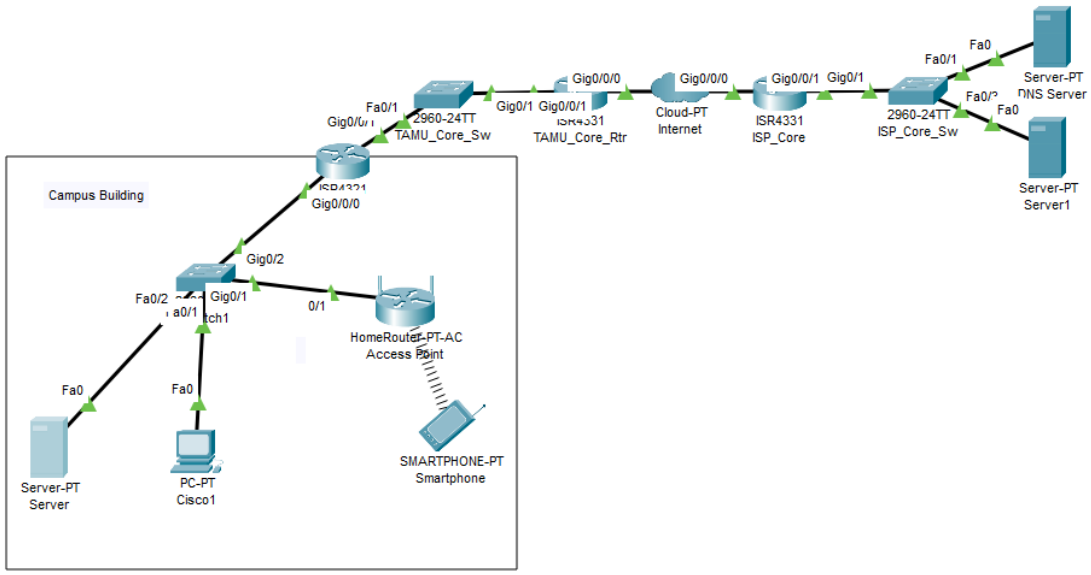
Campus Building Network Solution Example

Purpose:
The following is a network solution for a building on campus with various network configurations on its LAN, that will then connect to the pre-existing campus core network and a DNS server located off the campus network. This network solution allows all internal wired-desktop locations to access the internal server on the LAN, and access to the internet. The network also allows visitors on the Wifi subnet to access the internet, but not access any of the internal services.



Part 1: Address Scheme

This network consists of 2 private IP address subnets 192.168.1.0 /25 and 192.168.1.128 /25. The external facing interface on the router is on the 10.1.1.0 /24 subnet, which is the core layer of the network.

- Wired internal network: 192.168.1.0 /25
- Wireless internal network: 192.168.1.128 /25
- Wired external network: 10.1.1.0 /24

Part 2: Router Security

The following are basic configurations on the router such as hostname and the enable mode password. This router has also been configured for ssh, allowing for remote access.

- The following commands name the router and set the enable mode password
  - `router> enable`
  - `router# configure terminal`
  - `router(config)# hostname R1`
  - `R1(config)# enable secret aggies`
  - `R1(config)# service password-encryption`
  - `R1(config)# banner motd "This is the access router for the Campus Building"`

- The following commands configure SSH on the router
  - `R1(config)# username texas password aggies`
  - `R1(config)# ip domain-name tamu.com`
  - `R1(config)# crypto key generate rsa general-keys modulus 1024`
  - `R1(config)# ip ssh version 2`
  - `R1(config)# line vty 0 4`
  - `R1(config-line)# login local`
  - `R1(config-line)# transport input ssh`
  - `R1(config-line)# end`
  - `R1# copy run start`

Part 3: Router IP Addressing

In this part, the router's IP addresses are assigned to its interfaces. Two DHCP pools were also configured so that each subnet on the LAN is supported.

- The following commands are to configure the IP addresses on the router's ports
  - `R1# configure terminal`

```
R1(config)# interface g0/0/1
R1(config-if)# ip address 10.1.1.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface g0/0/0
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface g0/0/0.1
R1(config-if)# encapsulation dot1q 10
R1(config-if)# ip address 192.168.1.1 255.255.255.128
R1(config-if)# exit
R1(config)# interface g0/0/0.2
R1(config-if)# encapsulation dot1q 20
R1(config-if)# ip address 192.168.1.129
 255.255.255.128
R1(config-if)# exit
```

- The following commands are to configure DHCP pools on the router

```
R1(config)# ip dhcp excluded-address 192.168.1.1
R1(config)# ip dhcp pool Internal-Wired
R1(dhcp-config)# network 192.168.1.0 255.255.255.128
R1(dhcp-config)# default-router 192.168.1.1
R1(dhcp-config)# dns-server 12.12.12.12
R1(dhcp-config)# exit
R1(config)# ip dhcp excluded-address 192.168.1.129
R1(config)# ip dhcp pool Guest-Wifi
R1(dhcp-config)# network 192.168.1.128 255.255.255.128
R1(dhcp-config)# default-router 192.168.1.129
R1(dhcp-config)# dns-server 12.12.12.12
R1(dhcp-config)# end
R1# copy run start
```

- The following command will show what DHCP clients are on the network. To troubleshoot DHCP requests from the PC, use the “release” and “renew” commands in Windows command prompt.
    - `R1# show ip dhcp binding`

Part 4: NAT Overload

The following commands are to configure NAT (overload) on the internal network so that the LAN is protected, while also conserving subnet blocks.

- The following commands are to configure PAT on the router
    - `R1# configure terminal`
    - `R1(config)# int g0/0/0.1`
    - `R1(config-if)# ip nat inside`
    - `R1(config-if)# exit`
    - `R1(config)# int g0/0/0.2`
    - `R1(config-if)# ip nat inside`
    - `R1(config-if)# exit`
    - `R1(config)# int g0/0/1`
    - `R1(config-if)# ip nat outside`
    - `R1(config-if)# exit`
    - `R1(config)# ip access-list standard NAT-ACL`
    - `R1(config-std-nacl)# permit 192.168.1.0 0.0.0.127`
    - `R1(config-std-nacl)# permit 192.168.1.128 0.0.0.127`
    - `R1(config-std-nacl)# exit`
    - `R1(config)# ip nat inside source list NAT-ACL int g0/0/1 overload`

Part 5: Router Access Control

The following commands are to create a standard ACL that will prevent traffic from the Guest Wifi from reaching the internal network.

- Use the following commands to configure standard ACL on the router

```
R1(config)# ip access-list standard BLOCK-GUEST-WIFI
R1(config-std-nacl)# deny 192.168.1.128 0.0.0.127
R1(config-std-nacl)# permit any
R1(config-std-nacl)# exit
R1(config)# interface g0/0/0.1
R1(config-if)# ip access-group BLOCK-GUEST-WIFI out
R1(config-if)# end
```

Part 6: Routing

The following commands are to configure OSPF on the router. This will allow the router to automatically find new routes on the larger campus network and update its table in the case of any failures. A default route is also used to allow traffic to get to the internet by pointing towards the TAMU Core Router.

- The following commands are to configure OSPF on the router

```
R1# configure terminal
R1(config)# router ospf 1
R1(router-config)# router-id 1.1.1.1
R1(router-config)# network 10.1.1.0 0.0.0.255 area 0
R1(router-config)# network 192.168.1.0 0.0.0.127 area 1
R1(router-config)# network 192.168.1.128 0.0.0.127 area 1
R1(router-config)# exit
R1(config)# ip route 0.0.0.0 0.0.0.0 10.1.1.2
R1(router)# exit
R1# copy run start
```

- The following commands are to verify that OSPF has been configured correctly and is working properly.
    - The following command checks the OSPF information on the router
        - `R1# show run | section ospf`
    - The following command shows what routes the router has discovered
        - `R1# show ip route`
    - The following command verifies that the router has found its neighbors
        - `R1# show ip ospf neighbor`

Part 7: Switch Security

The following are basic configurations on the router such as hostname and the enable mode password.

- Use the following commands to name the router
    - `switch> enable`
    - `switch# configure terminal`
    - `switch(config)# hostname SW1`
    - `SW1(config)# enable secret aggies`
    - `SW1(config)# service password-encryption`
    - `SW1(config)# banner motd "This is the access switch for the Campus Building"`

Part 8: Switch VLANs

The following commands are to create VLANs on the switch to segment LAN traffic.

- Use the following commands to configure VLANs on the switch
    - `SW1> enable`
    - `SW1# configure terminal`
    - `SW1(config)# vlan 10`
    - `SW1(config-vlan)# name Wired-Internal`
    - `SW1(config-vlan)# exit`

```
SW1(config)# vlan 20
SW1(config-vlan)# name Guest-Wifi
SW1(config-vlan)# exit
SW1(config)# interface range g1/0/1-2
SW1(config-if)# switchport mode access
SW1(config-if)# switchport access vlan 10
SW1(config-if)# exit
SW1(config)# interface g1/0/3
SW1(config-if)# switchport mode access
SW1(config-if)# switchport access vlan 20
SW1(config-if)# exit
SW1(config)# interface g1/0/25
SW1(config-if)# switchport mode trunk
SW1(config-vlan)# end
SW1# copy run start
```

Part 9: Network Connectivity

The following commands are used to verify connectivity on the network.

- In Windows command prompt, type the following to test internal connectivity
  - `C:\Users\R1> ping 192.168.1.1`
- In Windows command prompt, type the following to test DNS connectivity
  - `C:\Users\R1> ping 12.12.12.12`
- Use the following commands to test access to the website aggie-facts.cisco
  - Open Microsoft Edge
  - In the URL bar, enter the IP address of the website
    - `http://12.12.12.12`

Conclusion:

This network solution for a campus building allows for internal services to run while keeping the Guest Wifi network separated. All parts of the network have access to the internet, but security measures such as ACLs and NATing have been implemented to protect the campus building's network.