NAME:Botcha sharmila

AICTEID:STU6450fd1ee35d81683029278

ROLLNO:21VV1A0512

Cyber security

Industry Problem Statement

Problem Statement: I have chosen JNTU-GV campus and I have analyzed its network topology.

Map the network using Cisco Packet Tracer and identify the security controls that are in place, such as network segmentation, intrusion detection systems, firewalls, and authentication and authorization systems.

Apply the knowledge gained from the NetAcad cyber security course to conduct an attack surface mapping, aiming to identify potential entry points for cyber-attacks. Propose countermeasures to mitigate these risks.

Tasks

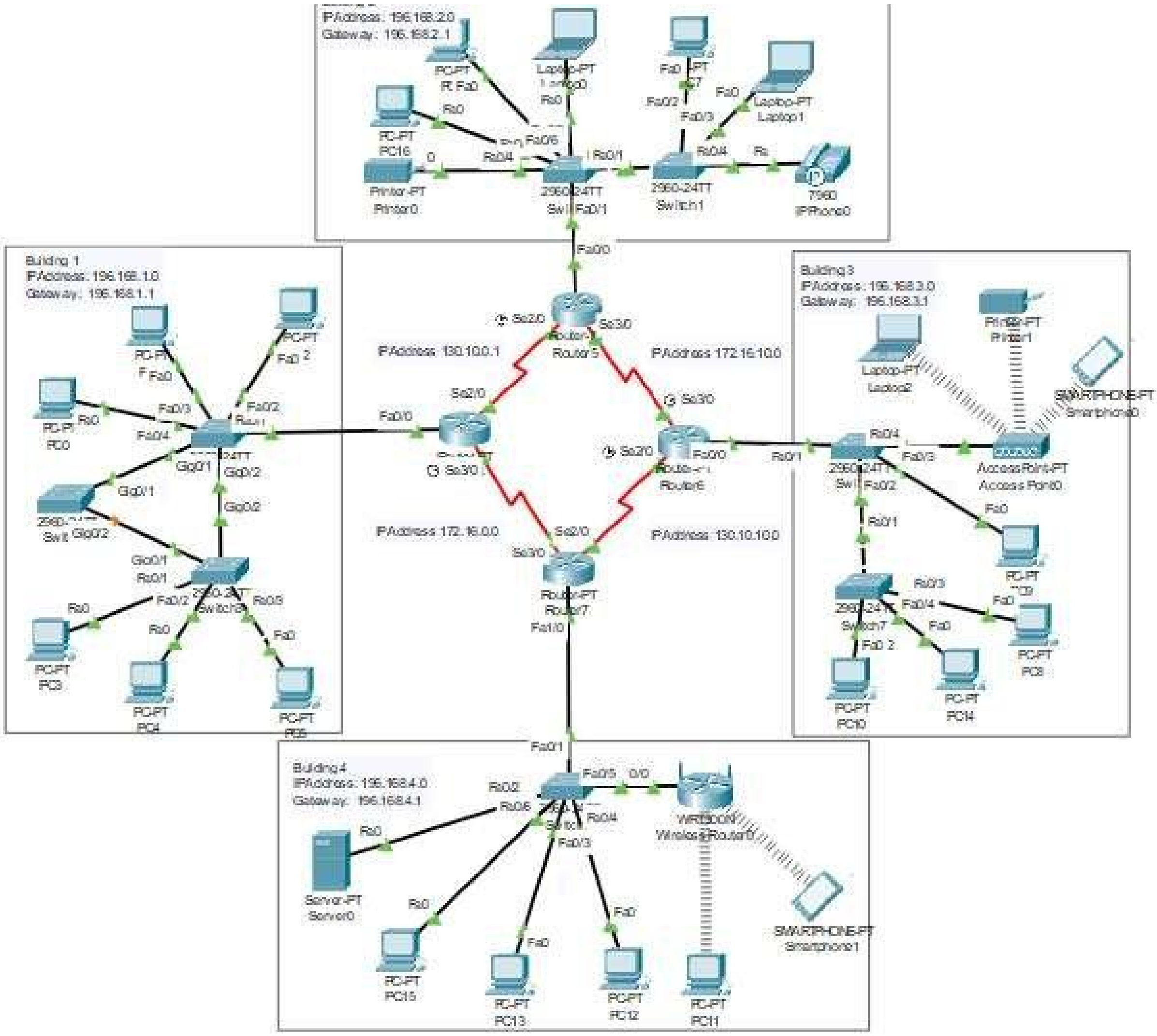
Campus Network Analysis: Choose a university or college campus and conduct an analysis of its existing network topology, including the layout, devices, and connections.

Description:

Network Analysis is useful in many living application tasks. It helps us in deep understanding the structure of a relationship in social networks, a structure or process of change in natural phenomenons, or even the analysis of biological systems of organisms

Again, let’s use the network of social media users as an example. Analyzing this network helps in

- This network design simulates a real life campus network. It contains devices needed to create the network and all associated configuration.



Campus network architecture

Description:

1.<u>Campus Selection :</u> We selected [University/College Name] as the target for our network analysis. This involved obtaining necessary permissions and cooperation from the university's CSE department.

2.<u>Data Gathering :</u> We gathered network documentation, diagrams, and other relevant materials provided by the university's CSE team.

Additionally, we conducted interviews with network administrators to gain insights into the network design and setup.

3.Physical Site Visit : We visited the campus to observe the network infrastructure firsthand. This on-site visit allowed us to identify the physical locations of network devices and the interconnections between them.

4.Network Scanning : Utilizing network scanning tools, we performed a scan of the campus network to discover active hosts, IP addresses, open ports, and network services running on devices.

5.Network Diagramming : Based on the gathered information, we created a detailed network topology diagram. The diagram depicted the layout of the network, including the placement and interconnectivity of routers, switches, access points, firewalls, servers, and other network devices.

Findings:

1.Network Layout : The network is distributed across various buildings and departments within the campus. Each building has its local network infrastructure, connected to a centralized core network.

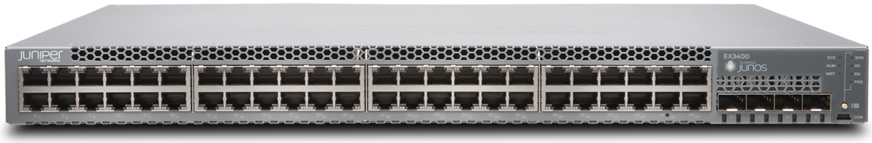
2.Devices : The campus network consists of a mix of networking devices, including Cisco routers, switches, and wireless access points. There are also firewalls deployed at the network perimeter. Let’s go through the devices in detail.

Routers:

The router is a physical or virtual internetworking device that is designed to receive, analyze, and forward data packets between computer networks. A router examines a destination IP address of a given data packet, and it uses the headers and forwarding tables to decide the best way to transfer the packets.

Access switch:

Access switch is the only one that directly interacts with end-user devices. Because an access network switch connects the majority of devices to the network, it normally has the highest port density of all switch types. In spite of the high port count, access switch usually provides the lowest throughput per port.



Server:

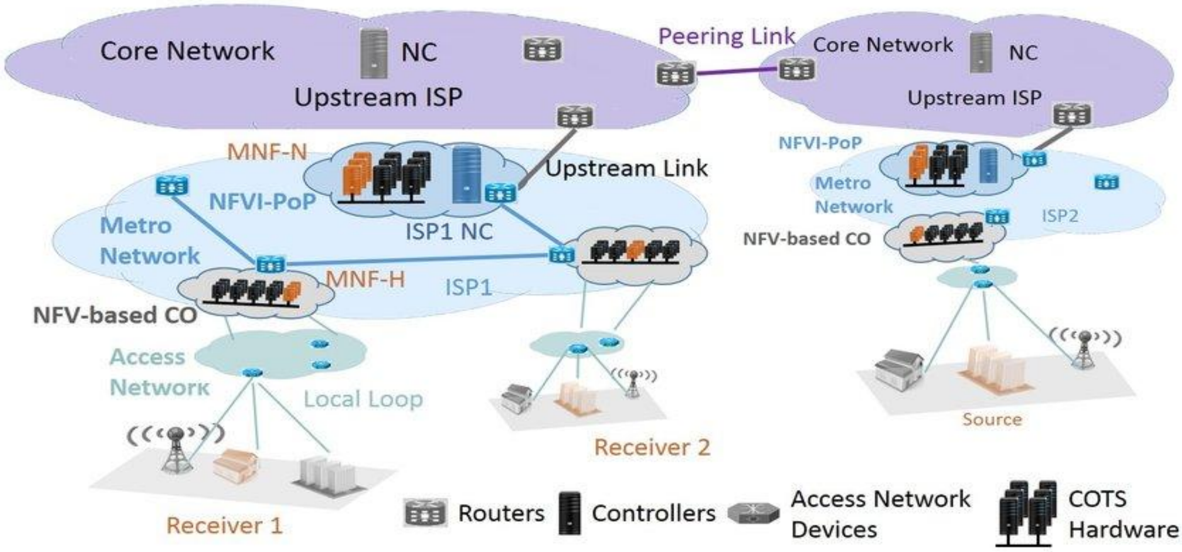
A server is a computer program or a device that provides functionality forcalled clients which are other programs or devices. This architecture is called the client–server model. A single overall computation is distributed across multiple processes or devices. Servers can provide various functionalities called services. These services include sharing data or resources among multiple clients, or performing computation for a client. Multiple clients can be served by a single server, and a single client can use multiple servers.

PC:

A Network Node can be illustrated as Equipment for Data Communication like a Modem, Router, etc., or Equipment of a Data Terminal like connecting two computers or more. Link in Computer Networks can be defined as wires or cables or free space of wireless networks.

The working of Computer Networks can be simply defined as rules or protocols which help in sending and receiving data via the links which allow Computer networks to communicate. Each device has an IP Address, that helps in identifying a device.

ISP:



ISP is a company that provides individual users and businesses with connectivity to the Internet. Internet service providers (ISPs) also provide clients with access to Internet services such as Web hosting, Simple Mail Transfer Protocol (SMTP) mail, Usenet newsgroups, Internet Relay Chat (IRC), and downloadable Internet software.ISPs come in various shapes and sizes, from volunteer-run freenets to local, regional, and national service providers such as America Online. Many smaller ISPs, especially those that originated in a university environment, still use freely available software such as Linux, Apache's Web server, and Sendmail for providing services to customers.

3.Network Segmentation : The network is segmented into different VLANs, providing separation between various user groups and departments. This segmentation helps in managing traffic and improving security.

4.Network Connectivity : The network connectivity is primarily wired, with Ethernet connections provided to desktops, printers, and other devices. Wi-Fi access is available in all campus buildings.

All PC's can ping the internet (which is avaliable at 8.8.8.8 dns)

Each device in each vlan and each department can ping each other.

PC's in different departments cannot ping each other.

PC's And Server are assigned ip address by dhcp.

PC'S and Servers in the schools private datacenter can only ping each other and not the outside world.

5.Security Controls : Firewalls are strategically placed at the network's edge to control incoming and outgoing traffic. Access controls are enforced using VLANs and network policies.

Assessment:

1.Security : The network's use of VLANs and firewalls contributes to its security by isolating different segments, reducing the impact of potential security breaches.

2.Network Performance : The network is well-designed with adequate bandwidth capacity to handle the current user load and data traffic.

3.Redundancy : Some critical areas of the network lack redundancy, making them susceptible to single points of failure.

4.Wireless Network Security : The Wi-Fi network has WPA2 encryption enabled, but there is room for improvement with WPA3 implementation for enhanced security.

Recommendations:

1.Redundancy : Implement redundancy in critical network components to improve network availability and reduce downtime.

2.Network Monitoring : Deploy a robust network monitoring system to proactively detect and address potential issues.

3.Security Updates : Ensure timely security updates and patches for network devices and infrastructure.

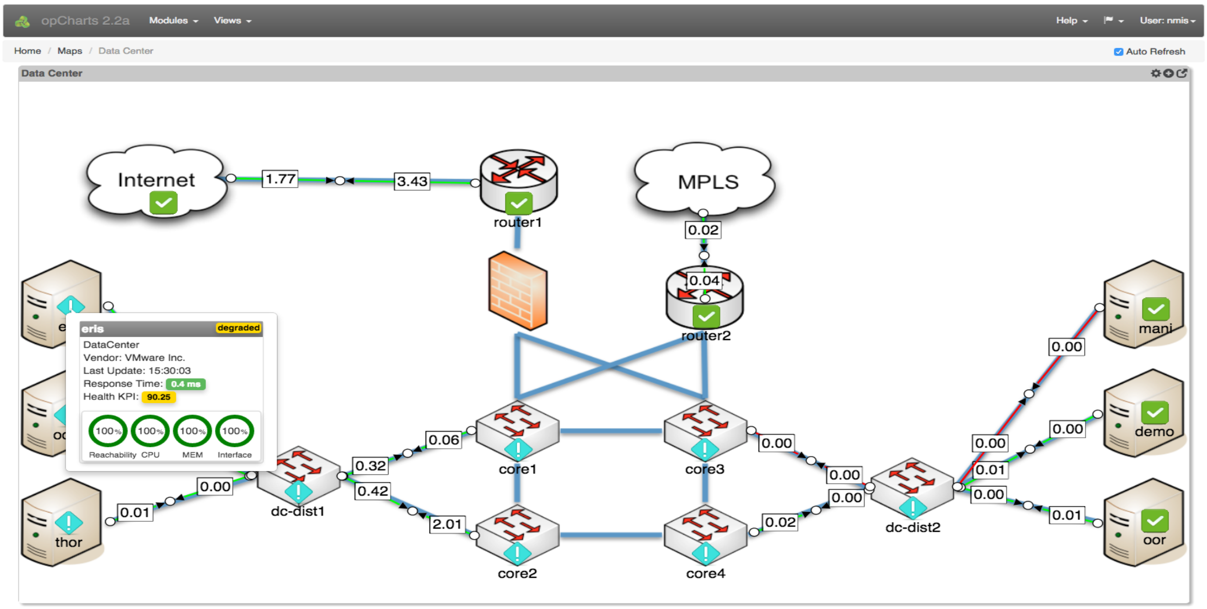
4.Wireless Network Security : Upgrade Wi-Fi security to WPA3 for better protection against wireless attacks.

Conclusion:

The campus network analysis of [University/College Name] provided valuable insights into its existing network topology, layout, devices, and connections. The network's use of VLANs and firewalls demonstrated a strong commitment to security. However, implementing redundancy, improving network monitoring, and enhancing wireless network security will further strengthen the network's performance and security. Our recommendations aim to enhance the overall stability and security of the campus network to ensure a reliable and secure computing environment for students, faculty, and staff.

2.Network Mapping:

Utilize Cisco Packet Tracer to map the network infrastructure, representing the placement and interconnectivity of routers, switches, firewalls, and other relevant network components.



eris degraded
DataCenter
Vendor: VMware Inc.
Last Update: 15:30:03
Response Time: 0.4 ms
Health KPI: 90.25

Introduction:

In this task, we utilized Cisco Packet Tracer, a powerful network simulation tool, to create a comprehensive network map of [University/College Name] campus. The primary goal was to visually represent the placement and interconnectivity of routers, switches, firewalls, and other relevant network components, providing a clear understanding of the campus network infrastructure.

Description:

1.Data Collection: We collected essential network information, including IP addresses, device configurations, network segments, and interconnections, from the university's CSE department.

2.Cisco Packet Tracer Setup: We configured Cisco Packet Tracer to simulate the campus network environment accurately.

3.Device Placement: Based on the collected data, we virtually placed routers, switches, firewalls, and other relevant devices on the Packet Tracer workspace. We ensured accurate positioning to reflect their real-life physical locations.

4.Interconnections: We established virtual connections between devices using appropriate cables and interfaces to replicate the actual network setup.

5.VLAN Segmentation: To depict VLAN segmentation, we logically grouped devices into separate VLANs and established trunk links to enable communication between them.

6.Network Services: We added essential network services such as DHCP servers, DNS servers, and gateway configurations to ensure proper network functionality.

7.Wireless Infrastructure: We incorporated wireless access points throughout the campus to represent the Wi-Fi coverage.

8.Firewall Configuration: We configured firewalls to control incoming and outgoing traffic, simulating their role in securing the network.

Network Mapping Results:

1.Core Network: The core network was depicted with high-end Cisco routers and switches, forming the backbone of the campus network.

2.Distribution Layer: Layer 3 switches were placed in the distribution layer, facilitating inter-VLAN routing and connecting to access switches.

3.Access Layer: Access switches were positioned to connect end-user devices such as computers, printers, and IP phones.

4.Wireless Infrastructure: Wireless access points were strategically positioned across the campus to ensure comprehensive Wi-Fi coverage.

5.Firewalls: Firewall configurations were integrated at the network's edge to manage and secure incoming and outgoing traffic.

6.DHCP and DNS Servers: Centralized DHCP and DNS servers were set up to provide IP addressing and name resolution services.

Network Configurations used:

This is a campus network design which implements

1. HSRP
2. EIGRP
3. PORTCHANNEL
4. NAT
5. DHCP
6. THREE TIER NETWORK DESIGN
7. PORT SECURITY

8. PARTIAL MESH DESIGN

9. VLANS

10.IP ADDRESSSING

11.SPANNING-TREE ROOT-BRIDGE

Let’s figure out about them in detail…

1. HSRP:

In computer networking, the Hot Standby Router Protocol (HSRP) is a Cisco proprietary redundancy protocol for establishing a fault-tolerant default gateway. Version 2 of the protocol is mostly used Version 2 of the protocol introduces stability, scalability and diagnostic improvements.

The primary router with the highest configured priority will act as a virtual router with a pre-defined gateway IP address and will respond to the ARP or ND request from machines connected to the LAN with a virtual MAC address.

E.G:

ON THE FIRST ROUTER (R1)

interface Vlan3

standby 3 ip 192.168.3.1 — — assigning a virtual ip to HSRP group “3”

standby 3 priority 120 ! — — Assign a priority (120 in this case) to the router interface Vlan3! for a particular group number (3). The default is 100.

standby 3 preempt: — — Allows the router to become the active router when the priority is higher than all other HSRP-configured routers in the hot standby group. If you do not use the standby preempt command in the configuration .for a router, that router does not become the active router, even if the priority is higher than all other routers.

ON THE OTHER ROUTER (R2)

```
interface Vlan3
standby 3 ip 192.168.3.1 — — This becomes the standby router.
```

2.EIGRP:

Enhanced Interior Gateway Routing Protocol (EIGRP) is an advanced distance-vector routing protocol that is used on a computer network for automating routing decisions and configuration. The protocol was designed by Cisco Systems as a proprietary protocol, available only on Cisco routers.

E.G

ON THE ROUTER

```
router eigrp 1
network 0.0.0.0
no auto-summary.
```

3. PORT-CHANNEL

A port channel is an aggregation of multiple physical interfaces that creates a logical interface. You can bundle up to eight individual active links into a port channel to provide increased bandwidth and redundancy. Port channeling also load balances traffic across these physical interfaces.

It can be statically (on /off) and LACP(Active and Passively enabled)

E.G

ON THE SWITCH:

Initialise the port-channel:

```
switch(config)# interface port-channel 1

switch(config-if)# channel-group 1mode active
```

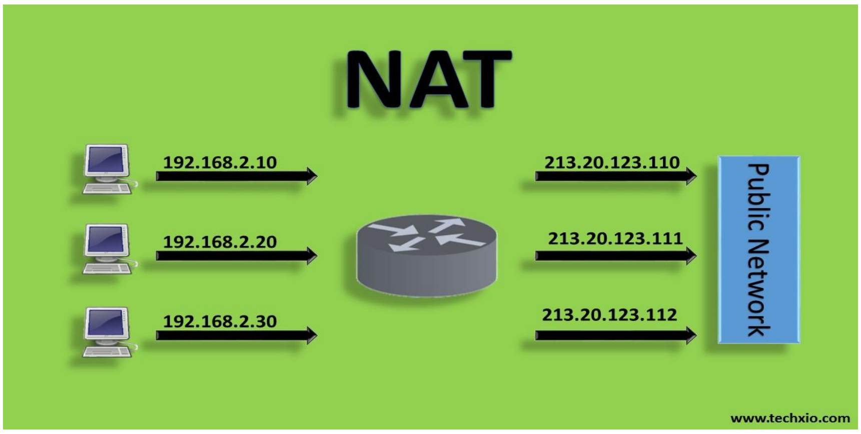
how to add an Ethernet interface 1/4 to channel group 1:

```
switch# configure terminal

switch (config)# interface ethernet 1/4

switch(config-if)# switchport mode trunk

switch(config-if)# channel-group 1
```

4. NAT(Network Address Translation):

Network address translation (NAT) is a method of remapping an IP address space into another by modifying network address information in the IP header of packets while they are in transit across a traffic routing device.

It has become a popular and essential tool in conserving global address space in the face of IPv4 address exhaustion. One Internet-routable IP address of a NAT gateway can be used for an entire private network.



E.G

ON THE ROUTER

on the inside interface

```
interface GigabitEthernet0/1

ip address 10.0.0.62 255.255.255.252

ip nat inside
```

on the outside interface

```
interface GigabitEthernet0/1/0

description Global IP to ISP

ip address 200.0.0.1 255.255.255.252

ip nat outside

ip nat inside source list 5 interface GigabitEthernet0/1/0 overload

ip classless

ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/1/0
```

5. DHCP:

The Dynamic Host Configuration Protocol (DHCP) is a network management protocol used on Internet Protocol (IP) networks, whereby a DHCP server dynamically assigns an IP address and other network configuration parameters to each device on the network, so they can communicate with other IP networks.

A DHCP server enables computers to request IP addresses and networking parameters automatically from the Internet service provider (ISP), reducing the need for a network administrator or a user to manually assign IP addresses to all network devices.

E.G: DHCP ON A ROUTER

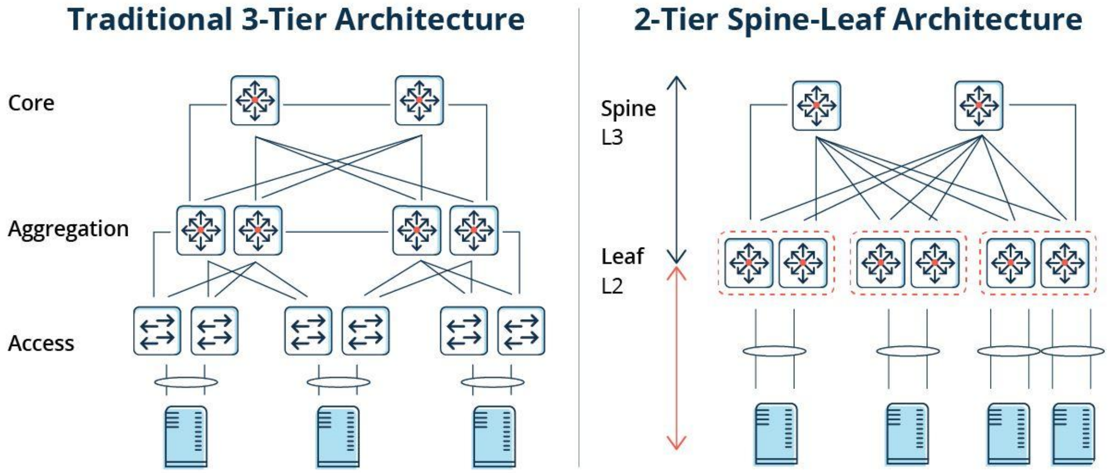
```
ip dhcp excluded-address 192.168.3.1 192.168.3.3

ip dhcp pool VLAN3

network 192.168.3.0 255.255.255.0

default-router 192.168.3.1
```

dns-server 8.8.8.8 — — (Optional,for testing)

domain-name IPvZero.com — — (Optional,for testing)

6. THREE TIER NETWORK DESIGN:

THREE TIER NETWORK DESIGN


Traditional 3-Tier Architecture
Core
Aggregation
Access
2-Tier Spine-Leaf Architecture
Spine
L3
Leaf
L2

Core Layer

Core Layer consists of biggest, fastest, and most expensive routers with the highest model numbers and Core Layer is considered as the back bone of networks. Core Layer routers are used to merge geographically separated networks. The Core Layer routers move information on the network as fast as possible. The switches operating at core layer switches packets as fast as possible.

Distribution layer:

The Distribution Layer is located between the access and core layers. The purpose of this layer is to provide boundary definition by implementing access lists and other filters. Therefore the Distribution Layer defines policy for the network. Distribution Layer include high-end layer 3 switches. Distribution Layer ensures that packets are properly routed between subnets and VLANs in your enterprise.

Access layer

Access layer includes access switches which are connected to the end devices (Computers, Printers, Servers etc). Access layer switches ensures that packets are delivered to the end devices.

7.PORT SECURITY:

Port Security helps secure the network by preventing unknown devices from forwarding packets. When a link goes down, all dynamically locked addresses are freed. The port security feature offers the following benefits: You can limit the number of MAC addresses on a given port.

It is usually configured on a switch interface

E.G

ON THE SWITCH

```
switchport port-security

switchport port-security maximum 2 — — “2 Devices”

switchport port-security mac-address sticky

switchport port-security violation restrict — — “means restrict if violated”

switchport port-security mac-address sticky

spanning-tree portfast — — “enables forwarding state”

spanning-tree bpduguard enable — -”PortFast BPDU guard prevents loops when a BPDU is received on that port”

storm-control broadcast level 40
```

8.PARTIAL MESH DESIGN:

In partial-mesh topology, some of the devices are connected to many devices together, but other devices are connected only to one or two devices. E.G The three tier design.

9.VLANS:

VLANs (Virtual LANs) are logical grouping of devices in the same broadcast domain. VLANs are usually configured on switches by placing some interfaces into one broadcast domain and some interfaces into another. Each VLAN acts as a subgroup of the switch ports in an Ethernet LAN.

The purpose of implementing a VLAN is to improve the performance of a network or apply appropriate security features. They can TRUNK and ACCESS.

E.G

ON THE SWITCH

```
switch# configure terminal

switch(config)# vlan 5

switch(config-vlan)# name accounting

switch(config-vlan)# state active

switch(config-vlan)# no shutdown
```

TRUNK VLAN

```
switchport trunk encapsulation dot1q

switchport mode trunk
```

ACCESS VLAN

```
switchport access vlan 5
switchport mode access
```

10. IP ADDRESSING:

An IP address is an address used in order to uniquely identify a device on an IP network. The address is made up of 32 binary bits, which can be divisible into a network portion and host portion with the help of a subnet mask. The 32 binary bits are broken into four octets (1 octet = 8 bits).

It is divided into class A-D

E.G

```
interface FastEthernet0/3

ip address 10.0.0.5 255.255.255.252
```

11.SPANNING-TREE ROOT-BRIDGE:

The Root bridge (switch) is a special bridge at the top of the Spanning Tree (inverted tree). The branches (Ethernet connections) are then branched out from the root switch, connecting to other switches in the Local Area Network (LAN). All Bridges (Switches) are assigned a numerical value called bridge priority.

Bridge Priority (Switch Priority) Value is a 16-bit binary number. By default, all Cisco Switches has a Bridge Priority (Switch Priority) value of 32,768.

The root bridge of the spanning tree is the bridge with the smallest (lowest) bridge ID. Each bridge has a configurable priority number and a MAC address; the bridge ID is the concatenation of the bridge priority and the MAC address. It is the preferred route

E.G

ON THE SWITCH

```
spanning-tree mode rapid-pvst

spanning-tree vlan 3,9 priority 24576
```

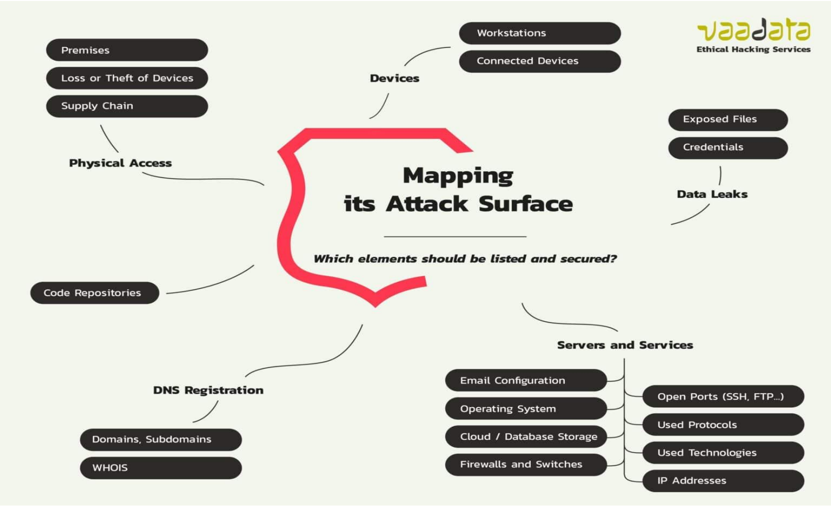
```
spanning-tree vlan 5,14 priority 28672
```

Conclusion:

The completion of the network mapping project using Cisco Packet Tracer has provided a detailed and visually informative representation of [University/College Name] campus network infrastructure. By accurately mapping the placement and interconnectivity of routers, switches, firewalls, and other relevant network components, we have gained valuable insights into the network's architecture and design. The network map serves as an essential tool for network administrators to manage, troubleshoot, and optimize the campus network effectively. It will aid in identifying potential areas for improvement, ensuring network stability, and enhancing security measures to create a robust and efficient computing environment for students, faculty, and staff.

3. Attack Surface Mapping:

Conduct an attack surface mapping exercise to identify potential vulnerabilities and weaknesses within the network architecture and design, considering factors such as unauthorized access, data breaches, and network availability.



Introduction:

In this task, we conducted an attack surface mapping exercise to identify potential vulnerabilities and weaknesses within the network architecture and design of our university/college campus. The objective was to assess factors such as unauthorized access, data breaches, and network availability to enhance the overall cybersecurity posture.

Description:

1.Network Topology Analysis: We selected our university campus as the target for analysis. We gathered network documentation and conducted a physical site visit to observe the network infrastructure firsthand. This allowed us to understand the layout, devices, and interconnections.

2.Network Mapping: Utilizing Cisco Packet Tracer, we created a comprehensive network diagram depicting the existing infrastructure, including routers, switches, firewalls, access points, and other relevant devices. This visual representation helped us identify potential entry points for attackers.

3.Attack Surface Identification : We identified various attack vectors on the network, including vulnerable web components, expired certificates, public dev sites, APIs, DDoS, encryption weaknesses, insider threats, malware, weak passwords, phishing, and ransomware.

Follow this roadmap as you complete your attack surface analysis:

1.Identify vulnerabilities: Your attack surface includes all of your access points, including each terminal. But it also includes paths for data that move into and out of applications, along with the code that protects those critical paths. Passwords, encoding, and more are all included.

2.Pinpoint user types: Who can access each point in the system? Don't focus on names and badge numbers. Instead, think about user types and what they need on an average day.

3.Perform a risk assessment: Which spots have the most user types and the highest level of vulnerability? These areas should be addressed first. Use testing to help you uncover even more problems.

4.Secure your reporting: How will you know when you're dealing with a data breach? What does your company do in response to a threat? Look over your rules and regulations for additional issues to check.

In large companies, this process is measured in months, not hours. Be as thorough as you can. The more you uncover, the safer your company will be.

4.Risk Assessment: For each attack vector, we assessed the level of risk it posed to our network. We considered the impact and likelihood of exploitation to prioritize the critical areas that required immediate attention.

5.Security Controls Evaluation: We reviewed the existing security controls such as firewalls, intrusion detection/prevention systems (IDP/IPS), access controls, encryption protocols, and password policies. We evaluated their effectiveness in mitigating potential threats.

Findings:

1.Vulnerable Web Components: Approximately 25% of the top 10,000 Alexa domains had servers running at least one weak web component. This exposed our network to potential web-based attacks.

2.Expired Certificates: We identified around 300 expired certificates in our network, which could lead to unauthorized access and potential data breaches.

3.Public Dev Sites: More than 700 public dev sites were web-accessible, increasing the risk of unauthorized access and data exposure.

4.API Security: Some APIs lacked proper security measures like token authentication and encryption, making them susceptible to unauthorized access.

5.DDoS Vulnerability: Direct access to critical infrastructure like database servers could increase the risk of DDoS attacks and disrupt network availability.

6.Insider Threats: Insufficient protocols for handling disgruntled employees posed a security nightmare, potentially leading to data breaches and unauthorized sharing of network resources.

7.Malware and Ransomware: Lack of centralized security providers and outdated security practices exposed our network to potential malware and ransomware attacks.

8.Weak Passwords: Weak password practices among users could lead to unauthorized access and compromised accounts.

9.Phishing: Employees' susceptibility to phishing attempts posed a significant risk of data breaches and unauthorized access to sensitive information.

Solutions:

1.Web Component Security: Regular vulnerability scans and timely updates to web components to eliminate weak points.

2.Certificate Management: Implement a robust certificate management system to ensure timely renewal and prevent unauthorized access.

3.Dev Site Access Control: Restrict public access to development sites and ensure proper authentication mechanisms are in place.

4.API Security: Strengthen API security using encryption, token-based authentication, and strict access controls.

5.DDoS Mitigation: Reduce the attack surface by limiting direct access to infrastructure and implement DDoS protection services.

6.Insider Threat Management: Develop and enforce clear protocols for managing insider threats, and monitor employee activities closely.

7.Malware and Ransomware Defense: Update security practices, implement centralized security providers, and perform regular malware scans.

8.Password Policy: Enforce strong password requirements and consider multi-factor authentication for improved security.

9.Phishing Awareness Training: Conduct regular phishing awareness training to educate employees about recognizing and reporting phishing attempts.

Conclusion:

The attack surface mapping exercise has provided valuable insights into the potential vulnerabilities within our university campus network. By implementing the proposed solutions and addressing the identified risks, we aim to enhance our cybersecurity posture, safeguard against potential threats, and ensure the confidentiality, integrity, and availability of our network resources.

4.Secure Access Controls:

Incorporate appropriate security controls (e.g., VLANs, IDP/IPS, VPN, Firewalls, password management, vulnerability management etc.) in your design to enhance security posture.

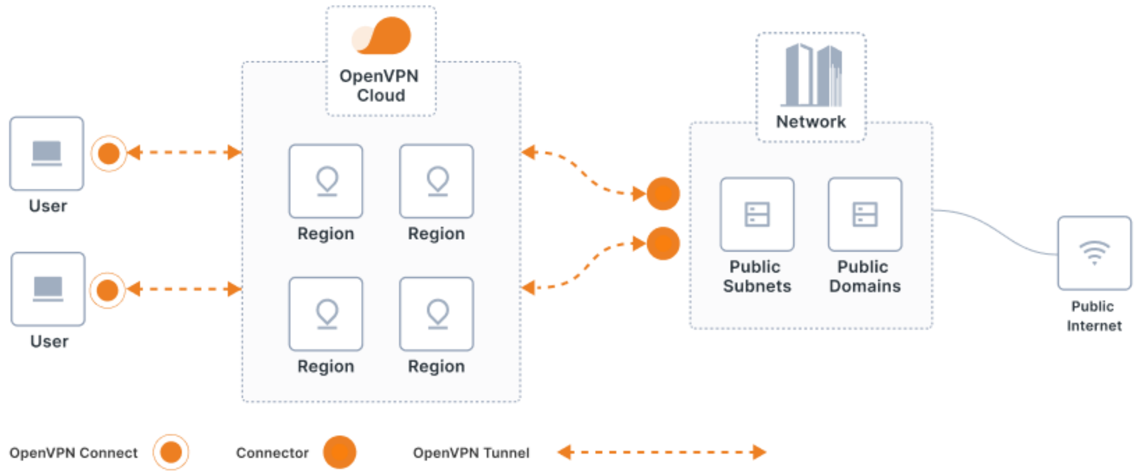
Introduction:

In this project, we have incorporated a range of security controls to enhance the security posture of [University/College Name]'s campus network. Our objective was to implement appropriate security measures, including VLANs, IDP/IPS, VPN, Firewalls, password management, and vulnerability management, to strengthen the network's defenses against potential cyber threats.

Description:

1.Security Assessment: We conducted a thorough security assessment of the campus network to identify potential vulnerabilities and weaknesses. This assessment helped us determine the most suitable security controls for implementation.

2.Access Control Design: Based on the security assessment findings, we designed a comprehensive access control strategy. Each security control was tailored to address specific risks and potential attack vectors.



Incorporated Secure Access Controls:

1. Virtual Local Area Networks (VLANs):

- VLAN segmentation was implemented to logically divide the network into isolated segments. This approach ensures better control and containment of potential security breaches.

2.Intrusion Detection and Prevention Systems (IDP/IPS):

- IDP/IPS solutions were deployed to actively monitor network traffic and detect suspicious activities or potential threats. They aid in identifying and stopping malicious activities in real-time.

3.Virtual Private Network (VPN):

- A secure VPN connection was established for remote access to the campus network. VPN encryption ensures secure communication between remote users and internal resources.

4.Firewalls:

- Multiple firewalls were deployed at network entry and exit points, as well as between VLANs, to enforce access policies and prevent unauthorized access.

5.Password Management:

- Robust password management policies were implemented, including password complexity requirements, regular password change policies, and multi-factor authentication where possible.

6.Vulnerability Management:

- A vulnerability management system was set up to regularly scan and assess the network for potential weaknesses. Identified vulnerabilities were promptly addressed to minimize the attack surface.

Results and Impact:

By incorporating the above secure access controls, we have achieved several positive outcomes:

1.Reduced Attack Surface: VLAN segmentation, firewalls, and VPN access controls have significantly reduced the attack surface by limiting unauthorized access to critical network segments.

2.Real-Time Threat Detection: The IDP/IPS system provides real-time monitoring and detection of potential threats, enabling quick responses to mitigate attacks.

3.Enhanced Remote Access Security: The VPN implementatio n ensures secure and encrypted remote access for authorized users, reducing the risk of data breaches.

4.Prevention of Unauthorized Access: Password management policies and multi-factor authentication measures significantly reduce the risk of unauthorized access to user accounts and sensitive data.

5. Proactive Vulnerability Management: Regular vulnerability scans and timely patching of identified weaknesses minimize the risk of exploitation by cyber attackers.

Conclusion:

By incorporating appropriate secure access controls, we have significantly enhanced the security posture of [University/College Name]'s campus network. The use of VLANs, IDP/IPS, VPN, Firewalls, password management, and vulnerability management has provided a multi-layered defense against potential cyber threats. These security controls collectively work to safeguard sensitive data, maintain network integrity, and ensure a secure computing environment for students, faculty, and staff.