

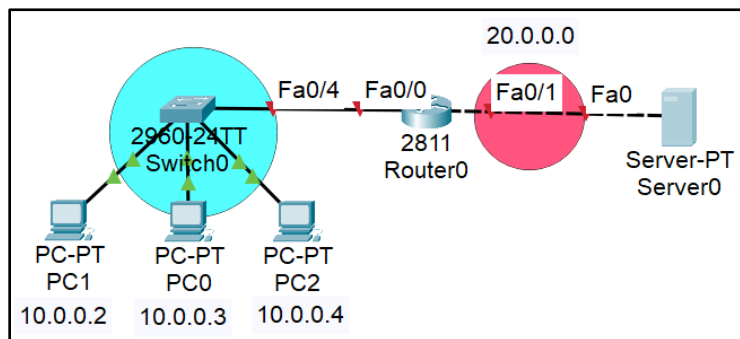


جلسه سیزدهم :

لیست‌های دسترسی (Access Lists) در مسیریاب‌ها مجموعه‌ای از قوانین و فیلترها هستند که برای کنترل ترافیک شبکه استفاده می‌شوند. این لیست‌ها به مدیران شبکه اجازه می‌دهند تا دسترسی به بخش‌های مختلف شبکه را بر اساس معیارهایی مانند آدرس IP، پورت‌های شبکه و پروتکل‌های مختلف مدیریت و محدود کنند. با استفاده از Access List، می‌توان ترافیک ورودی و خروجی را فیلتر کرد تا تنها کاربران مجاز به بخش‌های خاصی از شبکه دسترسی داشته باشند یا از ورود ترافیک‌های غیرمجاز و تهدیدات احتمالی جلوگیری شود. این ابزار در بهبود امنیت شبکه و بهینه‌سازی ترافیک نقش کلیدی دارد و به دو نوع اصلی تقسیم می‌شود: استاندارد (Standard) و توسعه‌یافته (Extended)، که هر کدام ویژگی‌ها و کاربردهای خاص خود را دارند.

سناریو :

توپولوژی زیر مفروض است :



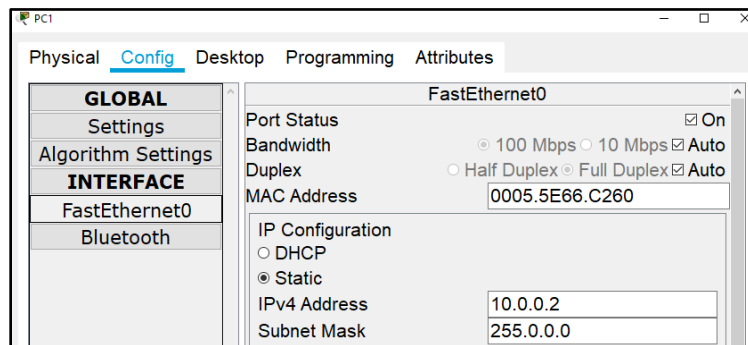
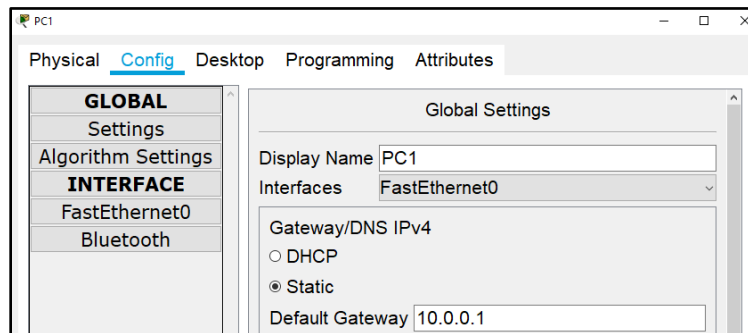
با استفاده از access list اجازه دسترسی سیستم 10.0.0.4 را به سرویس دهنده قطع نمایید.





دستور کار :

در مرحله اول پورت های سخت افزاری را مشخص کرده و آدرس های IP را در مسیریاب ها وارد می کنیم :



این کار را برای دو سیستم دیگر با ip های نوشته شده تکرار کنید ، مرحله بعدی تنظیم مسیریاب است :

```
Router>en
Router#conf t
Enter configuration commands, one per line. End
with CNTL/Z.
Router(config)#int
Router(config)#interface fast0/0
Router(config-if)#ip address 10.0.0.1 255.0.0.0
Router(config-if)#no shut
```

```
Router(config)#int fast0/1
Router(config-if)#ip address 20.0.0.1 255.0.0.0
Router(config-if)#no shut
```





آخرین مرحله هم تنظیمات سرویس دهنده است:

Server0

Physical **Config** Services Desktop Programming Attributes

GLOBAL

Settings

Algorithm Settings

INTERFACE

FastEthernet0

Global Settings

Display Name Server0

Gateway/DNS IPv4

☐ DHCP

☒ Static

Default Gateway 20.0.0.1

Server0

Physical **Config** Services Desktop Programming Attributes

GLOBAL

Settings

Algorithm Settings

INTERFACE

FastEthernet0

FastEthernet0

Port Status ☒ On

Bandwidth ☒ 100 Mbps ☐ 10 Mbps ☒ Auto

Duplex ☐ Half Duplex ☒ Full Duplex ☒ Auto

MAC Address 0001.428C.5236

IP Configuration

☐ DHCP

☒ Static

IPv4 Address 20.0.0.2

Subnet Mask 255.0.0.0

با این تنظیمات همه سیستم ها باید بتوانند سرویس دهنده را ping کنند ، مثلا در PC2 خواهیم داشت :

PC2

Physical Config **Desktop** Programming Attributes

Command Prompt

```
C:\>ping 20.0.0.2

Pinging 20.0.0.2 with 32 bytes of data:

Reply from 20.0.0.2: bytes=32 time<1ms TTL=127
Reply from 20.0.0.2: bytes=32 time<1ms TTL=127
```





برای قطع دسترسی سیستم 10.0.0.4 در مسیریاب :

```
Router(config)#ip access-list standard test
Router(config-std-nacl)#permit 10.0.0.1
Router(config-std-nacl)#permit 10.0.0.2
Router(config-std-nacl)#permit 10.0.0.3
Router(config-std-nacl)#deny 10.0.0.4
Router(config-std-nacl)#end
```

```
Router(config)#int fast0/1
Router(config-if)#ip acc
Router(config-if)#ip access-group test out
```

پس از اعمال این access list همه سیستم ها بجز 10.0.0.4 باید بتوانند سرویس دهنده را ping نمایند:

```
PC0
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 20.0.0.2

Pinging 20.0.0.2 with 32 bytes of data:

Reply from 20.0.0.2: bytes=32 time<1ms TTL=127
Reply from 20.0.0.2: bytes=32 time<1ms TTL=127
```

```
PC1
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 20.0.0.2

Pinging 20.0.0.2 with 32 bytes of data:

Reply from 20.0.0.2: bytes=32 time=2ms TTL=127
Reply from 20.0.0.2: bytes=32 time<1ms TTL=127
```

```
PC2
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 20.0.0.2

Pinging 20.0.0.2 with 32 bytes of data:

Reply from 10.0.0.1: Destination host unreachable.
Reply from 10.0.0.1: Destination host unreachable.
```

برای دریافت فایل شبیه سازی شده از آدرس زیر استفاده نمایید :

<https://github.com/serajcomputerarts/ciscolabs.git>

