

باسمه تعالی

گزارش مربوط به پروژه GNS3

درس:

شبکه‌های کامپیوتری پیشرفته

استاد:

دکتر خرسندی

میشم ملکی : ۹۰۱۳۱۰۲۴

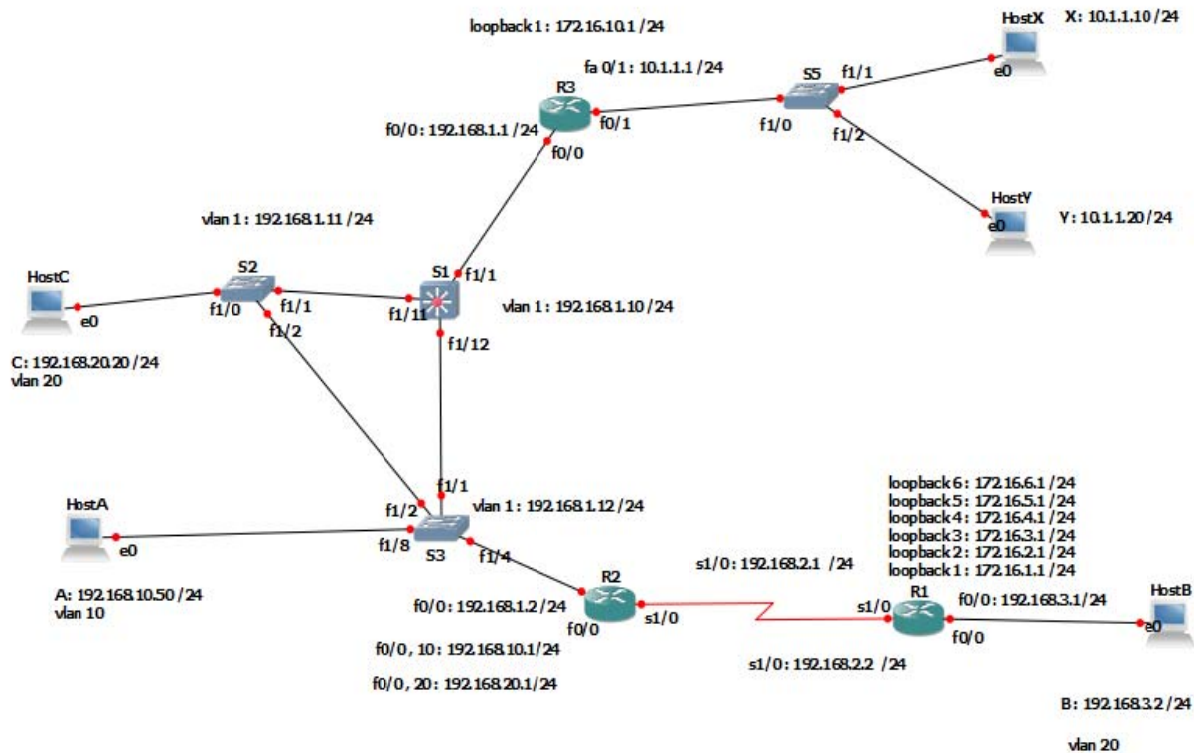
وحید ذوالفقاری: ۹۰۱۳۱۰۲۰

نیمسال اول: ۹۱-۹۰

۱. توپولوژی فوق پیاده شده و آدرسهای IP بر اساس شکل پیکربندی شوند.

توپولوژی اولیه بدین شکل ایجاد شد که مشاهده می نمایید . در شبیه سازی ما فقط از روتر مدل ۳۶۶۰ و از IOS، C3660-is-mz.122-8.T5 استفاده شده است که برای تبدیل روتر ها به سویچ اسلات NM-16ESW بکار گرفته شده است.

برای پیاده سازی Host ها از نرم افزار virtual Box استفاده شده است ، البته برای استفاده از این نرم افزار باید نسخه ی GNS3-0.8.1-VirtualBox-Edition استفاده گردد. در نرم افزار virtual box از hiren live CD استفاده شده است که نسخه ی کوچک شده ای از ویندوز XP را بر روی هر میزبان اجرا می کند.



تنظیمات مربوط به host ها و اختصاص آدرسهای IP به آنها درون خود host ها انجام شده است (هر host یک ماشین مجازی و دارای سیستم عامل ویندوز XP است).

ولی تنظیمات مربوط به سوئیچ‌ها و روترها، یعنی اختصاص آدرس IP به آن‌ها با استفاده از دستورات زیر انجام شده است.

سوئیچ S1:

Enable

Configure terminal

Host name S1

int vlan 1

ip address 192.168.1.10 255.255.255.0

no shutdown

سوئیچ S2:

Enable

Configure terminal

Host name S1

int vlan 1

ip address 192.168.1.11 255.255.255.0

no shutdown

سوئیچ S3:

Enable

Configure terminal

Host name S1

int vlan 1

ip address 192.168.1.11 255.255.255.0

no shutdown

روتر R1 :

Enable

configure terminal

hostname R1

interface fastEthernet0/0

ip add 192.168.3.1 255.255.255.0

no shutdown

Interface serial 0/0

ip add 192.168.2.2 255.255.255.0

no shutdown

روتر R2 :

Enable

configure terminal

hostname R2

interface fastEthernet0/0

ip add 192.168.1.2 255.255.255.0

no shutdown

Interface serial 0/0

```
ip add 192.168.2.1 255.255.255.0
```

```
no shutdown
```

روتر R3 :

Enable

```
configure terminal
```

```
hostname R2
```

```
interface fastEthernet0/0
```

```
ip add 192.168.1.1 255.255.255.0
```

```
no shutdown
```

```
Interface fastEthernet0/1
```

```
ip add 10.1.1.1 255.255.255.0
```

```
no shutdown
```

نمونه‌ای از دستورات وارد شده در روتر R1 در زیر آورده شده است.

```
Router#
Router#
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1
R1(config)#
R1(config)#int fa0/0
R1(config-if)#
R1(config-if)#ip address 192.168.3.1 255.255.255.0
R1(config-if)#
R1(config-if)#no shut
R1(config-if)#
R1(config-if)#
R1(config-if)#
R1(config-if)#
00:01:45: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
00:01:46: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
```

تذکره ۱: Default Gateway برای host های A,B روتر R2 و به ترتیب با آدرس های IP، ۱۹۲.۱۶۸.۱۰.۱ و ۱۹۲.۱۶۸.۲۰.۱ منظور شده است. و برای host C روتر R3 ، با آدرس IP ۱۹۲.۱۶۸.۳۰.۱ انتخاب شده است.

تذکره ۲: تنظیمات مربوط Vlan ها و آدرس های IP ، loopback در روترها در ادامه و در سوال های بعدی توضیح داده شده است.

(۲) Host A در VLAN 10 و Host B در VLAN 20 تعریف شوند. برای VLAN 10 سوئیچ S1 و برای VLAN 20 سوئیچ S2 به عنوان Root Bridge انتخاب شوند. Rapid STP بر روی سوئیچهای S1, S2, S3 به صورت Per VLAN پیکربندی شود. از مدل Router as a stick برای برقراری ارتباط مابین VLAN ها استفاده شود بنحوی که Host A و Host B باید از طریق روتر R2 با یکدیگر ارتباط برقرار کنند.

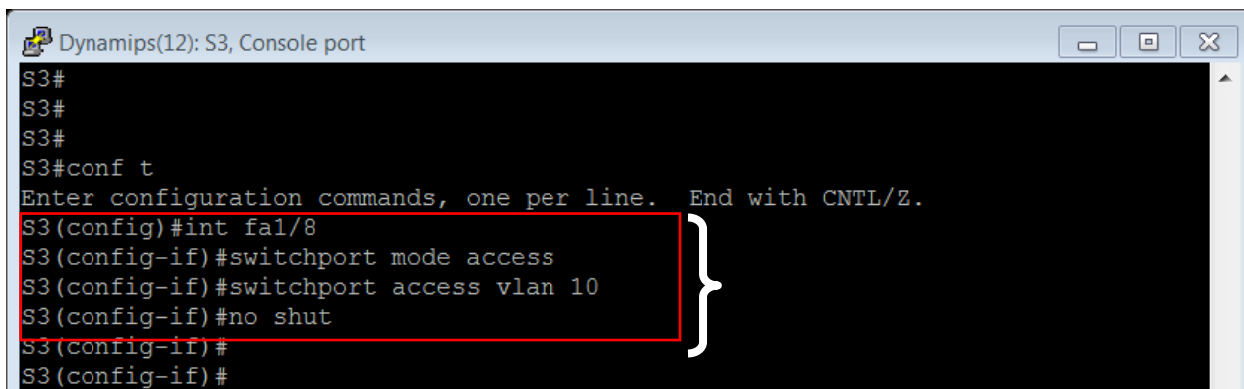
host های A و C در حالت عادی بدون تنظیمات یکدیگر را نمی بینند. برای اینکه میزبانها در Vlan های مختلف بتوانند یکدیگر را ببینند باید یک روتر بین آنها بعنوان Router as a stick عمل کند. البته چون حلقه در توپولوژی ما وجود دارد باید spanning-tree را برای هر Vlan اجرا کنیم. مراحل کار از این قرار است :

۱- ابتدا باید Vlan 10 و Vlan 20 را بر روی vlan database همه ی سوئیچهای ۱ و ۲ و ۳ تعریف کنیم. بعنوان نمونه دستورات لازم برای اینکار که بر روی S1 انجام شده است آورده شده است: البته می توان به کمک پروتکل VTP یا Virtual Trunking Protocol ، Vlan database یک سوئیچ را تغییر داد و بقیه را بگونه ای تنظیم کرد که تغییرات Vlan database را از vtp server دریافت کنند.

```
Dynamips(10): S1, Console port
S1#
S1#vlan da
S1#vlan database
S1(vlan)#vlan 10
VLAN 10 added:
    Name: VLAN0010
S1(vlan)#vlan 20
VLAN 20 added:
    Name: VLAN0020
S1(vlan)#app
S1(vlan)#apply
APPLY completed.
S1(vlan)#exit
APPLY completed.
Exiting....
S1#
```

۲- یک لینک را با کمک دستورات زیر به vlan مورد نظر اختصاص می دهیم :

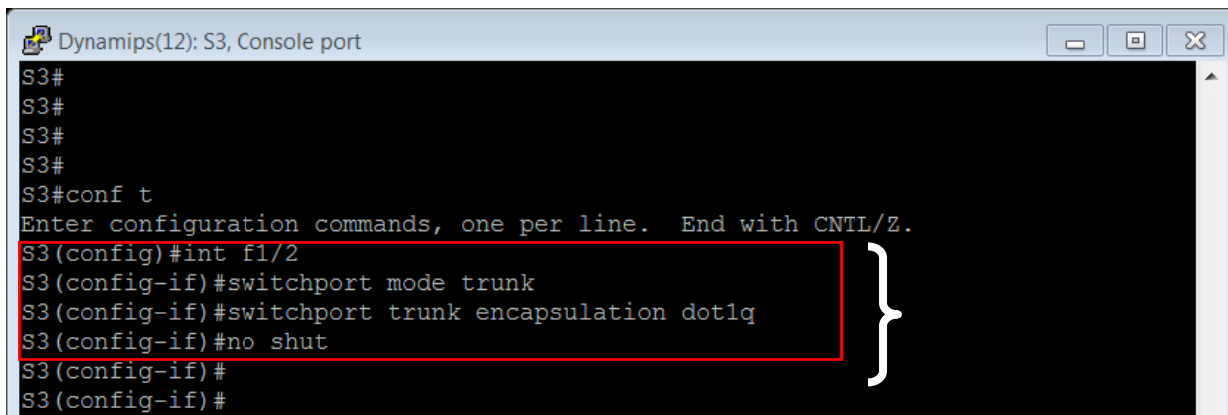
access mode :



```
Dynamips(12): S3, Console port
S3#
S3#
S3#
S3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#int fa1/8
S3(config-if)#switchport mode access
S3(config-if)#switchport access vlan 10
S3(config-if)#no shut
S3(config-if)#
S3(config-if)#
```

The screenshot shows a terminal window titled "Dynamips(12): S3, Console port". The user enters the command "conf t" to enter configuration mode. Then, they enter "int fa1/8" to select the interface. Finally, they enter "switchport mode access" and "switchport access vlan 10" to configure the port as an access port for VLAN 10. The command "no shut" is also entered. A red box highlights the last three commands, and a white bracket on the right indicates they are grouped together.

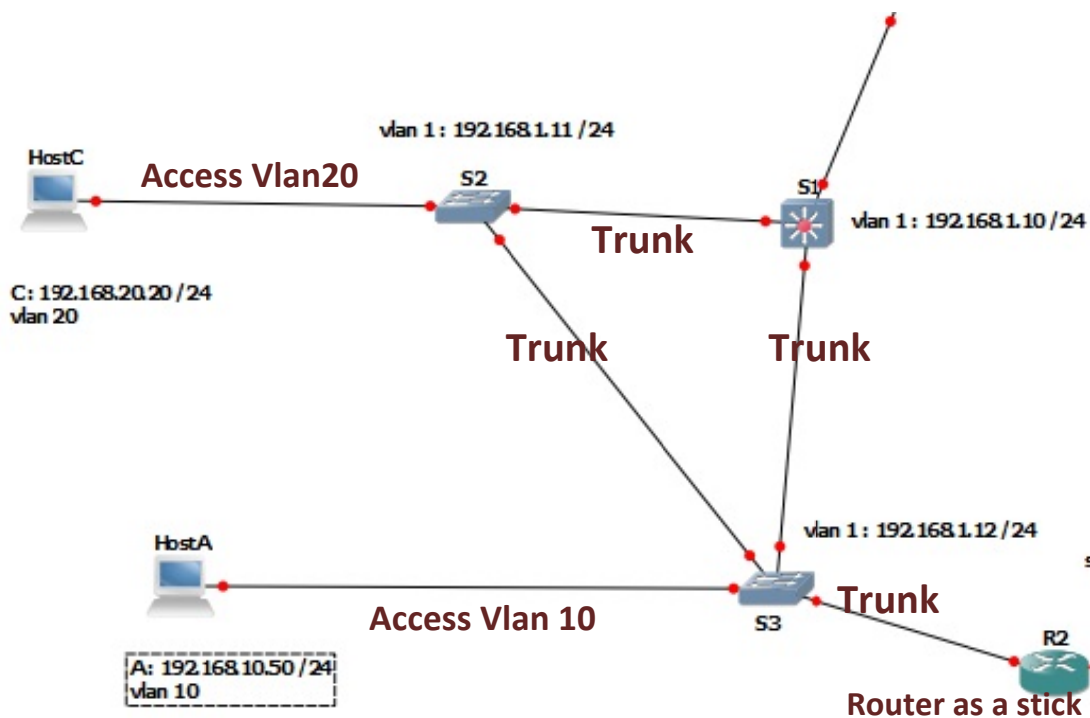
Trunk mode :



```
Dynamips(12): S3, Console port
S3#
S3#
S3#
S3#
S3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#int f1/2
S3(config-if)#switchport mode trunk
S3(config-if)#switchport trunk encapsulation dot1q
S3(config-if)#no shut
S3(config-if)#
S3(config-if)#
```

The screenshot shows a terminal window titled "Dynamips(12): S3, Console port". The user enters the command "conf t" to enter configuration mode. Then, they enter "int f1/2" to select the interface. Finally, they enter "switchport mode trunk", "switchport trunk encapsulation dot1q", and "no shut" to configure the port as a trunk port. A red box highlights the last three commands, and a white bracket on the right indicates they are grouped together.

لینکهای access و trunk را بر اساس شکل زیر تعیین می کنیم . نکته مهم این است که برای تعریف پورتهای trunk، باید پورتهای سویچهای دو سر لینک هردویشان trunk شوند.



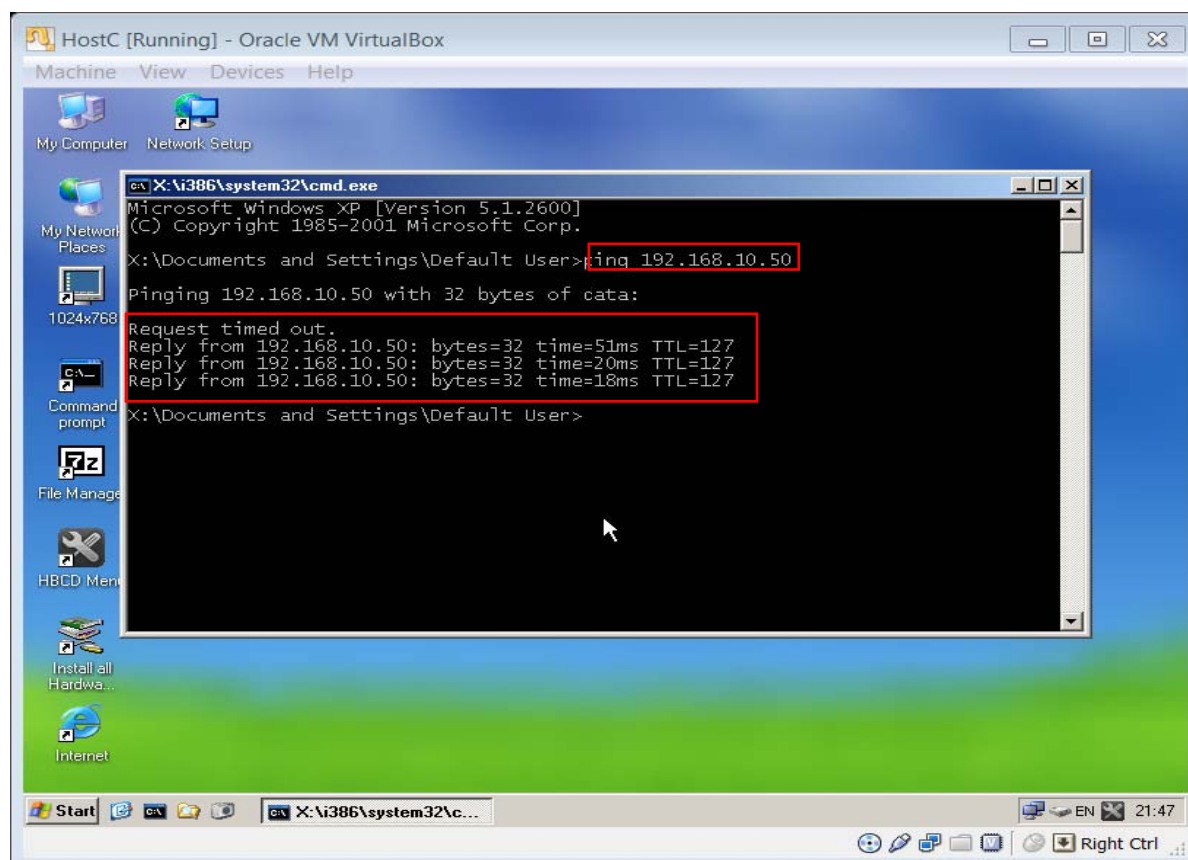
۳- در این مرحله برای هر Vlan باید spanning-tree را Run کرده و یک root bridge انتخاب نماییم. بنا به گفته ی سوال برای Vlan 10 سویچ S1 و برای Vlan 20 سویچ S2 بعنوان root bridge ست می شوند. بعنوان نمونه تنظیمات اینکار بر روی سویچ S2 به این شکل است :

```
S2(config)#
S2(config)#spanning-tree vlan 20 root primary
VLAN 20 bridge priority set to 8192
VLAN 20 bridge max aging time unchanged at 20
VLAN 20 bridge hello time unchanged at 2
VLAN 20 bridge forward delay unchanged at 15
```


۴- در این مرحله از مدل Router as a stick برای برقراری ارتباط مابین VLAN ها استفاده می شود بدینصورت که بر روی پورت fa 0/0 از روتر R2 باید به تعداد Vlan ها (۱۰ و ۲۰) subinterface ایجاد می کنیم. آدرس IP این subinterface ها همان default gateway هاست های A و C (یعنی ۱۹۲.۱۶۸.۱۰.۱ و ۱۹۲.۱۶۸.۲۰.۱) می باشند. دستورات لازم برای پیاده سازی آن بر روی روتر R2 از این قرار است :

```
R2(config)#int f0/0
R2(config-if)#int f0/0.10
R2(config-subif)#encapsulation dot1q 10
R2(config-subif)#ip add
R2(config-subif)#ip address 192.168.10.1 255.255.255.0
R2(config-subif)#no shut
R2(config-subif)#
R2(config-subif)#
```

حال با انجام این تنظیمات هاست A و هاست C که در دو Vlan متفاوت قرار دارند می توانند یکدیگر را ببینند. همانطور که در شکل زیر نشان داده شده است host c ، host A را با آدرس IP ، ۱۹۲.۱۶۸.۱۰.۵۰ با موفقیت ping کرده است.



نکته ۱: هنگام تعریف Vlan های ۱۰،۲۰ بر روی سوئیچ ها، سوئیچ S2 خطای پر شدن Flash سوئیچ و ناتوانی آن در ذخیره تغییرات را می داد که با دستور زیر این خطا رفع شد:

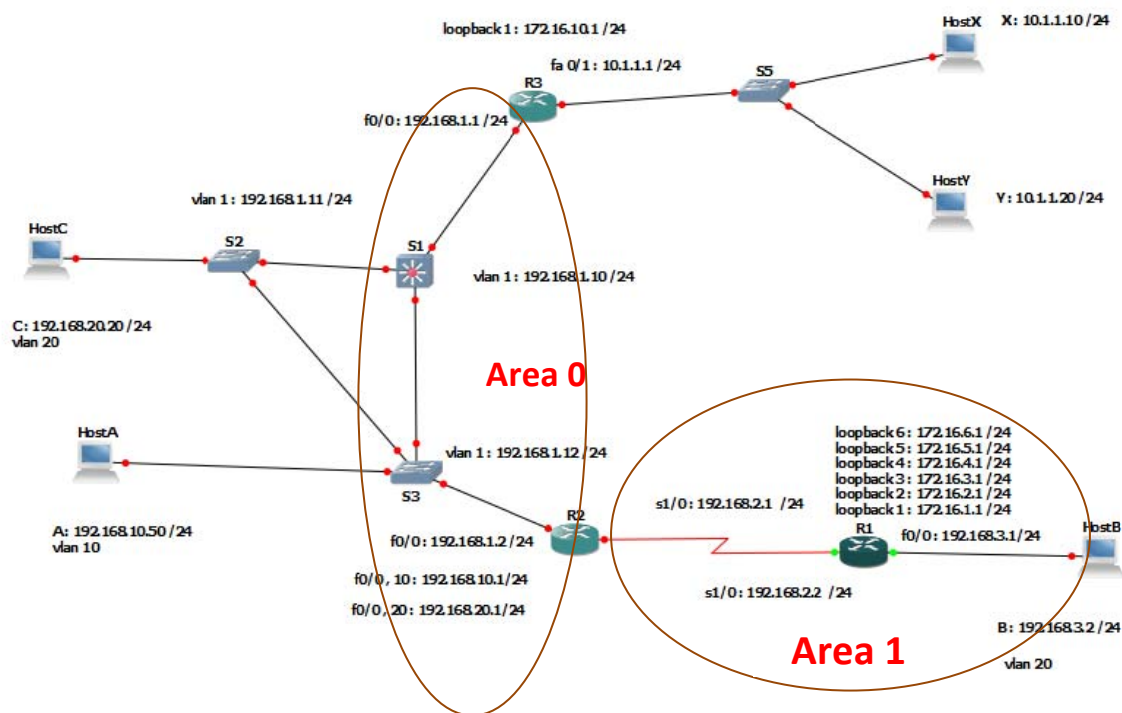
S2# erase flash

نکته ۲: در سوال آورده شده است که می بایست Rapid STP اجرا شود اما بدلیل اینکه ما از اسلات روتر بجای سوئیچ استفاده کرده ایم این دستور بر روی روترها در GNS3 قابل اجرا نیست. بهر حال شکل کلی دستور Rapid STP به این صورت است:

S2(config) # spanning-tree mode rapid-pvst

۳) پروتکل مسیریابی OSPF در روترهای R1, R2 و R3 پیکربندی شود. R2 به عنوان ABR تعریف شود به نحوی که اینترفیس fa0/0 آن در Area 0 و S0/0 در Area 1 تعریف شود. کلیه اینترفیس های روترها بجز اینترفیس f0/1 روتر R3 در OSPF تعریف شوند. با توجه به اینکه در OSPF تنها روترهای ABR توانایی Address Summarization را دارند، در روتر R2 باید auto summary غیرفعال شده و آدرسها به بهترین حالت Summarize شوند.

با توجه به صورت سوال، شکل کلی شبکه با توجه به تعریف پروتکل OSPF و ناحیه های مذکور به شکل زیر می باشد



شکل کلی دستور قرار دادن شبکه ها در OSPF بدین صورت است :

```
R2(config)# router ospf (process ID)
```

```
R2(config-router)#network (Ip address)(wild card mask) area (Area ID)
```

Area ID : یک شبکه‌ی OSPF را می‌توان به زیر دامنه‌هایی تقسیم کرد که Area نامیده می‌شود. یک Area مجموعه‌ای منطقی از شبکه‌های OSPF، روترها و لینک‌هایی است که Area ID یکسانی دارند. یک روتر در Area باید database ای از توپولوژی Area ای که در آن قرار دارد را نگهداری می‌کند. روتر اطلاعات جزئی از توپولوژی‌های بیرون از Area خود را ندارد که باعث کاهش اندازه‌ی Database آن می‌شود. روترهایی که در یک Area قرار دارند باید یک Area ID داشته باشند.

Process ID : روترهای سیستم می‌توانند چندین پروسه‌ی OSPF اجرا کنند و Process ID صرفاً بین این پروسه‌ها تمایز ایجاد می‌کند. Process ID بصورت محلی در خود روتر تعریف می‌شود و دو روتر همسایه OSPF می‌توانند Process ID های متفاوتی داشته باشند ولی برای اینکه در یک Area قرار گیرند می‌بایست یک Area ID داشته باشند.

IP Address : در این قسمت باید آدرس شبکه‌ای را که می‌خواهیم در OSPF قرار دهیم را وارد می‌کنیم.

wild card mask : Subnet mask در OSPF ، هنگام انجام تنظیمات، با فرمت Wild Card وارد می‌شود. در این فرمت در subnet mask جای صفر و یک را باهم عوض می‌کنیم به عنوان نمونه در پروژه تعریف شده تمامی subnet mask ها به صورت ۲۵۵.۲۵۵.۲۵۵.۰ هستند، در فرمت Wild Card به صورت ۰.۰.۰.۲۵۵ می‌باشند.

هر روتر در OSPF یک Router ID دارد که بطور پیش فرض همان مقدار بزرگترین IP اینترفیس هایش است، که این امر مشکلاتی را به همراه دارد مثلاً چون با هر تغییر IP هر کدام از اینترفیس ها باید دوباره بزرگترین آدرس IP، پیدا و بعنوان router ID ست شود. همچنین ممکن است آدرس IP پورته انتخاب شود که یک flapping port باشد. flapping port به پورته اطلاق می‌شود که مرتباً up و down می‌شود. که اینکار موجب می‌شود با اجرای OSPF حتی ممکن است شبکه down شود.

برای رفع این مشکل بر روی هر روتر در OSPF یک loopback interface با یک آدرس IP مشخص ایجاد می کنیم تا آدرس این پورت بعنوان Router ID انتخاب شود. دلیل این انتخاب هم این است که loopback interface یک پورت مجازی است و همیشه up است .

مثلاً برای ایجاد loopback interface 1 دستورات زیر باید وارد گردد :

```
R2(config)# interface loopback 1
```

```
R2(config-int)# ip address 172.16.1.1 255.255.255.0
```

```
R2(config-int)# no shut
```

به عنوان نمونه دستورات انجام شده بر روی روتر R2 که بعنوان ABR انتخاب شده است آورده می شود.

```
R2#
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router ospf 1
R2(config-router)#network 192.168.1.0 0.0.0.255 area 0
R2(config-router)#network 192.168.2.0 0.0.0.255 area 1
R2(config-router)#
R2(config-router)#
```

پس از اجرای این دستورات، پروتکل OSPF بر روی روترها اجرا می شود که در ادامه مشخصات این پروتکل را که با دستور **show ip OSP** به دست آمده را بر روی همه روترها می بینیم .

روتر R1:

```
Dynamips(4): R1, Console port
R1#sho ip ospf
Routing Process "ospf 1" with ID 172.16.6.1
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msec
Retransmission pacing timer 66 msec
Number of external LSA 0. Checksum Sum 0x0
Number of opaque AS LSA 0. Checksum Sum 0x0
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
External flood list length 0
  Area 1
    Number of interfaces in this area is 7
    Area has no authentication
    SPF algorithm executed 1 times
    Area ranges are
    Number of LSA 1. Checksum Sum 0xEA65
    Number of opaque link LSA 0. Checksum Sum 0x0
    Number of DCbitless LSA 0
    Number of indication LSA 0
--More--
00:00:34: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, changed sta
t
  Number of DoNotAge LSA 0
  Flood list length 0
R1#
```

روتر R2:

```
Dynamips(0): R2, Console port
Supports only single TOS(TOS0) routes
Supports opaque LSA
It is an area border router
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msec
Retransmission pacing timer 66 msec
Number of external LSA 0. Checksum Sum 0x0
Number of opaque AS LSA 0. Checksum Sum 0x0
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 2. 2 normal 0 stub 0 nssa
External flood list length 0
  Area BACKBONE(0) (Inactive)
    Number of interfaces in this area is 1
    Area has no authentication
    SPF algorithm executed 2 times
    Area ranges are
    Number of LSA 2. Checksum Sum 0xFFDC
    Number of opaque link LSA 0. Checksum Sum 0x0
    Number of DCbitless LSA 0
    Number of indication LSA 0
    Number of DoNotAge LSA 0
    Flood list length 0
  Area 1
    Number of interfaces in this area is 1
    Area has no authentication
    SPF algorithm executed 2 times
    Area ranges are
    Number of LSA 2. Checksum Sum 0x10DCE
    Number of opaque link LSA 0. Checksum Sum 0x0
    Number of DCbitless LSA 0
    Number of indication LSA 0
    Number of DoNotAge LSA 0
    Flood list length 0
R2#
```

روتر R3:

```
Dynamips(5): R3, Console port
R3#
R3#sho ip ospf
Routing Process "ospf 1" with ID 172.16.10.1
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msecs
Retransmission pacing timer 66 msecs
Number of external LSA 0. Checksum Sum 0x0
Number of opaque AS LSA 0. Checksum Sum 0x0
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
External flood list length 0
Area BACKBONE (0)
Number of interfaces in this area is 2
Area has no authentication
SPF algorithm executed 4 times
Area ranges are
Number of LSA 4. Checksum Sum 0x1E667
Number of opaque link LSA 0. Checksum Sum 0x0
Number of DCbitless LSA 0
Number of indication LSA 0
Number of DoNotAge LSA 0
Flood list length 0
R3#
```

در ادامه با دستور **show ip route** بر روی هر روتر، شبکه‌هایی که هر روتر می‌شناسد را نشان می‌دهیم. آنهایی که با 0 شروع می‌شوند آدرس شبکه‌های دیگری است که از طریق پروتکل OSPF یادگرفته شده‌اند. همانطور که می‌بینیم روترها، همه شبکه‌های دیگری را که وجود دارند را می‌شناسند.

روتر R1:

```
Dynamips(4): R1, Console port
R1#
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

O IA 192.168.10.0/24 [110/65] via 192.168.2.1, 00:06:40, Serial1/0
    172.16.0.0/16 is variably subnetted, 7 subnets, 2 masks
O IA 172.16.10.1/32 [110/66] via 192.168.2.1, 00:06:40, Serial1/0
C    172.16.4.0/24 is directly connected, Loopback4
C    172.16.5.0/24 is directly connected, Loopback5
C    172.16.6.0/24 is directly connected, Loopback6
C    172.16.1.0/24 is directly connected, Loopback1
C    172.16.2.0/24 is directly connected, Loopback2
C    172.16.3.0/24 is directly connected, Loopback3
O IA 192.168.20.0/24 [110/65] via 192.168.2.1, 00:06:42, Serial1/0
O IA 192.168.1.0/24 [110/65] via 192.168.2.1, 00:06:42, Serial1/0
C    192.168.2.0/24 is directly connected, Serial1/0
C    192.168.3.0/24 is directly connected, FastEthernet0/0
R1#
```

روتر R2:

```
Dynamips(0): R2, Console port
R2#
R2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.10.0/24 is directly connected, FastEthernet0/0.10
    172.16.0.0/32 is subnetted, 7 subnets
O    172.16.10.1 [110/2] via 192.168.1.1, 00:06:36, FastEthernet0/0
O    172.16.5.1 [110/65] via 192.168.2.2, 00:01:39, Serial1/0
O    172.16.4.1 [110/65] via 192.168.2.2, 00:01:39, Serial1/0
O    172.16.6.1 [110/65] via 192.168.2.2, 00:01:39, Serial1/0
O    172.16.1.1 [110/65] via 192.168.2.2, 00:01:39, Serial1/0
O    172.16.3.1 [110/65] via 192.168.2.2, 00:01:39, Serial1/0
O    172.16.2.1 [110/65] via 192.168.2.2, 00:01:41, Serial1/0
C    192.168.20.0/24 is directly connected, FastEthernet0/0.20
C    192.168.1.0/24 is directly connected, FastEthernet0/0
C    192.168.2.0/24 is directly connected, Serial1/0
O    192.168.3.0/24 [110/65] via 192.168.2.2, 00:01:41, Serial1/0
R2#
```


روتر R3 :

```
Dynamips(5): R3, Console port
R3#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

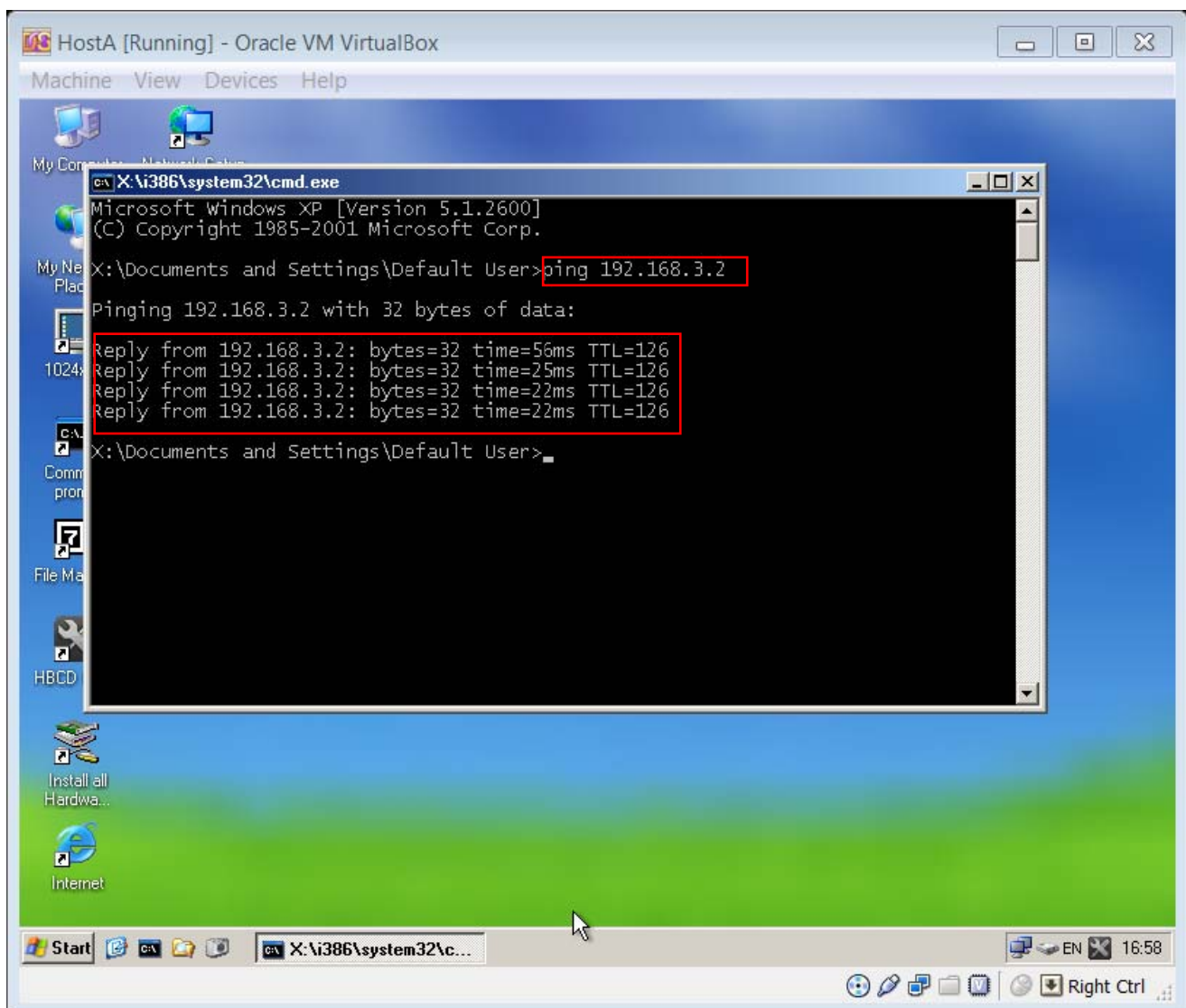
Gateway of last resort is not set

O   192.168.10.0/24 [110/2] via 192.168.1.2, 00:14:58, FastEthernet0/0
    172.16.0.0/16 is variably subnetted, 7 subnets, 2 masks
C   172.16.10.0/24 is directly connected, Loopback1
O IA 172.16.5.1/32 [110/66] via 192.168.1.2, 00:10:01, FastEthernet0/0
O IA 172.16.4.1/32 [110/66] via 192.168.1.2, 00:10:01, FastEthernet0/0
O IA 172.16.6.1/32 [110/66] via 192.168.1.2, 00:10:01, FastEthernet0/0
O IA 172.16.1.1/32 [110/66] via 192.168.1.2, 00:10:01, FastEthernet0/0
O IA 172.16.3.1/32 [110/66] via 192.168.1.2, 00:10:03, FastEthernet0/0
O IA 172.16.2.1/32 [110/66] via 192.168.1.2, 00:10:03, FastEthernet0/0
O   192.168.20.0/24 [110/2] via 192.168.1.2, 00:15:00, FastEthernet0/0
    10.0.0.0/24 is subnetted, 1 subnets
C   10.1.1.0 is directly connected, FastEthernet0/1
C   192.168.1.0/24 is directly connected, FastEthernet0/0
O IA 192.168.2.0/24 [110/65] via 192.168.1.2, 00:15:04, FastEthernet0/0
O IA 192.168.3.0/24 [110/66] via 192.168.1.2, 00:10:06, FastEthernet0/0
R3#
```

با اجرای پروتکل OSPF بر روی شبکه، دیگر تمامی روترها آدرس های IP شبکه های دیگر را در جدول مسیریابی خود وارد کرده و می توانند یکدیگر را ping کنند. که در ادامه جداول مسیریابی همه روترها آورده شده است.

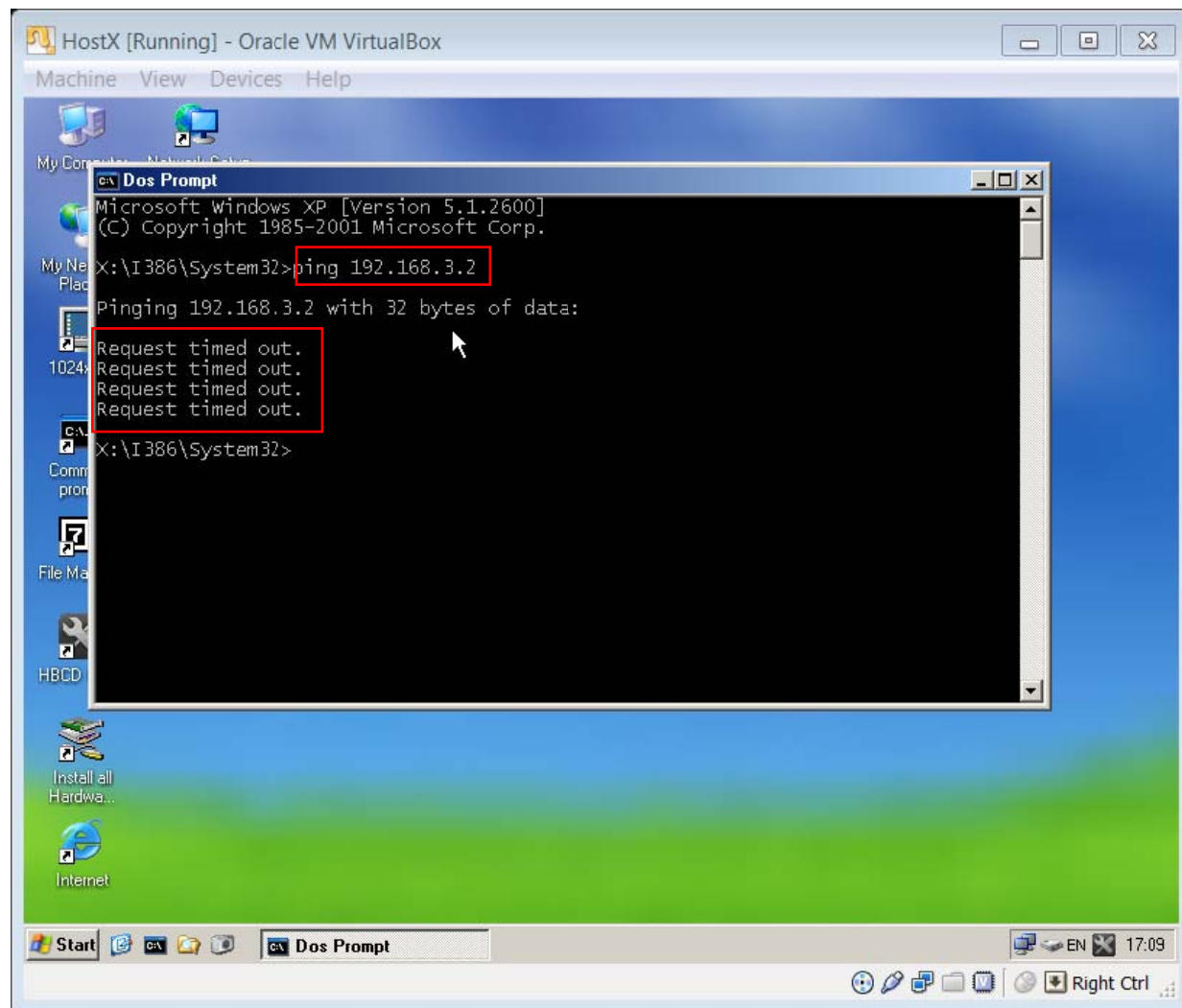
حال با توجه به مستندات ارائه شده دیدیم که پروتکل OSPF به درستی بر روی روترها در حال اجراست : در انتها نیز بعنوان نمونه تست زیر را انجام می دهیم که در آن Host A با Host B ارتباط برقرار می کند.

: HostB ping Host A



یکی از نکاتی که در صورت سوال قید شده بود این موضوع بود که پورت f0/1 روتر R3 در OSPF تعریف نگردد، تاثیر این موضوع را در شکل زیر می بینیم که Host X که Gateway آن همین پورت است، نتوانسته است Host B را ping کند.

: Host B ping Host X



قسمت آخر سوال مربوط به OSPF Summarization است. این کار بدین معنی است که آدرس های مربوط به چند شبکه با IP های شبیه به هم در داخل یک area را summarize کنیم تا هنگامیکه از طریق ABR بسته های OSPF Update به Area های دیگر ارسال می شود اطلاعات تک تک آن شبکه های شبیه به هم ارسال نشود بلکه آنها را summarize کرده و IP address ای که نماینده ی همه ی آنهاست advertise شود.

در مثال داده شده شبکه های ۱۷۲.۱۶.۱.۰ و ۱۷۲.۱۶.۲.۰ و ۱۷۲.۱۶.۳.۰ و ۱۷۲.۱۶.۴.۰ و ۱۷۲.۱۶.۵.۰ و ۱۷۲.۱۶.۶.۰ را می توان بصورت شبکه ی ۲۵۵.۲۵۵.۲۴۸.۰ ۱۷۲.۱۶.۰.۰ نشان داد. تنظیمات مربوط به summarization تنها بر روی روترهای لبه (ABR) قابل انجام است.

نتیجه ی دستور show ip route بر روی روتر R3 که در Area 1 قرار دارد قبل از اینکه summarization انجام شود آورده شده است .

```
Dynamips(5): R3, Console port
R3#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

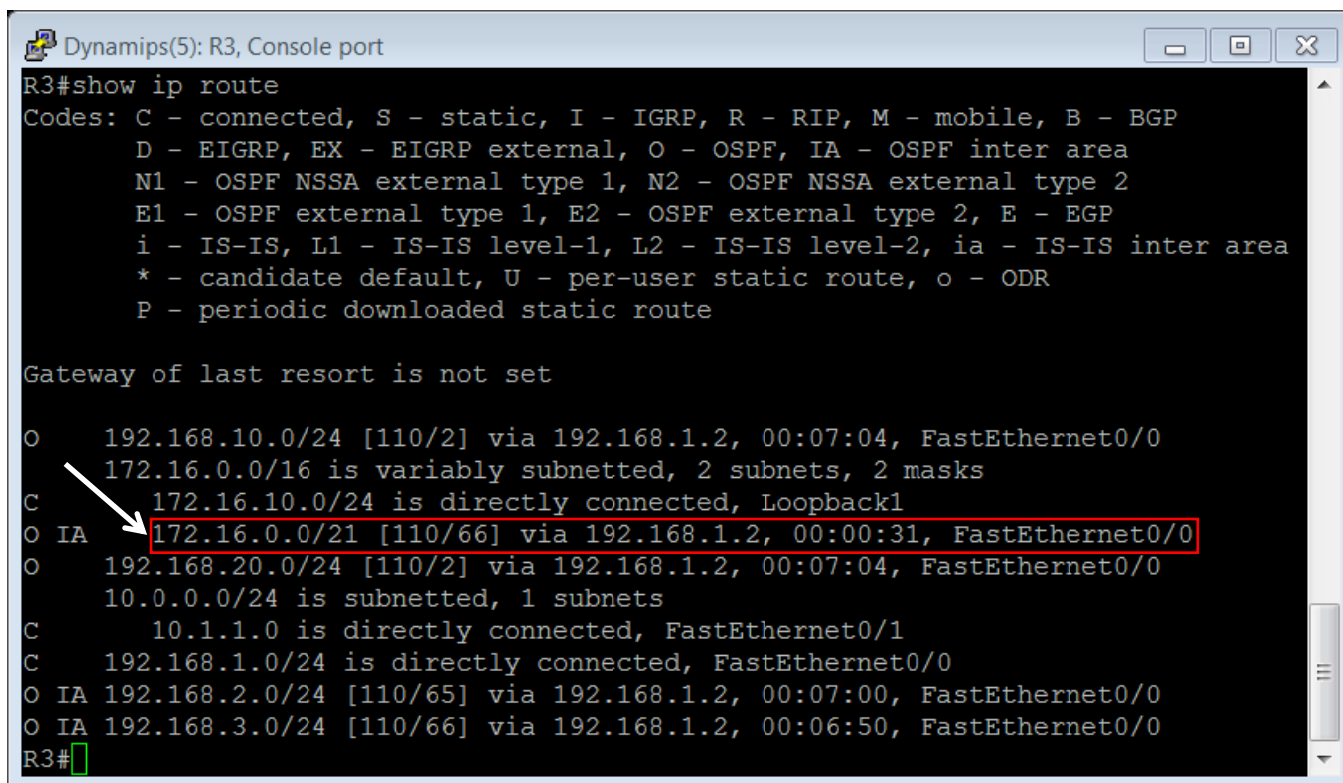
Gateway of last resort is not set

O    192.168.10.0/24 [110/2] via 192.168.1.2, 00:04:37, FastEthernet0/0
    172.16.0.0/16 is variably subnetted, 7 subnets, 2 masks
C     172.16.10.0/24 is directly connected, Loopback1
O IA   172.16.5.1/32 [110/66] via 192.168.1.2, 00:04:22, FastEthernet0/0
O IA   172.16.4.1/32 [110/66] via 192.168.1.2, 00:04:22, FastEthernet0/0
O IA   172.16.6.1/32 [110/66] via 192.168.1.2, 00:04:22, FastEthernet0/0
O IA   172.16.1.1/32 [110/66] via 192.168.1.2, 00:04:22, FastEthernet0/0
O IA   172.16.3.1/32 [110/66] via 192.168.1.2, 00:04:23, FastEthernet0/0
O IA   172.16.2.1/32 [110/66] via 192.168.1.2, 00:04:23, FastEthernet0/0
O     192.168.20.0/24 [110/2] via 192.168.1.2, 00:04:38, FastEthernet0/0
    10.0.0.0/24 is subnetted, 1 subnets
C     10.1.1.0 is directly connected, FastEthernet0/1
C     192.168.1.0/24 is directly connected, FastEthernet0/0
O IA  192.168.2.0/24 [110/65] via 192.168.1.2, 00:04:45, FastEthernet0/0
O IA  192.168.3.0/24 [110/66] via 192.168.1.2, 00:04:35, FastEthernet0/0
R3#
```

تنظیمات مربوط به اینکار بر روی روتر R2 در زیر نشان داده شده است :

```
R2>ena
R2#
R2#
R2#
R2#
R2#
R2#
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router ospf 1
R2(config-router)#area 1 range 172.16.0.0 255.255.248.0
R2(config-router)#
R2(config-router)#
```

بعد از انجام این تنظیمات نتیجه ی دستور `show ip route` در زیر آورده شده است که مشخصاً آدرسهای متعدد ۱۷۲.۱۶.۱۰ و غیره تنها به یک آدرس ۱۷۲.۱۶.۰.۰/۲۱ تبدیل شده است.



```
Dynamips(5): R3, Console port
R3#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

O    192.168.10.0/24 [110/2] via 192.168.1.2, 00:07:04, FastEthernet0/0
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C    172.16.10.0/24 is directly connected, Loopback1
O IA 172.16.0.0/21 [110/66] via 192.168.1.2, 00:00:31, FastEthernet0/0
O    192.168.20.0/24 [110/2] via 192.168.1.2, 00:07:04, FastEthernet0/0
     10.0.0.0/24 is subnetted, 1 subnets
C    10.1.1.0 is directly connected, FastEthernet0/1
C    192.168.1.0/24 is directly connected, FastEthernet0/0
O IA 192.168.2.0/24 [110/65] via 192.168.1.2, 00:07:00, FastEthernet0/0
O IA 192.168.3.0/24 [110/66] via 192.168.1.2, 00:06:50, FastEthernet0/0
R3#
```

OSPF Authentication مابین همسایه ها پیکربندی شود. پروتکل کپسوله سازی لینک سریال مابین R1 و R2 برابر PPP تعریف شده و PPP Authentication مابین دو سر لینک پیکربندی شود.

دو نوع OSPF Authentication داریم :

۱- Plain-text encryption

Plain-text Authentication وقتی استفاده می شود که device های داخل یک Area از الگوریتم تایید صلاحیت MD5 پشتیبانی نکنند. این روش شبکه را در برابر sniffer attack آسیب پذیر می کند. در این حمله بسته های رد و بدل شده بین device ها توسط یک آنالیز کننده پروتکل ضبط شده و رمز های عبور از داخل آن خوانده می شود.

۲- MD5 encryption

MD5 Authentication امنیت بالاتری را نسبت به Plain-text Authentication ارائه می دهد. این متد از الگوریتم MD5 برای محاسبه ی مقدار hash شده ی محتویات بسته های OSPF به همراه یک password (or key) استفاده می کند. این مقدار hash در داخل بسته قرار داده شده و به همراه یک key ID و شماره ترتیب صعودی ارسال می شود. گیرنده که همان password را می داند دوباره مقدار hash را محاسبه می کند. اگر در طول مسیر هیچ چیز در بسته تغییر نکند مقدار محاسبه شده باید با مقدار hash داخل بسته یکسان باشد.

بدلیل امنیت بالاتر و پشتیبانی شدن دستورات MD5 توسط IOS ما روش MD5 Authentication را انتخاب کرده ایم. با استفاده از دستورات زیر می توان OSPF Authentication را مابین همسایه ها پیکربندی نمود. برای اجرای این دستورات ابتدا باید وارد اینترفیس مورد نظر شده و دستور زیر را اعمال نمود:

```
ip ospf message-digest-key (key ID) md5 (password)
```

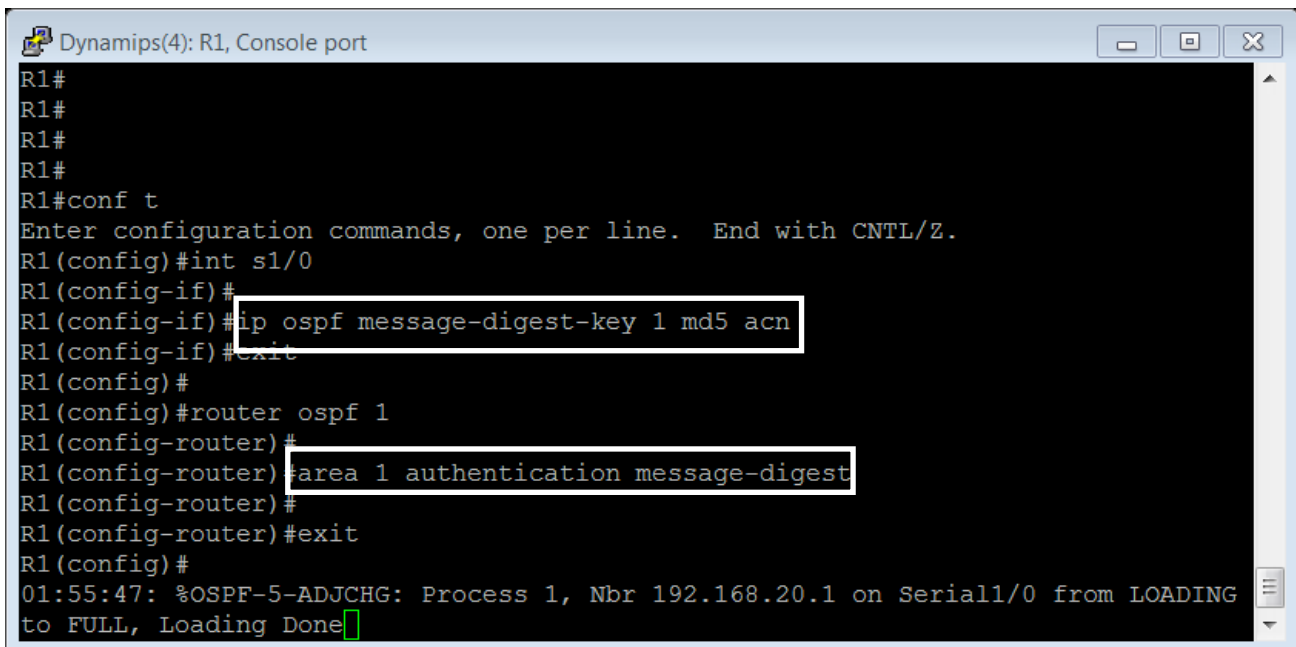
Key ID : در این قسمت ID مربوط به کلید را وارد می کنیم.

Password : در این قسمت password ای را که بین دو پورت همسایه برای hash کردن بسته های OSPF توافق می شود را وارد می کنیم. که در سوال داده شده مقدار این فیلد "acn" است.

سپس وارد تنظیمات مسیریابی OSPF می شویم و دستور زیر را وارد می کنیم.

```
area (Area ID) authentication message-digest
```

بعنوان نمونه دستوراتی که بر روی پورت سریال روتر R1 زده شده است آورده می شود.



```
Dynamips(4): R1, Console port
R1#
R1#
R1#
R1#
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int s1/0
R1(config-if)#
R1(config-if)#ip ospf message-digest-key 1 md5 acn
R1(config-if)#exit
R1(config)#
R1(config)#router ospf 1
R1(config-router)#
R1(config-router)#area 1 authentication message-digest
R1(config-router)#
R1(config-router)#exit
R1(config)#
01:55:47: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.20.1 on Serial1/0 from LOADING
to FULL, Loading Done
```

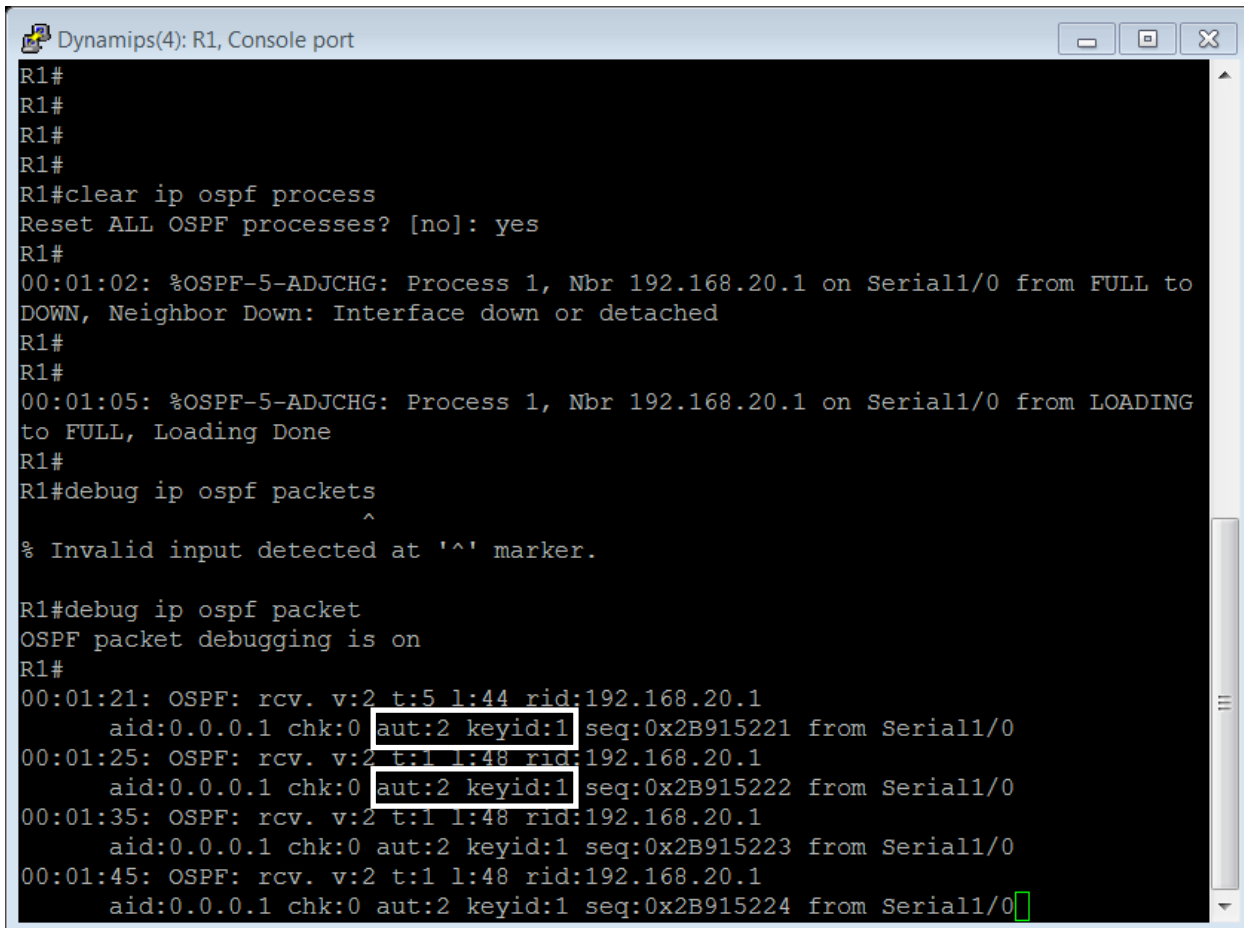
برای نشان دادن عملکرد درست MD5 Authentication به کمک دستور

```
R1#clear ipospf process
```

فرایند OSPF را بر روی این روتر restart می کنیم سپس به کمک دستور

```
R1#debugipospf packets
```

بسته های وارد شده به روتر را نشان می دهیم.



```
Dynamips(4): R1, Console port
R1#
R1#
R1#
R1#clear ip ospf process
Reset ALL OSPF processes? [no]: yes
R1#
00:01:02: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.20.1 on Serial1/0 from FULL to
DOWN, Neighbor Down: Interface down or detached
R1#
R1#
00:01:05: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.20.1 on Serial1/0 from LOADING
to FULL, Loading Done
R1#
R1#debug ip ospf packets
^
% Invalid input detected at '^' marker.

R1#debug ip ospf packet
OSPF packet debugging is on
R1#
00:01:21: OSPF: rcv. v:2 t:5 l:44 rid:192.168.20.1
aid:0.0.0.1 chk:0 aut:2 keyid:1 seq:0x2B915221 from Serial1/0
00:01:25: OSPF: rcv. v:2 t:1 l:48 rid:192.168.20.1
aid:0.0.0.1 chk:0 aut:2 keyid:1 seq:0x2B915222 from Serial1/0
00:01:35: OSPF: rcv. v:2 t:1 l:48 rid:192.168.20.1
aid:0.0.0.1 chk:0 aut:2 keyid:1 seq:0x2B915223 from Serial1/0
00:01:45: OSPF: rcv. v:2 t:1 l:48 rid:192.168.20.1
aid:0.0.0.1 chk:0 aut:2 keyid:1 seq:0x2B915224 from Serial1/0
```

قسمت aut=2 در شکل بالا نشان می دهد که authentication از نوع md5 است و keyid:1 نشان دهنده ID کلید ست شده در دستورات است.

برای قسمت دوم سوال هم:

دو نوع PPP Authentication داریم: PAP و CHAP : PAP روشی است که username و password ها در آن بصورت Plain-text ارسال و دریافت می شوند ولی در CHAP ابتدا بسته ی مورد نظر با Md5، hash شده سپس ارسال می شود. که در اینجا ما از روش PAP استفاده کرده ایم.

به منظور ست کردن PPP بین پورتهای سریال روترهای R1 و R2 به ترتیب مراحل زیر با دستورات ذکر شده اعمال می کنیم

(۱) ابتدا در هر دو روتر وارد interface mode سریال آنها شده و دستور زیر را وارد می کنیم.

```
R2(config-int)#encapsulation PPP
```

(۲) بر روی یکی از روترها مثلاً R1 دستور زیر را در interface mode سریال آن وارد می کنیم.

```
R1(config-int)#PPP authentication PAP
```

این دستور درخواستی را برای تایید صلاحیت از روتر R1 به R2 می فرستد.

(۳) در این مرحله روتر R2 پاسخ روتر R1 را با فرستادن username و password خود می دهد.

```
R2(config-int)# PPP PAP sent-username R2 password acn
```

(۴) تا اینجا روتر R1 با توجه به پاسخی که از R2 گرفته است هنوز نمی تواند آنها را ببیند. بدین منظور دستور زیر را در Config mode روتر R1 باید وارد کنیم.

```
R1(config)# username R2 password acn
```

بعد از انجام این مراحل R1 و R2 می توانند یکدیگر را ببینند.

```
R1#
R1#ping 192.168.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/29/32 ms
R1#
```

برای نشان دادن تبادل پیامهای مربوط به PPP دستور زیر را بر روی روتر R1 اجرا و خروجی آن را آورده‌ایم.

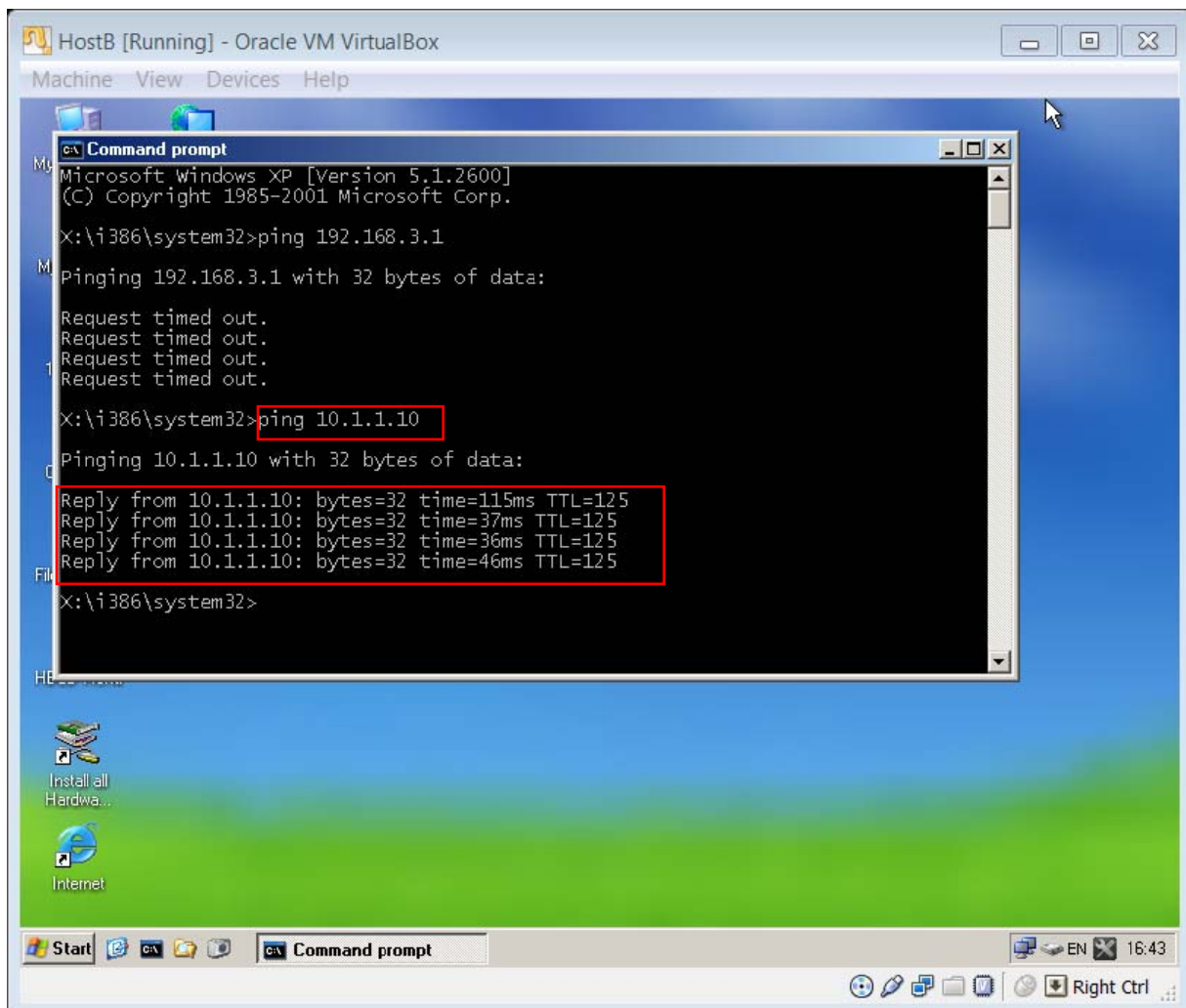
R1# debug ppp authentication

برای اینکه پیامهای تبادل شده بین دور روتر را debug کنیم ابتدا پورت s1/0 از روتر R1 را shut کردیم سپس دستور بالا را وارد کرده و باز دوباره همان پورت را no shut کردیم تا تبادلات بهتر مشخص شود حاصل تصویر زیر است :

```
Dynamips(4): R1, Console port
R1#
R1#debug ppp authentication
PPP authentication debugging is on
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int s1/0
R1(config-if)#no shut
R1(config-if)#
01:22:29: Se1/0 PPP: Treating connection as a dedicated line
01:22:29: Se1/0 PPP: Authorization NOT required
01:22:29: %LINK-3-UPDOWN: Interface Serial1/0, changed state to up^Z
R1#
01:22:29: Se1/0 PAP: I AUTH-REQ id 12 len 11 from "R2"
01:22:29: Se1/0 PAP: Authenticating peer R2
01:22:29: Se1/0 PPP: Sent PAP LOGIN Request to AAA
01:22:29: Se1/0 PPP: Received LOGIN Response from AAA = PASS
01:22:29: Se1/0 PAP: O AUTH-ACK id 12 len 5
01:22:29: Se1/0 CHAP: I CHALLENGE id 20 len 23 from "R2"
01:22:29: Se1/0 CHAP: Using hostname from configured hostname
01:22:29: Se1/0 CHAP: Using password from AAA
01:22:29: Se1/0 CHAP: O RESPONSE id 20 len 23 from "R1"
01:22:29: Se1/0 CHAP: I SUCCESS id 20 len 4
01:22:30: %SYS-5-CONFIG_I: Configured from console by console
01:22:30: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, changed state to up
R1#
01:22:39: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.20.1 on Serial1/0 from LOADING to FULL, Loading Done
R1#no de all
All possible debugging has been turned off
R1#
```

۵) هاست های A, B و C باید از طریق پیکربندی NAT Overload در روتر R3 به هاست های X, Y دسترسی داشته باشند. بر روی اینترفیس f0/1 روتر R3 باید یک ACL به نحوی پیکربندی شود که دسترسی بسته هایی با آدرس 192.168.0.0/16 به شبکه 10.1.1.0/24 امکان پذیر نباشد. این بسته ها باید تنها از طریق NAT به شبکه مقصد ارسال شوند. (Default Gateway برای هاست های A, B, C برابر 192.168.1.1 تعریف شود). امکان ping هاست C از هاست B باید از طریق پیکربندی ACL مسدود گردد. نحوه پیکربندی ACL باید به گونه ای باشد تا دیگر دسترسی های هاست C از هاست B امکان پذیر باشد.

در این بخش باید ابتدا شبکه ی 10.1.1.0 /24 را در OSPF قرار دهیم تا شبکه های 192.168.1.0 و 10.1.1.0 همدیگر را ببینند. بعد از اضافه کردن شبکه ی مزبور به OSPF، مثلاً هاست های B و X هم را می-بینند. که در شکل زیر Ping B به X نشان داده شده است.



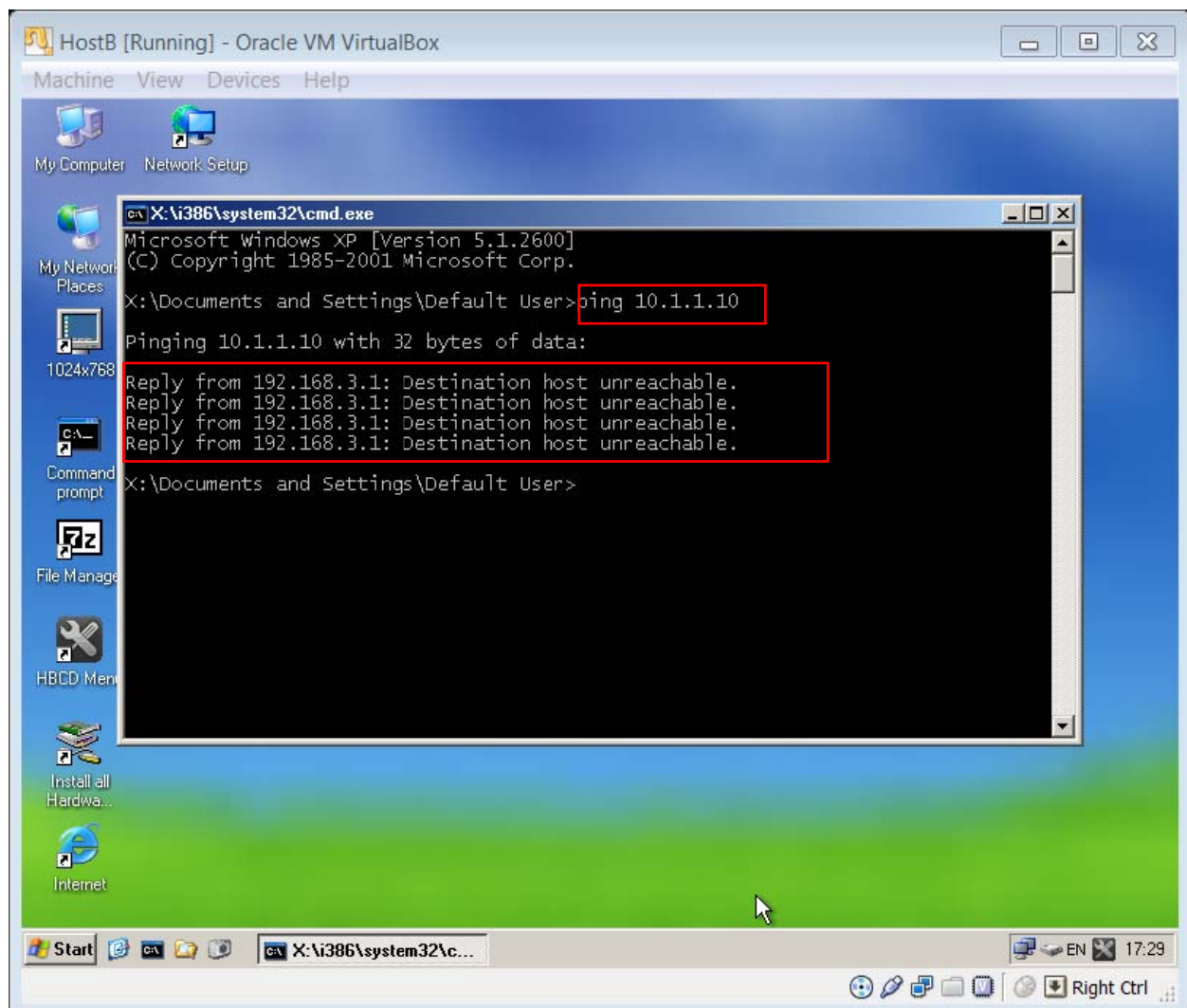
حال می خواهیم به کمک یک access list جلوی دسترسی شبکه ی 192.168.0.0 /16 را به شبکه ی 10.1.1.0 /24 را ببندیم. که اینکار به کمک دستورات زیر انجام می شود.

```
R3(config)#  
R3(config)#  
R3(config)#access-list 1 deny 192.168.0.0 0.0.255.255  
R3(config)#  
R3(config)#
```

سپس این ACL را به fa0/1 اختصاص می دهیم.

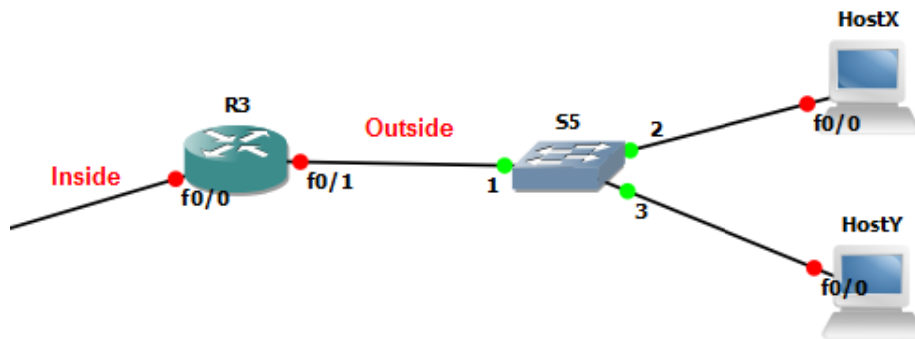
R3(config-int)# ip access-group 1 out

حال دیگر هاست B نمی تواند هاست X را ببیند.



حال در ادامه می خواهیم هم nat داشته باشیم هم ACL :

برای راه اندازی nat اول باید interface Fa0/0 را باید بعنوان inside و interface fa0/1 را بعنوان outside تعریف کنیم.



این کار با استفاده از دستورات زیر انجام می شود.

Int f0/0

Ip nat inside

Int f0/1

Ip nat out side

سپس range آدرسهای را که می خواهیم به آنها Nat کنیم را با دستور زیر مشخص می کنیم. همانطور که

مشخص است range آدرس را بین آدرسهای 10.1.1.2 تا 10.1.1.9 تعیین کردیم.

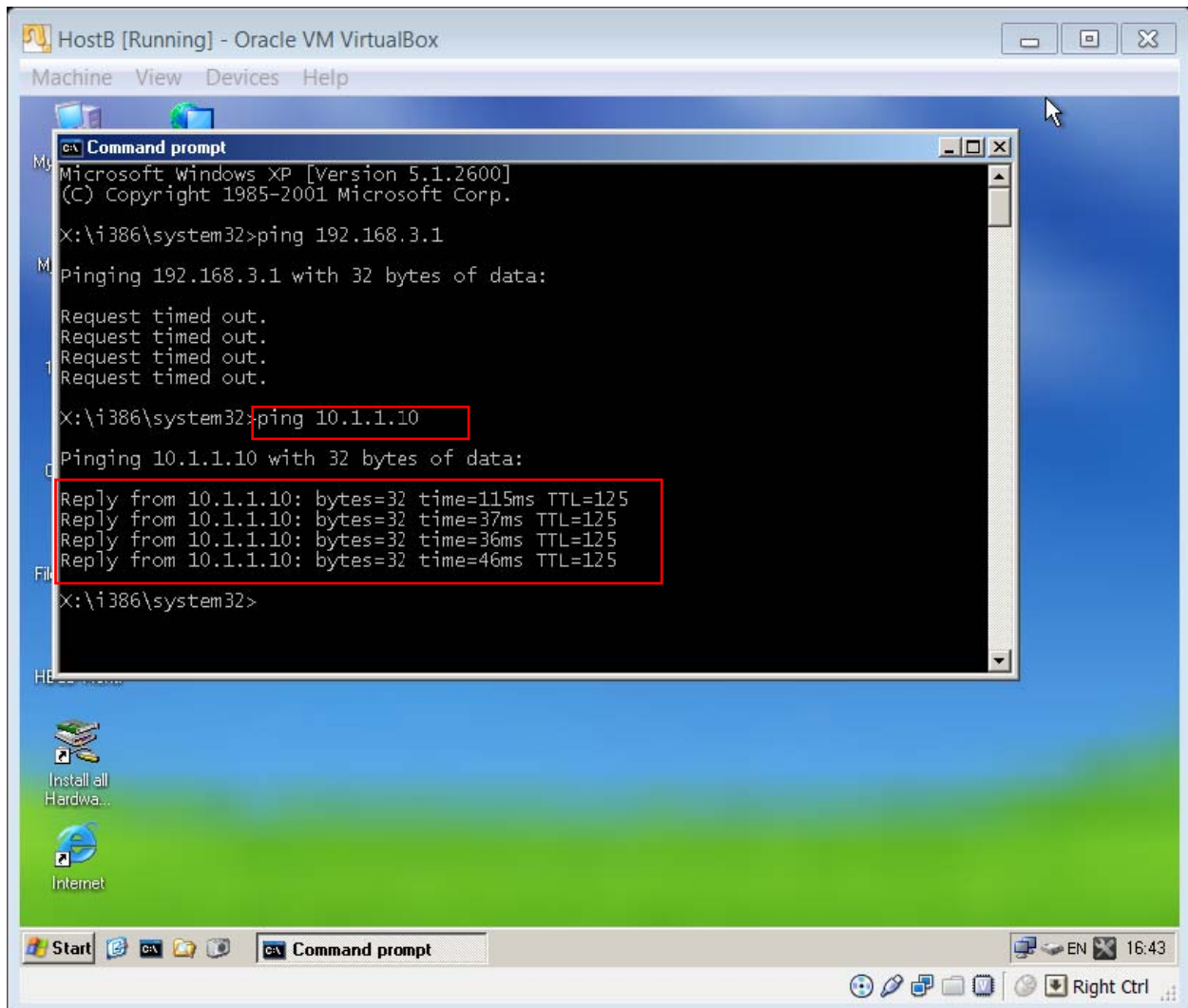
```
R3(config)#ip nat pool pool1 10.1.1.2 10.1.1.9 ne
R3(config)#ip nat pool pool1 10.1.1.2 10.1.1.9 netmask 255.255.255.240
```

سپس IP های ورودی به پورت (Fa0/0) inside را با 1 access-list تنظیم می کنیم.

حال دستور نهایی برای انجام nat و ترجمه ی آدرسهای منطبق با 1 access-list به آدرسهای pool1 را وارد می کنیم.

```
R3(config)#  
R3(config)#ip nat inside source list 1 pool pool1  
R3(config)#  
R3(config)#  
R3(config)#
```

حال می توان مشاهده کرد که هاست B می تواند هاست X را ببیند.



نتیجه ی این دستور به کمک دستور **show ipnat translations** نیز دیده می شود. بعنوان مثال از روی روتر R2 با آدرس 192.168.1.2 سعی شده است که هاست X، با آدرس 10.1.1.10، ping شود. همانطور که مشخص است عمل ترجمه ی آدرس انجام شده است.

```
R3#
R3#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
--- 10.1.1.2            192.168.1.2      ---               ---
--- 10.1.1.3            192.168.2.2      ---               ---
R3#
R3#
R3#
```

دو نوع access-list داریم :

۱- standard ACL: که تنها یک رنج آدرس در آن تعیین می کنیم و می گوئیم این رنج آدرس برای عبور از یک روتر permit شود یا deny. و توانایی بستن پورت خاص و غیره را ندارد

۲ - Extended ACL که با آن می توان دقیقاً مشخص کرد که ارتباط کدام هاست با کدام هاست روی چه پورتهای permit یا deny شود.

برای قسمت آخر سوال یعنی به منظور جلوگیری کردن از ping هاست C از طرف هاست B، باید بر روی R2 یک access-list بسازیم که از نوع extended باشد. دستورات زیر این کار را انجام می دهد.

```
R2(config)#
R2(config)#ip access-list extended noping
R2(config-ext-nacl)#
R2(config-ext-nacl)#deny icmp host 192.168.3.2 host 192.168.20.20
R2(config-ext-nacl)#
R2(config-ext-nacl)#permit ip any any
R2(config-ext-nacl)#
R2(config-ext-nacl)#
```


حال می بایست این access-list را به S1/0 از روتر R2 اعمال کنیم.

```
R2(config)#
R2(config)#int s1/0
R2(config-if)#
R2(config-if)#
R2(config-if)#ip access-group noping in
R2(config-if)#
R2(config-if)#
R2(config-if)#
R2(config-if)#
```

پس از انجام اینکار می بینیم که B نمی تواند C را ping کند. در حالیکه می تواند پورت fa0/0 از روتر R3 را ببیند.

