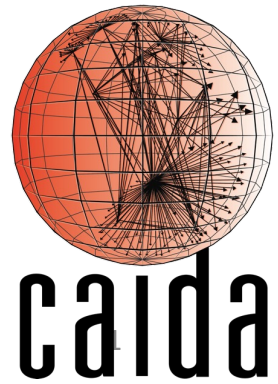
CSE291 Internet Data Science for Cybersecurity

BGP Hijacking

1/30/2023

Ben Du

UCSDCSE
Computer Science and Engineering



Learning Objectives

- Understand BGP route selection
- Understand the mechanisms of BGP hijacking
- Become familiar with the CAIDA Prefix2AS dataset

Overview

1. Recap of BGP
2. BGP Hijacking
3. Detecting BGP hijacking events
4. CAIDA prefix2as dataset

Decentralized Structure of the Internet

- The Internet is divided into Autonomous Systems (AS)
- Each AS owns a range of IP addresses (an IP prefix)

AS 15169
8.8.8.0/24

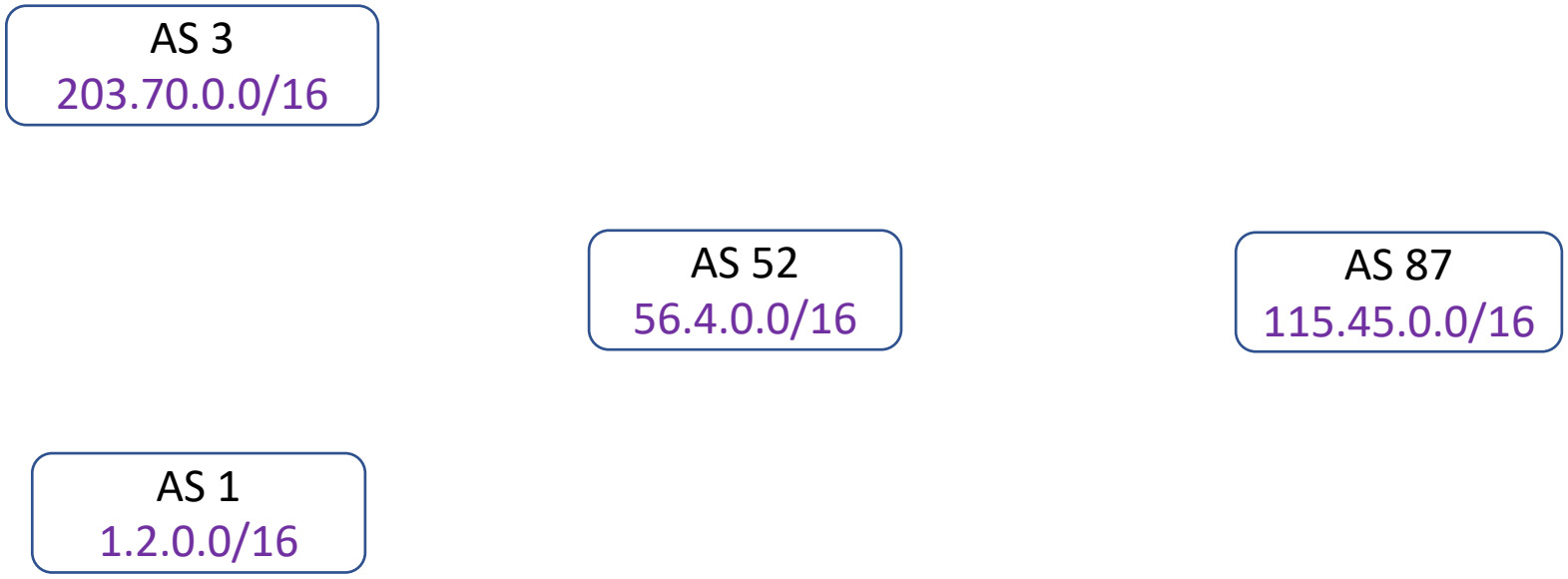
AS 6461

AS 7015

AS 7018

Simplified Diagram

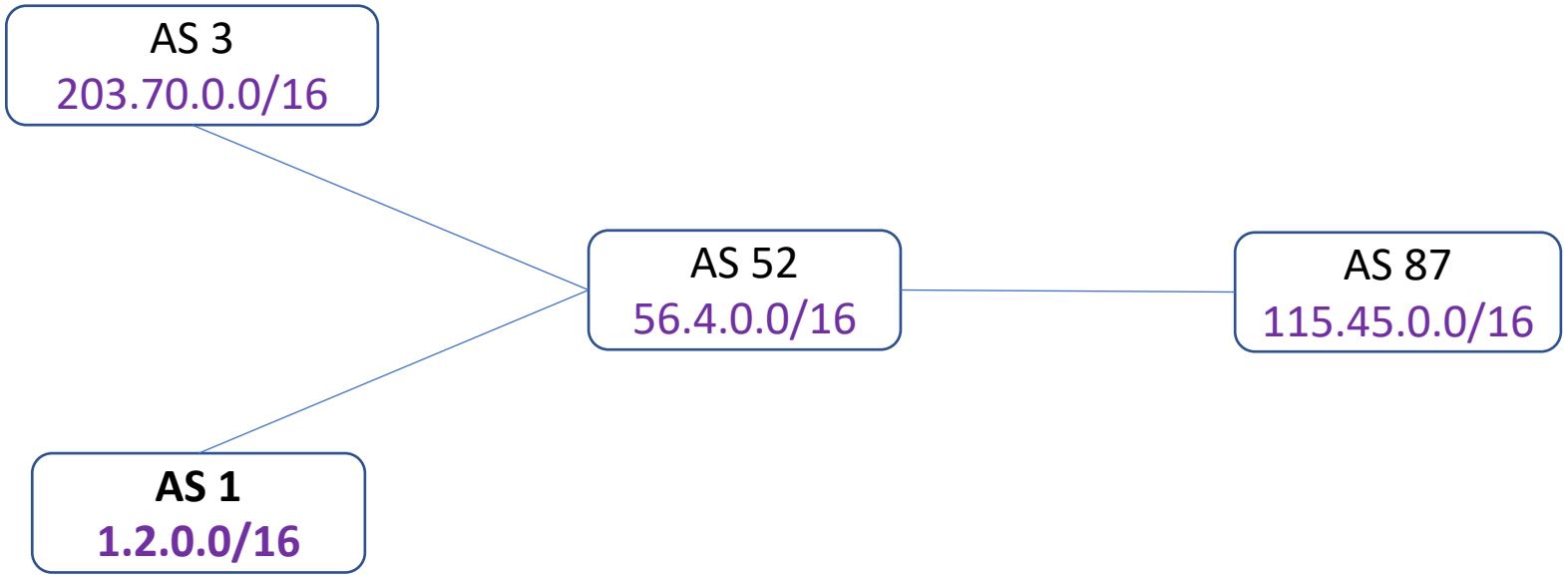
- The Internet is divided into Autonomous Systems (AS)
- Each AS owns a range of IP addresses (an IP prefix)



ASes Share Reachability Information via BGP

- ASes send BGP messages to each other (control plane)
- Traffic flow in the opposite direction (data plane)

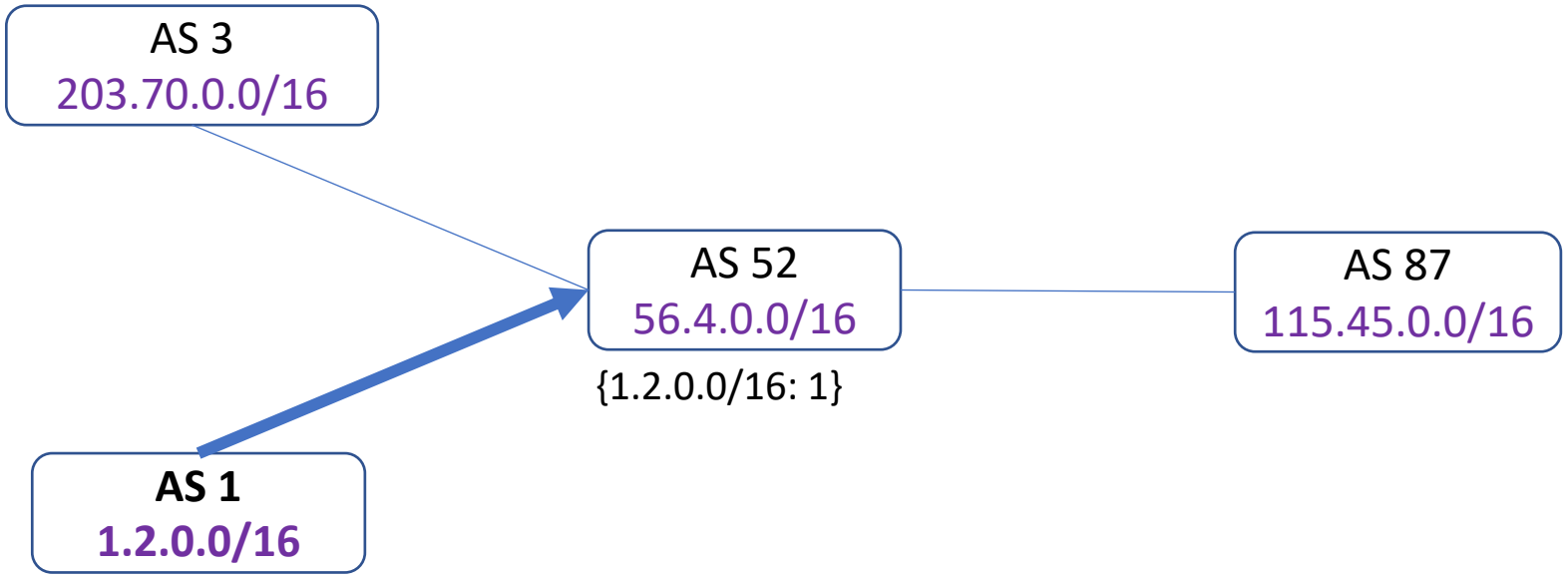
Where do I send an IP packet destined to 1.2.2.4?



ASes Share Reachability Information via BGP

- ASes send BGP messages to each other (control plane)
- Traffic flow in the opposite direction (data plane)

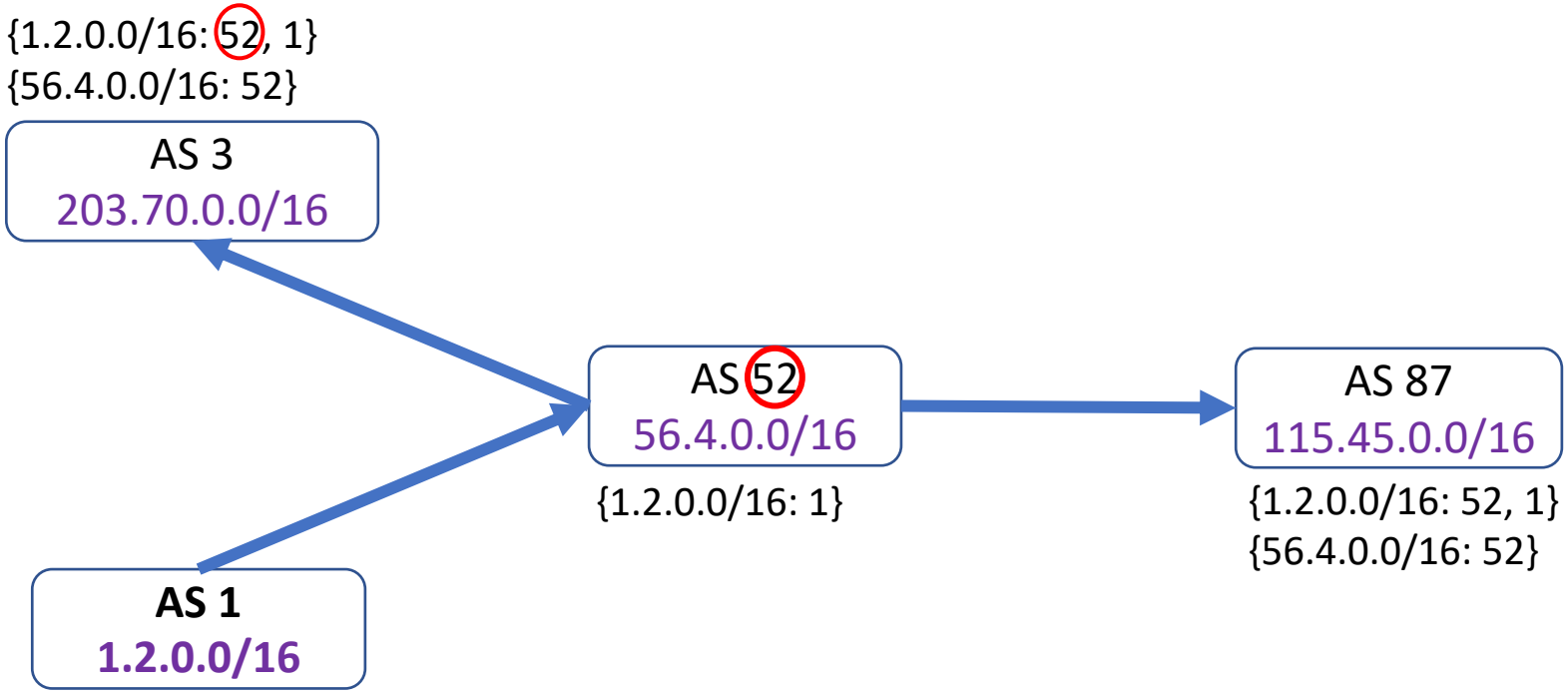
Where do I send an IP packet destined to 1.2.2.4?



ASes Share Reachability Information via BGP

- ASes send BGP messages to each other (control plane)
- Traffic flow in the opposite direction (data plane)

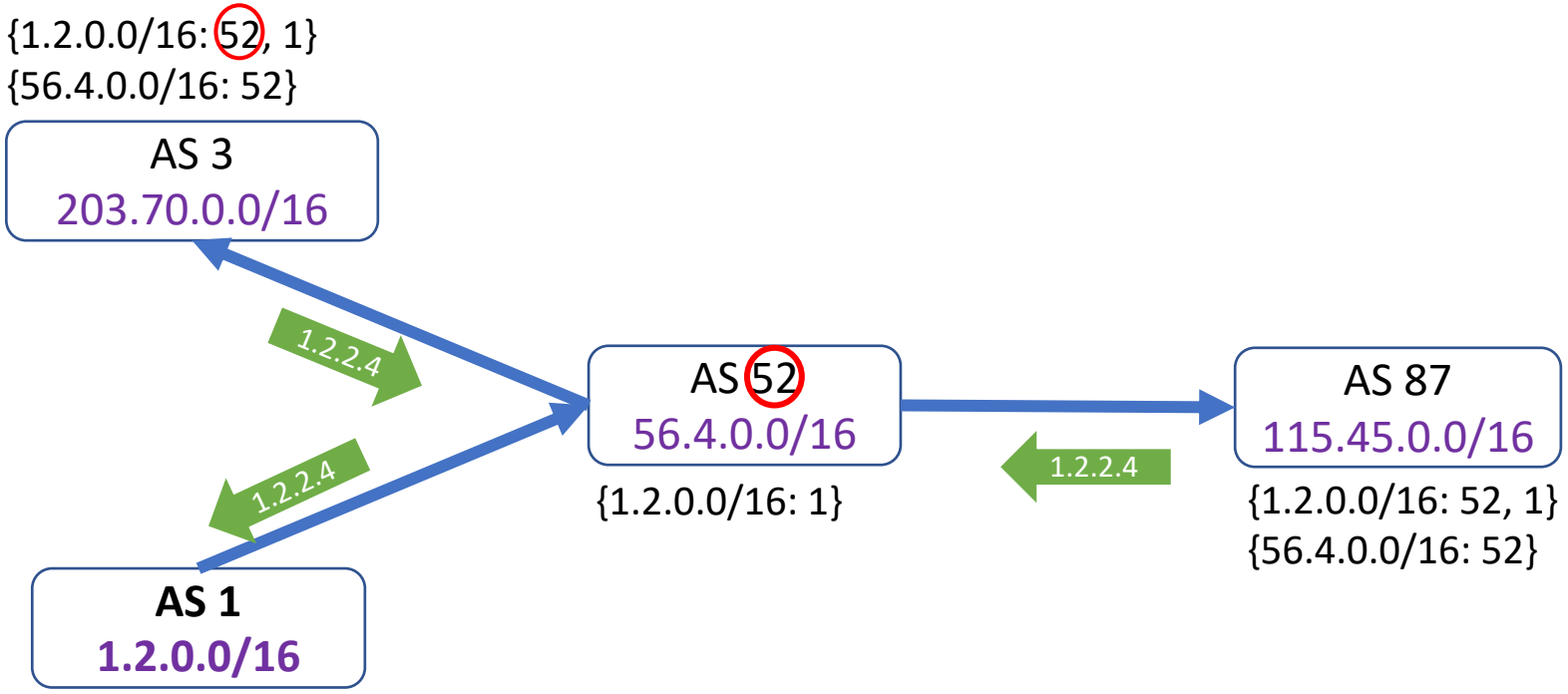
Where do I send an IP packet destined to 1.2.2.4?



ASes Share Reachability Information via BGP

- ASes send BGP messages to each other (control plane)
- Traffic flow in the opposite direction (data plane)

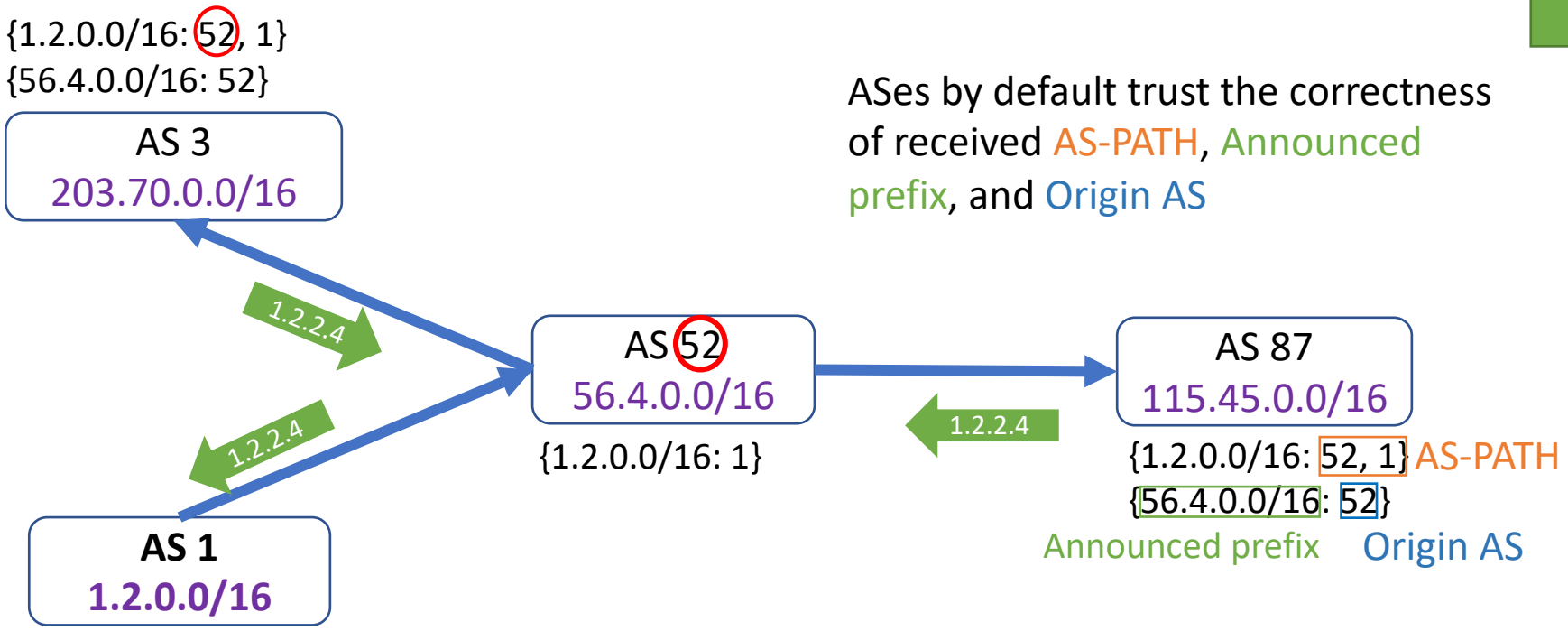
Where do I send an IP packet destined to 1.2.2.4?



ASes Share Reachability Information via BGP

- ASes send BGP messages to each other (control plane)
- Traffic flow in the opposite direction (data plane)

Where do I send an IP packet destined to 1.2.2.4?



BGP Route Selection

1. Longest prefix matching
2. Prefer customer over peer, prefer peer over provider
3. Shortest AS-PATH

For simplicity, we do not consider AS relationships in this context

- Ignore rule 2 for now

Longest Prefix Matching

- Longest prefix matching
  - A destination IP address will be mapped to its longest covering prefix

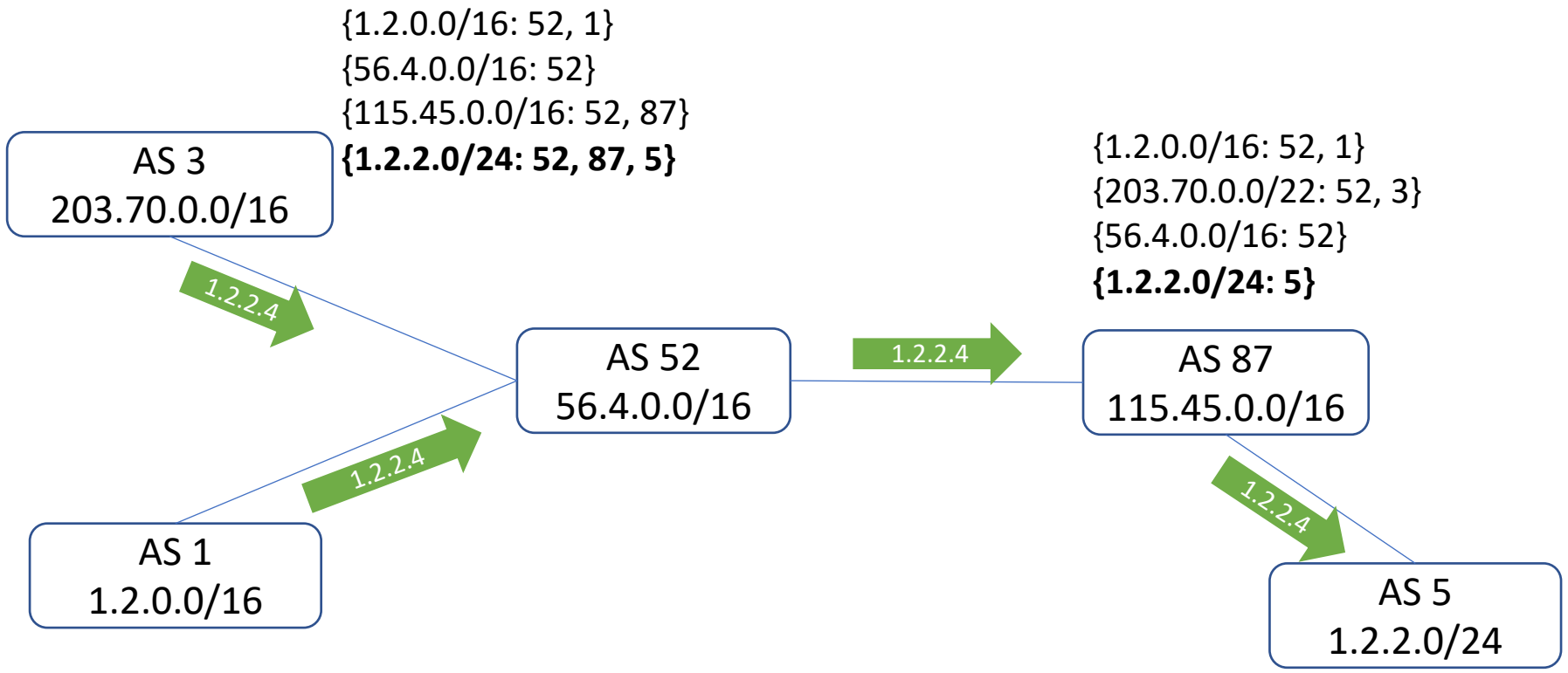
Example: Which prefix should 1.2.2.4 be matched to?

1.2.2.4	00000001.00000010.00000010.00000100
In your routing table	Prefix, 16-bit
1.2.0.0/16	00000001.00000010.00000000.00000000
1.2.2.0/24	00000001.00000010.00000010.00000000
	Prefix, 24-bit

Longest Prefix Matching

Where do I send an IP packet destined to 1.2.2.4?

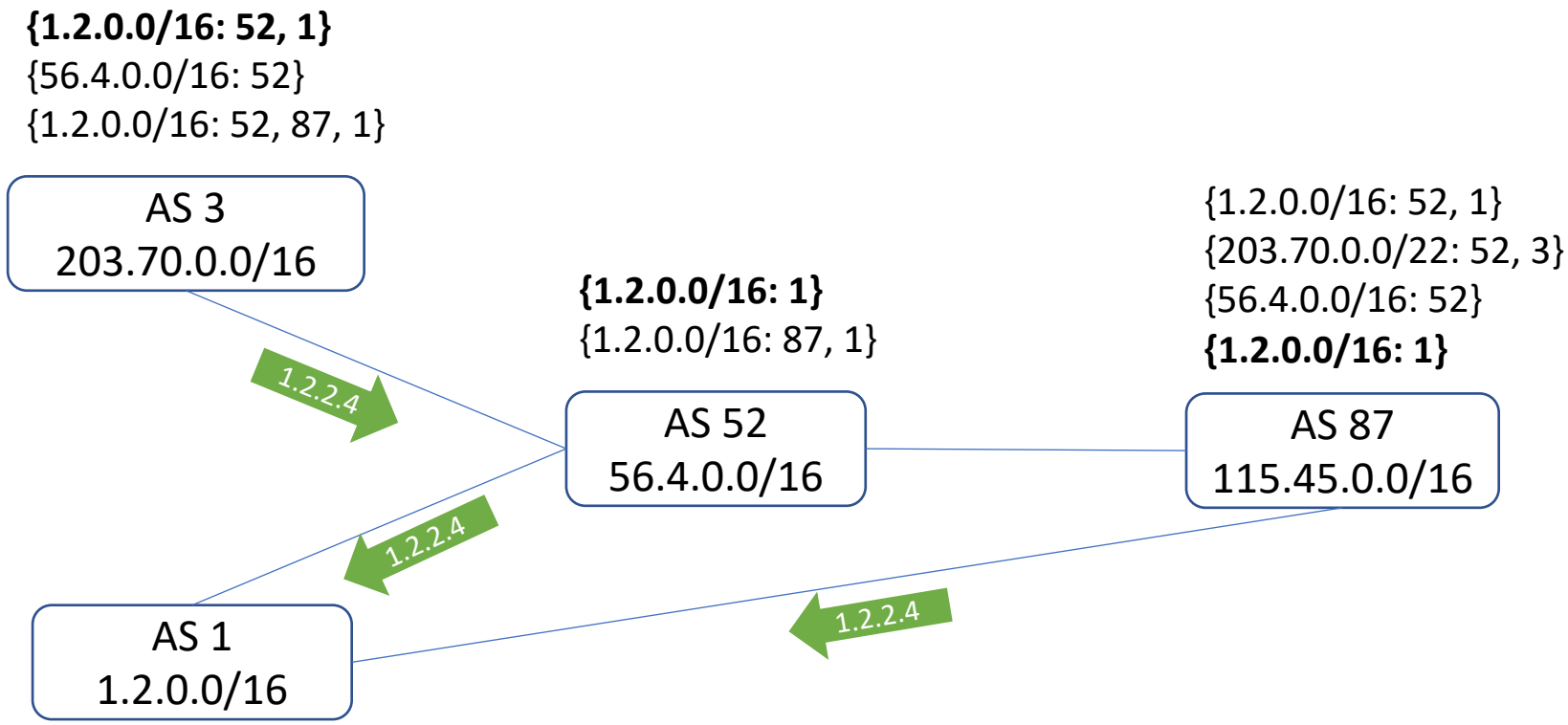
- Longest prefix matching
  - A destination IP address will be mapped to its longest covering prefix



Shortest AS path

Where do I send an IP packet destined to 1.2.2.4?

- The route toward a prefix with fewer AS hops will be selected



From Last Lecture

- We understood the risk of a mis-behaving router. In 1982, Rosen [41] first documented this vulnerability in RFC 827, in the context of a predecessor of BGP called the Exterior Gateway Protocol (EGP)
  - "If any gateway sends an NR [neighbor reachability] message with **false information**, claiming to be an appropriate first hop to a network which it in fact cannot even reach, traffic destined to that network may never be delivered. Implementers must bear this in mind."

Problem: Unauthorized re-routing of traffic

- BGP hijacking is the **malicious re-routing** of Internet **traffic** across network boundaries
- Internet routing was **originally designed** to operate in a **trusted environment**

THANKS, BGP. —

BGP event sends European mobile traffic through China Telecom for 2 hours

Improper leak to Chinese-government-owned telecom lasts up to two hours.

DAN GOODIN - 6/8/2019, 9:05 AM

BORDER GATEWAY PROTOCOL —

How 3ve's BGP hijackers eluded the Internet—and made $29M

3ve used addresses of unsuspecting owners—like the US Air Force.

DAN GOODIN - 12/21/2018, 9:30 AM

Harms of BGP Hijacks

- Interrupted service
  - Victim may become unreachable
- Compromised privacy
  - Attackers eavesdrop on your activities over the Internet
- Stolen Identity
  - Attackers use victim’s identity to conduct illegal activities such as phishing and spamming
- Monetary loss
  - Cryptocurrency hijacks

BGP Vulnerability

- BGP includes no mechanism to validate the correctness of the information exchanged between participants.
  - Attackers can originate any prefix without authorization (origin hijack)
  - Attackers can modify any part of received BGP messages (path hijack)
  - Misconfigurations can cause damage (route leak)

Types of Hijacks

{1.2.0.0/16: 52, 1} AS-PATH
{56.4.0.0/16: 52}
Announced prefix Origin AS

- Origin hijack
  - Exact prefix hijack
  - Sub-prefix hijack
  - Attacker changes the origin AS and/or the announced prefix

- AS-PATH manipulation
  - Attacker changes the one or more hops in AS-PATH

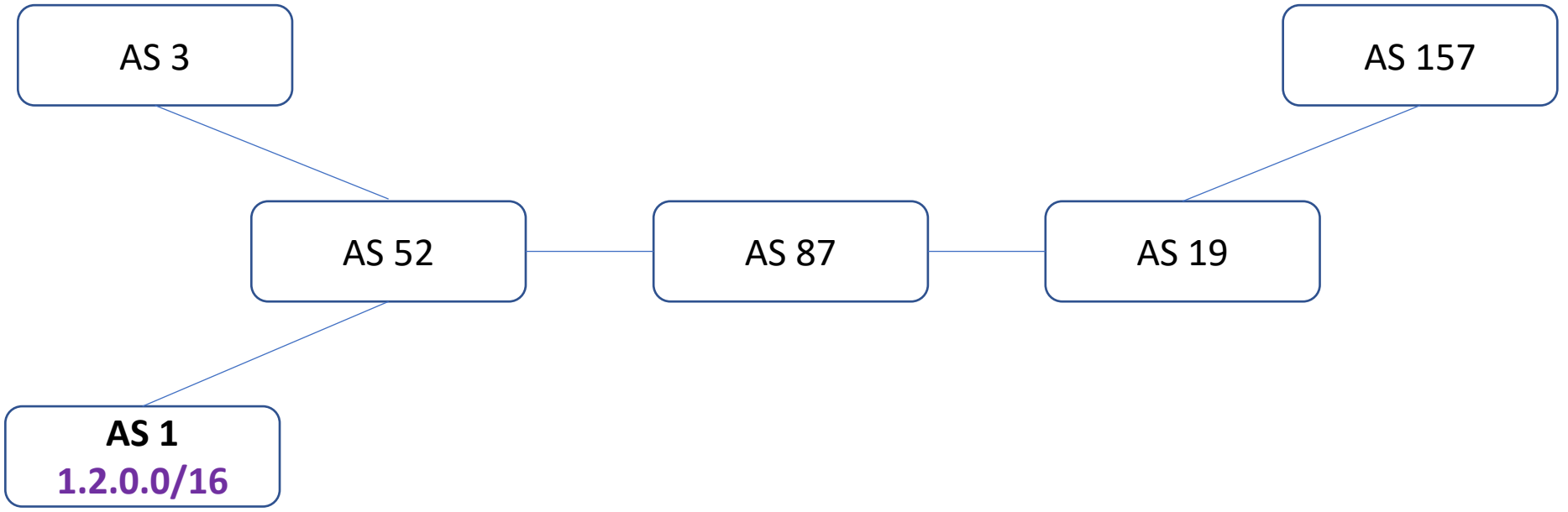
Man in the Middle!

- Prefix Alteration
  - Attacker only changes the announced prefix

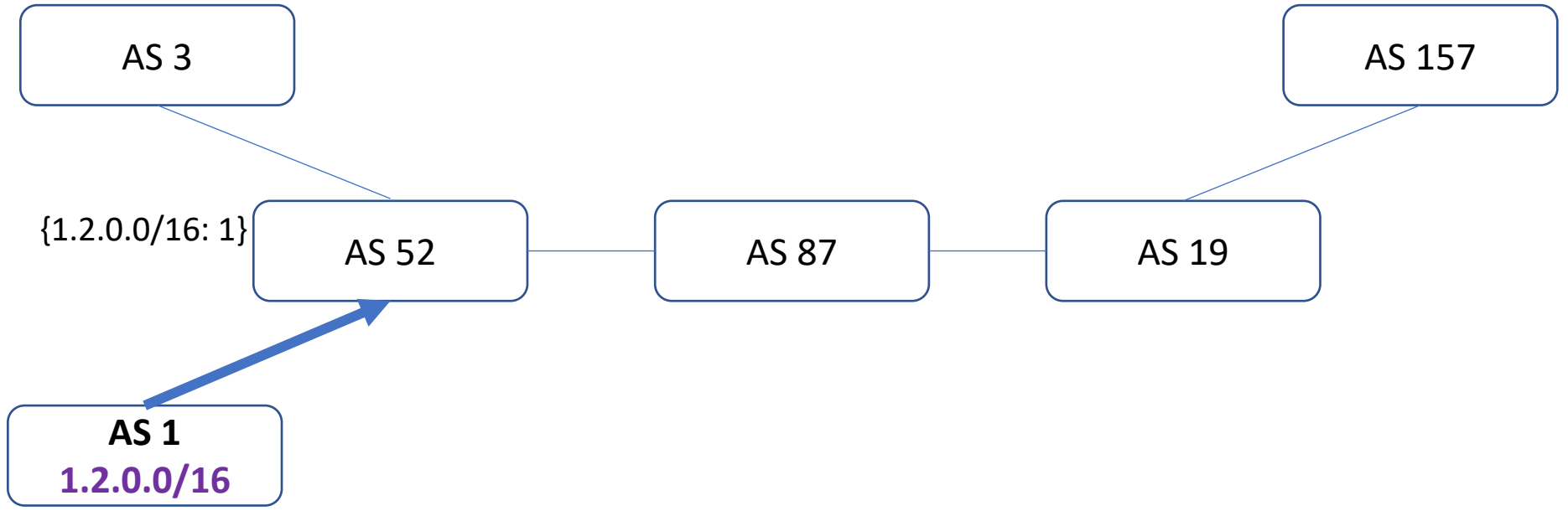
Origin Hijack - attacker changes the origin AS of a prefix to its own

- Exact-prefix hijacking
  - Hijacker announces the victim's prefix

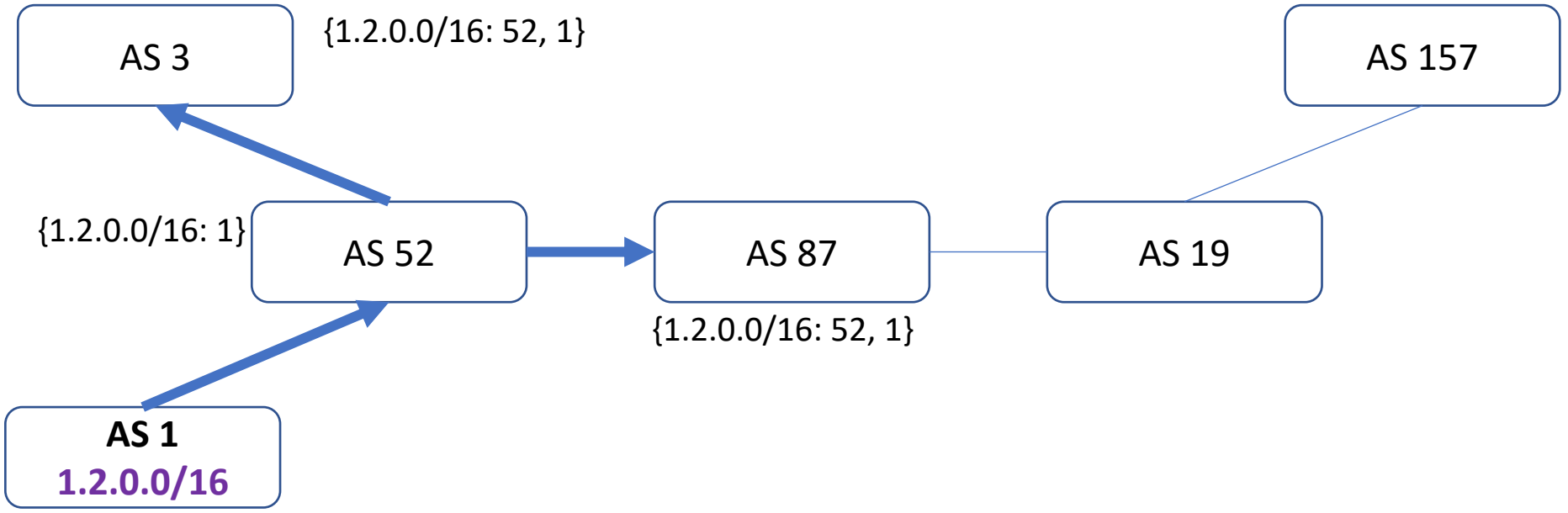
Origin Hijack - Exact Prefix Hijacking



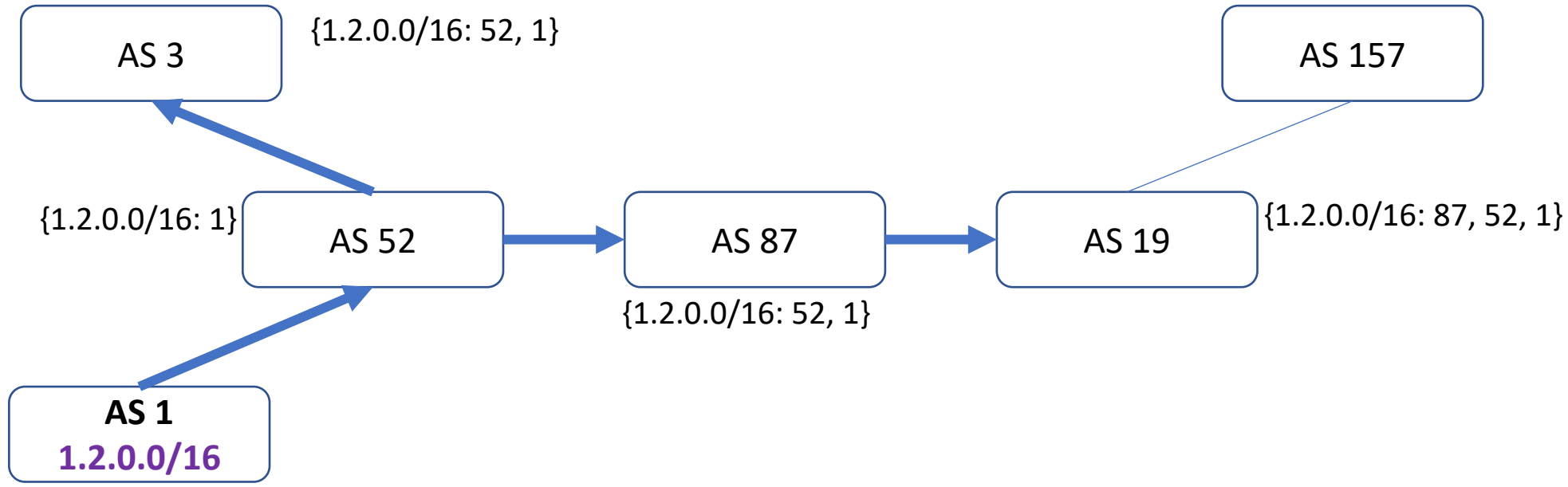
Origin Hijack - Exact Prefix Hijacking



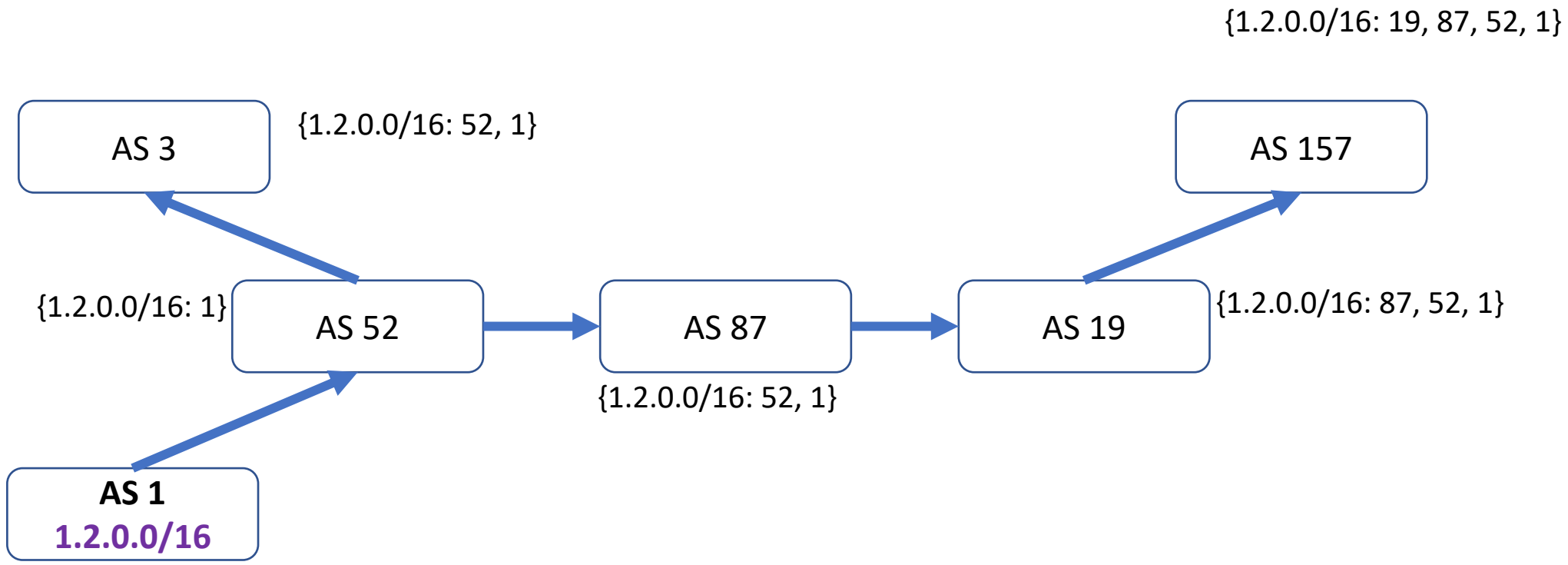
Origin Hijack - Exact Prefix Hijacking



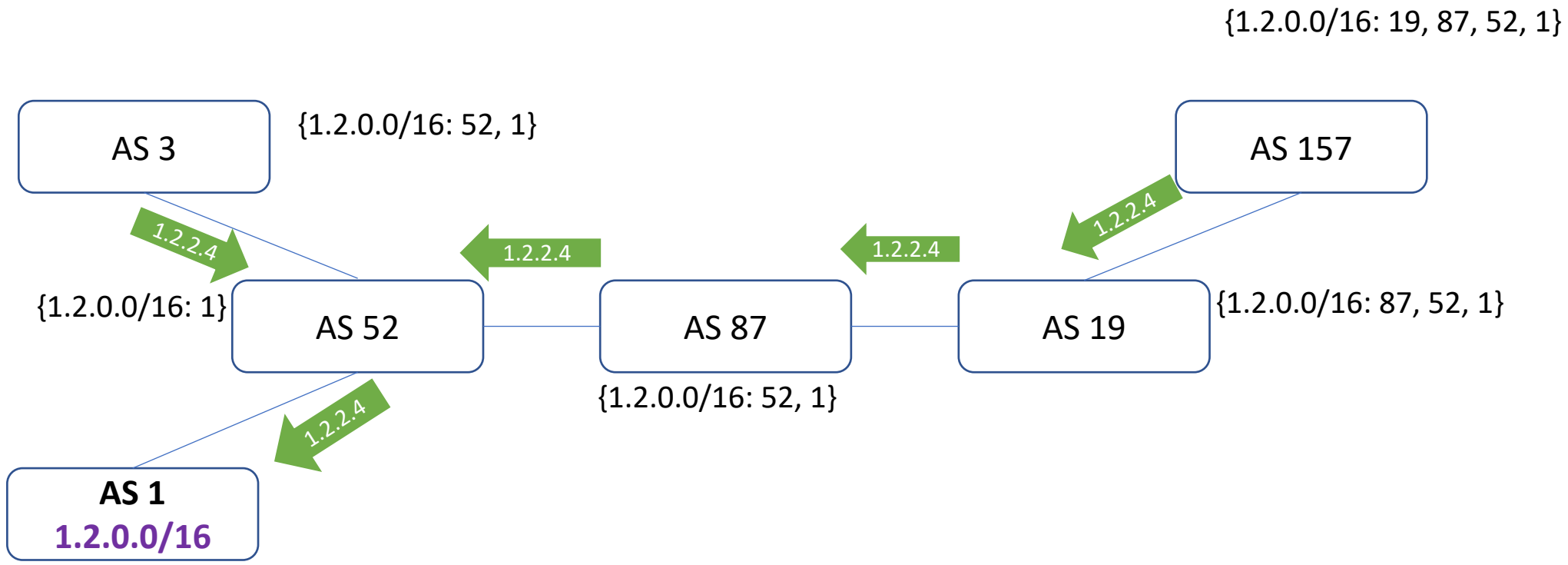
Origin Hijack - Exact Prefix Hijacking



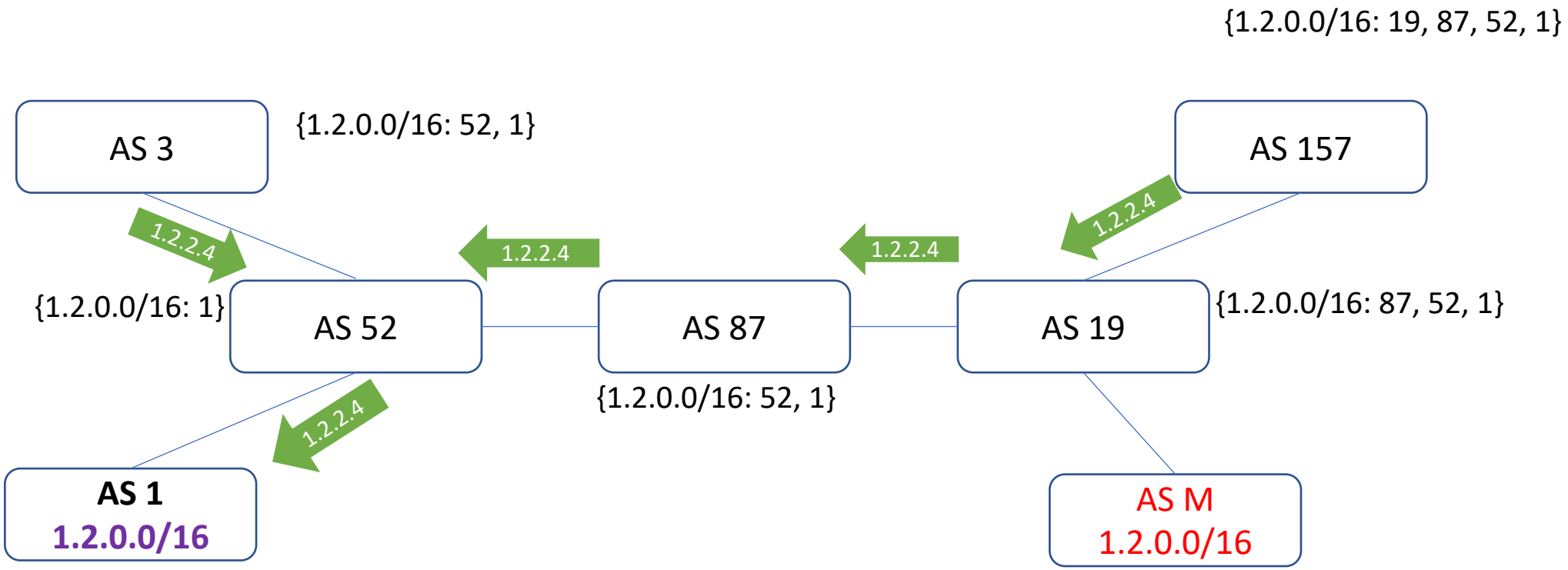
Origin Hijack - Exact Prefix Hijacking



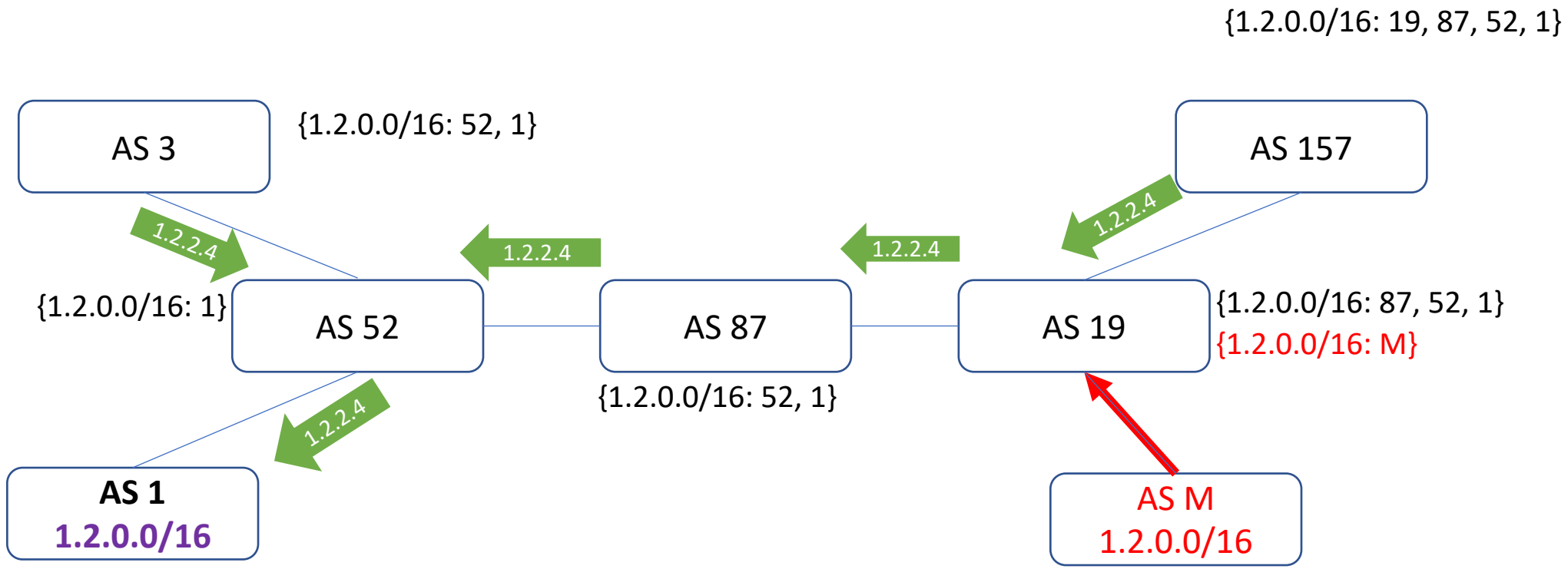
Origin Hijack - Exact Prefix Hijacking



Origin Hijack - Exact Prefix Hijacking

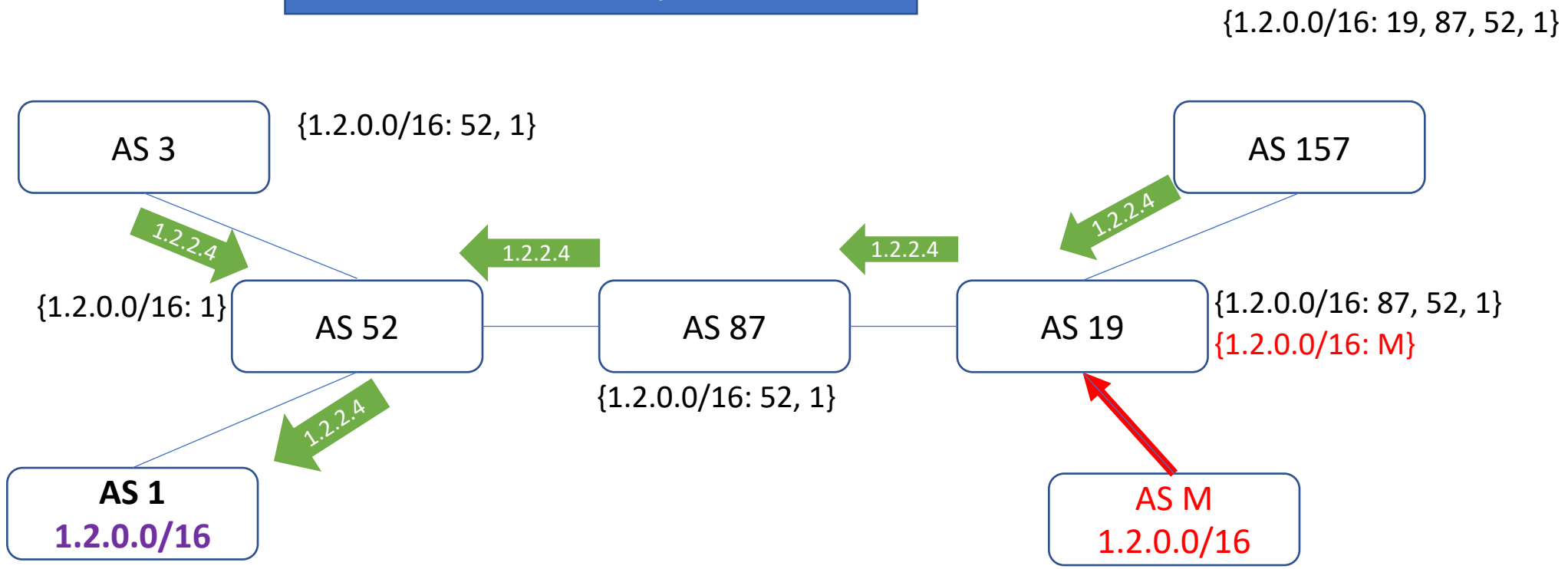


Origin Hijack - Exact Prefix Hijacking



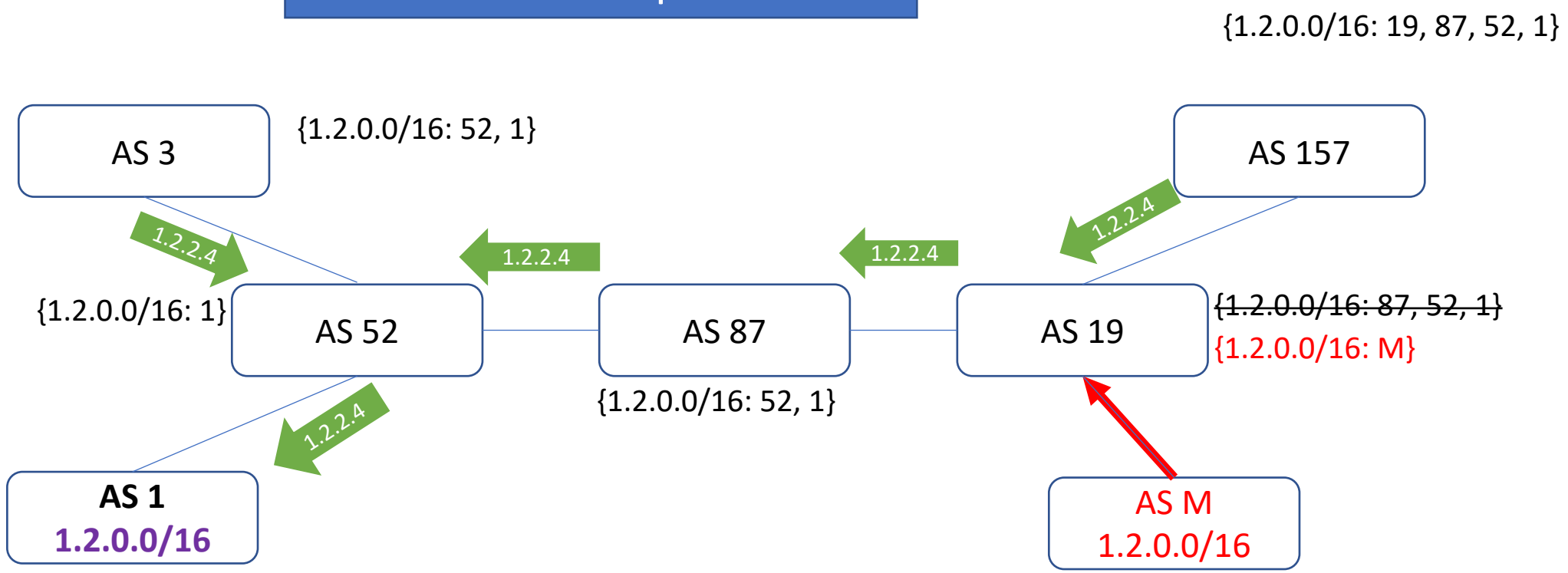
Origin Hijack - Exact Prefix Hijacking

Route selection:
Shortest AS-PATH preferred!



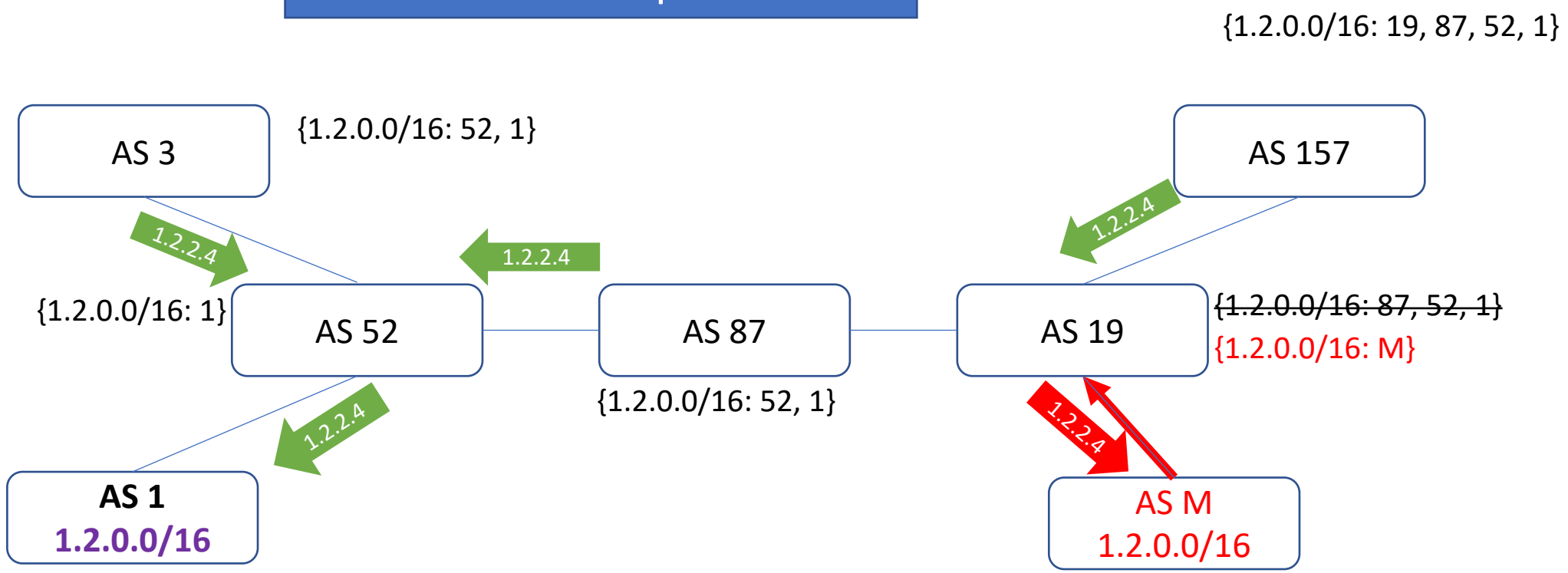
Origin Hijack - Exact Prefix Hijacking

Route selection:
Shortest AS-PATH preferred!

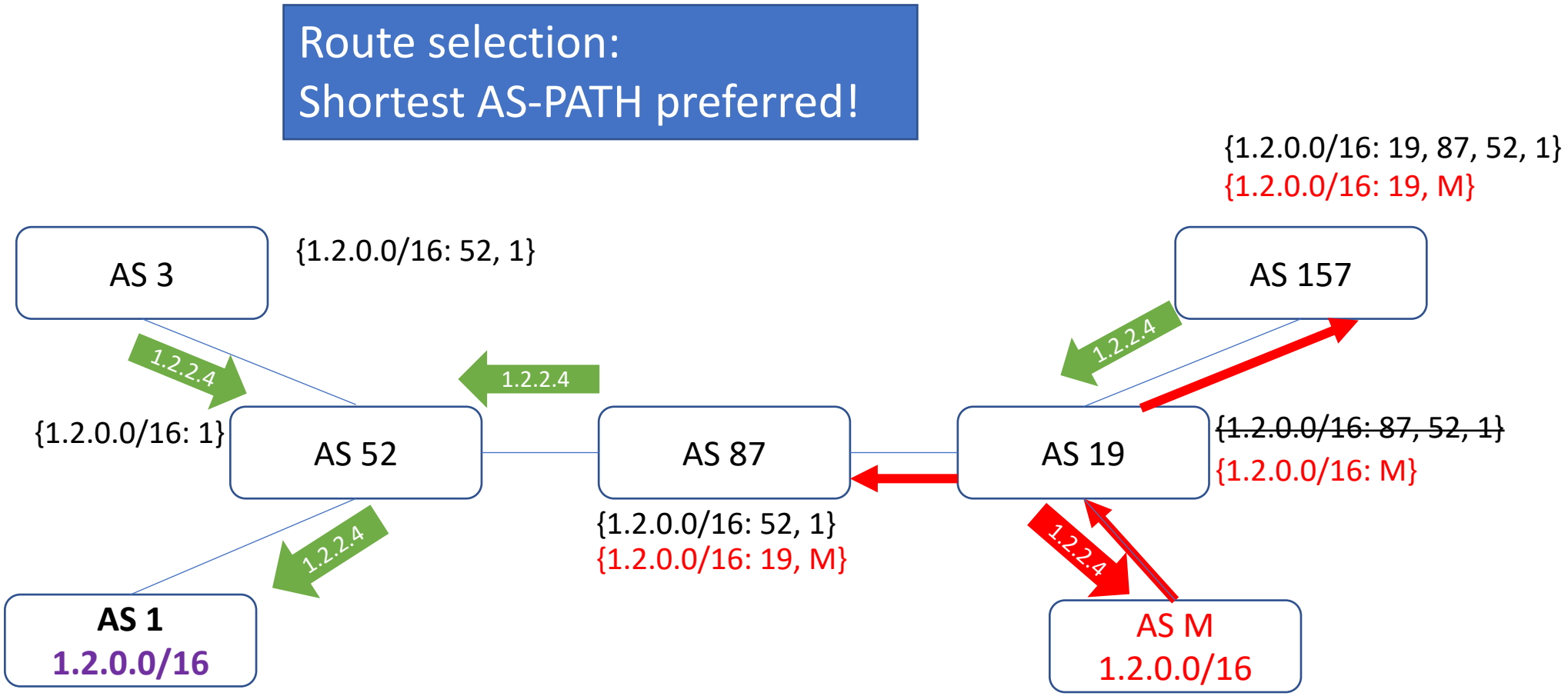


Origin Hijack - Exact Prefix Hijacking

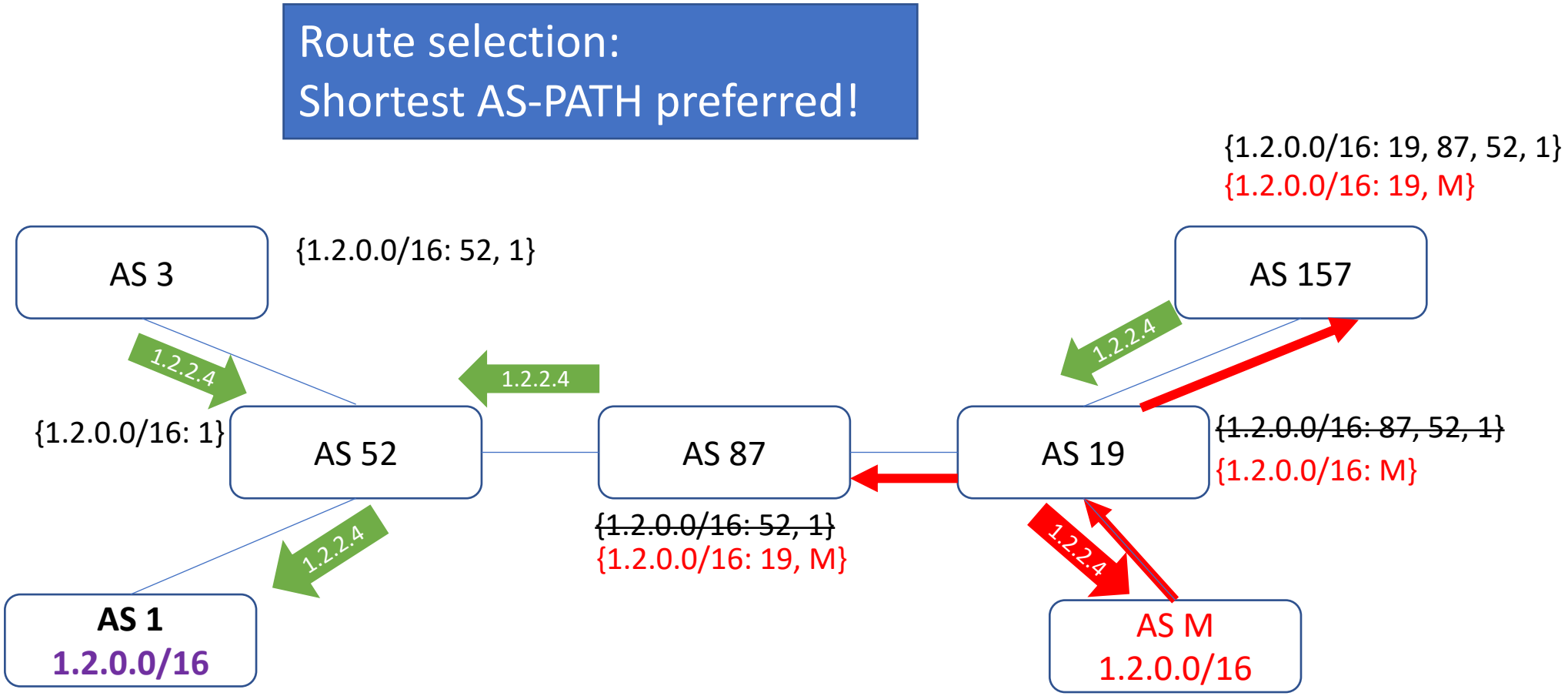
Route selection:
Shortest AS-PATH preferred!



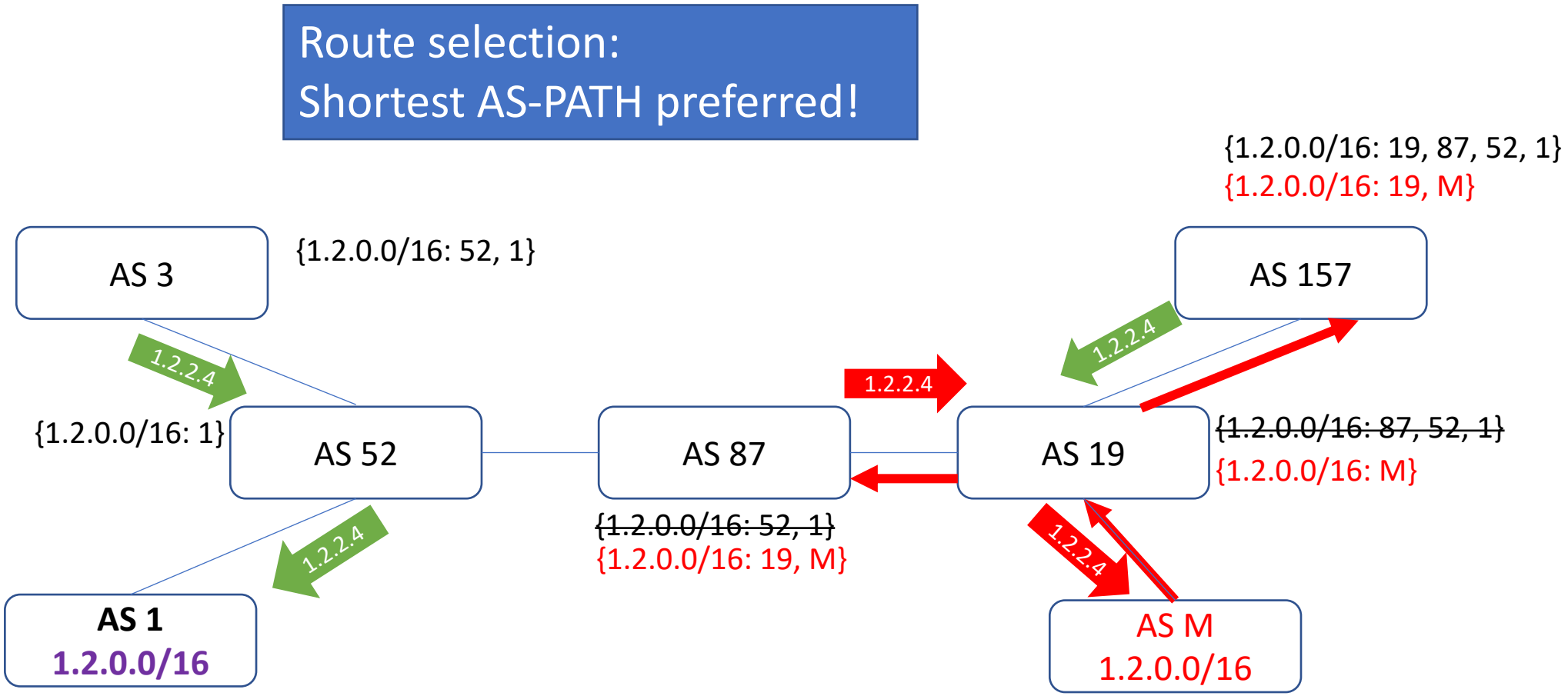
Origin Hijack - Exact Prefix Hijacking



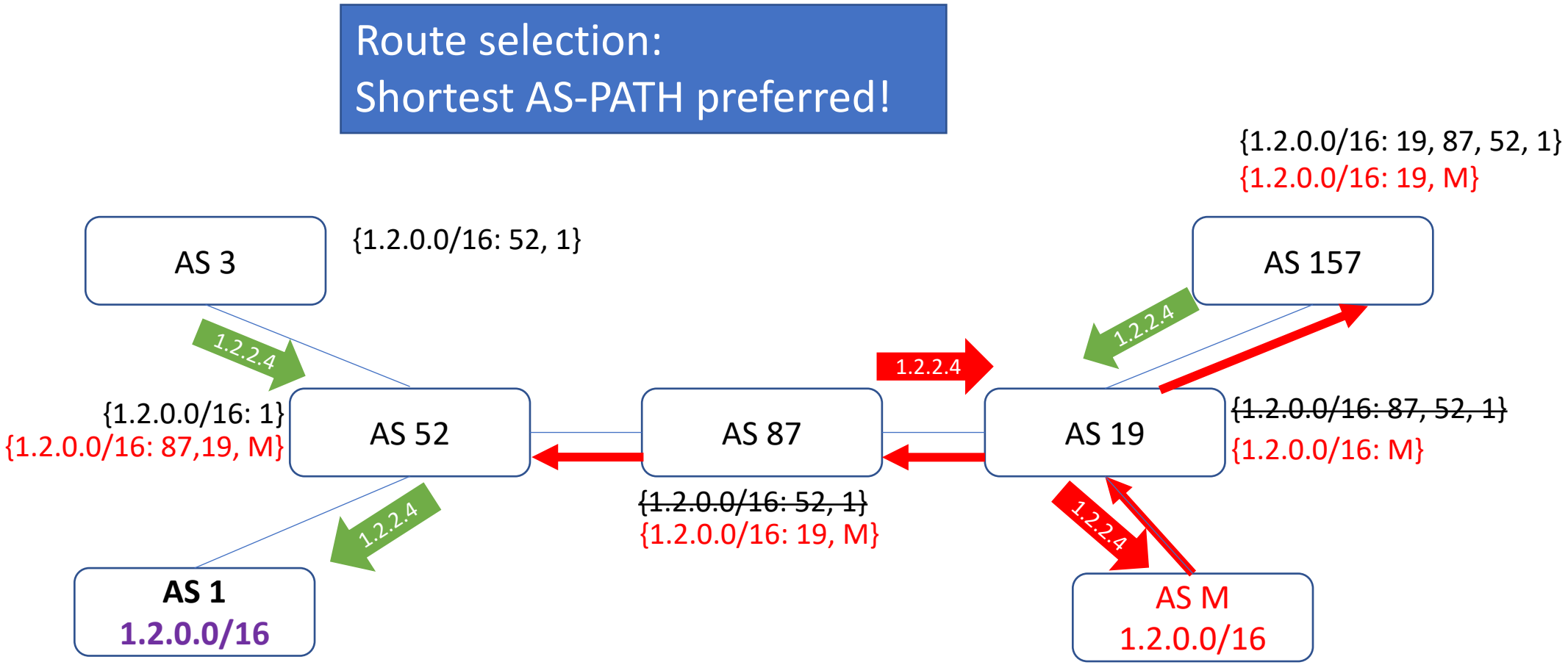
Origin Hijack - Exact Prefix Hijacking



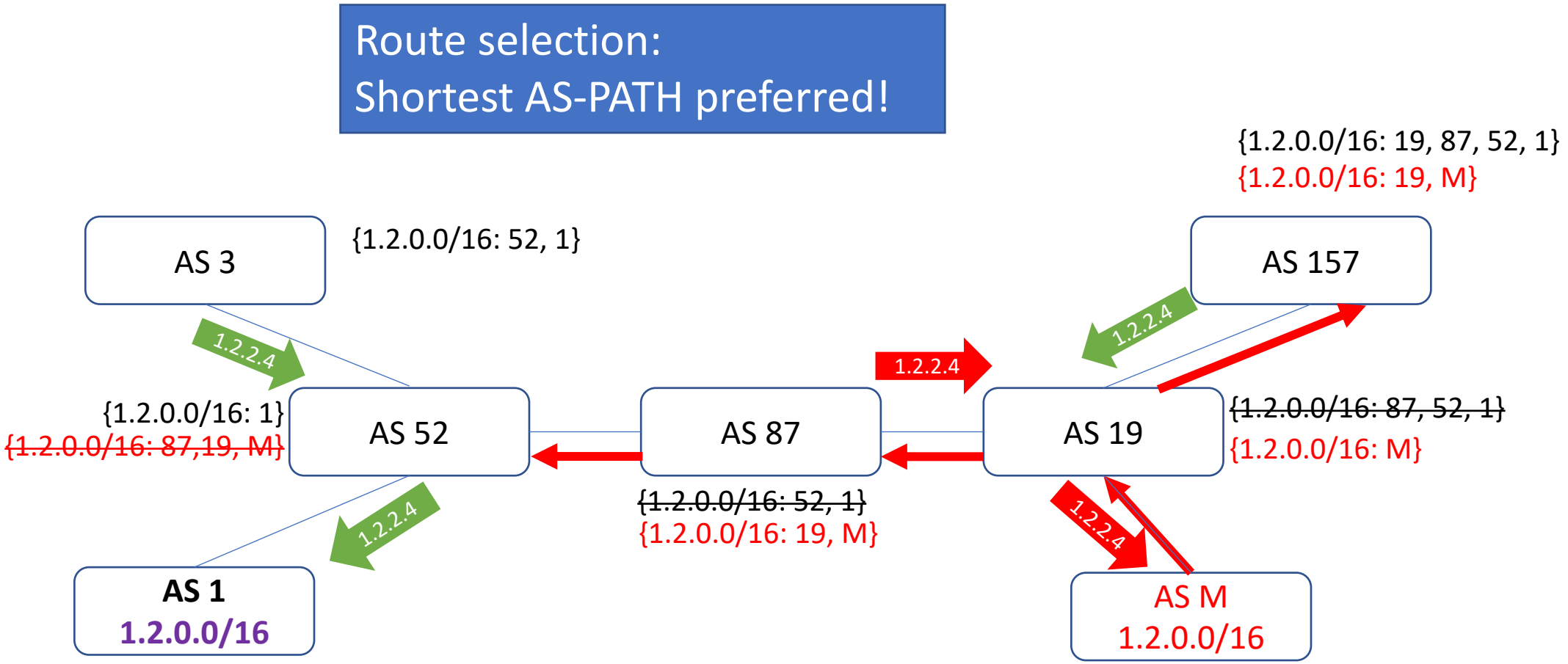
Origin Hijack - Exact Prefix Hijacking



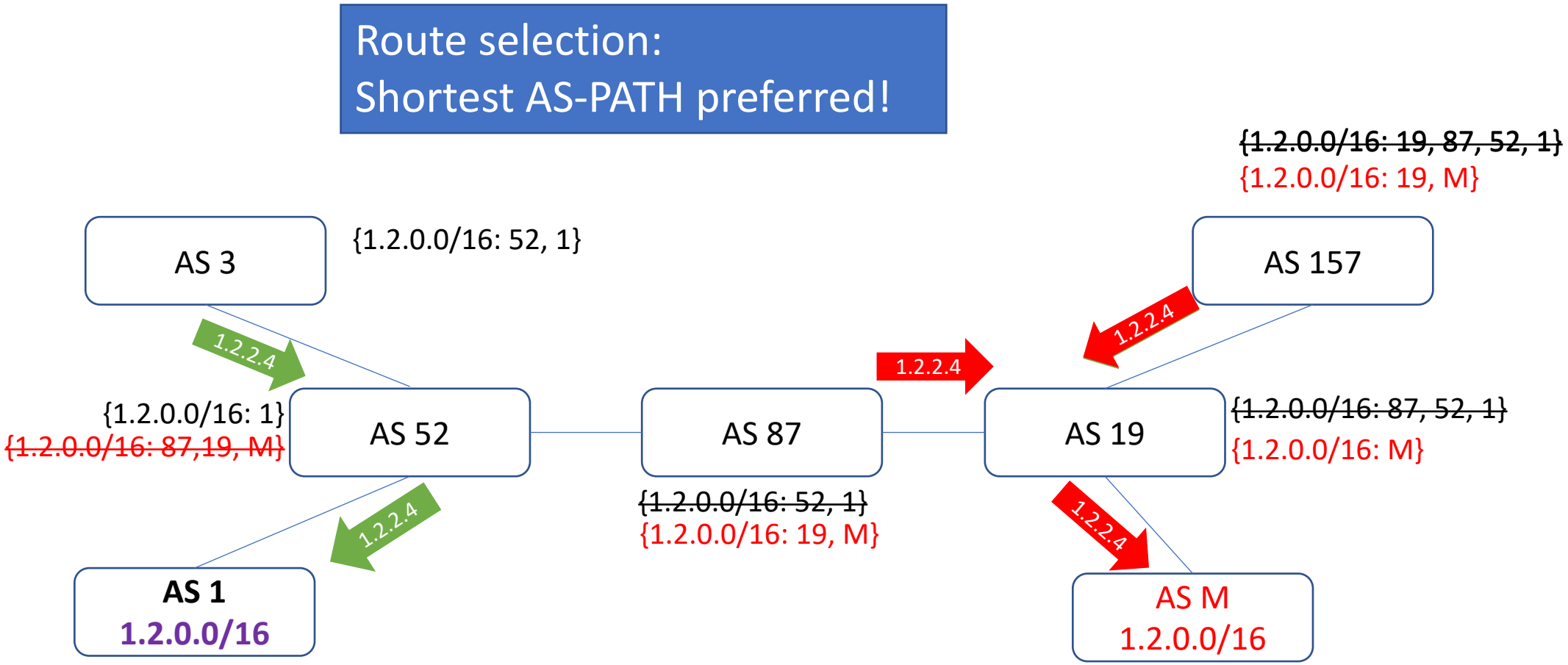
Origin Hijack - Exact Prefix Hijacking



Origin Hijack - Exact Prefix Hijacking



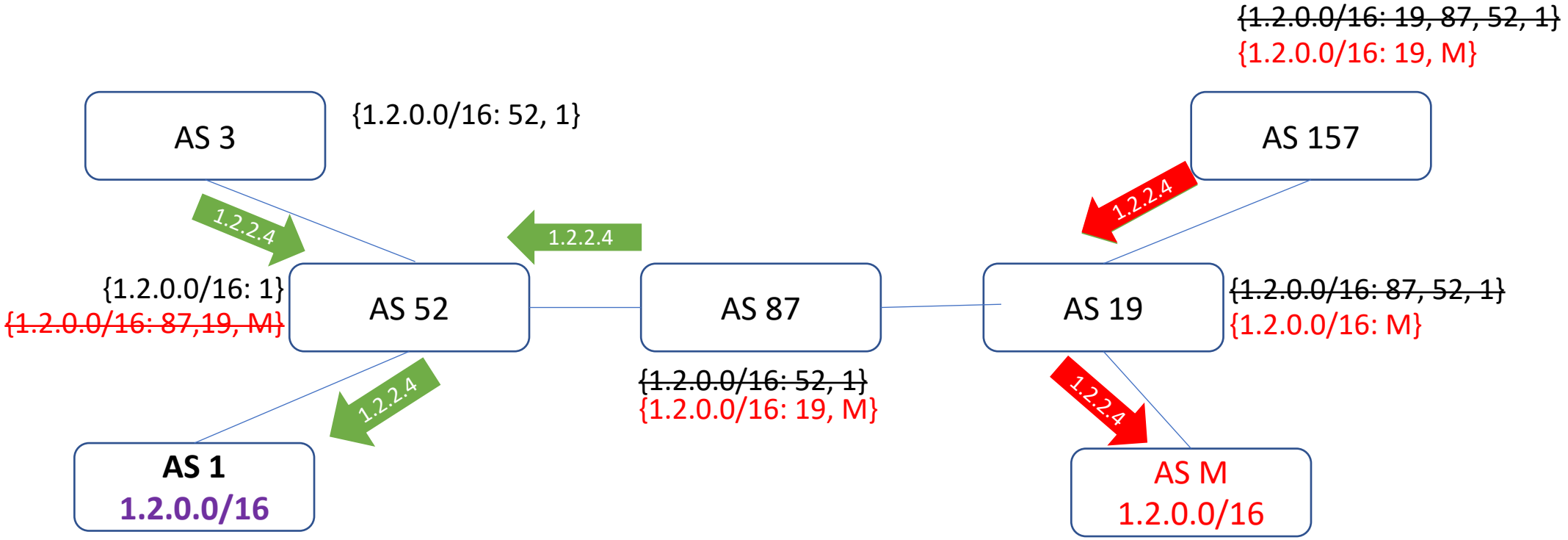
Origin Hijack - Exact Prefix Hijacking



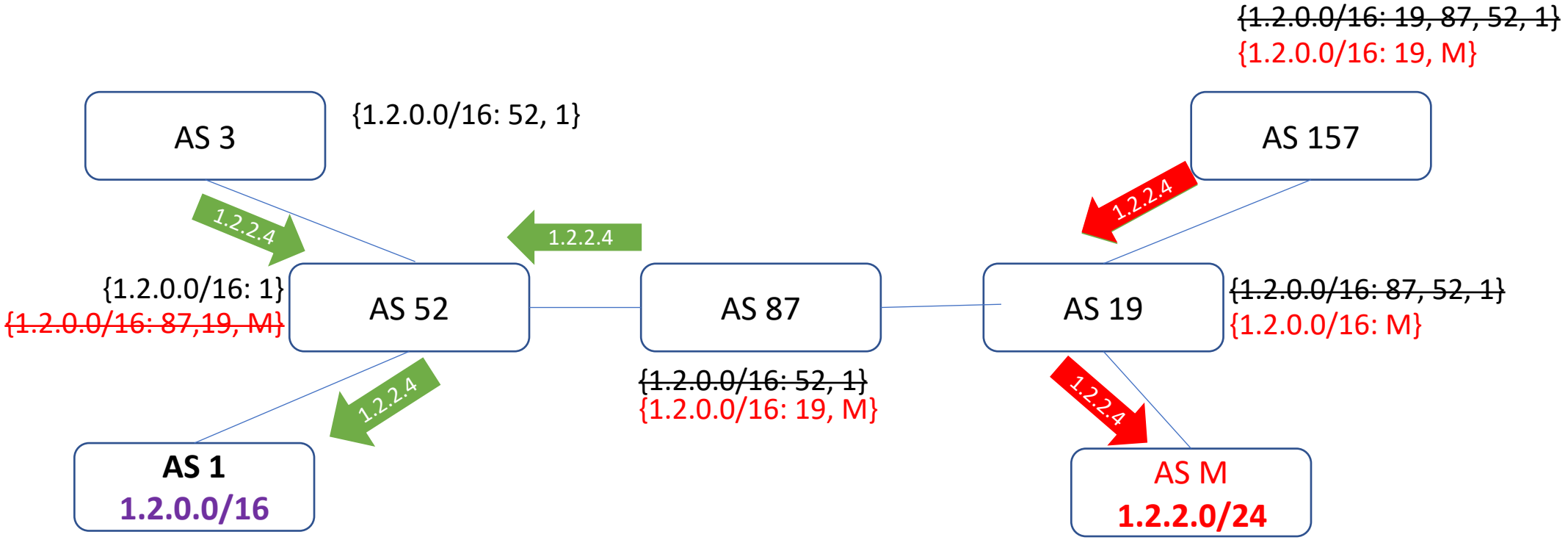
Origin Hijack – Exact Prefix Hijacking

- What malicious activity can it be used for?
- What are the limitations of exact-prefix hijacking?

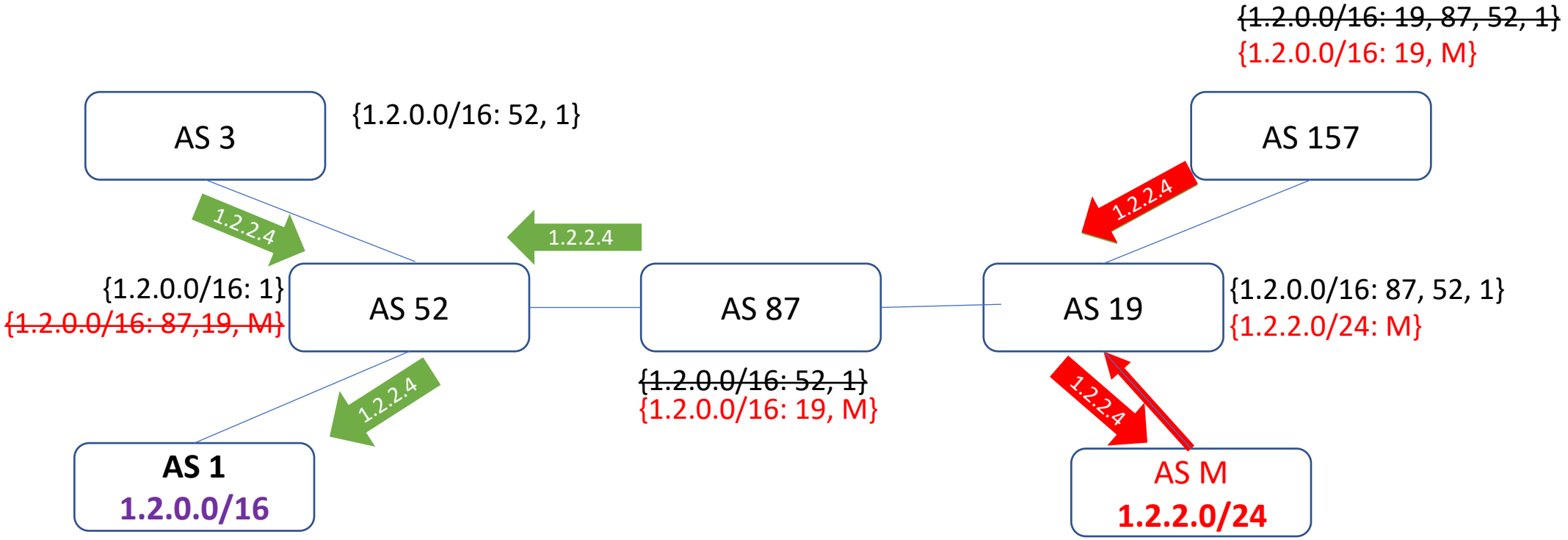
Origin Hijack - Sub-prefix Hijacking



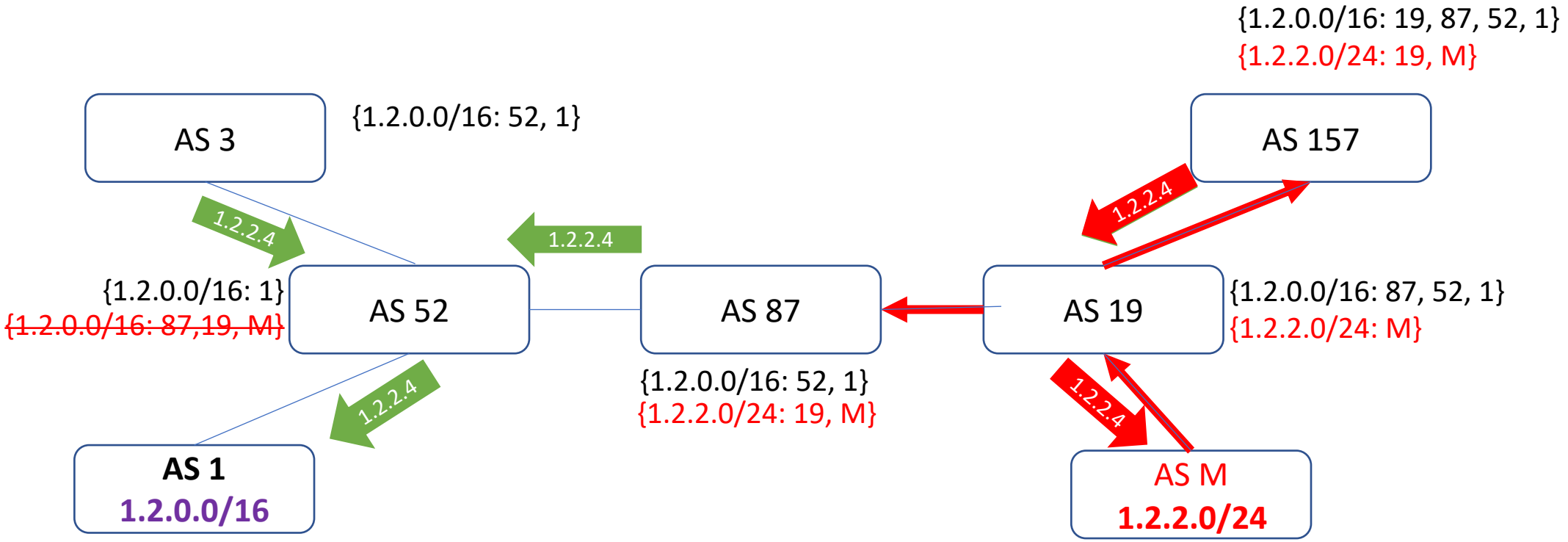
Origin Hijack - Sub-prefix Hijacking



Origin Hijack - Sub-prefix Hijacking

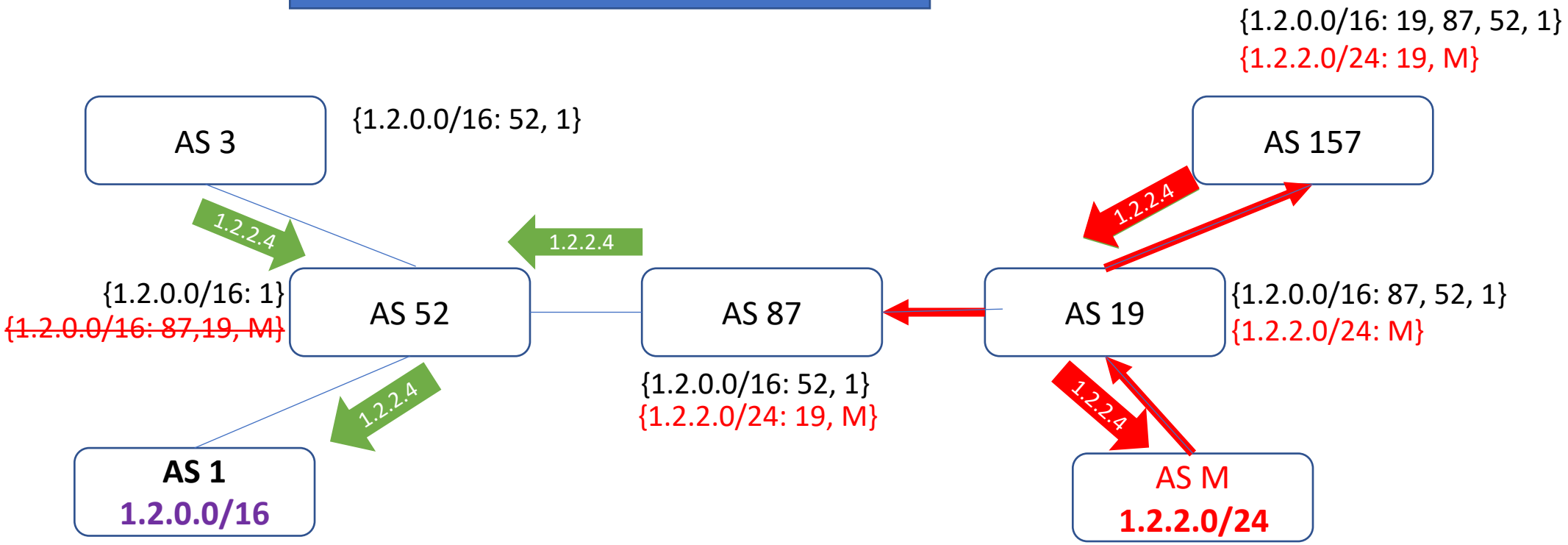


Origin Hijack - Sub-prefix Hijacking



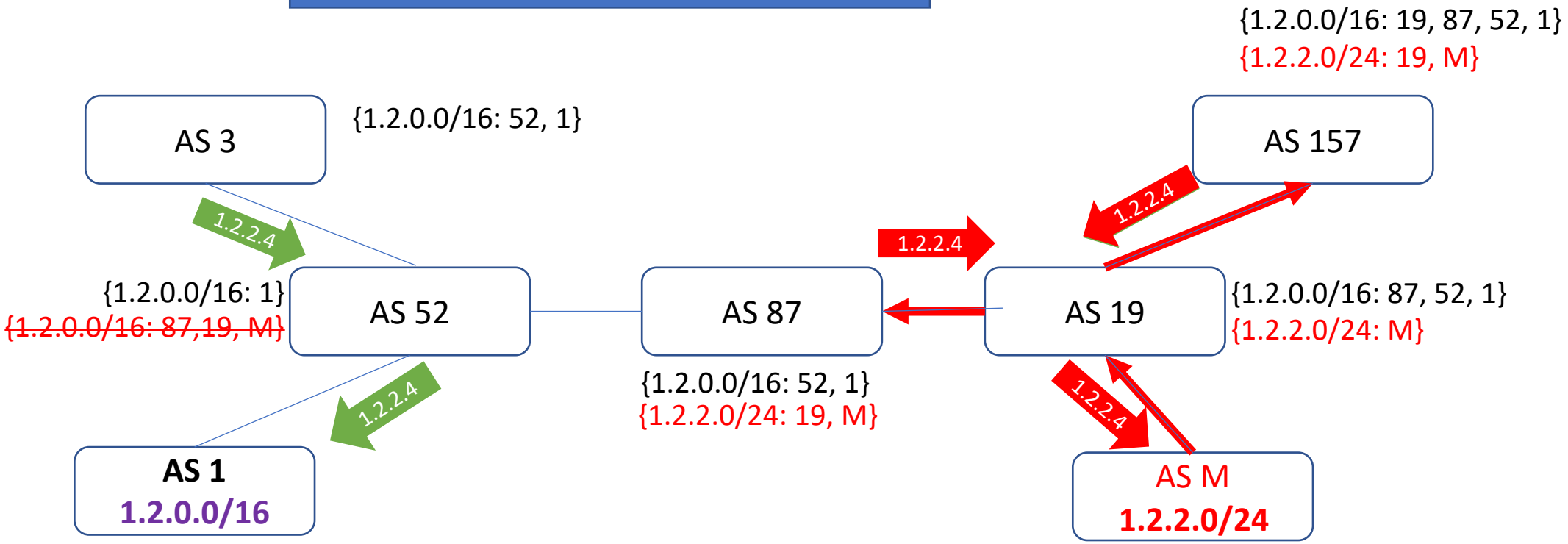
Origin Hijack - Sub-prefix Hijacking

Route selection:
Longest prefix matching!



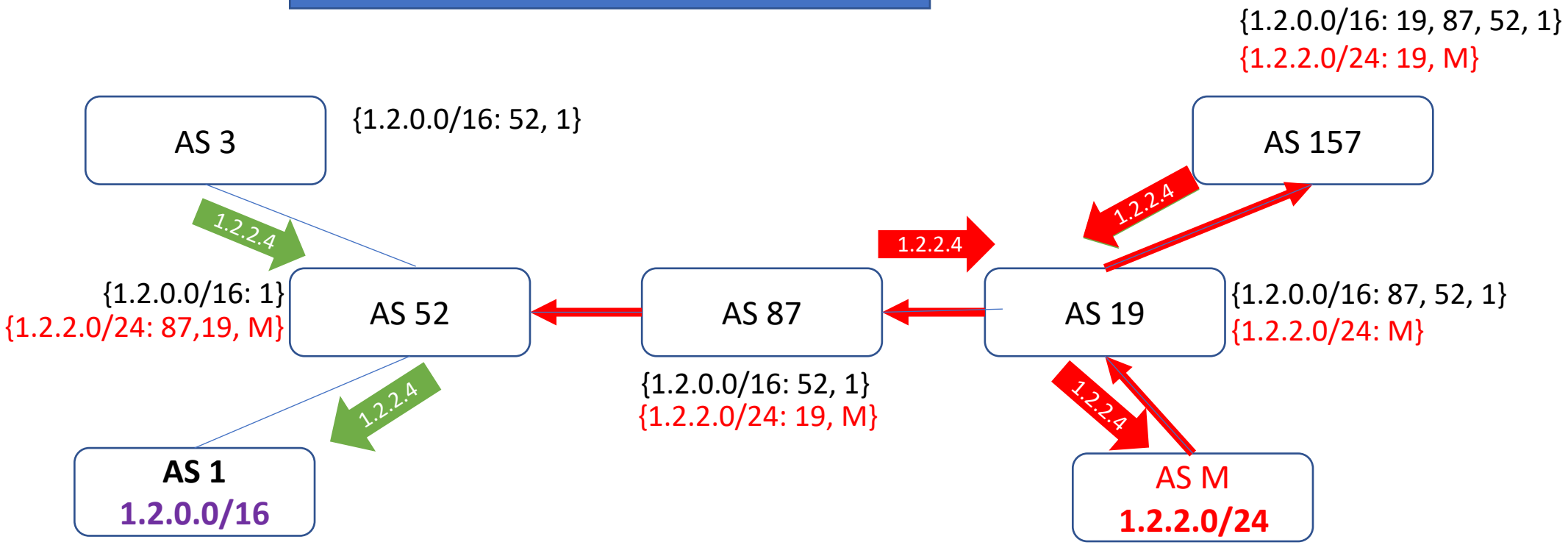
Origin Hijack - Sub-prefix Hijacking

Route selection:
Longest prefix matching!



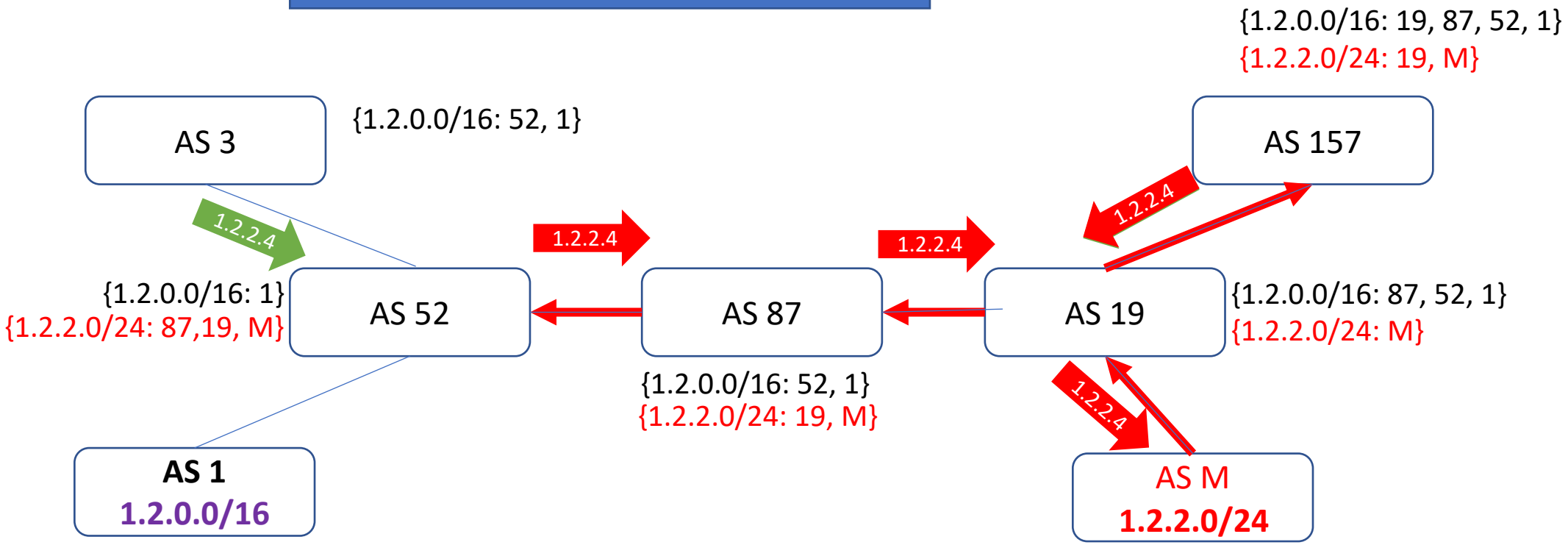
Origin Hijack - Sub-prefix Hijacking

Route selection:
Longest prefix matching!



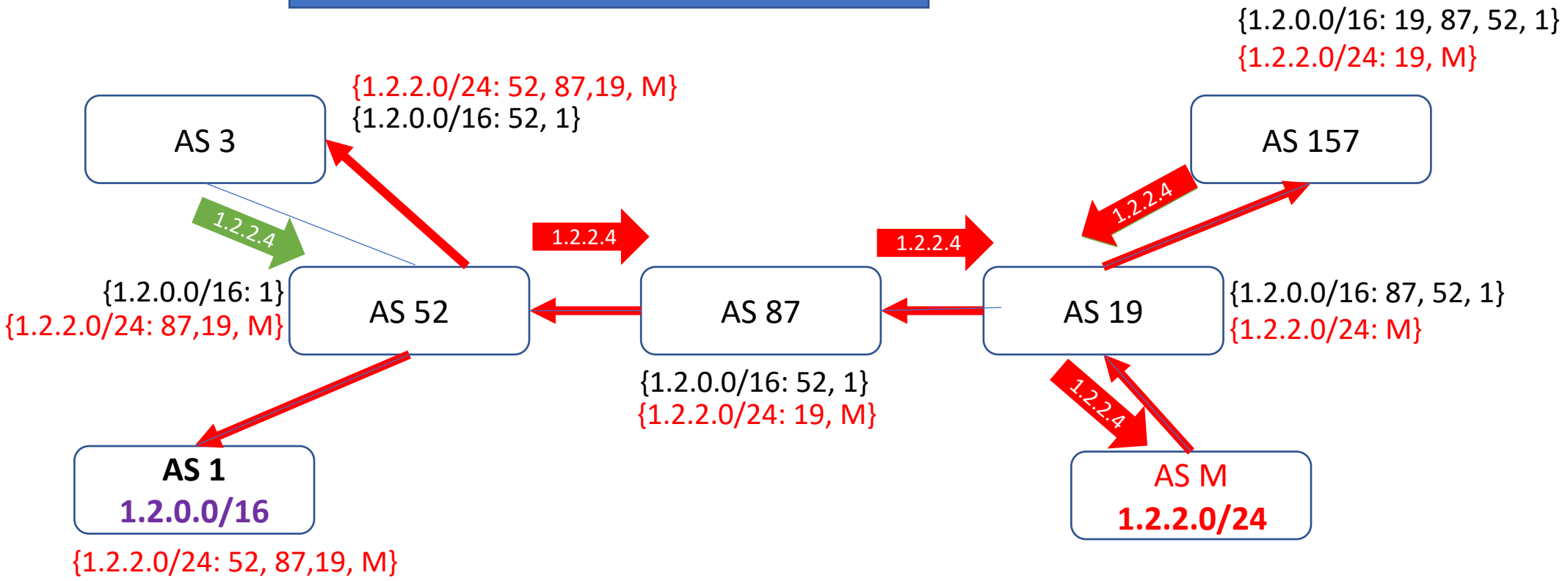
Origin Hijack - Sub-prefix Hijacking

Route selection:
Longest prefix matching!



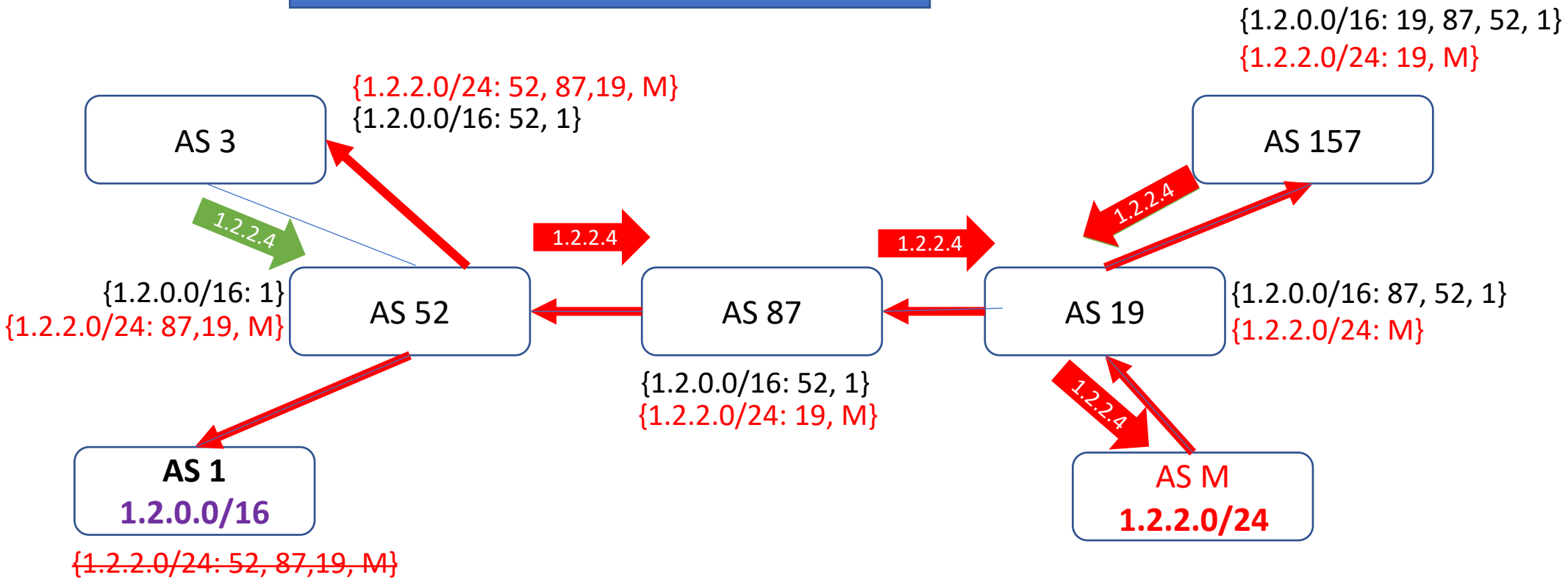
Origin Hijack - Sub-prefix Hijacking

Route selection:
Longest prefix matching!



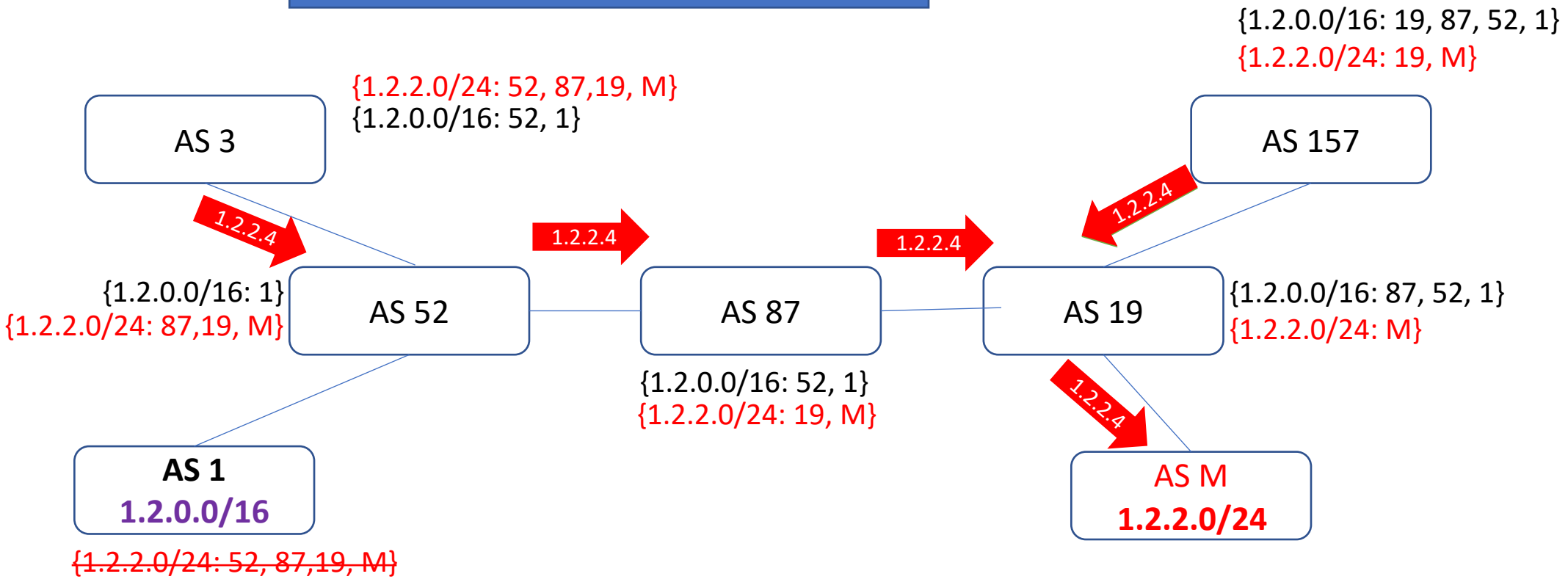
Origin Hijack - Sub-prefix Hijacking

Route selection:
Longest prefix matching!



Origin Hijack - Sub-prefix Hijacking

Route selection:
Longest prefix matching!

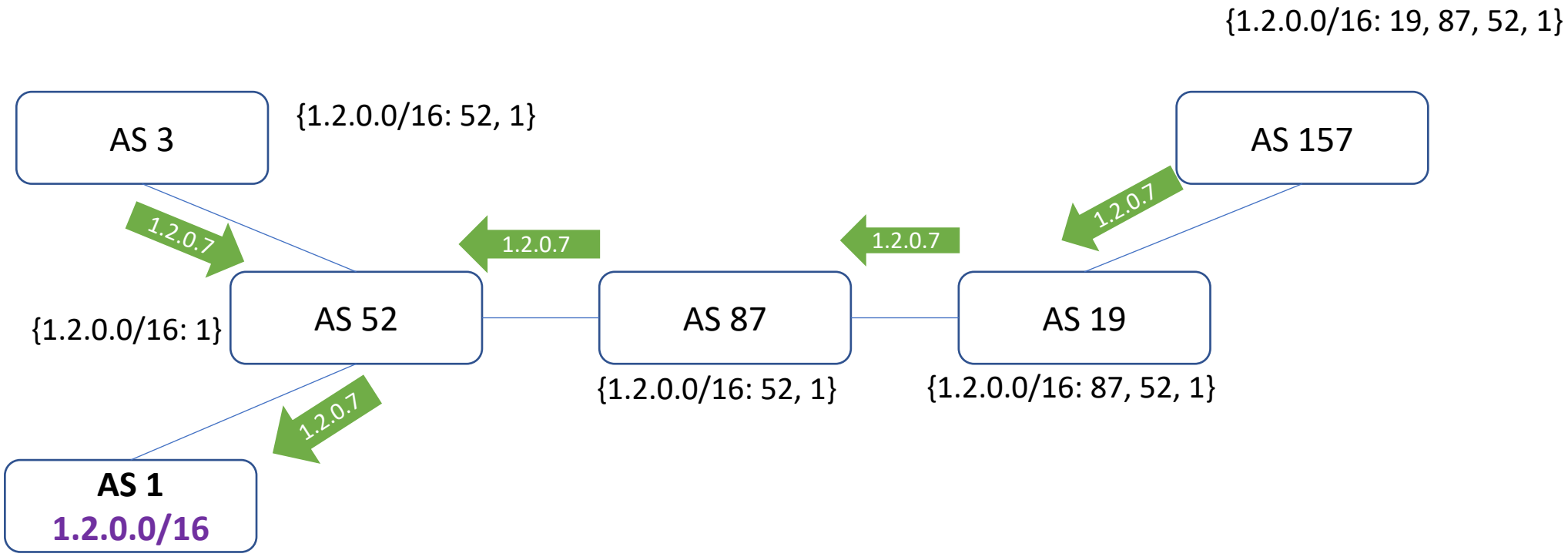


Origin Hijack – Sub-prefix Hijacking

- What can sub-prefix hijacking be used for?
- What are the limitations of sub-prefix hijacking?

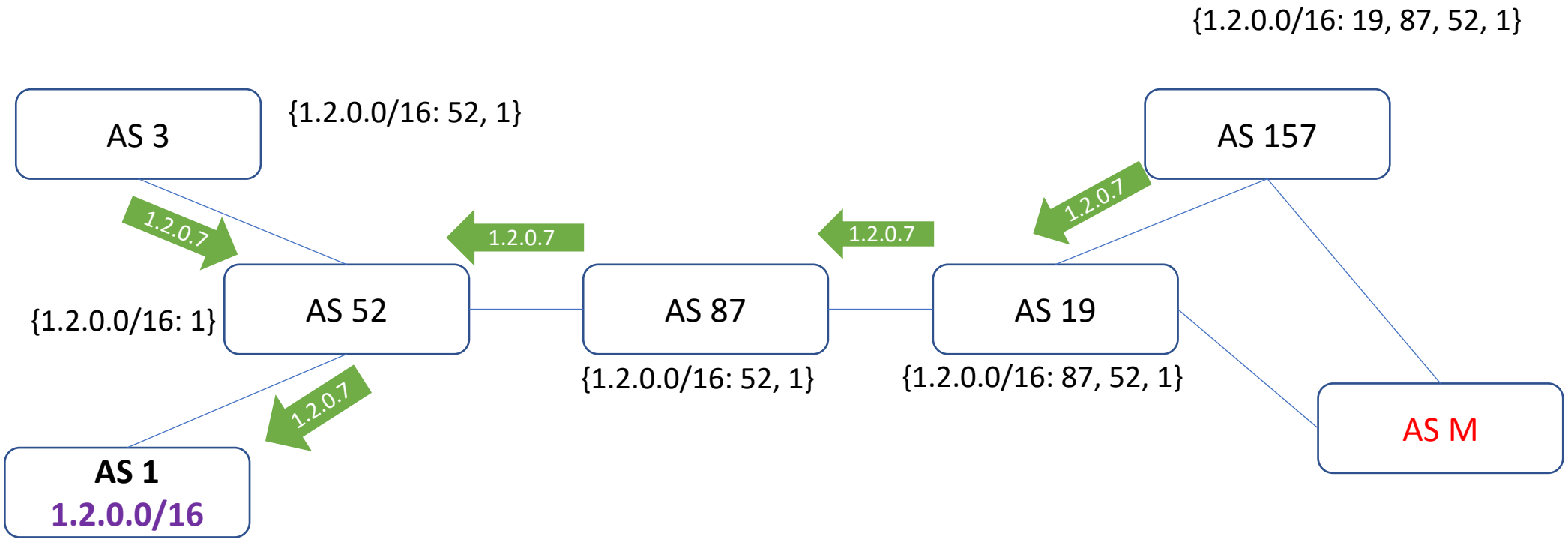
AS-PATH Hijacking (Man in the Middle)

- Attacker changes the one or more hops in AS-PATH



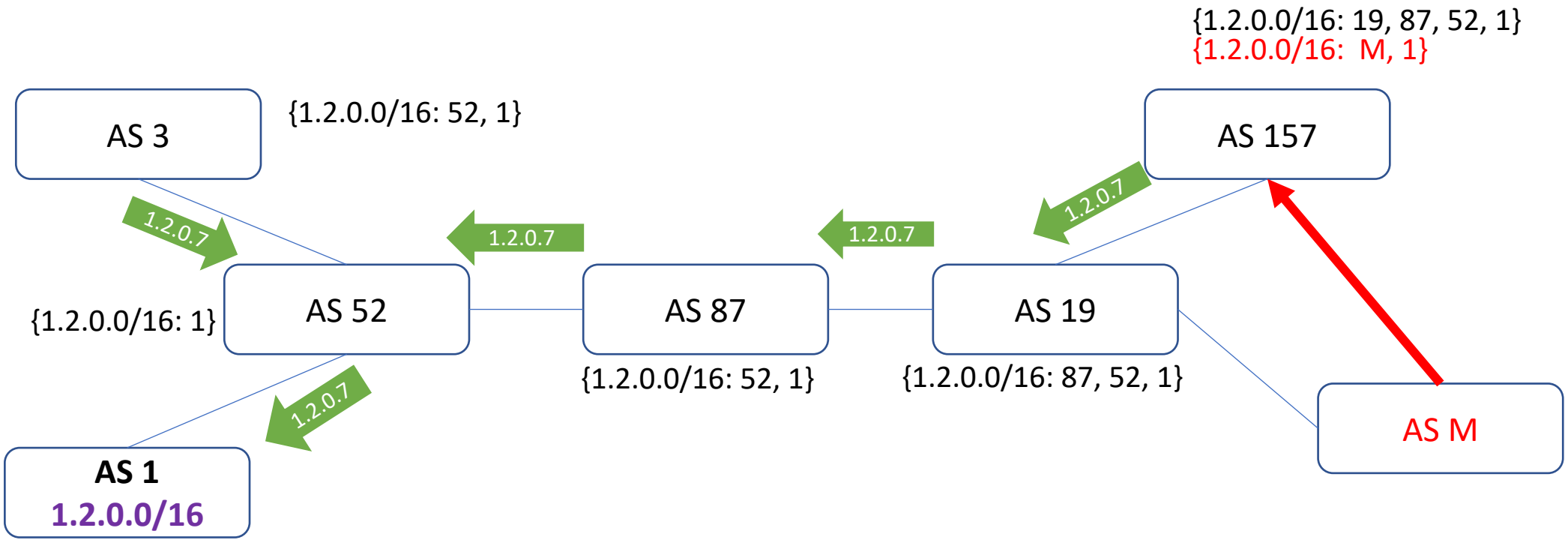
AS-PATH Hijacking (Man in the Middle)

- Attacker changes the one or more hops in AS-PATH



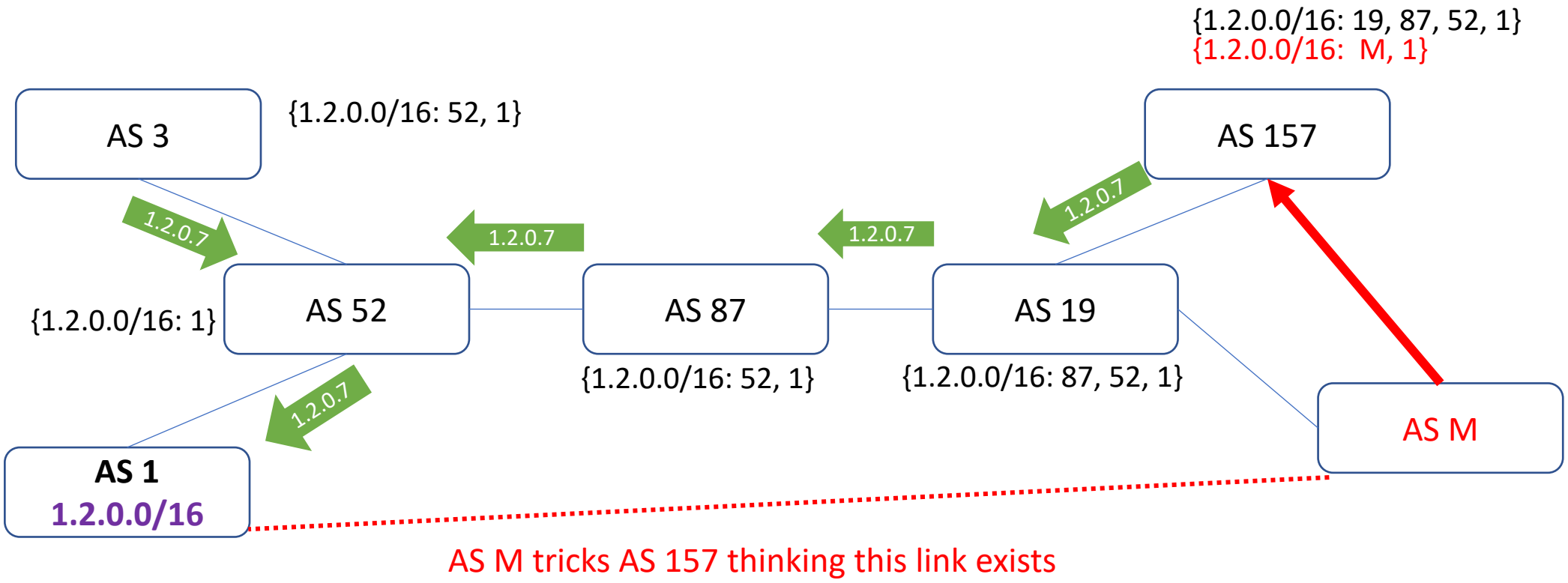
AS-PATH Hijacking (Man in the Middle)

- Attacker changes the one or more hops in AS-PATH



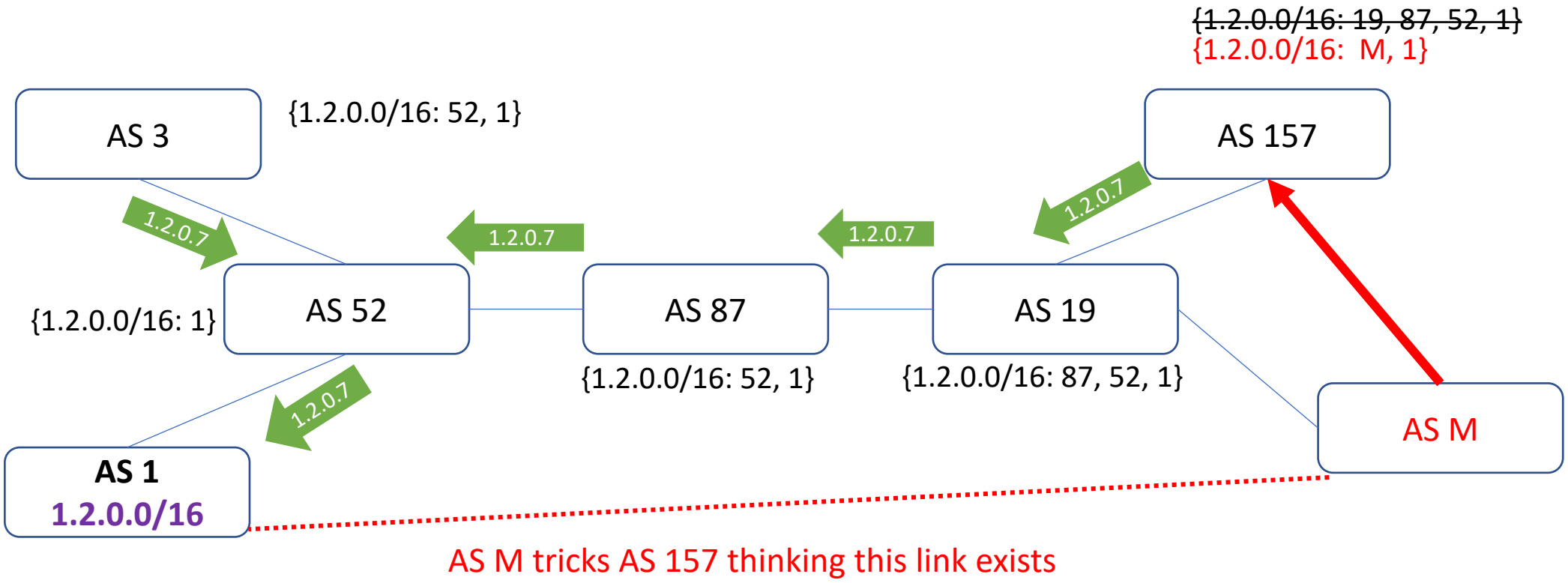
AS-PATH Hijacking (Man in the Middle)

- Attacker changes the one or more hops in AS-PATH



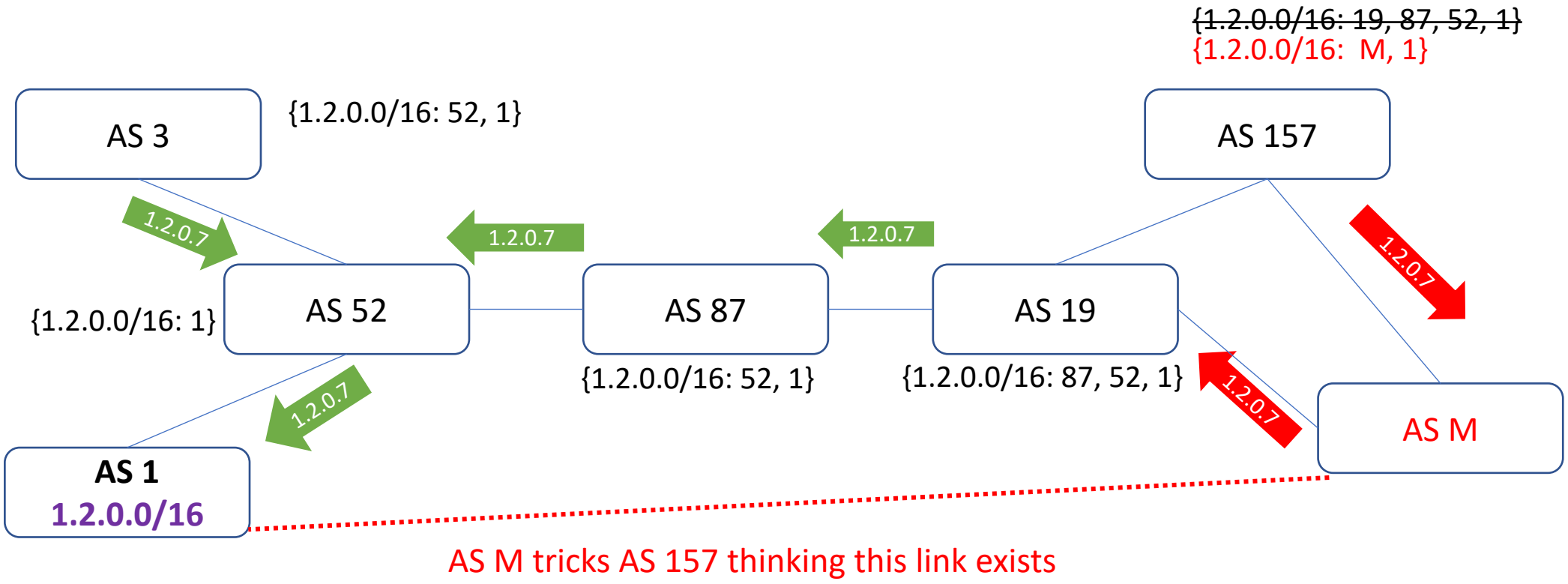
AS-PATH Hijacking (Man in the Middle)

- Attacker changes the one or more hops in AS-PATH



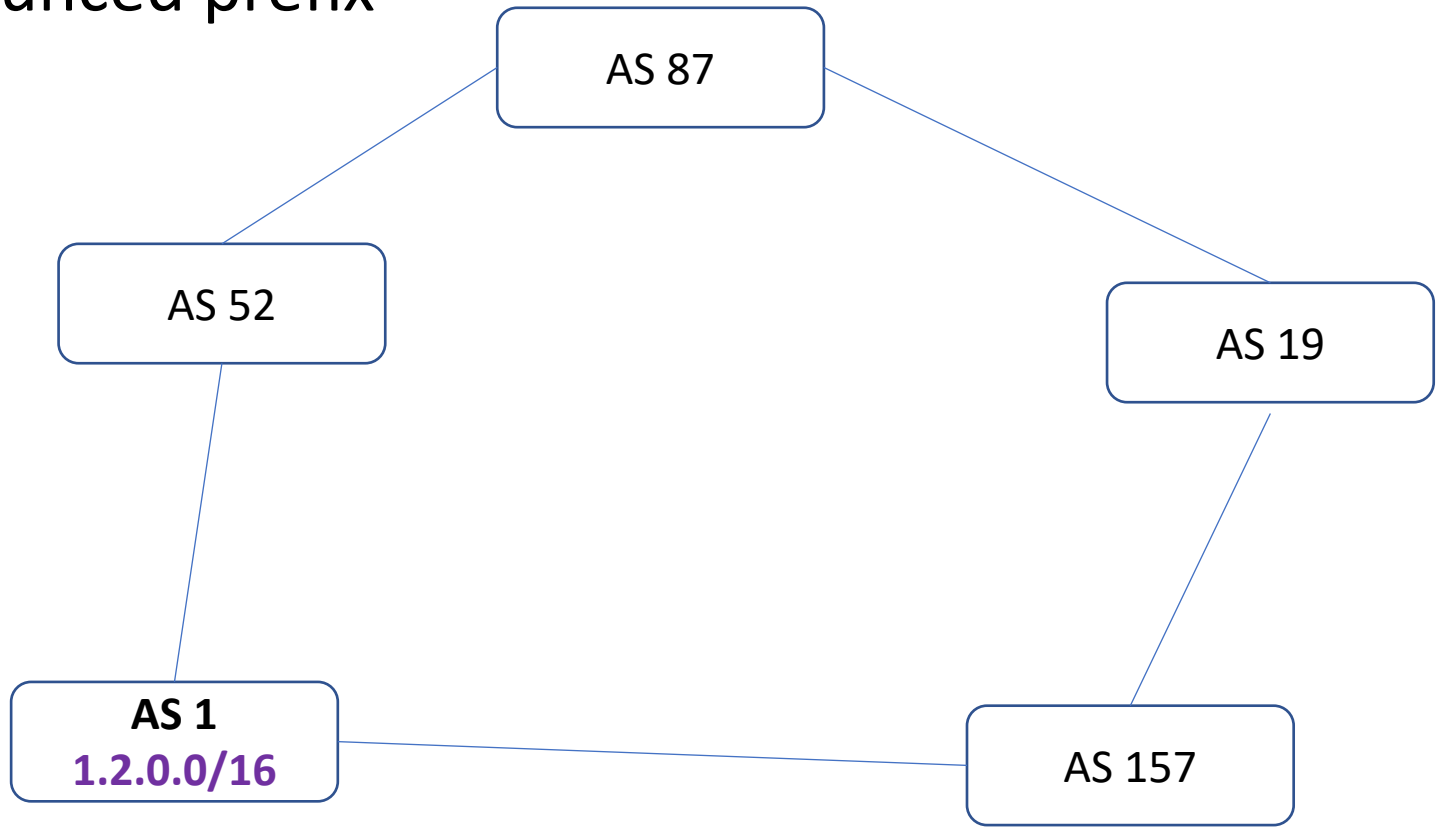
AS-PATH Hijacking (Man in the Middle)

- Attacker changes the one or more hops in AS-PATH



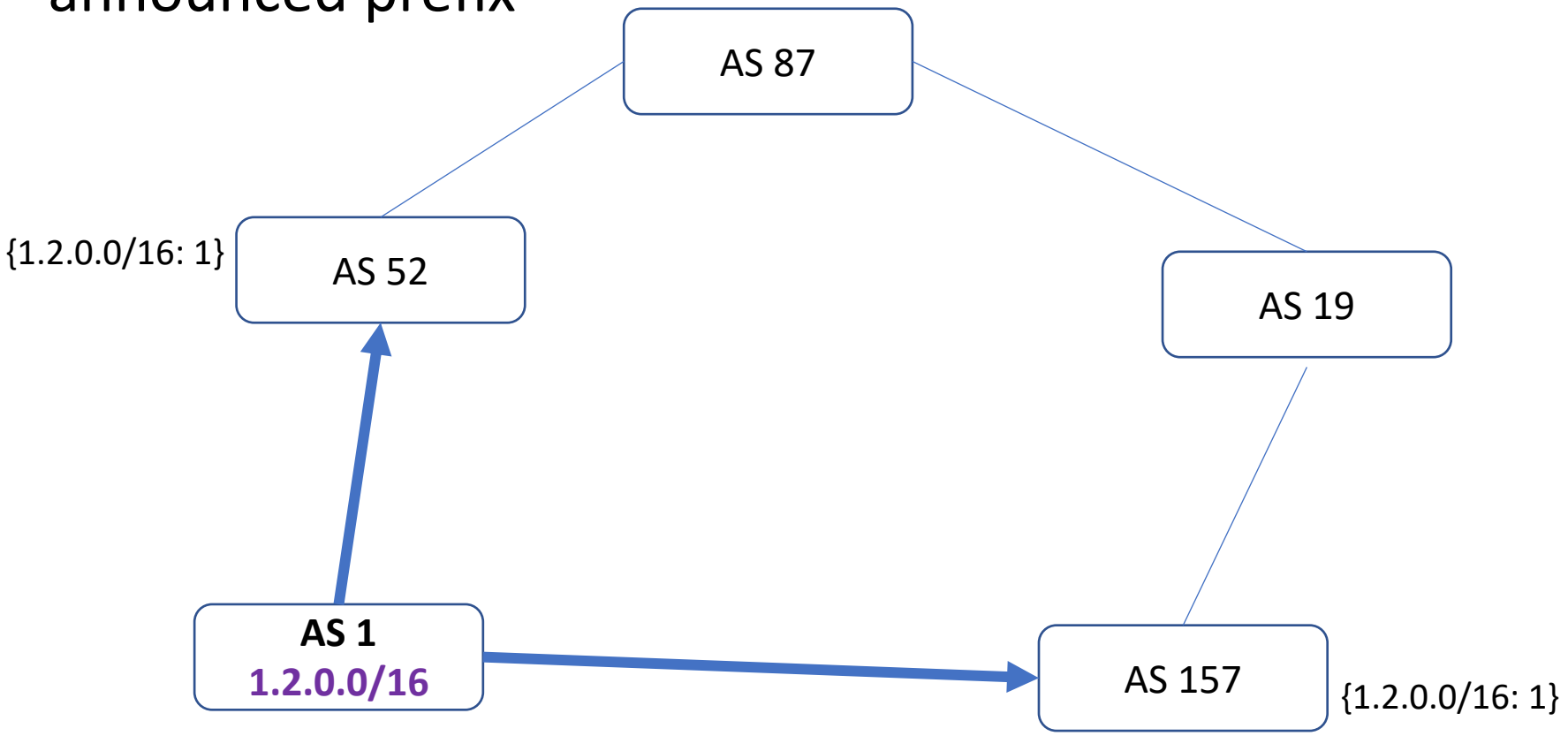
Prefix Alteration

- Attacker has to be on some legitimate path, and only changes the announced prefix



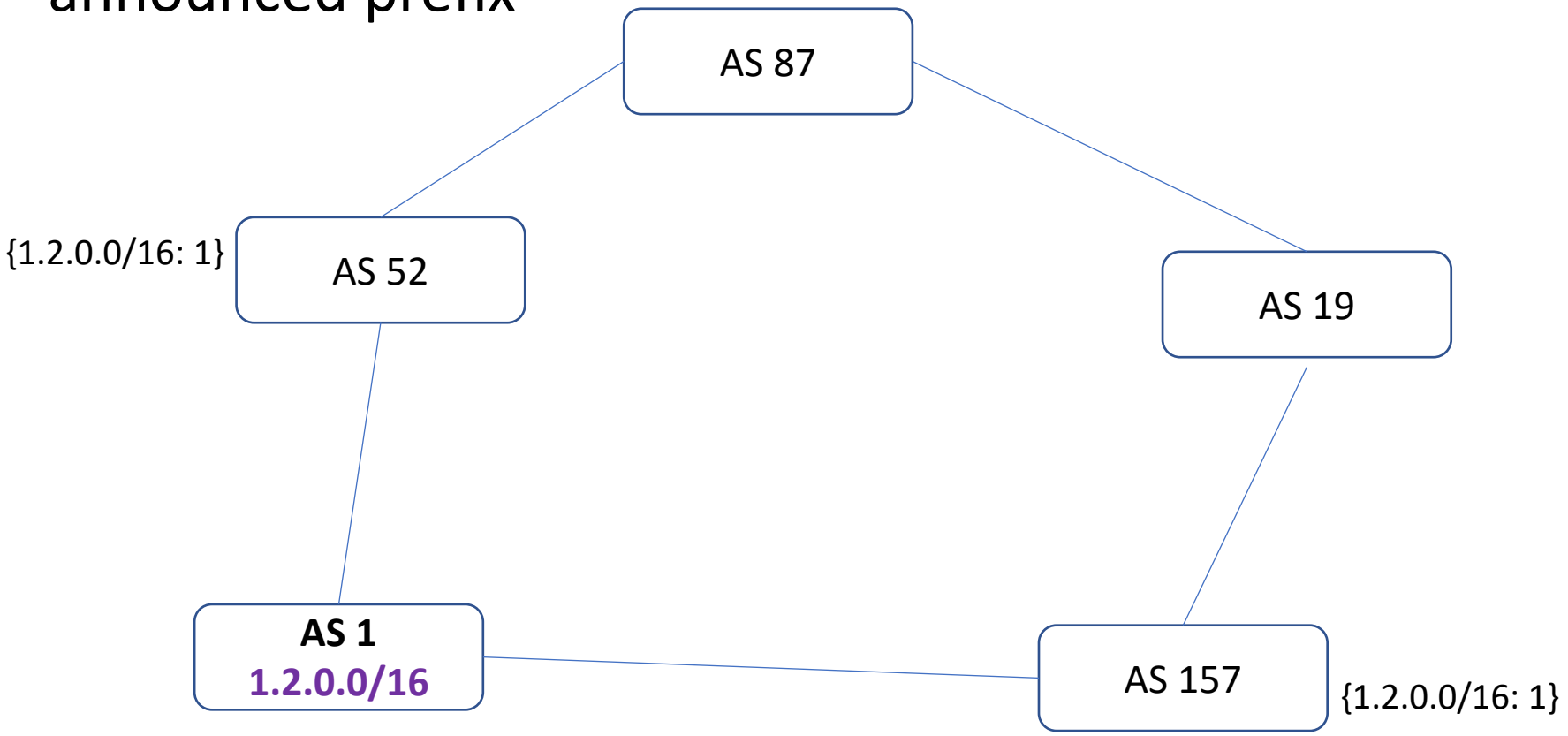
Prefix Alteration

- Attacker has to be on some legitimate path, and only changes the announced prefix



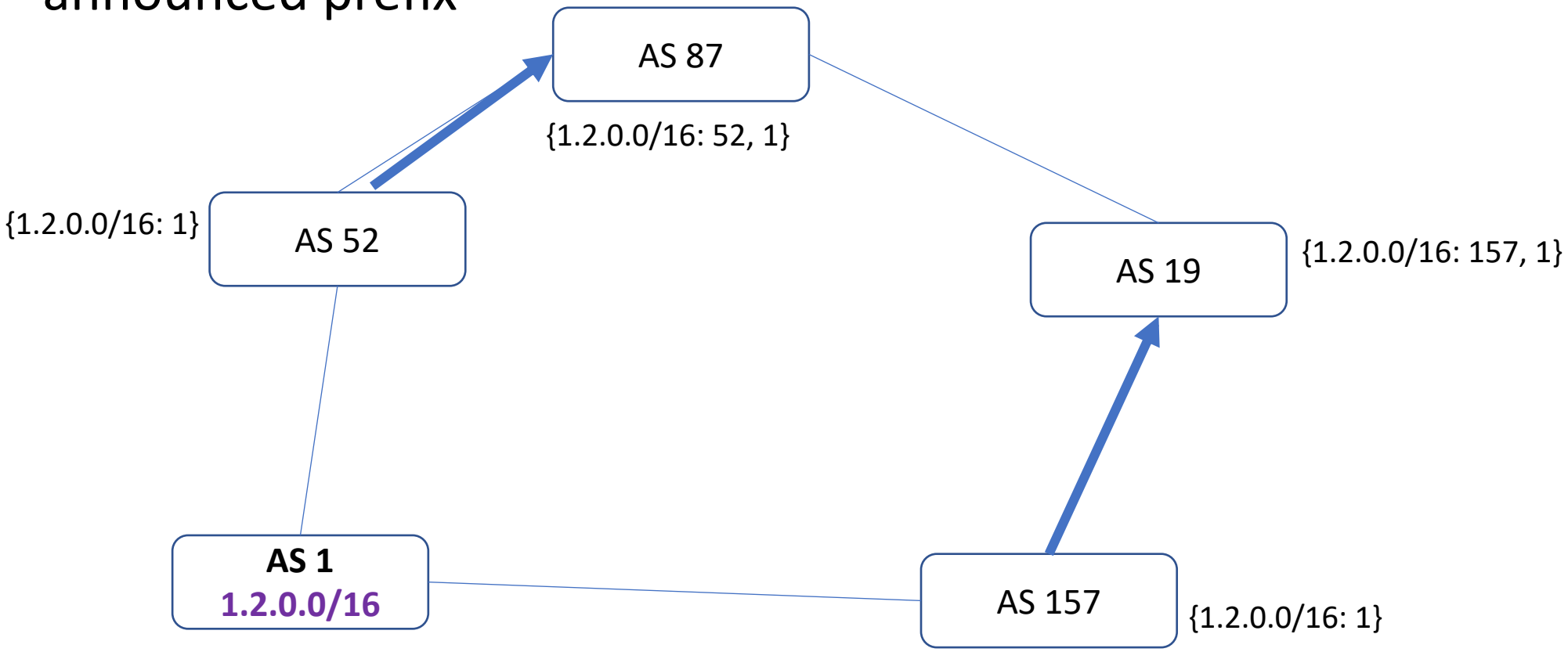
Prefix Alteration

- Attacker has to be on some legitimate path, and only changes the announced prefix



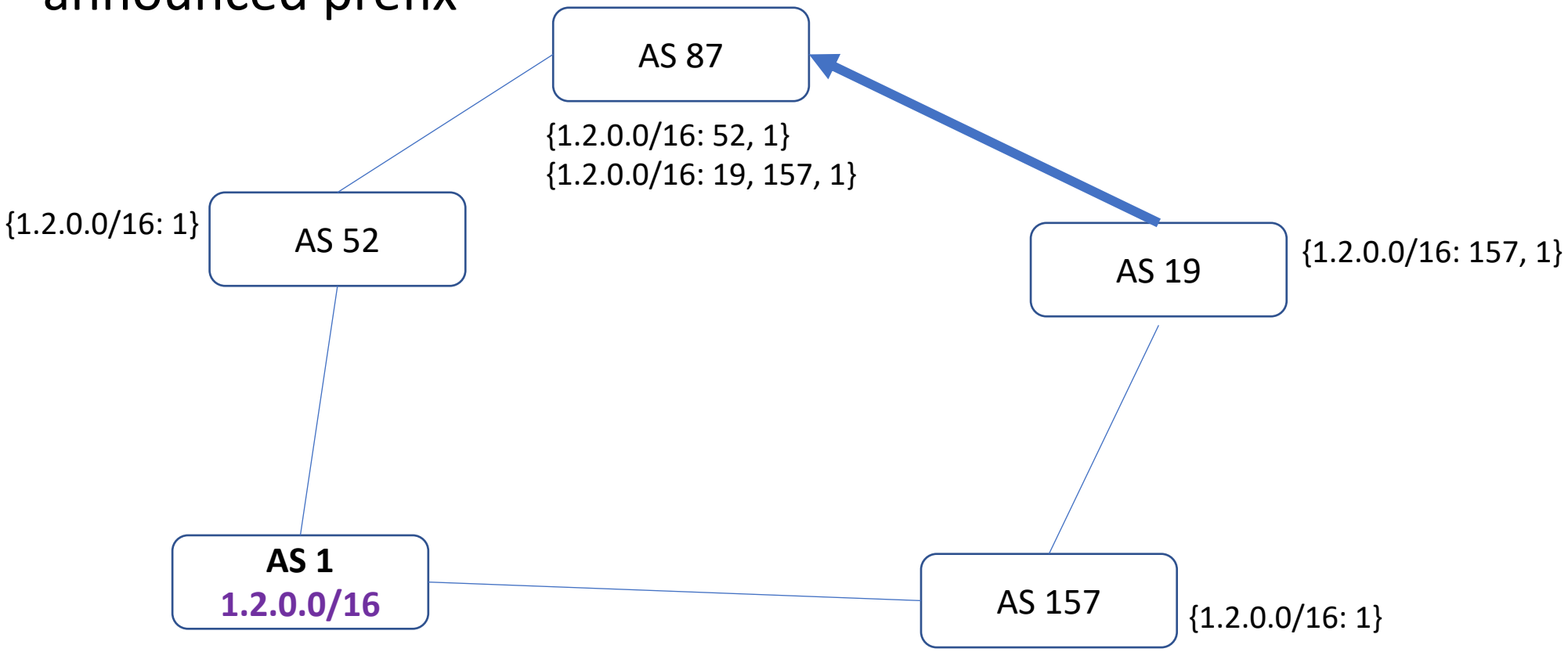
Prefix Alteration

- Attacker has to be on some legitimate path, and only changes the announced prefix



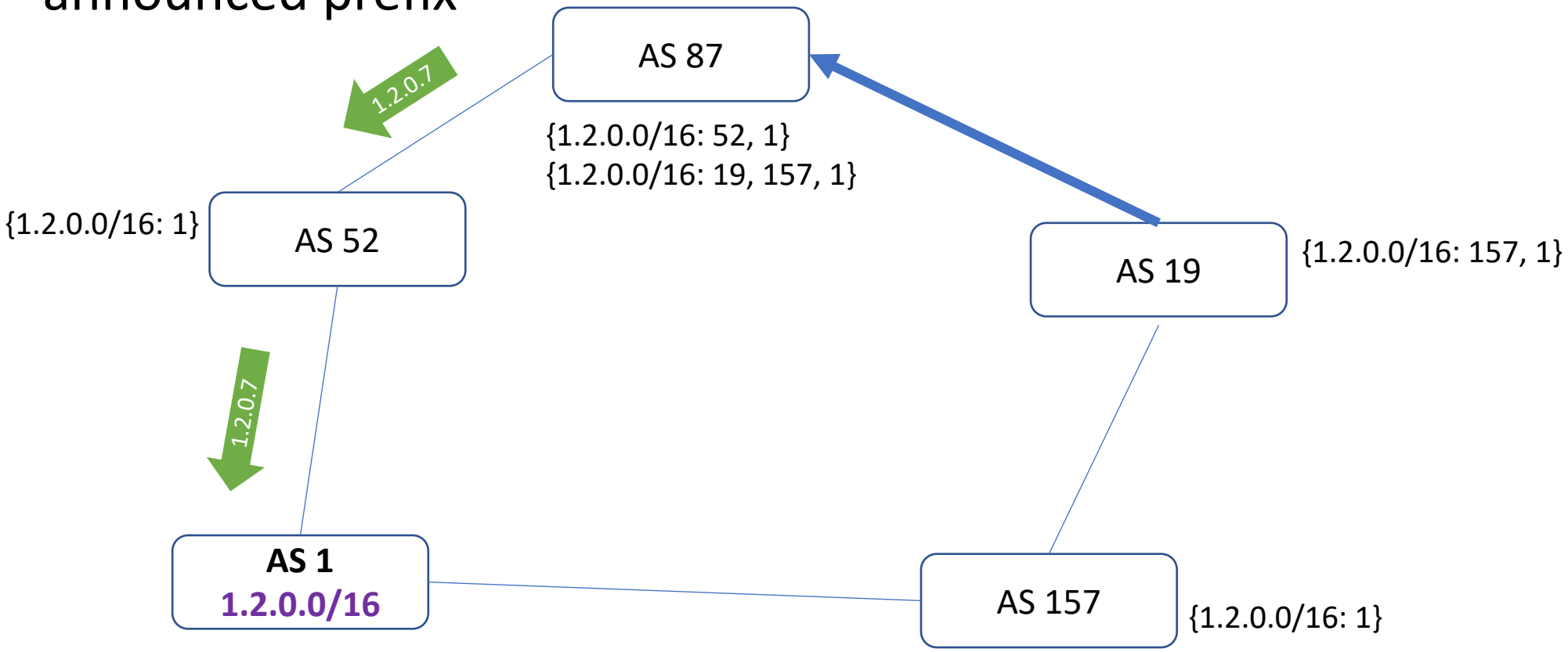
Prefix Alteration

- Attacker has to be on some legitimate path, and only changes the announced prefix



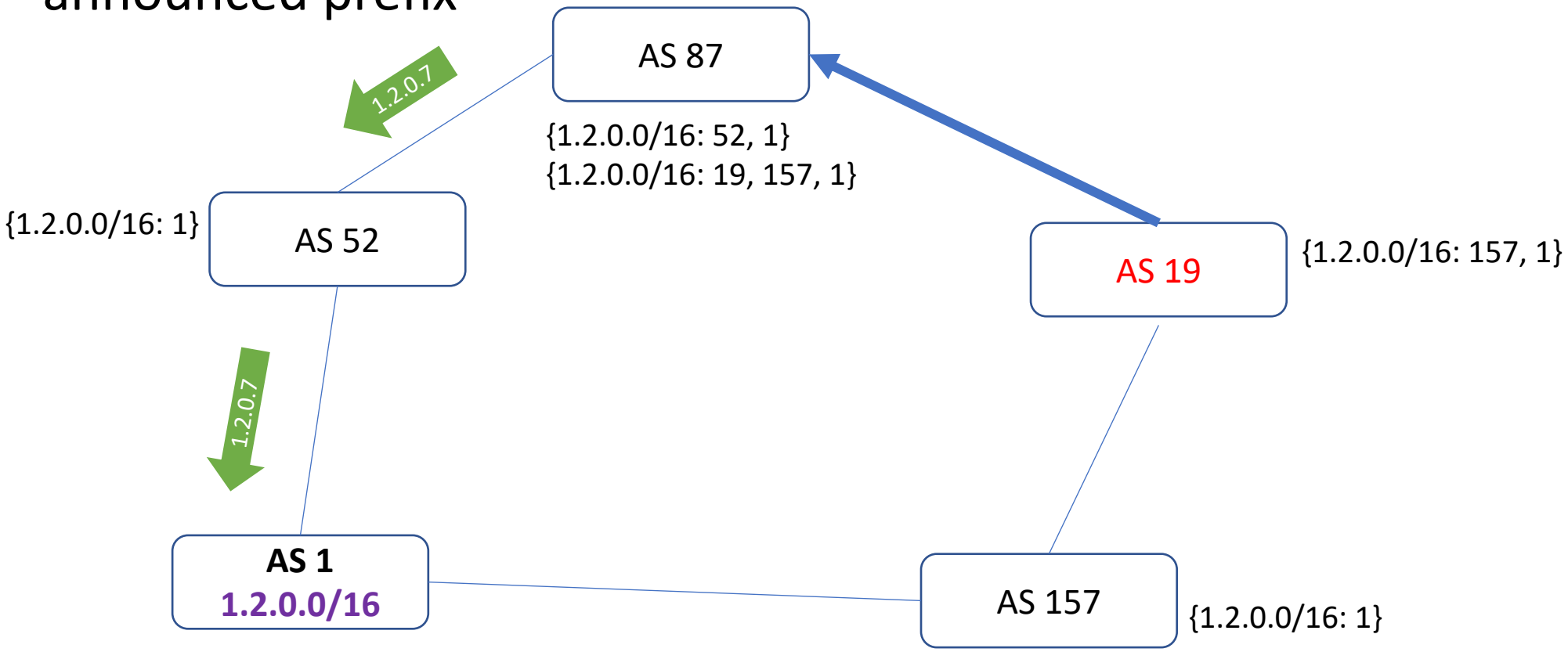
Prefix Alteration

- Attacker has to be on some legitimate path, and only changes the announced prefix



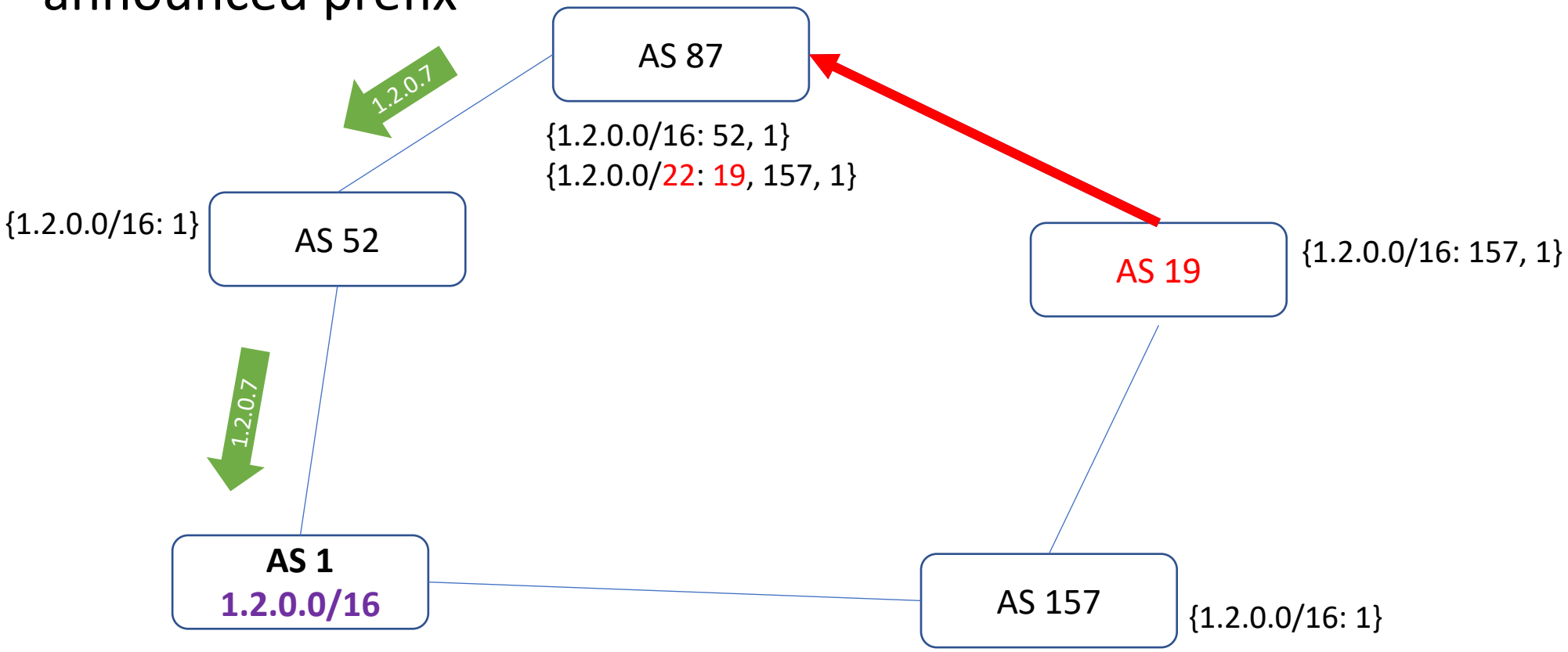
Prefix Alteration

- Attacker has to be on some legitimate path, and only changes the announced prefix



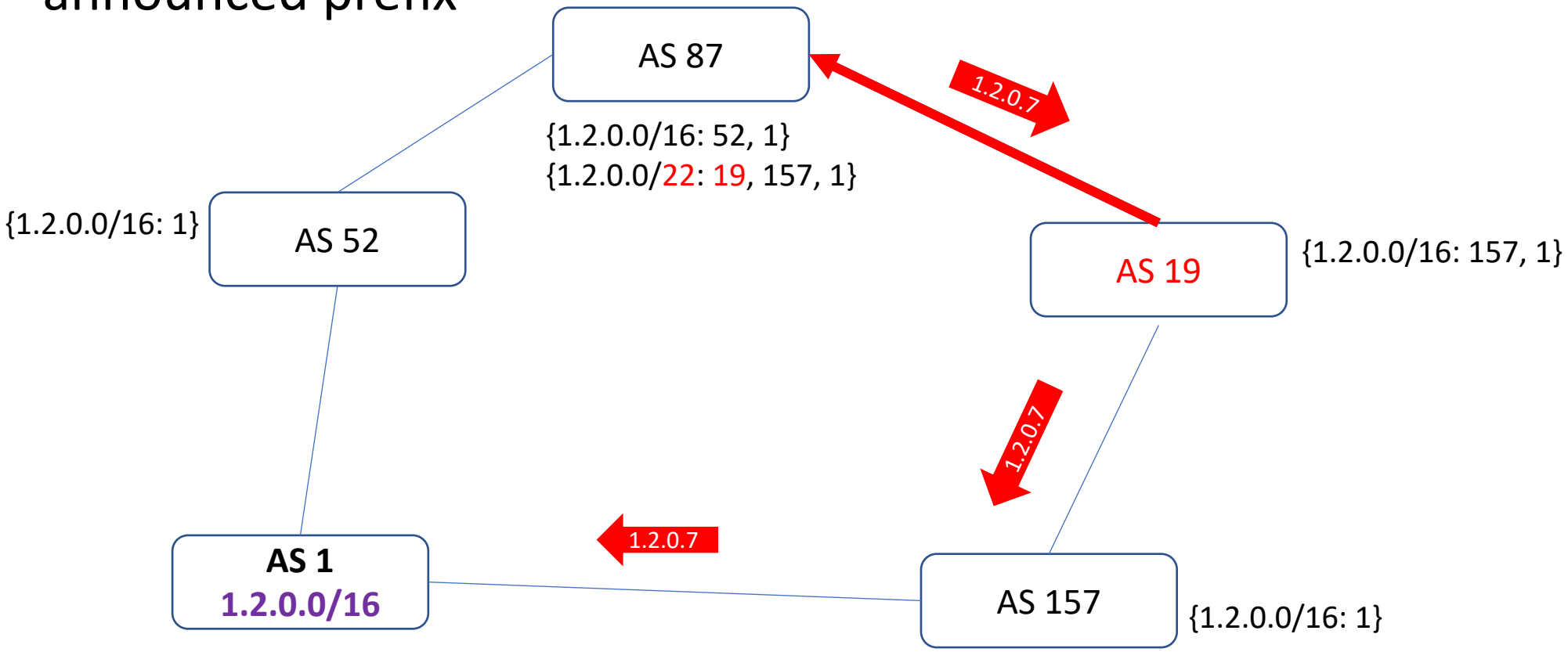
Prefix Alteration

- Attacker has to be on some legitimate path, and only changes the announced prefix



Prefix Alteration

- Attacker has to be on some legitimate path, and only changes the announced prefix



Acknowledgements

- This material is based on research sponsored by the National Science Foundation (NSF) grant OAC-2131987. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of NSF.