**Assignment 6**

**Routing Security: BGP / OSPF — simulating a BGP route hijack in Packet Tracer**

**Duration:** 2 academic hours

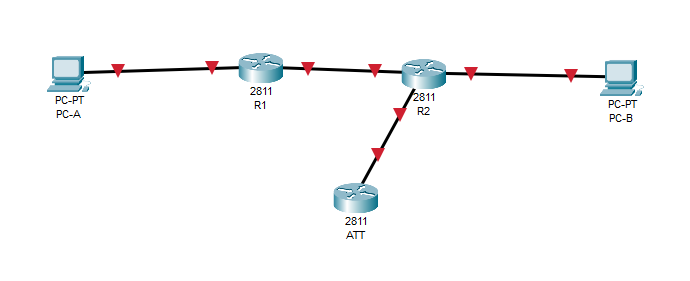
**Goal:** Build a simple BGP network, simulate announcing someone else’s prefix (route hijack) and protect the network using a simple prefix-filter.

**Tool:** Cisco Packet Tracer.

**Short instruction**

Open Packet Tracer, assemble the topology, enter the commands listed for each router, run checks with show ip bgp and traceroute, then simulate the hijack and apply the filter.

**Topology — build this in Packet Tracer**



**Addresses and interfaces**

**R1**

Fa0/0: 10.0.12.1/24 (link to R2 Fa0/0)

Fa0/1: 192.168.10.1/24 (PC-A gateway)

**R2**

Fa0/0: 10.0.12.2/24 (link to R1)

Fa0/1: 192.168.20.1/24 (PC-B gateway)

Fa1/0: 10.0.13.1/24 (link to ATT)

**ATT (Attacker)**

Fa0/0: 10.0.13.2/24 (link to R2 Fa0/1)

**PC-A**: 192.168.10.10/24, GW = 192.168.10.1

**PC-B**: 192.168.20.10/24, GW = 192.168.20.1

(Cisco 2811 routers in Packet Tracer; two Desktop PCs.)

**Изображение выглядит как текст, электроника, снимок экрана, программное обеспечение

Содержимое, созданное искусственным интеллектом, может быть неверным.** **Изображение выглядит как текст, электроника, снимок экрана, программное обеспечение

Содержимое, созданное искусственным интеллектом, может быть неверным.**

**Preparation**

1. In Packet Tracer add devices: R1, R2, ATT (routers), PC-A and PC-B (PCs).
2. Connect devices with straight-through cables (Fa ↔ Fa).
3. On PCs set IP and gateway (Desktop → IP Configuration).
4. Open CLI on each router.

**Configurations — enter these commands in each router’s CLI**

**R1 (AS 65010)**

enable

configure terminal

hostname R1

no ip domain-lookup

interface FastEthernet0/0

ip address 10.0.12.1 255.255.255.0

no shutdown

interface FastEthernet0/1

ip address 192.168.10.1 255.255.255.0

no shutdown

router bgp 65010

no synchronization

bgp log-neighbor-changes

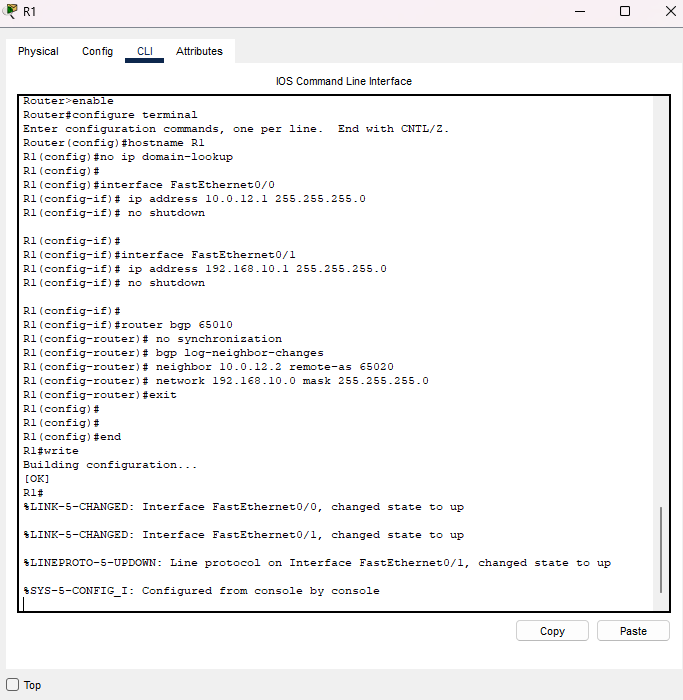
neighbor 10.0.12.2 remote-as 65020

network 192.168.10.0 mask 255.255.255.0

exit

end

write



**R2 (AS 65020)**

enable

configure terminal

hostname R2

no ip domain-lookup # disables delays caused by mistyped commands

interface FastEthernet0/0

ip address 10.0.12.2 255.255.255.0

no shutdown

interface FastEthernet0/1

ip address 192.168.20.1 255.255.255.0

no shutdown

interface FastEthernet1/0

ip address 10.0.13.1 255.255.255.0

no shutdown

router bgp 65020

no synchronization

bgp log-neighbor-changes

neighbor 10.0.12.1 remote-as 65010

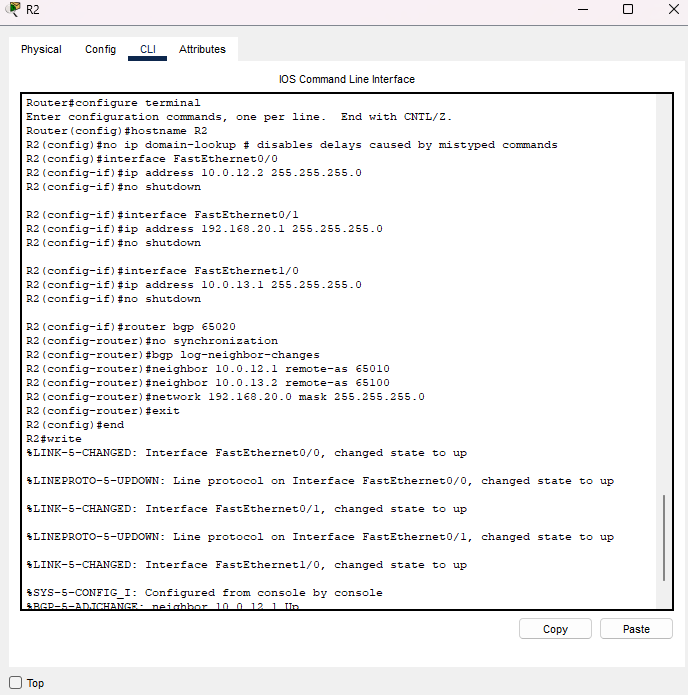
neighbor 10.0.13.2 remote-as 65100

network 192.168.20.0 mask 255.255.255.0

exit

end

write



**ATT (Attacker, AS 65100) — initial state (announce nothing)**

enable

configure terminal

hostname ATT

no ip domain-lookup

interface FastEthernet0/0

ip address 10.0.13.2 255.255.255.0

no shutdown

router bgp 65100

no synchronization

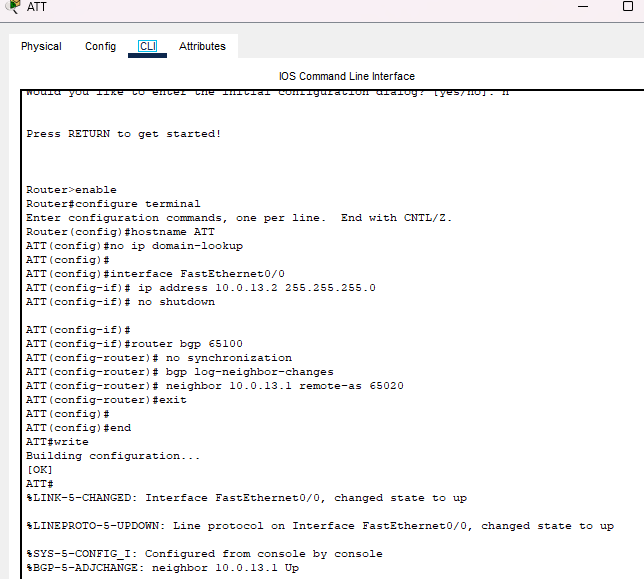
bgp log-neighbor-changes

neighbor 10.0.13.1 remote-as 65020

exit

end

write



Note: no ip domain-lookup disables delays caused by mistyped commands.

Изображение выглядит как снимок экрана, линия

Содержимое, созданное искусственным интеллектом, может быть неверным.

**Checks before the attack**

- On R1 and R2: show ip bgp summary — ensure neighbors are established (State = Established).

Изображение выглядит как текст, снимок экрана, Шрифт, число

Содержимое, созданное искусственным интеллектом, может быть неверным.

Изображение выглядит как текст, снимок экрана, Шрифт, число

Содержимое, созданное искусственным интеллектом, может быть неверным.

- On R2: show ip bgp — 192.168.20.0/24 should be advertised.

Изображение выглядит как текст, снимок экрана, Шрифт, дисплей

Содержимое, созданное искусственным интеллектом, может быть неверным.

- On PC-A: ping 192.168.20.10 — should reply.

Изображение выглядит как текст, снимок экрана, Шрифт

Содержимое, созданное искусственным интеллектом, может быть неверным.

Take screenshots: show ip bgp (before hijack) and successful ping.

**Simulating the hijack**

On **ATT**, enter:

enable

configure terminal

router bgp 65100

network 192.168.20.0 mask 255.255.255.0

end

write

Изображение выглядит как текст, снимок экрана, Шрифт, число

Содержимое, созданное искусственным интеллектом, может быть неверным.

— now ATT announces the same prefix 192.168.20.0/24.

After that:

- On R1 and R2: show ip bgp — compare to previous output (you should see a path via AS65100 or a new entry).

Изображение выглядит как текст, снимок экрана, Шрифт, число

Содержимое, созданное искусственным интеллектом, может быть неверным.

Изображение выглядит как текст, снимок экрана, Шрифт, дисплей

Содержимое, созданное искусственным интеллектом, может быть неверным.

- On PC-A: tracert 192.168.20.10 (or Trace in PT) — the path may go through ATT.

Изображение выглядит как текст, снимок экрана, Шрифт

Содержимое, созданное искусственным интеллектом, может быть неверным.

Take screenshots: show ip bgp (after hijack), traceroute/ping.

**Protection — simple filter on R2**

On **R2**, create a prefix-list and attach a route-map to the ATT neighbor to filter incoming announcements:

