CẤU HÌNH ROUTER JUNIPER CƠ BẢN

Cho Người Mới Làm Được

Người làm tài liệu: HaiNguyen-IT bit.ly/admin-qtm

Môi trường thực hiện: EVE-NG (Juniper Olive, SRX, vMX)

Join nhóm FB để lấy guide các môn khác: bit.ly/lab-network

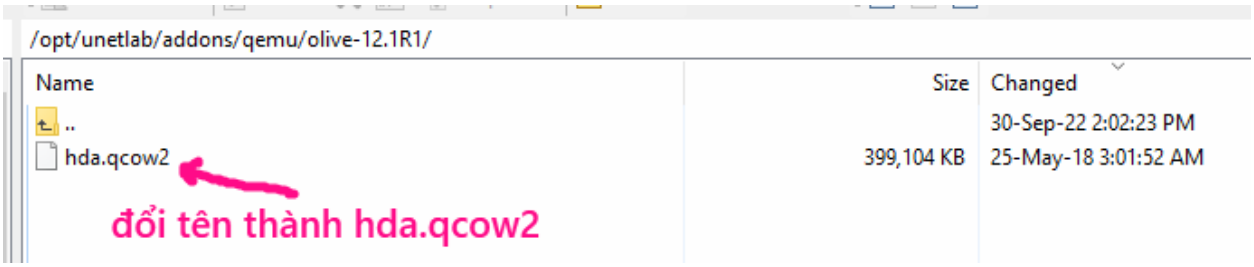
Học các môn khác tại bit.ly/hai-network

Mục lục

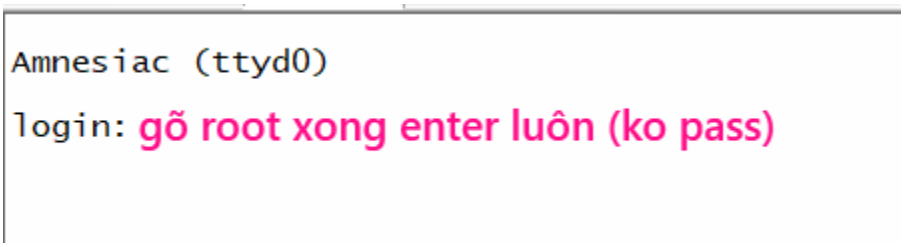
1. Download và cài đặt Juniper Olive trong EVE-NG

- Vào link https://mega.nz/#!sE1TiCLI!76bSiOrbqdA1a2vBxi_D1Hw37AqaF3fMViKk1rohM8Y

- Trên eve tạo thư mục như ảnh dưới và truyền file vào thư mục đấy bằng winscp



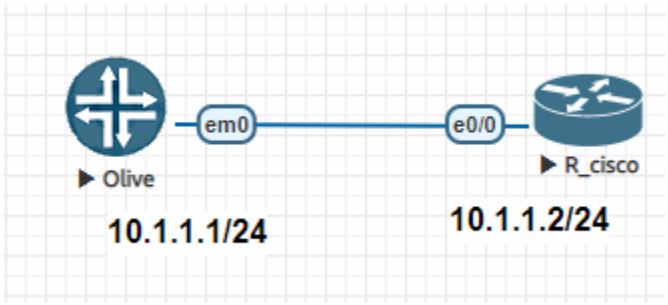
- Fix permission và mở web của eve ra; lấy node juniper olive ra và start node lên



DONE

2. Đặt IP cho cổng router Juniper

Ta tạo mô hình như dưới, sau đó đặt IP 2 đầu router và ping nhau



Juniper Olive:

```
cli
edit

set system root-authentication plain-text-password
Gõ pass mới 2 lần

set interfaces em0 unit 0 family inet address 10.1.1.1/24
commit
root> show interfaces terse
```

Cisco:

```
int e0/0
no shutdown
ip address 10.1.1.2 255.255.255.0
exit
show ip int brief
```

Ping thử 2 bên ok chưa

Juniper:

```
root# run ping 10.1.1.2
PING 10.1.1.2 (10.1.1.2): 56 data bytes
64 bytes from 10.1.1.2: icmp_seq=0 ttl=255 time=0.720 ms
64 bytes from 10.1.1.2: icmp_seq=1 ttl=255 time=0.727 ms
64 bytes from 10.1.1.2: icmp_seq=2 ttl=255 time=1.021 ms
64 bytes from 10.1.1.2: icmp_seq=3 ttl=255 time=0.750 ms
64 bytes from 10.1.1.2: icmp_seq=4 ttl=255 time=0.734 ms
```

Cisco:

```
Router#ping 10.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
Router#
```

Lưu ý: để off cổng đi dạng như shutdown bên cisco thì dùng lệnh:

set interface em1 disable

commit

Để mở lại thì

delete interface em1 disable

commit

3. Show, Backup và Restore lại cấu hình

SHOW:

Nếu Ở mode >

show configuration

show configuration | display set

Nếu Ở mode #

show

show | display set

run show configuration ## Có thêm chữ run để chạy được các lệnh ở mode >

…

BACKUP:

Cách 1: Lưu ra file config trên router

#save config_3_Otc_2022

```
[edit]
root# save config_3_oct_2022
Wrote 28 lines of configuration to 'config_3_oct_2022'
```

Đánh lệnh file list để xem file vừa tạo ra

```
root> file list

/root/:
.cshrc
.history
.login
.profile
config_3_oct_2022
```

Cách 2 : Backup và lưu trên FTP server (thủ công)

```
root@% ftp 192.168.1.10 (địa chỉ FTP server, có cài filezilla Server)

ftp> put config_11_5_2021
local: config_30_7 remote: config_11_5_2021
200 Port command successful
150 Opening data channel for file upload to server of "/config_30_7"
100% |***********************************************|  4464
--:-- ETA
226 Successfully transferred "/config_30_7"
4464 bytes sent in 0.02 seconds (191.71 KB/s)
ftp>
```

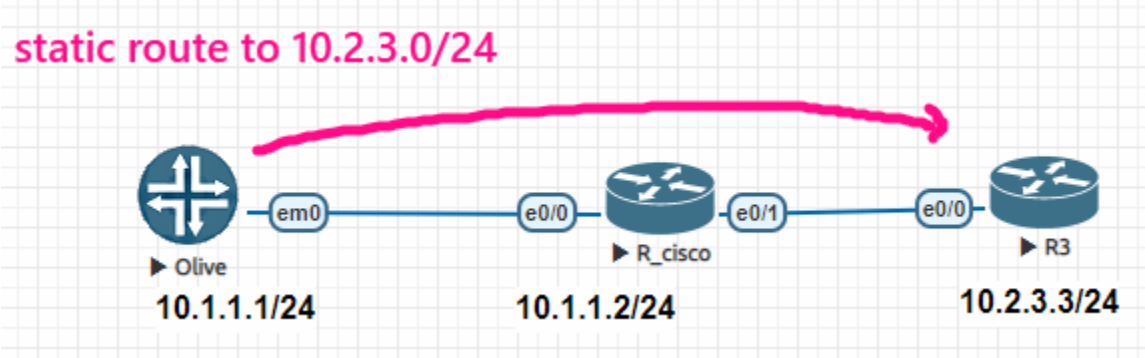
Cách 3: Backup tự động khi có thay đổi cấu hình

```
set system archival configuration transfer-on-commit
set system archival configuration archive-sites
ftp://u1:u1@192.168.1.50/ (mẫu: ftp://user:pass@<ip của FTP>)
```

RESTORE:

```
# load override config_3_oct_2022

#commit
```

4. Static route



Cấu hình static route để Olive đi đến dải 10.2.3.0/24 qua next-hop 10.1.1.2

```
# set routing-options static route 10.2.3.0/24 next-hop 10.1.1.2

#commit
```

Verify: (ta thấy AD của Juniper Static route là 5, còn trong Cisco là 1)

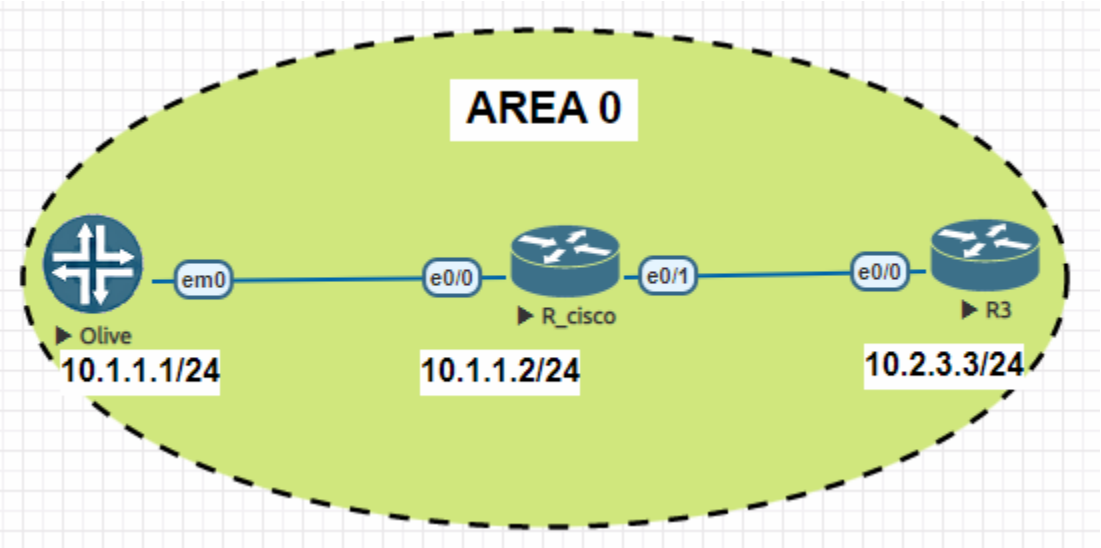
```
show route
```

```
10.2.3.0/24            *[Static/5] 00:17:12
                        > to 10.1.1.2 via em0.0
```

Ping thử

```
root# run ping 10.2.3.3
PING 10.2.3.3 (10.2.3.3): 56 data bytes
64 bytes from 10.2.3.3: icmp_seq=0 ttl=254 time=0.911 ms
64 bytes from 10.2.3.3: icmp_seq=1 ttl=254 time=0.854 ms
```

5. OSPF đơn vùng



Trong mô hình trên gồm 3 router chạy OSPF vùng 0. Trong đó 1 juniper và 2 cisco.

Cấu hình trên Olive:

```
###Tạo loopback0 có IP 1.1.1.1/32####
set interfaces lo0 unit 0 family inet address 1.1.1.1/32
###Cho loopback0 và em0 vào OSPF, thuộc vùng 0###
set protocols ospf area 0.0.0.0 interface lo0.0
set protocols ospf area 0.0.0.0 interface em0.0
```

Cấu hình trên Cisco: đã quá quen thuộc ☺

Verify:

Olive:

show ospf neighbor, thấy full là ok

```
[edit]
root# run show ospf neighbor
Address          Interface              State     ID               Pri  Dead
10.1.1.2         em0.0                  Full      10.2.3.2           1    37

[edit]
root#
```

show route, ta thấy AD của OSPF trong Juniper là 10, khác với Cisco là 110

```
1.1.1.1/32          *[Direct/0] 00:17:18
                     > via lo0.0
10.1.1.0/24         *[Direct/0] 03:43:11
                     > via em0.0
10.1.1.1/32         *[Local/0] 03:43:11
                       Local via em0.0
10.2.3.0/24         *[OSPF/10] 00:06:08, metric 11
                     > to 10.1.1.2 via em0.0
224.0.0.5/32        *[OSPF/10] 00:07:07, metric 1
                       MultiRecv
```

Ping thử sang Cisco

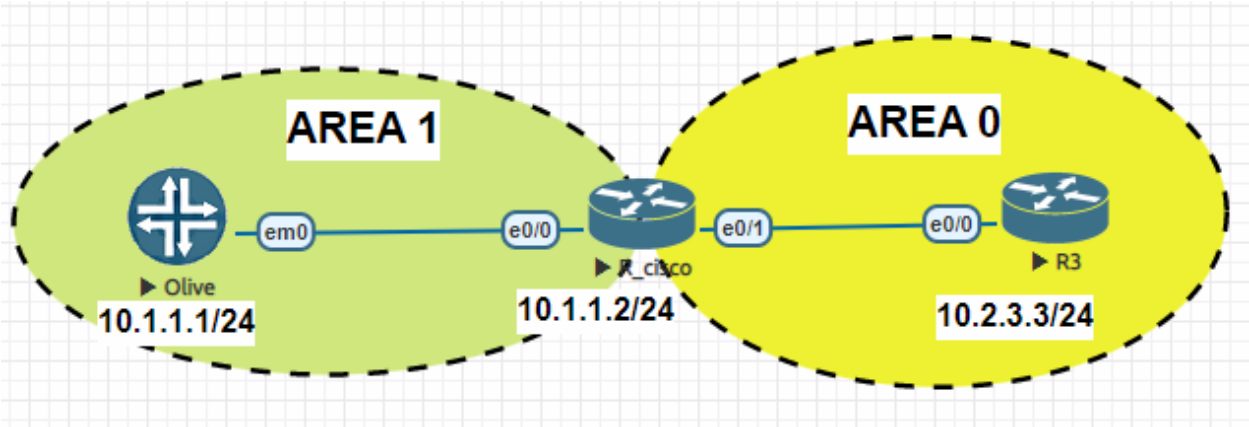
```
[edit]
root# run ping 10.1.1.2 source 1.1.1.1
PING 10.1.1.2 (10.1.1.2): 56 data bytes
64 bytes from 10.1.1.2: icmp_seq=0 ttl=255 time=0.547 ms
64 bytes from 10.1.1.2: icmp_seq=1 ttl=255 time=0.637 ms
64 bytes from 10.1.1.2: icmp_seq=2 ttl=255 time=0.733 ms
64 bytes from 10.1.1.2: icmp_seq=3 ttl=255 time=1.251 ms
```

Ping từ Cisco sang 1.1.1.1

```
R3#ping 1.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
R3#
```

DONE

6. OSPF đa vùng và redistribution



Cấu hình trên Olive:

```
###Tạo loopback0 có IP 1.1.1.1/32####

set interfaces lo0 unit 0 family inet address 1.1.1.1/32

###Cho loopback0 và em0 vào OSPF, thuộc vùng 1 ###

set protocols ospf area 0.0.0.1 interface lo0.0

set protocols ospf area 0.0.0.1 interface em0.0
```

Verify:

```
root# run show ospf route
```

```
[edit]
root# run show ospf route
Topology default Route Table:

Prefix             Path  Route      NH       Metric NextHop       Nexthop
                   Type  Type       Type             Interface     Address/LSP
10.2.3.2           Intra Area BR    IP            1 em0.0         10.1.1.2
1.1.1.1/32         Intra Network    IP            0 lo0.0
10.1.1.0/24        Intra Network    IP            1 em0.0
10.2.3.0/24        Inter Network    IP           11 em0.0         10.1.1.2
```

```
[edit]
root# run ping 10.2.3.3
PING 10.2.3.3 (10.2.3.3): 56 data bytes
64 bytes from 10.2.3.3: icmp_seq=0 ttl=254 time=0.835 ms
64 bytes from 10.2.3.3: icmp_seq=1 ttl=254 time=0.807 ms
```

REDISTRIBUTION CONNECTED ROUTE: tạo thêm 1 IP nữa cho loopback0 11.11.11.11/32 và redistribute nó vào OSPF.

```
###Gán thêm 1 IP 11.11.11.11/32 cho loopback0 ở trên####

###Khác với Cisco có thể tạo nhiều loopback1,2,3…Trong  Juniper chỉ cho tạo 1 loopback###

set interfaces lo0 unit 0 family inet address 11.11.11.11/32

###Bỏ Lo0.0 ra khỏi OSPF , sau đó redistribute chỉ loopback 11.11.11.11 vào ###

delete protocols ospf area 0.0.0.1 interface lo0.0

###Thực hiện redistribute loopback 11.11.11.11 vào OSPF####

set policy-options policy-statement REDIS_ONLY_11.11.11.11 term 1 from protocol direct

set policy-options policy-statement REDIS_ONLY_11.11.11.11 term 1 from route-filter 11.11.11.11/32 exact

set policy-options policy-statement REDIS_ONLY_11.11.11.11 term 1 then accept

set protocols ospf export REDIS_ONLY_11.11.11.11

commit
```

Verify:

Trên Cisco show ra đã thấy route dạng E2

```
      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
O IA     10.1.1.0/24 [110/20] via 10.2.3.2, 00:31:01, Ethernet0/0
C        10.2.3.0/24 is directly connected, Ethernet0/0
L        10.2.3.3/32 is directly connected, Ethernet0/0
      11.0.0.0/32 is subnetted, 1 subnets
O E2     11.11.11.11 [110/0] via 10.2.3.2, 00:00:28, Ethernet0/0
R3#
R3#
```

Tiếp theo trên R3, ta thử redistribute 1 loopback vào; sau đó check trên Olive xem học được chưa, với kiểu route gì và AD là bao nhiêu?

R3:

```
int lo0

ip address 3.3.3.3 255.255.255.255

no shut

router ospf 1

redistribute connected subnets
```

Check trên Olive đã thấy học được prefix 3.3.3.3 ở dạng E2, AD là 150, khác với Cisco là 110

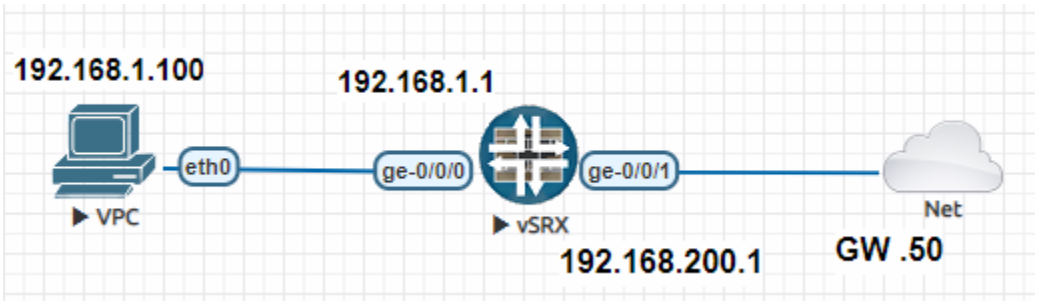
```
root# run show route

inet.0: 7 destinations, 7 routes (7 active, 0 holddown, 0 hidder
+ = Active Route, - = Last Active, * = Both

1.1.1.1/32          *[Direct/0] 01:31:58
                     > via lo0.0
3.3.3.3/32          *[OSPF/150] 00:00:14, metric 20, tag 0
                     > to 10.1.1.2 via em0.0
```

```
root# run show ospf route
Topology default Route Table:

Prefix             Path  Route      NH       Metric NextHop       Nexthop
                   Type  Type       Type             Interface     Address/LSP
10.2.3.2           Intra Area BR    IP            1 em0.0         10.1.1.2
10.2.3.3           Inter AS BR      IP           11 em0.0         10.1.1.2
3.3.3.3/32         Ext2  Network    IP           20 em0.0         10.1.1.2
10.1.1.0/24        Intra Network    IP            1 em0.0
10.2.3.0/24        Inter Network    IP           11 em0.0         10.1.1.2
```

NẾU REDISTRIBUTION STATIC ROUTE VÀO OSPF: ta chỉnh chỗ dưới từ direct thành static

```
REDIS_ONLY_11.11.11.11 term 1 from protocol direct
```

7. NAT overload truy cập internet (làm trên SRX do Olive router support)



Cấu hình tại VPC

```
ip 192.168.1.100/24 192.168.1.1
```

Cấu hình tại Juniper SRX

```
set system root-authentication plain-text-password
Gõ pass mới 2 lần
set interfaces ge-0/0/0 unit 0 family inet address 192.168.1.1/24
set interfaces ge-0/0/1 unit 0 family inet address 192.168.200.1/24
set security zones security-zone trust interfaces ge-0/0/0.0 host-inbound-traffic system-services all
```

```
set security zones security-zone untrust interfaces ge-0/0/1.0 host-inbound-traffic system-services all

set routing-options static route 0.0.0.0/0 next-hop 192.168.200.50
```

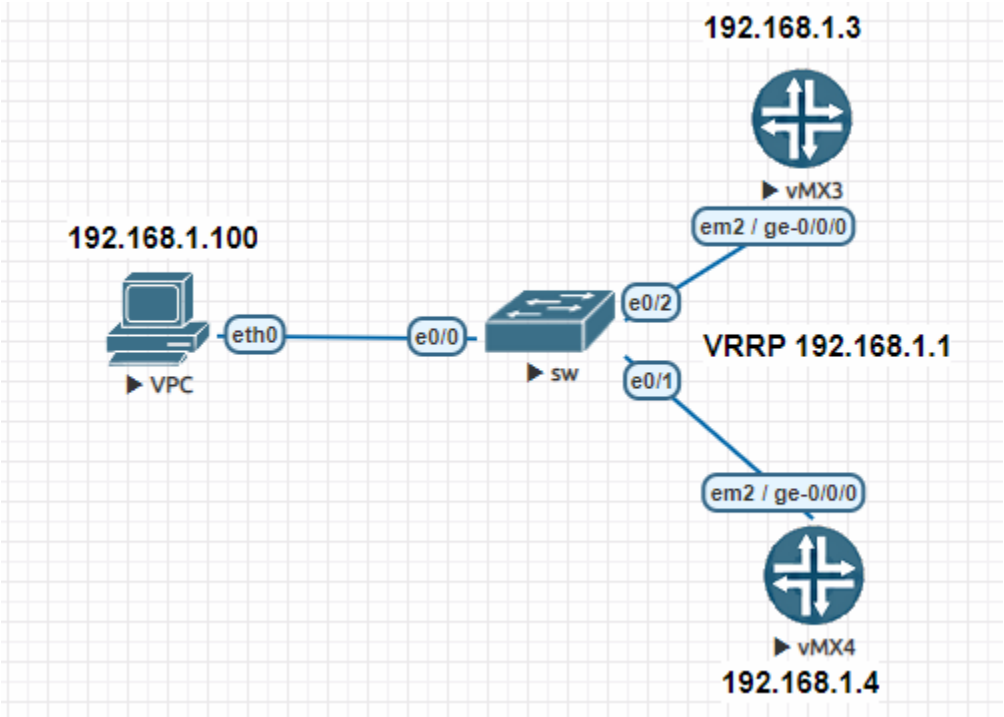
```
###Khai báo NAT overload###
set security nat source rule-set hainm-rule-set1 from zone trust
set security nat source rule-set hainm-rule-set1 to zone untrust
set security nat source rule-set hainm-rule-set1 rule hainm-rule1 match source-address 192.168.1.0/24
set security nat source rule-set hainm-rule-set1 rule hainm-rule1 match destination-address 0.0.0.0/0
set security nat source rule-set hainm-rule-set1 rule hainm-rule1 then source-nat interface
commit
```

Kiểm tra lại: Từ VPC ping ra 8.8.8.8 ok

```
VPCS> ping 8.8.8.8

84 bytes from 8.8.8.8 icmp_seq=1 ttl=112 time=65.864 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=112 time=28.627 ms
84 bytes from 8.8.8.8 icmp_seq=3 ttl=112 time=29.575 ms
84 bytes from 8.8.8.8 icmp_seq=4 ttl=112 time=29.335 ms
84 bytes from 8.8.8.8 icmp_seq=5 ttl=112 time=29.521 ms
```

8. VRRP (làm trên vMX 14, do Olive không support cổng ge)

Down image này ở bài chú ý trong nhóm bit.ly/lab-network



##Xóa cấu hình rác trên vMX14

delete logical-systems r1

delete logical-systems r2

##Khai báo vMX3 làm master###

set interfaces ge-0/0/0 unit 0 family inet address 192.168.1.3/24 vrrp-group 1 virtual-address 192.168.1.1

set interfaces ge-0/0/0 unit 0 family inet address 192.168.1.3/24 vrrp-group 1 priority 110

set interfaces ge-0/0/0 unit 0 family inet address 192.168.1.3/24 vrrp-group 1 accept-data

set interfaces ge-0/0/0 unit 0 family inet address 192.168.1.3/24 vrrp-group 1 track interface <cổng WAN> priority-cost 10 (không cần lệnh này vẫn chạy)

##Khai báo vMX4 làm backup###

set interfaces ge-0/0/0 unit 0 family inet address 192.168.1.4/24 vrrp-group 1 virtual-address 192.168.1.1

set interfaces ge-0/0/0 unit 0 family inet address 192.168.1.4/24 vrrp-group 1 priority 105

set interfaces ge-0/0/0 unit 0 family inet address 192.168.1.4/24 vrrp-group 1 accept-data

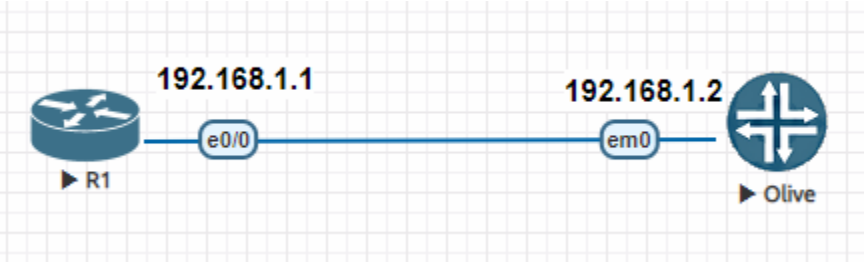
Verify:

show vrrp

```
[edit]
lab@vMX3# run show vrrp
Interface     State       Group   VR state VR Mode   Timer    Type   Address
ge-0/0/0.0    up              1   master   Active      A  0.092 lcl    192.168.1.3
                                                                vip    192.168.1.1
```

```
[edit]
lab@vMX4# run show vrrp
Interface     State       Group   VR state VR Mode   Timer    Type   Address
ge-0/0/0.0    up              1   backup   Active      D  2.918 lcl    192.168.1.4
                                                                vip    192.168.1.1
                                                                mas    192.168.1.3
```

9. GRE tunnel với Router Cisco



Trên Cisco:

```
interface Tunnel0
 ip address 1.1.1.1 255.255.255.0
 tunnel source Ethernet0/0
 tunnel destination 192.168.1.2
```

Trên Olive:

```
set interfaces gre unit 0 tunnel source 192.168.1.2
set interfaces gre unit 0 tunnel destination 192.168.1.1
set interfaces gre unit 0 family inet address 1.1.1.2/24
```

Verify:

show interface terse

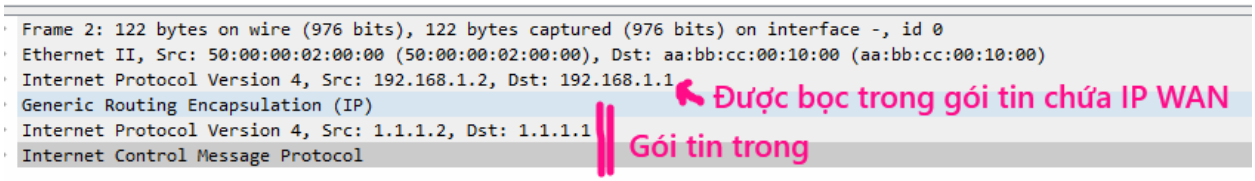
```
root# run show interfaces terse
Interface               Admin Link Proto    Local
cbp0                    up    up
demux0                  up    up
dsc                     up    up
em0                     up    up
em0.0                   up    up   inet     192.168.1.2/24
em1                     up    up
em2                     up    up
em3                     up    up
gre                     up    up
gre.0                   up    up   inet     1.1.1.2/24
ipip                    up    up
irb                     up    up
```

Ping thử 2 đầu và bắt wireshark

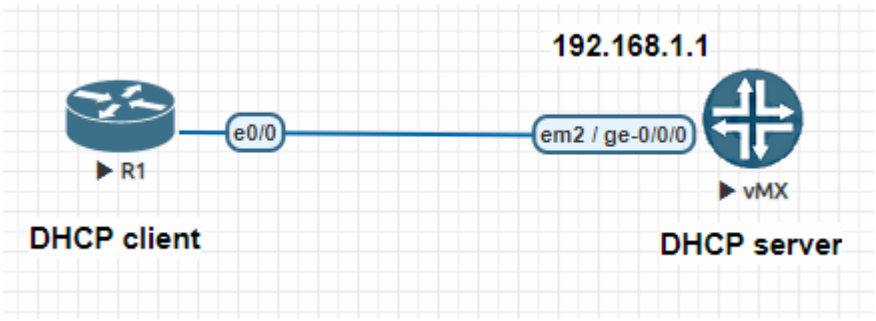
```
root# run ping 1.1.1.1
PING 1.1.1.1 (1.1.1.1): 56 data bytes
64 bytes from 1.1.1.1: icmp_seq=0 ttl=255 time=0.685 ms
64 bytes from 1.1.1.1: icmp_seq=1 ttl=255 time=0.678 ms
64 bytes from 1.1.1.1: icmp_seq=2 ttl=255 time=0.710 ms
64 bytes from 1.1.1.1: icmp_seq=3 ttl=255 time=0.650 ms
```

```
R1-Cisco#ping 1.1.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
R1-Cisco#
```

Wireshark log:



10. DHCP server (làm trên vMX, vì làm trên Olive không thấy chạy)



###Tạo ra pool để cấp dải 192.168.1.0/24 ###

set access address-assignment pool hai-pool family inet network 192.168.1.0/24

set access address-assignment pool hai-pool family inet range hai-range low 192.168.1.10

set access address-assignment pool hai-pool family inet range hai-range high 192.168.1.15

set access address-assignment pool hai-pool family inet dhcp-attributes name-server 8.8.8.8

set access address-assignment pool hai-pool family inet dhcp-attributes router 192.168.1.2

###Kích hoạt dịch vụ DHCP trên cổng ge-0/0/0###

###Khi gặp gói tin xin DHCP đến cổng ge-/0/0/0 nó sẽ cấp pool cùng dải IP vs cổng###

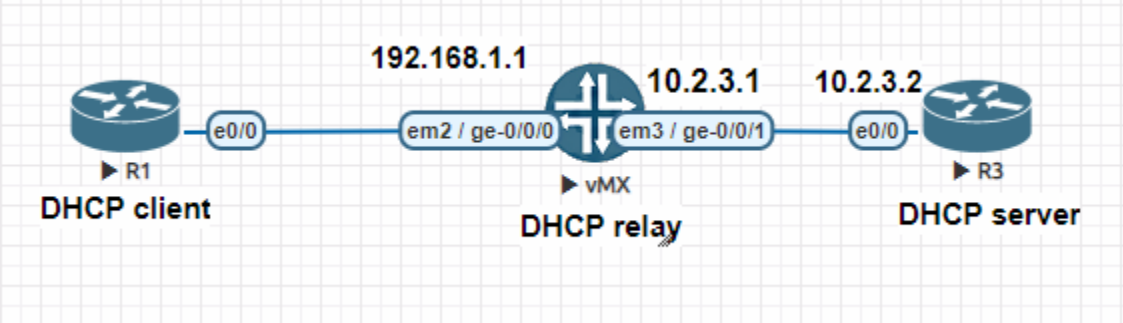
set system services dhcp-local-server group hai-group interface ge-0/0/0.0

Tuy nhiên khi commit bị báo cần license nên chưa test được:

Tham khảo thêm ở đây
https://www.juniper.net/documentation/us/en/software/junos/dhcp/topics/topic-map/dhcp-server-configuration.html

```
[edit]
lab@vMX-1# commit
[edit access address-assignment]
  'pool hai-pool'
    warning: requires 'subscriber-address-assignment' license
commit complete

[edit]
lab@vMX-1#
```

11. DHCP relay Agent



Cấu hình DHCP server trên R3:

```
ip dhcp pool 192.168.1.0_Pool
 network 192.168.1.0 255.255.255.0
 default-router 192.168.1.1

ip route 192.168.1.0   255.255.255.0  10.2.3.1
```

Cấu hình DHCP relay agent trên Juniper MX

```
set forwarding-options dhcp-relay server-group hai-group 10.2.3.2 ##IP của DHCP server##

set forwarding-options dhcp-relay active-server-group hai-group

set forwarding-options dhcp-relay group INTERFACE interface ge-0/0/0.0 ##Chỉ ra cổng xuống client#
```

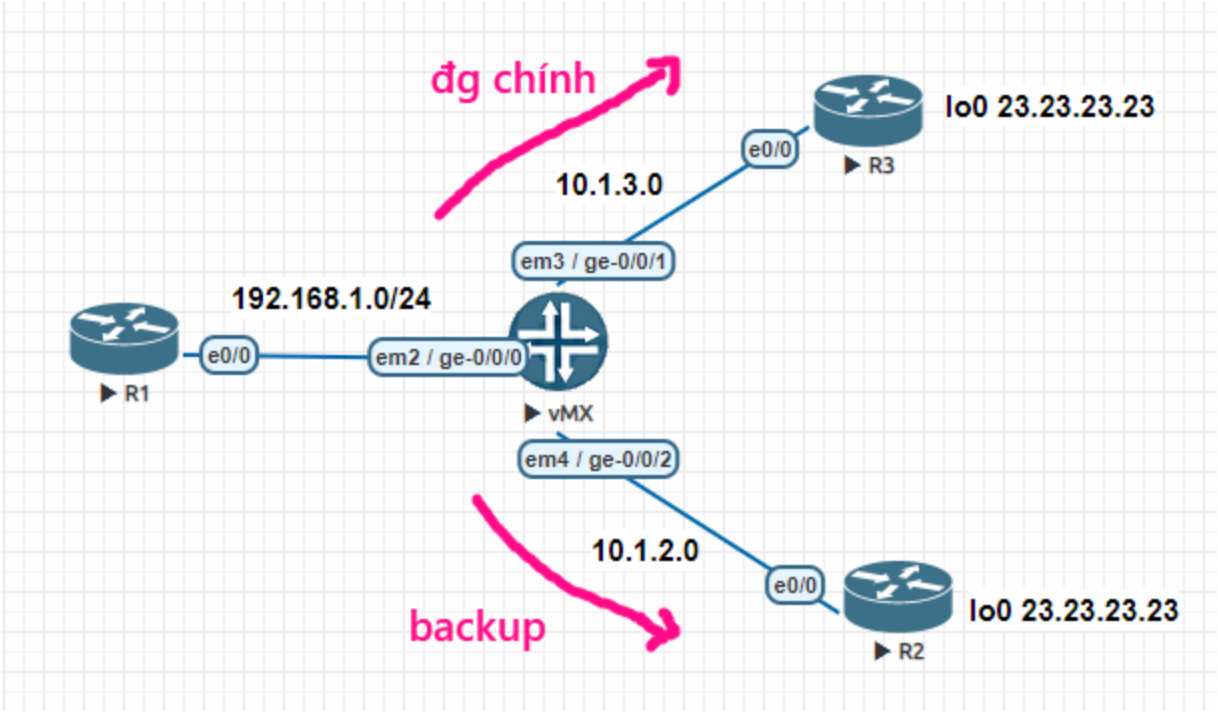
Trên R1

```
int e0/0
ip address dhcp
no shutdown
```

Verify: show ip int brief trên R1 đã thấy nhận IP

```
R1-Cisco#show ip int brief
Interface                  IP-Address      OK? Method Status                Prot
ocol
Ethernet0/0                192.168.1.10    YES DHCP   up                    up
```

12. SLA tracking in Juniper



>> Từ version Junos 18 trở lên, xem link https://iliketech2017.wordpress.com/2019/04/23/static-route-tracking-with-junos-rpm-tracking/

>> Nếu trong Juniper SRX, xem link https://hainguyenit.edubit.vn/blog/su-dung-ip-monitoring-trong-juniper-srx-tuong-tu-sla-cisco

>> Nếu dùng Junos vMX 14 thì dùng rpm probe kết hợp event-options (hơi dài)

https://supportportal.juniper.net/s/article/SRX-Example-RPM-with-event-options-for-route-failover?language=en_US

>> Trong lab này, ad dùng cách theo dõi link vật lí nếu bị down thì chuyển route sang WAN còn lại.

```
set routing-options static route 0.0.0.0/0 next-hop 10.1.3.3
set routing-options static route 0.0.0.0/0 qualified-next-hop 10.1.2.2 preference 10
commit
```

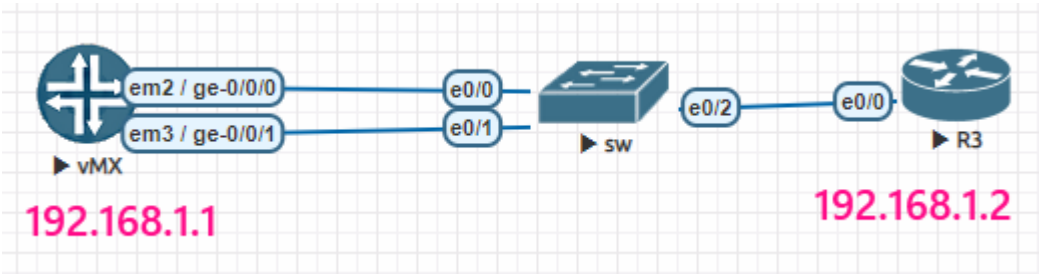
Verify:

Ta ping từ R1 lên 23.23.23.23 repeat 5000

Sau đó shutdown cổng ge-0/0/1 của vmX theo lệnh set interface ge-0/0/1.0 disable, commit

Sau đó thấy ping chỉ mất 1-2 gói rồi lại ok

13. Cấu hình LACP trên router Juniper



vMX:

```
set chassis aggregated-devices ethernet device-count 1 ##Chỉ ra số port-channel
set interfaces ge-0/0/0 gigether-options 802.3ad ae1
set interfaces ge-0/0/1 gigether-options 802.3ad ae1
set interfaces ae1 aggregated-ether-options lacp active
set interfaces ae1 unit 0 family inet address 192.168.1.1/24
set interfaces ae1 unit 0 family ethernet-switching port-mode access##Để port mode access
```

Sw Cisco:

```
interface Ethernet0/0
 channel-group 1 mode active
interface Ethernet0/1
 channel-group 1 mode active
```

Router Cisco:

```
interface Ethernet0/0

 ip address 192.168.1.2 255.255.255.0

no shutdown
```

Verify:

Juniper:

show interfaces terse | match ae1

```
[edit]
lab@vMX-1# run show interfaces terse | match ae1
ge-0/0/0.0              up    up   aenet    --> ae1.0
ge-0/0/1.0              up    up   aenet    --> ae1.0
ae1                     up    up
ae1.0                   up    up   inet     192.168.1.1/24
```

Cisco:

show etherchanel summary

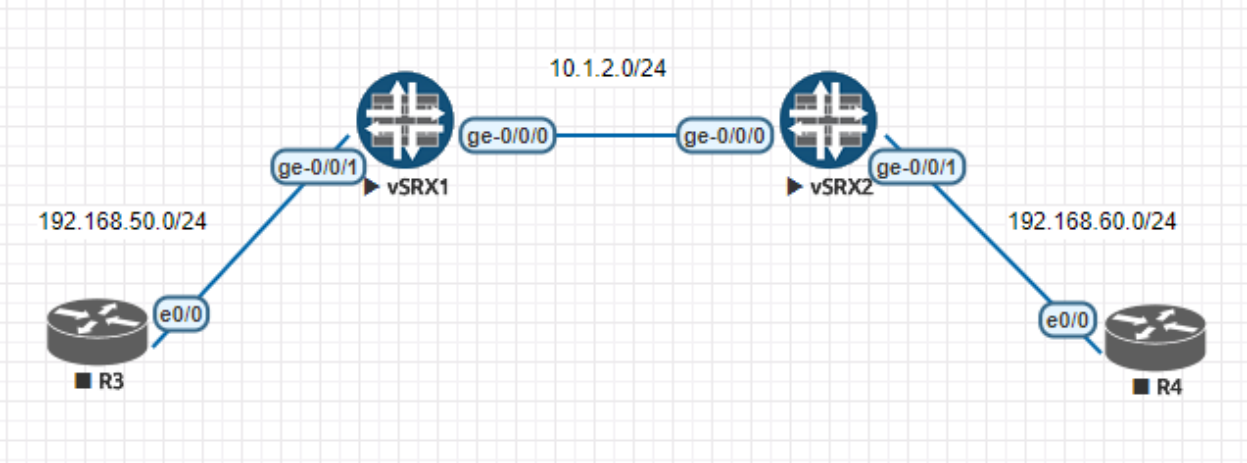
```
Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-------------------------------
1      Po1(SU)         LACP      Et0/0(P)    Et0/1(P)

Switch#
```

Ping thử:

```
Router#ping 192.168.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
```

```
[edit]
lab@vMX-1# run ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2): 56 data bytes
64 bytes from 192.168.1.2: icmp_seq=0 ttl=255 time=2.612 ms
64 bytes from 192.168.1.2: icmp_seq=1 ttl=255 time=1.558 ms
64 bytes from 192.168.1.2: icmp_seq=2 ttl=255 time=2.481 ms
64 bytes from 192.168.1.2: icmp_seq=3 ttl=255 time=2.790 ms
64 bytes from 192.168.1.2: icmp_seq=4 ttl=255 time=3.955 ms
64 bytes from 192.168.1.2: icmp_seq=5 ttl=255 time=1.715 ms
```

14. Cấu hình VPN site to site giữa 2 firewall SRX



Trên vSRX1

Bước 1: Tạo interface st0 và zone VPN

```
set interfaces st0 unit 0 family inet
set security zones security-zone VPN interfaces st0.0
```

Bước 2: Cấu hình address-book lưu địa chỉ LAN của 2 bên

```
set security address-book global address local 192.168.50.0/24
set security address-book global address remote 192.168.60.0/24
```

Bước 3: Định tuyến từ LAN đi sang LAN remote qua interface st0 ở trên

```
set routing-options static route 192.168.60.0/24 next-hop st0.0
```

Bước 4: Cấu hình IKE

```
set security ike proposal IKE-PROP authentication-method pre-shared-keys
set security ike proposal IKE-PROP dh-group group5
set security ike proposal IKE-PROP authentication-algorithm sha1
set security ike proposal IKE-PROP encryption-algorithm aes-128-cbc
set security ike proposal IKE-PROP lifetime-seconds 3600

set security ike policy IKE-POL mode main
set security ike policy IKE-POL proposals IKE-PROP
set security ike policy IKE-POL pre-shared-key ascii-text Juniper

set security ike gateway IKE-GW ike-policy IKE-POL
set security ike gateway IKE-GW address 10.1.2.2 (IP wan của SRX2)
set security ike gateway IKE-GW external-interface ge-0/0/0.0
```

Bước 5: Cấu hình IPSEC

```
Set security ipsec proposal IPSEC-PROP protocol esp
set security ipsec proposal IPSEC-PROP authentication-algorithm hmac-sha1-96
set security ipsec proposal IPSEC-PROP encryption-algorithm aes-128-cbc
set security ipsec proposal IPSEC-PROP lifetime-seconds 3600

set security ipsec policy IPSEC-POL perfect-forward-secrecy keys group5
set security ipsec policy IPSEC-POL proposals IPSEC-PROP

set security ipsec vpn IPSEC-VPN bind-interface st0.0
set security ipsec vpn IPSEC-VPN vpn-monitor
set security ipsec vpn IPSEC-VPN ike gateway IKE-GW
set security ipsec vpn IPSEC-VPN ike ipsec-policy IPSEC-POL
set security ipsec vpn IPSEC-VPN establish-tunnels immediately
```

Bước 6: Cho traffic đi vào zone VPN

```
set security zones security-zone untrust host-inbound-traffic system-services ike
```

```
set security policies from-zone trust to-zone VPN policy trust-to-vpn match source-address local
set security policies from-zone trust to-zone VPN policy trust-to-vpn match destination-address remote
set security policies from-zone trust to-zone VPN policy trust-to-vpn match application any
set security policies from-zone trust to-zone VPN policy trust-to-vpn then permit

set security policies from-zone VPN to-zone trust policy vpn-to-trust match source-address remote
set security policies from-zone VPN to-zone trust policy vpn-to-trust match destination-address local
set security policies from-zone VPN to-zone trust policy vpn-to-trust match application any
set security policies from-zone VPN to-zone trust policy vpn-to-trust then permit
```

Bước 7: Verify

root> show security ike active-peer

```
root@SRX1> show security ike active-peer
Remote Address                  Port     Peer IKE-ID
10.1.2.2                        500      10.1.2.2
```

root> show security ike security-associations

```
root> show security ike security-associations
Index   State  Initiator cookie  Responder cookie  Mode           Remote Address
4913192 UP     e86a913661eb5c1b  6e01d29c1f939426  Main           10.1.2.1
```

root> show security ipsec security-associations

```
root> show security ipsec security-associations
  Total active tunnels: 1
  ID    Algorithm       SPI      Life:sec/kb  Mon lsys Port  Gateway
  <131073 ESP:aes-cbc-128/sha1 88c064b8 1167/ unlim U root 500 10.1.2.1
  >131073 ESP:aes-cbc-128/sha1 864385b1 1167/ unlim U root 500 10.1.2.1
```

Ping LAN local to remote

R3>ping 192.168.60.2

Success rate is 100 percent (5/5), round-trip min/avg/max = 2/7/15 ms

R4#ping 192.168.50.2

Success rate is 100 percent (5/5), round-trip min/avg/max = 2/3/6 ms

Các gói tin ping giữa 2 bên LAN đã bị mã hóa, không còn thấy source và đích đâu nữa, chỉ thấy địa chỉ WAN của 2 firewall

```
    1342 2852.178116   10.1.2.1          10.1.2.2          ESP          166 ESP (SPI=0x88c064b8)
    1343 2859.449779   10.1.2.1          10.1.2.2          ESP          166 ESP (SPI=0x88c064b8)
    1344 2859.450169   10.1.2.2          10.1.2.1          ESP          166 ESP (SPI=0x864385b1)
```

```
> Frame 1343: 166 bytes on wire (1328 bits), 166 bytes captured (1328 bits) on interface 0
> Ethernet II, Src: 50:00:00:01:00:00 (50:00:00:01:00:00), Dst: 50:00:00:02:00:00 (50:00:00:02:00:00)
> Internet Protocol Version 4, Src: 10.1.2.1, Dst: 10.1.2.2
v Encapsulating Security Payload
    ESP SPI: 0x88c064b8 (2294310072)
    ESP Sequence: 52
```

Bước 8: Troubleshoot
Show ike và ipsec ở trên không thấy gì => kiểm tra lại cấu hinfh
Show ike thấy neighbor bị down
 ->Ping thử địa chỉ vật lí 2 bên
-> Check lại policy