Question 1

a) (i)

```
ip route   172.16.9.0   255.255.255.192   172.16.6.6
ip route   172.16.9.0   255.255.255.192   172.16.8.10   5
```

Assume that the route with next-hop address 172.16.6.6 is the primary route with administrative distance of 1. The route with next-hop address 172.16.8.10 is the backup route with administrative distance of 5 which is higher than 1, it will not become the preferred primary route.

(ii)

```
ip route   172.16.7.0   255.255.255.192   s0/1/1
ip route   172.16.7.0   255.255.255.192   s0/2/1   5
```

Assume that the route with exit interface s0/1/1 is the primary route with administrative distance of 1. The route with exit interface s0/2/1 is the backup route with administrative distance of 5 which is higher than 1, it will not become the preferred primary route.

(iii)

- Act as backup route
- Backup route be activated when primary route is down.

b) (i)

```
ip route 172.16.7.0 255.255.255.192 172.16.8.9
ip route 172.16.9.0 255.255.255.192 s0/2/1
```

(ii)

- Route with next-hop address only
  - ↳ Recursive lookup executed by router
  - ↳ More resources and time consumption to find out exit interface to forward out packet.

- Route with exit interface only
  - ↳ not able to handle multi-access connection
  - ↳ Only knows the correct exit interface for the received packet but does not know the correct next-hop address to reach
  - ↳ This type of route only suitable for point-to-point connection instead of multi-access connection.

c) BIOLOGY

```
router ospf 321
network 172.16.6.4 0.0.0.3 area 0
network 172.16.7.0 0.0.0.63 area 0
default-information originate
passive-interface g0/0/1
```

PHYSICS

```
router ospf 321
network 172.16.8.8 0.0.0.3 area 0
network 172.16.8.0 0.0.0.3 area 0
```

Question 2

a) (i) - A rogue DHCP server is connected to the network and provides false IP configuration parameters to legitimate clients.

- For example, the rogue server may provide wrong default gateway, wrong DNS server or wrong IP address.

(ii) - Man-in-the-Middle (MITM) attack
↳ Attacker assigns their own IP address as default gateway or DNS server
↳ All traffic from victim is routed through the attacker, allows for interception, modification or logging of sensitive data

- Denial of Service (DoS) attack
↳ Rogue DHCP server assign incorrect or non-functional IP configurations
↳ Devices lose network connectivity, disrupting business operations or user access.

- Network reconnaissance
- Malware injection

b) (i) R2

```
access-list 68 deny host 172.16 71.10
access-list 68 permit any

interface s0/1/0
ip access-group 68 in
```

(ii) R2

```
ip access-list extended ALLOW_ ACCESS
permit tcp 172.16.91.128 0.0.0.127 host 172.16.81.254 eq 443
permit icmp 172.16.91.128 0.0.0.127 172 16.61.1 0.0.0.254
deny ip any any

interface g0/0/0
ip access-group ALLOW_ACCESS in
```

Question 3

a) - Error : Wrong IP address is excluded in `ip dhcp excluded-address 172.16.81.1 172.16.81.8' statement

- Solution :

```
no ip dhcp excluded-address 172.16.81.1 172.16.81.8
ip dhcp excluded-address 172.16.81.1
```

- Justification :

  Only 172.16.81.1 is assigned as the default gateway of LAN_BB_POOL.
  The range from 172.16.81.2 to 172.16.81.8 should be inside the LAN_BB_POOL to be distributed to DHCP clients.

- Error : Wrong IP address is excluded from the `ip dhcp excluded-address 172.16.71.1 172.16.71.7' statement

- Solution :

```
no ip dhcp excluded-address 172.16.71.1 172.16.71.7
ip dhcp excluded-address 172.16.71.1
```

- Justification:

  Only the 172.16.71.1 has been taken as default gateway of LAN_AA_POOL.
  The other IP address (172.16.71.2 to 172.16.71.7) should be released into the pool for being distributed to DHCP clients.

- Error : Wrong subnet mask is used in the network statement in LAN_BB_POOL

- Solution :

```
ip dhcp pool LAN_BB_POOL
no network 172.16.81.0 255.255.255.252
network 172.16.81.0 255.255.255.0
```

- Justification :

  The pool network address is 172.16.81 0/24 , /24 should be converted into 255.255.255.0 in binary.

- Error : The default-router statement is missing in the LAN_BB_POOL configuration

- Solution :

```
ip dhcp pool LAN BB_POOL
default-router 172.16.81.1
```

- Justification :

  The 172.16.81.1 is the DHCP_ROUTER 's interface g0/0/1 's IP address which is facing to the LAN_BB_POOL subnet, it should be configured as default gateway to route the packet from one network to another network.

- Error : The configuration for LAN-AA-POOL is missing.

- Solution :

```
ip dhcp pool LAN_AA_POOL
network 172.16.71.0 255.255.255.128
default-router 172.16.71.1
```

- Justification :

The LAN_CC_POOL DHCP pool must be configured for allowing the DHCP server to distribute the DHCP IP address via DHCPv4 message to the DHCP client in LAN_AA_POOL.

- Error : The ip helper-address statement in NAT_ROUTER is missing.

- Solution :

```
interface g0/0/0
ip helper-address 172.16.61.2
```

- Justification :

The DHCP server is configured in DHCP_ROUTER.
The DHCP_ROUTER is located in a subnet which is different from the subnet of LAN_AA_POOL.
Thus, the DHCP clients in LAN_AA_POOL will not able to obtain the IP address from the DHCP server.
The default-router statement must be configured in NAT_ROUTER to relay the DHCP messages from the DHCP clients to the DHCP server.

b) (i) NAT_ROUTER

```
ip nat inside source static 172.16.81.254 19.9.9.5

interface s0/1/0
ip nat inside

interface s0/2/0
ip nat outside
```

(ii) - Error: The NAT-POOL definition statement is missing. The public network address that can be used is 19.9.9.6 with subnet mask of /30

- Solution:

```
ip nat pool NAT_POOL 19.9.9.6 19.9.9.6 netmask 255.255.255.252
```

- Error: The ACL statement is missing for allowing all internal PCs to ping to External_PC.

- Solution:

```
access-list 1 permit icmp any host 18.8.8.10
```

- Error: The 'ip nat inside' statement is missing on interface g0/0/0 in NAT_ROUTER

- Solution:

```
interface g0/0/0
ip nat inside
```