ASSIGNMENT 6

Q1- Identify the scenario using Cisco Packet Tracer for Network Configuration. Make a survey of active and passive nodes, and the component's participation in the communication. Write Configuration code.

We have to in this , simulate a basic client server model. Here. the PC's connect to router by a switch, and the server provides network services.

- Configure a LAN with a router , switch , many PC'S and server
- Assign static IP to the server and dynamic IP to client devices.
- Now client server communication needs to be enabled.
- Now analysis of packet flow,including capturing must be done. This shall be done using simulation mode.

Now, a survey of active and passive nodes must be done

- Active Nodes are those devices that process and transmit network traffic.
- Router - this will connect different networks and this will forward data packets.
- Switch - Connects multiple devices in the same network and it forwards frames.
- PC1 , PC2 are the clients. The request network services.
- Server - web and dhcp server- this will provide ip addressing and it hosts a website.

Passive nodes are devices that do not generate traffic. They do, facilitate transmission.
Ethernet cables- they connect the devices for communication.
Patch panels- they organize and manage the cables.

- PC's request an IP from the dhcp server - > the server will assign an IP dynamically
- Pc's send dns requests to resolve domain names- > the dns servers resolves then to ip addresses.
- PCs send http requests to access a webpage- the web server processes and responds.
- Router forwards packets between different subnets.
- Switch does the work of facilitating data transfer within the lan.

Configuration code

```
enable
configure terminal
```

```
hostname R1

! Configure Router Interfaces
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 no shutdown
exit

interface FastEthernet0/1
 ip address 192.168.2.1 255.255.255.0
 no shutdown
exit

! Configure DHCP on Router
ip dhcp excluded-address 192.168.1.1 192.168.1.10
ip dhcp pool CLIENTS
 network 192.168.1.0 255.255.255.0
 default-router 192.168.1.1
 dns-server 8.8.8.8
exit

end
write memory
```

This is the configuration of switch

```
enable
configure terminal
hostname S1

! Configure VLAN if needed
vlan 10
 name Client_Network
exit

! Assign ports to VLAN
interface FastEthernet0/1
 switchport mode access
 switchport access vlan 10
exit

interface FastEthernet0/2
 switchport mode access
 switchport access vlan 10
exit
```

end
write memory

After this you will need to test the network connectivity.
All of these steps ensure that

- Clients dynamically get IP addresses from the server
- The switch does enable communication within the network so the term intra
- Clients will be able to access the web server.

Q2 - Prepare a Scenarios with Cisco Packet Tracer and showcase the nodes are communicating with each other.

So we have to set up a basic network communication

- **Devices Used:** 2 PCS 1 switch 1 router and some cables which will be important.
- **Steps of setup:**

  First we connect both PCs to switch using the straight cables

  Then we connect the switch to the router using cable

  We need to assign IP addresses for both PC. We do that in the same subnet

  Now, configure the default gateway on both PCs

  Use the ping command so that communication that happens between the PCS shall be tested.

  OUTPUT:

  What we expect as an output here , will be that there will be successful ping replies between all the pcs. Now verify the communication using packet tracer simulation mode. So, in this network setup this confirms that the nodes are communicating successfully.

Q3-Observe the relevance of Client Server communication wrt packet transition across the networks

Client-server communication is crucial for networked applications, and packet transition plays a fundamental role in ensuring smooth data transfer between clients and servers. Here's a breakdown of its relevance:

1. Packetization of Data

When a client requests data from a server this data will be broken into packets. These packets , themselves have headers specifying things such as source , destination, addresses etc.

2. Routing Through Networks

Packets go through multiple networks like LAN WAN by the help of routers and switches.
Shortest or the best path is identified by the routing tables and IP addresses.

3. Protocols for Reliable Delivery

TCP((Transmission Control Protocol) ensures reliable packet delivery. Packet loss is also considered.
User diagram Protocol is faster but it does not guarantee delivery. This, is also useful in real life applications like video streaming
For web based client server communication , HTTP will be used.

4. Packet Reassembly

Packets can arrive out of order so the server or the client reorders and helps to reconstruct the data.
TCP handles this using something known as sequence numbers.

5. Error Checking & Security

- Checksums ensure integrity of packets.
- SSL for example, is a firewall. This, helps us in transmitting packets in a safe and secure way.

6. Network Congestion & Optimization

- Load balancers distribute packets to multiple servers.
- There are content delivery networks which optimize packet delivery for speed.

Conclusion :

Packet transition is very very crucial in client server communication. It is important to understand its flow , this in turn, helps in performance optimization and helps enhance security.

Q4- Prepare a case study on Cisco Packet Tracer with real time packet analysis.
Introduction

1. **Introduction**

Cisco packet tracer is a powerful too developed by Cisco Systems. This will help users in creating, configuring and troubleshooting virtual networks. This also helps provide real time analysis of packets.

2. Background

Network professionals and students face challenges on how do these data packets travel via these networks. Cisco packet tracer provides a great platform which is not only visual but also interactive. It helps in simulating real world network behaviour.

Networking professionals and students often face challenges in understanding how data packets travel through a network. Cisco Packet Tracer provides a visual and interactive platform for learning network protocols, simulating real-world network behavior, and analyzing packet flow between devices.

4. Methodology

To demonstrate analysis of packets in real time we shall create a network topology which is simple having
Two PCs a switch , a router and a packet sniffer tool.

Step 1: Network Configuration

- Assign IP addresses to both PCs
- Router configuration must be done so that communication is enabled
- Connect the devices using suitable cables like ethernet for lan and serial for wan.

Step 2: Enabling Packet Sniffing

- Add packet sniffer tool in the network topology
- Sniffer configuration must be done so that traffic between both PCS is captured

Step 3: Sending Data and Capturing Packets

- Use the first pc to ping the second one to generate network traffic.
- Observe how these packets move in real mode
- Now examine headers, protocols used and error messages.

5. Findings and Analysis

- The ICMP request and reply packets were captured, showing source and destination of the IP addresses.
- The arp request and reply packets did indeed show how MAC addresses were resolved which happened before communication
- A TCP session was established successfully between devices
- By inducing network congestion TCP retransmissions were observed and delays were also observed.

6. Applications

- **Network Troubleshooting**: this will help in solving the issues of connectivity and will also help identify the devices not configured properly..
- **Security Monitoring**: This detects unauthorized or malicious network activity by analysing packets that were captured.
- **Protocol Analysis**: This plays an important role in understanding how TCP/IP stack is implemented and how these networking protocols are implemented.

7. Conclusion

Real-time packet analysis in Cisco Packet Tracer is a very important tool for understanding network behavior, troubleshooting issues, and helping to enhance and improve security. By capturing and analyzing packets, the users will gain a thorough understanding of how data is transmitted. This skill, indeed is important for networking professionals.

CN assignment 6 part 4.pdf

Vishwakarma Group of Institutions

Document Details

Submission ID
trn:oid:::3618:84147436

Submission Date
Mar 2, 2025, 10:50 PM GMT+5:30

Download Date
Mar 2, 2025, 10:52 PM GMT+5:30

File Name
CN assignment 6 part 4.pdf

File Size
133.2 KB

6 Pages

1,285 Words

6,929 Characters

7% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Filtered from the Report

- Bibliography
- Quoted Text
- Cited Text
- Small Matches (less than 9 words)
- Abstract
- Methods and Materials

Match Groups

3 Not Cited or Quoted 7%
Matches with neither in-text citation nor quotation marks

0 Missing Quotations 0%
Matches that are still very similar to source material

0 Missing Citation 0%
Matches that have quotation marks, but no in-text citation

0 Cited and Quoted 0%
Matches with in-text citation present, but no quotation marks

Top Sources

7% Internet sources
6% Publications
0% Submitted works (Student Papers)

Integrity Flags

0 Integrity Flags for Review

No suspicious text manipulations found.

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.

Match Groups

- **3** Not Cited or Quoted 7%
  Matches with neither in-text citation nor quotation marks
- **0** Missing Quotations 0%
  Matches that are still very similar to source material
- **0** Missing Citation 0%
  Matches that have quotation marks, but no in-text citation
- **0** Cited and Quoted 0%
  Matches with in-text citation present, but no quotation marks

Top Sources

7% Internet sources
6% Publications
0% Submitted works (Student Papers)

Top Sources

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1 Internet
www.foxnetwork.ru **3%**

2 Internet
xushi.co.uk **2%**

3 Internet
cisconetworkadvanced.blogspot.com **2%**

ASSIGNMENT 6

Q1- Identify the scenario using Cisco Packet Tracer for Network Configuration. Make a survey of active and passive nodes, and the component's participation in the communication. Write Configuration code.

We have to in this , simulate a basic client server model. Here. the PC's connect to router by a switch, and the server provides network services.

- Configure a LAN with a router , switch , many PC'S and server
- Assign static IP to the server and dynamic IP to client devices.
- Now client server communication needs to be enabled.
- Now analysis of packet flow,including capturing must be done. This shall be done using simulation mode.

Now, a survey of active and passive nodes must be done

- Active Nodes are those devices that process and transmit network traffic.
- Router - this will connect different networks and this will forward data packets.
- Switch - Connects multiple devices in the same network and it forwards frames.
- PC1 , PC2 are the clients. The request network services.
- Server - web and dhcp server- this will provide ip addressing and it hosts a website.

Passive nodes are devices that do not generate traffic. They do, facilitate transmission.
Ethernet cables- they connect the devices for communication.
Patch panels- they organize and manage the cables.

- PC's request an IP from the dhcp server - > the server will assign an IP dynamically
- Pc's send dns requests to resolve domain names- > the dns servers resolves then to ip addresses.
- PCs send http requests to access a webpage- the web server processes and responds.
- Router forwards packets between different subnets.
- Switch does the work of facilitating data transfer within the lan.

Configuration code

enable
configure terminal

```
hostname R1

! Configure Router Interfaces
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 no shutdown
exit

interface FastEthernet0/1
 ip address 192.168.2.1 255.255.255.0
 no shutdown
exit

! Configure DHCP on Router
ip dhcp excluded-address 192.168.1.1 192.168.1.10
ip dhcp pool CLIENTS
 network 192.168.1.0 255.255.255.0
 default-router 192.168.1.1
 dns-server 8.8.8.8
exit

end
write memory

This is the configuration of switch
enable
configure terminal
hostname S1

! Configure VLAN if needed
vlan 10
 name Client_Network
exit

! Assign ports to VLAN
interface FastEthernet0/1
 switchport mode access
 switchport access vlan 10
exit

interface FastEthernet0/2
 switchport mode access
 switchport access vlan 10
exit
```

end
write memory

After this you will need to test the network connectivity.
All of these steps ensure that

- Clients dynamically get IP addresses from the server
- The switch does enable communication within the network so the term intra
- Clients will be able to access the web server.

Q2 - Prepare a Scenarios with Cisco Packet Tracer and showcase the nodes are communicating with each other.

So we have to set up a basic network communication

- **Devices Used:** 2 PCS 1 switch 1 router and some cables which will be important.
- **Steps of setup:**

  First we connect both PCs to switch using the straight cables

  Then we connect the switch to the router using cable

  We need to assign IP addresses for both PC. We do that in the same subnet

  Now, configure the default gateway on both PCs

  Use the ping command so that communication that happens between the PCS shall be tested.

  OUTPUT:

  What we expect as an output here , will be that there will be successful ping replies between all the pcs. Now verify the communication using packet tracer simulation mode. So, in this network setup this confirms that the nodes are communicating successfully.

Q3-Observe the relevance of Client Server communication wrt packet transition across the networks

Client-server communication is crucial for networked applications, and packet transition plays a fundamental role in ensuring smooth data transfer between clients and servers. Here's a breakdown of its relevance:

1. Packetization of Data

When a client requests data from a server this data will be broken into packets. These packets , themselves have headers specifying things such as source , destination, addresses etc.

2. Routing Through Networks

Packets go through multiple networks like LAN WAN by the help of routers and switches.
Shortest or the best path is identified by the routing tables and IP addresses.

3. Protocols for Reliable Delivery

TCP((Transmission Control Protocol) ensures reliable packet delivery. Packet loss is also considered.
User diagram Protocol is faster but it does not guarantee delivery. This, is also useful in real life applications like video streaming
For web based client server communication , HTTP will be used.

4. Packet Reassembly

Packets can arrive out of order so the server or the client reorders and helps to reconstruct the data.
TCP handles this using something known as sequence numbers.

5. Error Checking & Security

- Checksums ensure integrity of packets.
- SSL for example, is a firewall. This, helps us in transmitting packets in a safe and secure way.

6. Network Congestion & Optimization

- Load balancers distribute packets to multiple servers.
- There are content delivery networks which optimize packet delivery for speed.

Conclusion :

Packet transition is very very crucial in client server communication. It is important to understand its flow , this in turn, helps in performance optimization and helps enhance security.

Q4- Prepare a case study on Cisco Packet Tracer with real time packet analysis.
Introduction

1. **Introduction**

Cisco packet tracer is a powerful too developed by Cisco Systems. This will help users in creating, configuring and troubleshooting virtual networks. This also helps provide real time analysis of packets.

2. Background

Network professionals and students face challenges on how do these data packets travel via these networks. Cisco packet tracer provides a great platform which is not only visual but also interactive. It helps in simulating real world network behaviour.

Networking professionals and students often face challenges in understanding how data packets travel through a network. Cisco Packet Tracer provides a visual and interactive platform for learning network protocols, simulating real-world network behavior, and analyzing packet flow between devices.

4. Methodology

To demonstrate analysis of packets in real time we shall create a network topology which is simple having
Two PCs a switch , a router and a packet sniffer tool.

Step 1: Network Configuration

- Assign IP addresses to both PCs
- Router configuration must be done so that communication is enabled
- Connect the devices using suitable cables like ethernet for lan and serial for wan.

Step 2: Enabling Packet Sniffing

- Add packet sniffer tool in the network topology
- Sniffer configuration must be done so that traffic between both PCS is captured

Step 3: Sending Data and Capturing Packets

- Use the first pc to ping the second one to generate network traffic.
- Observe how these packets move in real mode
- Now examine headers, protocols used and error messages.

5. Findings and Analysis

- The ICMP request and reply packets were captured, showing source and destination of the IP addresses.
- The arp request and reply packets did indeed show how MAC addresses were resolved which happened before communication
- A TCP session was established successfully between devices
- By inducing network congestion TCP retransmissions were observed and delays were also observed.

6. Applications

- **Network Troubleshooting**: this will help in solving the issues of connectivity and will also help identify the devices not configured properly..
- **Security Monitoring**: This detects unauthorized or malicious network activity by analysing packets that were captured.
- **Protocol Analysis**: This plays an important role in understanding how TCP/IP stack is implemented and how these networking protocols are implemented.

7. Conclusion

Real-time packet analysis in Cisco Packet Tracer is a very important tool for understanding network behavior, troubleshooting issues, and helping to enhance and improve security. By capturing and analyzing packets, the users will gain a thorough understanding of how data is transmitted. This skill, indeed is important for networking professionals.