Network model report

***Dhcp:***

To implement DHCP for the two buildings in Cisco Packet Tracer, you can follow these steps:

1. Place a DHCP server device in each building:

- Open Cisco Packet Tracer and create a new project.

- Drag and drop a "Server-PT" device from the device list onto the workspace in each building.

2. Configure the DHCP server in each building:

- Double-click on the DHCP server device in Building 1 to access its configuration.

- Click on the "Services" tab.

- Enable the DHCP service by checking the "DHCP" box.

- Configure the DHCP pool by clicking on the "Add" button.

- Specify the pool name, network, subnet mask, default gateway, and DNS server addresses for Building 1.

- Repeat the above steps for the DHCP server device in Building 2, configuring the DHCP pool with the appropriate network settings for that building.

3. Configure the DHCP relay agent on the interconnecting router:

- Place a router device in each building and connect them using an Ethernet cable.

- Double-click on the router in Building 1 to access its configuration.

- Click on the "CLI" tab.

- Configure the interface connected to the other building by entering the interface configuration mode using the "interface <interface\_id>" command.

- Enable the DHCP relay agent using the "ip helper-address <dhcp\_server\_ip\_address>" command, where <dhcp\_server\_ip\_address> is the IP address of the DHCP server in Building 2.

- Repeat the above steps for the router in Building 2, configuring the interface connected to Building 1 with the IP address of the DHCP server in Building 1.

4. Verify DHCP operation:

- Place client devices (e.g., PCs) in each building and connect them to the switches.

- Double-click on a client device in Building 1 to access its configuration.

- Ensure that the client is set to obtain its IP address automatically via DHCP.

- Repeat the above steps for a client device in Building 2.

- Power on the client devices and observe if they successfully obtain IP addresses from the respective DHCP servers.

5. Test connectivity:

- Ping between client devices in different buildings to verify that they can communicate with each other using the assigned IP addresses.

By following these steps, you can implement DHCP for the two buildings in Cisco Packet Tracer. Remember to save your project regularly to preserve your progress and test the network configuration to ensure that DHCP is functioning as expected

***Vlan:***  
To implement VLANs for the two buildings in Cisco Packet Tracer, you can follow these steps:

1. Place switches in each building:

- Open Cisco Packet Tracer and create a new project.

- Drag and drop a "2960-24TT" switch from the device list onto the workspace in each building.

2. Configure VLANs on each switch:

- Double-click on the switch in Building 1 to access its configuration.

- Click on the "CLI" tab.

- Enter the global configuration mode by typing the "enable" command, followed by the "configure terminal" command.

- Create VLANs using the "vlan <vlan\_id>" command, where <vlan\_id> is the desired VLAN ID.

- Repeat the above steps for the switch in Building 2, creating VLANs with unique VLAN IDs.

3. Assign switch ports to VLANs:

- In the switch configuration mode of Building 1, enter the interface configuration mode for each switch port using the "interface <interface\_id>" command.

- Assign the interface to a specific VLAN using the "switchport mode access" and "switchport access vlan <vlan\_id>" commands, where <vlan\_id> is the VLAN ID you want to assign to the port.

- Repeat the above steps for the switch ports in Building 2, assigning them to the appropriate VLANs.

4. Interconnect the switches between buildings:

- Connect the switches in each building using Ethernet cables.

- Drag and drop Ethernet cables from one switch in Building 1 to the corresponding switch in Building 2 to establish the interconnection.

5. Verify VLAN configuration:

- Place client devices (e.g., PCs) in each building and connect them to the switches.

- Double-click on a client device in Building 1 to access its configuration.

- Configure the network settings of the client device to match the VLAN configuration (e.g., assign an IP address within the appropriate VLAN).

- Repeat the above steps for a client device in Building 2.

- Test connectivity between client devices within the same VLAN and between different VLANs to verify that VLAN separation is working as expected.

By following these steps, you can implement VLANs for the two buildings in Cisco Packet Tracer. Remember to save your project regularly to preserve your progress and test the network configuration to ensure that VLANs are functioning as expected

***Ip phone:***  
To implement IP phones for the two buildings in Cisco Packet Tracer, you can follow these steps:

1. Place switches and IP phones in each building:

- Open Cisco Packet Tracer and create a new project.

- Drag and drop a "2960-24TT" switch from the device list onto the workspace in each building.

- Drag and drop IP phone devices (e.g., "IP Phone 7960") from the device list onto the workspace in each building.

2. Connect the IP phones to the switches:

- Connect the IP phones to the appropriate switch ports using Ethernet cables.

- Ensure that each IP phone is connected to a switch port assigned to the same VLAN as the voice VLAN.

3. Configure VLANs for voice traffic:

- Double-click on the switch in Building 1 to access its configuration.

- Click on the "CLI" tab.

- Enter the global configuration mode by typing the "enable" command, followed by the "configure terminal" command.

- Create a VLAN for voice traffic using the "vlan <vlan\_id>" command, where <vlan\_id> is the desired VLAN ID for voice traffic.

- Assign the voice VLAN to the appropriate switch ports using the "interface <interface\_id>" command, followed by the "switchport voice vlan <vlan\_id>" command.

- Repeat the above steps for the switch in Building 2, using a different VLAN ID for voice traffic.

4. Configure IP addressing for the IP phones:

- Double-click on an IP phone in Building 1 to access its configuration.

- Configure the network settings of the IP phone, including the IP address, subnet mask, default gateway, and DNS server, according to the VLAN configuration and network requirements.

- Repeat the above steps for an IP phone in Building 2.

5. Configure the IP phone system:

- Set up a VoIP server or service provider in your network, and configure it to work with the IP phones.

- Configure call routing, extensions, voicemail, and other necessary settings according to your requirements.

6. Test the IP phone functionality:

- Power on the IP phones and verify that they obtain the correct IP addresses from the DHCP server.

- Test the IP phone system by placing calls between IP phones within the same building and across buildings.

- Verify that the IP phones can access other network services and resources as required.

By following these steps, you can implement IP phones for the two buildings in Cisco Packet Tracer. Remember to save your project regularly to preserve your progress and test the network configuration to ensure that the IP phones are functioning as expected

***Cloud tv:***  
...To implement a cloud TV solution for the two buildings, you can follow these steps:

1. Set up a cloud-based media server:

- Choose a cloud service provider (e.g., Amazon Web Services, Google Cloud, Microsoft Azure) that offers media streaming capabilities.

- Sign up for an account and create a virtual machine (VM) instance or container on the cloud platform.

- Install and configure media server software on the VM or container, such as Plex, Emby, or Jellyfin.

- Upload your media content (movies, TV shows, etc.) to the cloud media server.

2. Establish network connectivity between the cloud server and the two buildings:

- In each building, place a router device (e.g., Cisco router) to connect the local network to the internet.

- Configure the routers to establish an internet connection (e.g., using dynamic or static IP addressing, NAT, and firewall rules).

- Ensure that both buildings have a reliable internet connection with sufficient bandwidth to support media streaming.

3. Set up local network infrastructure in each building:

- Place switches in each building to connect the devices.

- Connect the routers in each building to the switches.

- Connect the devices (e.g., TVs, media players, streaming devices) to the switches.

4. Configure VLANs and subnets:

- Determine the VLAN and subnet structure for each building.

- Configure VLANs on the switches, assigning appropriate ports to each VLAN.

- Configure IP addressing for each VLAN/subnet, ensuring they are unique and do not overlap.

- Ensure that the VLANs associated with the media devices have access to the VLANs used by the cloud server.

5. Enable multicast and IGMP snooping:

- Enable multicast routing on the routers in each building.

- Enable IGMP snooping on the switches to optimize multicast traffic delivery.

6. Configure media playback devices:

- Connect the TVs or media players in each building to the appropriate VLAN ports on the switches.

- Configure the network settings on the devices, ensuring they are assigned IP addresses within the correct VLAN/subnet.

7. Configure the media streaming clients:

- Install media streaming client applications on the TVs or media players (e.g., Plex client, Emby client).

- Configure the client applications to connect to the cloud media server using the appropriate credentials or server address.

8. Test and verify:

- Power on the TVs or media players and launch the media streaming client applications.

- Verify that the devices can connect to the cloud media server and access the media content.

- Test media playback on the TVs or media players to ensure smooth streaming and quality playback.

By following these steps, you can implement a cloud TV solution for the two buildings, allowing access to media content from a central cloud media server. Remember to ensure proper network configuration, VLAN setup, and connectivity between the buildings and the cloud server to ensure optimal performance and streaming experience.

***ftp service:***

To implement an FTP (File Transfer Protocol) service for the two buildings, you can follow these steps:

1. Set up an FTP server:

- Choose an FTP server software to use, such as FileZilla Server, vsftpd, or ProFTPD.

- Install the FTP server software on a dedicated server or a computer that will act as the FTP server.

- Configure the FTP server software with the desired settings, such as security options, user authentication, and access permissions.

- Create user accounts on the FTP server for individuals who will access the FTP service.

2. Establish network connectivity between the two buildings:

- Place routers in each building to connect the local networks to each other and to the internet.

- Configure the routers to establish an internet connection and enable interconnectivity between the buildings.

- Ensure that both buildings have a reliable internet connection with sufficient bandwidth.

3. Set up local network infrastructure in each building:

- Place switches in each building to connect the devices.

- Connect the routers in each building to the switches.

- Connect the devices (e.g., computers, servers) to the switches.

4. Configure VLANs and subnets:

- Determine the VLAN and subnet structure for each building.

- Configure VLANs on the switches, assigning appropriate ports to each VLAN.

- Configure IP addressing for each VLAN/subnet, ensuring they are unique and do not overlap.

- Ensure that the VLANs associated with the FTP server and client devices have appropriate access to each other.

5. Configure port forwarding on the router:

- Set up port forwarding on the router in the building where the FTP server is located.

- Forward incoming FTP traffic (port 21) from the router's external IP address to the internal IP address of the FTP server.

6. Configure FTP clients in both buildings:

- Install FTP client software on the computers in each building (e.g., FileZilla, WinSCP).

- Configure the FTP client software with the necessary connection settings, including the FTP server's IP address, port number (typically 21), and credentials (username and password).

7. Test and verify:

- Start the FTP server and ensure it is running without any errors.

- Connect to the FTP server from the FTP clients in both buildings using the configured connection settings.

- Test file transfers (uploading and downloading files) between the FTP server and clients to verify connectivity and functionality.

- Verify the access permissions and security settings to ensure that users can only access the appropriate files and directories on the FTP server.

By following these steps, you can implement an FTP service for the two buildings, allowing users in both buildings to transfer files to and from the central FTP server. Remember to ensure proper network configuration, VLAN setup, and access controls to maintain security and control over the FTP service.

***Wire less access point:***

To implement wireless access points (APs) for the two buildings, you can follow these steps:

1. Determine the wireless network requirements:

- Identify the coverage area and capacity requirements for each building.

- Determine the frequency band (2.4 GHz, 5 GHz, or both) and wireless standards (e.g., 802.11n, 802.11ac) that will meet the desired performance and compatibility needs.

2. Select wireless access points:

- Choose wireless APs that meet the identified requirements and are capable of providing the desired coverage and capacity.

- Consider factors such as range, number of antennas, supported wireless standards, management features, and security capabilities.

- Ensure that the APs support the same wireless standards and offer seamless roaming between APs for uninterrupted connectivity.

3. Place wireless access points:

- Determine the optimal locations for placing the APs in each building to achieve the desired coverage.

- Consider factors such as building layout, obstacles (walls, furniture), and interference sources (microwaves, other wireless devices).

- Aim for AP placement that minimizes signal interference and maximizes coverage throughout each building.

4. Establish network connectivity:

- Place routers in each building to connect the local networks to the internet.

- Connect the routers to the switches in each building.

- Ensure that both buildings have a reliable internet connection with sufficient bandwidth.

5. Set up local network infrastructure in each building:

- Place switches in each building to connect the devices.

- Connect the APs to the switches using Ethernet cables.

- Connect the devices (e.g., computers, printers, servers) to the switches.

6. Configure wireless access points:

- Access the management interface of each AP using a web browser or dedicated management software.

- Configure the wireless network settings, including SSID (network name), security settings (WPA2, encryption), and wireless channel.

- Set the same SSID and security settings on all APs to create a seamless wireless network across both buildings.

- Configure power levels and channel assignments to minimize interference between APs.

7. Test and verify:

- Power on the APs and ensure they are connected to the network.

- Use wireless devices (laptops, smartphones) to connect to the wireless network in each building.

- Verify connectivity, signal strength, and data transfer rates by performing tests in various areas of each building.

- Test roaming between APs to ensure seamless handoff when moving between coverage areas.

8. Optimize and fine-tune:

- Monitor the wireless network performance and make adjustments as needed.

- Adjust AP locations, power levels, and channels to optimize coverage and minimize interference.

- Regularly update AP firmware to ensure the latest features, security patches, and performance improvements.

By following these steps, you can implement wireless access points for the two buildings, providing wireless connectivity throughout the premises. Remember to consider the specific requirements of each building, such as coverage area, capacity, and interference sources, to ensure optimal wireless network performance.

***Network analysis:***

To perform a network analysis of the entire network model, including the cloud TV, FTP service, and wireless access points for the two buildings, you can consider the following aspects:

1. Bandwidth Analysis:

- Determine the bandwidth requirements for each service, such as the cloud TV streaming, FTP file transfers, and wireless network traffic.

- Assess the available internet bandwidth and ensure it is sufficient to support the expected network usage.

- Monitor network traffic using network monitoring tools to identify any bottlenecks or congestion points.

2. Network Latency:

- Measure the network latency, which is the time it takes for data packets to travel between devices.

- Analyze the latency impact on services such as cloud TV streaming and FTP transfers, ensuring that the network latency is within acceptable limits.

- Optimize network routing and minimize latency by using efficient network protocols and ensuring network devices are properly configured.

3. Security Analysis:

- Evaluate the security measures implemented in the network model.

- Assess the encryption protocols used for the cloud TV streaming and FTP transfers to ensure data confidentiality.

- Verify the access controls and authentication mechanisms in place for the FTP service to prevent unauthorized access.

- Conduct vulnerability assessments and penetration testing to identify and address any potential security vulnerabilities.

4. Scalability:

- Assess the network's scalability to accommodate future growth and increased network usage.

- Consider factors such as the number of users, devices, and data volume that the network can handle.

- Ensure that the network infrastructure, including switches, routers, and access points, can support the expected scalability requirements.

5. Redundancy and High Availability:

- Evaluate the network's resilience and availability.

- Implement redundant network devices, such as routers and switches, to minimize single points of failure.

- Configure failover mechanisms and redundant connections to ensure uninterrupted network connectivity.

- Establish backup and disaster recovery strategies for critical network components and data.

6. Quality of Service (QoS):

- Analyze the network's QoS capabilities to prioritize and optimize network traffic.

- Prioritize real-time applications like cloud TV streaming to ensure a smooth and uninterrupted viewing experience.

- Set QoS policies to allocate sufficient bandwidth for FTP transfers and other network traffic to prevent congestion.

7. Monitoring and Management:

- Implement network monitoring and management tools to monitor the network's performance and troubleshoot issues.

- Set up network monitoring alerts and notifications to promptly identify and address network problems.

- Regularly review network logs and performance metrics to identify areas of improvement and optimize network performance.

By conducting a comprehensive network analysis, you can identify potential issues, optimize performance, and ensure the network model is robust, secure, and capable of meeting the desired requirements for all services, including cloud TV, FTP, and wireless access points.

***Security analysis:***

To perform a security analysis of the whole network model, including the cloud TV, FTP service, and wireless access points for the two buildings, you can consider the following security aspects:

1. Network Perimeter Security:

- Implement a firewall at the network perimeter to control incoming and outgoing traffic.

- Configure the firewall to allow only necessary ports and protocols for the different services (e.g., HTTP/HTTPS for cloud TV, FTP ports for FTP service).

- Regularly update the firewall's firmware and security rules to protect against emerging threats.

2. Access Control:

- Implement strong access control measures for all network devices, including routers, switches, and wireless access points.

- Use unique and strong passwords for device logins and enforce regular password changes.

- Disable unnecessary services and interfaces to reduce the attack surface.

3. Encryption and Secure Protocols:

- Ensure that all sensitive data transmitted over the network is encrypted using secure protocols.

- Use HTTPS for cloud TV streaming to encrypt the data in transit.

- Enable secure FTP protocols such as FTPS (FTP over SSL/TLS) or SFTP (SSH File Transfer Protocol) to protect FTP file transfers.

4. User Authentication and Authorization:

- Implement robust user authentication mechanisms for accessing the FTP service and network devices.

- Enforce strong password policies and consider implementing multi-factor authentication for enhanced security.

- Assign appropriate user roles and permissions to limit access to sensitive resources.

5. Intrusion Detection and Prevention:

- Deploy intrusion detection and prevention systems (IDPS) to monitor network traffic and detect suspicious activities.

- Configure the IDPS to generate alerts or block malicious traffic based on predefined rules.

- Regularly update the IDPS signatures and rules to detect and prevent the latest threats.

6. Network Segmentation:

- Segment the network into different security zones to isolate sensitive systems and data from the rest of the network.

- Use VLANs (Virtual Local Area Networks) to separate traffic and implement access control between different network segments.

- Implement proper firewall rules and access policies to control communication between network segments.

7. Regular Patching and Updates:

- Regularly update and patch all network devices, including routers, switches, APs, and servers, to address known vulnerabilities.

- Enable automatic updates whenever possible to ensure timely application of security patches.

- Keep firmware and software versions up to date to benefit from the latest security features and improvements.

8. Employee Awareness and Training:

- Conduct security awareness training for employees to educate them about best practices, such as avoiding phishing emails, using strong passwords, and reporting suspicious activities.

- Promote a security-conscious culture and encourage employees to follow security policies and procedures.

9. Monitoring and Logging:

- Implement network monitoring and logging solutions to track and analyze network activities.

- Monitor network logs regularly for signs of suspicious behavior or security incidents.

- Implement centralized log management to streamline log analysis and correlation.

10. Incident Response and Disaster Recovery:

- Develop an incident response plan to address security incidents promptly and effectively.

- Establish a backup and disaster recovery strategy to ensure data integrity and availability in case of a security breach or system failure.

- Regularly test and update the incident response and disaster recovery plans.

By conducting a thorough security analysis and implementing appropriate security measures, you can enhance the overall security posture of the network model, protecting sensitive data, preventing unauthorized access, and mitigating potential security risks.

***Budget analysis:***

To perform a budget analysis of the whole network model, including the cloud TV, FTP service, and wireless access points for the two buildings, you need to consider various cost factors. Here are some elements to include in your budget analysis:

1. Hardware Costs:

- Calculate the cost of network infrastructure components such as routers, switches, and wireless access points.

- Consider the number of devices required for both buildings and the desired specifications and features.

- Research the market for competitive prices and choose reliable vendors.

2. Software Costs:

- Determine the cost of any required network management software, firewall software, or monitoring tools.

- Consider license fees, subscription costs, or one-time purchase costs for the software solutions you need.

3. Cloud TV Service Costs:

- If you're using a cloud TV streaming service, consider the subscription fees or licensing costs associated with the service.

- Research different cloud TV providers and compare their pricing plans to find the most suitable and cost-effective option.

4. FTP Service Costs:

- Assess the cost of implementing and maintaining the FTP service.

- Consider any software licenses, server hardware, or storage costs associated with the FTP service.

5. Internet Service Provider (ISP) Costs:

- Determine the cost of the internet connection required to support the network model.

- Consider the monthly or annual fees charged by the ISP for the desired bandwidth and service level agreement (SLA).

6. Maintenance and Support Costs:

- Account for ongoing maintenance and support costs for network devices, including firmware updates, bug fixes, and troubleshooting.

- Consider any service contracts, warranties, or support agreements with vendors or third-party providers.

7. Security Costs:

- Include the cost of implementing security measures such as firewalls, intrusion detection systems, and antivirus software.

- Consider any subscription fees for security services or ongoing security assessments.

8. Training and Documentation Costs:

- Allocate a budget for training employees on network management, security best practices, and troubleshooting procedures.

- Consider the cost of creating or purchasing documentation and user manuals for the network model.

9. Scalability and Future Expansion Costs:

- Anticipate future growth and consider the cost implications of scaling the network model.

- Account for potential hardware and software upgrades, additional network devices, and increased bandwidth requirements.

10. Miscellaneous Costs:

- Consider any additional costs that may arise, such as cabling, installation, or professional services for network setup and configuration.

It's important to note that the budget analysis will vary depending on the scale and complexity of the network model and the specific requirements of the buildings and services involved. Conduct thorough research, gather quotes from vendors, and create a detailed budget plan to accurately estimate the costs associated with implementing and maintaining the network model.