

Troubleshooting Lab

Q1. PC 110 cannot access R7/R8, fix the problem so that PC 110 can ping R7

Q2. R17 should have one default route which points to R12 via PPP as shown below

```
R17# sh ip route
S* 0.0.0.0/0 via 202.34.7.25
172.16.0.0/16 is variable subnetted, 4 subnets, 3 masks
C 172.16.3.56/30 is directly connected, ethernet 0/0
L 172.16.3.57/32 is directly connected, ethernet 0/0
C 172.16.3.88/29 is directly connected via Tunnel 0
L 172.16.3.90/32 is directly connected via Tunnel 0
  202.34.7.0/32 is subnetted. 2 subnets
C 202.34.7.25 is directly connected via Serial 1/0
C 202.34.7.26 is directly connected via Serial 1/0
```

Q3. When R1 tries to access the network 134.56.78.48/29 which is between R21 and R22, the traffic should be load balanced as shown in the exhibit.

```
R1# traceroute 134.56.78.49

1. 123.45.67.25 {mpls: label 26 exp 0} 0 msec
   123.45.67.33 [mpls : label 30 exp 0] 0 msec
   123.45.67.25 [mpls: label 26 exp 0] 0 msec
2. 123.45.67.17 0msec
   123.45.67.1 0 msec
   123.45.67.17
```

Q4. Traffic from R11 destined to loopback 0 of R14 should be load balanced via EIGRP as shown in the exhibit.

```
R11# traceroute 123.14.14.14

1. 203.34.7.2
   203.34.7.13
   203.34.7.2
2. 203.34.7.9
   203.34.7.6
```

Q5. When R12 traces the following routes

194.1.0.0/24

194.1.1.0/24

194.1.2.0/24

194.1.3.0/24

it should get the same result as shown in the following exhibit

R12# traceroute 194.1.0.1

```
1. 202.12.5.1
   202.12.5.2
   202.12.5.1
2. 123.45.67.57 [AS 12345] [MPLS: Label 27 Exp 0]
   123.45.67.49 [AS 12345] [MPLS: Label 27 Exp 0]
   123.45.67.57 [AS 12345] [MPLS: Label 27 Exp 0]
3. 123.45.67.41 [AS 12345] [MPLS: Label 27 Exp 0]
4. 123.45.67.33 [AS 12345] [MPLS: Label 28 Exp 0]
5. 123.45.67.17
6. 123.10.1.5
```

.....
R12# traceroute 194.1.1.1

```
1. 202.12.5.1
   202.12.5.2
   202.12.5.1
2. 123.45.67.57 [AS 12345] [MPLS: Label 25 Exp 0]
   123.45.67.49 [AS 12345] [MPLS: Label 25 Exp 0]
   123.45.67.57 [AS 12345] [MPLS: Label 25 Exp 0]
3. 123.45.67.41 [AS 12345] [MPLS: Label 25 Exp 0]
4. 123.45.67.25 [AS 12345] [MPLS: Label 26 Exp 0]
5. 123.45.67.1
6. 123.10.1.1
```

.....
R12# traceroute 194.1.2.1

```
1. 202.12.5.1
   202.12.5.2
   202.12.5.1
2. 123.45.67.57 [AS 12345] [MPLS: Label 27 Exp 0]
   123.45.67.49 [AS 12345] [MPLS: Label 27 Exp 0]
   123.45.67.57 [AS 12345] [MPLS: Label 27 Exp 0]
3. 123.45.67.41 [AS 12345] [MPLS: Label 27 Exp 0]
4. 123.45.67.33 [AS 12345] [MPLS: Label 28 Exp 0]
5. 123.45.67.17
```

6. 123.10.1.5

.....
R12# traceroute 194.1.3.1

```
1. 202.12.5.1
   202.12.5.2
   202.12.5.1
2. 123.45.67.57 [AS 12345] [MPLS: Label 27 Exp 0]
   123.45.67.49 [AS 12345] [MPLS: Label 27 Exp 0]
   123.45.67.57 [AS 12345] [MPLS: Label 27 Exp 0]
3. 123.45.67.41 [AS 12345] [MPLS: Label 27 Exp 0]
4. 123.45.67.33 [AS 12345] [MPLS: Label 28 Exp 0]
5. 123.45.67.17
6. 123.10.1.5
```

Q6.PC 103 is not able to ping 2001:0::26/128 located on R26, fix the problem so that the following is successful.

PC 103 # ping 2001:0::26
!!!!

Q7.DMVPN is configured on R15,17,18 and 19. R15 is hub and rest of devices are spokes. fix the problem so that

server 2 can access PC 107 as shown below

Server2# ping 172.16.3.58
!!!!

PC108# traceroute 17.16.3.82

```
1. 172.16.3.65
2. 172.16.3.89
3. 172.16.3.92
4. 172.16.3.82
```

Q8.MPLS/VPN

R7 and R8 are configured as backbone for VPN network. R9, R10, PC 104 and PC 106 are VPN clients. ensure that the output matches the following exhibit.

PC104# ping 172.16.2.18
!!!!

PC104# traceroute 172.16.2.18

1. 172.16.1.9
2. 172.16.1.1
3. 123.61.1.1
4. 123.45.67.34 [mpls: label 22/16]
5. 123.61.1.2 [mpls: label 16]
6. 123.61.1.1
7. 123.61.1.2
8. 123.45.67.26 [mpls: label 19/16]
9. 123.45.67.42 [mpls: label 19/16]
10. 123.61.2.1 [mpls: label 16]
11. 123.61.2.2
12. 172.16.2.2
13. 172.16.2.18

R1# sh bgp vpnv4 unicast all

RD: 12345:12345

*>i 0.0.0.0 123.3.3.3 0 100 0 61000 i

*i 123.4.4.4 0 100 0 61000 i

*>i 123.61.0.0/30 123.3.3.3 0 100 0 61000 i

*>i 172.9.9.9/32 123.5.5.5 0 100 0 61001 ?

*>i 172.10.10.10/32 123.6.6.6 0 100 0 61002 ?

*>i 172.16.1.0/30 123.5.5.5 0 100 0 61001 ?

*>i 172.16.1.8/30 123.5.5.5 11 100 0 61001 ?

*>i 172.16.2.0/30 123.6.6.6 0 100 0 61002 ?

*>i 172.16.1.8/30 123.5.5.5 11 100 0 61001 ?

*>i 172.16.2.0/30 123.6.6.6 0 100 0 61002 ?

Q9.R21 should manage NAS via telnet. Fix the problem so that telnet to NAS is successful as shown in exhibit.

R21# telnet 202.123.1.1 2323

trying 202.123.1.1, 2323....Open

user access vderification

password:

NAS>

Q10.There is DMVPN configured between R7 (Hub) and R24 (Spoke) via Nat Network (R23). ensure that PC 109 can access server 1 as shown.

PC109# ping 172.16.0.50

!!!!

PC109# traceroute 172.16.0.50

1. 10.1.1.2

2. 172.16.0.54
3. 172.16.0.10
4. 172.16.0.50

Diagnostics Tickets

Q1.Missing connectivity after replacement of SW3

Answer -> [sho ip int bri] + [ask the mac-address of host]

Q2.DMVPN + EIGRP Flapping

Answer -> [select the hub router] + [supress the EIGRP advertisement from all spoke router]

Q3.BGP Routing Policy

Drag and Drop + Drop Down List

Configuration Lab

SECTION 1.1

Configure the ACME Headquarters network (AS 12345) as per the following requirements.

- The VTP domain must be set to CCIE
- Use VTP ver 2
- SW1 must be the VTP server and SW2 must be the VTP client
- Secure all VTP updates with an MD5 digest of the ASCII string "CCIErocks\$"
- In order to avoid as much as possible unknown unicast flooding in all vlans the administrator requires that any dynamic entries learned by other SW1 and SW2 must be retained for 2 hours before being refreshed.

Configure the network of the New York office (AS 34567) as per the following requirements

- The VTP domain must be set to CCIE
- Use VTP ver 2
- SW3 and SW4 must not advertise their vlan config but must forward VTP advertisement that they receive out their trunk ports
- Secure all VTP updates with an MD5 digest of the ASCII string "CCIErocks\$"

SECTION 1.2 - Layer 2 ports

Configure your network as per the following requirements.

- Complete the config of all vlans so that all routers that are located in ACME's headquarters (AS12345) and New York office (AS 34567) can ping their directly connected neighbors
- All four switches (SW1-SW4) must have dot1q trunks that do not rely on negotiation do not configure any etherchannel
- Ensure that the following unused ports on all four switches are shutdown and configured as access ports in vlan 999

E3/0 - E3/3 are unused on SW1 and SW2

E1/0 - E1/3 are unused on SW3 and SW4

E3/0 - E3/3 are unused on SW3 and SW4

Section 1.3 Spanning tree**Configure the ACME network as per the following requirements**

- SW1 must be the root switch for all odd vlans and must be the backup for all even vlans
- SW2 must be the root switch for all even vlans and must be the backup for all odd vlans
- SW3 must be the root switch for all odd vlans and must be the backup for all even vlans
- SW4 must be the root switch for all even vlans and must be the backup for all odd vlans
- Explicitly configure the root and backup roles, assuming that other switches with default configuration may eventually be added in the network in the future
- All switches must maintain one STP instance per vlan
- Use the STP mode that has only three possible states
- All access ports must immediately transitioned to the forwarding state upon link up and they must still participate in STP. use single command per switch to enable this
- Access ports must automatically shut down if they receive any BPDU and an administrator must still manually re-enable the port. use a single command per switch to enable this feature.

Section 2.1 OSPF in AS12345**Configure OSPFv2 area 0 in ACME HQ (AS12345) according to the following requirements**

- Configure the OSPF process id to 12345 and set the router id to interface lo0 on all seven routers
- The interface lo0 at each router must be seen as an internal OSPF prefix by all other routers
- Ensure that OSPF is not running on any interface that is facing another AS. use any method to accomplish this requirement
- SW1 and SW2 must not participate in routing at all
- Do not change the default OSPF cost of any interface in AS12345
- R1 must see the following OSPF routes in the routing table

R1# sh ip route OSPF

123.0.0.0/8 is variably subnetted, 17 subnets, 2 masks

- O 123.2.2.2/32 [110/21] via 123.10.1.1 4d20h ethernet e0/2
- O 123.3.3.3/32 [110/21] via 123.10.1.6 4d20h ethernet e0/1
- O 123.4.4.4/32 [110/21] via 123.10.1.1 4d20h ethernet e0/2
- O 123.5.5.5/32 [110/21] via 123.10.1.6 4d20h ethernet e0/1
- O 123.6.6.6/32 [110/21] via 123.10.1.1 4d20h ethernet e0/2
- O 123.7.7.7/32 [110/21] via 123.10.1.6 4d20h ethernet e0/1
- O 123.10.1.8/30 [110/30] via 123.10.1.6 4d20h ethernet e0/1
[110/30] via 123.10.1.1 4d20h ethernet e0/2
- O 123.10.1.12/30 [110/20] via 123.10.1.6 4d20h ethernet e0/1
- O 123.10.1.16/30 [110/20] via 123.10.1.1 4d20h ethernet e0/2
- O 123.10.1.20/30 [110/20] via 123.10.1.1 4d20h ethernet e0/2
- O 123.10.1.24/30 [110/30] via 123.10.1.6 4d20h ethernet e0/1
[110/30] via 123.10.1.1 4d20h ethernet e0/2
- O 123.10.1.28/30 [110/20] via 123.10.1.6 4d20h ethernet e0/1

SECTION 2.2 - EIGRP IN AS34567

Configure EIGRP for ipv4 in the New York office (AS34567) according to the following requirements

- The EIGRP AS is 34567
- The interface lo0 must be seen as an internal EIGRP prefix by all other routers
- Ensure the EIGRP is not running on any interface that is facing another AS use any method to accomplish this
- Using a single command on one switch only ensure that R8 installs two equal-cost route for the following three path

vlan 411

int lo0 at SW4

int lo0 at R11

- Using a single command on one switch only ensure that R9 installs two equal cost route for the following three path

vlan 310

int lo0 at SW3

int lo0 at R10

SECTION 2.3 - EIGRP IN AS45678

Configure EIGRP in AS45678 according to the following requirements

- The EIGRP AS is 45678
- The interface lo0 must be seen as an internal EIGRP prefix by all other routers
- Ensure the EIGRP is not running on any interface that is facing another AS use any method to accomplish this requirement

- Sw5 and sw6 are layer 3 switches and must configure EIGRP
- On all three routers R15, 16, 17 use EIGRP with 64bit version
- Do not change the interface bandwidth on any physical interface in AS 45678

Section 2.4 EIGRP in AS 65222

- The EIGRP AS is 45678
- The interface lo0 at each router must be seen as an internal EIGRP prefix by all other routers
- Ensure that EIGRP is not running on any interface that is facing another AS use any method to accomplish this requirement
- R17 is the DMVPN hub, R18, R19 as the spoke, use the pre-config tunnel 0

Section 2.5 BGP in AS 12345

BGP is partially configured in ACME headquarters, complete the config as required

Configure the BGP in ACME's HQ (AS 12345) according to the following requirements

- R4 and R5 must not establish any BGP session at any time
- All BGP routers must use their int lo0 as their router-id
- Disable the default ipv4 unicast address family for peering session establishment in all BGP routers
- R1 must be the ipv4 route-reflector for BGP AS12345

Configure eBGP between ACME's San Francisco and San Jose sites according to the following requirements

- R20 is the CE router and used eBGP to connect to the manages services that are provided by the PE routers R2 and R3
- R20 must establish separate eBGP peerings with both R2 and R3 for every V
- R20 must advertise the following prefix to all the BGP peers
123.0.0.0/8 summary-only
10.0.0.0/8 summary-only
- R20 must advertise a default route to all of its BGP peers except to 10.120.99.1 and 10.120.99.5

Section 2.6 BGP in AS 34567

BGP is partially pre-configured in ACME New York office, complete the config as required

Configure IBGP in AS 34567 according to the following requirements

- SW3 and SW4 must not establish any BGP session at any time
- All BGP routers must use their int lo0 as their router-id
- Configure full mesh IBGP peering between all four routers use any configuration method
- R9 must be selected as the preferred exit point for traffic destined to remote AS's
- R11 must selected as the next preferred exit in case R9 fails
- No BGP speaker must use network statement under the BGP router config.
- Ensure that all the BGP nexthop is never marked as unreachable as long as int lo0 of the remote peer is known via IGP

Configure EIGRP in AS 34567 according to the following requirements

- All four BGP routers must establish eBGP peerings with their neighboring AS as shown in diagram 3 (BGP topology)
- All four BGP routers must redistribute EIGRP into BGP
- Ensure that R9 is the only router that sees the default as a BGP route and that all other routers (R8, R10, R11) see it as an EIGRP external

Section 2.7 BGP in AS 45678 and 65222

refer to diagram 3 (BGP routing)

configure EBGP in ACME's APAC region (AS45678 and AS 65222) according to the following requirements

- SW5 and SW6 must not establish any BGP session at any time
- All BGP routers must use their int lo0 as their router-id
- No iBGP peering sessions are allowed in AS AS45678
- R15 must establish an EBGP peering with AS 10003 and must receive default route as well as other prefix.
- R15 must redistribute BGP into EIGRP and vice versa
- R15 must also advertise an aggregate prefix 123.20.1.0/24 to AS 1003 and must suppress all component prefixes
- R16, 17, 18, 19 must establish an eBGP peering with AS 20003 and must receive a default route as well as other prefix
- R15, 17, 18, 19 must not advertise any prefix to AS 20003
- As long as R15 is operational, R16, R17, R18, R19 must prefer the EIGRP default route over the EBGP default route
- Do not create any VRF anywhere in order to accomplish the above requirements

Section 2.8 BGP routing policies

Configure the ACME network as per the following requirements

- All ACME border routers in AS 12345 must filter the BGP prefixes that are advertised to their SP in VRF INET and must allow all prefixes that belong to class A 123.0.0.0/8 and all other VRF's must propagate all prefix
- All ACME border routers in AS 12345 must filter the BGP prefixes that are advertised to their SP and must allow only all prefixes that belong to the class A 123.0.0.0/8
- Do not use any route-map or access-list to accomplish the above requirements
- R13 must route traffic preferably via AS 20002, use any method to accomplish this requirement
- All three remote sites in AS 65111 must be able to ping 1.2.3.4 and traceroute must reveal the exact same path as shown in the following output

R12# ping 1.2.3.4 so lo0

!!!!

R12# traceroute 1.2.3.4 so lo0

1. 201.1.12.1 [AS 65112]

2. 201.1.123.2 [AS 65112]
3. 10.120.12.1 [AS 65112] [MPLS: label 135 EXP 0]
4. 10.120.12.2 [AS 65112]
5. 10.120.99.5 [AS 65112]
6. 102.2.123.1 [AS 65112]
7. 33.10.2.1 [AS 65112]

Section 2.9 IPV6 OSPF

Configure OSPFv3 in the ACME New York office as per the following requirements

- Configure the OSPF process id 1 and set the router-id as interface lo0
- Sw4 must be selected as the DR on vlan 34 and must have the best chance
- Sw3 must be selected as the backup DR on vlan 34 and must take over DR if SW4 is down

Section 2.10 BGP for IPV6

Configure ACME network as per the following requirements

- Establish the four eBGP peering as indicated on "diagram IPV6 routing"
- Do not use the network command under the BGP address-family ipv6 on either R10 or R11
- Both regional SP will advertise the necessary prefixes
 - Advertise the ipv6 prefix on interface E0/0 into BGP on both R12 and R14
- Configure your network such that any ipv6 that any user can communicate with any ipv6 user that is located and vice versa
- Do not use any static route or default route anywhere
- Use the following ping to verify your config

R12# ping 2001:CC1E:BEF:14:10:1:14::1 so E0/0
!!!!

Section 2.11 Layer 3 multicast

Streaming server is connected in vlan 5 on sw5. Receivers are located at the DMVPN spokes R18 and R19.

Configure the ACME network as per the following requirements

- Only network segments with active receivers that explicitly require the data must receive the multicast traffic
- Interface lo0 of R15 must be configured as RP
- Use a standard method of dynamically distributing the RP
- Both R16 and R17 must participate in the multicast routing
- To test configure int E0/0 of both R18 and R19 to join group 232.1.1.1

Sw5# ping 232.1.1.1 so vlan 5
reply to request 0 from 10.2.19.1 3ms

reply to request o from 10.2.18.1 4ms

Section 3 VPN Technology

Refer to "diagram 3 BGP topology" and "diagram 4 VPN technology"

- The ACME HQ network (AS12345) uses MPLS L3VPN in order to clearly separate remote site networks
- The ACME corporate security policies are centralized and enforced at the San Jose site (AS 65112) for all remote sites. the policies require that all traffic that is originated from any remote sites (with the exception of New York office)
- Configure mpls L3 VPN in the ACME network according to the following requirements
- Enable ldp only on required interfaces on all seven routers in AS 12345
- Use the interface lo0 to establish ldp peerings
- Ensure that no mpls interface that belongs to any router ins AS12345 is visible on a trace route that originates outside of the AS
- R2, R3, R6 and R7 must be configured as PE routers
- R1, R4 and R5 must be configured as P routers

3.2 MPLS VPN part 2

Refer to "diagram 3 BGP topology" and "diagram 4 VPN technology"

The global and regional service providers have agreed to transport the ACME VPN via PE to PE eBGP peering that are already preconfigured. Complete all the config of mpls L3 VPN in the ACME network according to the following requirements

- R1 must reflect VPNv4 prefixes from any PE to any other PE in AS 12345
- R2 and R3 must establish eBGP peering with both global SP (As 10001 and AS 10002) for the following VRF's

BLUE
GREEN
RED
YELLOW
INET

- R3 must establish an eBGP peering with the regional SP (AS 20001) for the following VRFs

GREEN
BLUE
INET

- R7 must establish an eBGP peering with the regional SP (AS 20002) for the following VRFs

BLUE
RED
INET

- All ip add used for eBGP peering must pass the BGP's directly connected check
- No BGP speaker is AS 12345 may use the network or redistribute statement under any address-family of the BGP router config
- At the end of the exam scenario the interface E0/0 of the gateway router in any remote site must be able to connect to the int E0/0 of any other remote gateway that belongs to AS 65111 or AS 65222
- Use the following tests as examples of connectivity checks

R12# ping 10.2.19.1 so E0/0
!!!!

R12# trace 10.2.19.1 so E0/0
(10 hops)

3.3 DMVPN

Configure DMVPN phase 3 in the ACME APAC region (AS 45678 and 65222) as per the following requirements

- Use the preconfigured interface tunnel 0 on all the three routers in order to accomplish this task
- R17 must be the hub router
- R18 and R19 must be the spoke and must participate in NHRP information exchange
- Disable send icmp redirect message on all three tunnel interfaces
- Configure the following parameters on all the three tunnel interfaces

bandwidth 1000 kbps
delay 10000 msec
mtu 1400 bytes
tcp mss 1380

- Authenticate NHRP using the string 45678key
- Use NHRP network-id 45678
- Config NHRP hold time to 5 min
- Ensure that spoke to spoke traffic does not transit via the hub

3.4 DMVPN Encryption

Refer to "Diagram 4 VPN technology"

Secure the DMVPN tunnel using IPSEC according to the following requirements

- configure IKE phase 1 as per the following

Use AES encryption with the pre-shared key CCIE

The key must appear in plain text in the config

All IPSEC tunnels must be authenticated using the same IKE phase 1 pre-shared key

Use 1024 bits for the key exchange using the Diffie-Hellman algorithm

- configure a single policy using priority 10
- config IKE phase 2 as per the following requirements
 - use CCIEXFORM as transform set name
 - use DMVPNPROFILE as IPSEC profile name
 - use IPSEC in transport mode
 - use the IPSEC protocol ESP and algorithm AES with 128 bits
- Ensure that the DMVPN cloud is secured using above parameters. use tunnel protection in your config

Section 4 Infrastructure security

4.1 Device security

- Configure R20 int the ACME San Jose office as per the following
- All users who connect to R20 via the console or via any of VTY lines using SSH must be prompted with the below message before any other prompt is displayed

WARNING!ACCESS RESTRICTED

- Do not use any other spaces or any other characters

4.2 Network Security

Configure ACME New York office as per the following

- Ensure that int E0/0-3 of Sw3 forward the traffic send from expected and legitimate users only
- Sw3 must dynamically learn only one mac address per port and must save the mac address in its startup config
- Sw3 must shut down the port if security violation occurs on any of the four ports

SECTION 5 Infrastructure Services

5.1 System management

- Configure R20 int the ACME San Jose office as per the following
- Establish SSH access in R20 using the domain name acme.org
- R20 must accept up to five remote authorized users to connect at the same time using SSH
- Create the user "test" with password "test" in local database of R20
- Ensure that R20 accepts SSH connections with clients with source ip in 123.10.2.0/24. All other source ip should be denied. Use standard ACL to accomplish this

- R20 must generate a syslog message for all SSH connection attempts whether permitted or denied
- When authenticate the username test must be granted privilege level 1
- Do not enable aaa new model on R20
- Ensure that SSH is the only remote access method permitted on VTY lines of R20
- Ensure that the console is not affected by your solution and no username prompt is presented on the console port
- Test your solution from any device that is located in AS 34567 and ensure that the following sequence of command produce the following output

R10 # ssh -l 123.20.20.20

WARNING!ACCESS RESTRICTED

R20>

R20>sh privilege

current privilege level is 1

R20>

R20>q

R10#

5.2 Network Services

Configure the ACME network as per the following

- R20 must enable all private corporate traffic that is originated from any host with source ip address 10.1.0.0/16 or 10.2.0.0/16 to connect to any public destination that is located in AS 34567
- All remote sites in AS 65111 and 65222 must be able to connect to the public destinations
- R20 must swap the source ip address in these packets with the ip address of its lo0
- R20 must allow multiple concurrent connections
- Use a standard ACL to accomplish this.
- The following tests must succeed after the above requirements (in addition to previous requirements) are achieved

R12# ping 1.2.3.4 so E0/0

!!!!

R18# ping 1.2.3.4 so E0/0

!!!!

5.3 Network Optimization

Configure R17 as per the following requirements

- The output shown below must be seen on R19 during 10 sec after R15 successfully pings interface lo0 of R19

```
R15# ping 123.19.19.19
!!!!
```

```
R17 sh ipflow top
```

```
srcif  srcipadd  destif  destipadd  pr  srcp  dstp  byte
e0/1   123.20.1.9  tun0    123.19.19.9  01   000   000 500
```

5.4 Network Services

Configure ACME as per the following requirements

- Sw3 must provide an authoritative time source to the ACME network
- R10 and R12 must sync their clock to Sw3 using ntpv4 for ipv6
- R10 and R12 must operate in client mode
- Sw3 must not capture or use any time info that is sent by R12 and R14
- All NTP traffic must be sourced and destined to interface lo0 of the corresponding devices