An assignment report on

BGP Lab 2

Submitted for fufillment of award of
Bachelor of Computing and Network Communications
degree

By
Chance Page
11/11/2024

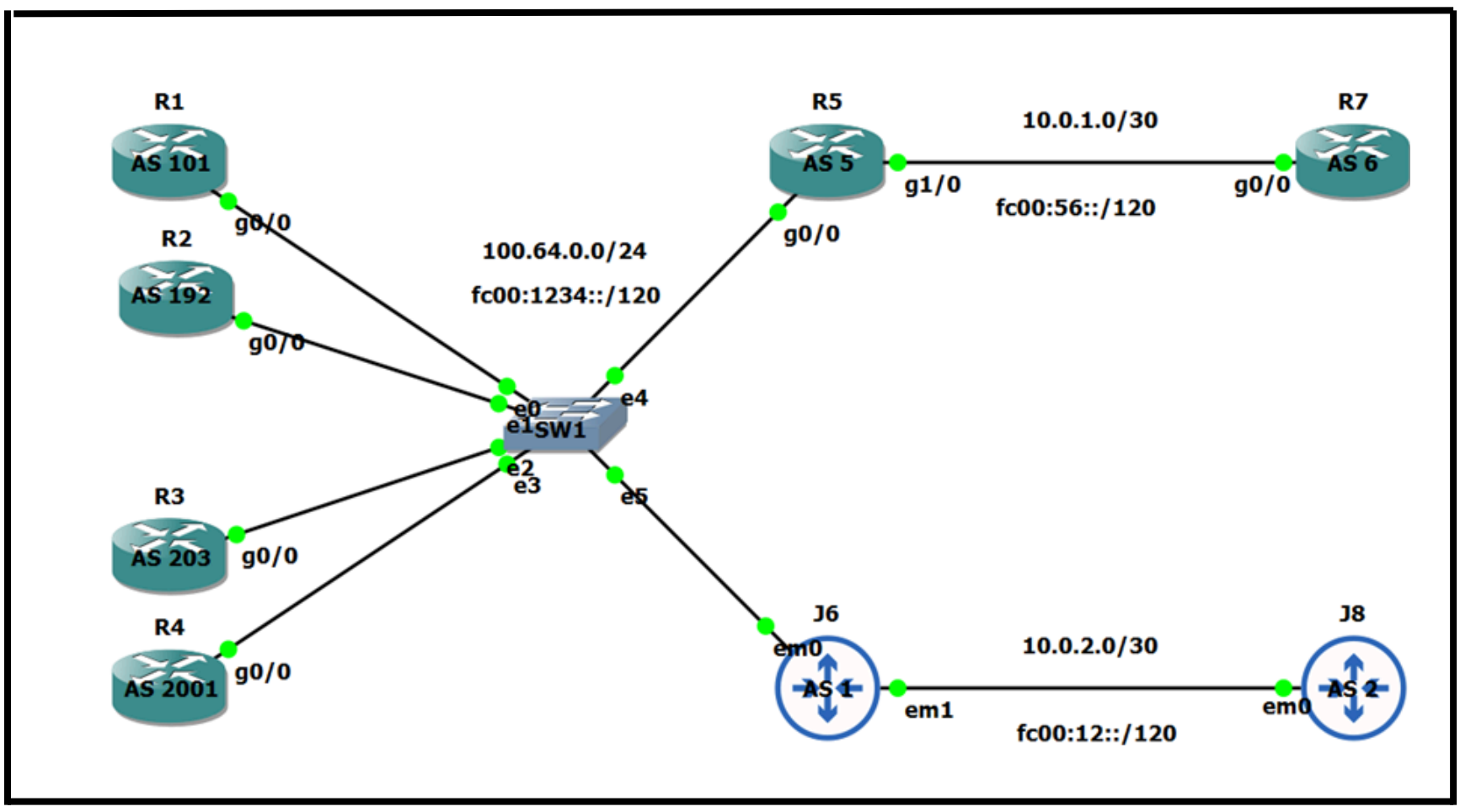
Sheridan College
Faculty of Applied Science & Technology
Professor. Felix Carapaica
Network Engineering 3
TELE31063

Table of Contents

Introduction

In this assignment, we will explore and implement a series of **BGP** (Border Gateway Protocol) **policies** designed to filter and manage **IPv4 and IPv6** prefixes based on specific Autonomous System (AS) criteria. By applying these policies on routers within a given topology, we aim to observe and analyze the effect of the **filtering rules** on the routes propagated and received by different routers. This will enhance our understanding of BGP's route filtering capabilities and the impact of AS path-based policies. We will also dive into **learning** about how to use **regex** within each operating system.

Network Topology



The network topology for this BGP policy assignment includes multiple routers from Cisco to Juniper, simulating a real-world environment for studying BGP route filtering. Routers **R1**, **R2**, **R3**, and **R4** act as feeders, sourcing a variety of prefixes. Routers **R5** and **J6** implement the same BGP policies, while **R7** and **J8** observe the results. This setup allows for thorough **testing** and **verification** of **BGP policies**, enhancing practical understanding of **route management**.

Preamble

In total, **50** policies were created and tested: **25 for Cisco** and **25 for Juniper**. I will **not be showing all the configurations**, just the **key** portions that involve the policies to complete the tasks. We will assume that the **policy accept and policy reject** commands are **correctly implemented**, and the policy export is **functioning as expected** to route traffic to the neighboring **AS 2** or **AS 6**. I also gave each router its own Loopback IP address corresponding to the router number ie: R1 has lo0 1.1.1.1/32

Challenges

During this assignment, I encountered some **challenges**. Specifically, I was unable to figure out how to filter routes based on **specific digits in Juniper for AS Numbers**, although I could do this with **Cisco**. The Juniper documentation **did not provide examples** or discussions about filtering routes based **on digits or patterns**, such as allowing only routes from AS numbers that include "20" (e.g., AS620, AS50200, AS201). I may have **missed something** in the documentation, but I believe that **filtering routes** based on **specific numbers within AS paths** is **neither correct nor efficient**. It seems **impractical** to filter routes based on the presence of a **particular digit**, as it could lead to a **confusing and non-future-proof configuration**.

Filtering routes based on specific digits within AS numbers can lead to **unintended consequences**. For example, if a policy is set to **forward routes** from any AS containing the digit "2", it could inadvertently permit routes from both **AS202 and AS22002**, despite the intent being to only include routes from a **specific set of ASes**. This could result in **increased complexity** in **managing and troubleshooting network issues**, as the policy might forward routes that were **not meant to be included**, complicating the network's **behavior and maintenance.**

Such filtering can d**isrupt the intended traffic flow** and compromise the **reliability and cost of the network**, making precise and well-defined routing policies crucial for **effective** network management.

Understanding AS Path Regular Expressions for Use as Routing Policy Match Conditions | Junos OS | Juniper Networks https://www.juniper.net/documentation/us/en/software/junos/routing-policy/topics/concept/policy-configuring-as-path-regular-expressions-to-use-as-routing-policy-match-conditions.html

Router 1 Network Spaces

VLAN #	Address space	Prefix	Mask /
2	4,096 addresses	101.0.0.0	/20
3	4,096 addresses	101.0.16.0	/20
4	8,192 addresses	101.0.32.0	/19
5	16,384 addresses	101.0.64.0	/18
6	32,768 addresses	101.0.128.0	/17
7	65,536 addresses	101.1.0.0	/16
8	131,072 addresses	101.2.0.0	/15
9	262,144 addresses	101.4.0.0	/14
10	524,288 addresses	101.8.0.0	/13
11	1,048,576 addresses	101.16.0.0	/12
12	2,097,152 addresses	101.32.0.0	/11
13	4,194,304 addresses	101.64.0.0	/10
14	8,388,608 addresses	101.128.0.0	/9
Loopback	1 address	1.1.1.1	/32

Router 2 Network Spaces

VLAN #	Address space	Prefix	Mask /
2	256 addresses	192.0.0.0	/24
3	256 addresses	192.0.1.0	/24
4	512 addresses	192.0.2.0	/23
5	1,024 addresses	192.0.4.0	/22
6	2,048 addresses	192.0.8.0	/21
7	4,096 addresses	192.0.16.0	/20
8	8,192 addresses	192.0.32.0	/19
9	16,384 addresses	192.0.64.0	/18
10	32,768 addresses	192.0.128.0	/17
Loopback	1 address	2.2.2.2	/32

Router 3 Network Spaces

VLAN #	Address space	Prefix	Mask /
2	8 addresses	203.0.0.0	/29
3	8 addresses	203.0.0.8	/29
4	16 addresses	203.0.0.16	/28
5	32 addresses	203.0.0.32	/27
6	64 addresses	203.0.0.64	/26
7	128 addresses	203.0.0.128	/25

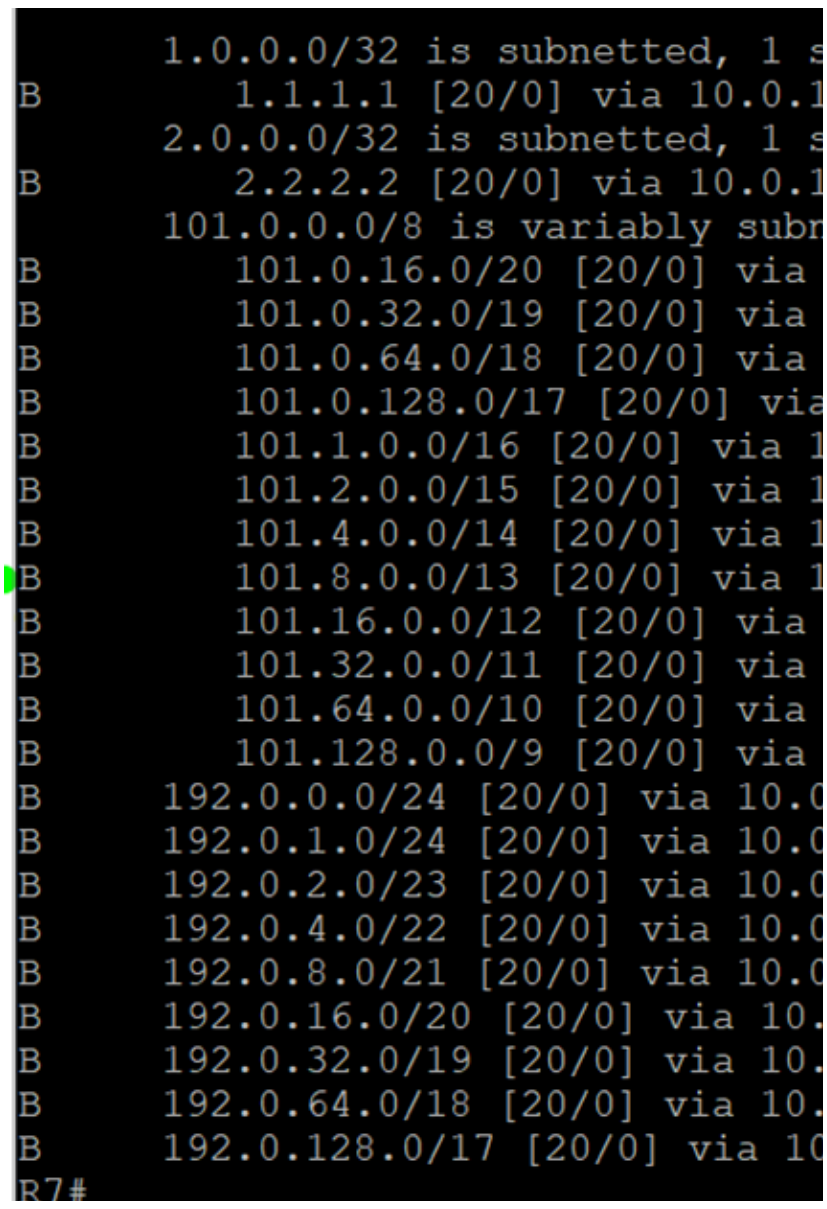
Router 4 Network Spaces

VLAN #	Prefix	Mask /
2	2001:4443:8000::	/34
3	2001:4443:C000::	/34
4	2001:4443:2000::	/35
5	2001:4444:3000::	/36
6	2001:4444:0000::	/37
7	2001:4444:0800::	/37
8	2001:4444:4000::	/34
9	2001:4444:8000::	/35
10	2001:4444:A000::	/35
11	2001:4444:C000::	/34
12	2001:4444:2000::	/36

Policy 1

Task: Allow only IPv4 prefixes originated in any AS that has a 1 in any place on the AS string.

Routes on R6



Policy on R5

This command permits BGP routes that have an AS path starting with any sequence of characters followed by _1 and any subsequent characters, allowing routes that include 1 anywhere in the AS path.

ip as-path access-list 1 permit ^_1.*_

Routes on J8

Policy on J6

I could not figure out how to catch the routes via Juniper regex. I tried a lot of different option but what I think should be the right command would be

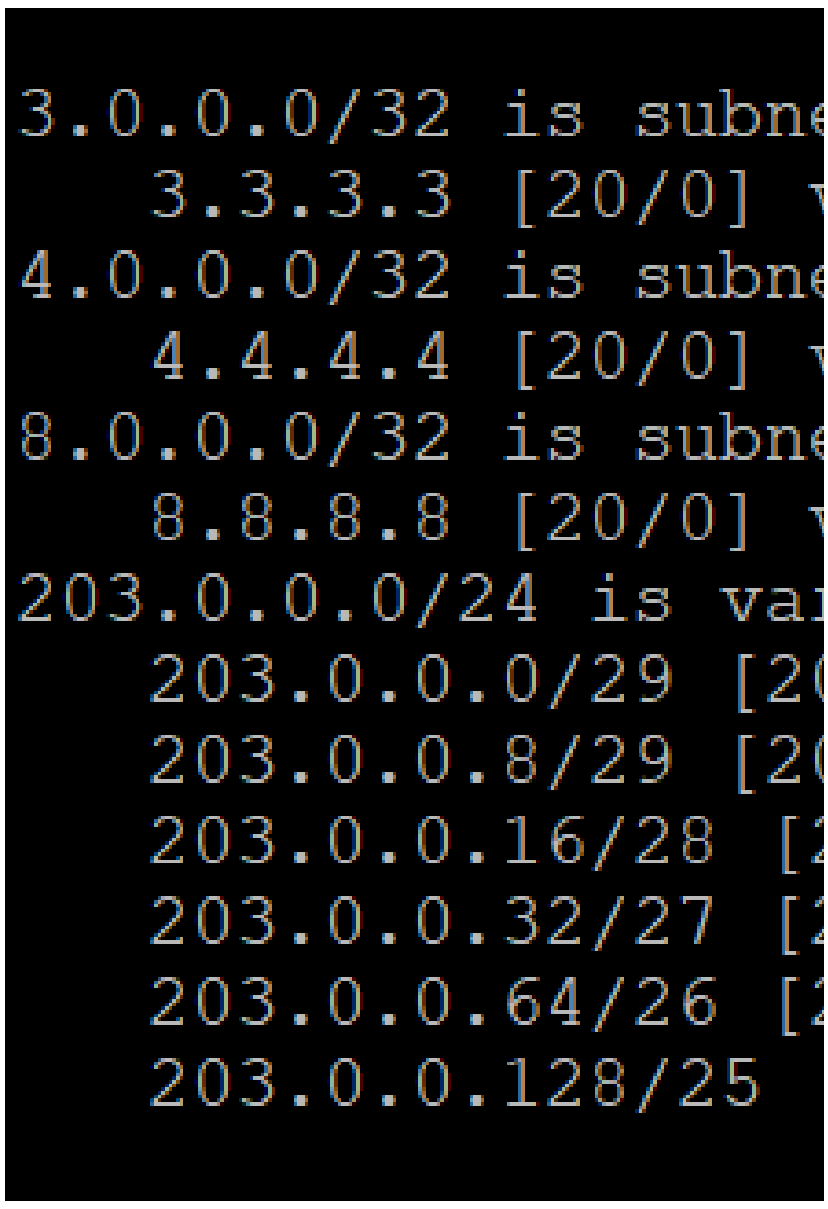
set policy-options as-path AS_PATH_1 "^([0-9]*1[0-9]*).*"

The regular expression **^([0-9]*1[0-9]*).*** matches AS paths containing the digit "1" anywhere within the path. The ^ denotes the start of the string, while **[0-9]*1[0-9]*** identifies any sequence of digits that includes **"1."** The **.*** ensures any following characters are included. **This effectively matches any AS path with a "1" in it.**

Policy 2

Task: Allow only prefixes originated in an AS that has a 2 someplace in the AS string.

Routes on R6



Policy on R5

This command permits BGP routes that have an AS path starting with any sequence of characters followed by _1 and any subsequent characters, allowing routes that include 1 anywhere in the AS path.
ip as-path access-list 1 permit ^_2.*_

We can see all the correct routes, additionally we can also see the loopback from AS2! 8.8.8.8/32

Routes on J8

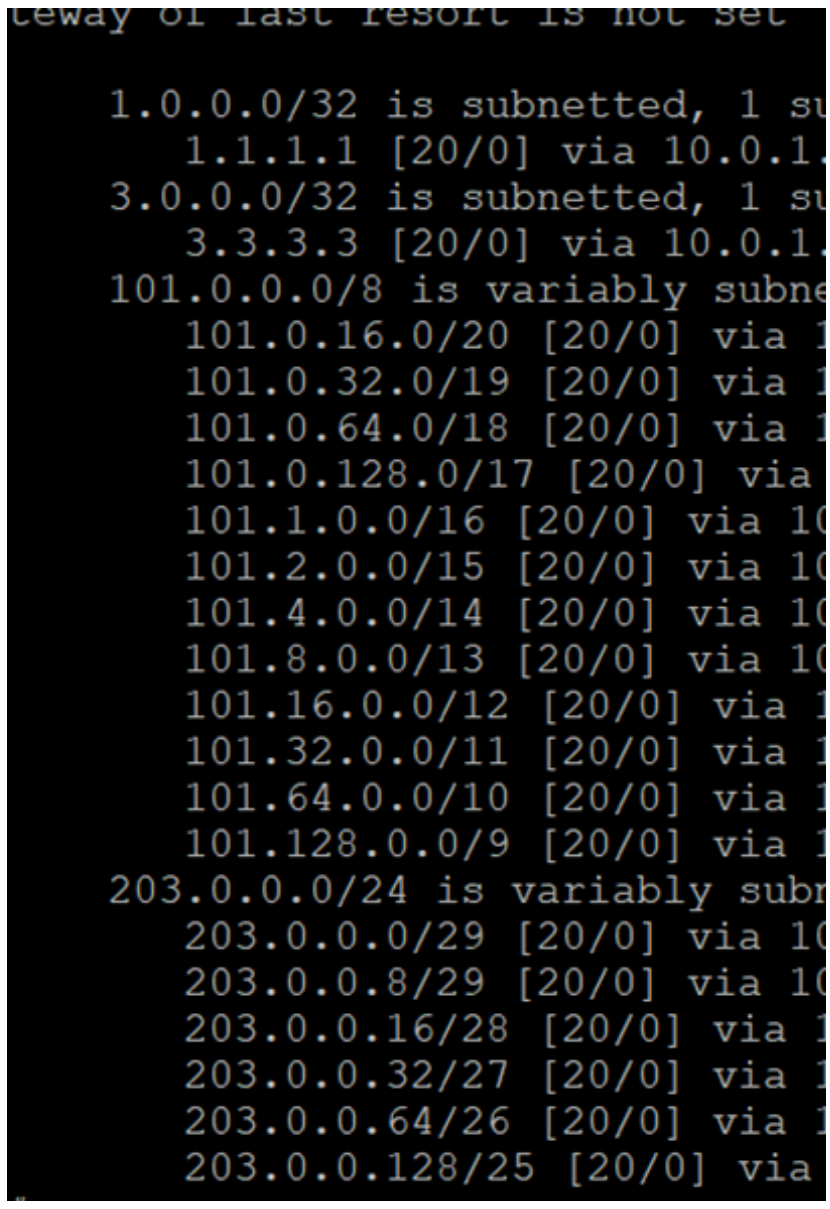
Policy on J6

This is what I think the correct expression is but is not,
set policy-options as-path AS_PATH_2 "^([0-9]*2[0-9]*).*"
The regular expression **^([0-9]*2[0-9]*).*** matches AS paths containing the **digit "2"** anywhere within the path. The ^ denotes the start of the string, while **[0-9]*2[0-9]*** identifies any sequence of digits that includes **"2."** The **.*** ensures any following characters are included. **This effectively matches any AS path with a "2" in it.**

Policy 3

Task: Allow only prefixes originated in either AS101 or AS203.

Routes on R6

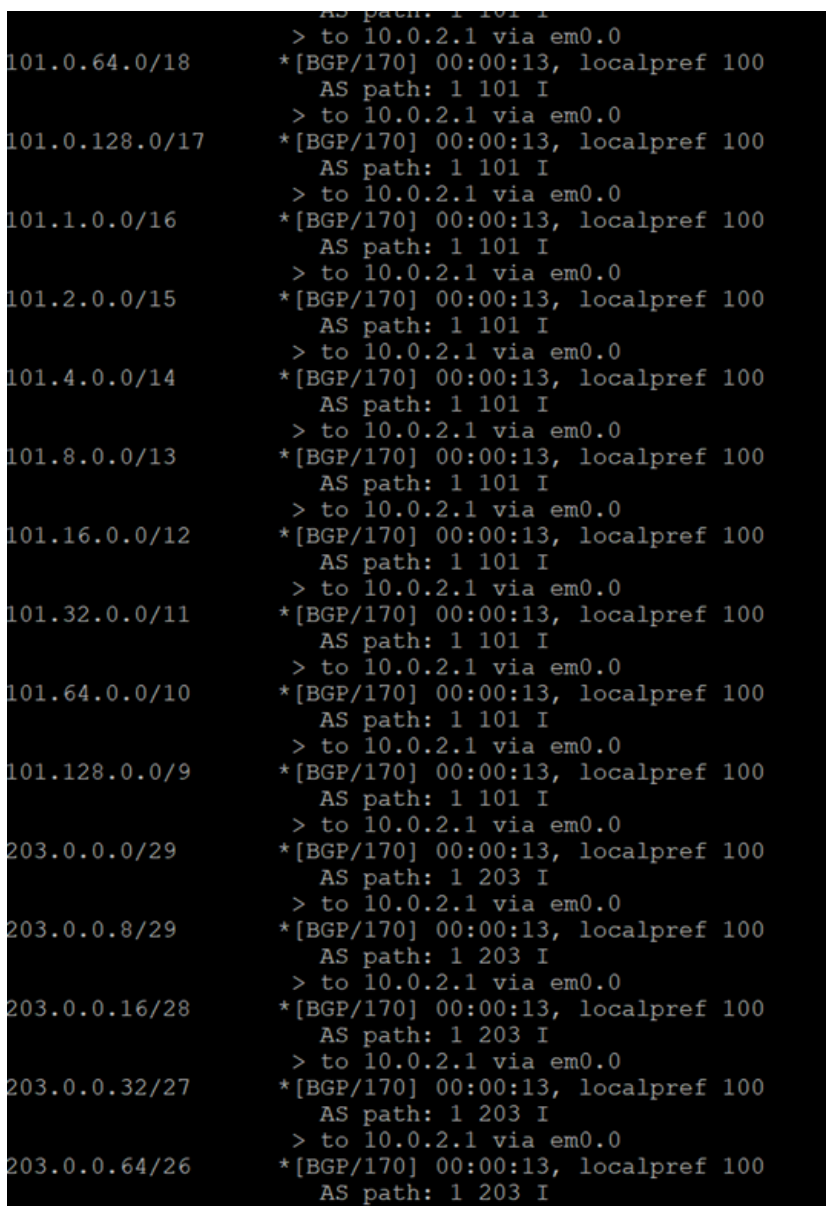


Policy on R5

The regular expression ^(101|203)$ is used to match AS paths that are exactly "101" or "203". The ^ denotes the start of the string, while (101|203) indicates that the AS path must be either "101" or "203". The $ signifies the end of the string. This ensures the AS path is strictly "101" or "203" without any additional digits before or after.

ip as-path access-list 1 permit ^(101|203)$

Routes on J8



Policy on J6

The regular expression ^(101|203)$ is designed to match AS paths that are exactly "101" or "203". The ^ symbol indicates the start of the string, while (101|203) specifies that the AS path must be either "101" or "203". The $ symbol denotes the end of the string. Together, this regex ensures that the AS path is exactly "101" or "203" without any other digits before or after.

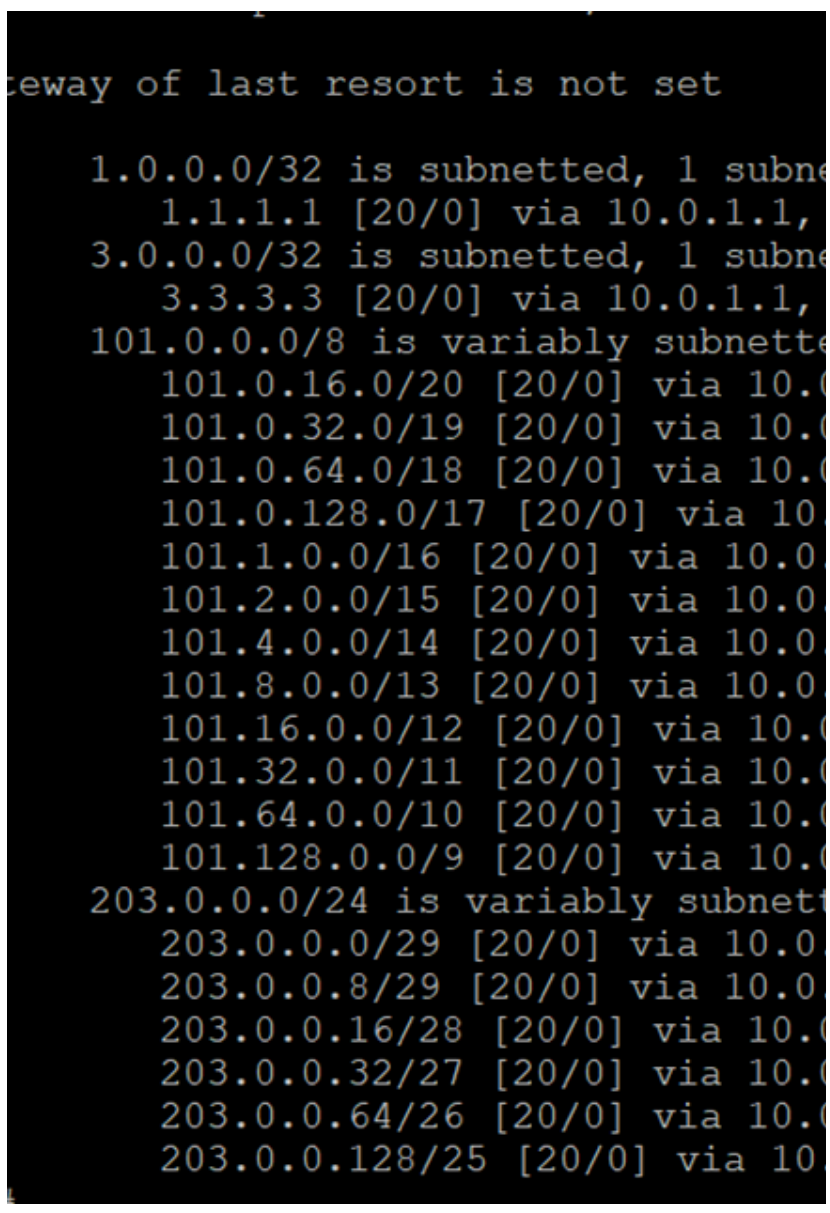
set policy-options as-path AS101_203 "^(101|203)$"

set policy-options policy-statement EXPORT term 1 from as-path AS101_203 then accept

Policy 4

Task: Allow only prefixes originated in an AS that has a 0 in the middle of the string, but it excludes AS2001.

Routes on R6



Policy on R5

These commands permit routes from AS paths containing the digit "0" within the AS path boundaries and deny prefixes exactly from AS2001. The regex _0_ matches any AS path including the digit "0" anywhere within it, while ^2001$ ensures that only the exact AS number 2001 is matched and blocked.

ip as-path access-list 10 permit _0_
ip as-path access-list 10 deny ^2001$

Routes on J8

Policy on J6

I said earlier I could not figure out how to filter the digits witihin an AS number but here are the commands that I thought would work.

set policy-options as-path AS_WITH_0 “^([0-9]*0[0-9]*).*”
set policy-options as-path REJECT_2001 "^2001$"

Policy 5

Task: Allow only IPv4 prefixes that used to belong to Class A.

Routes on R6

```
ateway of last resort is not set

     1.0.0.0/32 is subnetted, 1 sub
        1.1.1.1 [20/0] via 10.0.1.1
     2.0.0.0/32 is subnetted, 1 sub
        2.2.2.2 [20/0] via 10.0.1.1
     3.0.0.0/32 is subnetted, 1 sub
        3.3.3.3 [20/0] via 10.0.1.1
     4.0.0.0/32 is subnetted, 1 sub
        4.4.4.4 [20/0] via 10.0.1.1
     5.0.0.0/32 is subnetted, 1 sub
        5.5.5.5 [20/0] via 10.0.1.1
     8.0.0.0/32 is subnetted, 1 sub
        8.8.8.8 [20/0] via 10.0.1.1
     101.0.0.0/8 is variably subnet
        101.0.16.0/20 [20/0] via 10
        101.0.32.0/19 [20/0] via 10
        101.0.64.0/18 [20/0] via 10
        101.0.128.0/17 [20/0] via 1
        101.1.0.0/16 [20/0] via 10.
        101.2.0.0/15 [20/0] via 10.
        101.4.0.0/14 [20/0] via 10.
        101.8.0.0/13 [20/0] via 10.
        101.16.0.0/12 [20/0] via 10
        101.32.0.0/11 [20/0] via 10
        101.64.0.0/10 [20/0] via 10
        101.128.0.0/9 [20/0] via 10
7#
```

Policy on R5

This range encompasses all IP addresses that start with a binary 0, covering the entire Class A address space. It means any IP address within this range will be allowed by access list 10. This can be useful for filtering or allowing a large block of IP addresses in network access control.

access-list 10 permit 0.0.0.0 127.255.255.255

Routes on J8

```
                   AS path: 1 203 I
                  > to 10.0.2.1 via em0.0
1.4.4.4/32         *[BGP/170] 00:00:01, localpref 100
                   AS path: 1 2001 I
                  > to 10.0.2.1 via em0.0
5.5.5.5/32         *[BGP/170] 00:00:01, localpref 100
                   AS path: 1 101 5 I
                  > to 10.0.2.1 via em0.0
5.6.6.6/32         *[BGP/170] 00:00:01, localpref 100
                   AS path: 1 I
                  > to 10.0.2.1 via em0.0
7.7.7.7/32         *[BGP/170] 00:00:01, localpref 100
                   AS path: 1 101 5 6 I
                  > to 10.0.2.1 via em0.0
8.8.8.8/32         *[Direct/0] 01:35:53
                  > via lo0.0
10.0.2.0/30        *[Direct/0] 01:35:53
                  > via em0.0
                   [BGP/170] 00:00:01, localpref 100
                   AS path: 1 I
                  > to 10.0.2.1 via em0.0
10.0.2.2/32        *[Local/0] 01:35:53
                   Local via em0.0
100.64.0.0/24      *[BGP/170] 00:00:01, localpref 100
                   AS path: 1 I
                  > to 10.0.2.1 via em0.0
101.0.16.0/20      *[BGP/170] 00:00:01, localpref 100
                   AS path: 1 101 I
                  > to 10.0.2.1 via em0.0
101.0.32.0/19      *[BGP/170] 00:00:01, localpref 100
                   AS path: 1 101 I
                  > to 10.0.2.1 via em0.0
101.0.64.0/18      *[BGP/170] 00:00:01, localpref 100
                   AS path: 1 101 I
                  > to 10.0.2.1 via em0.0
101.0.128.0/17     *[BGP/170] 00:00:01, localpref 100
                   AS path: 1 101 I
                  > to 10.0.2.1 via em0.0
101.1.0.0/16       *[BGP/170] 00:00:01, localpref 100
                   AS path: 1 101 I
                  > to 10.0.2.1 via em0.0
101.2.0.0/15       *[BGP/170] 00:00:01, localpref 100
                   AS path: 1 101 I
                  > to 10.0.2.1 via em0.0
101.4.0.0/14       *[BGP/170] 00:00:01, localpref 100
                   AS path: 1 101 I
```

Policy on J6

This command in Juniper configures a policy statement to match and export any route that falls within the 0.0.0.0/1 prefix or longer. It effectively covers all IP addresses from 0.0.0.0 to 127.255.255.255, allowing routes within this range to be included in the export policy.

set policy-options policy-statement EXPORT term 1 from route-filter 0.0.0.0/1 orlonger

Policy 6

Task: Allow only IPv4 prefixes that used to belong to Class B.

Routes on R6

Policy on R5

All of the networks involved were **not** in a **Class B** address so there were **no results** for the Cisco Policy or the Juniper but I will list the commands I used.

access-list 10 permit 128.0.0.0 0.63.255.255

Routes on J8

Policy on J6

set policy-options policy-statement EXPORT term 1 from route-filter 128.0.0.0/2 orlonger

Policy 7

Task: Allow only IPv4 prefixes that used to belong to Class C.

Routes on R6

```
192.0.0.0/24 [20/0] v
192.0.1.0/24 [20/0] v
192.0.2.0/23 [20/0] v
192.0.4.0/22 [20/0] v
192.0.8.0/21 [20/0] v
192.0.16.0/20 [20/0]
192.0.32.0/19 [20/0]
192.0.64.0/18 [20/0]
192.0.128.0/17 [20/0]
203.0.0.0/24 is varia
    203.0.0.0/29 [20/0
    203.0.0.8/29 [20/0
    203.0.0.16/28 [20/
    203.0.0.32/27 [20/
    203.0.0.64/26 [20/
    203.0.0.128/25 [20
```

Policy on R5

This Cisco access-list rule exports routes from all Class C networks (192.0.0.0 to 223.255.255.255) to the neighboring Autonomous System (AS) 6. By doing this, it ensures that these routes are shared.

access-list 10 permit 192.0.0.0 31.255.255.255

Routes on J8

```
192.0.1.0/24       *[BGP/170] 00:02:00, localpref 100
                      AS path: 1 192 I
                    > to 10.0.2.1 via em0.0
192.0.2.0/23       *[BGP/170] 00:02:00, localpref 100
                      AS path: 1 192 I
                    > to 10.0.2.1 via em0.0
192.0.4.0/22       *[BGP/170] 00:02:00, localpref 100
                      AS path: 1 192 I
                    > to 10.0.2.1 via em0.0
192.0.8.0/21       *[BGP/170] 00:02:00, localpref 100
                      AS path: 1 192 I
                    > to 10.0.2.1 via em0.0
192.0.16.0/20      *[BGP/170] 00:02:00, localpref 100
                      AS path: 1 192 I
                    > to 10.0.2.1 via em0.0
192.0.32.0/19      *[BGP/170] 00:02:00, localpref 100
                      AS path: 1 192 I
                    > to 10.0.2.1 via em0.0
192.0.64.0/18      *[BGP/170] 00:02:00, localpref 100
                      AS path: 1 192 I
                    > to 10.0.2.1 via em0.0
192.0.128.0/17     *[BGP/170] 00:02:00, localpref 100
                      AS path: 1 192 I
                    > to 10.0.2.1 via em0.0
203.0.0.0/29       *[BGP/170] 00:02:00, localpref 100
                      AS path: 1 203 I
                    > to 10.0.2.1 via em0.0
203.0.0.8/29       *[BGP/170] 00:02:00, localpref 100
                      AS path: 1 203 I
                    > to 10.0.2.1 via em0.0
203.0.0.16/28      *[BGP/170] 00:02:00, localpref 100
                      AS path: 1 203 I
                    > to 10.0.2.1 via em0.0
203.0.0.32/27      *[BGP/170] 00:02:00, localpref 100
                      AS path: 1 203 I
                    > to 10.0.2.1 via em0.0
203.0.0.64/26      *[BGP/170] 00:02:00, localpref 100
                      AS path: 1 203 I
                    > to 10.0.2.1 via em0.0
203.0.0.128/25     *[BGP/170] 00:02:00, localpref 100
                      AS path: 1 203 I
                    > to 10.0.2.1 via em0.0
```

Policy on J6

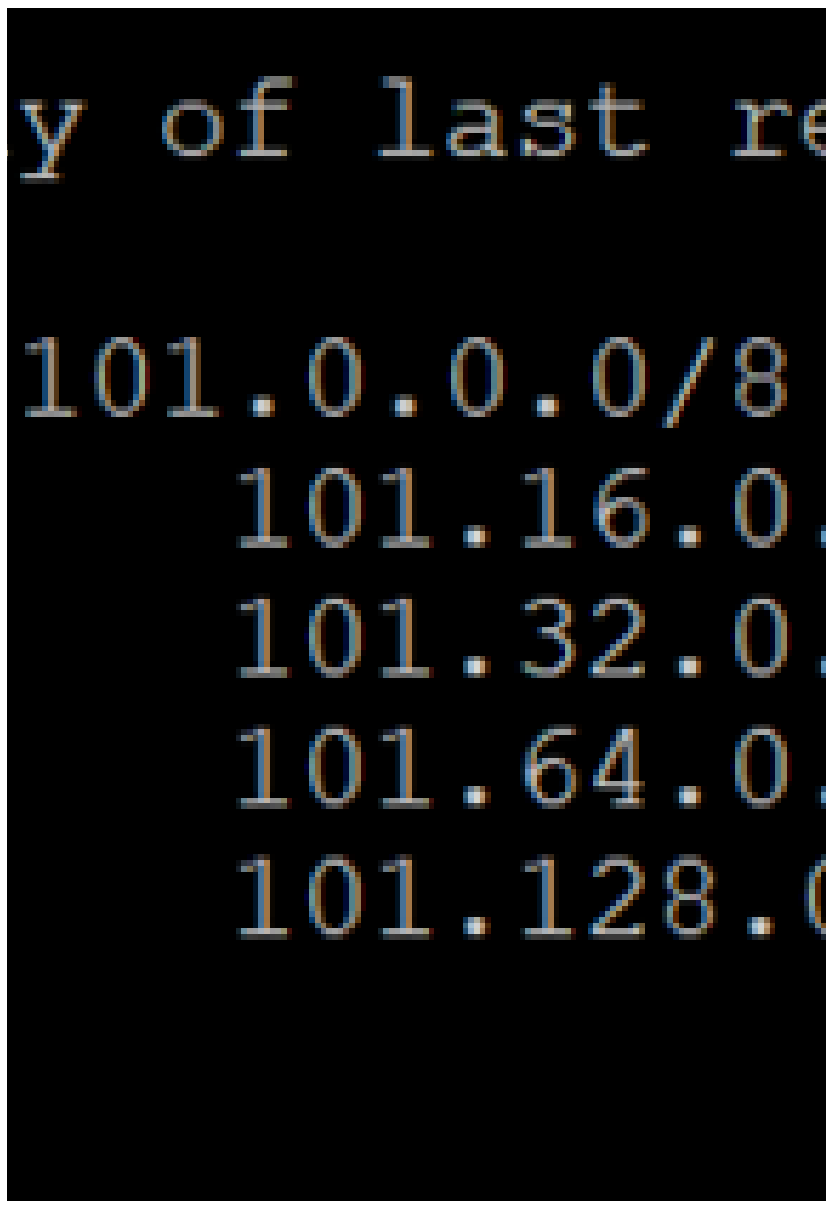
This Juniper command is configured to export **15 specific routes** within the **192.0.0.0 to 223.255.255.255 range**, including any more specific ones. It ensures these routes are **shared** with the other autonomous system AS 2.

set policy-options policy-statement EXPORT term 1 from route-filter 192.0.0.0/3 orlonger

Policy 8

Task: Allow only IPv4 prefixes that has a mask between /9 and /12 inclusive.

Routes on R6

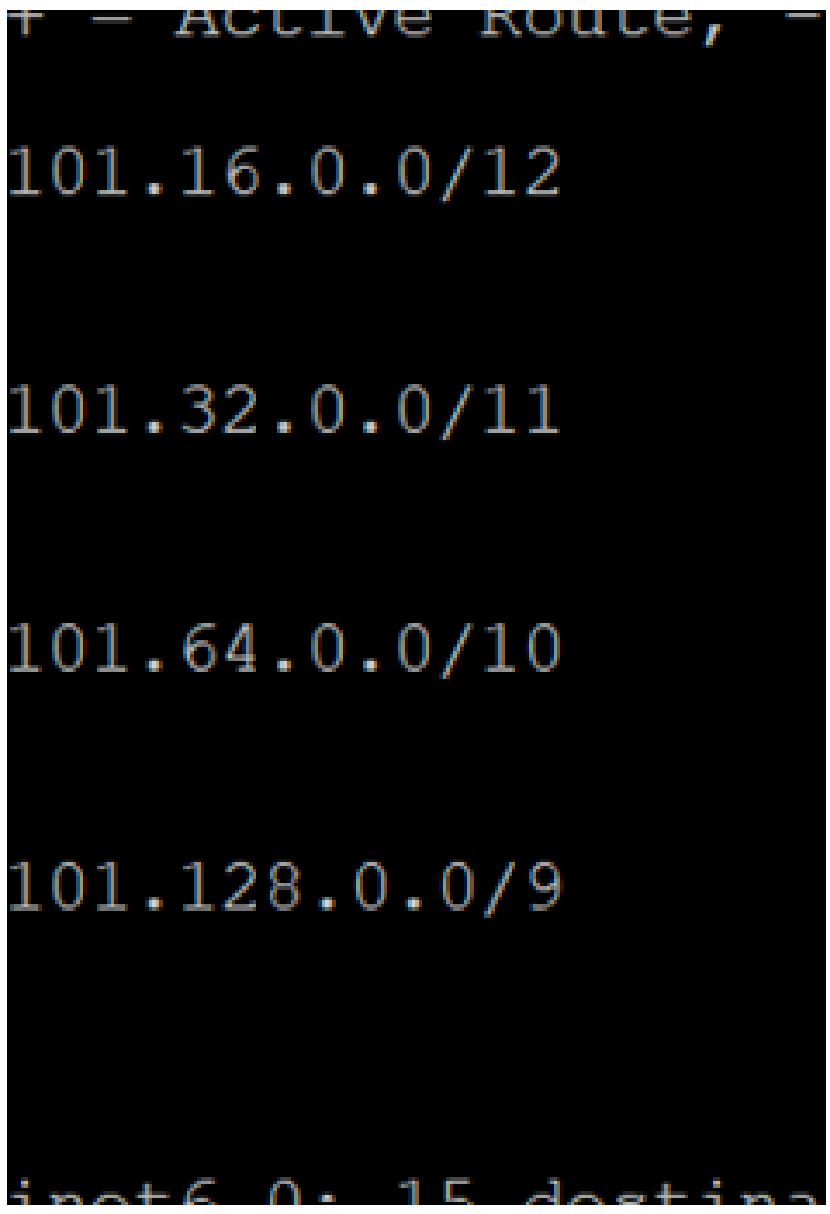


Policy on R5

This command creates a prefix list named P9 that permits IP addresses within the range of 0.0.0.0/0, specifically those with subnet masks greater than or equal to /9 and less than or equal to /12.

ip prefix-list P9 seq 5 permit 0.0.0.0/0 ge 9 le 12

Routes on J8



Policy on J6

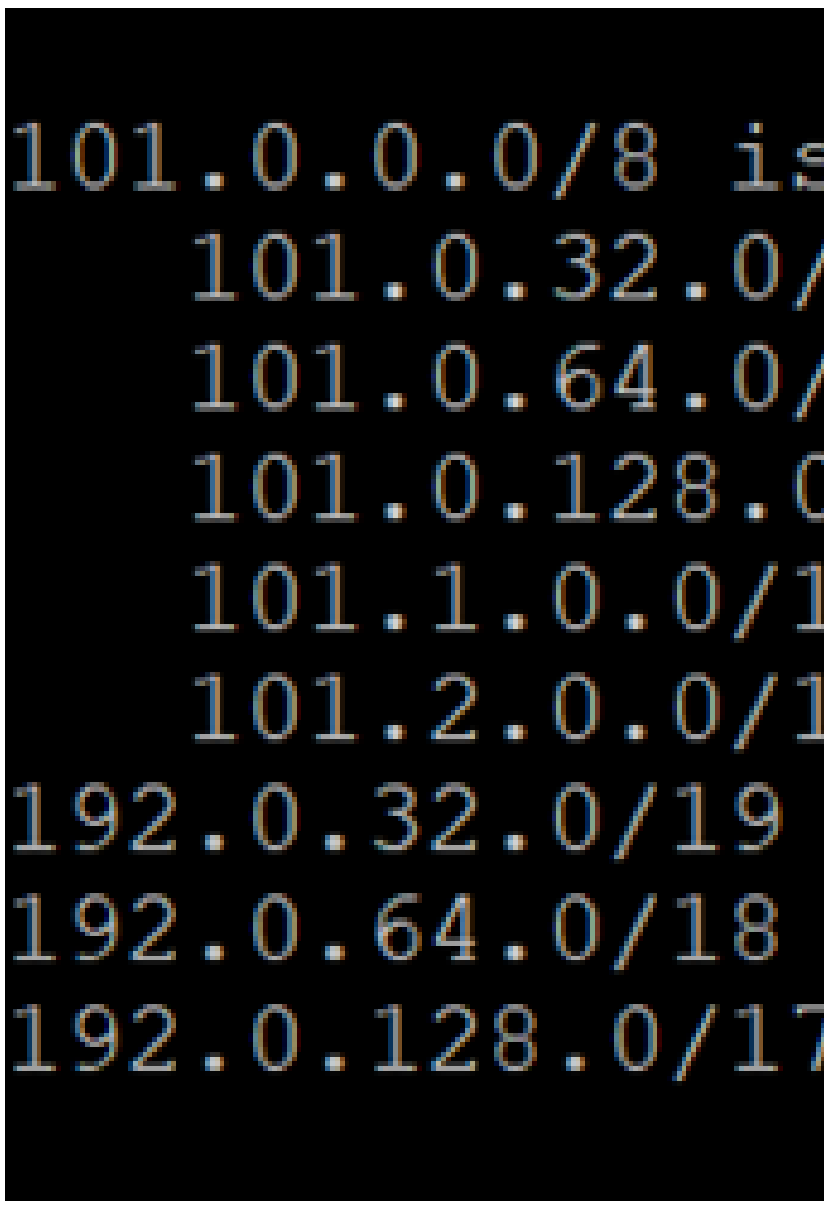
This Juniper command sets up a policy to export routes that match the 0.0.0.0/0 prefix and have a subnet mask length between /9 and /12. Essentially, it filters and permits the export of routes falling within this specific range of prefix lengths, ensuring they are shared.

set policy-options policy-statement EXPORT term 1 from route-filter 0.0.0.0/0 prefix-length-range /9-/12

Policy 9

Task: Allow only IPv4 prefixes that has a mask between /15 and /19 inclusive.

Routes on R6



Policy on R5

This prefix list named P9 permits IP addresses within the range 0.0.0.0/0, specifically those with subnet masks from /15 to /19.

ip prefix-list P9 seq 5 permit 0.0.0.0/0 ge 15 le 19

Routes on J8

Policy on J6

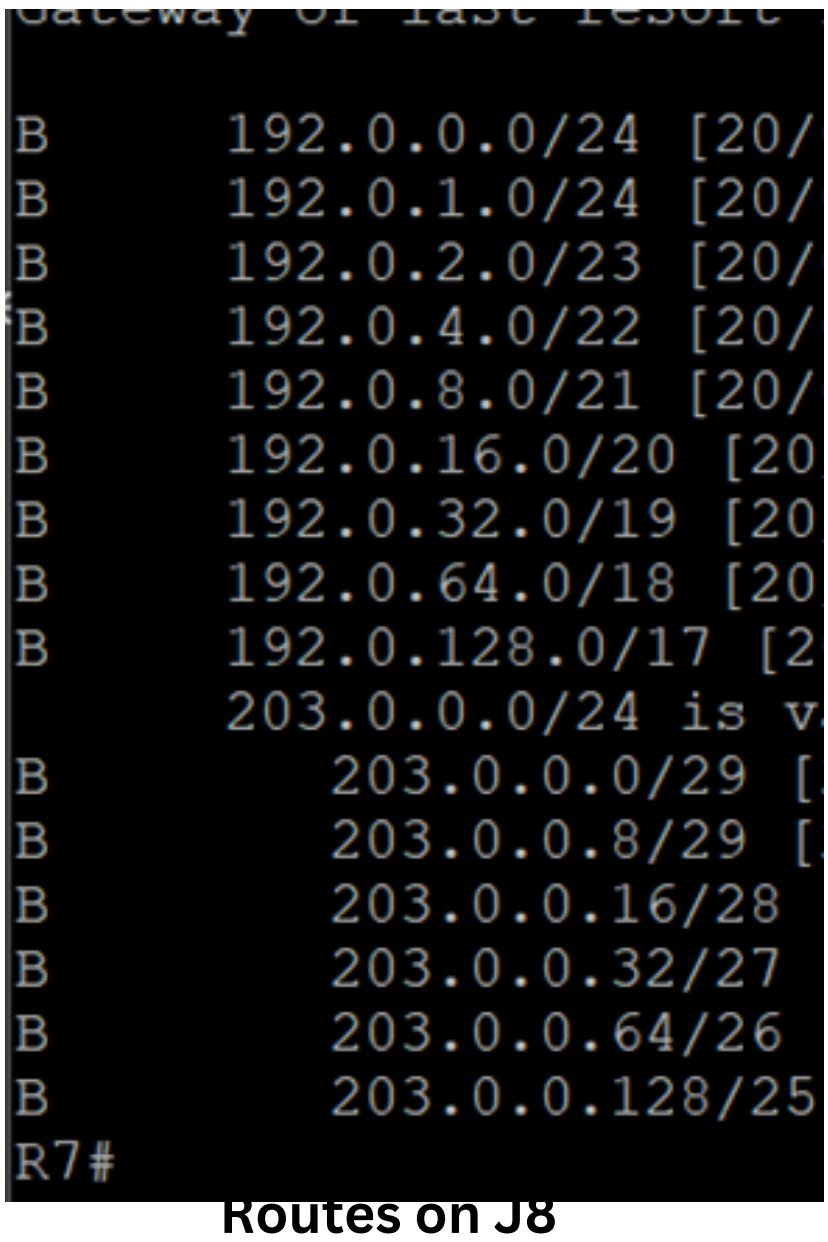
This Juniper command configures a policy to export routes with a prefix of **0.0.0.0/0 (aanywhere)** and subnet masks ranging from **/15 to /19**.

set policy-options policy-statement EXPORT term 1 from route-filter 0.0.0.0/0 prefix-length-range /15-/19

Policy 10

Task: Allow only IPv4 prefixes that has a binary 1 in its most significant bit.

Routes on R6

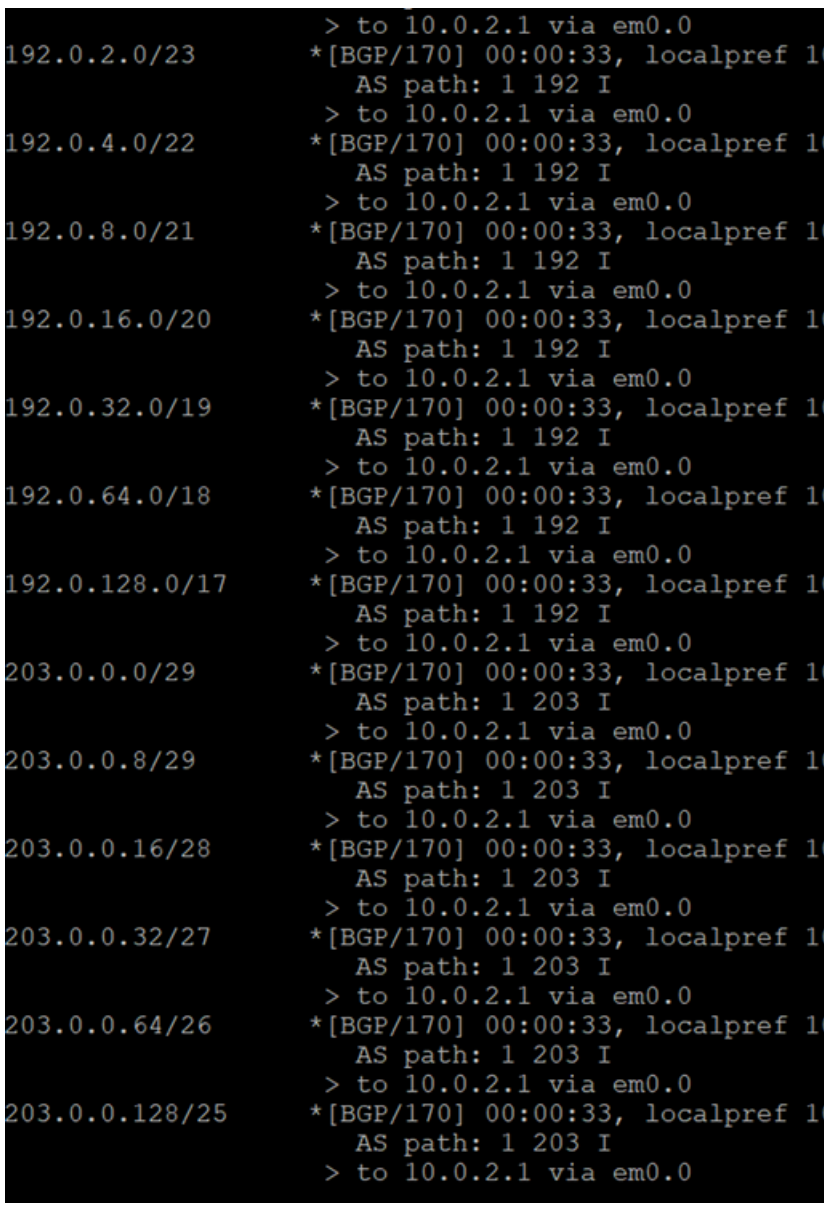


Policy on R5

This access list permits traffic from IP addresses starting at 128.0.0.0 and above, up to 255.255.255.255. Notably, addresses in this range have their most significant bit (MSB) always set to 1, signifying they fall within the higher half of the IP address space.

access-list 10 permit 128.0.0.0 127.255.255.255

Routes on J8



Policy on J6

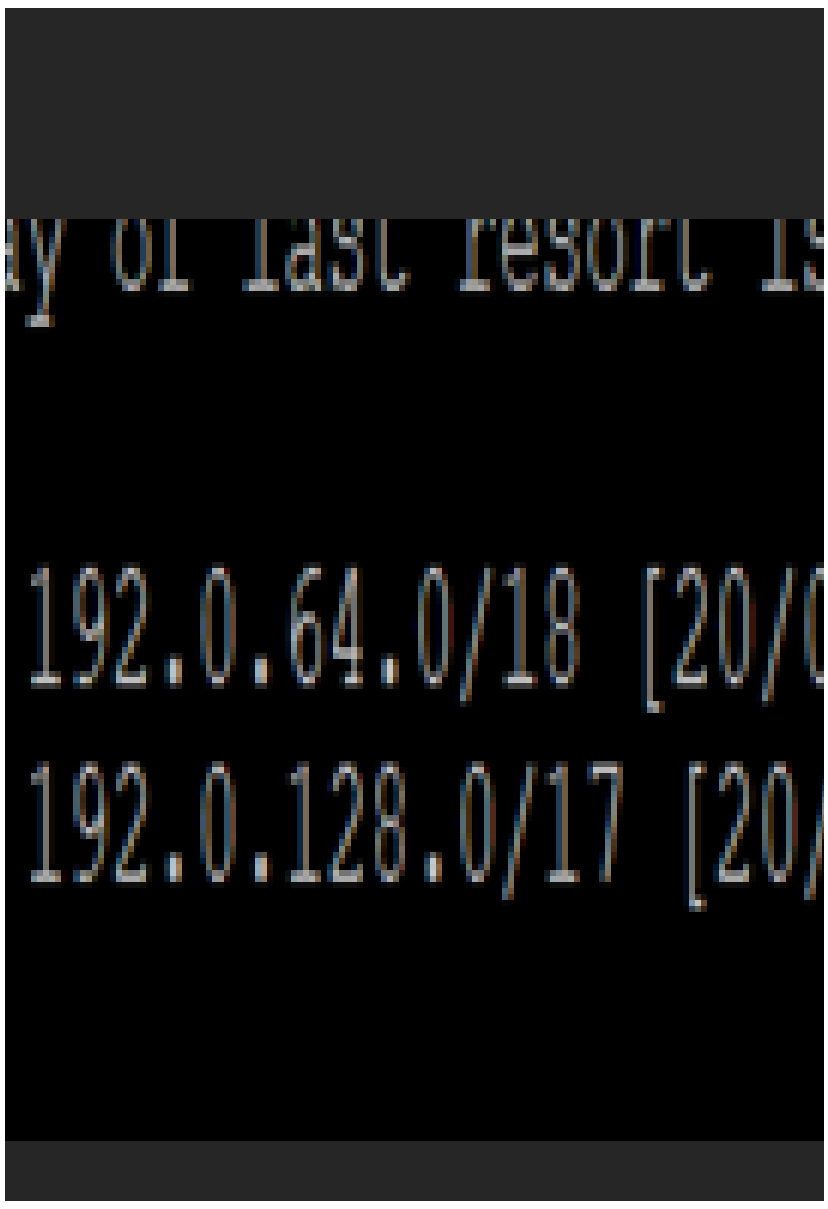
This Juniper policy sets a policy to export routes with a prefix starting at 128.0.0.0 and larger, up to any prefix length. This also means it includes all IP addresses whose most significant bit (MSB) is 1.

set policy-options policy-statement EXPORT term 1 from route-filter 128.0.0.0/1 orlonger

Policy 11

Task: Allow only IPv4 prefixes that begin with a binary 1 in its most significant bit but with masks between /16 and /18.

Routes on R6

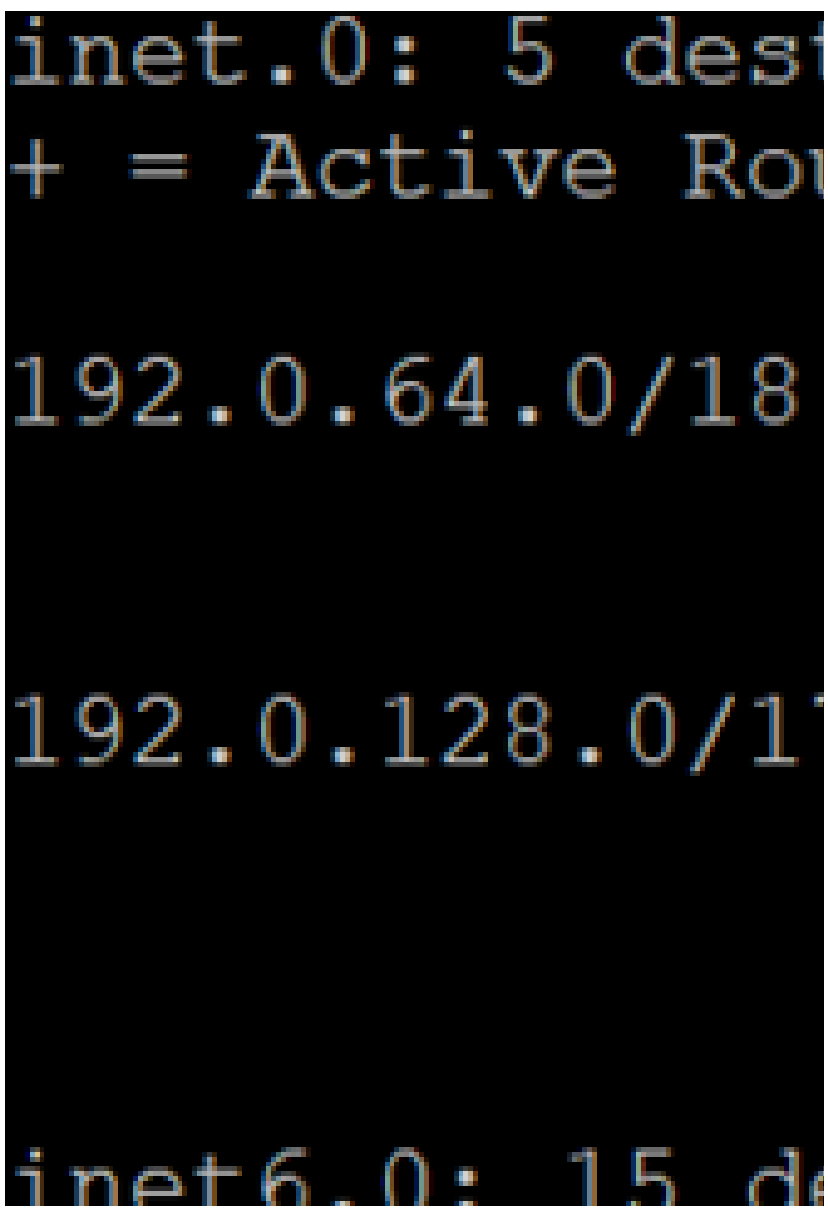


Policy on R5

This prefix list named P9 is to permit IP addresses that start with 128.0.0.0/1 and have subnet masks between /16 and /18.

ip prefix-list P9 seq 5 permit 128.0.0.0/1 ge 16 le 18

Routes on J8



Policy on J6

This Juniper policy exports routes that match the 128.0.0.0/1 prefix and have subnet masks between /16 and /18.

set policy-options policy-statement EXPORT term 1 from route-filter 128.0.0.0/1 prefix-length-range /16-/18

Policy 12

Task: Allow only any IPv4 prefixes that are originated in AS101 with masks between /9 and /16 inclusive.

Routes on R6

```
l.0.0.0/8 is va
101.1.0.0/16
101.2.0.0/15
101.4.0.0/14
101.8.0.0/13
101.16.0.0/12
101.32.0.0/11
101.64.0.0/10
101.128.0.0/9
```

Routes on J8

```
inet.0: 11 destinations, 11 routes
+ = Active Route, - = Last Active,

101.1.0.0/16       *[BGP/170] 00:00
                      AS path: 1 10
                    > to 10.0.2.1 v
101.2.0.0/15       *[BGP/170] 00:00
                      AS path: 1 10
                    > to 10.0.2.1 v
101.4.0.0/14       *[BGP/170] 00:00
                      AS path: 1 10
                    > to 10.0.2.1 v
101.8.0.0/13       *[BGP/170] 00:00
                      AS path: 1 10
                    > to 10.0.2.1 v
101.16.0.0/12      *[BGP/170] 00:00
                      AS path: 1 10
                    > to 10.0.2.1 v
101.32.0.0/11      *[BGP/170] 00:00
                      AS path: 1 10
                    > to 10.0.2.1 v
101.64.0.0/10      *[BGP/170] 00:00
                      AS path: 1 10
                    > to 10.0.2.1 v
101.128.0.0/9      *[BGP/170] 00:00
                      AS path: 1 10
                    > to 10.0.2.1 v
```

Policy on R5

The prefix list creates an entry named P9 that permits IP addresses within the range 0.0.0.0/0, specifically those with subnet masks from /9 to /16. The AS-path access list permits routes originating from an autonomous system with the number 101.

ip prefix-list P9 seq 5 permit 0.0.0.0/0 ge 9 le 16
ip as-path access-list 10 permit ^101$

Policy on J6

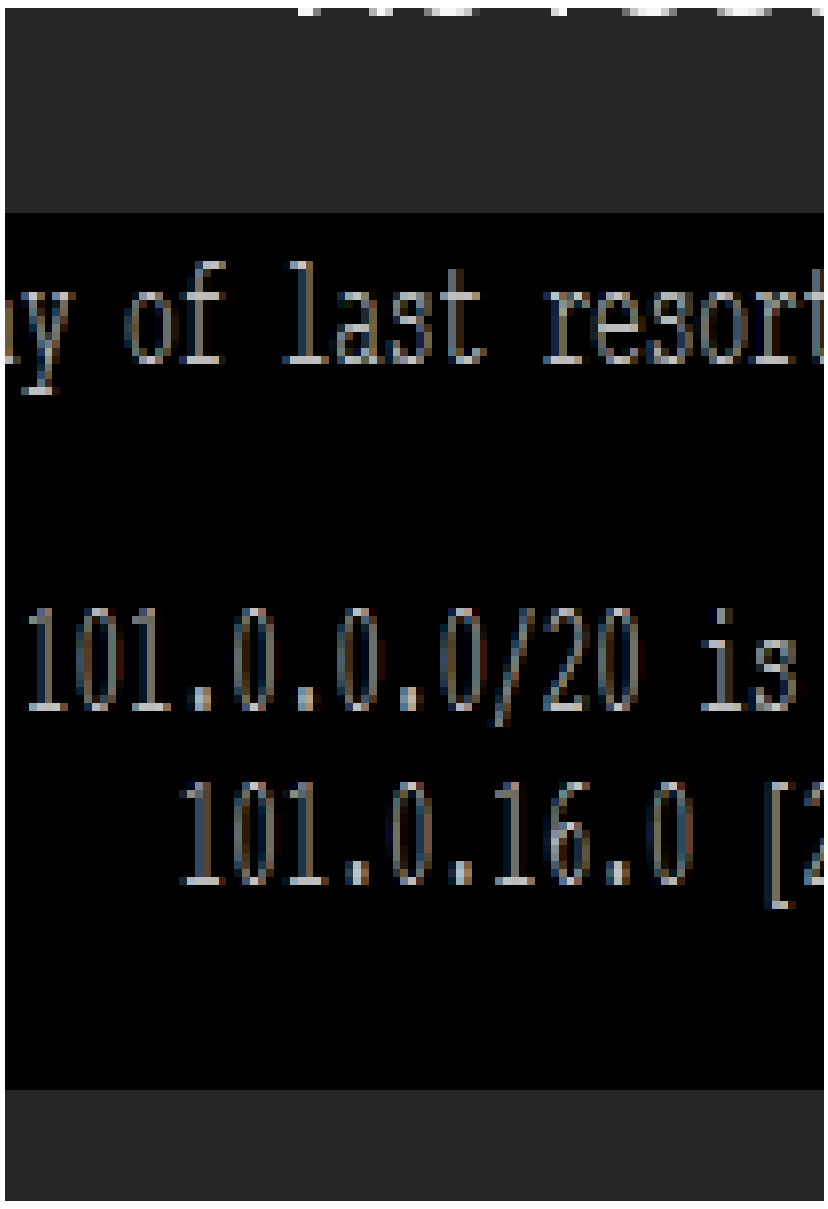
The first policy creates an AS-path list named AS101 to match routes originating from AS 101. The next two policies set a statement to export routes within the 0.0.0.0/0 prefix with subnet masks ranging from /9 to /16, and to export routes that match the AS-path AS101.

set policy-options as-path AS101 "^101$"
set policy-options policy-statement EXPORT term 1 from route-filter 0.0.0.0/0 prefix-length-range /9-/16
set policy-options policy-statement EXPORT term 1 from as-path AS101

Policy 13

Task: Allow only any IPv4 prefixes that are originated in AS101 with masks exactly /20.

Routes on R6



Policy on R5

The prefix list named P9 permits IP addresses within the 0.0.0.0/0 range that have a subnet mask of exactly /20. The AS-path access list permits routes originating specifically from the autonomous system numbered 101.

ip prefix-list P9 seq 5 permit 0.0.0.0/0 ge 20 le 20
ip as-path access-list 10 permit ^101$

Routes on J8

Policy on J6

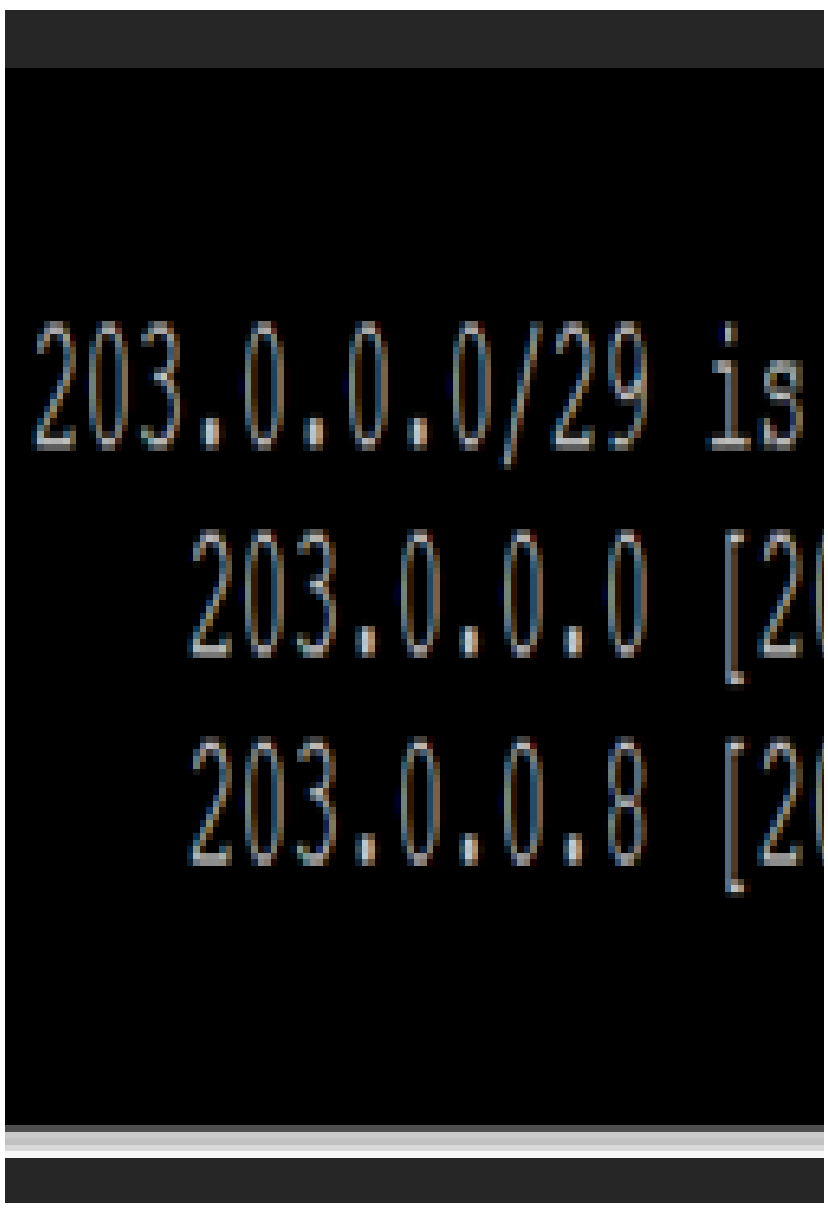
The first policy creates an AS-path list named AS101 to match routes originating from AS 101. The next two policies set a statement to export routes within the 0.0.0.0/0 prefix with an exact subnet mask of /20, and to export routes that match the AS-path AS101.

set policy-options as-path AS101 "^101$"
set policy-options policy-statement EXPORT term 1 from route-filter 0.0.0.0/0 prefix-length-range /20-/20
set policy-options policy-statement EXPORT term 1 from as-path AS101

Policy 14

Task: Allow only any IPv4 prefixes originated in AS203 that contain 8 addresses.

Routes on R6



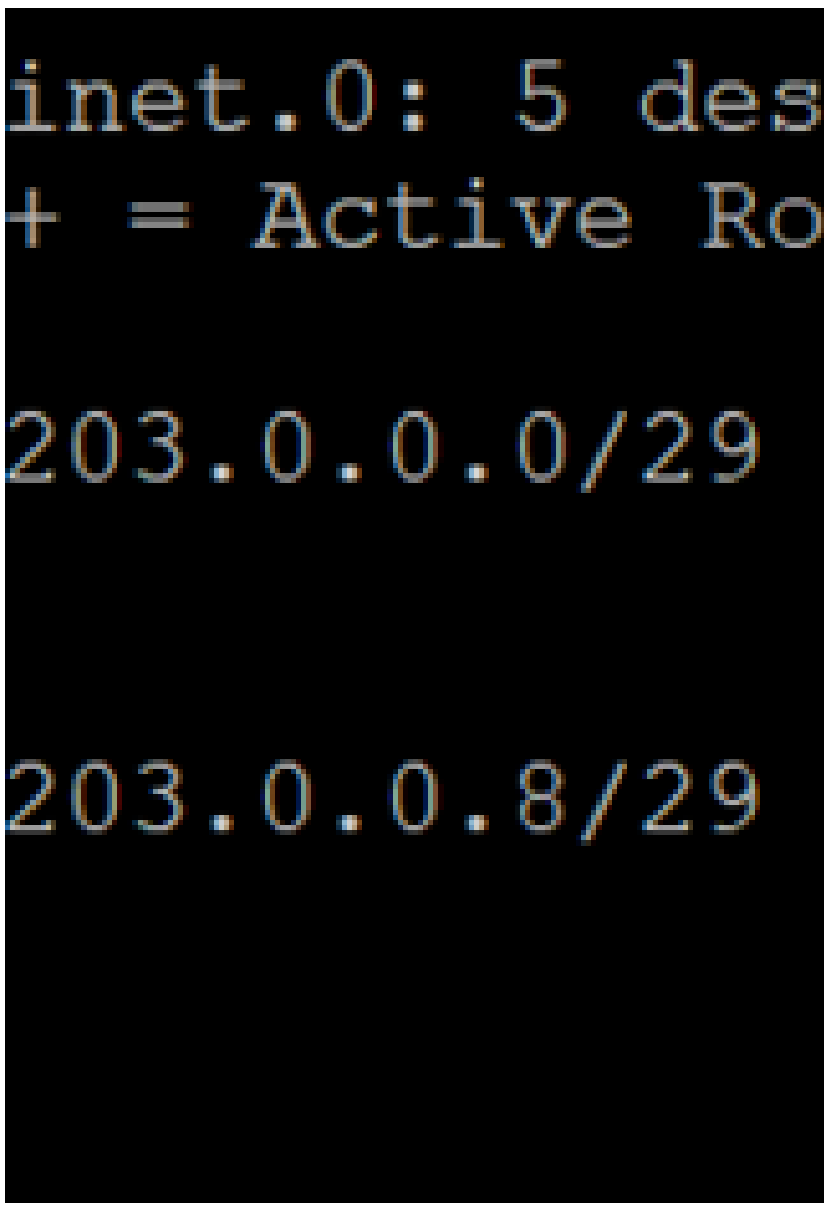
Policy on R5

The prefix list P9 permits IP addresses in the 0.0.0.0/0 range with an exact subnet mask of /29. The AS-path access list permits routes originating specifically from the autonomous system numbered 203.

ip prefix-list P9 seq 5 permit 0.0.0.0/0 ge 29 le 29

ip as-path access-list 10 permit ^203$

Routes on J8



Policy on J6

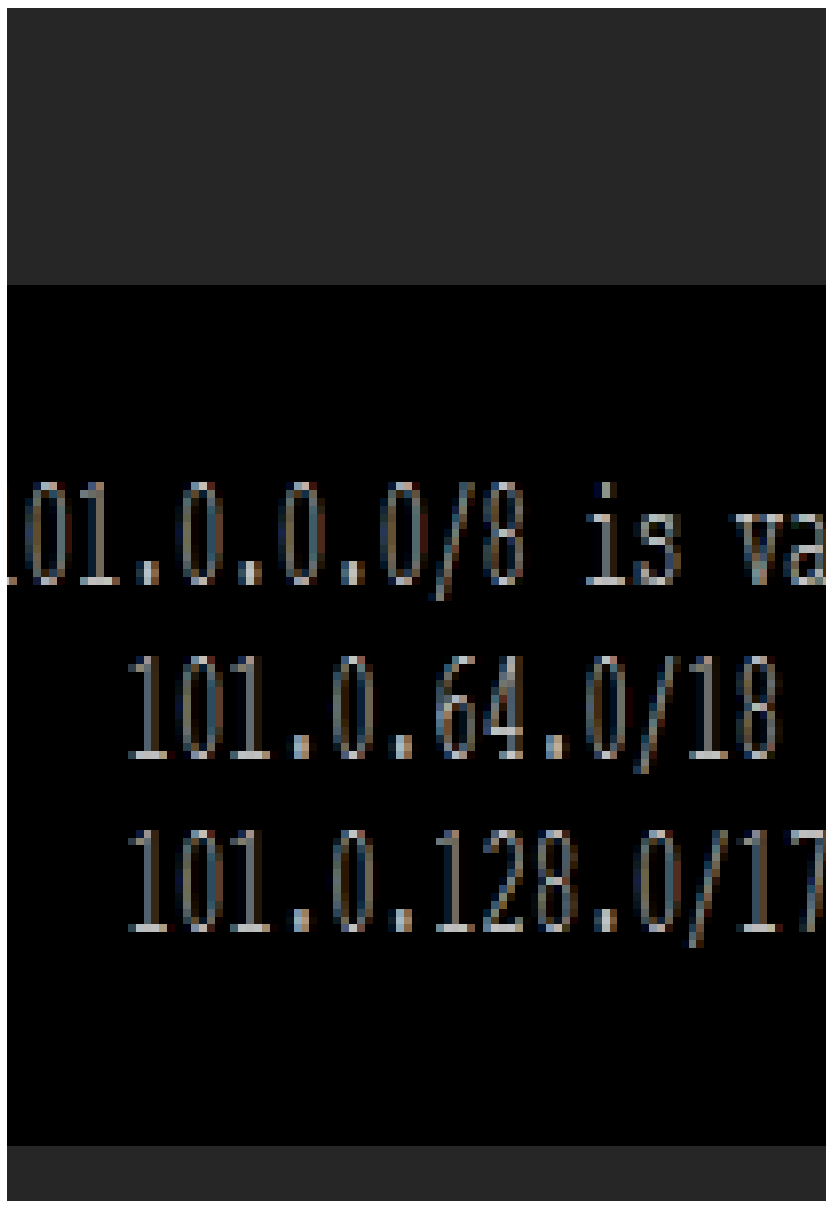
The first policy creates an AS-path list named AS203 to match routes originating from AS 203. The next two policies set a statement to export routes within the 0.0.0.0/0 prefix with an exact subnet mask of /29, and to export routes that match the AS-path AS203.

set policy-options as-path AS203 "^203$"
set policy-options policy-statement EXPORT term 1 from route-filter 0.0.0.0/0 prefix-length-range /29-/29
set policy-options policy-statement EXPORT term 1 from as-path AS203

Policy 15

Task: Allow only any IPv4 prefixes originated in AS101 with masks from /17 through /18.

Routes on R6



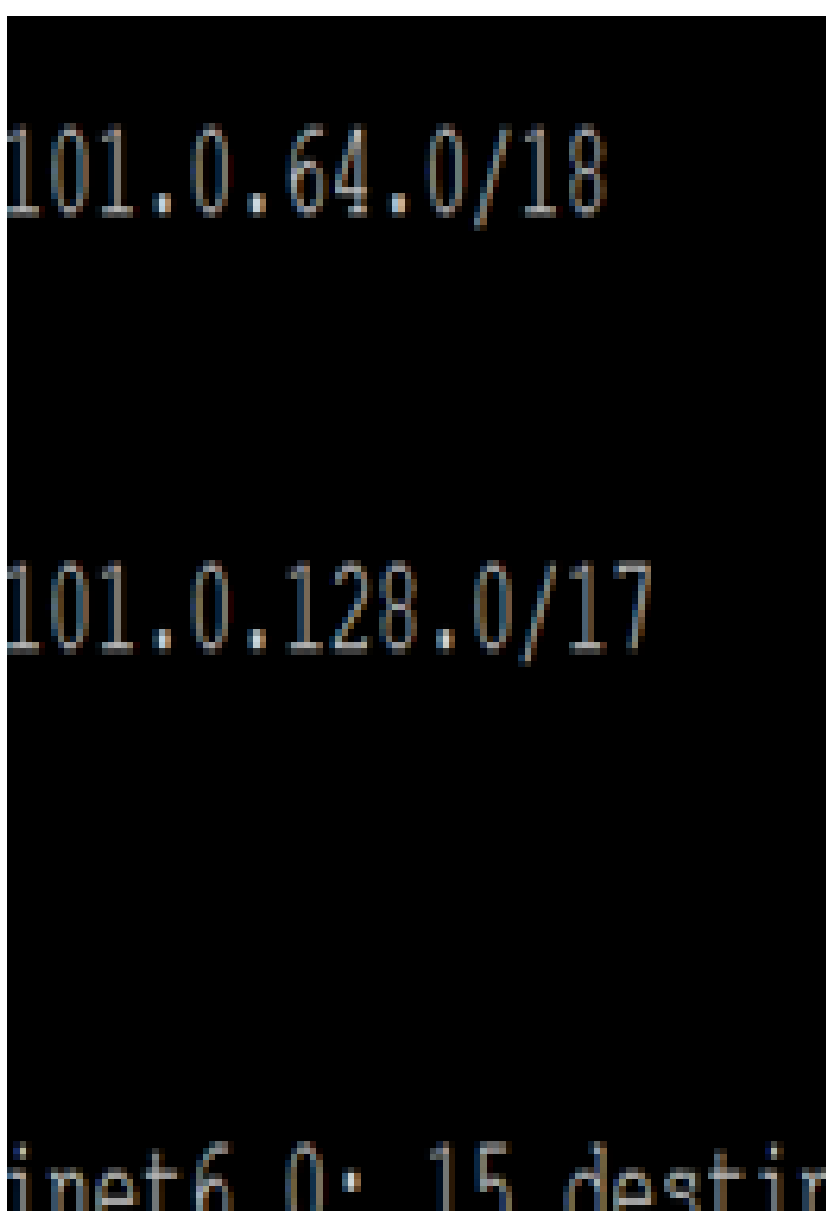
Policy on R5

The prefix list P9 permits IP addresses within the 0.0.0.0/0 range that have subnet masks between /17 and /18. The AS-path access list allows routes originating specifically from the autonomous system numbered 101.

ip prefix-list P9 seq 5 permit 0.0.0.0/0 ge 17 le 18

ip as-path access-list 10 permit ^101$

Routes on J8



Policy on J6

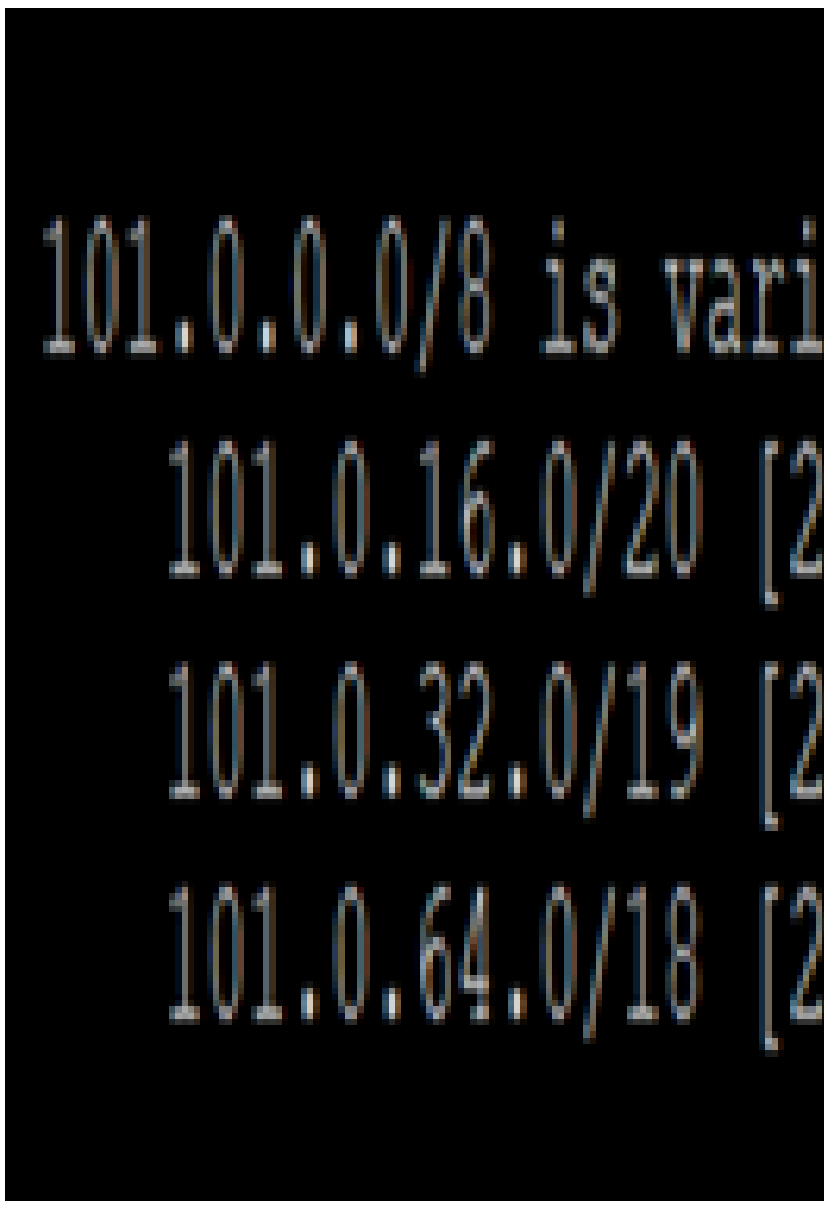
The first policy creates an AS-path list named AS101 to match routes originating from AS 101. The next two policies set a statement to export routes within the 0.0.0.0/0 prefix with subnet masks ranging from /17 to /18, and to export routes that match the AS-path AS101.

set policy-options as-path AS101 "^101$"
set policy-options policy-statement EXPORT term 1 from route-filter 0.0.0.0/0 prefix-length-range /17-/18
set policy-options policy-statement EXPORT term 1 from as-path AS101

Policy 16

Task: Allow only any IPv4 prefixes originated in either AS101 or AS203 with masks from /18 to /20 inclusive.

Routes on R6

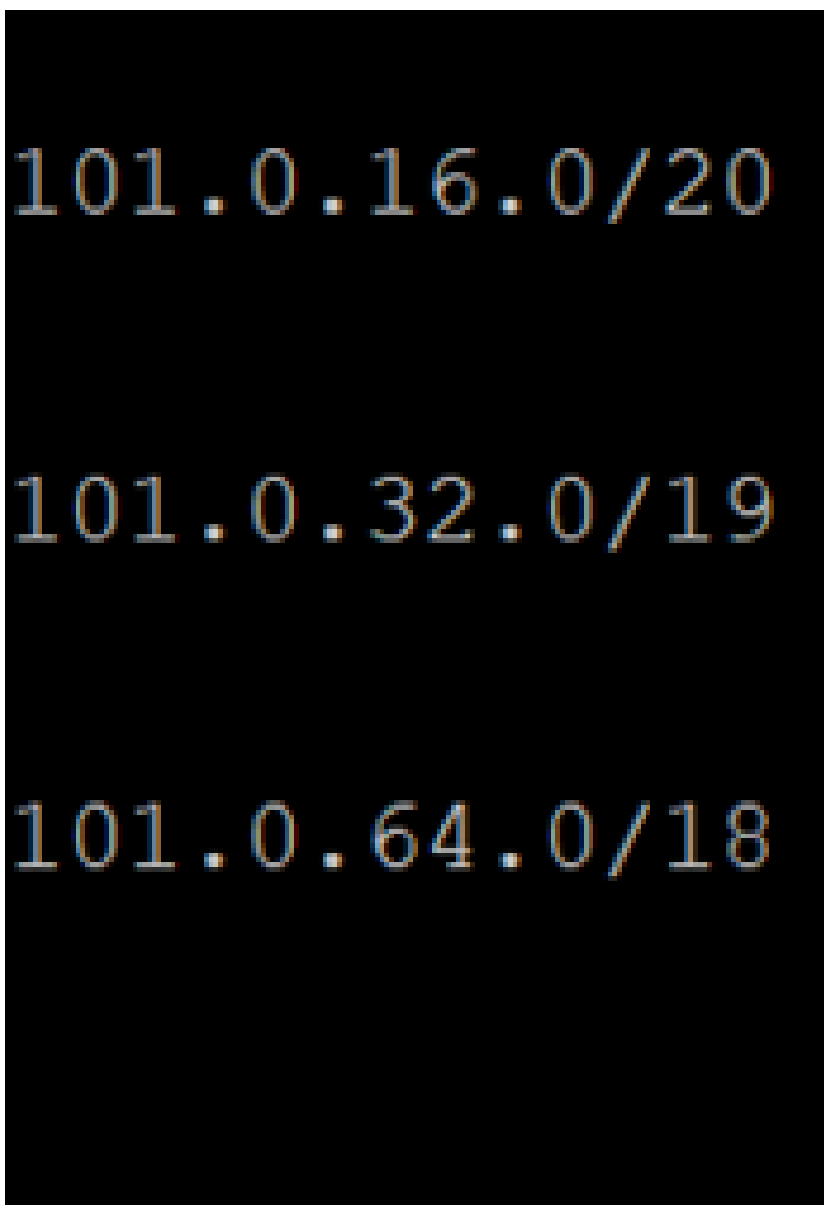


Policy on R5

The prefix list P9 permits IP addresses within the 0.0.0.0/0 range that have subnet masks between /18 and /20. The AS-path access list allows routes originating from autonomous systems 101 or 203.

ip prefix-list P9 seq 5 permit 0.0.0.0/0 ge 18 le 20
ip as-path access-list 10 permit ^(101|203)$

Routes on J8



Policy on J6

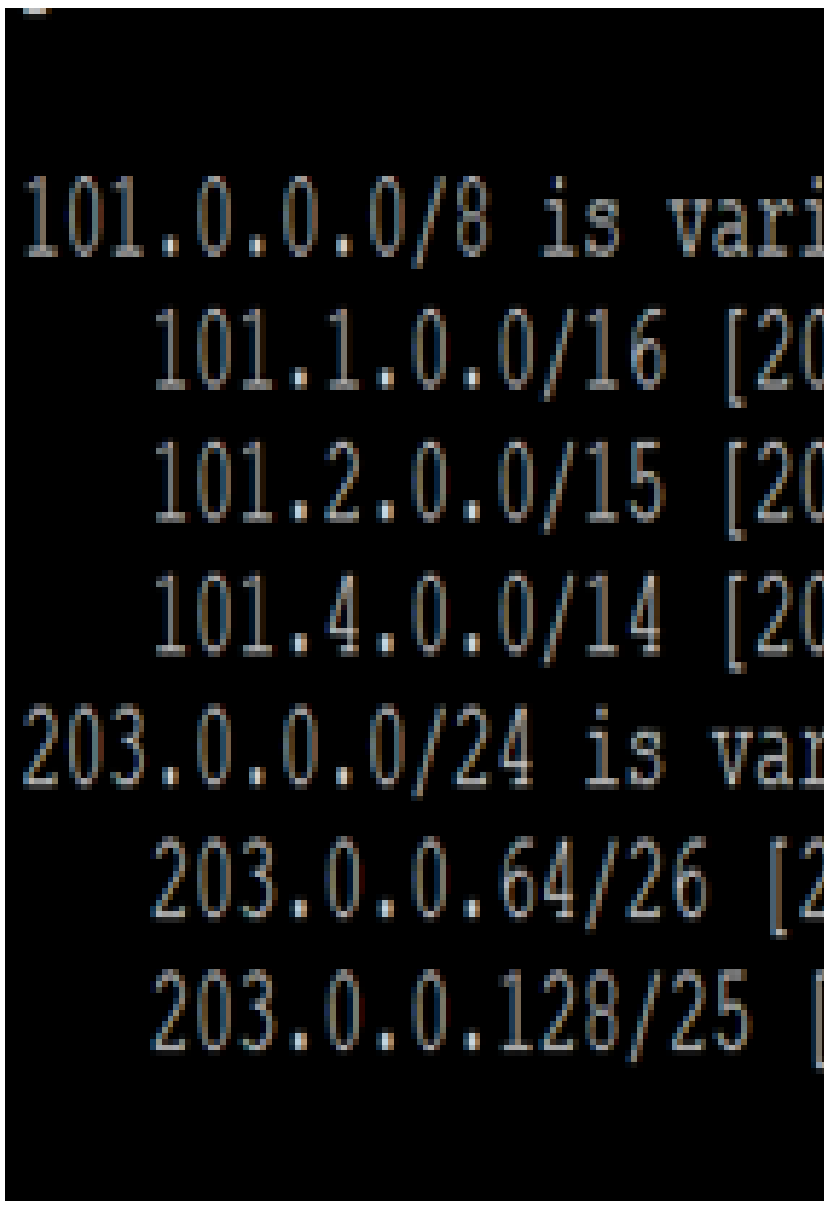
This policy exports routes within the 0.0.0.0/0 prefix with subnet masks ranging from /18 to /20 and routes originating from either AS 101 or AS 203.

set policy-options as-path AS101_203 "^(101|203)$"
set policy-options policy-statement EXPORT term 1 from route-filter 0.0.0.0/0 prefix-length-range /18-/20
set policy-options policy-statement EXPORT term 1 from as-path AS101_203

Policy 17

Task: Allow only any IPv4 prefixes originated from AS101 with masks from /14 to /16 inclusive, originated from AS203 with masks from /19 to /21 inclusive and from AS203 with mask from /25 to /26 inclusive.

Routes on R6



Policy on R5

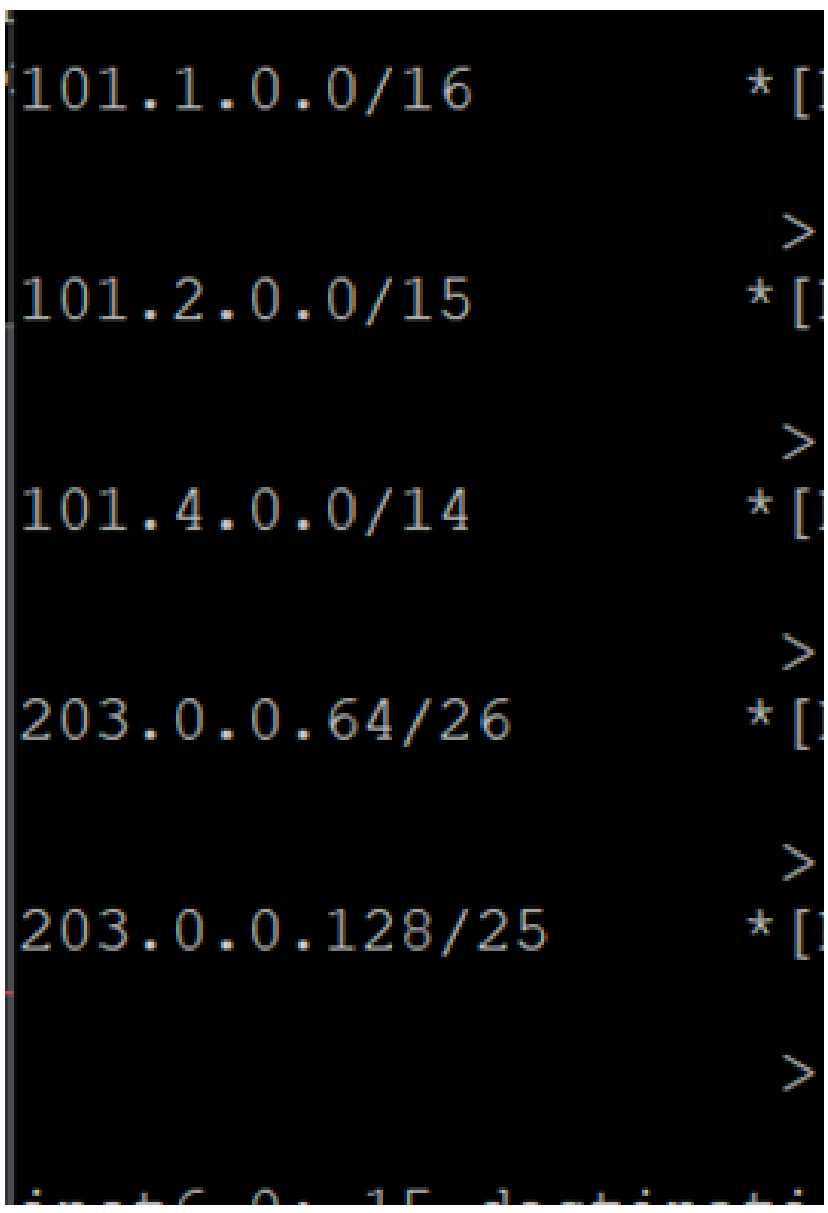
ip prefix-list P101 seq 5 permit 0.0.0.0/0 ge 14 le 16

ip prefix-list P203_1 seq 5 permit 0.0.0.0/0 ge 19 le 21

ip prefix-list P203_2 seq 10 permit 0.0.0.0/0 ge 25 le 26

ip as-path access-list 101 permit ^101$
ip as-path access-list 203 permit ^203$
route-map EXPORT permit 10
match as-path 101
match ip address prefix-list P101
route-map EXPORT permit 20
match as-path 203
match ip address prefix-list P203_1 P203_2

Routes on J8



Policy on J6

set policy-options as-path AS101 "^101$"
set policy-options as-path AS203 "^203$"
set policy-options policy-statement EXPORT term 1 from route-filter 0.0.0.0/0 prefix-length-range /14-/16
set policy-options policy-statement EXPORT term 1 from as-path AS101
set policy-options policy-statement EXPORT term 2 from route-filter 0.0.0.0/0 prefix-length-range /19-/21
set policy-options policy-statement EXPORT term 2 from as-path AS203
set policy-options policy-statement EXPORT term 3 from route-filter 0.0.0.0/0 prefix-length-range /25-/26
set policy-options policy-statement EXPORT term 3 from as-path AS203

Policy 18

Task: Allow only IPv6 prefixes sourced by AS2001 with masks in the range /34 to /36 inclusive.

Routes on R6

```
B   2001:4443:2000::/35 [20/0]
     via FE80::C805:A4FF:FECF:1C
B   2001:4443:8000::/34 [20/0]
     via FE80::C805:A4FF:FECF:1C
B   2001:4443:C000::/34 [20/0]
     via FE80::C805:A4FF:FECF:1C
B   2001:4444:2000::/36 [20/0]
     via FE80::C805:A4FF:FECF:1C
B   2001:4444:3000::/36 [20/0]
     via FE80::C805:A4FF:FECF:1C
B   2001:4444:4000::/34 [20/0]
     via FE80::C805:A4FF:FECF:1C
B   2001:4444:8000::/35 [20/0]
     via FE80::C805:A4FF:FECF:1C
B   2001:4444:A000::/35 [20/0]
     via FE80::C805:A4FF:FECF:1C
B   2001:4444:C000::/34 [20/0]
     via FE80::C805:A4FF:FECF:1C
C   FC00:56::/120 [0/0]
     via GigabitEthernet0/0, dir
L   FC00:56::2/128 [0/0]
     via GigabitEthernet0/0, rec
L   FF00::/8 [0/0]
     via Null0, receive
R7#
```

Policy on R5

The prefix list P18 permits IPv6 addresses within the 2001::/16 range that have subnet masks between /34 and /36. The AS-path access list permits routes originating from AS 2001.

ipv6 prefix-list P18 seq 5 permit 2001::/16 ge 34 le 36
ip as-path access-list 10 permit ^2001$
route-map EXPORT permit 10
match as-path 10
match ipv6 address prefix-list P18

Routes on J8

```
2001:4443:2000::/35*[BGP/170] 02:27
                      AS path: 1 20
                    > to fc00:12::1
2001:4443:8000::/34*[BGP/170] 02:27
                      AS path: 1 20
                    > to fc00:12::1
2001:4443:c000::/34*[BGP/170] 02:27
                      AS path: 1 20
                    > to fc00:12::1
2001:4444:2000::/36*[BGP/170] 02:27
                      AS path: 1 20
                    > to fc00:12::1
2001:4444:3000::/36*[BGP/170] 02:27
                      AS path: 1 20
                    > to fc00:12::1
2001:4444:4000::/34*[BGP/170] 02:27
                      AS path: 1 20
                    > to fc00:12::1
2001:4444:8000::/35*[BGP/170] 02:27
                      AS path: 1 20
                    > to fc00:12::1
2001:4444:a000::/35*[BGP/170] 02:27
                      AS path: 1 20
                    > to fc00:12::1
2001:4444:c000::/34*[BGP/170] 02:27
                      AS path: 1 20
                    > to fc00:12::1
```

Policy on J6

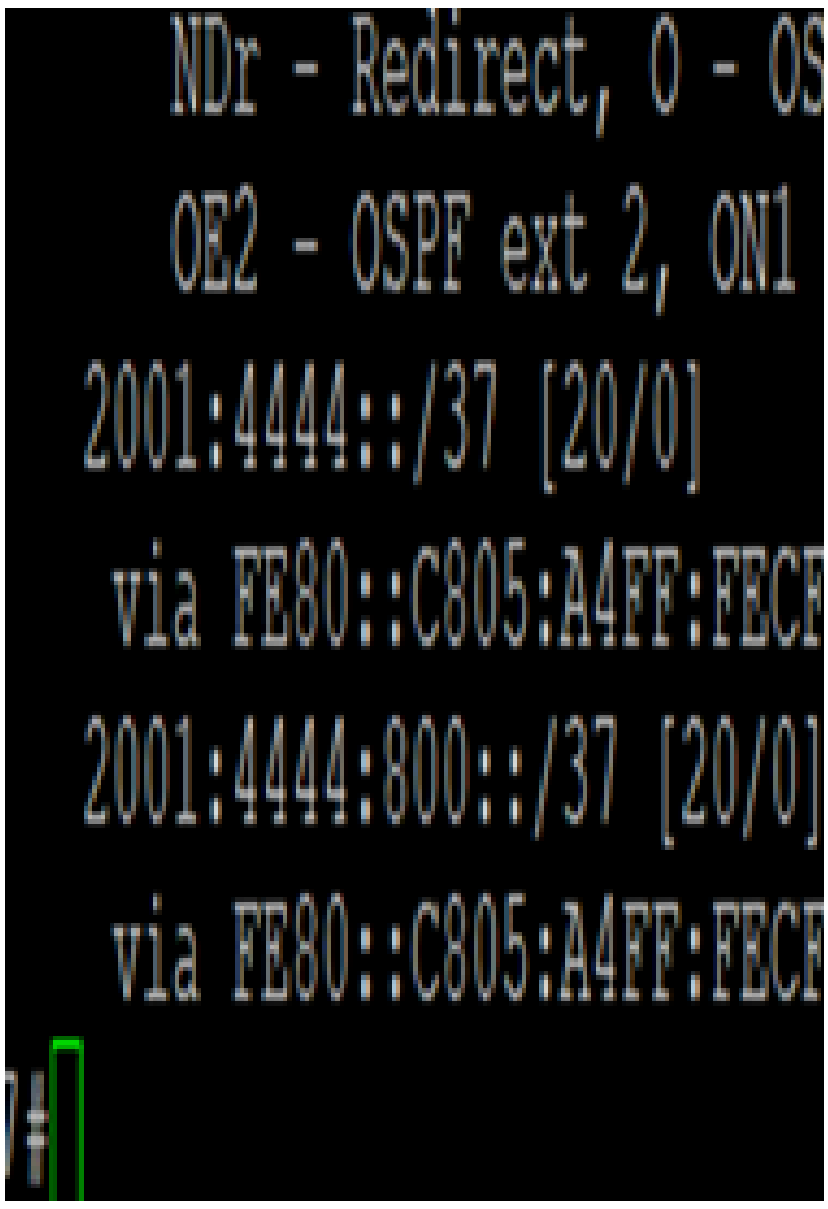
This policy exports routes within the ::/0 prefix with subnet masks ranging from /34 to /36 and routes originating from AS 2001.

set policy-options as-path AS2001 "^2001$"
set policy-options policy-statement EXPORT term 1 from route-filter ::/0 prefix-length-range /34-/36
set policy-options policy-statement EXPORT term 1 from as-path AS2001

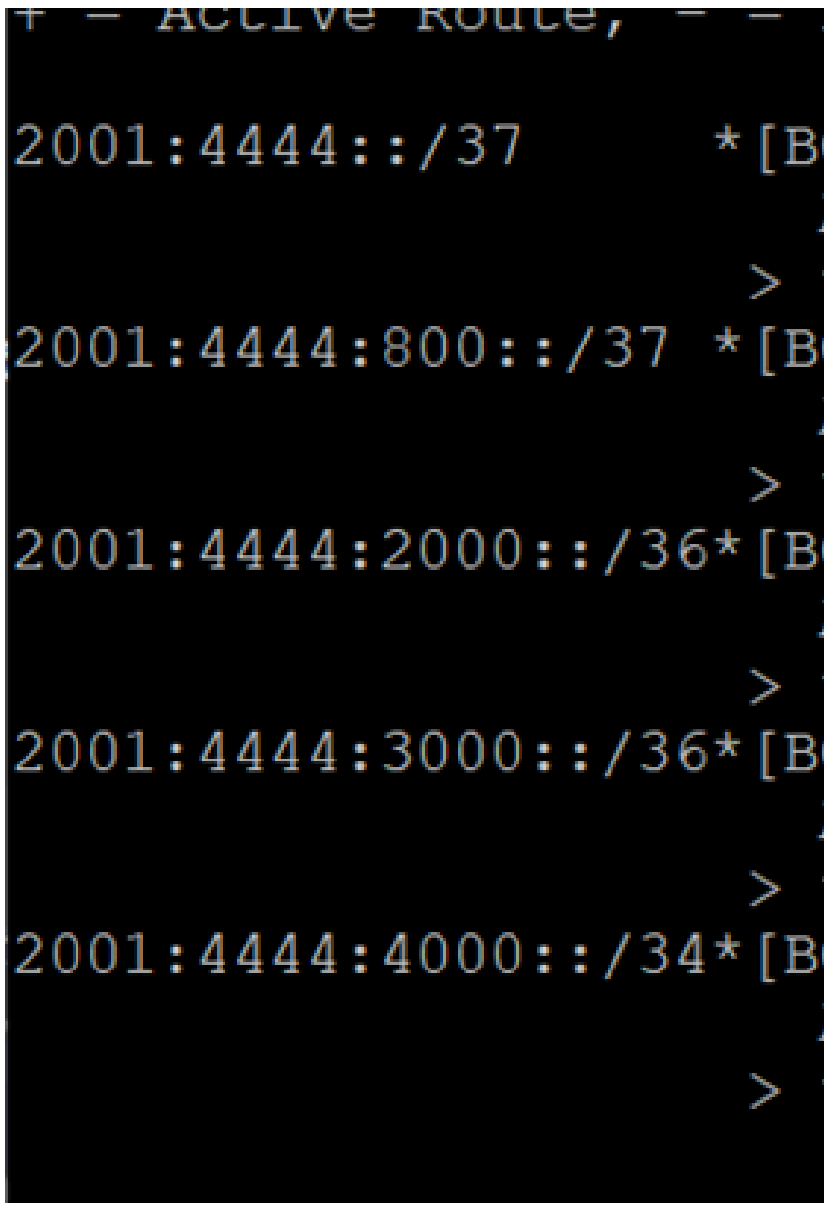
Policy 19

Task: Allow only any IPv6 prefixes sourced by AS2001 with the pattern 2001:4444:0xxx000::/any mask. The symbols xxx means three bit positions with any binary value.

Routes on R6



Routes on J8



Policy on R5

The first two entries in the IPv6 prefix list P19 permit addresses within the 2001:4444:0000::/36 and 2001:4444:7000::/36 ranges, extending to any subnet mask length up to /128. The AS-path access list allows routes that originate from 2001.

ipv6 prefix-list P19 seq 5 permit 2001:4444:0000::/36 le 128
ipv6 prefix-list P19 seq 10 permit 2001:4444:7000::/36 le 128
ip as-path access-list 10 permit ^2001$

Policy on J6

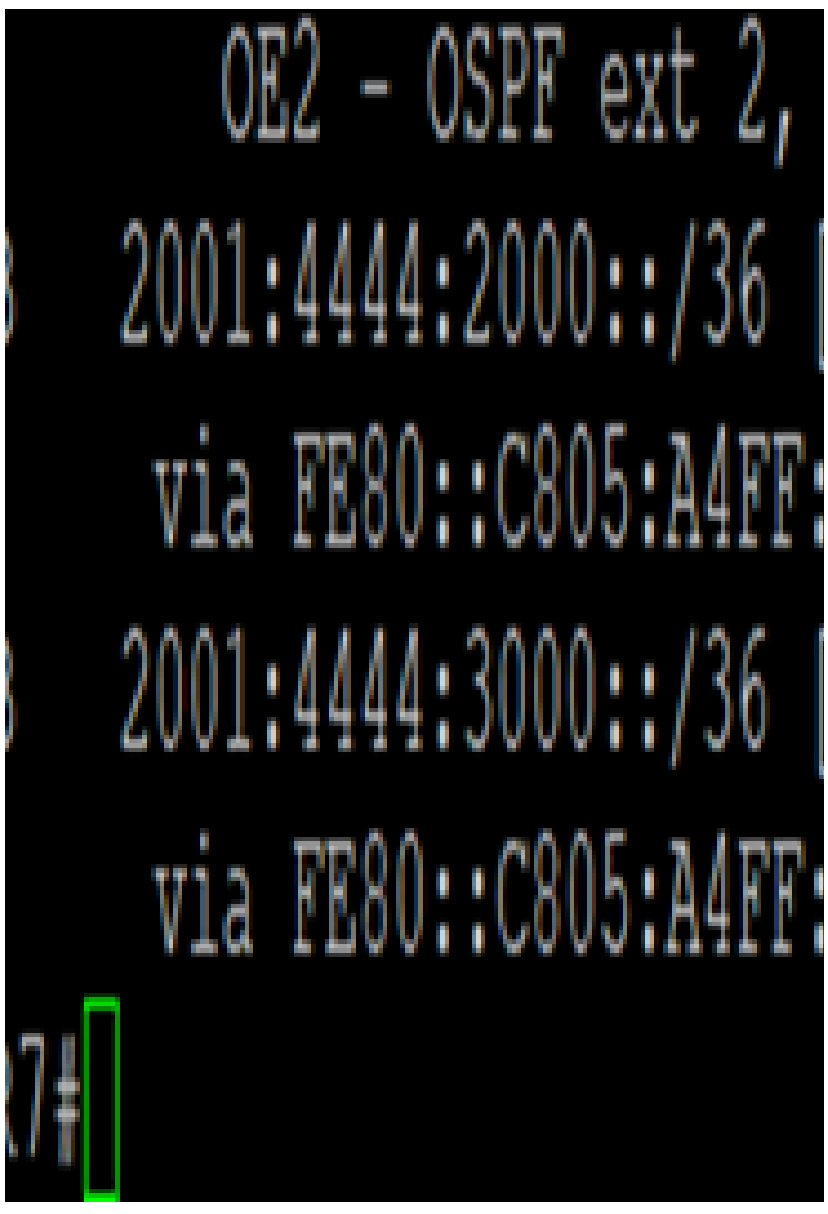
This policy exports routes that match the 2001:4444::/33 prefix and longer subnet masks. It also exports routes originating from AS 2001.

set policy-options as-path AS2001 "^2001$"
set policy-options policy-statement EXPORT term 1 from route-filter 2001:4444::/33 orlonger
set policy-options policy-statement EXPORT term 1 from as-path AS2001

Policy 20

Task: Allow only IPv6 prefixes sourced by AS2001 that catches 2001:4444:2000::/36 and 2001:4444:3000::/36.

Routes on R6

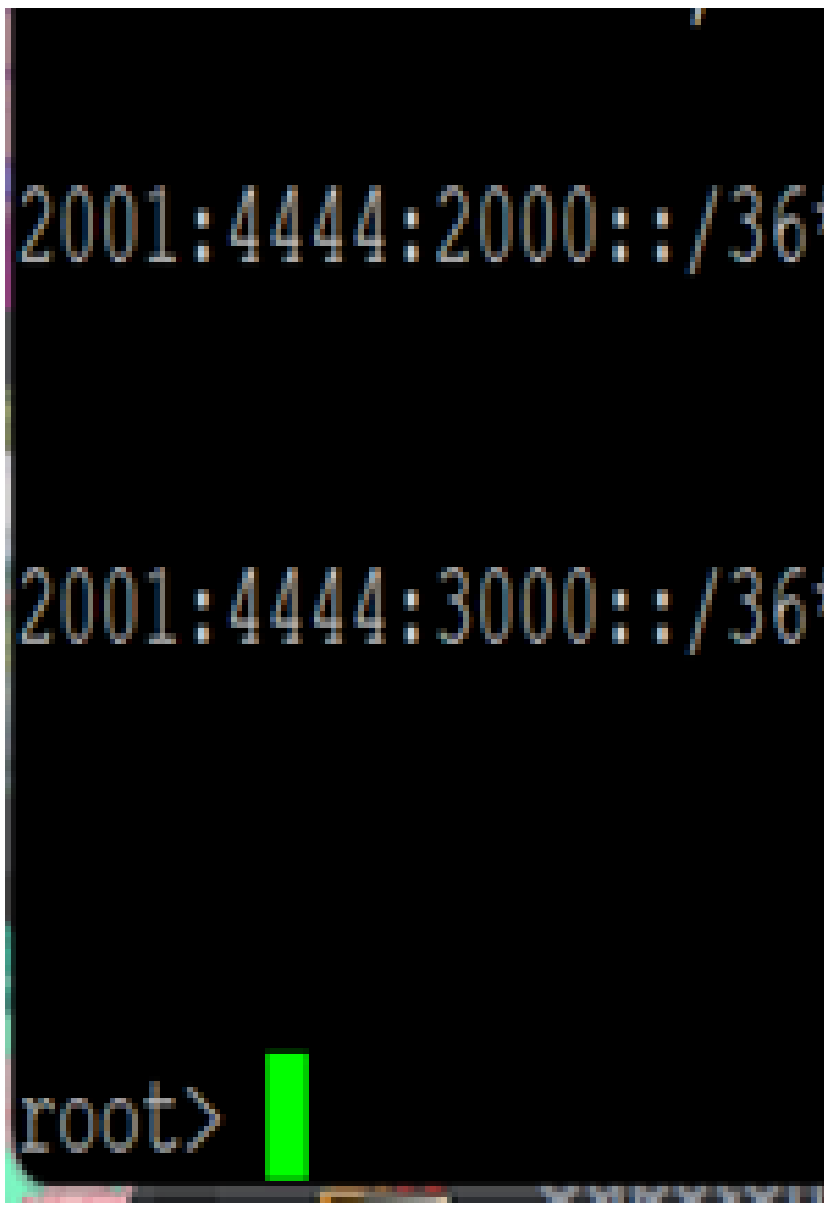


Policy on R5

The IPv6 prefix list P20 allows IP addresses within the 2001:4444:2000::/36 and 2001:4444:3000::/36 ranges and originate from AS 2001.

ipv6 prefix-list P20 seq 5 permit 2001:4444:2000::/36
ipv6 prefix-list P20 seq 10 permit 2001:4444:3000::/36
ip as-path access-list 10 permit ^2001$

Routes on J8



Policy on J6

This policy exports routes originating from AS 2001. It includes routes that match the exact prefixes 2001:4444:2000::/36 and 2001:4444:3000::/36.

set policy-options as-path AS2001 "^2001$"
set policy-options policy-statement EXPORT term 1 from route-filter 2001:4444:2000::/36 exact
set policy-options policy-statement EXPORT term 1 from route-filter 2001:4444:3000::/36 exact
set policy-options policy-statement EXPORT term 1 from as-path AS2001

Policy 21

Task: Allow only IPv6 prefixes sourced by AS2001 that catches 2001:4444:8000::/any mask, 2001:4444:A000::/any mask, 2001:4444:C000::/any mask.

Routes on R6

When creating this I assumed that all routes need to come from AS 2001 AND either start with 2001:444:8000:: or start with 2001:4444:A000:: or start with 2001:4444:C000::

There are no routes that start with that. That is also the reason I chose /48 because I want the 48 bits to be static. I was unsure about the question. I could have changed the /48 to something lower like /33 but then the bits would not be static.

Policy on R5

ipv6 prefix-list P20 seq 5 permit 2001:4444:8000::/48 le 128
ipv6 prefix-listaP20 seq 10 permit 2001:4444:A000::/48 le 128
ipv6 prefix-list P20 seq 15 permit 2001:4444:C000::/48 le 128
ip as-path access-list 10 permit _2001_

Routes on J8

Policy on J6

set policy-options as-path AS2001 "^2001$"
set policy-options policy-statement EXPORT term 1 from route-filter 2001:4444:8000::/48 orlonger
set policy-options policy-statement EXPORT term 1 from route-filter 2001:4444:A000::/48 orlonger
set policy-options policy-statement EXPORT term 1 from route-filter 2001:4444:C000::/48 orlonger
set policy-options policy-statement EXPORT term 1 from as-path AS2001

Policy 22

Task: Allow only any IPv6 prefixes sourced by AS2001 with the pattern 2001:4444:8000::/any mask. That means if there were many prefixes with the pattern 2001:4444:8000::/, they should be allowed.

Routes on R6

When creating this I assumed that all routes need to come from AS 2001 AND either start with 2001:444:8000::
There are no routes that start with that in between those masks.. That is also the reason I chose /48 because I want the 48 bits to be static. I was unsure about the question. I could have changed the /48 to something lower like /33 but then the bits would not be static.

Policy on R5

ipv6 prefix-list P20 seq 5 permit 2001:4444:8000::/48 le 128
ip as-path access-list 10 permit _2001_

Routes on J8

Policy on J6

set policy-options as-path AS2001 "^2001$"
set policy-options policy-statement EXPORT term 1 from route-filter 2001:4444:8000::/48 orlonger
set policy-options policy-statement EXPORT term 1 from as-path AS2001

Policy 23

Task: Allow only IPv6 prefixes sourced by AS2001 with the pattern 2001:4444:8000::/any mask. That means if there were many prefixes with the pattern 2001:4444:8000::/, they should be allowed.

Routes on R6

When creating this I assumed that all routes need to come from AS 2001 AND either start with 2001:444:8000:: There are no routes that start with that in between those masks.. That is also the reason I chose /48 because I want the 48 bits to be static. I was unsure about the question. I could have changed the /48 to something lower like /33 but then the bits would not be static.

Routes on J8

Policy on R5

ipv6 prefix-list P20 seq 5 permit 2001:4444:8000::/48 le 128
ip as-path access-list 10 permit _2001_

Policy on J6

set policy-options as-path AS2001 "^2001$"
set policy-options policy-statement EXPORT term 1 from route-filter 2001:4444:8000::/48 orlonger
set policy-options policy-statement EXPORT term 1 from as-path AS2001

Policy 24

Task: Allow only any IPv6 prefixes sourced by AS2001 with masks longer than /35.

Routes on R6

```
B   2001:4443:2000::/35 [20/0]
     via FE80::C805:A4FF:FECF:1C,
B   2001:4444::/37 [20/0]
     via FE80::C805:A4FF:FECF:1C,
B   2001:4444:800::/37 [20/0]
     via FE80::C805:A4FF:FECF:1C,
B   2001:4444:2000::/36 [20/0]
     via FE80::C805:A4FF:FECF:1C,
B   2001:4444:3000::/36 [20/0]
     via FE80::C805:A4FF:FECF:1C,
B   2001:4444:8000::/35 [20/0]
     via FE80::C805:A4FF:FECF:1C,
B   2001:4444:A000::/35 [20/0]
     via FE80::C805:A4FF:FECF:1C,
R7#
```

Policy on R5

The IPv6 prefix list P20 permits any IP address (::/0) with a subnet mask of /35 or larger. The AS-path access list allows routes that originate from AS 2001.

ipv6 prefix-list P20 seq 5 permit ::/0 ge 35
ip as-path access-list 10 permit ^2001$

Routes on J8

```
inet6.0: 11 destinations, 11 rou
+ = Active Route, - = Last Activ

2001:4443:2000::/35*[BGP/170] 0
                      AS path: 1
                    > to fc00:12
2001:4444::/37     *[BGP/170] 0
                      AS path: 1
                    > to fc00:12
2001:4444:800::/37 *[BGP/170] 0
                      AS path: 1
                    > to fc00:12
2001:4444:2000::/36*[BGP/170] 0
                      AS path: 1
                    > to fc00:12
2001:4444:3000::/36*[BGP/170] 0
                      AS path: 1
                    > to fc00:12
2001:4444:8000::/35*[BGP/170] 0
                      AS path: 1
                    > to fc00:12
2001:4444:a000::/35*[BGP/170] 0
                      AS path: 1
                    > to fc00:12
```

Policy on J6

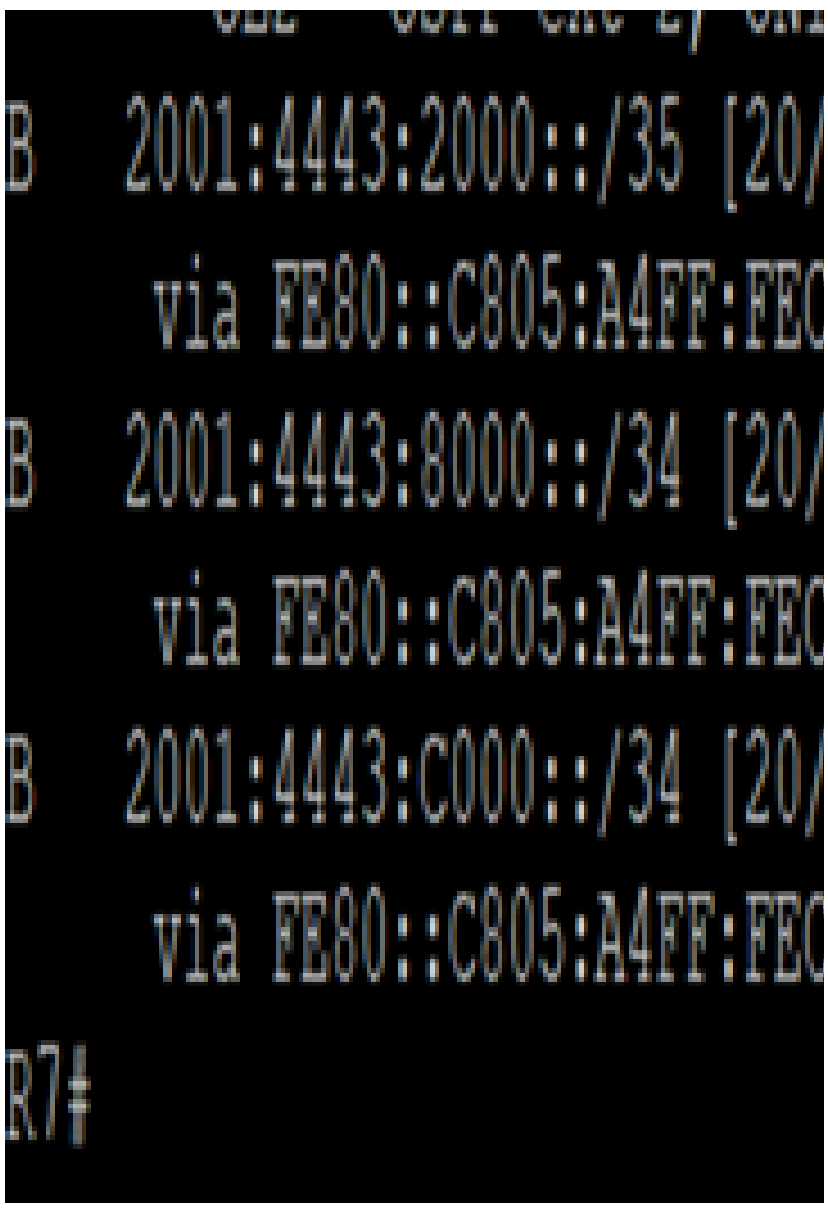
This policy exports routes originating from AS 2001 and includes any IP address (::/0) with subnet masks ranging from /35 to /128. It combines the criteria of matching the AS-path for AS 2001 and the specified prefix length range.

set policy-options as-path AS2001 "^2001$"
set policy-options policy-statement EXPORT term 1 from route-filter ::/0 prefix-length-range /35-/128
set policy-options policy-statement EXPORT term 1 from as-path AS2001

Policy 25

Task: Allow only any IPv6 prefixes sourced by AS2001 that begin with 2001:4443:

Routes on R6

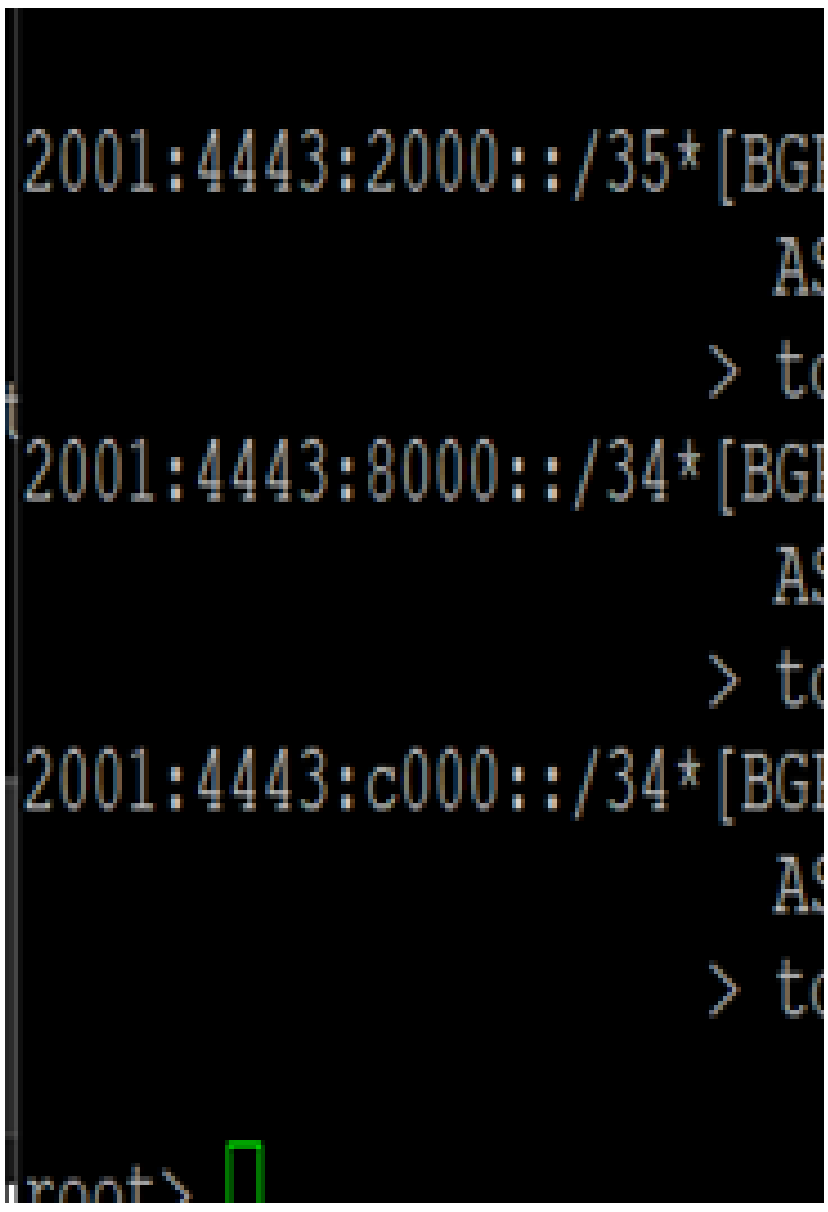


Policy on R5

The IPv6 prefix list P20 permits IP addresses within the 2001:4443::/32 range, extending to any subnet mask length up to /128. The AS-path access list allows routes that originate specifically from the autonomous system number 2001.

ipv6 prefix-list P20 seq 5 permit 2001:4443::/32 le 128
ip as-path access-list 10 permit ^2001$

Routes on J8



Policy on J6

This policy exports routes originating from AS 2001 and includes routes that match the 2001:4443::/32 prefix and any longer subnet masks. It combines the criteria of matching the AS-path for AS 2001 and the specified prefix range.

set policy-options as-path AS2001 "^2001$"
set policy-options policy-statement EXPORT term 1 from route-filter 2001:4443::/32 orlonger
set policy-options policy-statement EXPORT term 1 from as-path AS2001

Conclusion

In this lab, I successfully implemented and observed route filtering policies to **control the propagation** of routes between different autonomous systems. The topology setup involved multiple routers (**R1, R2, R3, R4, R5, J6, R7, and J8**) with feeder routers and Juniper routers working together to showcase the **impact of my policies**.

I used various prefix lists and AS-path access lists to define and apply specific route-filtering criteria. These policies were **implemented** on routers **R5 and J6**, and their effects were observed on routers **R7 and J8**. Each policy was carefully crafted to allow or deny specific prefixes based on their origin AS and prefix length, ensuring **precise control** over the routing information exchanged **between peers**.

Although I encountered some **challenges**, particularly with filtering routes based on **specific digits in Juniper AS numbers** *(an approach that proved efficient on Cisco but problematic with Juniper due to lack of documentation)*, the overall experience emphasized the **importance of precise**, well-defined routing policies. But I believe filtering routes based on specific digits within AS numbers can lead to **unintended consequences** and **increased complexity in managing network issues**.

Throughout this lab, I gained a better understanding of lot about **IPv6 subnet masks**. I also gained a better understanding of how regular expressions (**regex**) work in the context of **AS-path filtering**. The lab demonstrated to me the critical need for **clear and effective** BGP policies to maintain the reliability and efficiency of network traffic, illustrating how precise control of routing information is essential for robust network management.