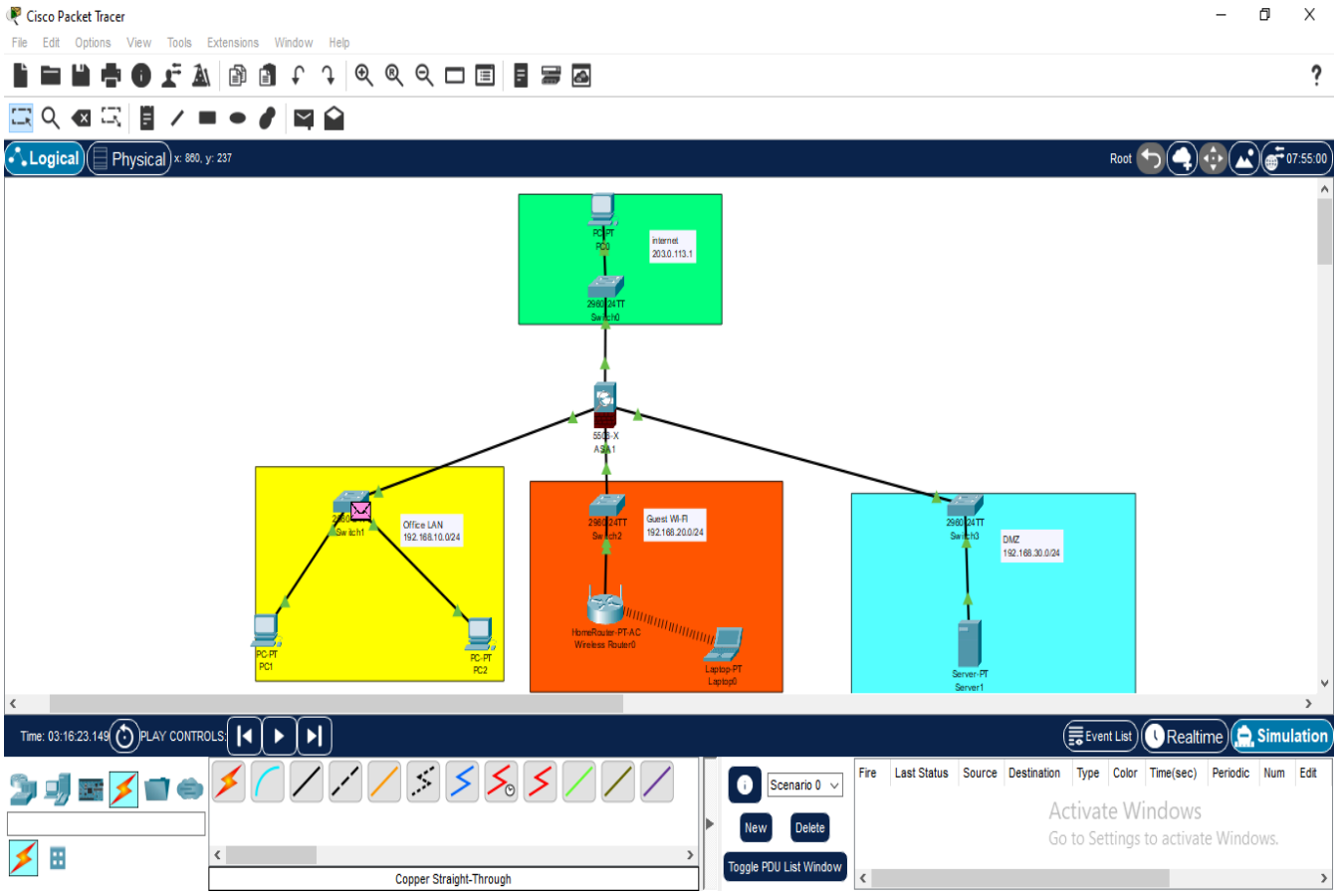
Designing a Secure Network Topology for a Small Office

Diagram of my network topology



Details of IP ranges, VLANS, and Firewall Rules

IP Ranges and VLAN Assignments

Zone	VLAN ID	Subnet	ASA Interface	IP Address
Inside LAN	10	192.168.10.0/24	`GigabitEthernet0/1`	192.168.10.1
Guest Wi-Fi	20	192.168.20.0/24	`GigabitEthernet0/2`	192.168.20.1

DMZ	30	192.168.30.0/24	`GigabitEthernet0/3`	192.168.30.1
Outside (ISP)	N/A	Public IP (Internet)	`GigabitEthernet0/0`	203.0.113.1

Firewall Rules Configuration

✅ Allow Internal Traffic (Inside Zone)

bash

Copy

Edit

```
access-list inside_access_in extended permit ip any any access-group inside_access_in in interface inside
```

🚫 Restrict Guest Wi-Fi Access to Internal LAN

bash

Copy

Edit

```
access-list guest_access_in extended deny ip any 192.168.10.0 255.255.255.0 access-list guest_access_in extended permit ip any any access-group guest_access_in in interface guest
```

✅ Allow External Access to DMZ Services (HTTP/HTTPS)

bash

Copy

Edit

```
access-list outside_access_in extended permit tcp any host 192.168.30.2 eq 80 access-list outside_access_in extended permit tcp
```

```
any host 192.168.30.2 eq 443 access-group outside_access_in in
interface outside
```

NAT Rules

🔁 PAT (Port Address Translation)

bash

Copy

Edit

```
! Inside LAN to Outside object network INSIDE_NET subnet 192.168.10.0
255.255.255.0 nat (inside,outside) dynamic interface ! Guest Wi-Fi to
Outside object network GUEST_NET subnet 192.168.20.0 255.255.255.0
nat (guest,outside) dynamic interface
```

Static NAT for Public Access to DMZ Web Server

bash

Copy

Edit

```
object network WEB_SERVER host 192.168.30.2 nat (dmz,outside) static
203.0.113.2
```

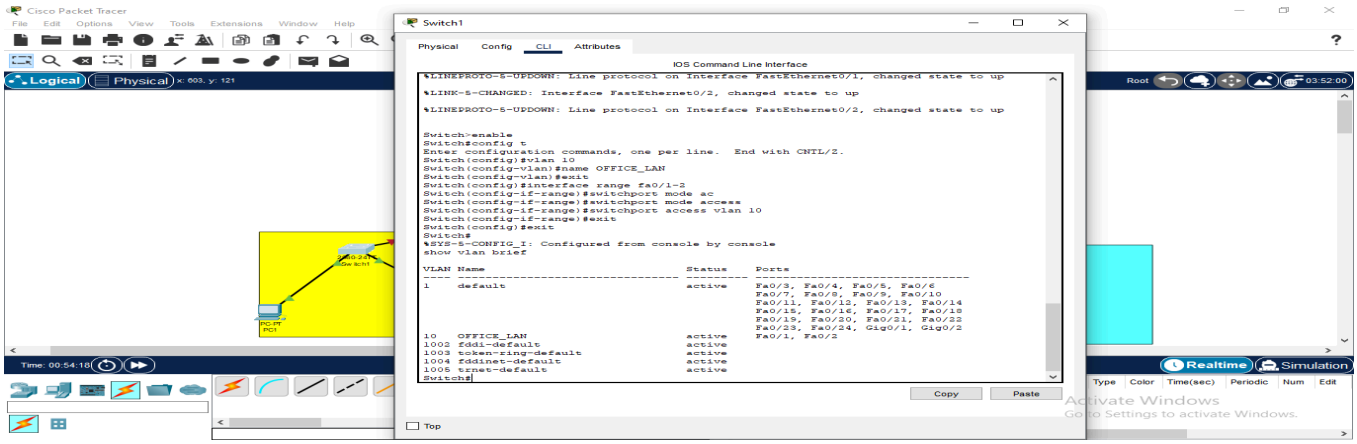
Identity NAT (Tracking)

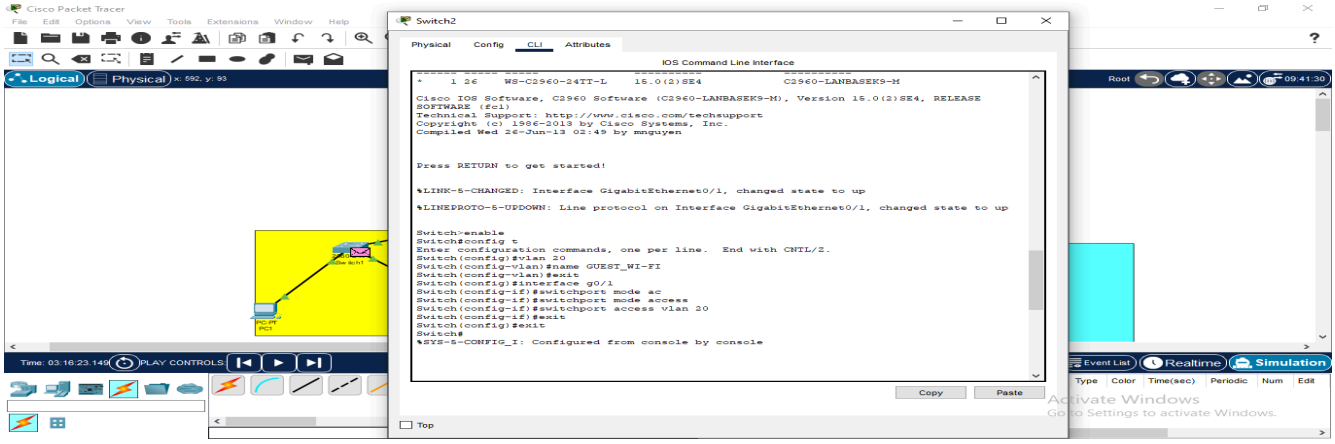
bash

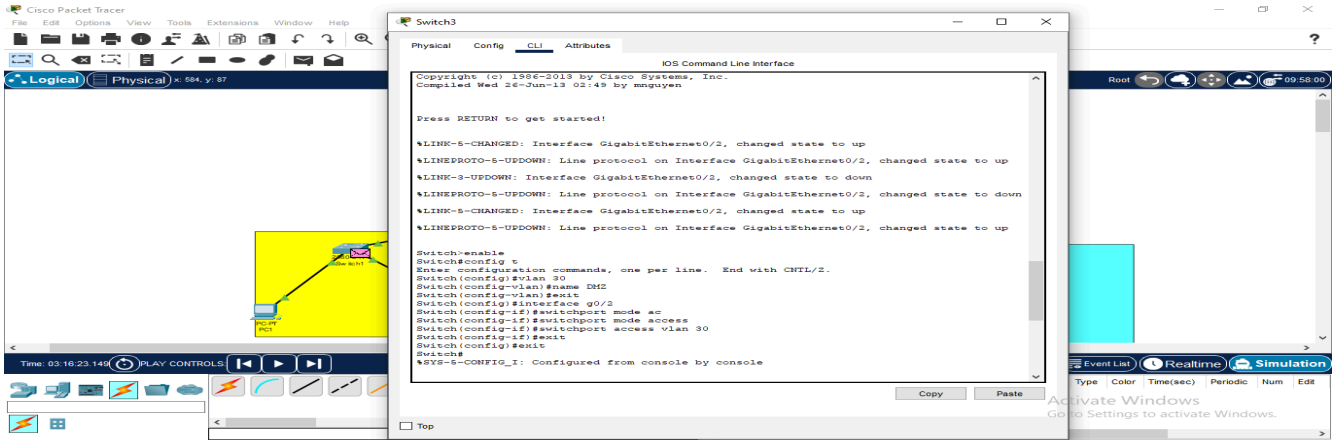
Copy

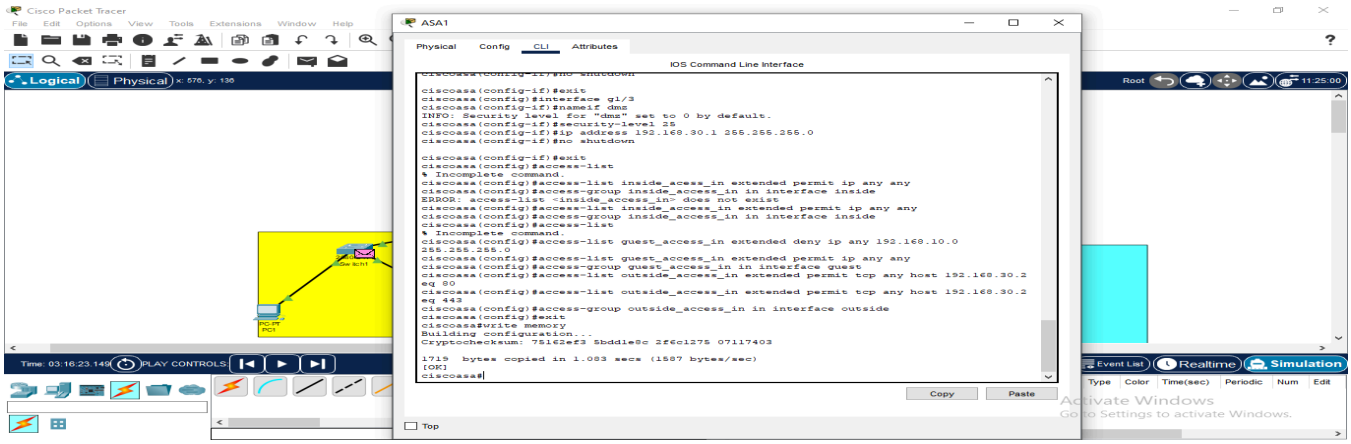
Edit

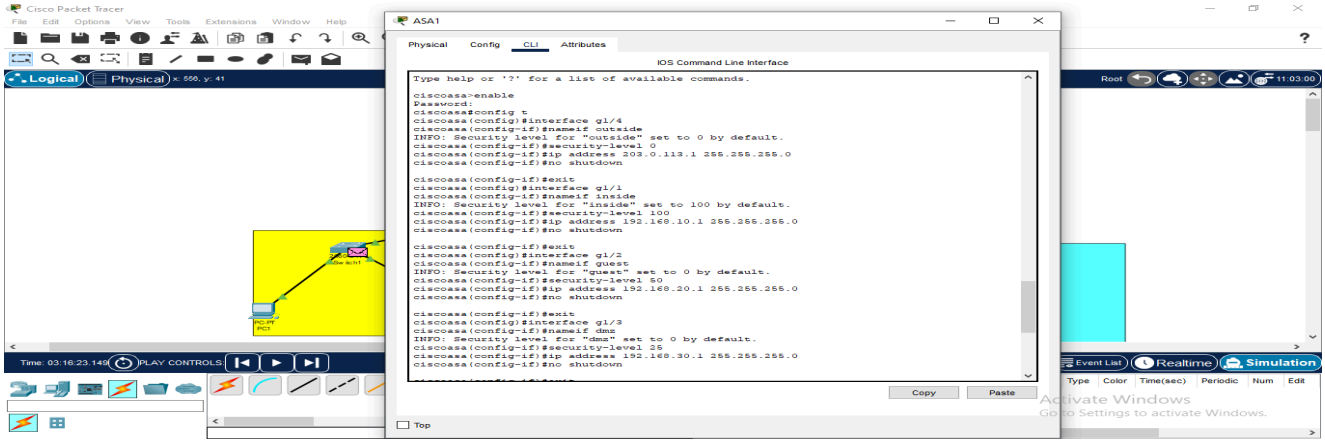
```
nat (inside,guest) source static INSIDE_NET INSIDE_NET destination
static GUEST_NET GUEST_NET no-proxy-arp
```

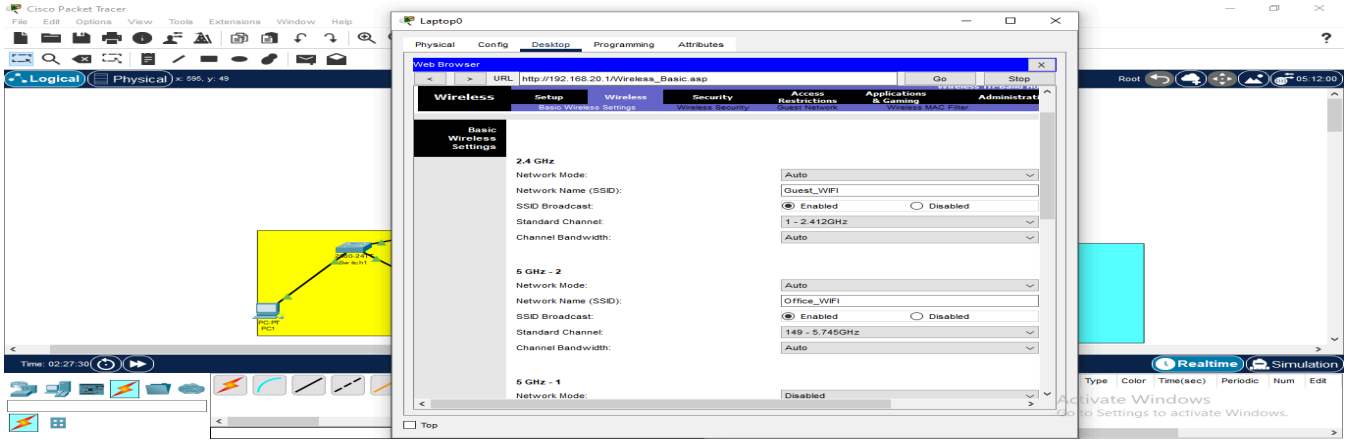

Cisco Packet Tracer
Switch1
Physical
Config
CLI
Attributes
IOS Command Line Interface
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up
Switch>enable
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name OFFICE_LAN
Switch(config-vlan)#exit
Switch(config)#interface range fa0/1-2
Switch(config-if-range)#switchport mode ac
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console
show vlan brief
VLAN Name Status Ports
1 default active Fa0/3, Fa0/4, Fa0/5, Fa0/6
Fa0/7, Fa0/8, Fa0/9, Fa0/10
Fa0/11, Fa0/12, Fa0/13, Fa0/14
Fa0/15, Fa0/16, Fa0/17, Fa0/18
Fa0/19, Fa0/20, Fa0/21, Fa0/22
Fa0/23, Fa0/24, Gig0/1, Gig0/2
10 OFFICE_LAN active Fa0/1, Fa0/2
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active
Switch#
Copy
Paste
Top
Logical
Physical
Root
Realtime
Simulation
Activate Windows
Go to Settings to activate Windows.

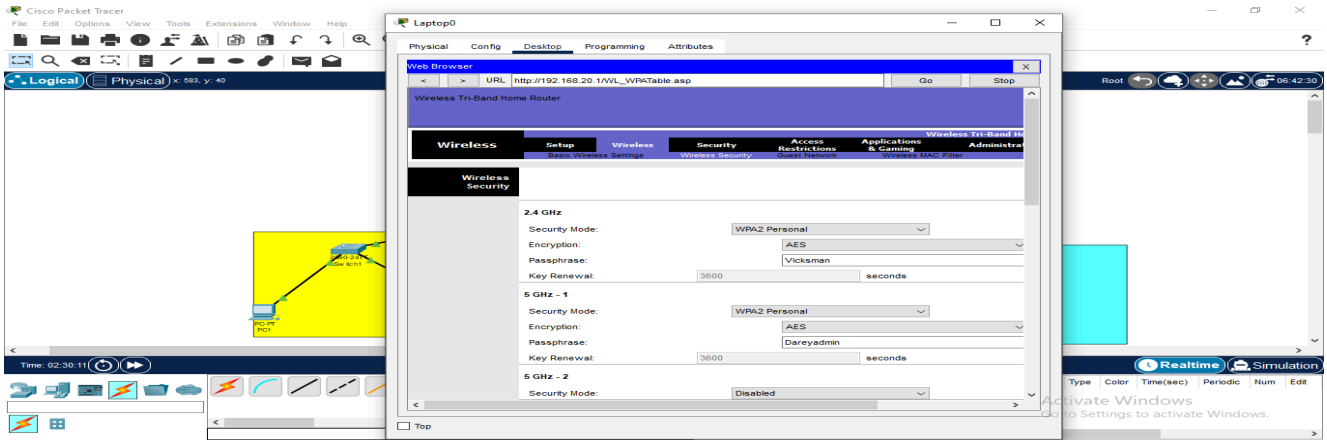

Cisco Packet Tracer
Switch2
Physical
Config
CLI
Attributes
IOS Command Line Interface
* 1 26 WS-C2960-24TT-L 15.0(2)SE4 C2960-LANBASEK9-M
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Wed 26-Jun-13 02:49 by mnguyen
Press RETURN to get started!
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
Switch>enable
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 20
Switch(config-vlan)#name GUEST_WI-FI
Switch(config-vlan)#exit
Switch(config)#interface g0/1
Switch(config-if)#switchport mode ac
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console
Copy
Paste
Top
Logical
Physical
Root
Realtime
Simulation
Activate Windows
Go to Settings to activate Windows.

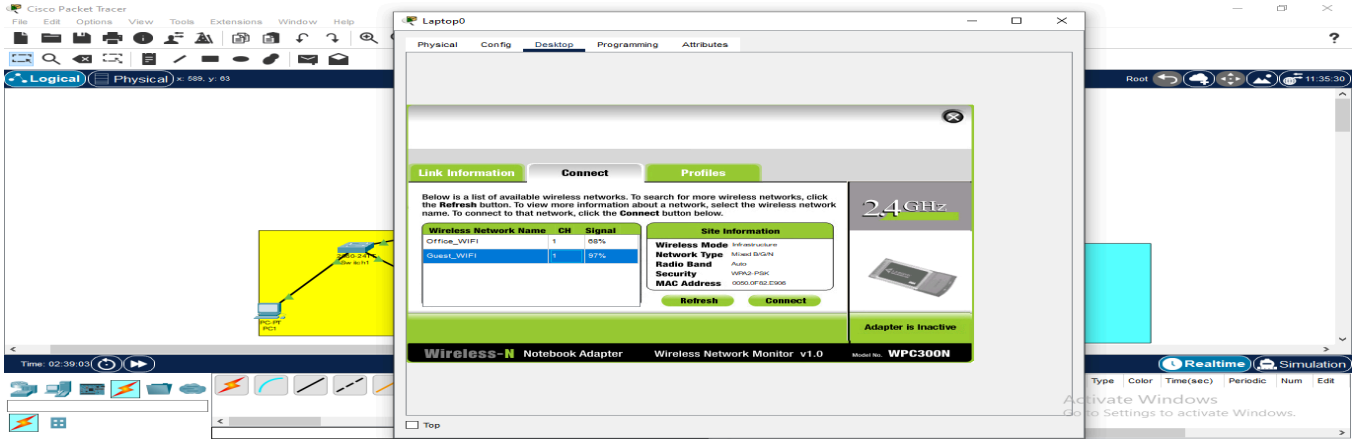

Cisco Packet Tracer
Switch3
Physical
Config
CLI
Attributes
IOS Command Line Interface
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Wed 26-Jun-13 02:49 by mnguyen
Press RETURN to get started!
%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/2, changed state to up
%LINK-3-UPDOWN: Interface GigabitEthernet0/2, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/2, changed state to down
%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/2, changed state to up
Switch>enable
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 30
Switch(config-vlan)#name DMZ
Switch(config-vlan)#exit
Switch(config)#interface g0/2
Switch(config-if)#switchport mode ac
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 30
Switch(config-if)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console
Copy
Paste
Top
Logical
Physical
Root
Realtime
Simulation
Activate Windows
Go to Settings to activate Windows.


Cisco Packet Tracer
ASA1
Physical
Config
CLI
Attributes
IOS Command Line Interface
ciscoasa(config-if)#exit
ciscoasa(config)#interface gi/3
ciscoasa(config-if)#nameif dmz
INFO: Security level for "dmz" set to 0 by default.
ciscoasa(config-if)#security-level 25
ciscoasa(config-if)#ip address 192.168.30.1 255.255.255.0
ciscoasa(config-if)#no shutdown
ciscoasa(config-if)#exit
ciscoasa(config)#access-list
% Incomplete command.
ciscoasa(config)#access-list inside_acess_in extended permit ip any any
ciscoasa(config)#access-group inside_access_in in interface inside
ERROR: access-list <inside_access_in> does not exist
ciscoasa(config)#access-list inside_access_in extended permit ip any any
ciscoasa(config)#access-group inside_access_in in interface inside
ciscoasa(config)#access-list
% Incomplete command.
ciscoasa(config)#access-list guest_access_in extended deny ip any 192.168.10.0
255.255.255.0
ciscoasa(config)#access-list guest_access_in extended permit ip any any
ciscoasa(config)#access-group guest_access_in in interface guest
ciscoasa(config)#access-list outside_access_in extended permit tcp any host 192.168.30.2
eq 80
ciscoasa(config)#access-list outside_access_in extended permit tcp any host 192.168.30.2
eq 443
ciscoasa(config)#access-group outside_access_in in interface outside
ciscoasa(config)#exit
ciscoasa#write memory
Building configuration...
Cryptochecksum: 75162ef3 5bddle8c 2f6c1275 07117403
1719 bytes copied in 1.083 secs (1587 bytes/sec)
[OK]
ciscoasa#
Copy
Paste
Top
Logical
Physical
Root
Time: 03:16:23.149
PLAY CONTROLS:
Event List
Realtime
Simulation
Type
Color
Time(sec)
Periodic
Num
Edit
Activate Windows
Go to Settings to activate Windows.


Cisco Packet Tracer
ASA1
Physical
Config
CLI
Attributes
IOS Command Line Interface
Type help or '?' for a list of available commands.
ciscoasa>enable
Password:
ciscoasa#config t
ciscoasa(config)#interface gi/4
ciscoasa(config-if)#nameif outside
INFO: Security level for "outside" set to 0 by default.
ciscoasa(config-if)#security-level 0
ciscoasa(config-if)#ip address 203.0.113.1 255.255.255.0
ciscoasa(config-if)#no shutdown
ciscoasa(config-if)#exit
ciscoasa(config)#interface gi/1
ciscoasa(config-if)#nameif inside
INFO: Security level for "inside" set to 100 by default.
ciscoasa(config-if)#security-level 100
ciscoasa(config-if)#ip address 192.168.10.1 255.255.255.0
ciscoasa(config-if)#no shutdown
ciscoasa(config-if)#exit
ciscoasa(config)#interface gi/2
ciscoasa(config-if)#nameif guest
INFO: Security level for "guest" set to 0 by default.
ciscoasa(config-if)#security-level 50
ciscoasa(config-if)#ip address 192.168.20.1 255.255.255.0
ciscoasa(config-if)#no shutdown
ciscoasa(config-if)#exit
ciscoasa(config)#interface gi/3
ciscoasa(config-if)#nameif dmz
INFO: Security level for "dmz" set to 0 by default.
ciscoasa(config-if)#security-level 25
ciscoasa(config-if)#ip address 192.168.30.1 255.255.255.0
ciscoasa(config-if)#no shutdown
Copy
Paste
Top
Logical
Physical
Root
Time: 03:16:23.149
PLAY CONTROLS:
Event List
Realtime
Simulation
Type
Color
Time(sec)
Periodic
Num
Edit
Activate Windows
Go to Settings to activate Windows.

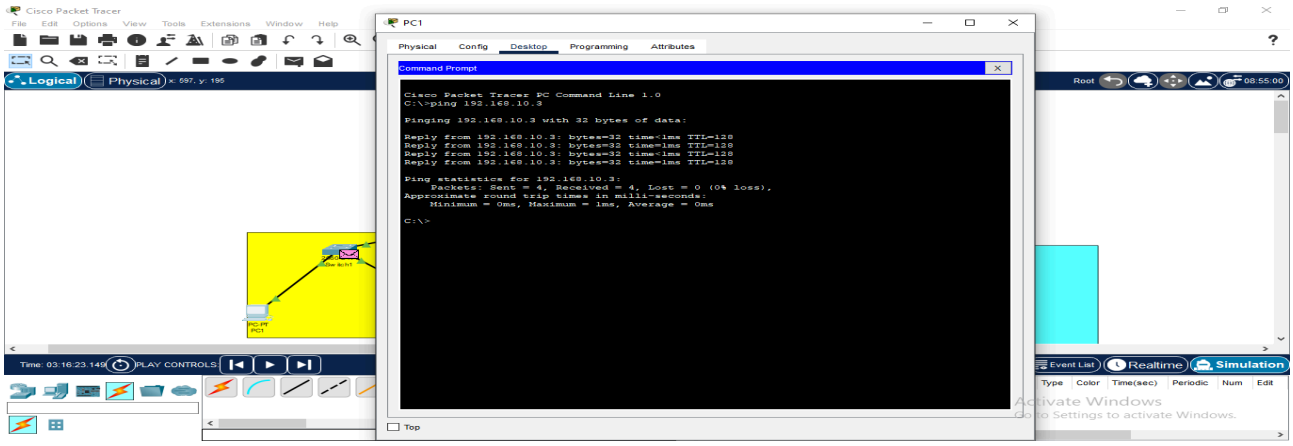

Cisco Packet Tracer
Laptop0
Physical
Config
Desktop
Programming
Attributes
Web Browser
URL
http://192.168.20.1/Wireless_Basic.asp
Go
Stop
Wireless
Setup
Wireless
Security
Access Restrictions
Applications & Gaming
Administrat
Basic Wireless Settings
Wireless Security
Guest Access
WMM & MAC Filter
Basic Wireless Settings
2.4 GHz
Network Mode:
Auto
Network Name (SSID):
Guest_WIFI
SSID Broadcast:
Enabled
Disabled
Standard Channel:
1 - 2.412GHz
Channel Bandwidth:
Auto
5 GHz - 2
Network Mode:
Auto
Network Name (SSID):
Office_WIFI
SSID Broadcast:
Enabled
Disabled
Standard Channel:
149 - 5.745GHz
Channel Bandwidth:
Auto
5 GHz - 1
Network Mode:
Disabled
Top
Logical
Physical
Root
Time: 02:27:30
Realtime
Simulation
Type
Color
Time(sec)
Periodic
Num
Edit
Activate Windows
Go to Settings to activate Windows.


Cisco Packet Tracer
Laptop0
Physical
Config
Desktop
Programming
Attributes
Web Browser
URL
http://192.168.20.1/WL_WPATable.asp
Go
Stop
Wireless Tri-Band Home Router
Wireless
Setup
Wireless
Security
Access Restrictions
Applications & Gaming
Administra
Basic Wireless Settings
Wireless Security
Guest Access
Wireless MAC Filter
Wireless Security
2.4 GHz
Security Mode:
WPA2 Personal
Encryption:
AES
Passphrase:
Vicksman
Key Renewal:
3600
seconds
5 GHz - 1
Security Mode:
WPA2 Personal
Encryption:
AES
Passphrase:
Dareyadmin
Key Renewal:
3600
seconds
5 GHz - 2
Security Mode:
Disabled
Top
Logical
Physical
Root
Realtime
Simulation
Activate Windows
Go to Settings to activate Windows.


Cisco Packet Tracer
Laptop0
Physical
Config
Desktop
Programming
Attributes
Link Information
Connect
Profiles
Below is a list of available wireless networks. To search for more wireless networks, click the Refresh button. To view more information about a network, select the wireless network name. To connect to that network, click the Connect button below.
Wireless Network Name
CH
Signal
Office_WIFI
1
68%
Guest_WIFI
1
97%
Site Information
Wireless Mode
Network Type
Radio Band
Security
MAC Address
Refresh
Connect
2.4GHz
Adapter is Inactive
Wireless-N Notebook Adapter
Wireless Network Monitor v1.0
Model No.
WPC300N
Top
Logical
Physical
Root
Realtime
Simulation
Activate Windows
Go to Settings to activate Windows.


Cisco Packet Tracer
Laptop0
Physical
Config
Desktop
Programming
Attributes
Link Information
Connect
Profiles
More Information
Infrastructure Mode
You have successfully connected to the access point
2.4GHz
Signal Strength
Link Quality
Adapter is Active
Wireless-N Notebook Adapter
Wireless Network Monitor v1.0
Model No.
WPC300N
Top
Logical
Physical
Root
Event List
Realtime
Simulation
Activate Windows
Go to Settings to activate Windows.

Results of Connectivity and Security tests



Connectivity Test Results

Test	Source → Destination	Result	Notes
Ping LAN Host to Internet	192.168.10.x → 8.8.8.8	✅ Success	PAT working as expected.
Ping Guest to Internet	192.168.20.x → 8.8.8.8	✅ Success	Guest subnet has internet access via PAT.
Ping Guest to Inside LAN	192.168.20.x → 192.168.10.x	❌ Blocked	Correctly blocked by firewall rule.
Ping Inside LAN to Guest	192.168.10.x → 192.168.20.x	✅ Success	Identity NAT allows this direction.
Ping Outside to DMZ Web Server	Public IP → 192.168.30.2	✅ Success	NAT and ACL rules correctly allow HTTP/HTTPS access.

Ping Inside LAN to DMZ Server	192.168.10.x → 192.168.30.2	✅ Success	Routed and allowed by default policy.
DMZ Server to Inside LAN	192.168.30.2 → 192.168.10.x	❌ Blocked	Implicit deny from lower to higher security zone.

Security Test Results

Test	Expected Behavior	Result	Comments
Guest can't reach internal services	Deny	✅ Pass	Access list successfully enforces isolation.
Inside users can access Internet safely	Allow via PAT	✅ Pass	PAT is translating inside addresses correctly.
Unsolicited traffic from outside is blocked	Deny	✅ Pass	Default deny on outside interface.
Outside access only to HTTP/HTTPS on DMZ	Allow only ports 80/443	✅ Pass	ACL and static NAT enforce port-specific access.
DMZ → Inside initiated connections blocked	Deny	✅ Pass	Security levels and ACLs prevent this path.

Recommendations for Improvement

- Enable logging on ACLs and NATs for better visibility and troubleshooting.
- Consider adding rate-limiting or IPS/IDS on the DMZ interface if public access is significant.
- Use object-groups in ACLs for scalability as more services are added.