MANRS Lab

Students' Guide

Lab guide PacNOG29

Version 4 – November 2021

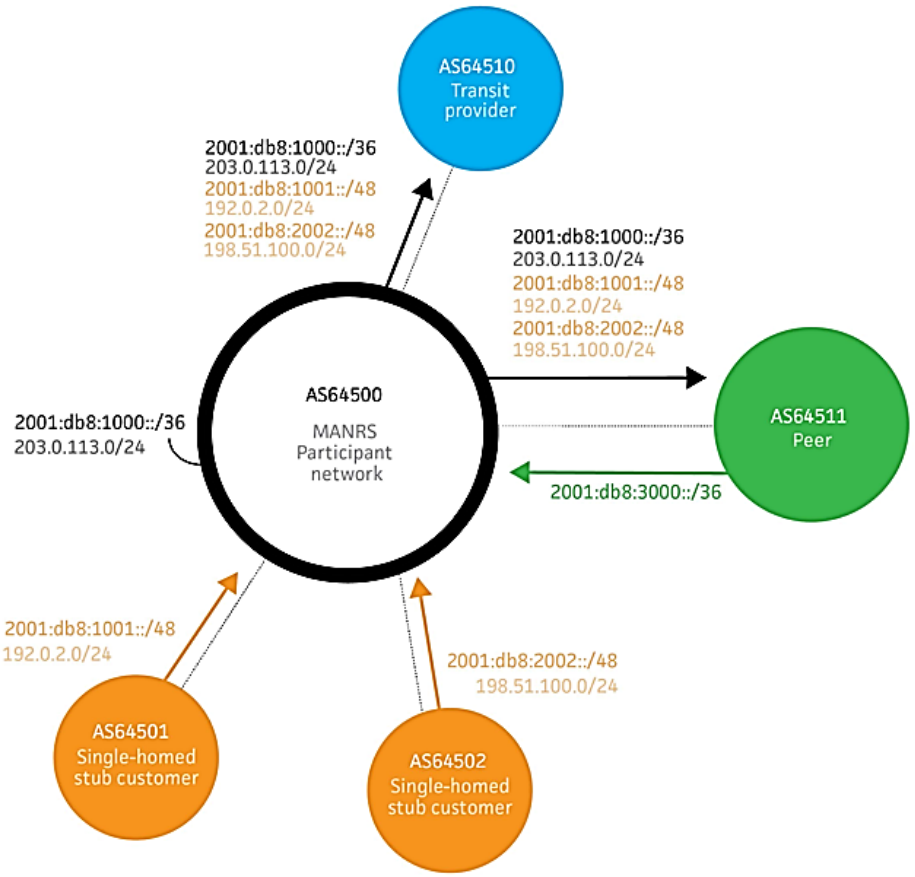
Naveen K Lakshman, MANRS Fellow (Training)

Kunal Krishnil Raj, MANRS Fellow (Training)

Table of Contents

Introduction

This MANRS Lab is designed to let you gain experience with implementing MANRS on a router. The exercises will follow the MANRS Implementation guide at https://www.manrs.org/isps/guide/ very closely, including the network topology:



Exercises are provided for Cisco IOS.

In these exercises the neighbours around you are not behaving properly. They announce routes that don't belong to them. They even try to hijack your address space! They also send traffic with spoofed source addresses and traffic for destinations that you don't announce to them. It is your task to properly filter route announcements to stop traffic with spoofed source addresses.

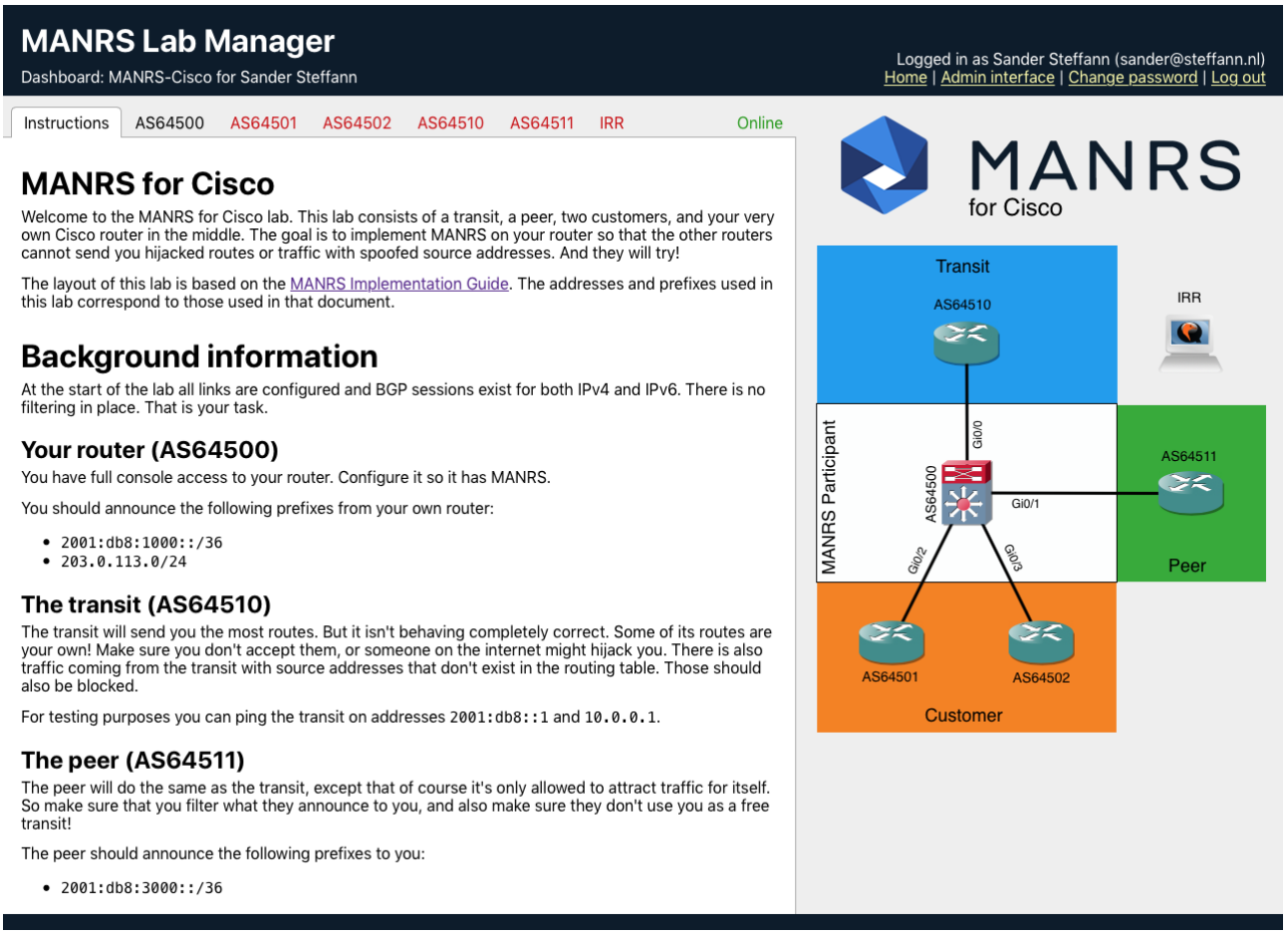
The goals of the exercise are:

- to filter incoming routes announced by your customers AS64501 and AS64502
- to filter incoming routes announced by your transit provider AS64510
- to filter incoming routes announced by your peer AS64511
- to filter outgoing routes as you announce them to your customers, peer and transit
- to filter traffic with spoofed source addresses from your customers

User interface

The lab is web-based and can be used with any modern browser. You do not need any other tools for doing the exercises. Configuring the routers is done through a browser based terminal window, and interaction with the IRR database is web based as well.

Your main interface to the lab environment is through the exercise dashboard:



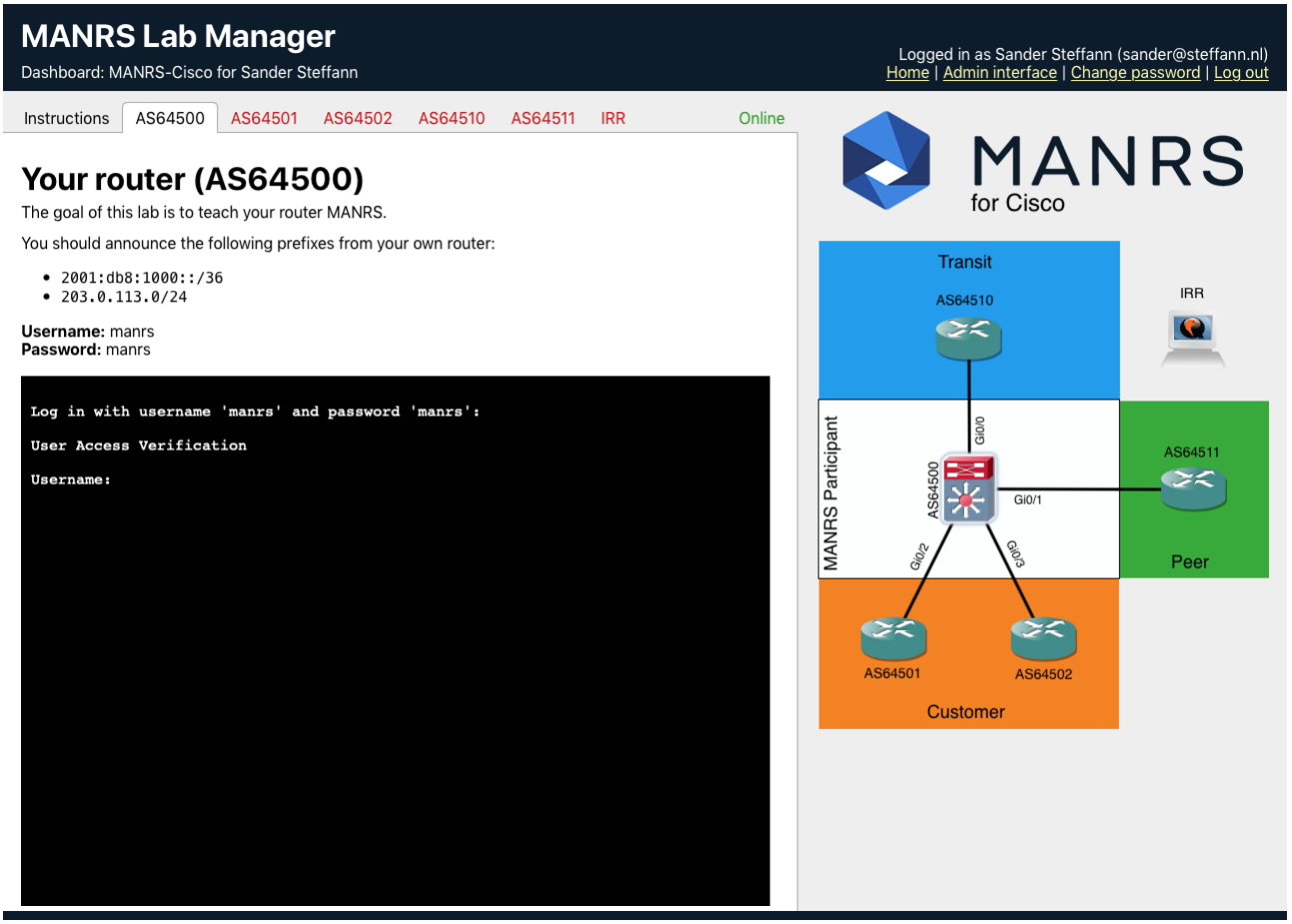
The dashboard contains several tabs, each representing a different part of the exercise. Some of the tabs are coloured. The colour shows you whether what is seen on that tab is correct according to the exercise goals or whether there is still work to be done.

Instructions

This tab contains basic instructions about the exercise. It is the tab you see in the screenshot above. The exercises are all based on the instructions in the MANRS Implementation guide. Follow that guide to complete the exercises!

AS64500

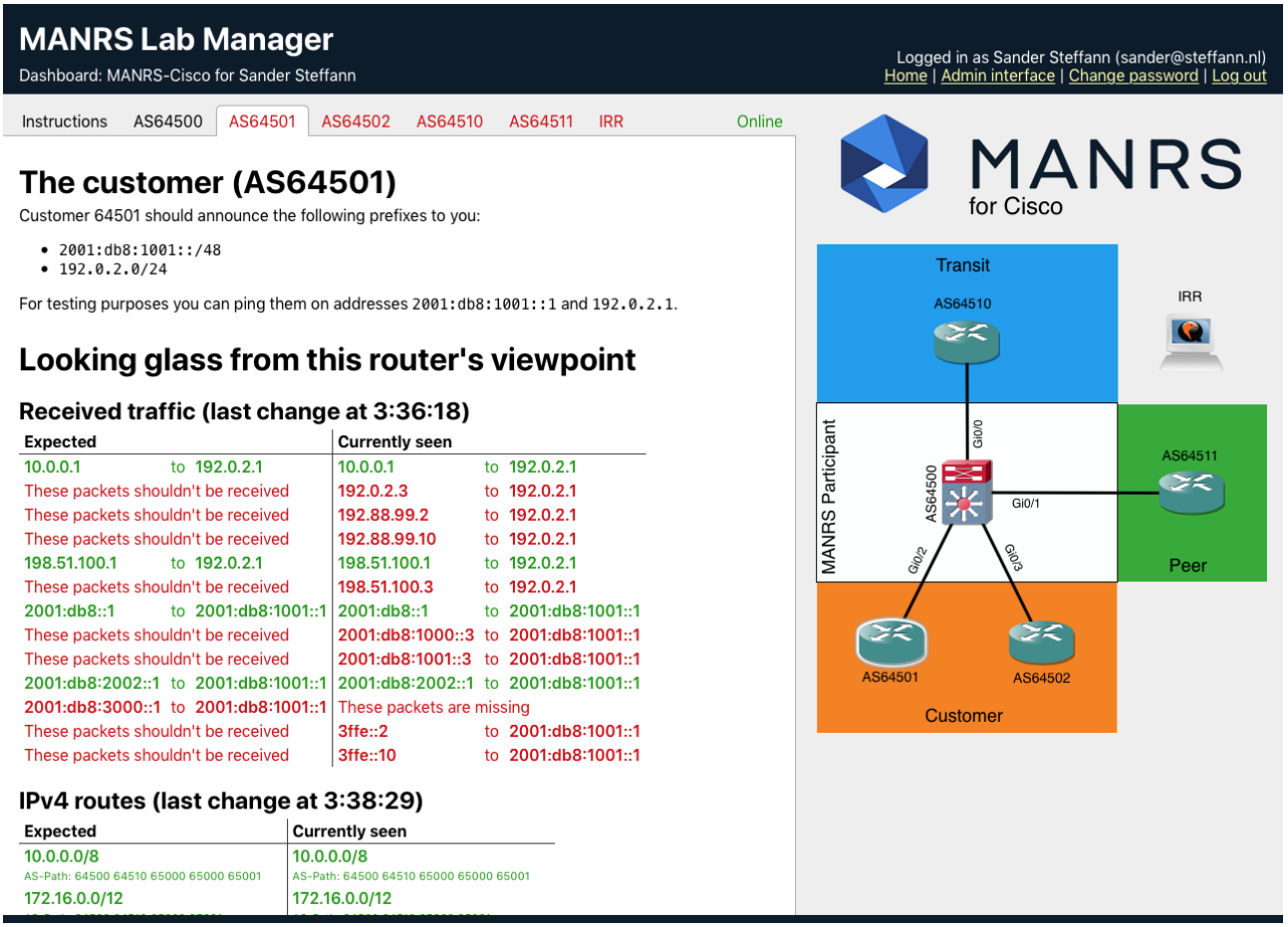
This tab contains the interface to the router you'll be working on. It contains basic information about your router and a terminal window for the router's console:



This is where you will do most of your work.

AS64501, AS64502, AS64510 and AS64511

These tabs contain information as seen from your neighbours points of view. It will show you which routes they receive from you and which traffic they receive through you:



The main part of these tabs is the looking glass that lets you see what is happening from the neighbour's point of view. We will now explain the different sections of information contained in the looking glass.

Received traffic

This section shows you the source and destination addresses of packets being received by this neighbour's router:

Received traffic (last change at 3:36:18)

Expected	Currently seen
10.0.0.1 to 192.0.2.1	10.0.0.1 to 192.0.2.1
These packets shouldn't be received	192.0.2.3 to 192.0.2.1
These packets shouldn't be received	192.88.99.2 to 192.0.2.1
These packets shouldn't be received	192.88.99.10 to 192.0.2.1
198.51.100.1 to 192.0.2.1	198.51.100.1 to 192.0.2.1
These packets shouldn't be received	198.51.100.3 to 192.0.2.1
2001:db8::1 to 2001:db8:1001::1	2001:db8::1 to 2001:db8:1001::1
These packets shouldn't be received	2001:db8:1000::3 to 2001:db8:1001::1
These packets shouldn't be received	2001:db8:1001::3 to 2001:db8:1001::1
2001:db8:2002::1 to 2001:db8:1001::1	2001:db8:2002::1 to 2001:db8:1001::1
2001:db8:3000::1 to 2001:db8:1001::1	These packets are missing
These packets shouldn't be received	3ffe::2 to 2001:db8:1001::1
These packets shouldn't be received	3ffe::10 to 2001:db8:1001::1

As you can see in the screenshot above there are packets being received that shouldn't be received. This is probably because they are sent with spoofed source addresses. There are also packets that should have been received but aren't. Could it be that someone is hijacking traffic? Of course there is also legitimate traffic. Make sure that you don't filter that out!

IPv4 routes

This part of the looking glass shows you the IPv4 routes that are received by your neighbour:

IPv4 routes (last change at 3:38:29)

Expected	Currently seen
10.0.0.0/8 AS-Path: 64500 64510 65000 65000 65001	10.0.0.0/8 AS-Path: 64500 64510 65000 65000 65001
172.16.0.0/12 AS-Path: 64500 64510 65002 65001	172.16.0.0/12 AS-Path: 64500 64510 65002 65001
This route shouldn't be received	192.0.2.64/26 AS-Path: 64500 64502
This route shouldn't be received	192.0.2.128/25 AS-Path: 64500 64502
192.168.0.0/16 AS-Path: 64500 64510 65002 65003	192.168.0.0/16 AS-Path: 64500 64510 65002 65003
198.51.100.0/24 AS-Path: 64500 64502	198.51.100.0/24 AS-Path: 64500 64502
203.0.113.0/24 AS-Path: 64500	203.0.113.0/24 AS-Path: 64500
This route shouldn't be received	203.0.113.64/26 AS-Path: 64500 64510

In the example above some routes are received that shouldn't be. Make sure that you announce exactly the right routes to your neighbours! That is usually done with both filtering which routes you accept and which routes you announce.

https://manrs.nog-oc.org/

username: manrs

password: manrs

MANRS Action 2: Anti Spoofing

Lab 1: Anti-Spoofing

a. Access Lists

b. uRPF (Unicast Resource Path Forwarding)

Context: One of the ways attackers can affect the network is by sending spoofed packets, using IPs that do not belong to them.

Solution: On each interface connecting to an outside network, make sure packets sourced from your IP block are dropped. All vendors have a feature to verify and drop such spoofed packets. So, you can either use the feature shipped with your router or create and apply an ACL on the corresponding interface.

a) Anti-spoofing using ACL (Access Control Lists)

Here, we will create an access list to deny packet sourced from the block

- 203.0.113.0/24 (AS64500)
- 192.0.2.0/24 (AS64501)
- 198.51.100.0/24 (AS64502)

Creating the ACL

as64500# configure terminal

as64500(config)# ip access-list ext anti-spoof510

as64500(config-ext-nacl)# deny ip 203.0.113.0 0.0.0.255 any

as64500(config-ext-nacl)# deny ip 192.0.2.0 0.0.0.255 any

as64500(config-ext-nacl)# deny ip 198.51.100.0 0.0.0.255 any

as64500(config-ext-nacl)# permit ip any any

as64500(config-ext-nacl)# exit

as64500# configure terminal

as64500(config)# ip access-list ext anti-spoof511

as64500(config-ext-nacl)# deny ip any any

```
as64500(config-ext-nacl)# exit

as64500# configure terminal
as64500(config)# ip access-list ext anti-spoof501
as64500(config-ext-nacl)# permit ip 192.0.2.0 0.0.0.255 any
as64500(config-ext-nacl)# deny ip any any
as64500(config-ext-nacl)# exit

as64500# configure terminal
as64500(config)# ip access-list ext anti-spoof502
as64500(config-ext-nacl)# permit ip 198.51.100.0 0.0.0.255 any
as64500(config-ext-nacl)# deny ip any any
as64500(config-ext-nacl)# exit
```

Applying the ACLs to the interface

```
as64500(config)#interface gi0/0
as64500(config-if)#ip access-group anti-spoof510 in

as64500(config)#interface gi0/1
as64500(config-if)#ip access-group anti-spoof511 in

as64500(config)#interface gi0/2
as64500(config-if)#ip access-group anti-spoof501 in

as64500(config)#interface gi0/3
as64500(config-if)#ip access-group anti-spoof502 in
```

Note that for interfaces connecting to AS64501 and 64502, you only need to block their respectives IPblocks and not the block of AS64500 as well as the other customer.

Configuring uRPF (Unicast Reverse Path Forwarding) (Recommended Solution)

uRPF is an effective solution against defeating DoS attacks.

Strict Mode

- Source address must be reachable via the source (incoming) interface

Loose Mode

- Source address must be in the FIB
- Typically used to drop non-routed address blocks
- Can be used in designs where asymmetric traffic flows are present (multihomed networks)

```
as64500#configure terminal
as64500(config)#interface gigabitEthernet 0/0
as64500(config-if)#ip verify unicast source reachable-via rx
as64500(config-if)#ipv6 verify unicast source reachable-via rx
as64500(config-if)#exit
as64500(config)#
as64500(config)#interface gigabitEthernet 0/1
as64500(config-if)#ip verify unicast source reachable-via rx
as64500(config-if)#ipv6 verify unicast source reachable-via rx
as64500(config-if)#exit
as64500(config)#
as64500(config)#interface gigabitEthernet 0/2
as64500(config-if)#ip verify unicast source reachable-via rx
as64500(config-if)#ipv6 verify unicast source reachable-via rx
as64500(config-if)#exit
as64500(config)#
as64500(config)#interface gigabitEthernet 0/3
as64500(config-if)#ip verify unicast source reachable-via rx
as64500(config-if)#ipv6 verify unicast source reachable-via rx
as64500(config-if)#exit
```

Verification#

show cef interface gig0/0

show cef int gig 0/2 | inc RPF

show ip interface gig0/0

show ipv6 interface gig0/0

show ip interface gig 0/2 | include drop

show ipv6 interface gig 0/2 | inc drop

show ip traffic

show ipv6 traffic

as64500#show cef interface gigabitEthernet 0/0

GigabitEthernet0/0 is up (if_number 2)
  Corresponding hwidb fast_if_number 2
  Corresponding hwidb firstsw->if_number 2
  Internet address is 192.168.255.255/31
  ICMP redirects are never sent
  Per packet load-sharing is disabled
  IP unicast RPF check is enabled
  Input features: uRPF
  IP policy routing is disabled
  BGP based policy accounting on input is disabled
  BGP based policy accounting on output is disabled
  IPv6 CEF switching enabled
  Hardware idb is GigabitEthernet0/0
  Fast switching type 1, interface type 27
  IP CEF switching enabled
  IP CEF switching turbo vector
  IP prefix lookup IPv4 mtrie 8-8-8-8 optimized
  Input fast flags 0x4000, Output fast flags 0x0
  ifindex 2(2)
  Slot Slot unit 0 VC -1
  IP MTU 1500
as64500#

```
as64500#show ip int gig 0/2 | include drop
  324 verification drops
  0 suppressed verification drops
  0 verification drop-rate
as64500#

as64500#show ipv6 int gig 0/2 | include drop
  0 verification drop(s) (process), 896 (CEF)
  0 suppressed verification drop(s) (process), 0 (CEF)
as64500#

as64500#show ip traffic
IP statistics:
  Rcvd:  38933381 total, 124110 local destination
         0 format errors, 0 checksum errors, 0 bad hop count
         0 unknown protocol, 0 not a gateway
         0 security failures, 0 bad options, 0 with options
  Mcast: 0 received, 0 sent
  Sent:  26056072 generated, 134183450 forwarded
 Drop:  99423 encapsulation failed, 0 unresolved, 0 no adjacency
         25787724 no route, 56669 unicast RPF, 0 forced drop
         0 options denied
  Drop:  0 packets with source IP address zero

as64500#show ip traffic | inc drop
        4462 no route, 1812 unicast RPF, 0 forced drop
  Queue drops: 0
  Queue drops: 0
as64500#

as64500#show ipv6 traffic | inc drop
            2940 RPF drops, 0 RPF suppressed drops
        0 no port, 0 dropped
as64500#
```

MANRS Action 1: Filtering

Lab 2: IPv4/IPv6 Filtering

Filtering – Preventing propagation of incorrect routing information

Relevant MANRS expected actions:

- Network operator defines a clear routing policy and implements a system that ensures correctness of their own announcements and announcements from their customers to adjacent networks with prefix and AS-path granularity.
- Network operator applies due diligence when checking the correctness of its customer's announcements, specifically that the customer legitimately holds the ASN and the address space it announces.

https://www.manrs.org/isps/guide/filtering/

Tasks:

A. to filter incoming routes announced by your customers AS64501 and AS64502
B. to filter incoming routes announced by your transit provider AS64510
C. to filter incoming routes announced by your peer AS64511
D. to filter outgoing routes as you announce them to your customers, peer and transit

[A] Filter incoming IPv4 routes announced by your customers AS64501 and AS64502

Customer 1: (AS64501)

ip prefix-list AS64501-v4 permit **192.0.2.0/24**

ip prefix-list AS64501-v4 deny 0.0.0.0/0 le 32

Customer 2: (AS64502)

ip prefix-list AS64502-v4 permit 198.51.100.0/24

ip prefix-list AS64502-v4 deny 0.0.0.0/0 le 32

Applying the Prefix-list to the Customers (AS64501, AS64502)

router bgp 64500
address-family ipv4 unicast
  neighbor 203.0.113.253 prefix-list AS64501-v4 in
  neighbor 203.0.113.255 prefix-list AS64502-v4 in
 exit-address-family

#clear ip bgp * soft in

[B] Filter incoming routes announced by your transit provider AS64510

ip prefix-list DENY-OUR-v4 deny 203.0.113.0/24 le 32
ip prefix-list DENY-OUR-v4 deny 192.0.2.0/24 le 32
ip prefix-list DENY-OUR-v4 deny 198.51.100.0/24 le 32
!
Private Address, Benchmarking, Tesnet1,2,3, APIPA, CGNAT.
ip prefix-list DENY-OUR-v4 permit 0.0.0.0/0 le **24**

Apply the prefix-list to the Transit

router bgp 64500
address-family ipv4 unicast
neighbor 192.168.255.254 prefix-list DENY-OUR-v4 in

#clear ip bgp * soft in

[C] Filter incoming routes announced by your peer AS64511

The Peer should not announce any IPv4 Prefix to AS64500)

ip prefix-list AS64511-v4 deny 0.0.0.0/0 le 32

Apply the prefix-list to the Peer

router bgp 64500

address-family ipv4 unicast

neighbor 203.0.113.251 prefix-list AS64511-v4 in

[D] Filter outgoing routes as you announce them to your customers, peer and transit

Create a Prefix list to advertise IPv4 Prefixes to the Transit and Peer.

ip prefix-list ANNOUNCE-v4 permit 203.0.113.0/24

ip prefix-list ANNOUNCE-v4 permit 192.0.2.0/24

ip prefix-list ANNOUNCE-v4 permit 198.51.100.0/24

ip prefix-list ANNOUNCE-v4 deny 0.0.0.0/0 le 32

Applying the Prefix List to the Transit and Peer eBGP neighbors

router bgp 64500

address-family ipv4 unicast

neighbor 192.168.255.254 prefix-list ANNOUNCE-v4 out

neighbor 203.0.113.251 prefix-list ANNOUNCE-v4 out

exit

#clear ip bgp * soft out

IPv6 Filtering

[A] Filter incoming routes announced by your customers AS64501 and AS64502

Customer 1: (AS64501)

ipv6 prefix-list AS64501-v6 permit 2001:db8:1001::/48

ipv6 prefix-list AS64501-v6 deny ::/0 le 128

Customer 2: (AS64502)

ipv6 prefix-list AS64502-v6 permit 2001:db8:2002::/48

ipv6 prefix-list AS64502-v6 deny ::/0 le 128

Applying the Prefix-list to the Customers

router bgp 64500

address-family ipv6 unicast

neighbor 2001:DB8:1000:FFFE::B prefix-list AS64501-v6 in
neighbor 2001:DB8:1000:FFFF::B prefix-list AS64502-v6 in

[B] Filter incoming IPv6 routes announced by your transit provider AS64510

ipv6 prefix-list DENY-OUR-v6 deny 2001:db8:1000::/36 le 128
ipv6 prefix-list DENY-OUR-v6 deny 2001:db8:1001::/48 le 128
ipv6 prefix-list DENY-OUR-v6 deny 2001:db8:2002::/48 le 128
ipv6 prefix-list DENY-OUR-v6 permit ::/0 le 48

Apply the IPv6 prefix-list to the Transit

router bgp 64500
address-family ipv6 unicast
neighbor 2001:DB8:F000:FFFF::A prefix-list DENY-OUR-v6 in
exit-address-family

#clear bgp ipv6 unicast * soft in

[C] Filter incoming routes announced by your peer AS64511

The Peer should announce only the prefix 2001:db8:3000::/36 to AS64500

ipv6 prefix-list AS64511-v6 permit 2001:db8:3000::/36 le 48
ipv6 prefix-list AS64511-v6 deny ::/0 le 48

Apply the IPv6 prefix-list to the Peer

router bgp 64500
address-family ipv6 unicast
neighbor 2001:DB8:1000:FFFD::B prefix-list AS64511-v6 in
exit-address-family

#clear bgp ipv6 unicast * soft in
#clear bgp * ipv6 unicast 2001:DB8:F000:FFFF::A soft in

[D] Filter outgoing routes as you announce them to your customers, peer and transit

Create a Prefix list to advertise IPv6 Prefixes to the Transit and Peer

ipv6 prefix-list ANNOUNCE-v6 permit 2001:db8:1000::/36

ipv6 prefix-list ANNOUNCE-v6 permit 2001:db8:1001::/48

ipv6 prefix-list ANNOUNCE-v6 permit 2001:db8:2002::/48

ipv6 prefix-list ANNOUNCE-v6 deny ::/0 le 128

Applying the Prefix List to the Transit and Peer eBGP neighbors

router bgp 64500

address-family ipv6 unicast

neighbor 2001:DB8:1000:FFFD::B prefix-list ANNOUNCE-v6 out

neighbor 2001:DB8:F000:FFFF::A prefix-list ANNOUNCE-v6 out

exit-address-family

#clear bgp ipv6 unicast * soft out

#clear bgp * ipv6 unicast 2001:DB8:F000:FFFF::A soft out

#clear bgp * ipv6 unicast 2001:DB8:F000:FFFD::B soft out

Lab 3: Configuring Max Prefix Limit

```
as64500(config)#router bgp 64500
as64500(config-router)#
as64500(config-router)#address-family ipv4 unicast
as64500(config-router-af)#neighbor 192.168.255.254 maximum-prefix ?
  <1-2147483647>  maximum no. of prefix limit
```

as64500(config-router-af)#neighbor 192.168.255.254 maximum-prefix 200 ?

```
  <1-100>        Threshold value (%) at which to generate a warning msg
  restart        Restart bgp connection after limit is exceeded
  warning-only   Only give warning message when limit is exceeded
  <cr>
```

Show running configuration for AS64500 Router

```
as64500#show run
Building configuration...

Current configuration : 6403 bytes
!
! Last configuration change at 04:51:34 UTC Sat Jun 19 2021 by manrs
!
version 15.6
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname as64500

****************Output Omitted**********************************
!
interface GigabitEthernet0/0
 description To AS64510 - Transit
 ip address 192.168.255.255 255.255.255.254
 no ip redirects
 ip verify unicast source reachable-via rx
 duplex auto
 speed auto
 media-type rj45
 ipv6 address 2001:DB8:F000:FFFF::B/127
 no ipv6 redirects
 ipv6 verify unicast source reachable-via rx
!
interface GigabitEthernet0/1
 description To AS64511 - Peer
```

```
 ip address 203.0.113.250 255.255.255.254
 no ip redirects
 ip verify unicast source reachable-via rx
 duplex auto
 speed auto
 media-type rj45
 ipv6 address 2001:DB8:1000:FFFD::A/127
 no ipv6 redirects
 ipv6 verify unicast source reachable-via rx
!
interface GigabitEthernet0/2
 description To AS64501 - Customer
 ip address 203.0.113.252 255.255.255.254
 no ip redirects
 ip verify unicast source reachable-via rx
 duplex auto
 speed auto
 media-type rj45
 ipv6 address 2001:DB8:1000:FFFE::A/127
 no ipv6 redirects
 ipv6 verify unicast source reachable-via rx
!
interface GigabitEthernet0/3
 description To AS64502 - Customer
 ip address 203.0.113.254 255.255.255.254
 no ip redirects
 ip verify unicast source reachable-via rx
 duplex auto
 speed auto
 media-type rj45
 ipv6 address 2001:DB8:1000:FFFF::A/127
 no ipv6 redirects
 ipv6 verify unicast source reachable-via rx
!
interface GigabitEthernet0/4
```

```
 no ip address
 shutdown
 duplex auto
 speed auto
 media-type rj45
!
router bgp 64500
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor 2001:DB8:1000:FFFD::B remote-as 64511
 neighbor 2001:DB8:1000:FFFD::B description Peer
 neighbor 2001:DB8:1000:FFFE::B remote-as 64501
 neighbor 2001:DB8:1000:FFFE::B description Customer
 neighbor 2001:DB8:1000:FFFF::B remote-as 64502
 neighbor 2001:DB8:1000:FFFF::B description Customer
 neighbor 2001:DB8:F000:FFFF::A remote-as 64510
 neighbor 2001:DB8:F000:FFFF::A description Transit
 neighbor 192.168.255.254 remote-as 64510
 neighbor 192.168.255.254 description Transit
 neighbor 203.0.113.251 remote-as 64511
 neighbor 203.0.113.251 description Peer
 neighbor 203.0.113.253 remote-as 64501
 neighbor 203.0.113.253 description Customer
 neighbor 203.0.113.255 remote-as 64502
 neighbor 203.0.113.255 description Customer
 !
 address-family ipv4
  network 203.0.113.0
  neighbor 192.168.255.254 activate
  neighbor 192.168.255.254 prefix-list DENY-OUR-v4 in
  neighbor 192.168.255.254 prefix-list ANNOUNCE-v4 out
  neighbor 203.0.113.251 activate
  neighbor 203.0.113.251 prefix-list AS64511-v4 in
  neighbor 203.0.113.251 prefix-list ANNOUNCE-v4 out
  neighbor 203.0.113.253 activate
```

```
  neighbor 203.0.113.253 prefix-list AS64501-v4 in
  neighbor 203.0.113.255 activate
  neighbor 203.0.113.255 prefix-list AS64502-v4 in
 exit-address-family
 !
 address-family ipv6
  network 2001:DB8:1000::/36
  neighbor 2001:DB8:1000:FFFD::B activate
  neighbor 2001:DB8:1000:FFFD::B prefix-list AS64511-v6 in
  neighbor 2001:DB8:1000:FFFD::B prefix-list ANNOUNCE-v6 out
  neighbor 2001:DB8:1000:FFFE::B activate
  neighbor 2001:DB8:1000:FFFE::B prefix-list AS64501-v6 in
  neighbor 2001:DB8:1000:FFFF::B activate
  neighbor 2001:DB8:1000:FFFF::B prefix-list AS64502-v6 in
  neighbor 2001:DB8:F000:FFFF::A activate
  neighbor 2001:DB8:F000:FFFF::A prefix-list DENY-OUR-v6 in
  neighbor 2001:DB8:F000:FFFF::A prefix-list ANNOUNCE-v6 out
 exit-address-family
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip route 203.0.113.0 255.255.255.0 Null0
!
!
ip prefix-list ANNOUNCE-v4 seq 5 permit 203.0.113.0/24
ip prefix-list ANNOUNCE-v4 seq 10 permit 192.0.2.0/24
ip prefix-list ANNOUNCE-v4 seq 15 permit 198.51.100.0/24
ip prefix-list ANNOUNCE-v4 seq 20 deny 0.0.0.0/0 le 32
!
ip prefix-list AS64501-v4 seq 5 permit 192.0.2.0/24
ip prefix-list AS64501-v4 seq 10 deny 0.0.0.0/0 le 32
!
```

```
ip prefix-list AS64502-v4 seq 5 permit 198.51.100.0/24
ip prefix-list AS64502-v4 seq 10 deny 0.0.0.0/0 le 32
!
ip prefix-list AS64511-v4 seq 5 deny 0.0.0.0/0 le 32
!
ip prefix-list DENY-OUR-v4 seq 5 deny 203.0.113.0/24 le 32
ip prefix-list DENY-OUR-v4 seq 10 deny 192.0.2.0/24 le 32
ip prefix-list DENY-OUR-v4 seq 15 deny 198.51.100.0/24 le 32
ip prefix-list DENY-OUR-v4 seq 20 permit 0.0.0.0/0 le 32
ipv6 route 2001:DB8:1000::/36 Null0
!
!
ipv6 prefix-list ANNOUNCE-v6 seq 5 permit 2001:DB8:1000::/36
ipv6 prefix-list ANNOUNCE-v6 seq 10 permit 2001:DB8:1001::/48
ipv6 prefix-list ANNOUNCE-v6 seq 15 permit 2001:DB8:2002::/48
ipv6 prefix-list ANNOUNCE-v6 seq 20 deny ::/0 le 128
!
ipv6 prefix-list AS64501-v6 seq 5 permit 2001:DB8:1001::/48
ipv6 prefix-list AS64501-v6 seq 10 deny ::/0 le 128
!
ipv6 prefix-list AS64502-v6 seq 5 permit 2001:DB8:2002::/48
ipv6 prefix-list AS64502-v6 seq 10 deny ::/0 le 128
!
ipv6 prefix-list AS64511-v6 seq 5 permit 2001:DB8:3000::/36 le 48
ipv6 prefix-list AS64511-v6 seq 10 deny ::/0 le 48
!
ipv6 prefix-list DENY-OUR-v6 seq 5 deny 2001:DB8:1000::/36 le 128
ipv6 prefix-list DENY-OUR-v6 seq 10 deny 2001:DB8:1001::/48 le 128
ipv6 prefix-list DENY-OUR-v6 seq 15 deny 2001:DB8:2002::/48 le 128
ipv6 prefix-list DENY-OUR-v6 seq 20 permit ::/0 le 48
!
********************************************************************************
!
end
```