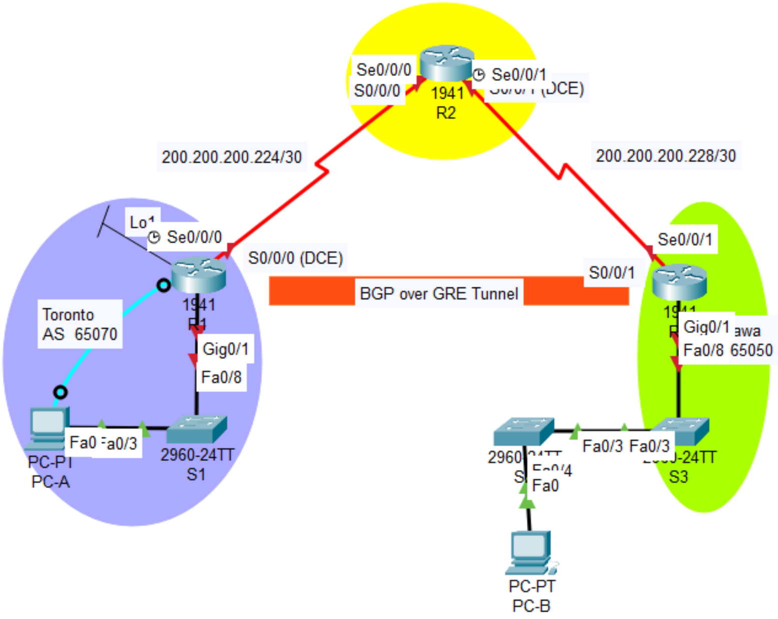
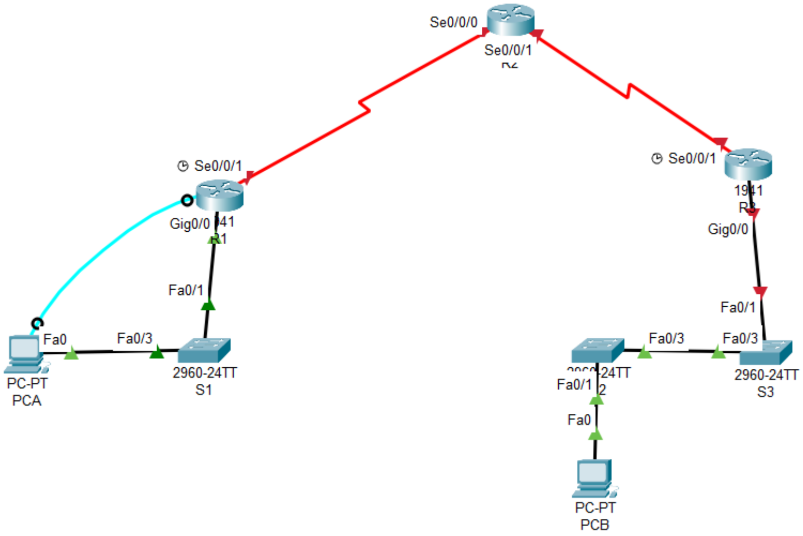
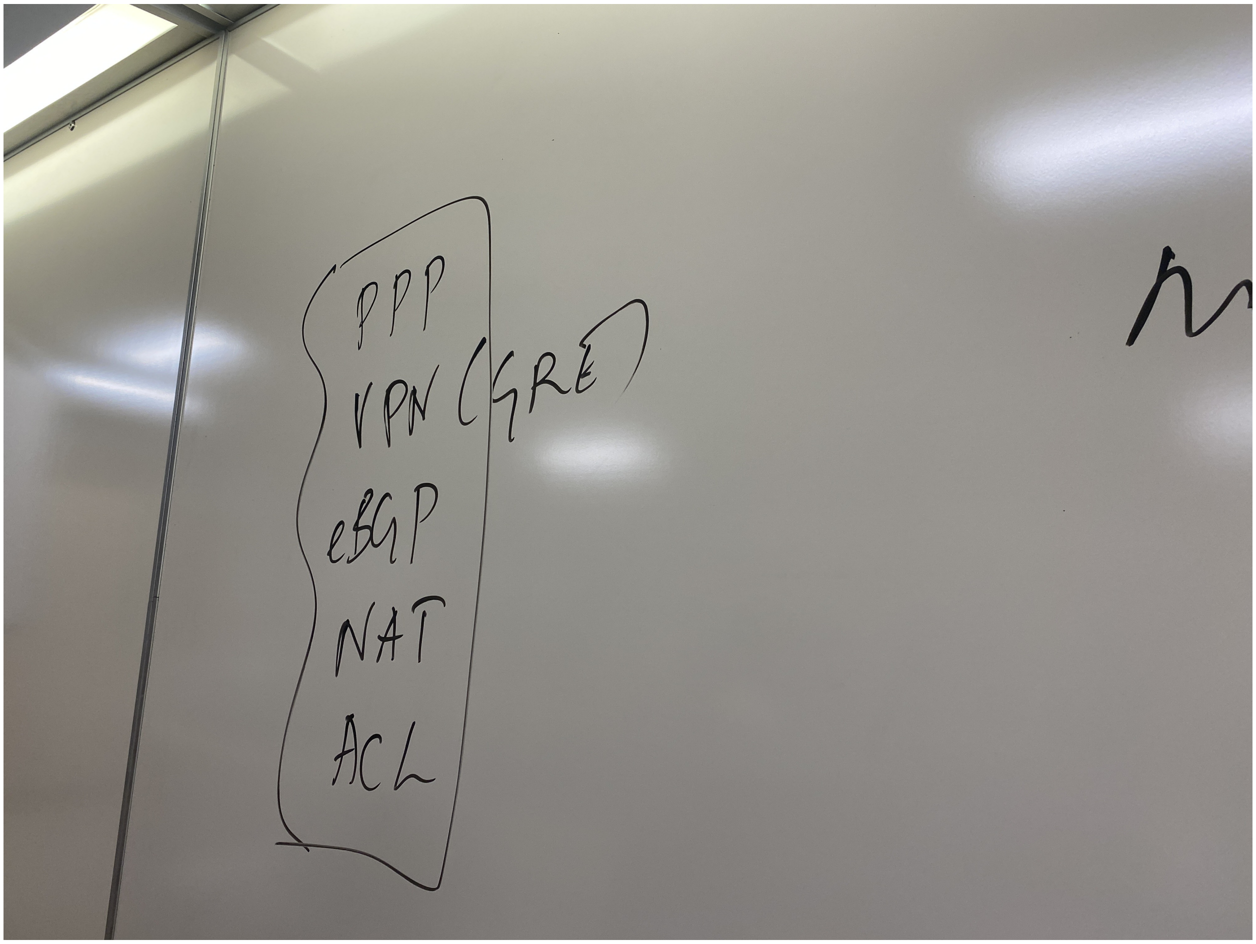
DCOM 4 final

Topology




Se0/0/0
Se0/0/1
Se0/0/1
Gig0/0
R1
Fa0/1
Fa0
Fa0/3
2960-24TT
S1
PC-PT
PCA
Se0/0/1
Gig0/0
Fa0/1
Fa0/3
Fa0/3
2960-24TT
S3
Fa0/1
Fa0
PC-PT
PCB


PPP
VPN (GRE)
eBGP
NAT
ACL

Addressing Table (Replace xxx by last two-digit of your student number)

Devices	Ports	IP Address	Subnet mask	Default Gateway
PC-A	Ethernet	100.52.1.10	255.255.255.252	10.52.1.1
R1	G0/0	100.52.10.1	255.255.255.0	
R1	S0/0/1	100.52.1.1	255.255.255.252	
R1	Lo 10	11.52.11.11	255.255.255.0	
R2	S0/0/0 (DCE)	100.52.1.2	255.255.255.252	
R2	S0/0/1	200.52.1.2	255.255.255.252	
PC-B	Ethernet	10.52.2.10	255.255.255.0	10.52.2.1
R3	S0/0/1	200.52.1.1	255.255.255.0	
R3	G0/0	200.52.2.1	255.255.255.0	

Step1: Copy and Paste the basic configurations given for all the three routers.

Step 2: Set up PPP with CHAP

For R1

S0/0/1

- PPP w/ CHAP; Link quality as 75
  - ppp authentication chap
  - exit
  - username R2_DS5352 password cisco
- Local database for CHAP – username R2 use **cisco** as password

For R2

S0/0/0 - Appropriate configuration of PPP as relates to R1's S0/0/1

S0/0/1 - Appropriate configuration of PPP as relates to R3's S0/0/0

R3

- PPP w/ CHAP; Link quality as 75
- Local database for CHAP – username R2 use **cisco** as password

Step 3: Set up NAT using ACL

Use NAT on both R1 & R3 using the following specs:

- Permit the networks to be translated on both that are attached to their G0/0 interface (use Standard ACL 10 for R1, Standard ACL 20 for R3)
- The outside interface for R1 is S0/0/1
- The outside interface for R3 is S0/0/0

- Use PAT for translation on both using only a single address – the Serial interface of the outside interface

Step 4: Set up IP Routing

- Set up OSPF single area routing on all 3 routers with an AS number of 10
- Make OSPF routing happen between all three routers and check the interconnectivity.

Step 5: Set up GRE Tunnel with BGP Toronto & Oshawa

(Replace xx and 52 by last two-digit student number)

R1 tunnel 1 & eBGP

- Set up tunnel with IPv4 address 192.168.52.1/30
- Set the host route to tunnel destination using exit interface
- For BGP, use Autonomous Systems (AS) 65210 - Configure neighbour and network

R3 tunnel 1 & eBGP

- Set up tunnel with IPv4 address 192.168.52.2/30
- Set the host route to tunnel destination using exit interface
- For BGP, use AS 65220 – Configure neighbour and network

From PC-A, should be able to ping PC-B; **From PC-B, should be able to ping PC-A**

Step 6: IP ACLs

R1 ACL specs

- Configure an IPv4 extended ACL named ACCESS so that no one can ping any device on R1 LAN
- Everything else is allowed
- Test by pinging from PC-B to PC-A (should NOT work); PC-B to Lo10 (Should work)
- Ping PC-A to PC-B (**should** work)

Create a folder on the desktop called **yourfirstnamefinal** and copy the necessary files mentioned below as per instruction, zip it and submit via DC Connect (**FinalLabExam** assignment folder)

- Save final configurations as individual text or document for each router. (3 doc or txt or pdf)
- Save a document as **verification.doc**(pdf),
- Attach routing information for each router that shows all eBGP learned routes plus static route where applicable. (3 screenshots)
- Attach NAT translations in the routers configured. (2 screenshots)
- Attach access list information to prove your configurations (1 screenshots)
- Attach successful ping from PC-A to PC-B and unsuccessful ping from PC-B to PC-A (2 screenshots)

Wish you all the best

Here's a detailed script for configuring the routers (R1, R2, and R3) according to your requirements. This script includes setting up PPP with CHAP, NAT using ACLs, OSPF routing, GRE Tunnel with BGP, and IP ACLs.

Verification and Documentation

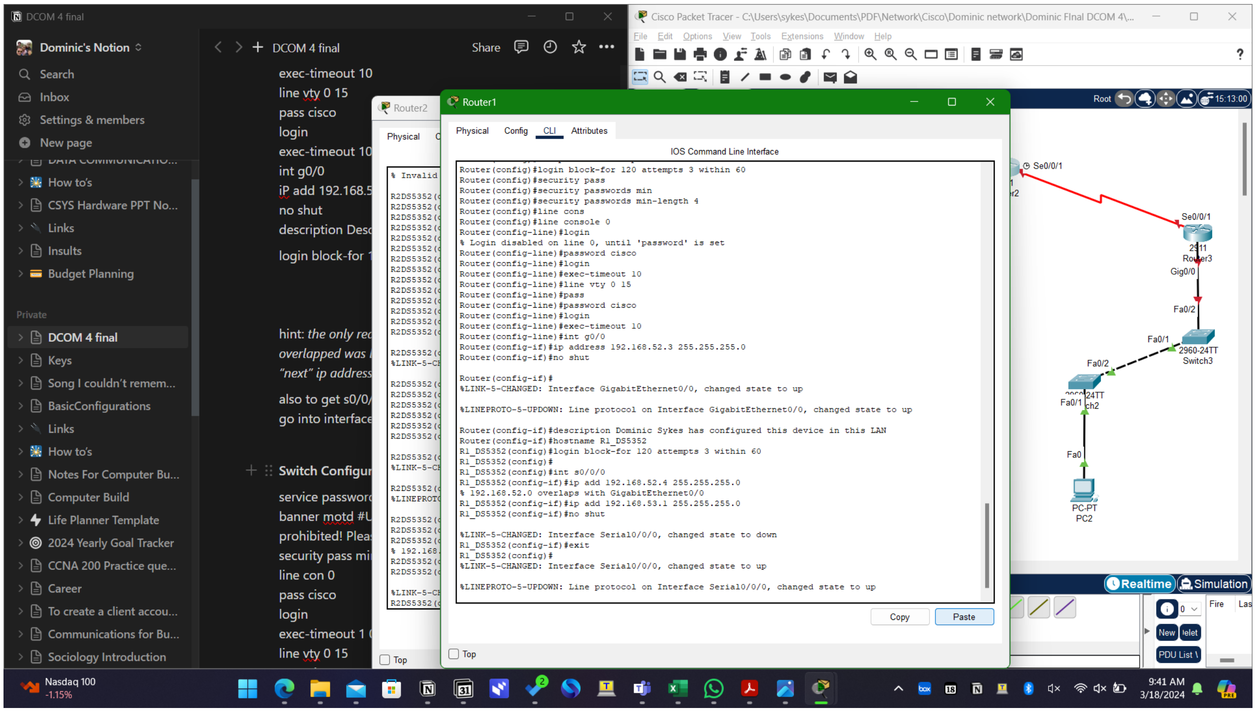
1. **Save Configurations**: Use `copy running-config startup-config` on each router to save configurations.
2. **Verification Document**:
    - **Routing Information:** `show ip route` on each router
    - **NAT Translations:** `show ip nat translations`
    - **ACL Information:** `show access-lists`
    - **Ping Results**: Use `ping` commands to capture successful and unsuccessful pings.

Creating the Final Folder

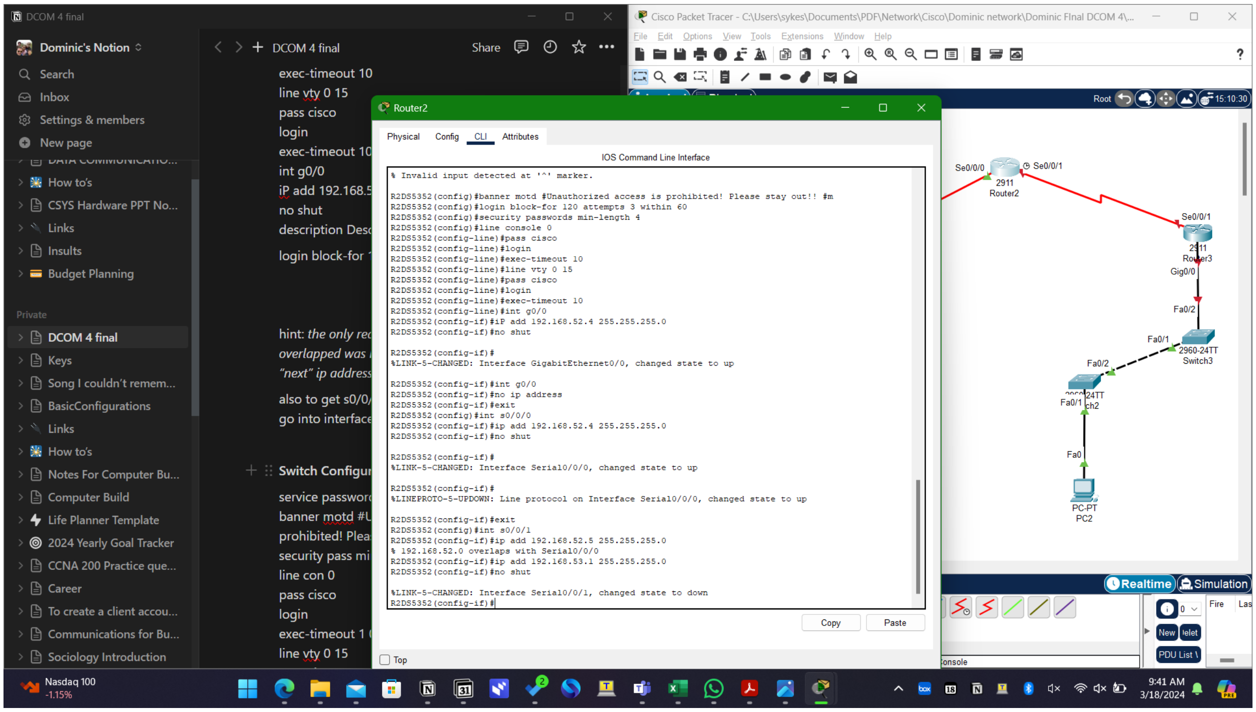
1. Create a folder named `yourfirstnamefinal`.
2. Save configurations as `R1_config.txt`, `R2_config.txt`, and `R3_config.txt`.
3. Create a document named `verification.doc` with screenshots and necessary verification details.
4. Zip the folder and submit it as required.

This script should cover the configurations mentioned in the video and fulfill the specified requirements. Make sure to replace placeholders with the actual IP addresses and interfaces based on your network setup.

****



```
Router(config)#login block-for 120 attempts 3 within 60
Router(config)#security pass
Router(config)#security passwords min
Router(config)#security passwords min-length 4
Router(config)#line cons
Router(config)#line console 0
Router(config-line)#login
% Login disabled on line 0, until 'password' is set
Router(config-line)#password cisco
Router(config-line)#login
Router(config-line)#exec-timeout 10
Router(config-line)#line vty 0 15
Router(config-line)#pass
Router(config-line)#password cisco
Router(config-line)#login
Router(config-line)#exec-timeout 10
Router(config-line)#int g0/0
Router(config-if)#ip address 192.168.52.3 255.255.255.0
Router(config-if)#no shut

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

Router(config-if)#description Dominic Sykes has configured this device in this LAN
Router(config-if)#hostname R1_DS5352
R1_DS5352(config)#login block-for 120 attempts 3 within 60
R1_DS5352(config)#
R1_DS5352(config)#int s0/0/0
R1_DS5352(config-if)#ip add 192.168.52.4 255.255.255.0
% 192.168.52.0 overlaps with GigabitEthernet0/0
R1_DS5352(config-if)#ip add 192.168.53.1 255.255.255.0
R1_DS5352(config-if)#no shut

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R1_DS5352(config-if)#exit
R1_DS5352(config)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
```



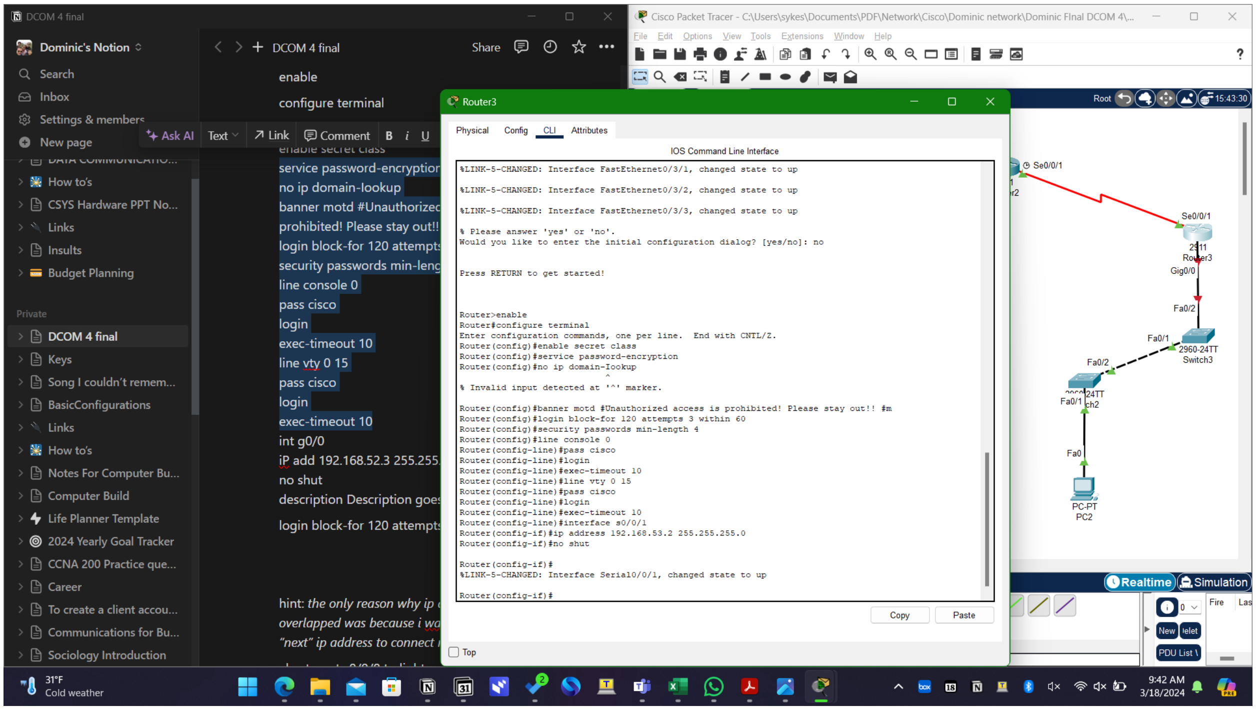
exec-timeout 10
line vty 0 15
pass cisco
login
exec-timeout 10
int g0/0
iP add 192.168.5
no shut
description Desc
login block-for

hint: the only rea
overlapped was
"next" ip address
also to get s0/0/
go into interface

Switch Configur

service passwor
banner motd #U
prohibited! Plea
security pass mi
line con 0
pass cisco
login
exec-timeout 1
line vty 0 15

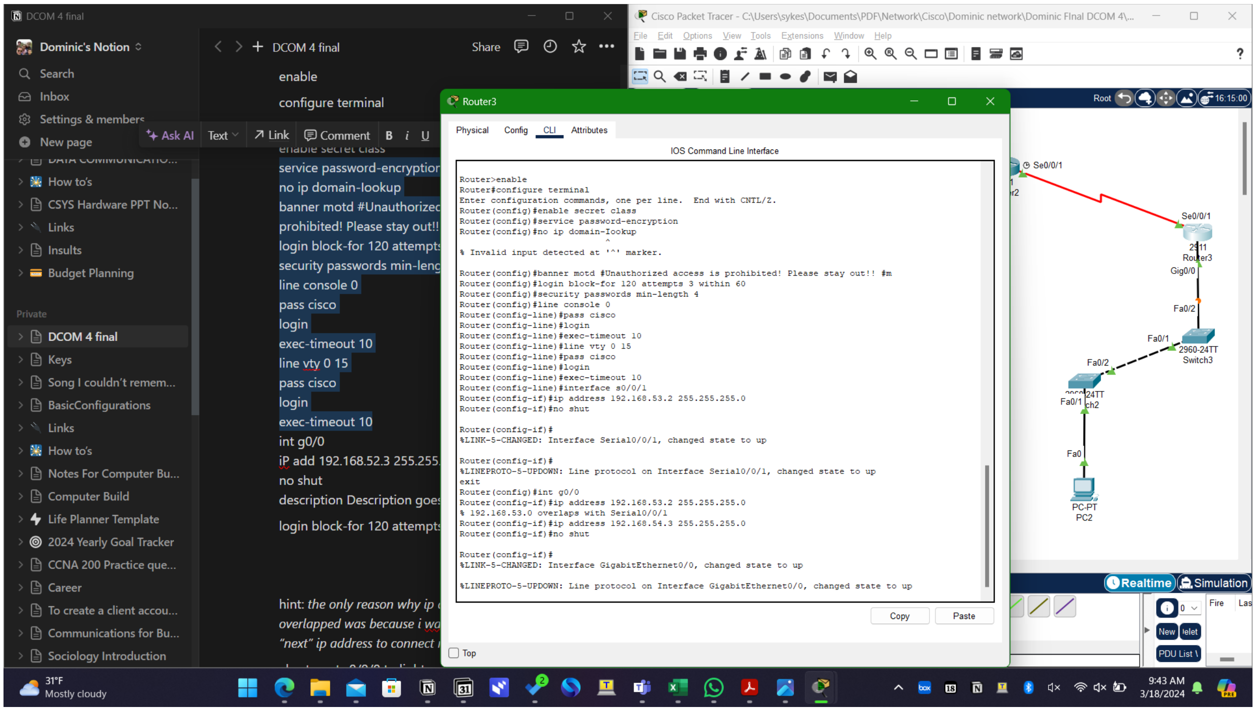
```
% Invalid input detected at '^' marker.

R2DS5352(config)#banner motd #Unauthorized access is prohibited! Please stay out!! #m
R2DS5352(config)#login block-for 120 attempts 3 within 60
R2DS5352(config)#security passwords min-length 4
R2DS5352(config)#line console 0
R2DS5352(config-line)#pass cisco
R2DS5352(config-line)#login
R2DS5352(config-line)#exec-timeout 10
R2DS5352(config-line)#line vty 0 15
R2DS5352(config-line)#pass cisco
R2DS5352(config-line)#login
R2DS5352(config-line)#exec-timeout 10
R2DS5352(config-line)#int g0/0
R2DS5352(config-if)#iP add 192.168.52.4 255.255.255.0
R2DS5352(config-if)#no shut

R2DS5352(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

R2DS5352(config-if)#int g0/0
R2DS5352(config-if)#no ip address
R2DS5352(config-if)#exit
R2DS5352(config)#int s0/0/0
R2DS5352(config-if)#ip add 192.168.52.4 255.255.255.0
R2DS5352(config-if)#no shut

R2DS5352(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

R2DS5352(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

R2DS5352(config-if)#exit
R2DS5352(config)#int s0/0/1
R2DS5352(config-if)#ip add 192.168.52.5 255.255.255.0
% 192.168.52.0 overlaps with Serial0/0/0
R2DS5352(config-if)#ip add 192.168.53.1 255.255.255.0
R2DS5352(config-if)#no shut

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
R2DS5352(config-if)#
```



enable
configure terminal
enable secret class
service password-encryption
no ip domain-lookup
banner motd #Unauthorized
prohibited! Please stay out!!
login block-for 120 attempts
security passwords min-leng
line console 0
pass cisco
login
exec-timeout 10
line vty 0 15
pass cisco
login
exec-timeout 10
int g0/0
iP add 192.168.52.3 255.255
no shut
description Description goes
login block-for 120 attempts

hint: the only reason why ip
overlapped was because i wa
"next" ip address to connect

```
%LINK-5-CHANGED: Interface FastEthernet0/3/1, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/3/2, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/3/3, changed state to up

% Please answer 'yes' or 'no'.
Would you like to enter the initial configuration dialog? [yes/no]: no


Press RETURN to get started!



Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#enable secret class
Router(config)#service password-encryption
Router(config)#no ip domain-Iookup
                              ^
% Invalid input detected at '^' marker.

Router(config)#banner motd #Unauthorized access is prohibited! Please stay out!! #m
Router(config)#login block-for 120 attempts 3 within 60
Router(config)#security passwords min-length 4
Router(config)#line console 0
Router(config-line)#pass cisco
Router(config-line)#login
Router(config-line)#exec-timeout 10
Router(config-line)#line vty 0 15
Router(config-line)#pass cisco
Router(config-line)#login
Router(config-line)#exec-timeout 10
Router(config-line)#interface s0/0/1
Router(config-if)#ip address 192.168.53.2 255.255.255.0
Router(config-if)#no shut

Router(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up

Router(config-if)#
```



```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#enable secret class
Router(config)#service password-encryption
Router(config)#no ip domain-Iookup
                          ^
% Invalid input detected at '^' marker.

Router(config)#banner motd #Unauthorized access is prohibited! Please stay out!! #m
Router(config)#login block-for 120 attempts 3 within 60
Router(config)#security passwords min-length 4
Router(config)#line console 0
Router(config-line)#pass cisco
Router(config-line)#login
Router(config-line)#exec-timeout 10
Router(config-line)#line vty 0 15
Router(config-line)#pass cisco
Router(config-line)#login
Router(config-line)#exec-timeout 10
Router(config-line)#interface s0/0/1
Router(config-if)#ip address 192.168.53.2 255.255.255.0
Router(config-if)#no shut

Router(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up

Router(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up
exit
Router(config)#int g0/0
Router(config-if)#ip address 192.168.53.2 255.255.255.0
% 192.168.53.0 overlaps with Serial0/0/1
Router(config-if)#ip address 192.168.54.3 255.255.255.0
Router(config-if)#no shut

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
```

References:

- Cisco: Configure and Understand PPP CHAP Authentication https://www.cisco.com/c/en/us/support/docs/wan/point-to-point-protocol-ppp/10241-ppp-callin-hostname.html
- [YouTube] Video tutorial on configuring PPP with CHAP for Cisco routers (YouTube: https://www.youtube.com/watch?v=VXQyNdo1TxY)

```
bashCopy code
ping 100.52.10.1
```

Submitting Final Configuration Files

1. Save the final configurations for each router as separate text files:
    - `R1_config.txt`
    - `R2_config.txt`
    - `R3_config.txt`
2. Save verification documents including routing information, NAT translations, access list info, and ping tests:
    - `verification.doc` or `verification.pdf`

3. Create a folder named `yourfirstnamefinal` on the desktop and place all the saved files inside. Zip this folder and submit via DC Connect under the `FinalLabExam` assignment folder.

By following these steps, you should have a complete configuration for your network setup, including PPP with CHAP, NAT, OSPF routing, GRE tunnel with BGP, and IP ACLs.

The router bgp commands don’t work

Let's troubleshoot and correct the BGP commands for configuring the GRE tunnel with BGP between R1 and R3. Here is a refined approach with more explicit commands and verification steps.

Router Configuration

```
ho R1
ena sec class
ser pass
no ip dom lo
banner motd #Banner goes here#
login block-for 120 attempts 3 within 60
security pass min 8

line console 0
pass cisco
login
exec-timeout 10
line vty 0 15
pass cisco
login
exec-timeout 10
```

Router 1 DCOM IV Final

Interface Config

```
interface Ethernet0
ip address 100.52.1.1 255.255.255.252
no shutdown

interface G0/0
ip address 100.52.10.1 255.255.255.0
no shutdown

interface S0/0/1
ip address 100.52.1.1 255.255.255.252
no shutdown
```

```
interface Lo10
ip address 11.52.11.1 255.255.255.0
no shutdown
```

Step 2: PPP with CHAP

```
interface S0/0/1
ppp chap
link-quality 75
ppp authentication chap
exit
username R2_DS52 password cisco
```

local database for CHAP – username R2 use cisco as password

Step 3: NAT using ACL

```
access-list 10 permit 100.52.10.0 0.0.0.255
interface G0/0
ip nat inside
interface S0/0/1
ip nat outside
ip nat outside source static any 100.52.1.1
```

Configure OSPF on all routers with AS number 10.

```
router ospf 10
network 100.52.10.0 0.0.0.255 area 0
network 100.52.1.0 0.0.0.255 area 0
```

```
access-list 100 deny icmp any any echo
access-list 100 permit ip any any
interface Ethernet0
ip access-group 100 out
```

```
R1# cop r s
Enabling SSH
R1(config)# ip domain-name
CCNA-labs.com
R1(config)# cry key gen rsa general-keys mod 1024
R1(config)# username Bob secret cisco
R1(config)# line vty 0 15
R1(config-line)# login local
R1(config-line)# transport input ssh
```

```
interface Ethernet0
ip address
no shutdown
description Description goes here
```

```
interface G0/0
ip address
no shutdown
description Description goes here
```

```
interface S0/0/1
ip address
no shutdown
description Description goes here
```

```
interface Lo10
ip address
no shutdown
description Description goes here
```

```
interface S0/0/0
ppp chap
link-quality 75
ppp authentication chap
exit
username R1_DS52 password cisco
```

local database for CHAP – username R1 use cisco as password

```
interface S0/0/1
ppp chap
link-quality 75
ppp authentication chap
exit
username R3_DS52 password cisco
```

local database for CHAP – username R3 use cisco as password

Router 3 DCOM IV Final

Router Configuration

```
ho R3
enable secret class
service pass
R1(config)# no ip dom lo
R1(config)# banner motd #Banner goes here#
R1(config)# login block-for 120 attempts 3 within 60
R1(config)# security pass min 8
```

```
line console 0
pass cisco
login
exec-timeout 10
line vty 0 15
pass cisco
login
exec-timeout 10
```

```
description Description goes here
```

```
R1# cop r s
```

Enabling SSH

```
ip domain-name
CCNA-labs.com
cry key gen rsa general-keys mod 1024
username Bob secret cisco
line vty 0 15
login local
transport input ssh

interface S0/0/0
ppp chap
link-quality 75
ppp authentication chap
exit
username R2_DS52 password cisco
local database for CHAP – username R2 use cisco as password

access-list 20 permit 200.52.2.0 0.0.0.255
interface G0/0
ip nat inside
interface S0/0/0
ip nat outside
ip nat outside source static any 100.52.1.2

interface Tunnel1
ip address 192.168.52.2 255.255.255.252
tunnel source G0/0
tunnel destination 100.52.1.1
ip route 192.168.52.1 255.255.255.252 Tunnel1

router bgp 65220
neighbor 192.168.52.1 remote-as 65210
network 200.52.2.0 mask 255.255.255.0
```