Task 1.1

R4:

```
interface Serial0/0/0
 frame-relay interface-dlci 405
  class DLCI_405
!
map-class frame-relay DLCI_405
 frame-relay end-to-end keepalive mode bidirectional
```

R5:

```
interface Serial0/0/0.54 point-to-point
backup interface Serial0/1/0
frame-relay interface-dlci 504
class DLCI_504
!
map-class frame-relay DLCI_504
frame-relay end-to-end keepalive mode bidirectional
!
interface Serial0/1/0
  clock rate 64000
```

Task 1.1 Verification

```
Rack1R5#show frame-relay end-to-end keepalive

End-to-end Keepalive Statistics for Interface Serial0/0 (Frame Relay
DTE)

DLCI = 504, DLCI USAGE = LOCAL, VC STATUS = ACTIVE (EEK UP)

SEND SIDE STATISTICS

Send Sequence Number: 1,        Receive Sequence Number: 2
Configured Event Window: 3,     Configured Error Threshold: 2
Total Observed Events: 4,       Total Observed Errors: 0
Monitored Events: 3,            Monitored Errors: 0
Successive Successes: 3,        End-to-end VC Status: UP

RECEIVE SIDE STATISTICS

Send Sequence Number: 2,        Receive Sequence Number: 1
Configured Event Window: 3,     Configured Error Threshold: 2
Total Observed Events: 4,       Total Observed Errors: 0
Monitored Events: 3,            Monitored Errors: 0
Successive Successes: 3,        End-to-end VC Status: UP
```

```
Rack1R5#show backup
Primary Interface   Secondary Interface   Status
-----------------   -------------------   ------
Serial0/0.54        Serial0/1             normal operation
```

To verify this task simulate a link fault:

```
Rack1R4(config)#interface s0/0
Rack1R4(config-if)#shutdown

Rack1R5#debug backup
Backup events debugging is on
BACKUP(Serial0/0.54): event = primary interface went down
BACKUP(Serial0/0.54): changed state to "waiting to backup"
BACKUP(Serial0/0.54): event = timer expired on primary
BACKUP(Serial0/0.54): secondary interface (Serial0/1) made active
BACKUP(Serial0/0.54): changed state to "backup mode"
%LINK-3-UPDOWN: Interface Serial0/1, changed state to up
BACKUP(Serial0/1): event = secondary interface came up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1, changed
state to up
BACKUP(Serial0/1): event = secondary interface came up

Rack1R5#show backup
Primary Interface   Secondary Interface   Status
-----------------   -------------------   ------
Serial0/0.54        Serial0/1             backup mode
```


Task 2.1

R1:

```
interface FastEthernet0/0
 ip ospf network point-to-multipoint
!
router ospf 1
 network 173.1.137.1 0.0.0.0 area 137
```

R3:

```
interface FastEthernet0/0
 ip ospf network point-to-multipoint
!
router ospf 1
 network 173.1.137.3 0.0.0.0 area 137
```

SW1:

```
ip routing
!
interface Vlan137
 ip ospf network point-to-multipoint
!
router ospf 1
 router-id 150.1.7.7
 network 173.1.137.7 0.0.0.0 area 137
 neighbor 173.1.137.3 cost 10
 neighbor 173.1.137.1 cost 1
```


Task 2.1 Verification

```
Rack1SW1#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
150.1.1.1         0   FULL/  -        00:01:39    173.1.137.1     Vlan137
150.1.3.3         0   FULL/  -        00:01:50    173.1.137.3     Vlan137

Rack1SW1#show ip ospf interface vlan 137
Vlan137 is up, line protocol is up
  Internet Address 173.1.137.7/24, Area 137
  Process ID 1, Router ID 150.1.7.7, Network Type POINT_TO_MULTIPOINT,
Cost: 1
  Transmit Delay is 1 sec, State POINT_TO_MULTIPOINT,
  Timer intervals configured, Hello 30, Dead 120, Wait 120,Retransmit 5
    oob-resync timeout 120
    Hello due in 00:00:04
  Supports Link-local Signaling (LLS)
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 2, Adjacent neighbor count is 2
    Adjacent with neighbor 150.1.1.1, cost is 1
    Adjacent with neighbor 150.1.3.3, cost is 10
  Suppress hello for 0 neighbor(s)

Rack1SW1#show ip route ospf
     173.1.0.0/16 is variably subnetted, 6 subnets, 2 masks
O       173.1.137.1/32 [110/1] via 173.1.137.1, 00:02:15, Vlan137
O       173.1.137.3/32 [110/2] via 173.1.137.1, 00:02:15, Vlan137
O IA    173.1.32.0/24 [110/129] via 173.1.137.1, 00:02:15, Vlan137
O IA    173.1.13.0/24 [110/65] via 173.1.137.1, 00:02:15, Vlan137
O IA    173.1.125.0/24 [110/65] via 173.1.137.1, 00:02:15, Vlan137
     150.1.0.0/16 is variably subnetted, 5 subnets, 2 masks
O IA    150.1.5.5/32 [110/66] via 173.1.137.1, 00:02:15, Vlan137
O IA    150.1.3.3/32 [110/3] via 173.1.137.1, 00:02:16, Vlan137
O IA    150.1.2.2/32 [110/66] via 173.1.137.1, 00:02:16, Vlan137
O IA    150.1.1.1/32 [110/2] via 173.1.137.1, 00:02:16, Vlan137
```

Task 2.2

R2:

```
router ospf 1
 network 173.1.23.2 0.0.0.0 area 23
```

R3:

```
router ospf 1
 network 173.1.23.3 0.0.0.0 area 23
```

SW1:

```
router ospf 1
 redistribute connected subnets route-map CONNECTED2OSPF
!
route-map CONNECTED2OSPF permit 10
```



```
 match interface Loopback0
```

SW2:

```
ip routing
!
router ospf 1
 router-id 150.1.8.8
 network 173.1.8.8 0.0.0.0 area 23
 redistribute connected subnets route-map CONNECTED2OSPF
 network 173.1.23.8 0.0.0.0 area 23
!
route-map CONNECTED2OSPF permit 10
 match interface Loopback0
```

Task 2.2 Verification

```
Rack1SW2#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
150.1.2.2         1   FULL/BDR        00:00:37    173.1.23.2      Vlan23
150.1.3.3         1   FULL/DR         00:00:39    173.1.23.3      Vlan23

Rack1R5#show ip route ospf
     173.1.0.0/16 is variably subnetted, 10 subnets, 2 masks
O IA    173.1.137.7/32 [110/65] via 173.1.125.1, 00:02:15,
Serial0/0.125
O IA    173.1.137.1/32 [110/64] via 173.1.125.1, 00:02:15,
Serial0/0.125
O IA    173.1.137.3/32 [110/65] via 173.1.125.1, 00:02:15,
Serial0/0.125
O       173.1.32.0/24 [110/128] via 173.1.125.2, 00:02:15,
Serial0/0.125
O       173.1.13.0/24 [110/128] via 173.1.125.1, 00:02:15,
Serial0/0.125
O IA    173.1.8.0/24 [110/66] via 173.1.125.2, 00:00:59, Serial0/0.125
O IA    173.1.23.0/24 [110/65] via 173.1.125.2, 00:01:13, Serial0/0.125
     150.1.0.0/16 is variably subnetted, 6 subnets, 2 masks
O E2    150.1.7.0/24 [110/20] via 173.1.125.1, 00:00:54, Serial0/0.125
O       150.1.3.3/32 [110/129] via 173.1.125.2, 00:02:15, Serial0/0.125
                     [110/129] via 173.1.125.1, 00:02:15, Serial0/0.125
O       150.1.2.2/32 [110/65] via 173.1.125.2, 00:02:15, Serial0/0.125
O       150.1.1.1/32 [110/65] via 173.1.125.1, 00:02:15, Serial0/0.125
O E2    150.1.8.0/24 [110/20] via 173.1.125.2, 00:00:55, Serial0/0.125
```


Task 2.3

R5:

```
router eigrp 10
 redistribute ospf 1 metric 1500 1000 255 1 1500
 redistribute connected metric 1500 1000 255 1 1500
!
router ospf 1
 redistribute eigrp 10 metric-type 1 subnets
```

Task 2.4

SW1:

```
router ospf 1
 redistribute rip subnets
 summary-address 31.0.0.0 255.252.0.0
!
router rip
 redistribute ospf 1 metric 1
!
route-map CONNECTED2OSPF permit 20
 match interface Vlan73
```

Tasks 2.3 – 2.4 Verification

```
Rack1R1#show ip route ospf
O E2 204.12.1.0/24 [110/20] via 173.1.137.7, 00:00:08, FastEthernet0/0
     54.0.0.0/24 is subnetted, 1 subnets
O E1    54.1.2.0 [110/84] via 173.1.125.5, 00:03:22, Serial0/0
     173.1.0.0/16 is variably subnetted, 13 subnets, 2 masks
O       173.1.137.7/32 [110/1] via 173.1.137.7, 00:15:52,
FastEthernet0/0
O       173.1.137.3/32 [110/1] via 173.1.137.3, 00:15:52,
FastEthernet0/0
O E1    173.1.46.0/24 [110/84] via 173.1.125.5, 00:03:22, Serial0/0
O       173.1.32.0/24 [110/128] via 173.1.125.2, 00:03:32, Serial0/0
O E1    173.1.54.0/24 [110/84] via 173.1.125.5, 00:03:22, Serial0/0
O IA    173.1.8.0/24 [110/66] via 173.1.125.2, 00:03:32, Serial0/0
O E1    173.1.4.0/24 [110/84] via 173.1.125.5, 00:03:22, Serial0/0
O E1    173.1.5.0/24 [110/84] via 173.1.125.5, 00:03:22, Serial0/0
O IA    173.1.23.0/24 [110/65] via 173.1.125.2, 00:03:32, Serial0/0
     31.0.0.0/14 is subnetted, 1 subnets
O E2    31.0.0.0 [110/20] via 173.1.137.7, 00:00:08, FastEthernet0/0
     150.1.0.0/16 is variably subnetted, 8 subnets, 2 masks
O E2    150.1.7.0/24 [110/20] via 173.1.137.7, 00:03:23,
FastEthernet0/0
O E1    150.1.6.0/24 [110/84] via 173.1.125.5, 00:03:23, Serial0/0
O E1    150.1.4.0/24 [110/84] via 173.1.125.5, 00:03:23, Serial0/0
O       150.1.5.5/32 [110/65] via 173.1.125.5, 00:03:33, Serial0/0
O       150.1.3.3/32 [110/65] via 173.1.13.3, 00:03:33, Serial0/1
O       150.1.2.2/32 [110/65] via 173.1.125.2, 00:03:33, Serial0/0
O E2    150.1.8.0/24 [110/20] via 173.1.125.2, 00:03:23, Serial0/0
O E1 200.0.0.0/22 [110/84] via 173.1.125.5, 00:03:24, Serial0/0
```


Confirm full connectivity with the following Tcl script:

```
foreach i {
173.1.137.1
173.1.125.1
173.1.13.1
150.1.1.1
173.1.23.2
173.1.125.2
173.1.32.2
150.1.2.2
173.1.137.3
173.1.23.3
173.1.13.3
173.1.32.3
150.1.3.3
173.1.46.4
173.1.54.4
173.1.4.4
173.1.44.4
150.1.4.4
173.1.54.5
173.1.125.5
173.1.5.5
150.1.5.5
192.10.1.5
173.1.46.6
54.1.2.6
150.1.6.6
204.12.1.7
173.1.137.7
150.1.7.7
173.1.8.8
173.1.23.8
150.1.8.8
173.1.4.9
173.1.109.9
150.1.9.9
173.1.5.10
173.1.109.10
150.1.10.10
} { ping $i }
```

Task 2.5

R3:

```
router ospf 1
area 23 nssa
area 23 nssa default-information-originate
```

R2 & SW2:

```
router ospf 1
area 23 nssa
```


Task 2.5 Verification

```
Rack1SW2#show ip ospf | beg Area 23
    Area 23
        Number of interfaces in this area is 2
        It is a NSSA area
        Area has no authentication
        SPF algorithm last executed 00:00:25.260 ago
        SPF algorithm executed 7 times
        Area ranges are
        Number of LSA 27. Checksum Sum 0x0E2136
        Number of opaque link LSA 0. Checksum Sum 0x000000
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0

Rack1SW2#show ip route ospf
     173.1.0.0/16 is variably subnetted, 8 subnets, 2 masks
O IA    173.1.137.7/32 [110/11] via 173.1.23.3, 00:01:10, Vlan23
O IA    173.1.137.1/32 [110/11] via 173.1.23.3, 00:01:10, Vlan23
O IA    173.1.137.3/32 [110/1] via 173.1.23.3, 00:01:10, Vlan23
O IA    173.1.32.0/24 [110/65] via 173.1.23.2, 00:01:10, Vlan23
O IA    173.1.13.0/24 [110/129] via 173.1.23.2, 00:01:10, Vlan23
O IA    173.1.125.0/24 [110/65] via 173.1.23.2, 00:01:10, Vlan23
     150.1.0.0/16 is variably subnetted, 5 subnets, 2 masks
O IA    150.1.5.5/32 [110/66] via 173.1.23.2, 00:01:11, Vlan23
O IA    150.1.3.3/32 [110/2] via 173.1.23.3, 00:01:11, Vlan23
O IA    150.1.2.2/32 [110/2] via 173.1.23.2, 00:01:11, Vlan23
O IA    150.1.1.1/32 [110/66] via 173.1.23.2, 00:01:11, Vlan23
O*N2 0.0.0.0/0 [110/1] via 173.1.23.3, 00:01:11, Vlan23
```

Task 2.6

R1:

```
router bgp 100
 neighbor 173.1.32.2 send-community
 neighbor 173.1.125.5 route-map NO_EXPORT in
 neighbor 173.1.137.3 send-community
 neighbor 173.1.137.7 send-community
!
route-map NO_EXPORT
 set community no-export
```

R2:

```
router bgp 100
 neighbor 173.1.13.1 send-community
 neighbor 173.1.23.3 send-community
 neighbor 173.1.125.5 route-map NO_EXPORT in
 neighbor 173.1.137.7 send-community
!
route-map NO_EXPORT
 set community no-export
```

R3:


```
router bgp 100
 neighbor 173.1.23.2 send-community
 neighbor 173.1.137.1 send-community
 neighbor 173.1.137.7 send-community
```

SW1:

```
router bgp 100
 neighbor 150.1.2.2 send-community
 neighbor 173.1.137.1 send-community
 neighbor 173.1.137.3 send-community
 neighbor 204.12.1.254 route-map NO_EXPORT in
!
route-map NO_EXPORT
 set community no-export
```

Task 2.6 Verification

```
Rack1SW1#show ip bgp q _200_
BGP table version is 19, local router ID is 150.1.7.7
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*>i192.10.1.0       173.1.125.5              0    100      0 200 i
* i                 173.1.125.5              0    100      0 200 i
*>i205.90.31.0      173.1.125.5              0    100      0 200 254 ?
* i                 173.1.125.5              0    100      0 200 254 ?
*>i220.20.3.0       173.1.125.5              0    100      0 200 254 ?
* i                 173.1.125.5              0    100      0 200 254 ?
*>i222.22.2.0       173.1.125.5              0    100      0 200 254 ?
* i                 173.1.125.5              0    100      0 200 254 ?

Rack1SW1#sh ip bgp 192.10.1.0
BGP routing table entry for 192.10.1.0/24, version 20
Paths: (2 available, best #2, table Default-IP-Routing-Table, not
advertised to EBGP peer)
  Not advertised to any peer
  200
    173.1.125.5 (metric 65) from 150.1.2.2 (150.1.2.2)
      Origin IGP, metric 0, localpref 100, valid, internal
      Community: no-export
  200
    173.1.125.5 (metric 65) from 173.1.137.1 (150.1.1.1)
      Origin IGP, metric 0, localpref 100, valid, internal, best
      Community: no-export
```

Check for AS54 prefixes in AS100 BGP tables:

```
Rack1R1#show ip bgp q _54_
BGP table version is 39, local router ID is 150.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              r RIB-failure, S Stale
```



```
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*>i28.119.16.0/24   204.12.1.254             0    100      0 54 i
*>i28.119.17.0/24   204.12.1.254             0    100      0 54 i
*>i112.0.0.0        204.12.1.254             0    100      0 54 50 60 i
*>i113.0.0.0        204.12.1.254             0    100      0 54 50 60 i
*>i114.0.0.0        204.12.1.254             0    100      0 54 i
*>i115.0.0.0        204.12.1.254             0    100      0 54 i
*>i116.0.0.0        204.12.1.254             0    100      0 54 i
*>i117.0.0.0        204.12.1.254             0    100      0 54 i
*>i118.0.0.0        204.12.1.254             0    100      0 54 i
*>i119.0.0.0        204.12.1.254             0    100      0 54 i


Rack1R1#show ip bgp 28.119.16.0
BGP routing table entry for 28.119.16.0/24, version 39
Paths: (1 available, best #1, table Default-IP-Routing-Table, not
advertised to EBGP peer)
Flag: 0x820
  Not advertised to any peer
  54
    204.12.1.254 (metric 20) from 173.1.137.7 (150.1.7.7)
      Origin IGP, metric 0, localpref 100, valid, internal, best
      Community: no-export
```

Task 2.7

```
R2:
router bgp 100
neighbor 173.1.13.1 route-map WEIGHT in
!
ip as-path access-list 1 permit _254$
!
route-map WEIGHT permit 10
match as-path 1
set weight 1
set ip next-hop 173.1.13.1
!
route-map WEIGHT permit 20
```

Task 2.7 Verification

```
Rack1R2#show ip bgp q _254$
BGP table version is 35, local router ID is 150.1.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
* i205.90.31.0      173.1.125.5              0    100      0 200 254 ?
*>                  173.1.125.5                           0 200 254 ?
* i220.20.3.0       173.1.125.5              0    100      0 200 254 ?
```



```
*>                  173.1.125.5                              0 200 254 ?
* i222.22.2.0       173.1.125.5              0    100      0 200 254 ?
*>                  173.1.125.5                              0 200 254 ?

Rack1R2#show ip bgp q _254$
BGP table version is 38, local router ID is 150.1.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*>i205.90.31.0      173.1.13.1               0    100      1 200 254 ?
*                   173.1.125.5                           0 200 254 ?
*>i220.20.3.0       173.1.13.1               0    100      1 200 254 ?
*                   173.1.125.5                           0 200 254 ?
*>i222.22.2.0       173.1.13.1               0    100      1 200 254 ?
*                   173.1.125.5                           0 200 254 ?
```

Task 2.8

R5:

```
router bgp 200
 bgp scan-time 20
 bgp update-delay 12
```

Task 5.1

R4:

```
interface Tunnel47
 ip unnumbered FastEthernet0/0
 ip pim dense-mode
 tunnel source Loopback0
 tunnel destination 150.1.7.7
!
!
ip mroute 0.0.0.0 0.0.0.0 Tunnel47
```

SW1:

```
interface Tunnel47
 ip unnumbered Vlan73
 ip pim dense-mode
 tunnel source Loopback0
 tunnel destination 150.1.4.4
```

Task 5.1 Verification

```
Rack1R4#show ip pim interface

Address          Interface      Ver/   Nbr    Query  DR     DR
                                Mode   Count  Intvl  Prior
173.1.46.4       FastEthernet0/0    v2/D   0      30     1
173.1.46.4
173.1.46.4       Tunnel47       v2/D   1      30     1      0.0.0.0
```



```
Rack1SW1#show ip pim interface

Address          Interface      Ver/   Nbr    Query  DR     DR
                                Mode   Count  Intvl  Prior
204.12.1.7       Tunnel47       v2/D   1      30     1      0.0.0.0
204.12.1.7       Vlan73         v2/D   0      30     1      204.12.1.7

Rack1R4#show ip pim neighbor
PIM Neighbor Table
Mode: B - Bidir Capable, DR - Designated Router, N - Default DR
Priority,
      S - State Refresh Capable
Neighbor          Interface      Uptime/Expires    Ver   DR
Address                                                  Prio/Mode
204.12.1.7        Tunnel47       00:18:09/00:01:21 v2    1 / S
Rack1R4#show ip mroute static
Mroute: 0.0.0.0/0, interface: Tunnel47
  Protocol: none, distance: 0, route-map: none
```

Task 5.2

R4:

```
interface FastEthernet0/0
 ip igmp join-group 227.69.53.7
```

Task 5.2 Verification

```
Rack1SW1#debug ip icmp
ICMP packet debugging is on

Rack1SW1#ping 227.69.53.7

Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 227.69.53.7, timeout is 2 seconds:

03:14:20: ICMP: echo reply rcvd, src 173.1.46.4, dst 204.12.1.7
Reply to request 0 from 173.1.46.4, 104 ms
```

Task 5.3

SW1:

```
interface Tunnel47
 ip access-group MULTICAST out
!
ip access-list extended MULTICAST
 permit ip any host 227.69.53.7
 deny   ip any 224.0.0.0 15.255.255.255
 permit ip any any
```


Task 6.1

R6:

```
interface Serial0/0
 ip access-group 1 in
!
access-list 1 deny 200.0.1.2 0.0.2.24
access-list 1 permit any
```

Task 6.2

R5:

```
interface FastEthernet0/1
 rate-limit output access-group 192 496000 4000 4000 conform-action
transmit exceed-action drop
!
access-list 192 permit tcp any 173.1.5.0 0.0.0.255 eq www syn
```

Task 6.2 Verification

```
Rack1R5#show interfaces FastEthernet0/1 rate-limit
FastEthernet0/1
  Output
    matches: access-group 192
      params:  496000 bps, 4000 limit, 4000 extended limit
      conformed 0 packets, 0 bytes; action: transmit
      exceeded 0 packets, 0 bytes; action: drop
      last packet: 12704588ms ago, current burst: 0 bytes
      last cleared 00:00:35 ago, conformed 0 bps, exceeded 0 bps
```

Task 6.3

```
aaa new-model
!
aaa authentication eou default group radius
!
ip admission name CISCO eapoudp inactivity-time 60
!
interface FastEthernet0/1.44
 ip access-group 102 in
 ip admission CISCO
!
ip radius source-interface Loopback0
!
radius-server host 173.1.137.252 auth-port 1645 acct-port 1646 key
CISCO
radius-server key CISCO
```

Task 6.4

R1:


```
username Rack1R3 password 0 CISCO
!
interface Serial0/1
 encapsulation ppp
 ppp chap hostname CHAPUSER
```

R2:

```
username Rack1R3 password 0 CISCO
!
interface Serial0/1
 encapsulation ppp
 ppp chap hostname CHAPUSER
```

R3:

```
username CHAPUSER password 0 CISCO
!
interface Serial1/2
 encapsulation ppp
 clockrate 64000
 ppp authentication chap
!
interface Serial1/3
 encapsulation ppp
 clockrate 64000
 ppp authentication chap
```

Task 6.4 Verification

```
Rack1R3#ping 173.1.32.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 173.1.32.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/29/32 ms

Rack1R3#ping 173.1.13.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 173.1.13.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/59/64 ms

Rack1R3#debug ppp authentication
PPP authentication debugging is on
Rack1R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Rack1R3(config)#interface Serial1/2
Rack1R3(config-if)#shutdown
Rack1R3(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial1/2, changed state to administratively
down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/2, changed
state to down
Se1/2 PPP: Using default call direction
```

```
Se1/2 PPP: Treating connection as a dedicated
Se1/2 PPP: Session handle[96000004] Session id[1]
Se1/2 PPP: Authorization required
%LINK-3-UPDOWN: Interface Serial1/2, changed state to up
Se1/2 CHAP: O CHALLENGE id 1 len 28 from "Rack1R3"
Se1/2 CHAP: I RESPONSE id 1 len 29 from "CHAPUSER"
Se1/2 PPP: Sent CHAP LOGIN Request
Se1/2 PPP: Received LOGIN Response PASS
Se1/2 PPP: Sent LCP AUTHOR Request
Se1/2 PPP: Sent IPCP AUTHOR Request
Se1/2 LCP: Received AAA AUTHOR Response PASS
Se1/2 IPCP: Received AAA AUTHOR Response PASS
Se1/2 CHAP: O SUCCESS id 1 len 4
Se1/2 PPP: Sent CDPCP AUTHOR Request
Se1/2 CDPCP: Received AAA AUTHOR Response PASS
Se1/2 PPP: Sent IPCP AUTHOR Request
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/2, changed
state to up
```

Task 6.5

SW1:

```
interface FastEthernet0/10
switchport protected
!
interface FastEthernet0/11
switchport protected
```

Task 6.5 Verification

To verify this temporarily put ports Fa0/1 and Fa0/3 on SW1 into protected mode. Before doing this, confirm connectivity between R1 and R3:

```
Rack1R1#ping 173.1.137.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 173.1.137.3, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/2/4 ms
```

Implement protected ports:

SW1:

```
!
interface range FastEthernet 0/1 , FastEthernet 0/3
switchport protected
```

Verify new configuration:

```
Rack1R1#ping 173.1.137.3

Type escape sequence to abort.
```



```
Sending 5, 100-byte ICMP Echos to 173.1.137.3, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Confirm that you still can ping SW1:

```
Rack1R1#ping 173.1.137.7

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 173.1.137.7, timeout is 2 seconds:
..!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 1/2/4 ms
```

Task 6.6

SW1:

```
interface FastEthernet0/10
 switchport block unicast
 switchport block multicast
!
interface FastEthernet0/11
 switchport block unicast
 switchport block multicast
```

Task 6.6 Breakdown

Port protection, as configured in the previous task, is designed to prevent devices in the same broadcast domain (VLAN) from directly exchanging traffic. Typically this configuration is used in a DMZ environment to prevent compromised devices from attacking the network from within. However there is a security flaw inherent to port protection that should not be overlooked. This flaw relates to the default processing behavior of unknown unicast and multicast MAC addresses.

When a switch receives a unicast or multicast frame it looks in the CAM table to pair the destination MAC address of the frame with the outgoing port. If there is not an entry in the CAM table the frame is treated as a broadcast frame and is flooded out all ports in the VLAN except that which it was received on. This mechanism is used to assist in discovering new hosts which have not previously sent traffic into the switch block, or those which have CAM entries which have timed out. By flooding the frame to all ports in the broadcast domain it can be reasonably assumed that the destination device will respond and the switch will be able to learn the outgoing interface for said device. In the case of port protection this behavior may not be desirable.

By sending traffic to random destination unicast and multicast MAC addresses an attacker can force a switch to flood the traffic out all interfaces. In the case that this traffic is received on a protected port the resulting behavior will be to flood the traffic out all ports in the VLAN, even to those that are protected. Since the ultimate goal of port protection is to prevent ports from communicating with each

other this behavior is not acceptable. By issuing the **switchport block unicast and switchport block multicast** interface level commands these unknown unicast and multicast frames will not be forwarded out the interfaces they are configured on.

Task 6.6 Verification

```
Rack1SW1#show interfaces f0/10 switchport
Name: Fa0/10
Switchport: Enabled
Administrative Mode: dynamic desirable
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 4 (VLAN0004)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: true
Unknown unicast blocked: enabled
Unknown multicast blocked: enabled
Appliance trust: none
```

Task 6.7

SW2:

```
interface FastEthernet0/22
 switchport mode access
 switchport port-security
 switchport port-security maximum 5
 switchport port-security aging time 5
 switchport port-security violation protect
 switchport port-security aging type inactivity
!
interface FastEthernet0/23
 switchport mode access
 switchport port-security
 switchport port-security maximum 5
 switchport port-security aging time 5
 switchport port-security violation protect
```



```
 switchport port-security aging type inactivity
```

Task 6.7 Breakdown

Previous configurations have addressed the issue of limiting the amount of hosts that can access the network through a single switchport. However these configurations have not addressed the issue of port-security aging.

The above task describes a situation in which a maximum of five hosts are allowed to access the network through a specific port. Once traffic is received from a host it is added to the secure MAC address list. Once there are five addresses in the secure list traffic from all other hosts is dropped. This has been accomplished by issuing the **`maximum 5`** and **`violation protect`** port-security options. The issue with this configuration however is that once these addresses are learned they are not aged out of the table.
In order to ensure that inactive hosts are not taking up space in the secure MAC list the **`aging type inactivity`** and **`aging time 5`** options have been added to the above port-security configuration. These commands indicate that a MAC address in the secure list will expire once it has been inactive for more than five minutes.

Task 6.7 Verification

```
Rack1SW2#show port-security interface fa0/22
Port Security              : Enabled
Port Status                : Secure-down
Violation Mode             : Protect
Aging Time                 : 5 mins
Aging Type                 : Inactivity
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 5
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0

Rack1SW2#show port-security interface fa0/23
Port Security              : Enabled
Port Status                : Secure-down
Violation Mode             : Protect
Aging Time                 : 5 mins
Aging Type                 : Inactivity
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 5
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
```


Task 6.8

R4:

```
zone security WAN-Serial
 description Covers S0/0/0 and S0/1/0
exit
zone security WAN-Ethernet
 description Covers Fa0/0
exit
zone security VLAN4
 description Covers VLAN 4 (Fa0/1)
exit

interface Serial0/0/0
 zone-member security WAN-Serial
interface Serial0/1/0
 zone-member security WAN-Serial
int fa0/0
 zone-member security WAN-Ethernet
int fa0/1
 zone-member security VLAN4

class-map type inspect VLAN4Web
 match protocol http

access-list 178 permit ip any any

class-map type inspect match-all VLAN4FTP
 match protocol ftp
 match access-group 178

class-map type inspect http DeepWeb
 match request uri length gt 222

policy-map type inspect http DeepWeb
 class type inspect http DeepWeb
  reset

policy-map type inspect Serial
 class VLAN4Web
  inspect
 class VLAN4FTP
  inspect

policy-map type inspect Ethernet
 class VLAN4Web
  inspect
  service-policy http DeepWeb

zone-pair security OutSerial source VLAN4 destination WAN-Serial
 service-policy type inspect Serial
zone-pair security OutEthernet source VLAN4 destination WAN-Ethernet
 service-policy type inspect Ethernet
```


Task 6.8 Verification

```
Rack1R4#show zone security
zone self
  Description: System defined zone


zone WAN-Serial
  Description: Covers S0/0/0 and S0/1/0
  Member Interfaces:
    Serial0/0/0
    Serial0/1/0


zone WAN-Ethernet
  Description: Covers Fa0/0
  Member Interfaces:
    FastEthernet0/0


zone VLAN4
  Description: Covers VLAN 4 (Fa0/1)
  Member Interfaces:
    FastEthernet0/1

Rack1R4#show zone-pair security
Zone-pair name OutSerial
    Source-Zone VLAN4  Destination-Zone WAN-Serial
    service-policy Serial
Zone-pair name OutEthernet
    Source-Zone VLAN4  Destination-Zone WAN-Ethernet
    service-policy Ethernet

Rack1R4#show policy-map type inspect zone-pair

policy exists on zp OutSerial
 Zone-pair: OutSerial

  Service-policy inspect : Serial

    Class-map: VLAN4Web (match-all)
      Match: protocol http

   Inspect
        Session creations since subsystem startup or last reset 0
        Current session counts (estab/half-open/terminating) [0:0:0]
        Maxever session counts (estab/half-open/terminating) [0:0:0]
        Last session created never
        Last statistic reset never
        Last session creation rate 0
        Maxever session creation rate 0
        Last half-open session total 0

    Class-map: VLAN4FTP (match-all)
      Match: protocol ftp
      Match: access-group 178
```



```
   Inspect
        Session creations since subsystem startup or last reset 0
        Current session counts (estab/half-open/terminating) [0:0:0]
        Maxever session counts (estab/half-open/terminating) [0:0:0]
        Last session created never
        Last statistic reset never
        Last session creation rate 0
        Maxever session creation rate 0
        Last half-open session total 0

    Class-map: class-default (match-any)
      Match: any
      Drop
        0 packets, 0 bytes

policy exists on zp OutEthernet
 Zone-pair: OutEthernet

  Service-policy inspect : Ethernet

    Class-map: VLAN4Web (match-all)
      Match: protocol http

   Inspect
        Session creations since subsystem startup or last reset 0
        Current session counts (estab/half-open/terminating) [0:0:0]
        Maxever session counts (estab/half-open/terminating) [0:0:0]
        Last session created never
        Last statistic reset never
        Last session creation rate 0
        Maxever session creation rate 0
        Last half-open session total 0

    Class-map: class-default (match-any)
      Match: any
      Drop
        0 packets, 0 bytes
Rack1R4#
```

Task 6.9

R4:

```
access-list 179 permit ip any any
!
class-map type inspect All
 match access-group 179
!
policy-map type inspect PermitAll
  class All
    pass
!
zone-pair security WAN-WAN1 source WAN-Serial destination WAN-Ethernet
  service-policy type inspect PermitAll
zone-pair security WAN-WAN2 source WAN-Ethernet destination WAN-Serial
  service-policy type inspect PermitAll
```


Task 6.9 Verification

```
Rack1R4(config-sec-zone-pair)#do sh zone-pair sec
Zone-pair name OutSerial
    Source-Zone VLAN4  Destination-Zone WAN-Serial
    service-policy Serial
Zone-pair name OutEthernet
    Source-Zone VLAN4  Destination-Zone WAN-Ethernet
    service-policy Ethernet
Zone-pair name WAN-WAN1
    Source-Zone WAN-Serial  Destination-Zone WAN-Ethernet
    service-policy PermitAll
Zone-pair name WAN-WAN2
    Source-Zone WAN-Ethernet  Destination-Zone WAN-Serial
    service-policy PermitAll
```

Task 7.1

R4:

```
logging rate-limit 10
```

Task 7.2

SW1:

```
ip access-list standard TELNET
 permit 173.1.0.0 0.0.255.255
 permit 150.1.0.0 0.0.15.255
 permit any log
!
logging file flash:LOCAL_LOGGING.TXT informational
!
line vty 0 15
 access-class TELNET in
```

Task 7.2 Verification

Telnet to SW1 from BB3:

```
BB3>telnet 204.12.1.7
Trying 204.12.1.7 ... Open


User Access Verification

Password: <cisco>
Rack1SW1>en
Password: <cisco>
Rack1SW1#more flash:LOCAL_LOGGING.TXT | inc SEC
Cisco IOS Software, C3550 Software (C3550-IPSERVICESK9-M), Version
12.2(25)SEC2, RELEASE SOFTWARE (fc1)
```



```
03:37:41: %SEC-6-IPACCESSLOGS: list TELNET permitted 204.12.1.254 1
packet
```

Task 7.3

R5:

```
interface FastEthernet0/0
 ip nat outside
!
interface Serial0/0/0.54
 ip nat inside
!
interface Serial0/0/0.125
 ip nat inside
!
interface FastEthernet0/1
 ip nat inside
!
interface Loopback0
 ip nat inside
!
ip nat inside source list INTERNAL_NETWORK interface FastEthernet0/0
overload
!
ip access-list standard INTERNAL_NETWORK
 permit 173.1.0.0 0.0.255.255
 permit 150.1.0.0 0.0.15.255
```

Task 7.3 Verification

```
Rack1R5#show ip nat statistics
Total active translations: 0 (0 static, 0 dynamic; 0 extended)
Outside interfaces:
  FastEthernet0/0
Inside interfaces:
  Serial0/0.54, Serial0/0.125, FastEthernet0/1, Loopback0
Hits: 0  Misses: 0
CEF Translated packets: 0, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 1] access-list INTERNAL_NETWORK interface FastEthernet0/0 refcount
0
Queued Packets: 0

Rack1R4#ping 192.10.1.254

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.10.1.254, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/62/64 ms

Rack1R5#show ip nat translations
```



```
Pro Inside global      Inside local   Outside local      Outside global
icmp 192.10.1.5:4      173.1.54.4:4   192.10.1.254:4     192.10.1.254:4
```

Task 7.4

R5:

```
ip nat inside source static tcp 173.1.5.100 25 192.10.1.5 25 extendable
ip nat inside source static tcp 173.1.5.100 80 192.10.1.5 80 extendable
ip nat inside source static tcp 173.1.5.100 443 192.10.1.5 443
extendable
ip nat inside source static tcp 173.1.5.100 110 192.10.1.5 110
extendable
```

Task 7.4 Verification

```
Rack1R5#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside
global
tcp 192.10.1.5:25      173.1.5.100:25     ---                ---
tcp 192.10.1.5:80      173.1.5.100:80     ---                ---
tcp 192.10.1.5:110     173.1.5.100:110    ---                ---
tcp 192.10.1.5:443     173.1.5.100:443    ---                ---
```

Task 7.5

R1:

```
ip domain-name cisco.com
crypto key generate rsa
!
ip ssh port 2001 rotary 2
ip ssh logging events
!
line aux 0
 rotary 2
 transport input ssh
```

Task 7.6

R5:

```
Ip traffic-export profile R5-WAN
  Int f0/1
  Bidirectional
  Mac-address 0010.1731.5100
  Incoming sample one-in-every 10
  Outgoing sample one-in-every 10
Interface Serial0/0/0.54
 Ip traffic-export apply R5-WAN
Interface Serial0/0/0.125
 Ip traffic-export apply R5-WAN
Interface Serial0/1/0
 Ip traffic-export apply R5-WAN
```


Task 7.6 Verification

```
R5:
%RITE-5-ACTIVATE: Activated IP traffic export on interface Serial0/0/0
%RITE-5-ACTIVATE: Activated IP traffic export on interface Serial0/1/0

Rack1R5#show ip traffic-export
Router IP Traffic Export Parameters
Monitored Interface             Serial0/0/0
        Export Interface                FastEthernet0/1
        Destination MAC address 0010.1731.5100
        bi-directional traffic export is on
Output IP Traffic Export Information    Packets/Bytes Exported    4/218
        Packets Dropped           40
        Sampling Rate             one-in-every 10 packets
        No Access List configured
Input IP Traffic Export Information     Packets/Bytes Exported    2/99
        Packets Dropped           22
        Sampling Rate             one-in-every 10 packets
        No Access List configured
        Profile R5-WAN is Active

Monitored Interface             Serial0/1/0
        Export Interface                FastEthernet0/1
        Destination MAC address 0010.1731.5100
        bi-directional traffic export is on
Output IP Traffic Export Information    Packets/Bytes Exported    0/0
Packets Dropped
        Sampling Rate             one-in-every 10 packets
        No Access List configured
Input IP Traffic Export Information     Packets/Bytes Exported    0/0
        Packets Dropped           0
        Sampling Rate             one-in-every 10 packets
        No Access List configured
        Profile R5-WAN is Active
```

Task 8.1

```
R5:
ip cef
!
interface FastEthernet0/0
 ip nbar protocol-discovery
!
interface FastEthernet0/1
 ip nbar protocol-discovery
```

Task 8.1 Verification

```
Rack1R5#show ip nbar protocol-discovery top-n 3

 FastEthernet0/0
```



```
              Input                     Output
              -----                     ------
  Protocol    Packet Count              Packet Count
              Byte Count                Byte Count
              5min Bit Rate (bps)       5min Bit Rate (bps)
              5min Max Bit Rate (bps)   5min Max Bit Rate (bps)
  ----------- ------------------------- -----------------
  icmp        10                        5
              1140                      570
              0                         0
              0                         0
  bgp         2                         1
              167                       93
              0                         0
              0                         0
  citrix      0                         0
              0                         0
              0                         0
              0                         0
  unknown     0                         0
              0                         0
              0                         0
              0                         0
  Total       12                        6
              1307                      663
              0                         0
              0                         0

FastEthernet0/1
              Input                     Output
              -----                     ------
  Protocol    Packet Count              Packet Count
              Byte Count                Byte Count
              5min Bit Rate (bps)       5min Bit Rate (bps)
              5min Max Bit Rate (bps)   5min Max Bit Rate (bps)
  ----------- ------------------------- -----------------
  eigrp       0                         14
              0                         1036
              0                         0
              0                         0
  bgp         0                         0
              0                         0
              0                         0
              0                         0
  citrix      0                         0
              0                         0
              0                         0
              0                         0
  unknown     0                         0
              0                         0
              0                         0
              0                         0
  Total       0                         14
              0                         1036
              0                         0
              0                         0
```


Task 8.2

R5:

```
class-map match-any PEER_TO_PEER
  match protocol kazaa2
  match protocol fasttrack
  match protocol gnutella
  match protocol napster
!
 policy-map DROP_PEER_TO_PEER
  class PEER_TO_PEER
   drop
!
interface FastEthernet0/0
 service-policy input DROP_PEER_TO_PEER
 service-policy output DROP_PEER_TO_PEER
!
interface FastEthernet0/1
 service-policy input DROP_PEER_TO_PEER
 service-policy output DROP_PEER_TO_PEER
```

Task 8.2 Verification

```
Rack1R5#show policy-map interface FastEthernet 0/0
 FastEthernet0/0

  Service-policy input: DROP_PEER_TO_PEER

    Class-map: PEER_TO_PEER (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: protocol kazaa2
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: protocol fasttrack
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: protocol gnutella
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: protocol napster
        0 packets, 0 bytes
        5 minute rate 0 bps
      drop

    Class-map: class-default (match-any)
      3 packets, 345 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any

  Service-policy output: DROP_PEER_TO_PEER

    Class-map: PEER_TO_PEER (match-any)
      0 packets, 0 bytes
```



```
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: protocol kazaa2
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: protocol fasttrack
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: protocol gnutella
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: protocol napster
        0 packets, 0 bytes
        5 minute rate 0 bps
      drop

    Class-map: class-default (match-any)
      8 packets, 619 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

Task 8.3

R5:

```
policy-map POLICE
 class class-default
  police cir 384000 bc 14400 pir 512000 be 19200
   conform-action transmit
   exceed-action set-dscp-transmit 0
   violate-action drop
!
interface FastEthernet 0/0
 service-policy input POLICE
```


Task 8.4

R5:

```
class-map match-any DLCI_501
 match fr-dlci 501
!
class-map VOICE
 match dscp EF
!
policy-map CBWFQ_DLCI_501
 class VOICE
  priority 256
 class class-default
  fair-queue
!
policy-map SHAPE_DLCI_501
 class DLCI_501
  shape average 512000
  service-policy CBWFQ_DLCI_501
!
interface Serial 0/0
 service-policy output SHAPE_DLCI_501
```

