposes of this network I decided to give networking equipment their own range (10.0.0.0/24) and servers their own range too (10.0.1.0/24), with all other equipment ending up between 10.0.2.0 and 10.0.255.255

> The in-between addresses shouldn't follow the same convention as the internal addresses

This feedback is interesting as it shows an issue in my philosophy behind assigning the IP ranges; I added the 6th pseudo-site (60.0.0.0/16) after setting up the routers to communicate with each other using public addresses in the 50.0.0.0/16 range. This is an issue because further sites past the original four would be in the 60 or 70 or 80 ip range. Additionally, there could only be a small number of sites.

A solution to this issue would be to use the second value in the IP to designate a site, and the first value to designate a general area. Ignoring reserved address pools, this would allow for around 65536 sites without even accommodating NAT. This shows that the current implementation is flawed and should be refactored, even if it's functional.

> Each site needs a firewall

Ideally I'd set each site up to have the local server in a DMZ, as well as having the servers mirror file hosting and web hosting on the first site. For simplicity, however, I didn't include any firewalls in this network design because I felt it would needlessly complicate what is effectively a mockup.

> DNS and DHCP both work well

I generally agree with this, DNS works as it should with DHCP providing a DNS server address correctly. DHCP could be improved as described in the first feedback quote, however.

> Connecting the sites with a switch is good for demonstration purposes

In the real world this connection would likely be replaced with a VPN for security and simplicity. This mockup benefits from having a simple implementation for demonstration, however.

The DNS and Office server isn't realistic as it wouldn't be on the company network

This is true, the Office server would be on the public internet, along with the DNS server. For demonstration, this setup implements these two services into a single server so that DNS could correctly be utilised.

There's no connection to the wider internet

This is an oversight, as I misinterpreted the way this system should be implemented. As with the commentary about the switch being good for demonstration purposes, it would be better suited to have the networks connect with both a VPN and a public internet connection in the current location of each router.

The routing works between each site

I configured the routing table correctly in each router, aided by the simple conversion that it utilises:

20.0.0.0/16 → 50.0.0.**2**/29

The first value of the target address is the last value of the 'next hop' address. This is possible thanks to the configuration in each router following the same rule.

I like how the access points are set up with security and names

This configuration was mostly implemented because Packet Tracer likes to connect all wireless devices to a single access point, regardless of distance. It does simulate signal strength, encryption, and SSIDs, so I implemented them to demonstrate how DHCP also works for access points on each network.