Question 1

a) - The route of 192.168.111.0/24 is using the exit interface while the route of 192.168.121.0/24 is using next-hop address.

- The route of 192.168.111.0/24 will not involve recursive lookup process while the route of 192.168.121.0/24 may involve recursive lookup to determine which exit interface should the received packets be forwarded out.

b) (i)

```
ip route 0.0.0 0 0.0.0.0 211.7.7.14
ip route 0.0.0.0 0.0.0.0 211.7.7.10 5
```

Assume that the default static route with next-hop address 211.7.7.14 is the primary route with administrative distance of 1.
The route with next-hop address 211.7.7.10 is the backup route with administrative distance of 5 which is higher than 1, it will not become the preferred primary route.

(ii) - Act as backup route
- Backup route will take over the workload of primary route and be activated once the primary route is down.

c) (i)

```
ip route 192.168.141.0 255.255.255.0 g0/0/0 192.168.131.2
```

(ii) - Both exit interface and next-hop address are given.
- Reduce CPU and time usage since no need to do recursive lookup for finding correct exit interface to forward received packets out.
- Support multi-access connection since the next-hop address indicates where the forwarded packets should reach at.

d) R1

```
router ospf 666
network 172.16.10.0 0.0.0.127 area 0
network 172.16.10.254 0.0.0.127 area 0
network 192.168.151.0 0 0.0.3 area 0
passive-interface g0/0/1
passive-interface g0/0/0
```

R2

```
router ospf 666
network 192.168.151.0 0.0.0.3 area 0
network 172.16.20.0 0.0.0.7 area 0
network 172.16.20.8 0.0.0.7 area 0
default-information originate
passive-interface s0/1/1
passive-interface g0/0/1
passive-interface g0/0/0
```

Question 2

a) (i) - Overwhelming quantity of traffic

↳ Sends large quantity of data at a rate that the network, host or application cannot handle.

↳ Causes transmission and response times to slow down, even crash a device or service.

- Maliciously formatted packets

↳ Sends a maliciously formatted packet to a host or application and the receiver is unable to handle it.

↳ It causes the receiving device to run very slowly or crash

(ii) - A Distributed DoS Attack (DDoS) is more serious to an enterprise.

- DDoS Attack will coordinate huge amount of device sources to send huge amount of data and packets to a single host or application.

- This will immediately exhaust all the resources of the receiver, and causing the server or application unable to be accessed by legitimate users

b) (i) BETA Router

```
ip access-list standard TELNET_ACCESS
permit host 172.16.4.7
deny any

line vty 0 4
access-class TELNET_ACCESS in
```

(ii) GAMMA Router

```
access-list 177 permit icmp 172.16.2.128 0.0.0.127 10.11.12.0 0.0.0.254
access-list 177 permit tcp 172.16 2.0 0.0.0.127 host 10.11.12.129 eq www
access-list 177 deny ip any any

interface g0/0/1
ip access-group 177 in
```

Question 3

a) - Error : The IP address of default gateway at ICT router is not excluded from the pool of addresses.

- Solution :

```
ip dhcp excluded-address 10.200.10.1
```

- Justification :

The default gateway of the ICT-DEPT network is using fixed or static IP address for routing packets from one network to another network. So, it shoud be excluded from the DHCP address pool.

- Error : The IP address of Web_DNS_Server is not excluded from the address pool.

- Solution :

```
ip dhcp excluded-address 10.200.10.254
```

- Justification :

Web_DNS_Server is a DNS server that is using static or fixed address for easily accessed by internal devices. Thus, the IP address of DNS server must be excluded from the DHCP address pool to avoid from being distributed to other DHCP clients.

- Error : Network command is missing in the configuration of ICT_DEPT pool.

- Solution :

```
ip dhcp pool ICT_DEPT
network 10.200.10.0 255.255.255.0
```

- Justification.

The network statement defines the range of available addresses in 10.200.10.0/24 network.

- Error : The default-router statement in ICT_DEPT pool configuration is missing.

- Solution :

```
ip dhcp pool ICT_DEPT
 default-router 10.200.10.1
```

- Justification:

  The default gateway at ICT router is used for routing the packets from ICT_DEPT network to other network.

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

- Solution:

```
interface g0/0/0
ip helper-address 10.200.20.2
```

- Justification:

  The DHCP server is configured at DHCP_NAT router while the router is located in a network different from DHCP clients' located network.

  The DHCP client will unable to obtain the IP addresses from the DHCP server.

  The ICT router should be configured with ip helper-address statement to relay the DHCP message from DHCP clients to the DHCP server.

b) (i) DHCP_NAT Router

```
ip nat inside source static 10.200.10.254 194.2.2.2

interface s0/2/0
ip nat inside

interface s0/1/1
ip nat outside
```

(ii) - Error: The NAT pool configuration in DHCP_NAT router is missing, the NAT pool should use the 194.2.2.2/30 as the inside global address.

- Solution:

```
ip nat pool NAT_POOL 194.2.2.2 194.2.2.2 netmask 255.255.255.252
```

- Error: The statement for binding the ACL to the NAT pool in DHCP_NAT router is missing.

- Solution:

```
ip nat inside source list 9 pool NAT_POOL overload
```