Marwadi University Marwadi Chandarana Group	**Marwadi University** **Faculty of Engineering and Technology** **Department of Information and Communication Technology**	
Subject: Computer Networks (01CT0503)	**Aim:** Guided Project	
Experiment No: 14	**Date:**	**Enrolment No: 92301733041**

Project Overview:

This project simulates a secure examination network environment using Cisco Packet Tracer. The aim is to design a controlled setup where **Admin**, **Server**, and **Student** systems operate in separate VLANs to ensure security and prevent unauthorized communication.

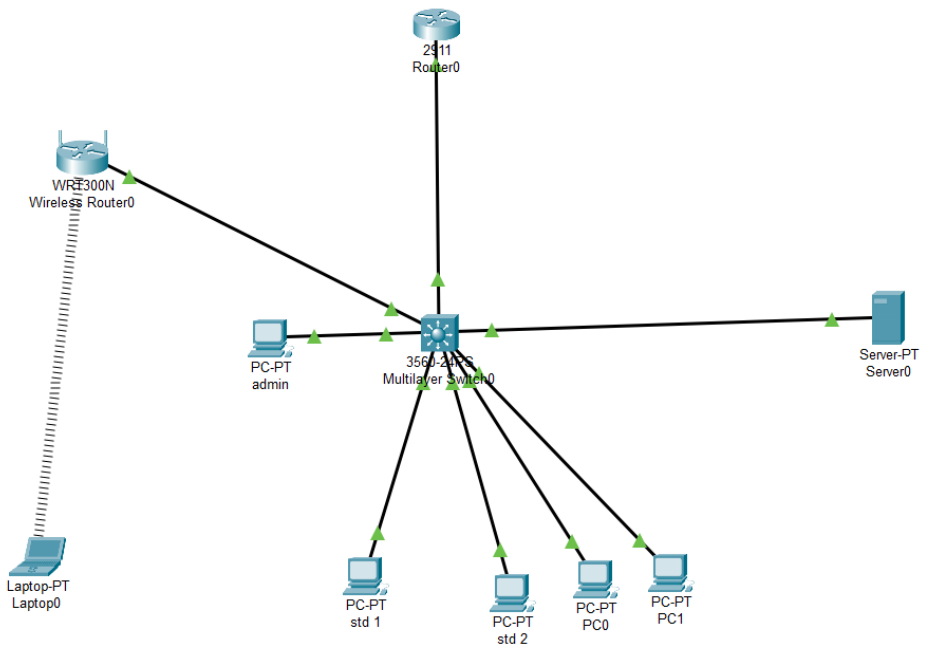
In a real-world exam environment, students must be restricted from accessing unauthorized websites or communicating with other networks. To achieve this, **VLAN segmentation**, **Router-on-Stick**, and **ACL-based filtering** are implemented.

- **Admin VLAN (10)** is used by examination staff with full access to all services.
- **Server VLAN (20)** hosts the internal Web and DNS services used during the exam.
- **Student VLAN (30)** contains student PCs and wireless users, where strict ACL rules are applied to **block AI tools, social media, and restricted websites** during examinations.

A wireless router is integrated into the Student VLAN to represent students connecting through Wi-Fi. All wired and wireless traffic is filtered using ACLs, ensuring that students can access only approved resources while Admin users retain full privileges.

This project demonstrates essential enterprise-grade networking concepts such as VLANs, trunking, inter-VLAN routing, DHCP, DNS, Web Server hosting, wireless integration, and policy enforcement. The final design closely mirrors a **real examination centre network** used in schools, colleges, and competitive exam labs.

Step 1: setup all components and assign IP add



Marwadi University Marwadi Chandarana Group	**Marwadi University** **Faculty of Engineering and Technology** **Department of Information and Communication Technology**	
Subject: Computer Networks (01CT0503)	**Aim:** Guided Project	
Experiment No: 14	**Date:**	**Enrolment No: 92301733041**

Device / VLAN	Interface / Port	IP Address	Subnet Mask	Default Gateway
Admin PC (VLAN 10)	Fa0/3	11.0.0.10	255.255.255.0	11.0.0.1
Server (VLAN 20)	Fa0/2	12.0.0.10	255.255.255.0	12.0.0.1
Student PC 1 (VLAN 30)	Fa0/4	13.0.0.10	255.255.255.0	13.0.0.1
Student PC 2 (VLAN 30)	Fa0/5	13.0.0.11	255.255.255.0	13.0.0.1
Student PC 3 (VLAN 30)	Fa0/6	13.0.0.12	255.255.255.0	13.0.0.1
Student PC 4 (Wi-Fi, VLAN 30)	Wireless LAN	DHCP (192.168.x.x → NAT)	—	13.0.0.1
Router - Admin VLAN	G0/1.10	11.0.0.1	255.255.255.0	—
Router - Server VLAN	G0/1.20	12.0.0.1	255.255.255.0	—
Router - Student VLAN	G0/1.30	13.0.0.1	255.255.255.0	—

Step 2: Config Switch-> CLI

1.Create VLAN

```
Switch>en
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)# name admin
Switch(config-vlan)#vlan 20
Switch(config-vlan)# name server
Switch(config-vlan)#vlan 30
Switch(config-vlan)# name student
Switch(config-vlan)#
```

2. Assign port to Respective VLANs

```
Switch(config)#interface fa0/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)#interface fa0/2
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 20
Switch(config-if)#interface range fa0/4 - 8
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 30
Switch(config-if-range)#exit
```

3. Configure the Trunk Port (Switch → Router Link)

```
Switch(config)#interface gi0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan 10,20,30
Switch(config-if)#
```

Marwadi University Marwadi Chandarana Group	**Marwadi University** **Faculty of Engineering and Technology** **Department of Information and Communication Technology**	
Subject: Computer Networks (01CT0503)	**Aim:** Guided Project	
Experiment No: 14	**Date:**	**Enrolment No: 92301733041**

Step 4: Configure Router-on-a-Stick (Router Subinterfaces)

1. **Line high**

```
Router(config)#interface g0/1
Router(config-if)# no ip address
Router(config-if)# no shutdown
Router(config-if)#
```

2. **Admin VLAN subinterface**

```
Router(config-if)#interface g0/1.10
Router(config-subif)# encapsulation dot1Q 10
Router(config-subif)# ip address 11.0.0.1 255.255.255.0
Router(config-subif)#
```

3. **Server VLAN subinterface:**

```
Router(config-subif)#interface g0/1.20
Router(config-subif)# encapsulation dot1Q 20
Router(config-subif)# ip address 12.0.0.1 255.255.255.0
Router(config-subif)#
```

4. **Student VLAN subinterface:**

```
Router(config-subif)#interface g0/1.30
Router(config-subif)# encapsulation dot1Q 30
Router(config-subif)# ip address 13.0.0.1 255.255.255.0
Router(config-subif)#
```

Step 6: ACL to Block Students from Accessing Restricted Websites

1. **Create ACL**

```
Router(config)#access-list 120 deny tcp 13.0.0.0 0.0.0.255 host 12.0.0.10 eq 80
Router(config)#access-list 120 deny tcp 13.0.0.0 0.0.0.255 host 12.0.0.10 eq 443
Router(config)#access-list 120 permit ip any any
```

2. **Apply ACL to Student VLAN subinterface:**

```
Router(config)#interface g0/1.30
Router(config-subif)# ip access-group 120 in
Router(config-subif)#
```

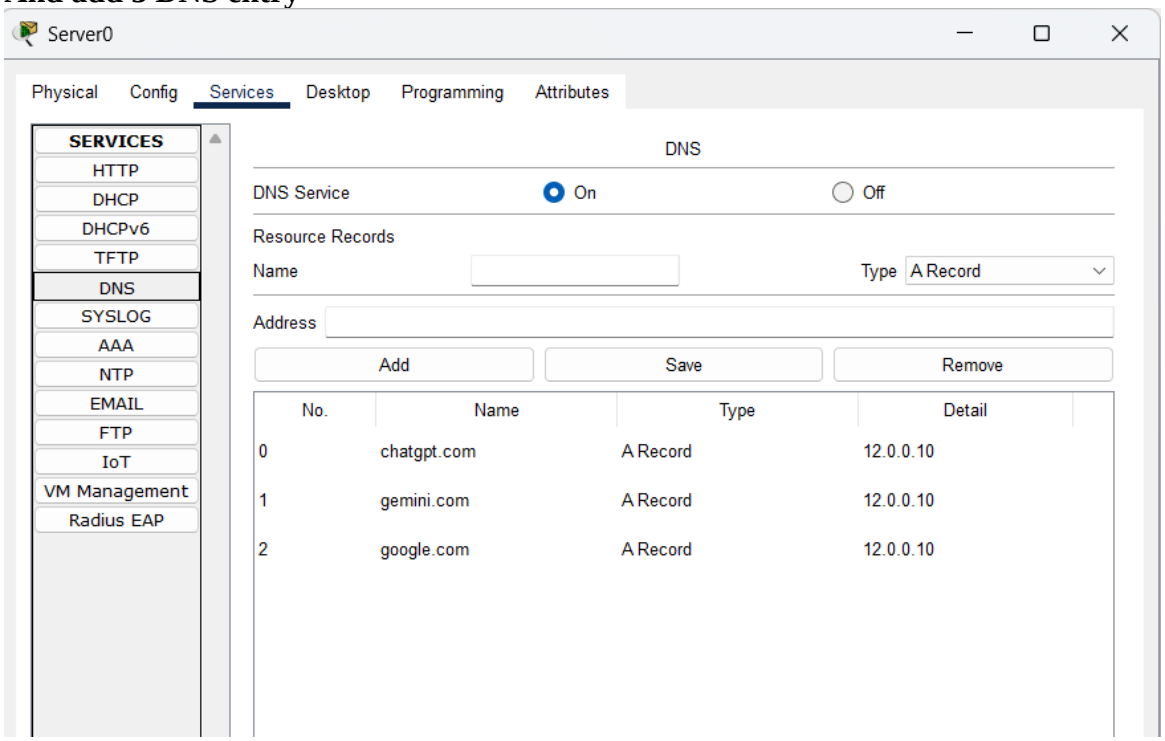
STEP 7: Verify the connectivity

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	admin	Server0	ICMP		0.000	N	5	(edit)	(delete)
	Successful	admin	std 1	ICMP		0.000	N	6	(edit)	(delete)
	Successful	std 1	Server0	ICMP		0.000	N	7	(edit)	(delete)

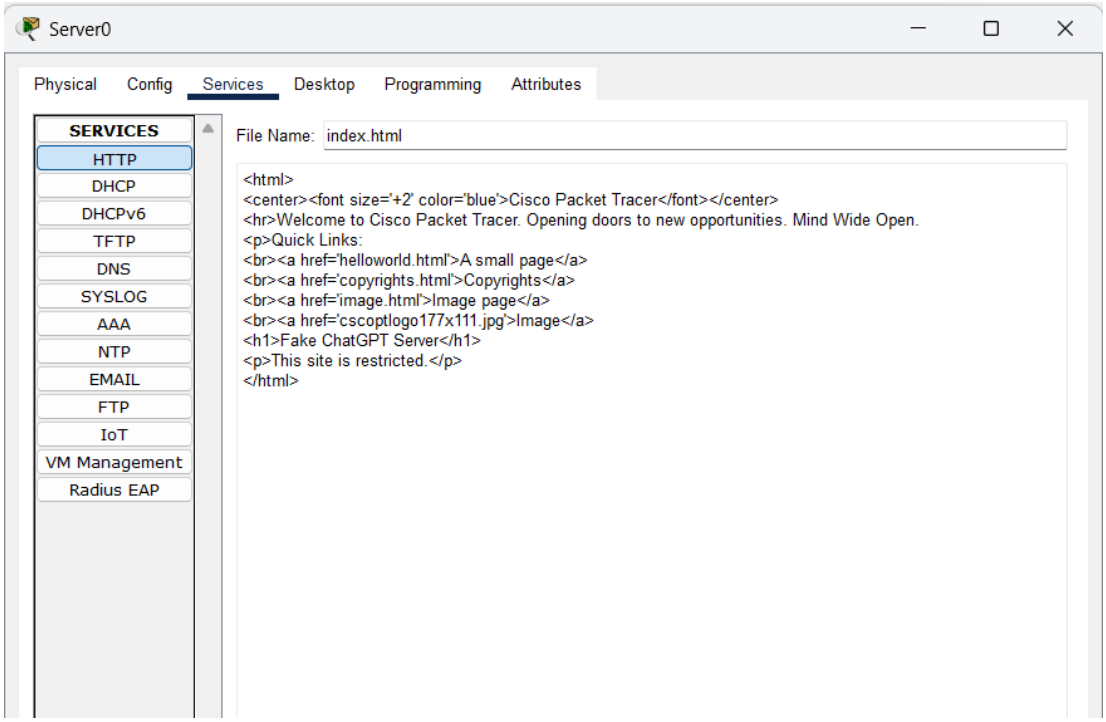
Marwadi University Marwadi Chandarana Group	**Marwadi University** **Faculty of Engineering and Technology** **Department of Information and Communication Technology**	
Subject: Computer Networks (01CT0503)	**Aim:** Guided Project	
Experiment No: 14	**Date:**	**Enrolment No: 92301733041**

Step 8: Configure DNS and Web server on server device

1. **Server->services->DNS/HTTPS mark ON**
2. **And add 3 DNS entry**



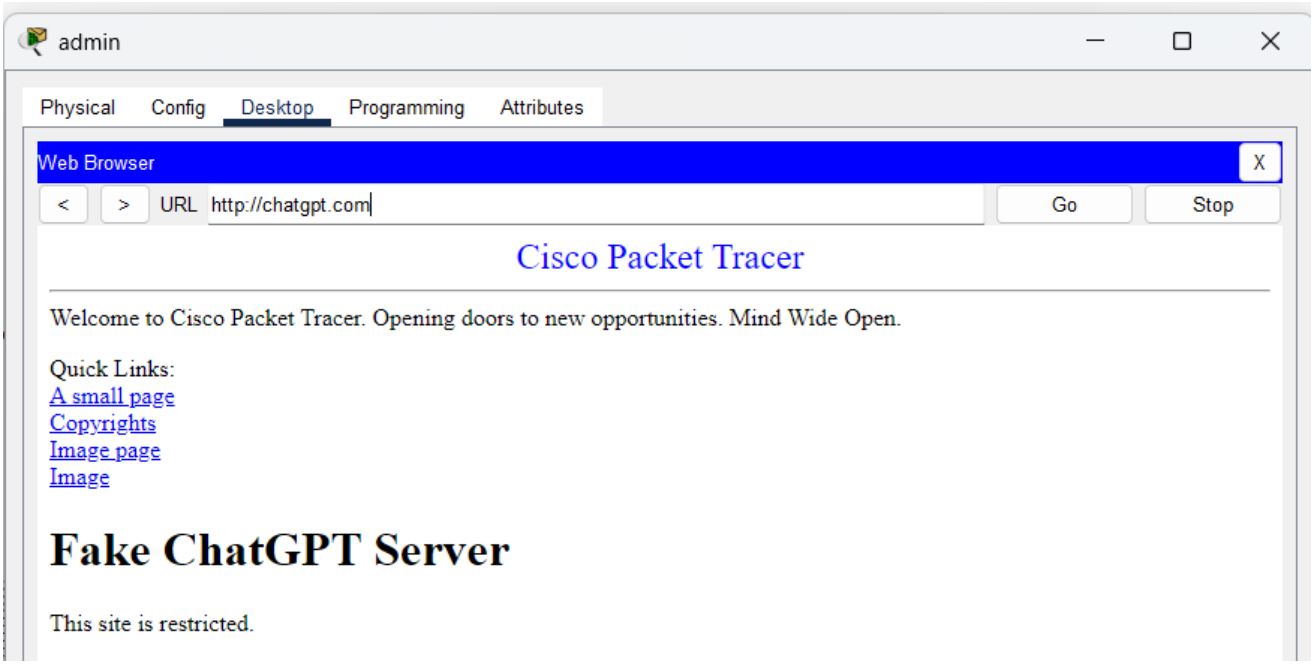
3. **Goto http->index.html->edit**
   And add some fake details and save it



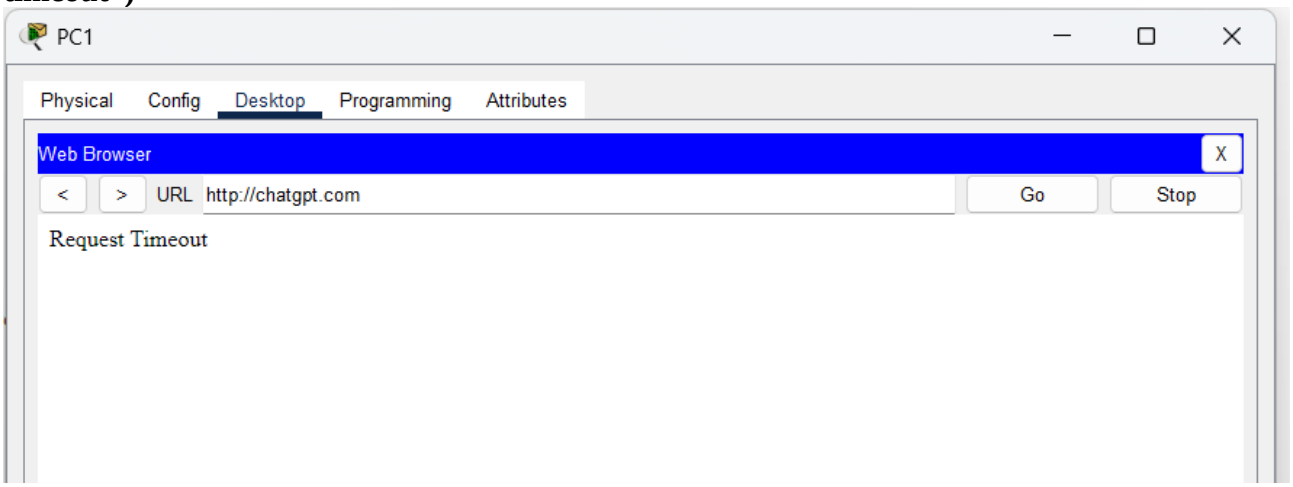
Marwadi University Marwadi Chandarana Group	**Marwadi University** **Faculty of Engineering and Technology** **Department of Information and Communication Technology**	
Subject: Computer Networks (01CT0503)	**Aim:** Guided Project	
Experiment No: 14	**Date:**	**Enrolment No: 92301733041**

Step 8: Verification

1. **Open chatgpt.com from admin pc**
   Admin pc->desktop->web browser (It should open)

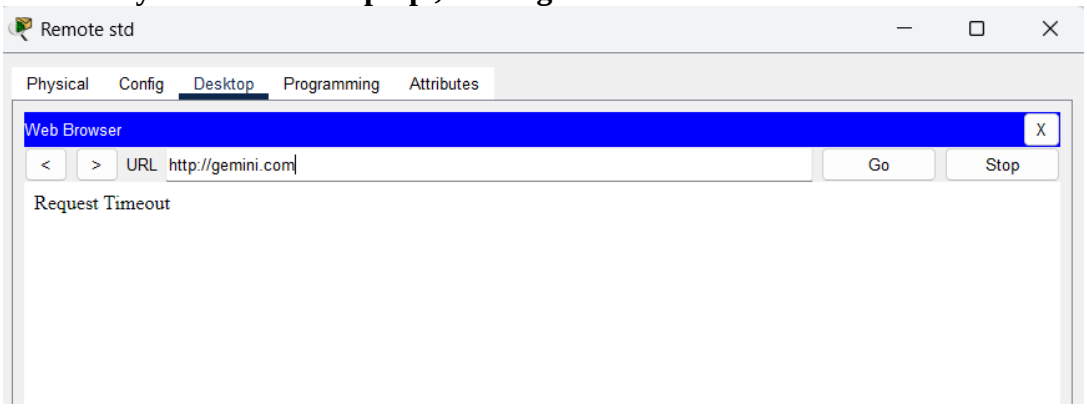


2. **Do the same from student pc (It will block an after some buffer it will show "request timeout")**



Marwadi University Marwadi Chandarana Group	**Marwadi University** **Faculty of Engineering and Technology** **Department of Information and Communication Technology**	
Subject: Computer Networks (01CT0503)	**Aim:** Guided Project	
Experiment No: 14	**Date:**	**Enrolment No: 92301733041**

3. **Also verify from remote laptop , it will give the same result**



Important terminology:

1. **VLAN (Virtual Local Area Network)**
   - Logically divides a single switch into multiple separate networks.
   - Different VLANs cannot communicate without a router.

2. **Trunk Port**
   - A switch port that carries multiple VLANs at the same time.
   - Used between Switch ↔ Router or Switch ↔ Switch links.

3. **Access Port**
   - A switch port assigned to only one VLAN.
   - Used for PCs, servers, printers, etc.

4. **Router-on-a-Stick**
   - Routing technique where one physical router interface carries multiple VLANs using subinterfaces.

5. **Subinterface**
   - A virtual interface created on a router to handle a specific VLAN.
     Example: G0/1.10 for VLAN 10.

6. **Encapsulation Dot1Q**
   - The command used to tag traffic for a specific VLAN on a router's subinterface.

7. **Default Gateway**
   - The router IP address that hosts use to reach other networks or VLANs.

8. **ACL (Access Control List)**
   - Firewall rules used to allow or block traffic based on IP, ports, or protocol.

9. HTTP / HTTPS (Port 80 / 443)

- Web traffic protocols.
- Used when blocking websites with ACL.

10. DNS (Domain Name System)

- Translates website names (e.g., chatgpt.com) into IP addresses.

11. Access Point (AP)

- Device that gives wireless connectivity.
- In this project, the AP is placed in VLAN 30 to apply the same restrictions to students.

12. Firewall Rule

- A condition inside an ACL that allows or blocks specific traffic.

Conclusion:

- Implemented a secure exam-style network using VLANs for Admin, Server, and Students.
- Router-on-Stick used to enable inter-VLAN communication while keeping traffic isolated.
- ACL firewall applied to Student VLAN to block restricted/AI websites.
- Wireless access point added so student Wi-Fi devices also follow the same security rules.
- Internal DNS + Web Server used to simulate real exam-center services.
- Overall setup demonstrates how VLANs, access points, and ACL firewalls create a safe and controlled examination network.