Copyright Information

Disclaimer

The following publication, ***CCIE Security Lab Workbook Volume I***, is designed to assist candidates in the preparation for Cisco Systems' CCIE Routing & Switching Lab exam. While every effort has been made to ensure that all material is as complete and accurate as possible, the enclosed material is presented on an "as is" basis. Neither the authors nor Internetwork Expert, Inc. assume any liability or responsibility to any person or entity with respect to loss or damages incurred from the information contained in this workbook.

This workbook was developed by Internetwork Expert, Inc. and is an original work of the aforementioned authors. Any similarities between material presented in this workbook and actual CCIE™ lab material is completely coincidental.

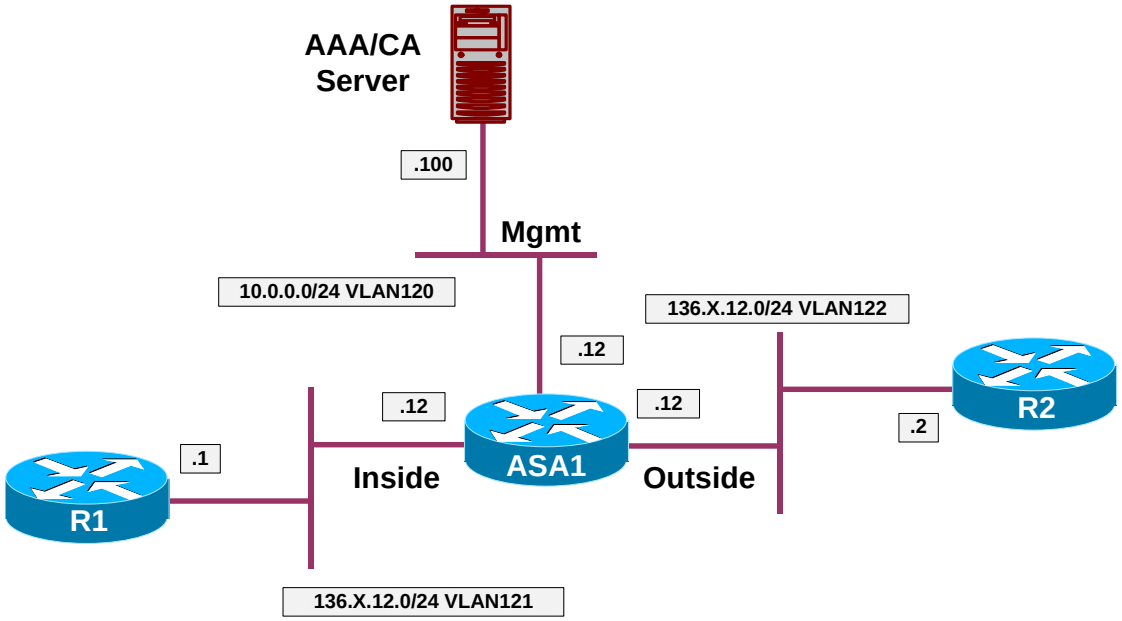
Table of Contents

Network Attacks

Layer2/3 Attacks

Mitigating ARP Spoofing Attack with PIX/ASA

Objective: Configure PIX/ASA appliance in transaprent mode to prevent ARP spoofing attacks



Directions

- Configure devices per the PIX/ASA Firewall/Advanced Firewall scenario "Filtering with L2 Transparent Firewall"
- Look for MAC addresses of R1 and R2 at ASA1 using the "**show interface**" on routers R1 and R2
- Configure static ARP entries at ASA1 for the IP addresses of R1 and R2 respectively, mapping them to the MAC addresses you learned
- Enable ARP inspection on the inside/outside interfaces of the ASA

Final Configuration


```
ASA1:
arp outside 136.1.12.2 0003.e335.1240
arp inside 136.1.12.1 0050.73f7.c0c0
!
arp-inspection outside enable
arp-inspection inside enable
```

Verification

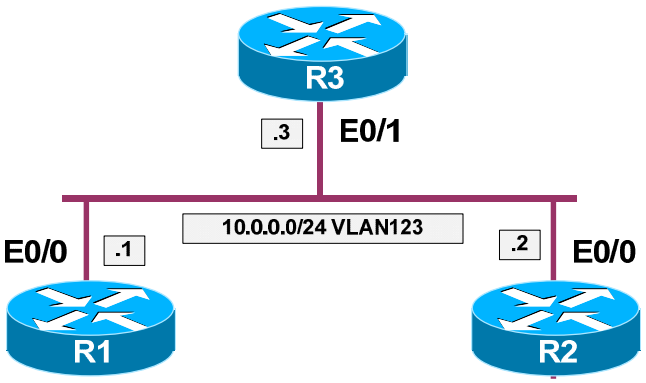
```
Rack1R1#show interfaces ethernet 0/0 | inc bia
  Hardware is AmdP2, address is 0050.73f7.c0c0 (bia 0050.73f7.c0c0)

Rack1R2#show interfaces ethernet 0/0 | inc bia
  Hardware is AmdP2, address is 0015.63c8.880d (bia 0003.e335.1240)

Try changing R2's MAC address, and clearing ARP cache at R1:

Rack1R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Rack1R2(config)#interface ethernet 0/0
Rack1R2(config-if)# mac-address  0003.e335.1242

Rack1ASA1(config)# debug arp-inspection 9
debug arp-inspection  enabled at level 9

Rack1R1#clear arp-cache
Rack1R1#ping 136.1.12.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 136.1.12.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

Rack1ASA1(config)#
%ASA-3-322002: ARP inspection check failed for arp response received
from host 0003.e335.1242 on interface outside. This host is advertising
MAC Address 0003.e335.1242 for IP Address 136.1.12.2, which is
statically bound to MAC Address 0003.e335.1240d
<output omitted>
```

🕮 Further Reading

Configuring ARP Inspection and Bridging Parameters

Mitigating DHCP Attacks with DHCP Snooping

Objective: Configure switches to dynamically inspect DHCP messages and guard against common DHCP attacks



Directions

- Configure logical topology per the diagram:
  - Create VLAN 123 and configure switchports
  - Configure trunking between SW1 and SW2
- Configure R1 and R2 to obtain IP addresses via DHCP
- Configure IP address on R3 and configure R3 to act as DHCP server for VLAN 123
- Enable DHCP snooping on SW1 and SW2, configure R3's switchport and SW2's uplink as DHCP-snooping trusted interfaces
- Make sure switches do not insert Option 82 into DHCP requests

Final Configuration

```
SW1:
vlan 123
!
interface range Fast 0/1 - 2
 switchport access vlan 123
!
interface Fast 0/23
 switchport trunk encapsulation dot1q
 switchport mode trunk

SW2:
vlan 123
!
interface range Fast 0/3
 switchport access vlan 123
!
interface Fast 0/23
 switchport trunk encapsulation dot1q
 switchport mode trunk
```



```
R1:
interface Ethernet 0/0
 no shutdown
 ip address dhcp

R2:
interface Ethernet 0/0
 no shutdown
 ip address dhcp

R3:
interface Ethernet 0/1
 no shutdown
 ip address 10.0.0.3 255.255.255.0
!
ip dhcp pool VLAN123
 network 10.0.0.0 /24
```

DHCP Snooping Configuration:

```
SW1:
ip dhcp snooping
ip dhcp snooping vlan 123
no ip dhcp snooping information option
!
interface Fast 0/23
 ip dhcp snooping trust

SW2:
ip dhcp snooping
ip dhcp snooping vlan 123
no ip dhcp snooping information option
!
interface Fast 0/3
 ip dhcp snooping trust
```

Verification

```
Rack1R3#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
10.0.0.2            0063.6973.636f.2d30.    Mar 19 1993 10:52 PM    Automatic
                    3035.302e.3733.6637.
                    2e63.3063.302d.4574.
                    302f.30
10.0.0.4            0063.6973.636f.2d30.    Mar 19 1993 10:52 PM    Automatic
                    3030.332e.6533.3335.
                    2e31.3234.322d.4574.
                    302f.30

Rack1SW1#show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
123
Insertion of option 82 is disabled
   circuit-id format: vlan-mod-port
    remote-id format: MAC
Option 82 on untrusted port is not allowed
```



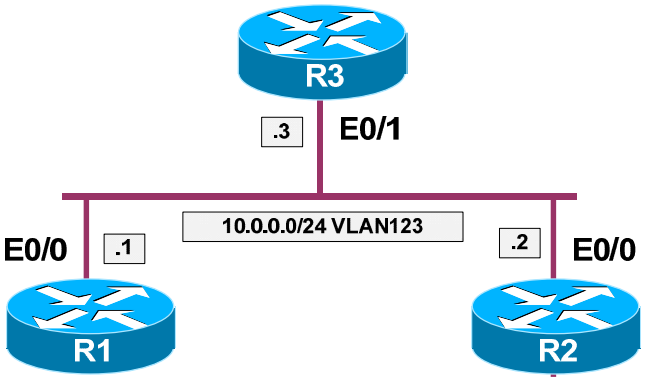
```
Verification of hwaddr field is enabled
Interface                   Trusted     Rate limit (pps)
------------------------    -------     ----------------
FastEthernet0/23            yes         unlimited

Rack1SW2#show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
123
Insertion of option 82 is disabled
   circuit-id format: vlan-mod-port
    remote-id format: MAC
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                   Trusted     Rate limit (pps)
------------------------    -------     ----------------
FastEthernet0/3             yes         unlimited

Rack1SW1#show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  ---------
-----------
00:03:E3:35:12:42   10.0.0.4         86371       dhcp-snooping  123
FastEthernet0/2
00:50:73:F7:C0:C0   10.0.0.2         86365       dhcp-snooping  123
FastEthernet0/1
Total number of bindings: 2

Rack1SW2#show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  ---------
-----------
00:03:E3:35:12:42   10.0.0.4         86340       dhcp-snooping  123
FastEthernet0/23
00:50:73:F7:C0:C0   10.0.0.2         86333       dhcp-snooping  123
FastEthernet0/23
Total number of bindings: 2
```

📖 Further Reading

Configuring DHCP Features and IP Source Guard

Mitigating ARP Attacks in DHCP Environment

Objective: Configure Dynamic ARP inspection in DHCP environment



Directions

- Configure devices per "Network Attacks" scenario "Mitigating DHCP Attacks with DHCP Snooping"
- Configure dynamic ARP inspection in VLAN 123 , valide IP address in ARP packets
- Learn MAC address of R3 using the command "**show interface**" at R3
- Configure static ARP access-list for R3's IP/MAC address pair. This ARP ACL should be applied to VLAN123
- Log any matches for static ACL within VLAN 123
- Re-request IP addresses for R1 and R2

Final Configuration

```
SW1 & SW2:
ip arp inspection vlan 123 logging acl-match matchlog
ip arp inspection validate ip
!
arp access-list VLAN123_ARP
 permit ip host 10.0.0.3 mac host 0050.5476.4101 log
!
ip arp inspection filter VLAN123_ARP vlan 123
```

Verification

```
Rack1R3#show interfaces ethernet 0/1
Ethernet0/1 is up, line protocol is up
  Hardware is AmdP2, address is 0050.5476.4101 (bia 0050.5476.4101)
<output omitted>

Rack1R3#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
```



```
                    User name
10.0.0.5            0063.6973.636f.2d30.    Mar 19 1993 11:10 PM    Automatic
                    3035.302e.3733.6637.
                    2e63.3063.302d.4574.
                    302f.30
10.0.0.6            0063.6973.636f.2d30.    Mar 19 1993 11:10 PM    Automatic
                    3030.332e.6533.3335.
                    2e31.3234.322d.4574.
                    302f.30

Rack1SW1#show ip arp inspection

Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Enabled

 Vlan     Configuration    Operation   ACL Match          Static ACL
 ----     -------------    ---------   ---------          ----------
  123     Enabled          Active      VLAN123_ARP        No

 Vlan     ACL Logging      DHCP Logging
 ----     -----------      ------------
  123     Acl-Match        Deny

 Vlan      Forwarded        Dropped     DHCP Drops      ACL Drops
 ----      ---------        -------     ----------      ---------
  123             12              0              0              0

 Vlan   DHCP Permits    ACL Permits   Source MAC Failures
 ----   ------------    -----------   -------------------
  123              7              5                     0

 Vlan   Dest MAC Failures   IP Validation Failures   Invalid Protocol Data
 ----   -----------------   ----------------------   ---------------------

 Vlan   Dest MAC Failures   IP Validation Failures   Invalid Protocol Data
 ----   -----------------   ----------------------   ---------------------
  123                   0                        0                      0

Rack1SW2#show ip arp inspection

Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Enabled

 Vlan     Configuration    Operation   ACL Match          Static ACL
 ----     -------------    ---------   ---------          ----------
  123     Enabled          Active      VLAN123_ARP        No

 Vlan     ACL Logging      DHCP Logging
 ----     -----------      ------------
  123     Acl-Match        Deny

 Vlan      Forwarded        Dropped     DHCP Drops      ACL Drops
 ----      ---------        -------     ----------      ---------
  123             12              0              0              0

 Vlan   DHCP Permits    ACL Permits   Source MAC Failures
 ----   ------------    -----------   -------------------
  123              7              5                     0

 Vlan   Dest MAC Failures   IP Validation Failures   Invalid Protocol Data
 ----   -----------------   ----------------------   ---------------------
```



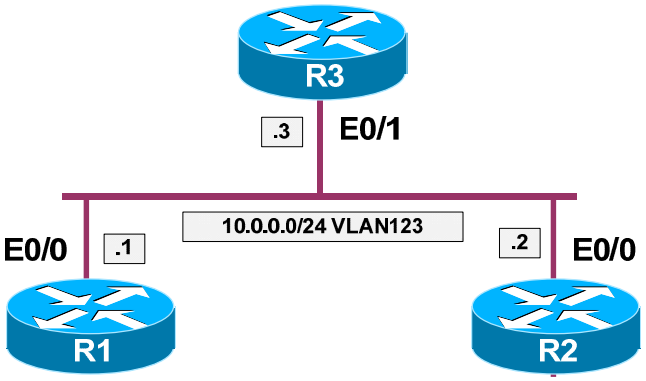
```
 Vlan   Dest MAC Failures   IP Validation Failures   Invalid Protocol Data
 ----   -----------------   ----------------------   ---------------------
  123                   0                        0                       0

Rack1SW1#show logging | inc ARP
00:36:58: %SW_DAI-6-ACL_PERMIT: 1 ARPs (Res) on Fa0/23, vlan
123.([0050.5476.4101/10.0.0.3/0050.73f7.c0c0/10.0.0.5/00:36:58 UTC Mon Mar 1
1993])

Rack1SW2#show logging | inc ARP
%SW_DAI-6-ACL_PERMIT: 1 ARPs (Res) on Fa0/3, vlan
123.([0050.5476.4101/10.0.0.3/0050.73f7.c0c0/10.0.0.5/00:36:54 UTC Mon Mar 1
1993])
```

🕮 Further Reading

Configuring Dynamic ARP Inspection

Mitigating MAC/IP Spoofing in DHCP Environment

Objective: Configure switches to automatically protect against IP/MAC spoofing



Directions

- Configure devices per "Network Attacks" scenario "Mitigating DHCP Attacks with DHCP Snooping"
- Learn R2's Ethernet interface MAC address by issuing the "**show interface**" command
- Configure R2 with static IP per the diagram provided
- Configure static IP to MAC/port binding for R2's IP/MAC addresses at SW1
- Enable IP source guard on R1 and R2's switchport
- Configue protection against MAC address spoofing along with IP source guard
- Make R1 re-request IP addresses via DHCP

Final Configuration

```
SW1:
ip source binding 0003.e335.1242 vlan 123 10.0.0.2 interface Fa0/2
!
interface range Fa 0/1 - 2
 ip verify source port-security
 !
 ! Mode access is required to enable port-security
 !
 switchport mode access
 switchport port-security

R2:
interface Ethernet 0/0
 ip address 10.0.0.2 255.255.255.0
```


Verification

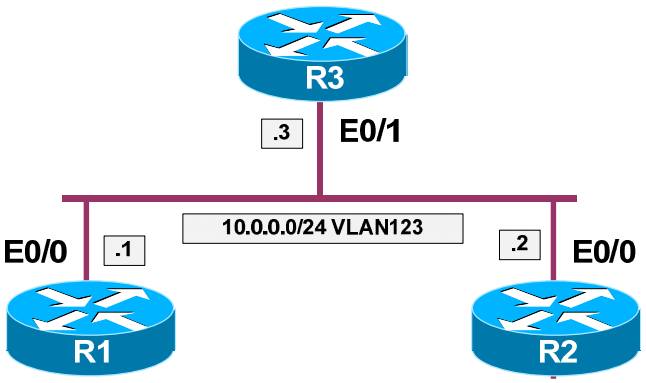
```
Rack1SW1#show ip verify source
Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan
---------  -----------  -----------  ---------------  -----------------  ------
----
Fa0/1      ip-mac       active       10.0.0.4         00:50:73:F7:C0:C0  123
Fa0/2      ip-mac       active       10.0.0.2         00:03:E3:35:12:42  123

Rack1SW1#show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  ---------
-----------
00:50:73:F7:C0:C0   10.0.0.4         85670       dhcp-snooping  123
FastEthernet0/1
Total number of bindings: 1

Rack1R2#ping 10.0.0.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

R2:
interface Ethernet0/0
 ip address 10.0.0.100 255.255.255.0

Rack1R2#ping 10.0.0.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.3, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

🕮 Further Reading

Understanding IP Source Guard

Protecting Spanning-Tree Protocol

Objective: Configure the switches to protect spanning tree instance for VLAN 123



Directions

- Configure logical topology per the diagram:
    - Create VLAN 123 and configure switchports
    - Configure trunking between SW1 and SW2
- Configure SW1 to be the STP root for VLAN 123
- Make sure SW1 protects itself against SW2 sending inferior BPDUs
- Make sure SW2 brings switchport connecto to SW2 to inconsistent state once it receives any BPDU from it
- Ensure SW1 does not send or receive any BPDUs to/from R1 and R2

Final Configuration

SW1:

```
spanning-tree vlan 123 root primary
!
interface Fa 0/23
 !
 ! Bring port to inconsistent state once any inferior BPDUs
 ! (someone other claims itself as root) is received
 !
 spanning-tree guard root
!
interface range Fa 0/1 - 2
 spanning-tree bpdufilter enable
```

SW2:

```
!
interface range Fa 0/3
 spanning-tree bpduguard enable
```


Verification

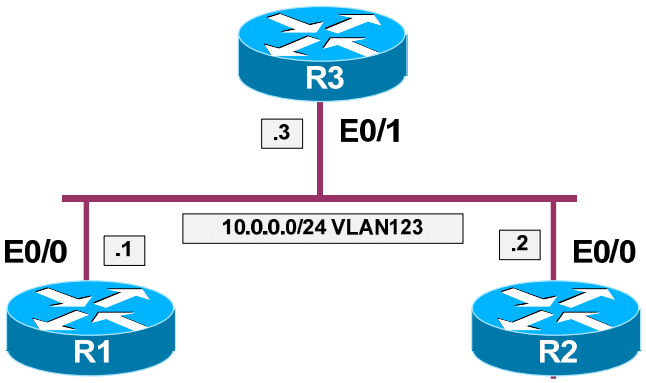
```
Rack1SW1#show spanning-tree vlan 123

VLAN0123
  Spanning tree enabled protocol ieee
  Root ID    Priority    24699
             Address     000d.bc33.d780
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    24699  (priority 24576 sys-id-ext 123)
             Address     000d.bc33.d780
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 100       128.1    Shr
Fa0/2            Desg FWD 100       128.2    Shr
Fa0/23           Desg FWD 19        128.23   P2p

Rack1SW1#show spanning-tree vlan 123 interface fastEthernet 0/23 detail
 Port 23 (FastEthernet0/23) of VLAN0123 is forwarding
   Port path cost 19, Port priority 128, Port Identifier 128.23.
   Designated root has priority 24699, address 000d.bc33.d780
   Designated bridge has priority 24699, address 000d.bc33.d780
   Designated port id is 128.23, designated path cost 0
   Timers: message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   Link type is point-to-point by default
   Root guard is enabled on the port
   BPDU: sent 1307, received 3

Rack1SW1#show spanning-tree vlan 123 interface fastEthernet 0/1 detail
 Port 1 (FastEthernet0/1) of VLAN0123 is forwarding
   Port path cost 100, Port priority 128, Port Identifier 128.1.
   Designated root has priority 24699, address 000d.bc33.d780
   Designated bridge has priority 24699, address 000d.bc33.d780
   Designated port id is 128.1, designated path cost 0
   Timers: message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   Link type is shared by default
   Bpdu filter is enabled
   BPDU: sent 1141, received 0

Rack1SW2#show spanning-tree vlan 123 interface fastEthernet 0/3 detail
 Port 3 (FastEthernet0/3) of VLAN0123 is forwarding
   Port path cost 100, Port priority 128, Port Identifier 128.3.
   Designated root has priority 24699, address 000d.bc33.d780
   Designated bridge has priority 32891, address 0015.63c8.8800
   Designated port id is 128.3, designated path cost 19
   Timers: message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   Link type is shared by default
   Bpdu guard is enabled
   BPDU: sent 1343, received 0
```


🕮 Further Reading

Configuring Optional Spanning-Tree Features

Protecting Against Broadcast Storms

Objective: Configure the switches to protect against floods of broadcast/multicast packets



Directions

- Configure logical topology per the diagram:
  - Create VLAN 123 and configure switchports
  - Configure trunking between SW1 and SW2
- Configure ports speeds on switchports of R1, R2 and R3 to 10Mbps
- Configure port speed on link between SW1 and SW2 to 100Mbps
- Ensure that no more than 1Mbps of broadcast traffic could be accepted from routers and passed between the switches
- Additionally, limit unicast packets to no more than 100K pps on all the mentioned ports

Final Configuration

```
SW1:
interface range FastEthernet 0/1 - 2
 speed 10
 speed 10
 storm-control broadcast level 10.00
 storm-control unicast level pps 100k
!
interface Fast 0/23
 speed 100
 storm-control broadcast level 1
 storm-control unicast level pps 100k

SW2:
interface range FastEthernet 0/3
 speed 10
 speed 10
 storm-control broadcast level 10.00
```



```
 storm-control unicast level pps 100k
!
interface Fast 0/23
 speed 100
 storm-control broadcast level 1
 storm-control unicast level pps 100k

R1:
interface Ethernet 0/0
 no shutdown
 ip address 10.0.0.1 255.255.255.0

R2:
interface Ethernet 0/0
 no shutdown
 ip address 10.0.0.2 255.255.255.0

R3:
interface Ethernet 0/1
 no shutdown
 ip address 10.0.0.3 255.255.255.0
```

Verification

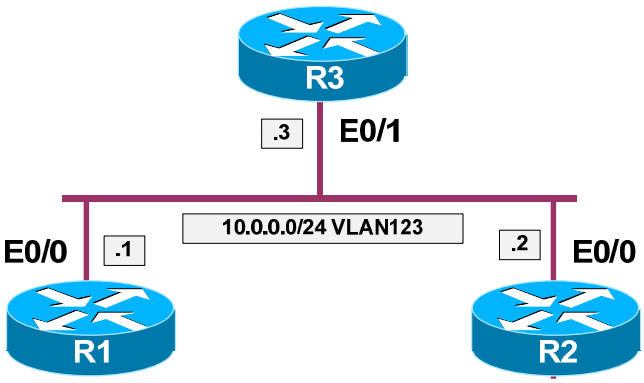
```
Rack1SW1#show storm-control broadcast
Interface  Filter State   Upper        Lower        Current
---------  ------------  -----------  -----------  ----------
Fa0/1      Forwarding      10.00%       10.00%       0.00%
Fa0/2      Forwarding      10.00%       10.00%       0.00%
Fa0/23     Forwarding       1.00%        1.00%       0.00%

Rack1SW1#show storm-control unicast
Interface  Filter State   Upper        Lower        Current
---------  ------------  -----------  -----------  ----------
Fa0/1      Forwarding       100k pps     100k pps        0 pps
Fa0/2      Forwarding       100k pps     100k pps        0 pps
Fa0/23     Forwarding       100k pps     100k pps        0 pps

Rack1R1#ping 10.0.0.3 repeat 10000 timeout 0

Type escape sequence to abort.
Sending 10000, 100-byte ICMP Echos to 10.0.0.3, timeout is 0 seconds:
.....................................................................
.....................................................................
.................................................!...................
<output omitted>

Rack1SW1#show storm-control unicast
Interface  Filter State   Upper        Lower        Current
---------  ------------  -----------  -----------  ----------
Fa0/1      Forwarding       100k pps     100k pps      556 pps
Fa0/2      Forwarding       100k pps     100k pps        0 pps
Fa0/23     Forwarding       100k pps     100k pps      542 pps
```


Further Reading

Understanding Storm Control

Mitigating VLAN Hopping Attacks

Objective: Configure the switches to protect against host ports becoming trunks, and filter all unused VLANs between switches



Directions

- Configure logical topology per the diagram:
  - Create VLAN 123 and configure switchports
  - Configure trunking between SW1 and SW2
- Ensure the switchports of R1, R2 and R3 do not run DTP and are set to the access mode permanently
- Manually enforce 802.1q tunk between SW1 and SW2
- Make sure that only VLAN123's traffic could be passed between SW1 and SW2

Final Configuration

Pre-Configuration:

SW1:

```
vlan 123
!
interface range Fa 0/1 - 2
 switchport host
 switchport access vlan 123
!
interface Fa 0/23
 switchport trunk encapsulation dot1q
 switchport mode trunk
```

SW2:

```
vlan 123
!
interface Fa 0/3
 switchport host
 switchport access vlan 123
```



```
!
interface Fa 0/23
 switchport trunk encapsulation dot1q
 switchport mode trunk
```

Solution:

SW1:

```
interface range FastEthernet 0/1 - 2
 switchport nonegotiate
 switchport mode access
!
interface Fast 0/23
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport nonegotiate
 switchport trunk allowed vlan 123
```

SW2:

```
interface range FastEthernet 0/3
 switchport nonegotiate
 switchport mode access
!
interface Fast 0/23
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport nonegotiate
 switchport trunk allowed vlan 123
```

Verification

```
Rack1SW1#show interfaces fastEthernet 0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 123 (VLAN0123)
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: false
```



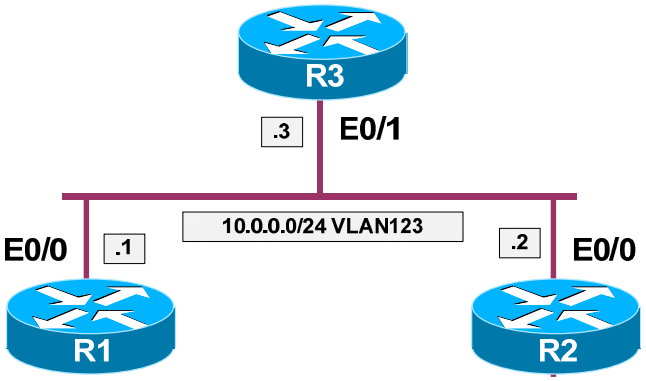
```
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none

Rack1SW1#show interfaces fastEthernet 0/23 switchport
Name: Fa0/23
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
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: 123
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

🕮 Further Reading

VLAN Security White Paper

Protecting Against Network Mapping

Objective: Configure R3 not to leak any useful information via ICMP



Directions

- Configure logical topology per the diagram:
  - Create VLAN 123 and configure switchports
  - Configure trunking between SW1 and SW2
- Configure R1 and R2 to use R3 as default gateway
- Configure R3 not to send any ICMP unreachables out of it Ethernet interface

Final Configuration

SW1:

```
vlan 123
!
interface range Fa 0/1 - 2
 switchport host
 switchport access vlan 123
!
interface Fa 0/23
 switchport trunk encapsulation dot1q
 switchport mode trunk
```

SW2:

```
vlan 123
!
interface Fa 0/3
 switchport host
 switchport access vlan 123
!
interface Fa 0/23
 switchport trunk encapsulation dot1q
 switchport mode trunk
```



```
R1:
interface Ethernet 0/0
 no shutdown
 ip address 10.0.0.1 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 10.0.0.3

R2:
interface Ethernet 0/0
 no shutdown
 ip address 10.0.0.2 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 10.0.0.3

R3:
interface Ethernet 0/1
 no shutdown
 ip address 10.0.0.3 255.255.255.0
!
interface Ethernet 0/1
 no ip unreachables
```

Verification

Before IP unreachables disabled:

```
Rack1R1#debug ip icmp
ICMP packet debugging is on
Rack1R1#ping 150.1.4.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.1.4.4, timeout is 2 seconds:
U.U.U
Success rate is 0 percent (0/5)

ICMP: dst (10.0.0.1) host unreachable rcv from 10.0.0.3
ICMP: dst (10.0.0.1) host unreachable rcv from 10.0.0.3
ICMP: dst (10.0.0.1) host unreachable rcv from 10.0.0.3|
```

After:

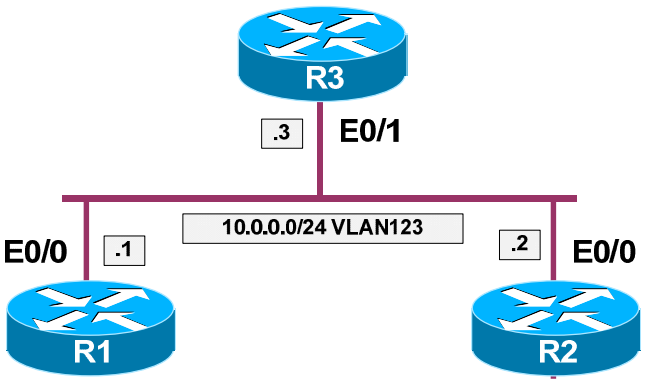
```
Rack1R1#ping 150.1.4.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.1.4.4, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

🕮 Further Reading

Enabling ICMP Protocol Unreachable Messages

Blackhole Routing using PBR

Objective: Configure R3 to block ICMP packet of size in range 100-200 going from R1 to R2



Directions

- Configure logical topology per the diagram:
  - Create VLAN 123 and configure switchports
  - Configure trunking between SW1 and SW2
- Configure R1 and R2 to use R3 as the default gateway
- Configure Loopback0 interfaces on R1 and R2 with the IP addresses 150.X.Y.Y/24
- Configure static routes for Loopback0 interfaces of R1 and R2 at R3
- Configure policy routing at R3 Ethernet interface to block ICMP packets of size in range 100-200

Final Configuration

```
SW1:
vlan 123
!
interface range Fa 0/1 - 2
 switchport host
 switchport access vlan 123
!
interface Fa 0/23
 switchport trunk encapsulation dot1q
 switchport mode trunk

SW2:
vlan 123
!
interface Fa 0/3
 switchport host
 switchport access vlan 123
```



```
!
interface Fa 0/23
 switchport trunk encapsulation dot1q
 switchport mode trunk

R1:
interface Ethernet 0/0
 no shutdown
 ip address 10.0.0.1 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 10.0.0.3
!
interface Loopback0
 ip address 150.1.1.1 255.255.255.0

R2:
interface Ethernet 0/0
 no shutdown
 ip address 10.0.0.2 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 10.0.0.3
!
interface Loopback0
 ip address 150.1.2.2 255.255.255.0

R3:
interface Ethernet 0/1
 no shutdown
 ip address 10.0.0.3 255.255.255.0
!
ip route 150.1.1.0 255.255.255.0 10.0.0.1
ip route 150.1.2.0 255.255.255.0 10.0.0.2
!
access-list 100 permit icmp any any
!
route-map BLACKHOLE permit 10
 match ip address 100
 match length 100 200
 set interface Null0
!
interface Ethernet 0/1
 ip policy route-map BLACKHOLE
```

Verification

```
Rack1R1#ping 150.1.2.2 size 500

Type escape sequence to abort.
Sending 5, 500-byte ICMP Echos to 150.1.2.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 8/8/8 ms

Rack1R1#ping 150.1.2.2 size 99

Type escape sequence to abort.
Sending 5, 99-byte ICMP Echos to 150.1.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/8 ms
```



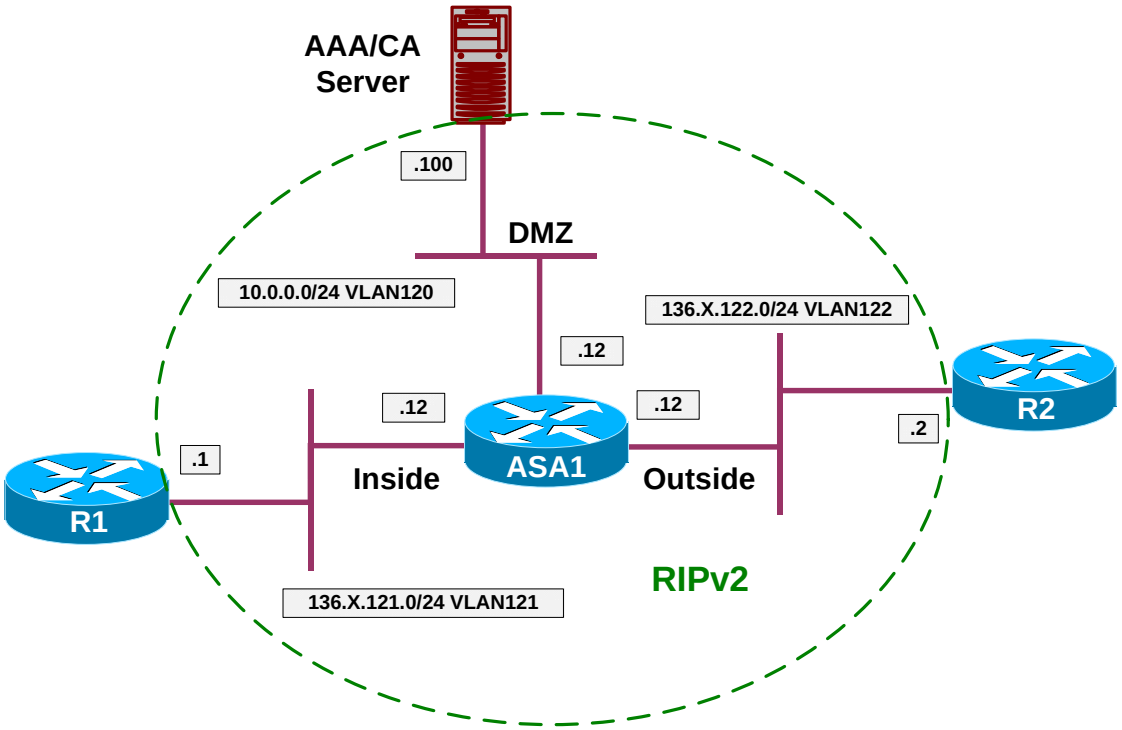
```
Rack1R1#ping 150.1.2.2 size 100

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.1.2.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

Rack1R3#show route-map BLACKHOLE
route-map BLACKHOLE, permit, sequence 10
  Match clauses:
    ip address (access-lists): 100
    length 100 200
  Set clauses:
    interface Null0
  Policy routing matches: 5 packets, 570 bytes
```

🕮 Further Reading

Enabling ICMP Protocol Unreachable Messages

Intrusion Prevention with PIX/ASA

Objective: Configure PIX/ASA appliance for intrusion prevention



Directions

- Configure devices as per the scenario "PIX/ASA Firewall/Access Control" "Common Configuration"
- Configure audit rule named OUTSIDE_ATTACK on the ASA1. Drop and reset on all attack signatures with this rule
- Configure audit rule named OUTSIDE_INFO on the ASA1. Drop and alarm on all information signature with this rule
- Apply both rules to the Outside interface
- In order to permit network testing with ping utility, disable signatures for ICMP echo and echo-reply, as well as for Large ICMP and Fragmented ICMP
- You can see signature names and numbes using command "**show ip audit count**"
- Finally apply an access-list to the outside interface to permit ICMP packets inbound

Final Configuration

ASA1:

```
ip audit name OUTSIDE_ATTACK attack action drop reset
ip audit name OUTSIDE_INFO info action drop alarm
!
ip audit interface outside OUTSIDE_ATTACK
ip audit interface outside OUTSIDE_INFO
!
ip audit signature 2000 disable
ip audit signature 2004 disable
ip audit signature 2150 disable
ip audit signature 2151 disable
!
access-list OUTSIDE_IN permit icmp any any
!
access-group OUTSIDE_IN in interface outside
```

Verification

Before ICMP signature were disabled:

```
Rack1R2#ping 136.1.121.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 136.1.121.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

Rack1ASA1(config)# show ip audit count | inc ICMP Echo
2000 I ICMP Echo Reply            0
2004 I ICMP Echo Request          5
2000 I ICMP Echo Reply            0
2004 I ICMP Echo Request          5
```

Disable 2000/2004 signatures and ping again:

```
Rack1R2#ping 136.1.121.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 136.1.121.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

Rack1R2#ping 136.1.121.1 size 1500

Type escape sequence to abort.
Sending 5, 1500-byte ICMP Echos to 136.1.121.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

Rack1R2#ping 136.1.121.1 size 1505

Type escape sequence to abort.
```



```
Sending 5, 1505-byte ICMP Echos to 136.1.121.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

Rack1ASA1(config)# show ip audit count | inc (Large|Fragmented) ICMP
2150 A Fragmented ICMP            10
2151 A Large ICMP                 5
2150 A Fragmented ICMP            10
2151 A Large ICMP                 5

Disable all ICMP signatures:

Rack1R2#ping 136.1.121.1 size 1505

Type escape sequence to abort.
Sending 5, 1505-byte ICMP Echos to 136.1.121.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/13/16 ms
```

🕮 Further Reading

Preventing Network Attacks