**Packet Tracer University Network - Independent Project**

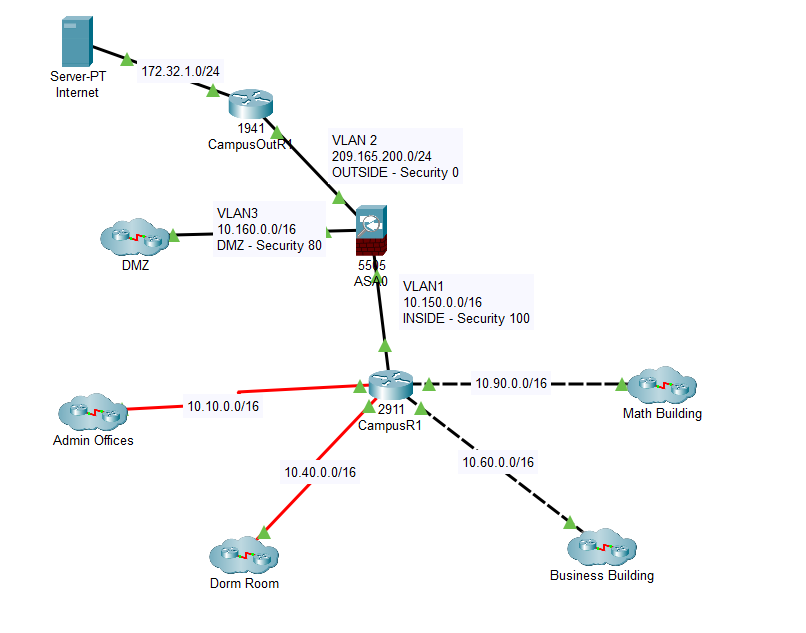
**Hiren Patel and Brooks Teasley**

**November 2023**

**Purpose:** The decision to embark on this project was driven by our shared passion for gaining a deeper understanding of networking and systems. We recognized that theoretical knowledge alone could only take us so far, and that there is no substitute for hands-on experience when it comes to learning the nuances of network architecture. The purpose of this project was to build a network and design the architecture of a university network using the Cisco Packet Tracer software.

**Building a Simple University Network:** To translate theory into practice, we chose to build a simple yet comprehensive university network. This endeavor allowed us to delve into the practical aspects of network design, implementation, and maintenance. By constructing this network from the ground up, we aimed to bridge the gap between textbook concepts and real-world applications.

**Abstract:** The operation of an organization is significantly impacted by computer networks. Universities rely on the efficient operation of their networks for automation, communication, e-learning, administration, and many other purposes. For an organization to transport information in the form of files, communications, and resources in a methodical and economical manner, an effective network is mandatory. This project offers insights into a number of topics, including IP address configuration, logical topology design, and data packets transferred to the many networks located across a university.



**Network Architecture**

Our network topology is split up into the following three sections, separated by a firewall:

1. A secure inside campus network
2. A demilitarized zone (DMZ)
3. An outside network that consists of the wider internet

**Inside Network**

We designed the inside network to replicate a university campus with a number of different buildings. For our example we included administrative offices, a dorm, a business building, and a math building. We set firewall security settings for the internal network to 100, meaning that this internal traffic has the highest level of trust.

Routers act as the core layer of our network topology. We created one router for each “building” in our campus network, with one additional router connecting each of the buildings. We intentionally used one router with both serial and gigabit connections to routers in the buildings to learn more about Network Architecture. We detail this more in Section 1 - Routers.

The admin offices include a couple local networks separated into broadcast domains by a building router. We added devices that may be found in a typical office LAN, such as a printer, IP phones, and desktop computers. We also included DNS and DHCP servers so the entire inside network has access to those services, and so that they can be centrally managed from the administrative offices.

The other network clusters include the Dorm, the Business Building, and the Math Building. These sites include a number of different types of end-devices such as PCs, Laptops, and smartphones. We added wireless access points in each cluster, assuming that this would be the primary way students would access the network in a modern university architecture.

**DMZ**

We created our DMZ as a way to filter traffic from the outside internet. However, traffic from inside the network is still able to access both the outside network and the DMZ. Because we are less trusting of traffic coming from the wider internet, we set the security for our DMZ to 80.

We added the DMZ to the Secure Byte University topology under the assumption that people would need to access the email and web server from both inside and outside the network. We assume that Secure Byte University will also have a good deal of traffic from outside the network trying to access the university. Finally, students, alumni, and university staff will want to access the University email server as well.

**Outside Network**

The outside network is meant to represent the wider internet. We added a router on the outside of the firewall to imitate a campus router that is connected to an Internet Service Provider. Because we trust traffic from the rest of the internet the least, we set the security on our firewall to 0, representing the highest level of security.

The firewall settings were configured so that traffic coming from the internet could access the DMZ, but not anywhere in the internal network. Each network is separated by a VLAN which connects to the firewall. This prevents outside traffic from reaching the inside network, while allowing traffic to access the DMZ containing an email and web server.

**Devices**

Our network consists of a wide variety of devices that can be found in a modern university network architecture. We used the following devices in our network:

1. Router (1941 & 2911)
2. Switches (2960-24TT)
3. Access Points
4. Firewall
5. Servers: DNS, Web, Email, DHCP
6. End-devices: Personal computers, laptops, smartphones
7. Peripherals: Printers, IP Phones

**Section 1 - Routers**

To get the routers to communicate with each other we used two separate methods to connect them. First, we statically assigned a 0.0.0.0 network address along with the default gateway, which is the IP address of the receiving router. This allowed the router to forward any unknown IP to the next hop router. In the case of the Math and Business buildings, we used a crossover cable that connected to the campus router’s gigabit ports. In the other case, we elected to use the router's serial ports. However, this required us to manually add a device to the campus router to allow it to communicate via the serial ports. This was the HWIC-2T device, a Cisco 2-Port Serial High-Speed WAN Interface Card, providing 2 serial ports. The use of the 0.0.0.0 route with routers is also known as the Gateway of Last Resort.

We elected to use a DHCP server in our network topology instead of having each router use its own DHCP service. To do this, we had to add the DHCP IP address to the router via IP helper, this way the router knows where to direct the traffic when a device is looking to dynamically get an IP address. The DHCP for all devices connected to the internal campus network from the Administrative Offices.

**Section 2 - Switches**

We added switches in the various buildings to add a distribution layer device so connect each of the devices on the individual networks. We changed the hostname of each device to reflect their location in the topology. We connected them to the end devices, access points, and routers with straight through cables.

**Section 3 - Access Points**

We decided to include wireless access points in our classrooms to simulate 2.4 and 5 GHz connections to be able to handle both types of devices. We secured our networks by changing the default SSID, changing security to WPA2 Personal, and creating a password: sburules!

**Section 4 - Firewall**

We applied the following steps for incoming traffic to the firewall. First, we added a class map to identify traffic coming in, followed by a policy map to identify action to take on the actual traffic. We then adjusted the service policy, which is what we used to implement the previous steps. We set up the host name, domain name, password, activated VLAN1 and 2 inside and outside, and added a password of “sbu1”.

We integrated Static IP routing mechanisms into the firewall configuration, introducing a strategic approach to defining routing paths for incoming traffic. Through the establishment of static routes, we ensured that incoming traffic could be efficiently directed back to the source IP, facilitating optimal bidirectional communication.

Dynamic NAT was configured for outbound traffic originating from internal networks, allowing the mapping of internal private IP addresses to a pool of public IP addresses when accessing external networks. Additionally, Static NAT was implemented for specific internal and DMZ resources, facilitating inbound traffic from the internet by maintaining consistent mappings.

To align with security policies and access controls, we applied NAT to incoming traffic destined for the DMZ from the outer layer. This involved strategically translating source IP addresses to ensure that the traffic could seamlessly reach the DMZ, striking a balance between accessibility and stringent security measures.

Throughout the project, we successfully addressed a number of challenges with our firewall, such as establishing efficient bidirectional communication channels, ensuring that incoming traffic, after undergoing NAT and static IP routing, could traverse back to the source IP. Additionally, we navigated the complexities of DMZ access control, strategically implementing NAT for incoming DMZ traffic to uphold security policies.

We encountered a limitation to the firewall for this free version of Packet Tracer so we could not add more than 3 VLANs and even this third one, we were limited because we had to put in that it was not allowed to forward traffic to one of our other VLANs.

**Section 5 - Servers**

Our network includes a web server, email server within the DMZ, and a DNS server, and DHCP server in the administrative offices.

We can type in their fully qualified domain name or partial domains, including www.sbu.edu, sbu.edu or even just “sbu” and still reach the Secure Byte University website, reflecting how websites in real life use the Domain Name System. However, when the site is loaded, the fully qualified domain name does not show on the URL toolbar as it would in the real world due to Packet Tracer DNS server limitations.

**Section 6 - End-devices & Peripherals**

We enabled DHCP on the end-devices to connect to the respective default gateways in each “building,” automatically assigning IP addresses, subnet masks, and the IP of the DNS server that we located in the admin office.

We added the IP addresses statically on the servers and other devices like printers because those addresses do not need to change or should not renew their IP addresses automatically.

Peripherals in our network simply consisted of a printer and IP phones. We assigned a static IP to the printer because it is considered a ‘best practice’ as a printer is a device that is meant to be constantly connected to the network.

|  | **Device** | **Interface** | **IP Address** | **Subnet Mask** | **Default Gateway** |
| --- | --- | --- | --- | --- | --- |
| Main Map | Firewall Inside | VLAN 1 | 10.150.0.1 | 255.255.0.0 |  |
| Firewall Outside | VLAN 2 | 209.165.200.1 | 255.255.255.0 |  |
| Firewall DMZ | VLAN3 | 10.160.0.1 | 255.255.0.0 |  |
| CampusOut R1 | G0/0 | 172.32.1.1 | 255.255.255.0 |  |
| G0/1 | 209.165.200.2 | 255.255.255.0 |  |
| Internet Server | Fe0/0 | 172.32.1.2 | 255.255.255.0 |  |
| CampusR1 | G0/0 | 10.150.0.2 | 255.255.0.0 |  |
| G0/1 | 10.90.0.1 | 255.255.0.0 |  |
| G0/2 | 10.60.0.1 | 255.255.0.0 |  |
| Se0/0/0 | 10.10.0.1 | 255.255.0.0 |  |
| Se0/0/1 | 10.40.0.1 | 255.255.0.0 |  |
| Admin Building  Admin Building (contd.) | Router ABR1 | Serial 0/0/1 | 10.10.0.2 | 255.255.0.0 |  |
| G0/1 | 10.20.0.1 | 255.255.0.0 |  |
| G0/2 | 10.30.0.1 | 255.255.0.0 |  |
| Switch  ABSW1 | Fe0/1 |  |  | 10.20.0.1 |
| Switch ABSW2 | Fe0/1 |  |  | 10.30.0.1 |
| DNS Server |  | 10.30.0.25 | 255.255.0.0 |  |
| DHCP Server |  | 10.30.0.20 | 255.255.0.0 |  |
| Dorm Building | Router DRR1 | Se0/0/0 | 10.40.0.2 | 255.255.0.0 |  |
| G0/1 | 10.50.0.1 | 255.255.0.0 |  |
| Switch DRSW1 |  |  |  | 10.50.0.1 |
| Math Building | Router MBR1 | G0/0 | 10.90.0.2 | 255.255.0.0 |  |
| G0/1 | 10.100.0.1 | 255.255.0.0 |  |
| G0/2 | 10.110.0.1 | 255.255.0.0 |  |
| Switch MBSW1 | Fe0/1 |  |  | 10.100.0.1 |
| Switch MBSW2 | Fe0/1 |  |  | 10.110.0.1 |
| Business Building  Business Building (contd.) | Router BBR1 | G0/0 | 10.60.0.2 | 255.255.0.0 |  |
| G0/1 | 10.70.0.1 | 255.255.0.0 |  |
| G0/2 | 10.80.0.1 | 255.255.0.0 |  |
| Switch BBSW1 |  |  |  | 10.70.0.1 |
| Switch BBSW2 |  |  |  | 10.80.0.1 |
| DMZ | Router DMZR1 | 0/0 | 10.160.0.2 | 255.255.0.0 |  |
| 0/1 | 10.170.0.1 | 255.255.0.0 |  |
| Switch DMZS1 |  |  |  | 10.170.0.1 |
| Web Server | Fe0/0 | 10.170.0.20 | 255.255.0.0 |  |
| Email Server | Fe0/0 | 10.170.0.30 | 255.255.0.0 |  |