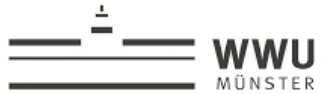
Assessing the security of Internet paths
A case study of Dutch critical infrastructures

Shyam Krishna Khadka[1], Suzan Bayhan[1], Ralph Holz[1,2], Cristian Hesselman[1,3]
[1]University of Twente, [2]University of Münster, [3]SIDN Labs



Dominance of cloud-based services

NOS News • Friday 1 March, 06:00

U.S. government can access e-mail from Dutch governments and critical companies

Joost Schellevis
Editor Tech

Dutch governments, so-called "vital" companies, schools and, to a lesser extent, healthcare institutions outsource their mail services to American companies on a large scale. This is evident from research by the NOS into the cloud use of more than 20,000 companies, organizations and governments.

Source: https://nos.nl/artikel/2510923-amerikaanse-overheid-kan-bij-e-mail-van-nederlandse-overheden-en-kritieke-bedrijven

Dominance of cloud-based services

NOS News • Friday 1 March, 06:00

U.S. government can access e-mail from Dutch governments and critical companies

Joost Schellevis
Editor Tech

Dutch governments, so-called "vital" companies, schools and, to a lesser extent, healthcare institutions outsource their mail services to American companies on a large scale. This is evident from research by the NOS into the cloud use of more than 20,000 companies, organizations and governments.

Source: https://nos.nl/artikel/2510923-amerikaanse-overheid-kan-bij-e-mail-van-nederlandse-overheden-en-kritieke-bedrijven

"...63 percent of the approximately 3800 largest companies of which the NOS was able to find a website use cloud services from Microsoft or Google...."

Dominance of cloud-based services

NOS News • Friday 1 March, 06:00

U.S. government can access e-mail from Dutch governments and critical companies

Joost Schellevis
Editor Tech

Dutch governments, so-called "vital" companies, schools and, to a lesser extent, healthcare institutions outsource their mail services to American companies on a large scale. This is evident from research by the NOS into the cloud use of more than 20,000 companies, organizations and governments.

"...63 percent of the approximately 3800 largest companies of which the NOS was able to find a website use cloud services from Microsoft or Google...."

Source: https://nos.nl/artikel/2510923-amerikaanse-overheid-kan-bij-e-mail-van-nederlandse-overheden-en-kritieke-bedrijven

Many companies and critical infrastructures such as ASML, KPN (a big telecom operator in the Netherlands), and Schiphol Airport (the main international airport of the Netherlands) rely on cloud services (such as email) for their daily operations.

Problem

Problem

- Critical Infrastructures(CIs) are physical and information technology facilities, networks, services, and assets
- Disruption of CIs impacts the health, safety, and security or economic well-being of citizens
- CIs traffic needs to traverse multiple autonomous systems to reach their cloud providers
- Limited insight into the security status of the paths
  - Limited visibility about the paths
  - No mechanism exists to measure the security of the whole path

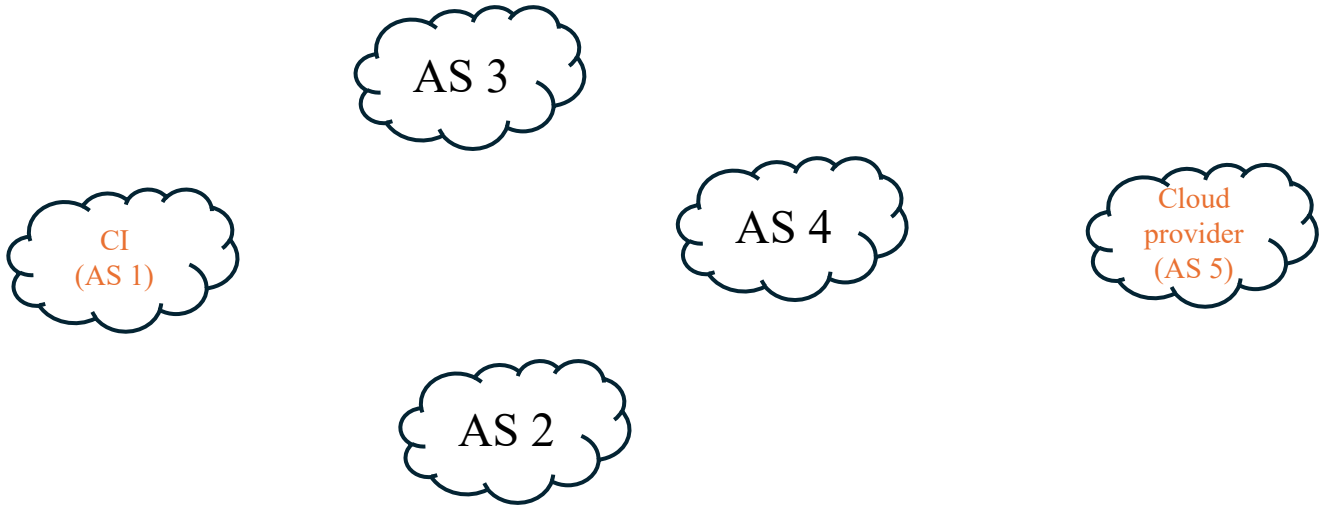
Problem

- Critical Infrastructures(CIs) are physical and information technology facilities, networks, services, and assets
- Disruption of CIs impacts the health, safety, and security or economic well-being of citizens
- CIs traffic needs to traverse multiple autonomous systems to reach their cloud providers
- Limited insight into the security status of the paths
  - Limited visibility about the paths
  - No mechanism exists to measure the security of the whole path

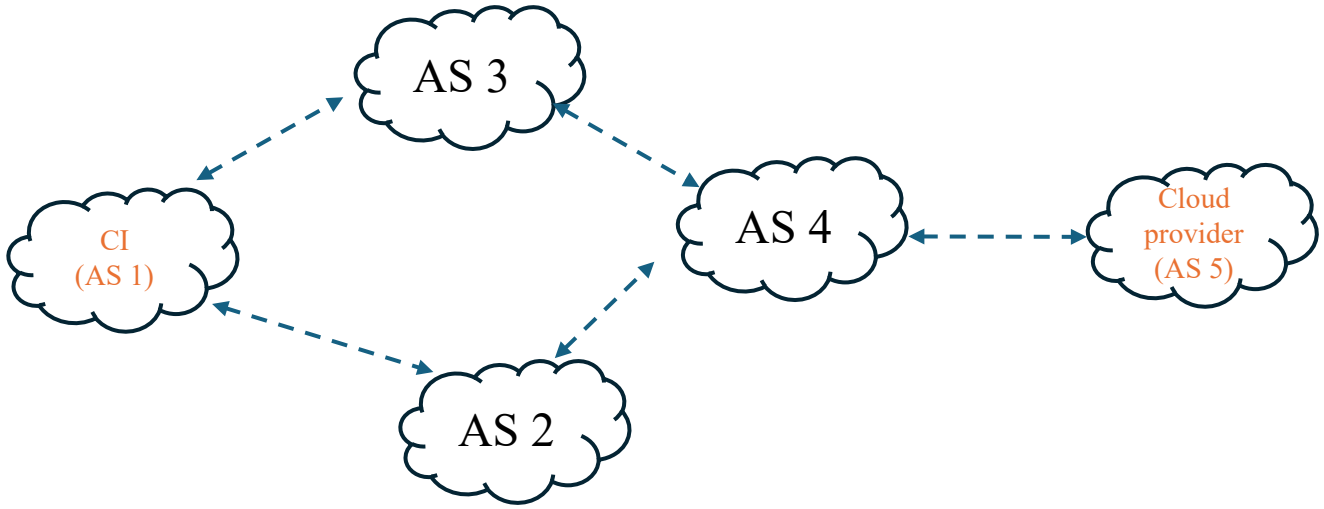
Problem

- Critical Infrastructures(CIs) are physical and information technology facilities, networks, services, and assets
- Disruption of CIs impacts the health, safety, and security or economic well-being of citizens
- CIs traffic needs to traverse multiple autonomous systems to reach their cloud providers
- Limited insight into the security status of the paths
  - Limited visibility about the paths
  - No mechanism exists to measure the security of the whole path

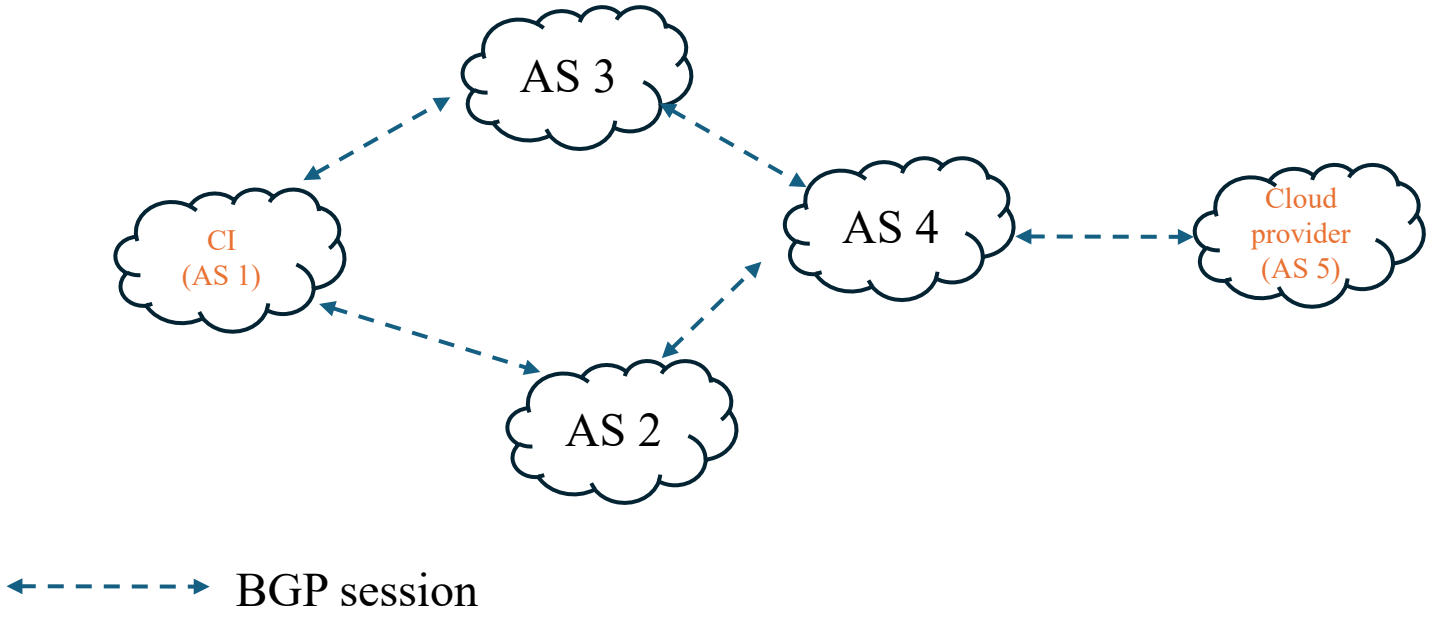
Border Gateway Protocol (BGP)



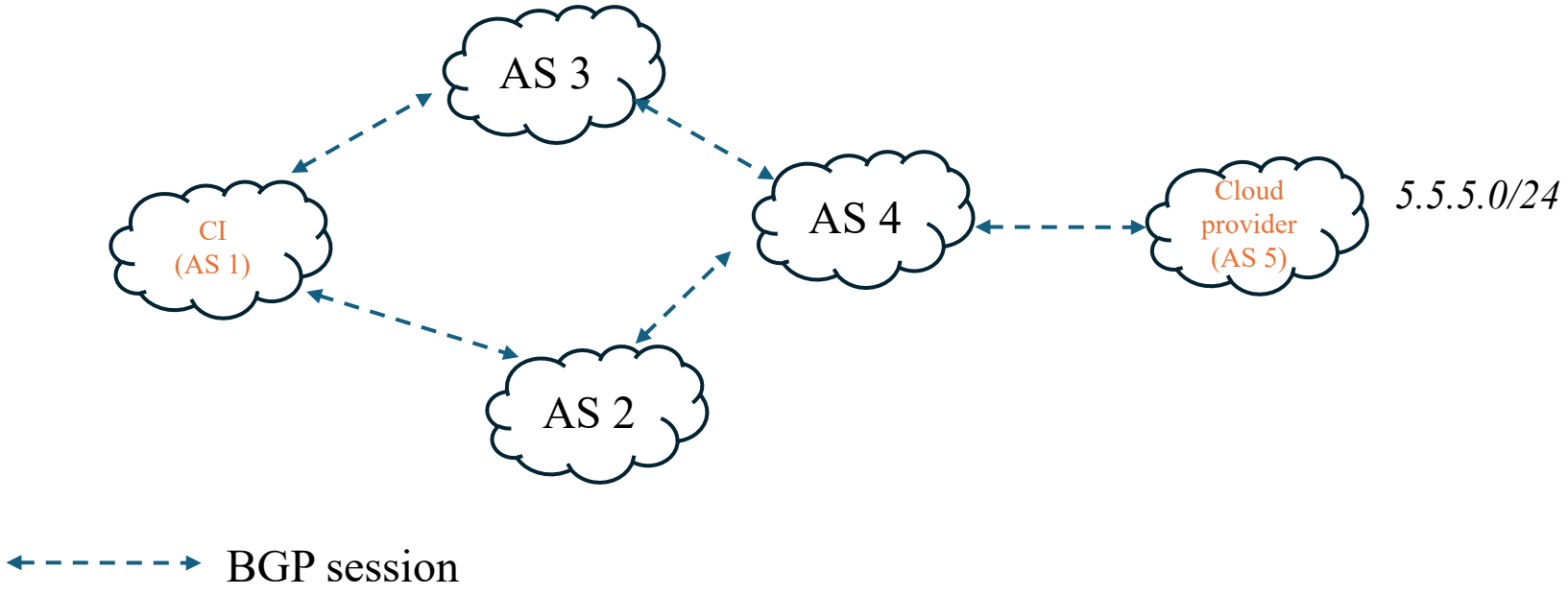
Border Gateway Protocol (BGP)



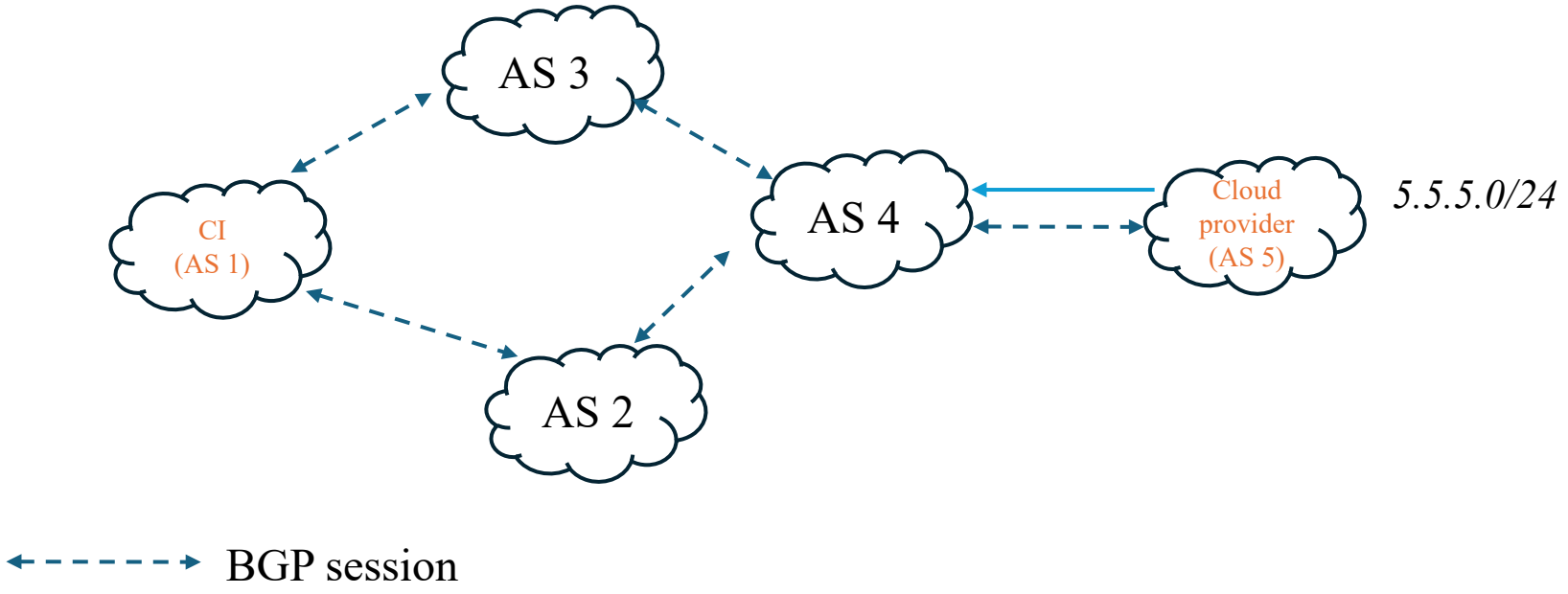
Border Gateway Protocol (BGP)



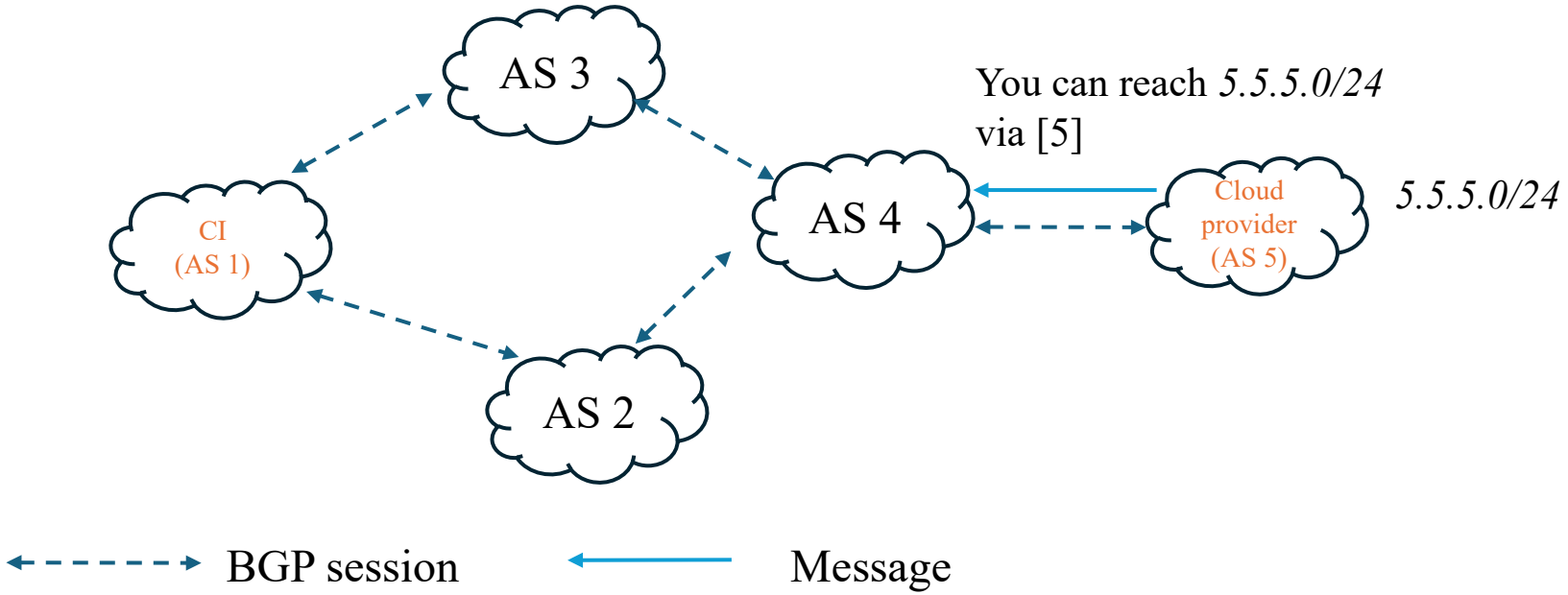
Border Gateway Protocol (BGP)



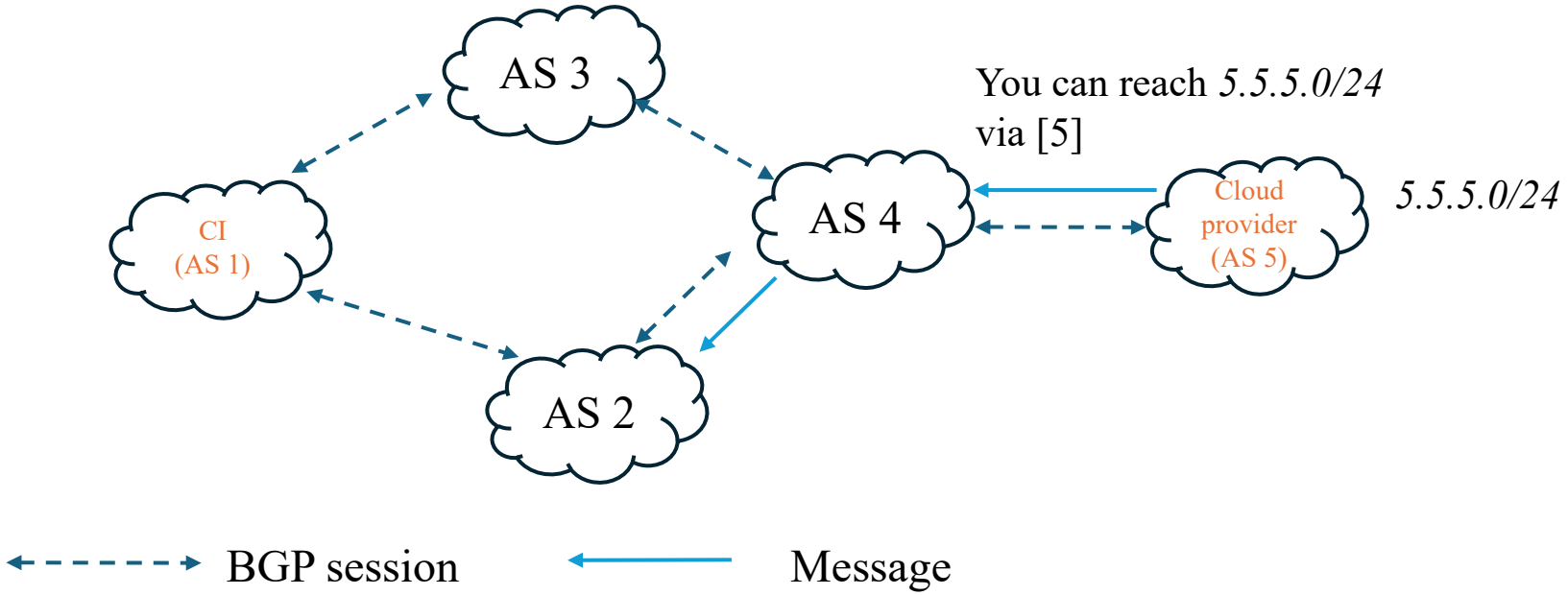
Border Gateway Protocol (BGP)



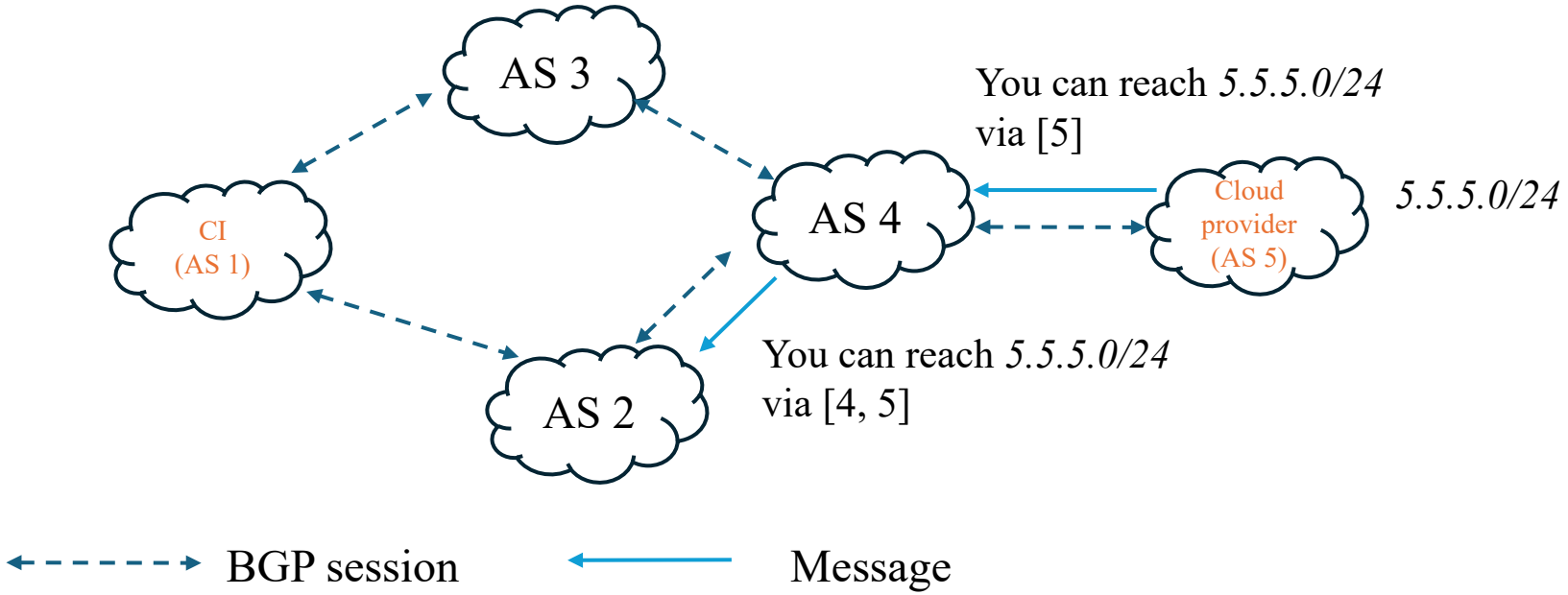
Border Gateway Protocol (BGP)



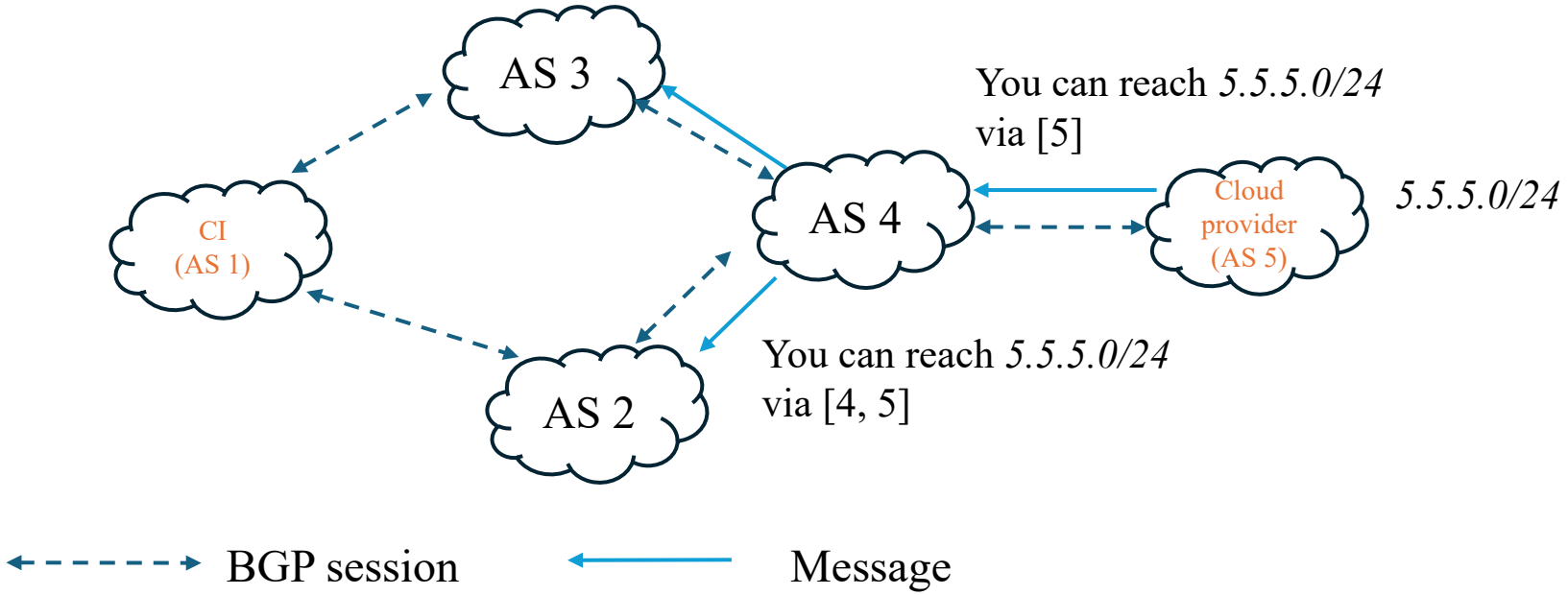
Border Gateway Protocol (BGP)



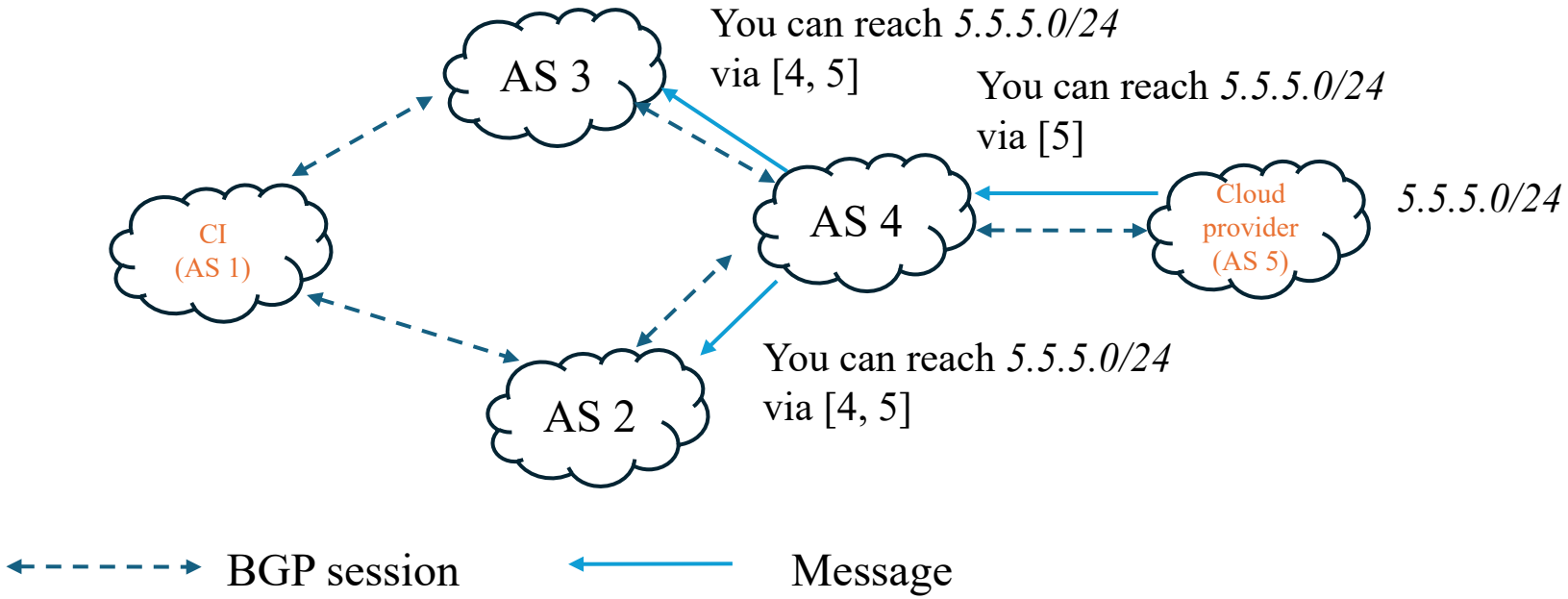
Border Gateway Protocol (BGP)



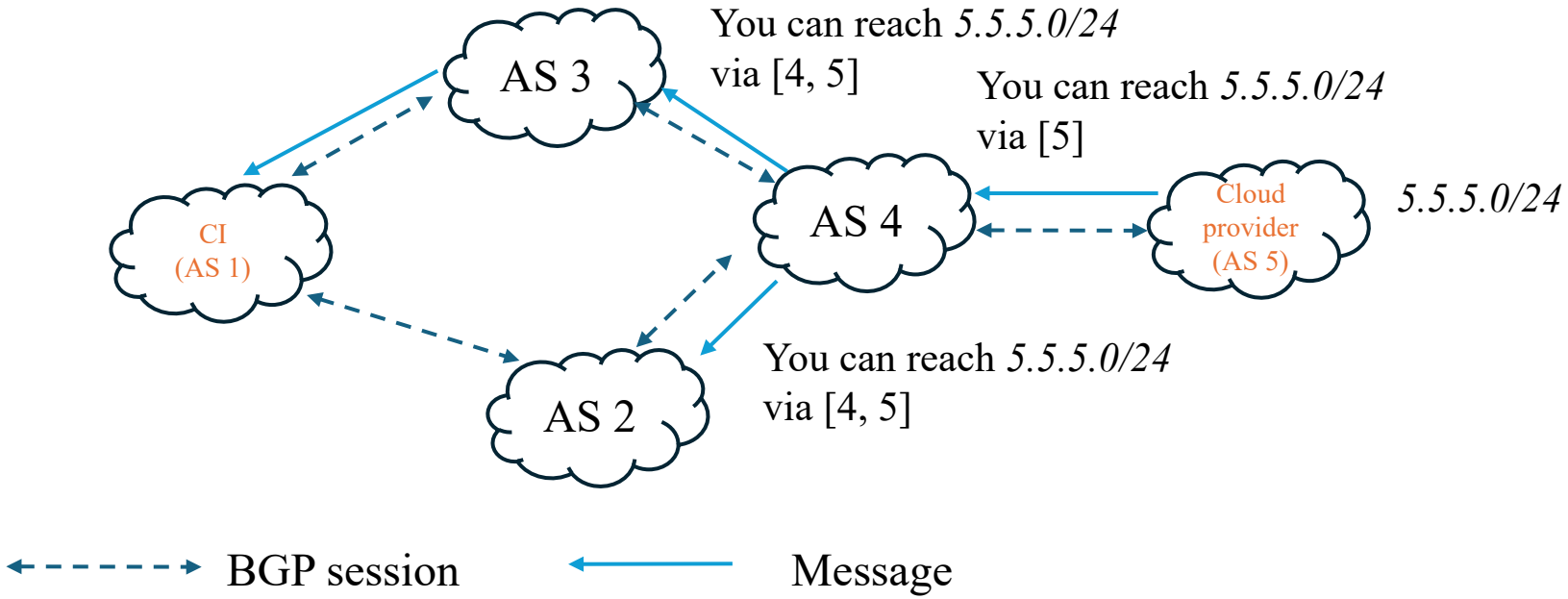
Border Gateway Protocol (BGP)



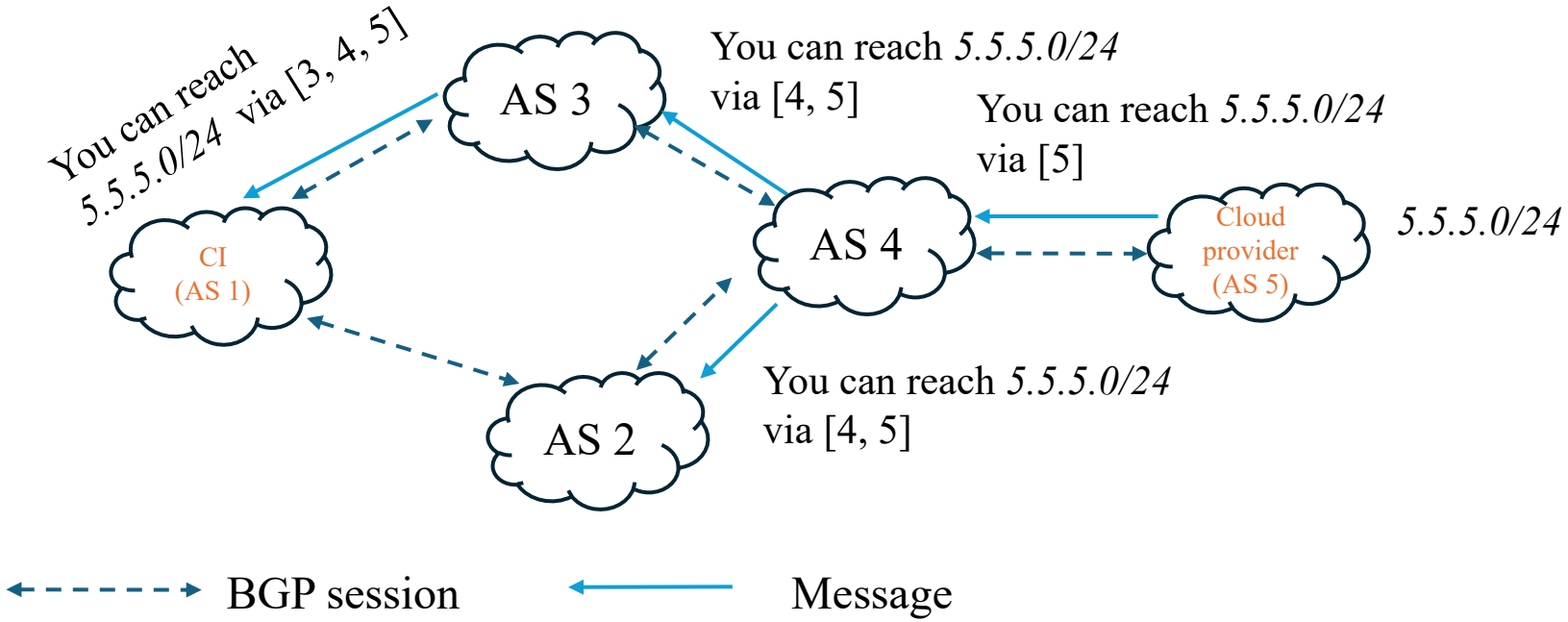
Border Gateway Protocol (BGP)



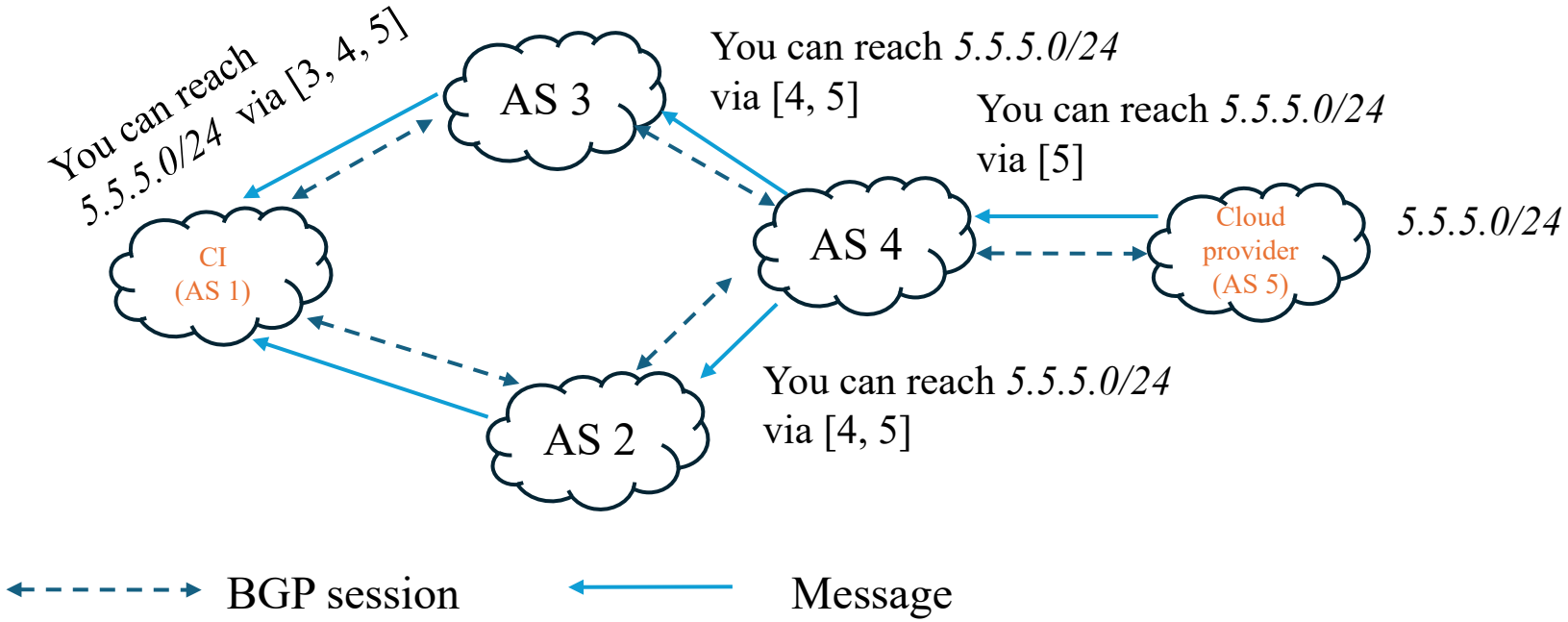
Border Gateway Protocol (BGP)



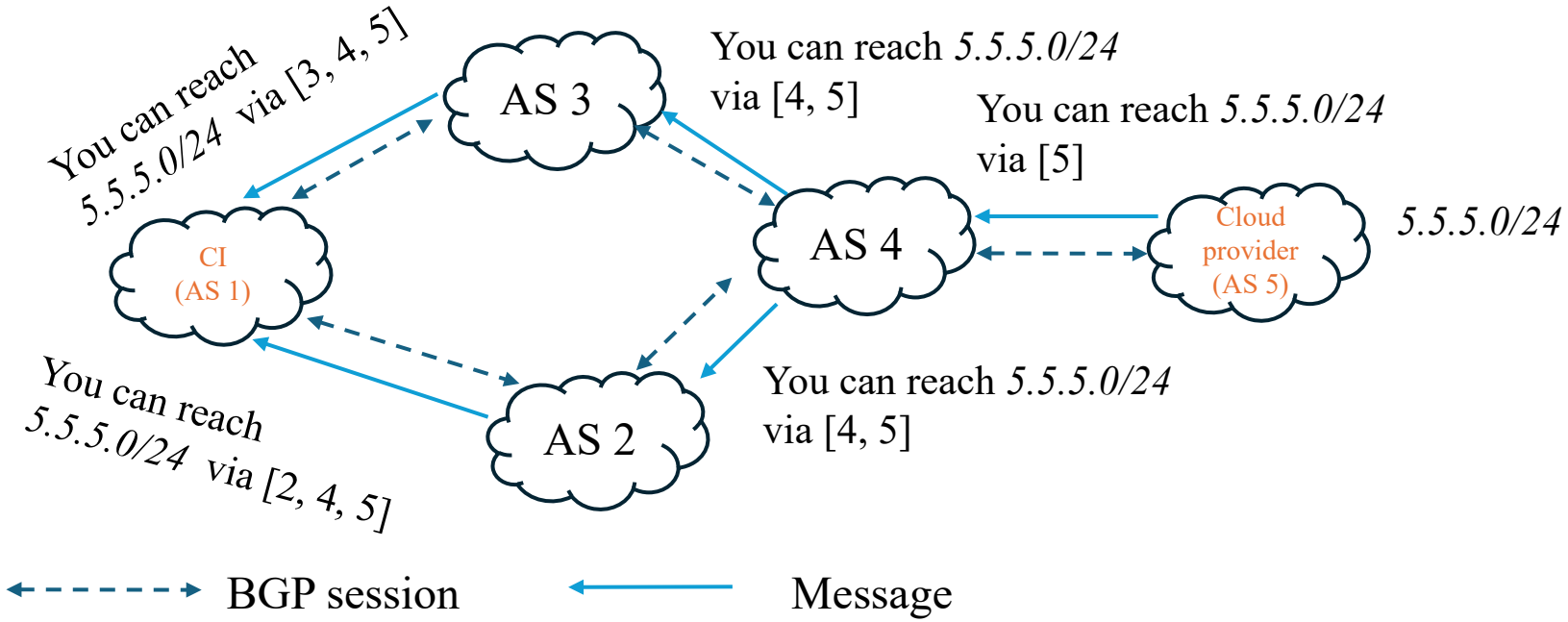
Border Gateway Protocol (BGP)



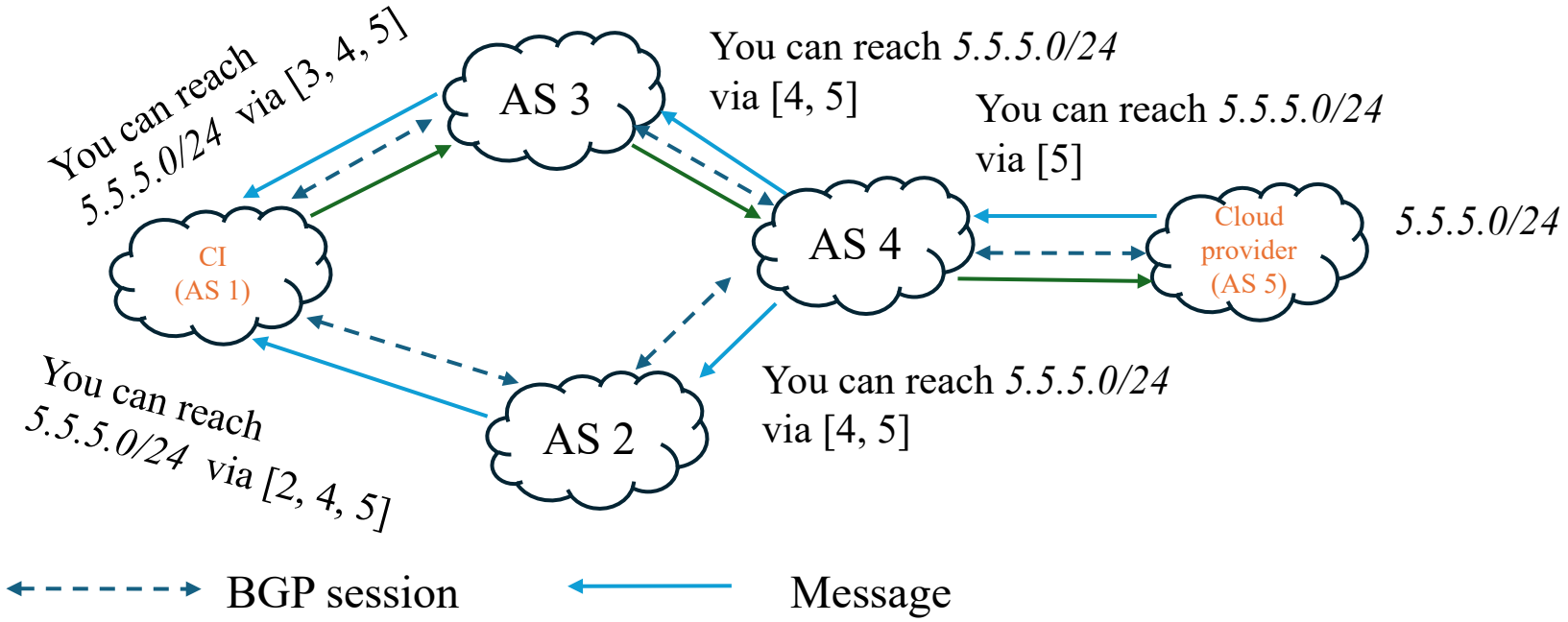
Border Gateway Protocol (BGP)



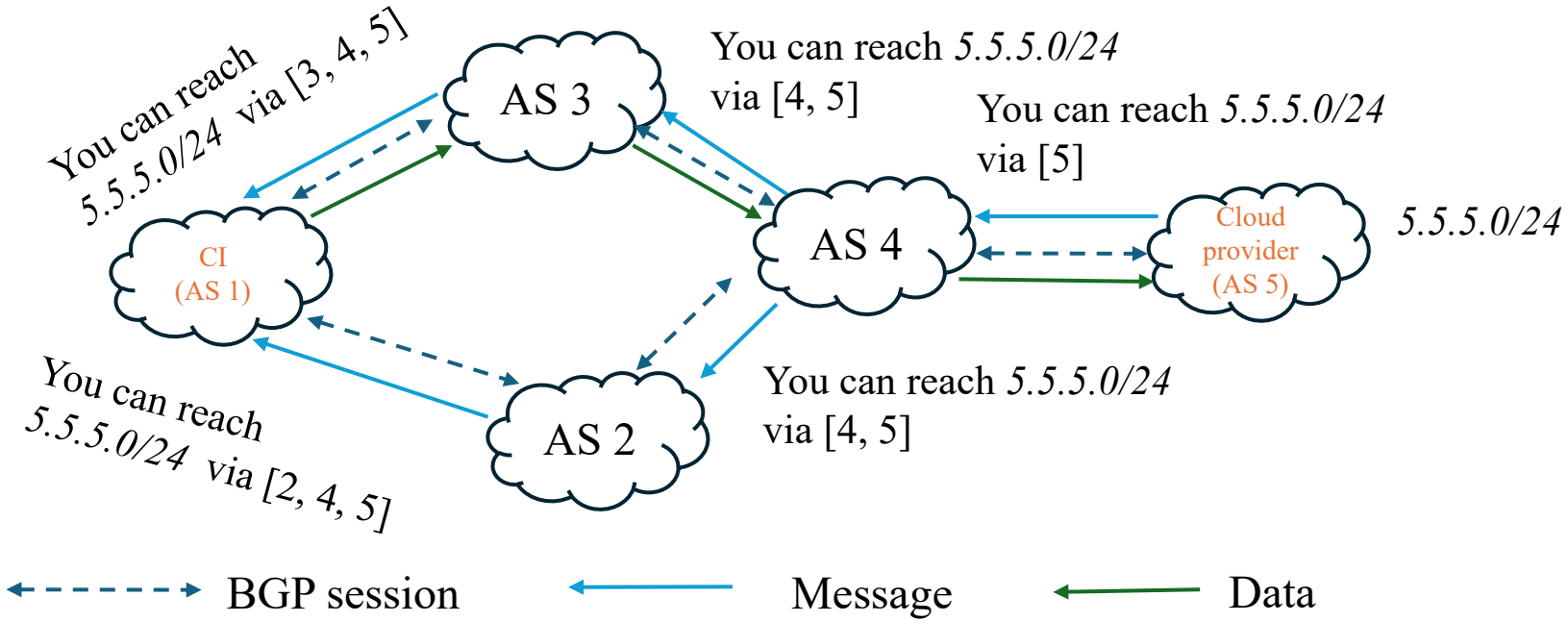
Border Gateway Protocol (BGP)



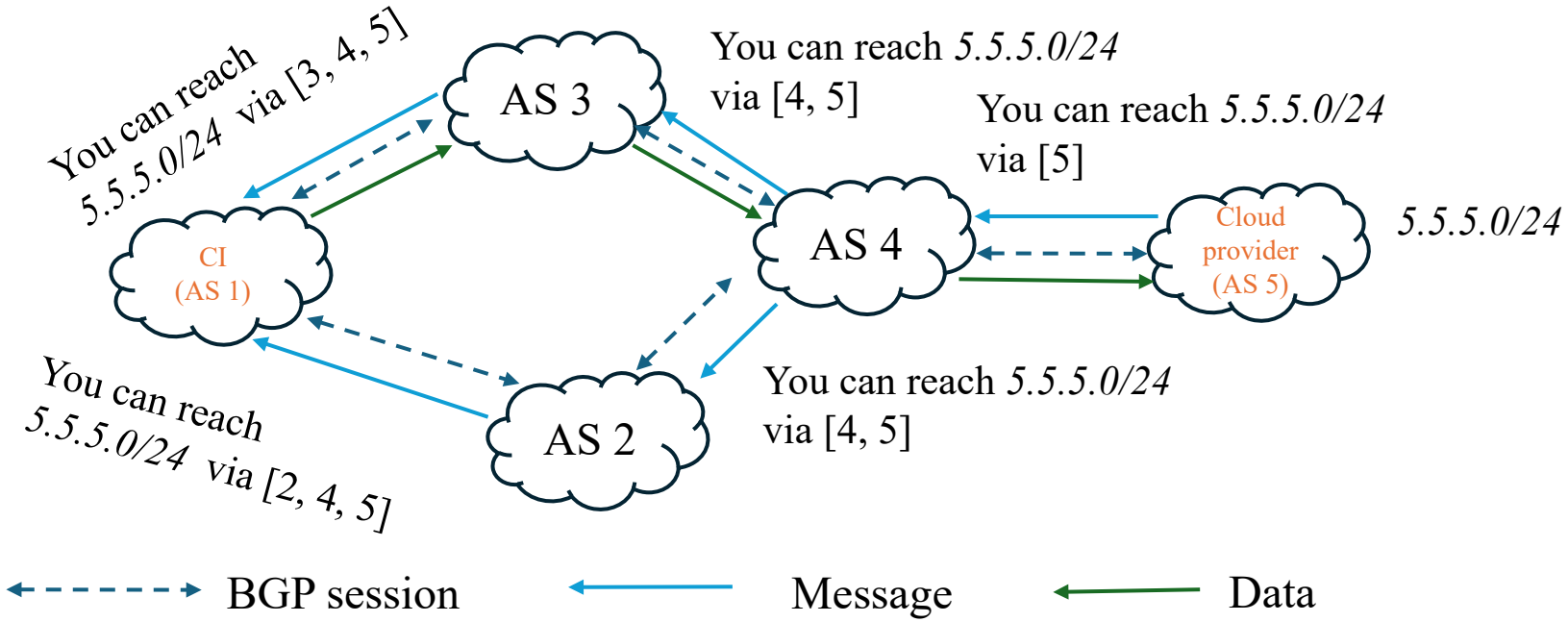
Border Gateway Protocol (BGP)



Border Gateway Protocol (BGP)

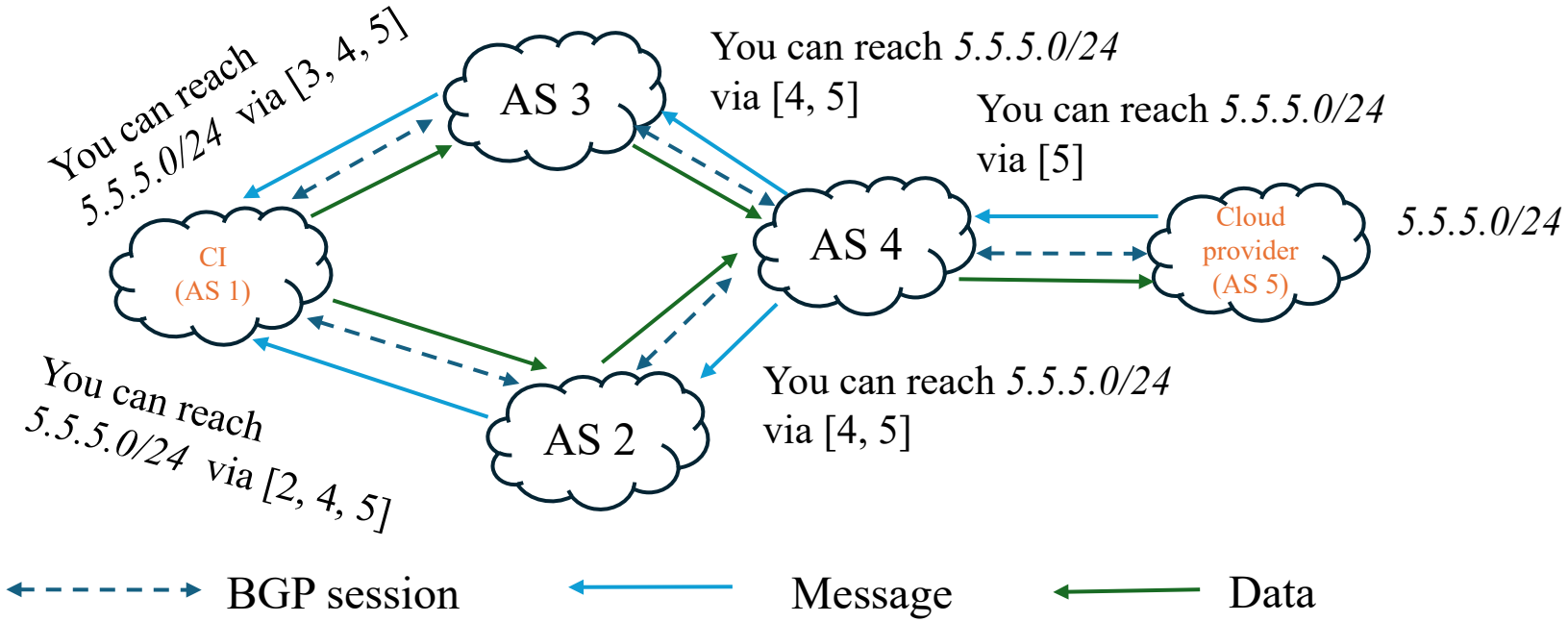


Border Gateway Protocol (BGP)



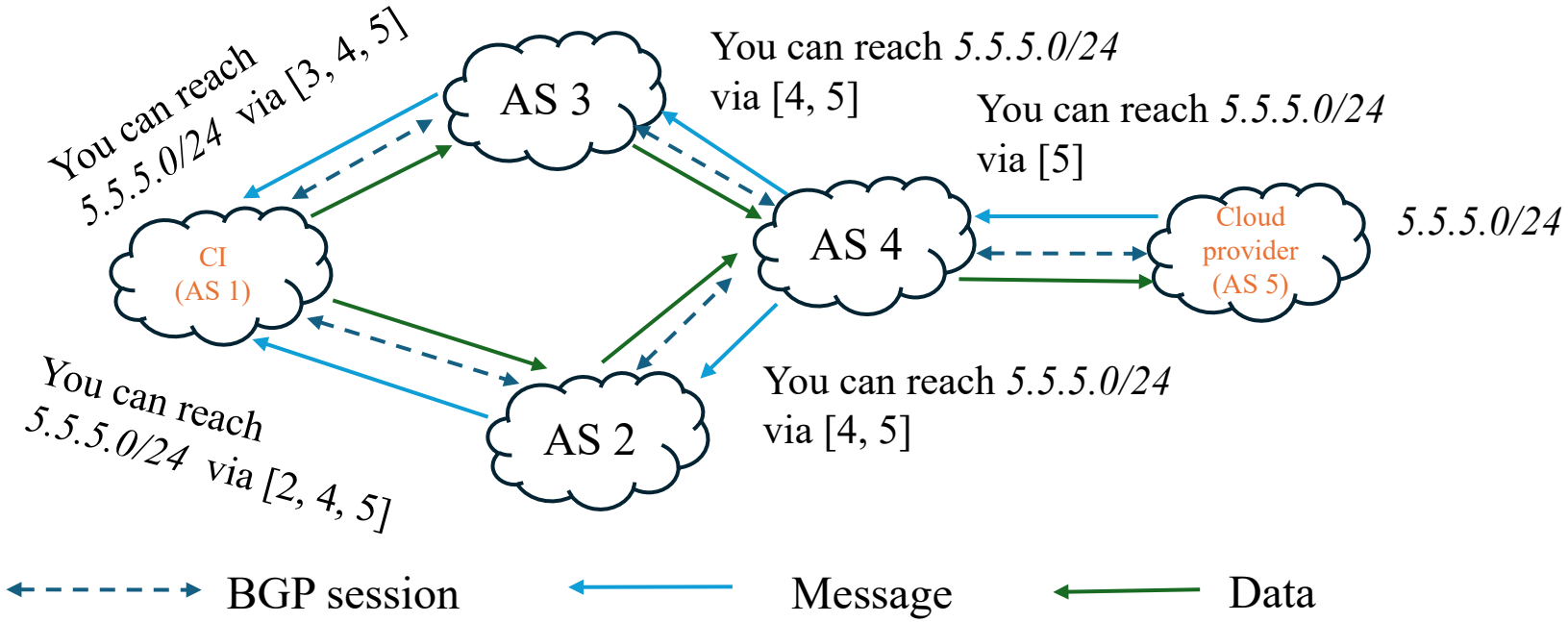
Path 1: [1,3,4,5]

Border Gateway Protocol (BGP)

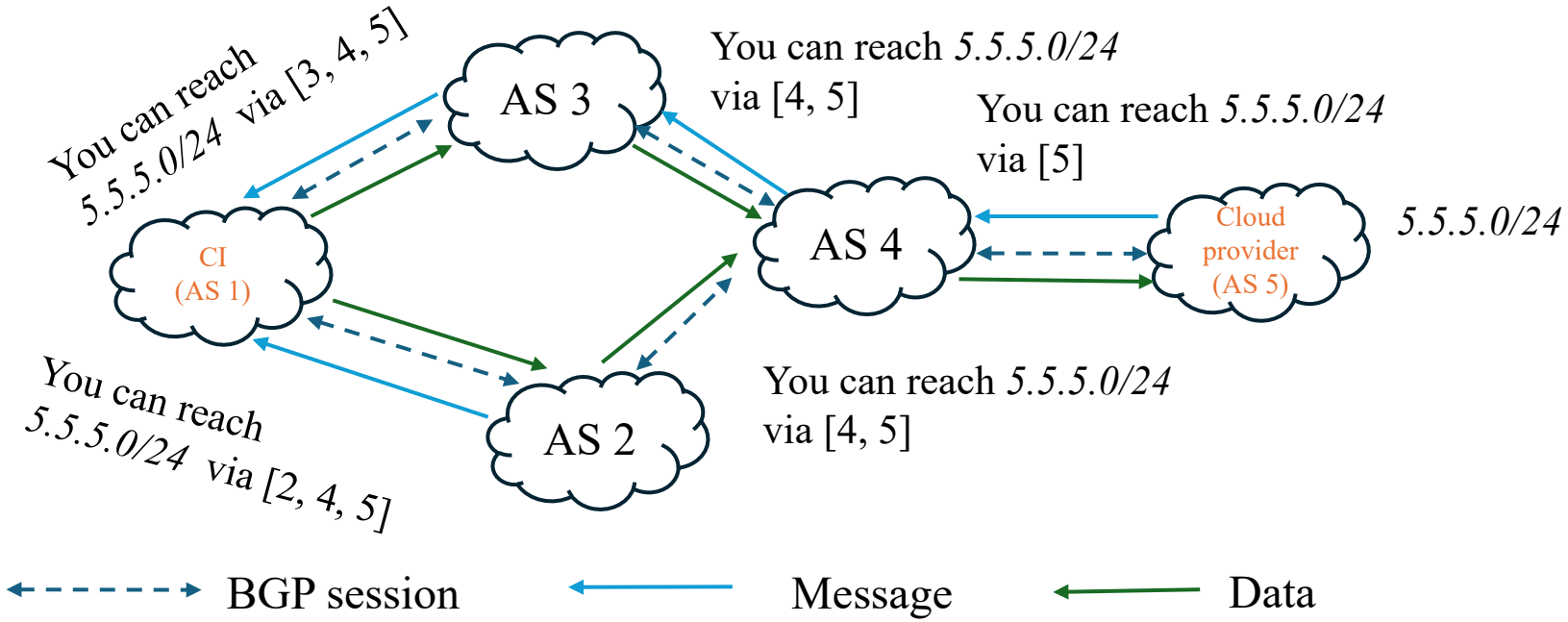


Path 1: [1,3,4,5]

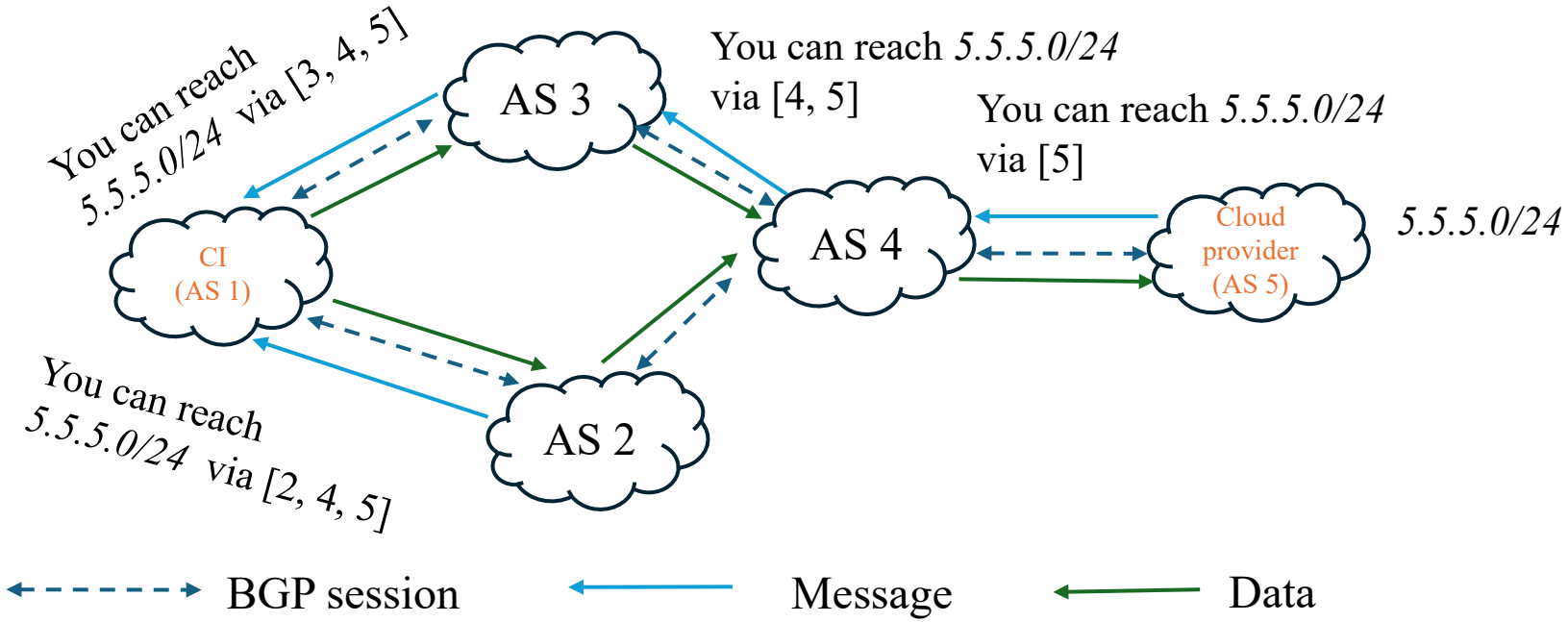
Border Gateway Protocol (BGP)



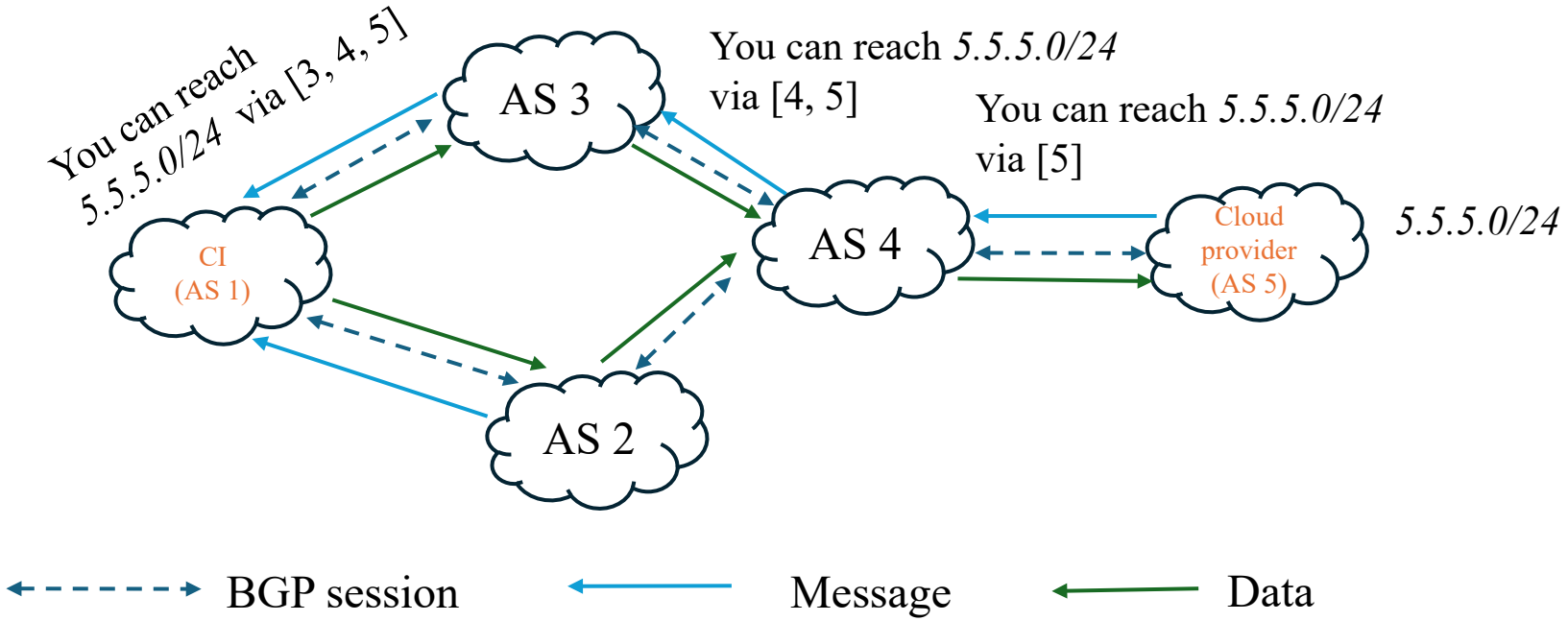
Border Gateway Protocol (BGP)



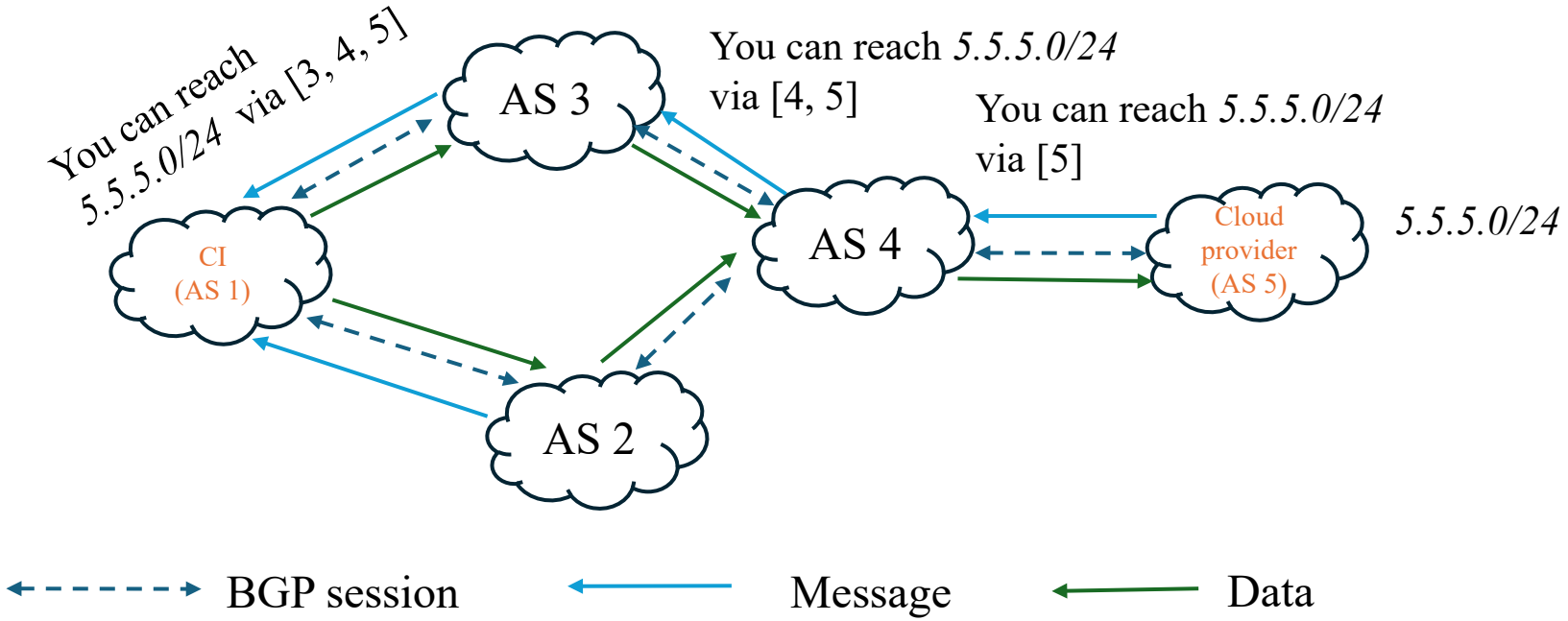
Border Gateway Protocol (BGP)



Border Gateway Protocol (BGP)

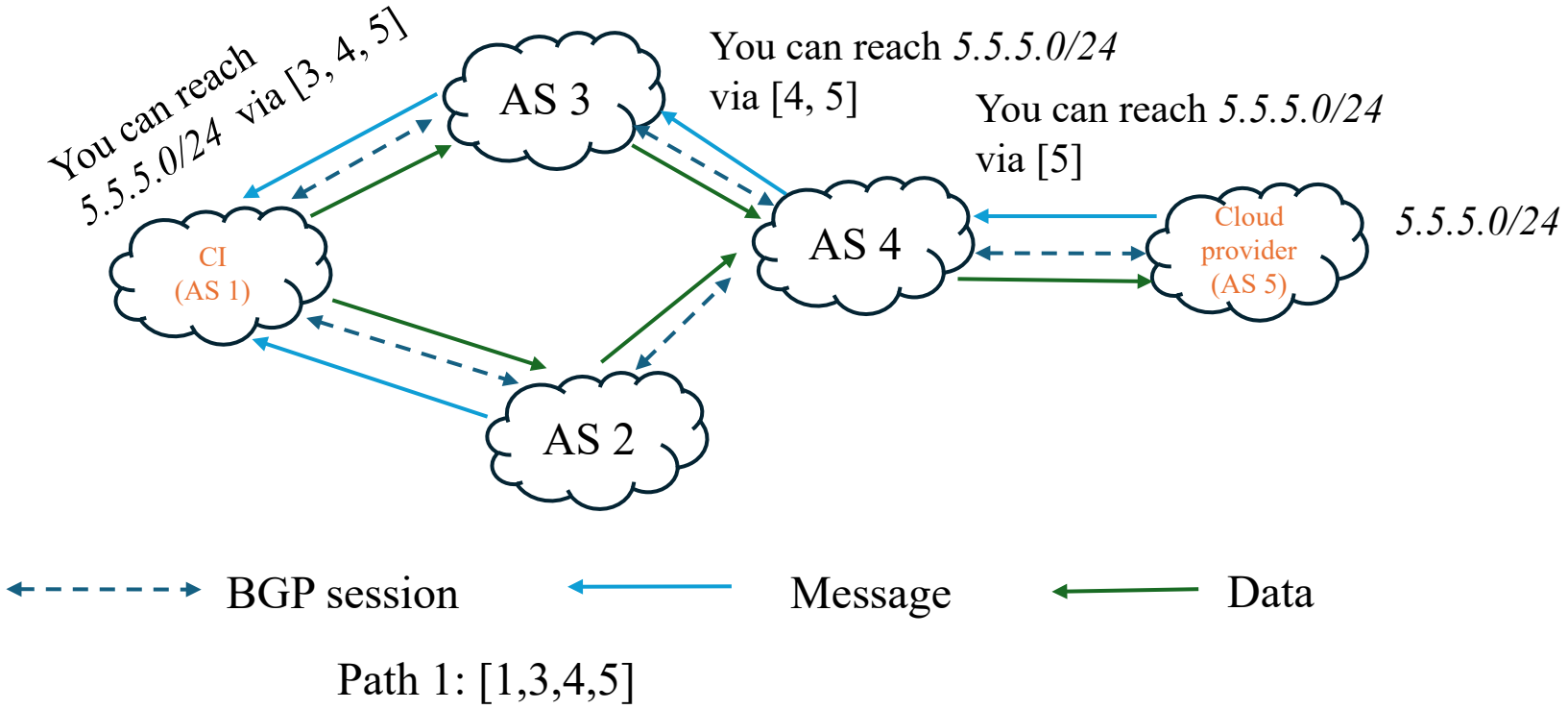


Border Gateway Protocol (BGP)



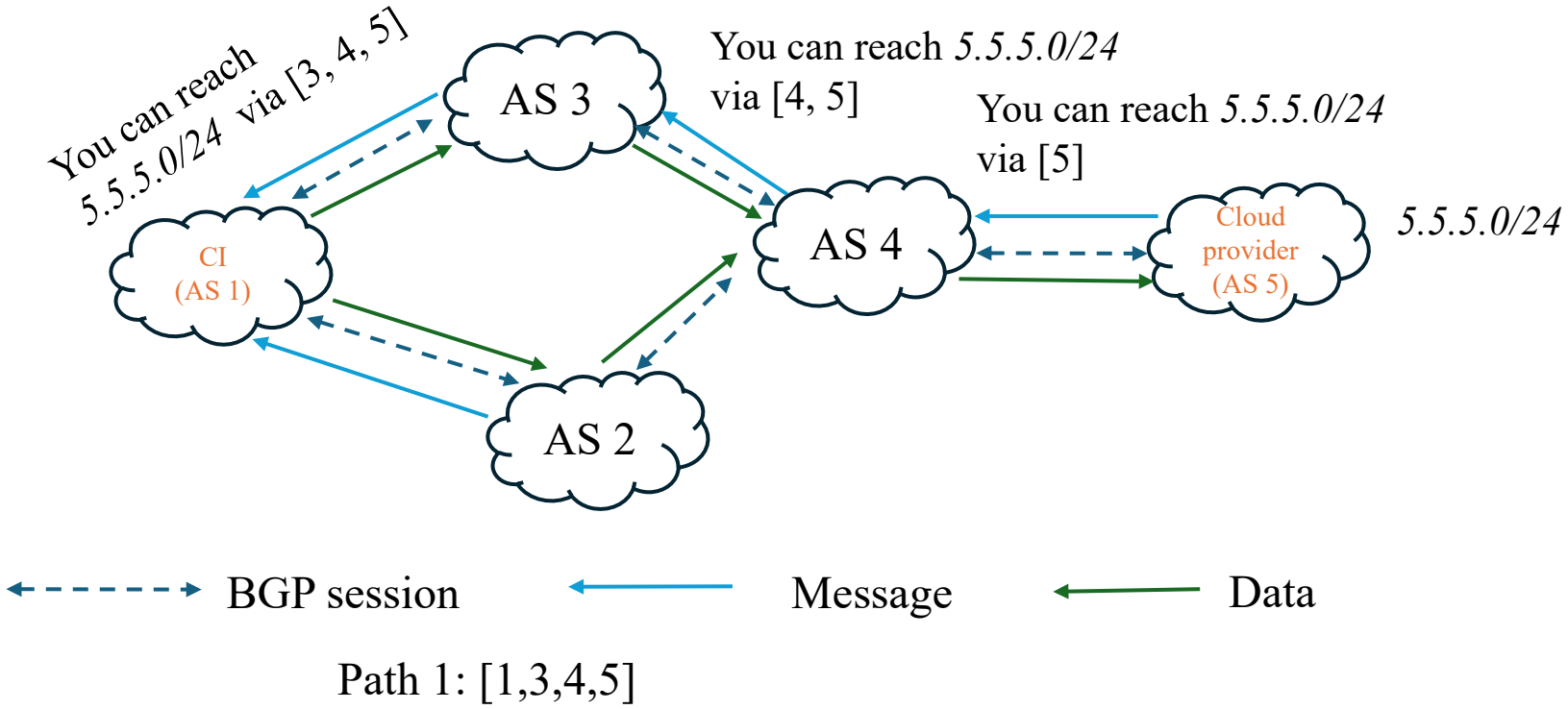
Path 1: [1,3,4,5]

Border Gateway Protocol (BGP)



Limited insights about the possible paths due to “selective announcement*”

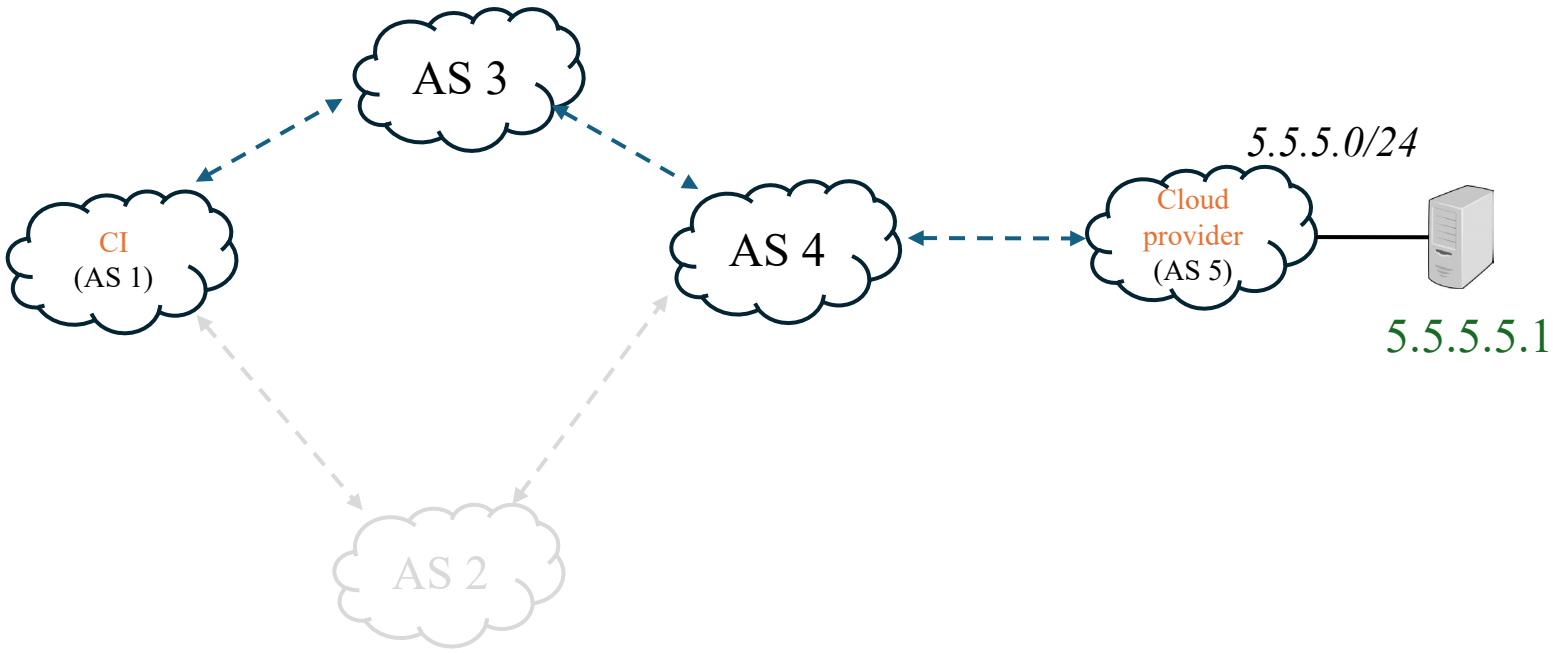
Border Gateway Protocol (BGP)



Limited insights about the possible paths due to "selective announcement*"

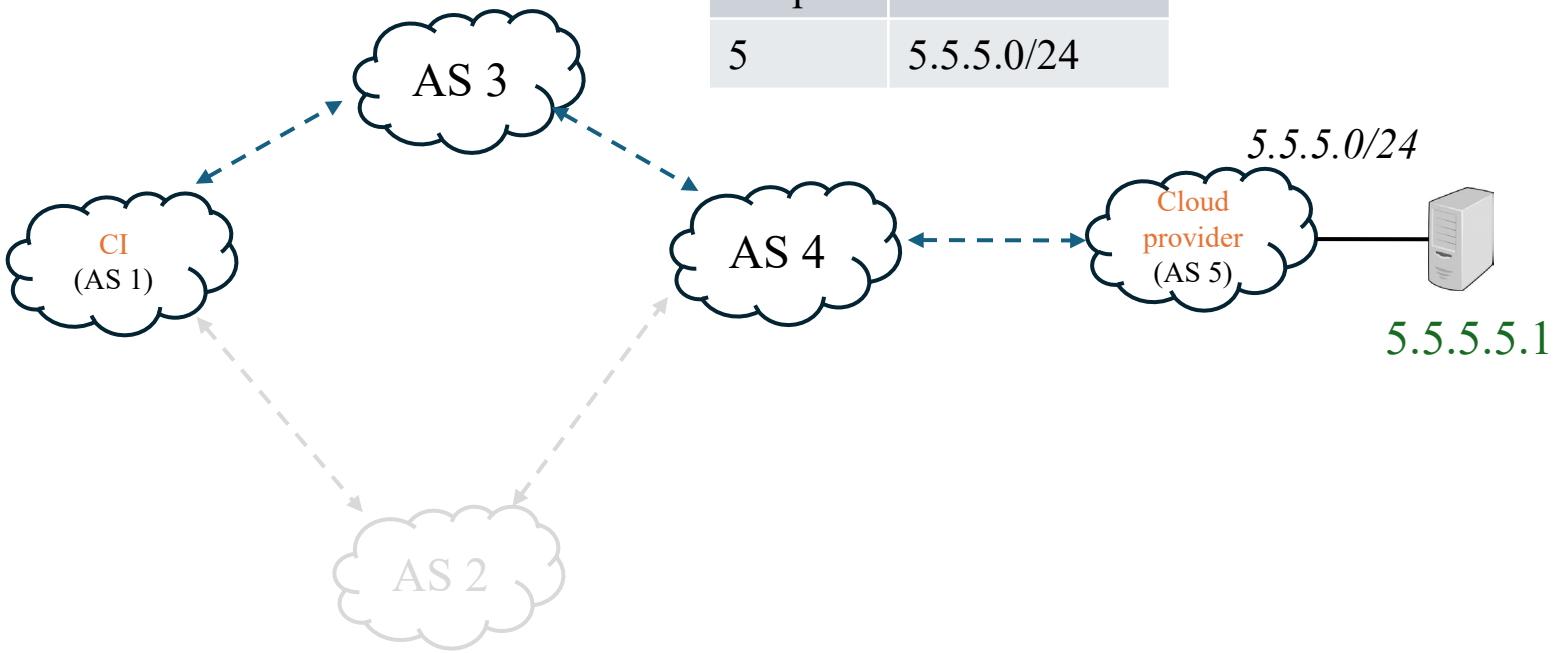
*Kastanakis, S., Giotsas, V., Livadariu, I., & Suri, N. (2023, October). Replication: 20 Years of Inferring Interdomain Routing Policies. In Proceedings of the 2023 ACM on Internet Measurement Conference (pp. 16-29).

Prefix hijacking and Route Origin Validation



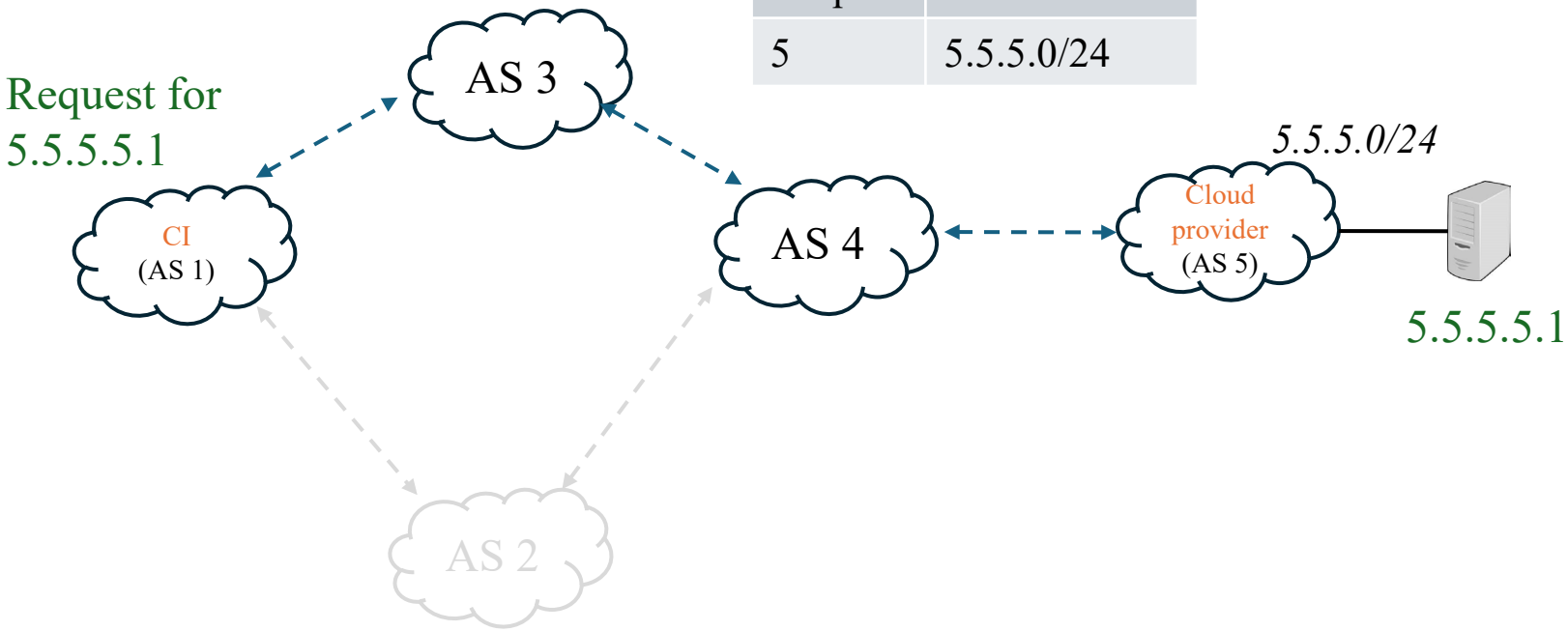
Prefix hijacking and Route Origin Validation

AS 4 routing table	
AS path	Prefix
5	5.5.5.0/24



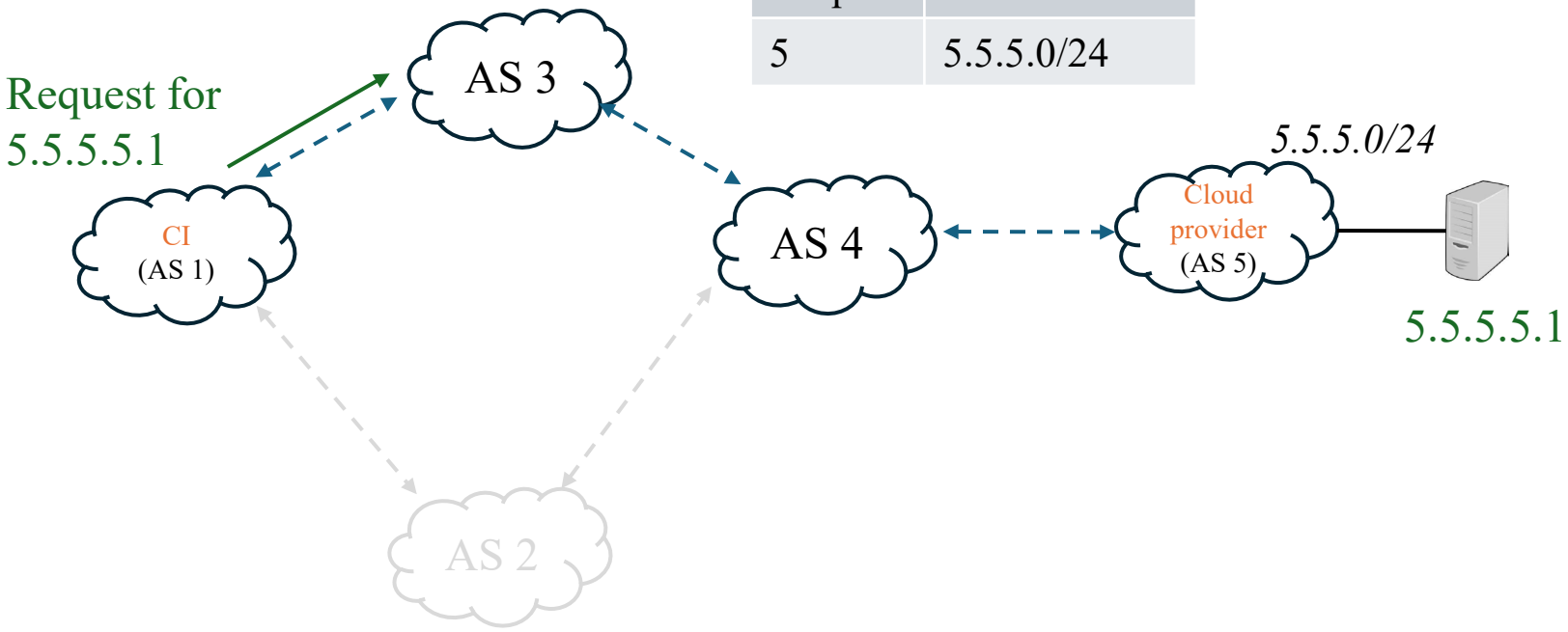
Prefix hijacking and Route Origin Validation

AS 4 routing table	
AS path	Prefix
5	5.5.5.0/24



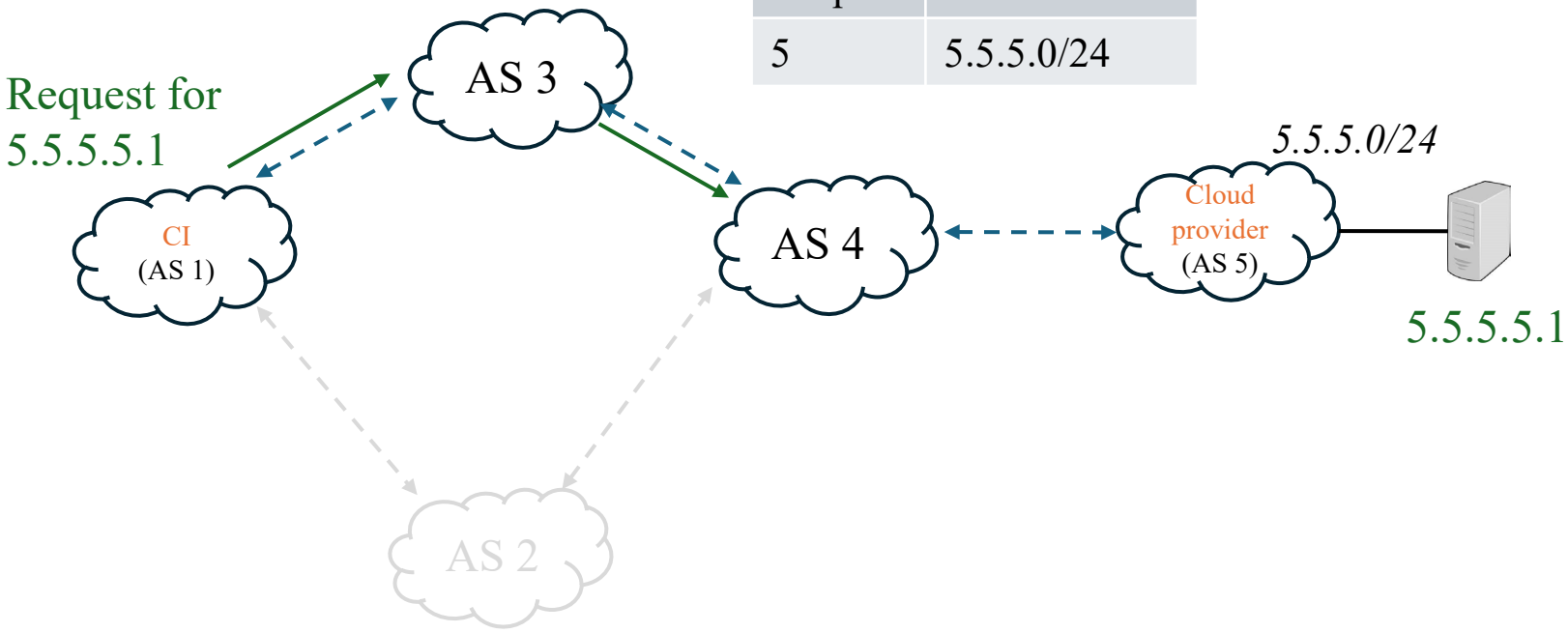
Prefix hijacking and Route Origin Validation

AS 4 routing table	
AS path	Prefix
5	5.5.5.0/24



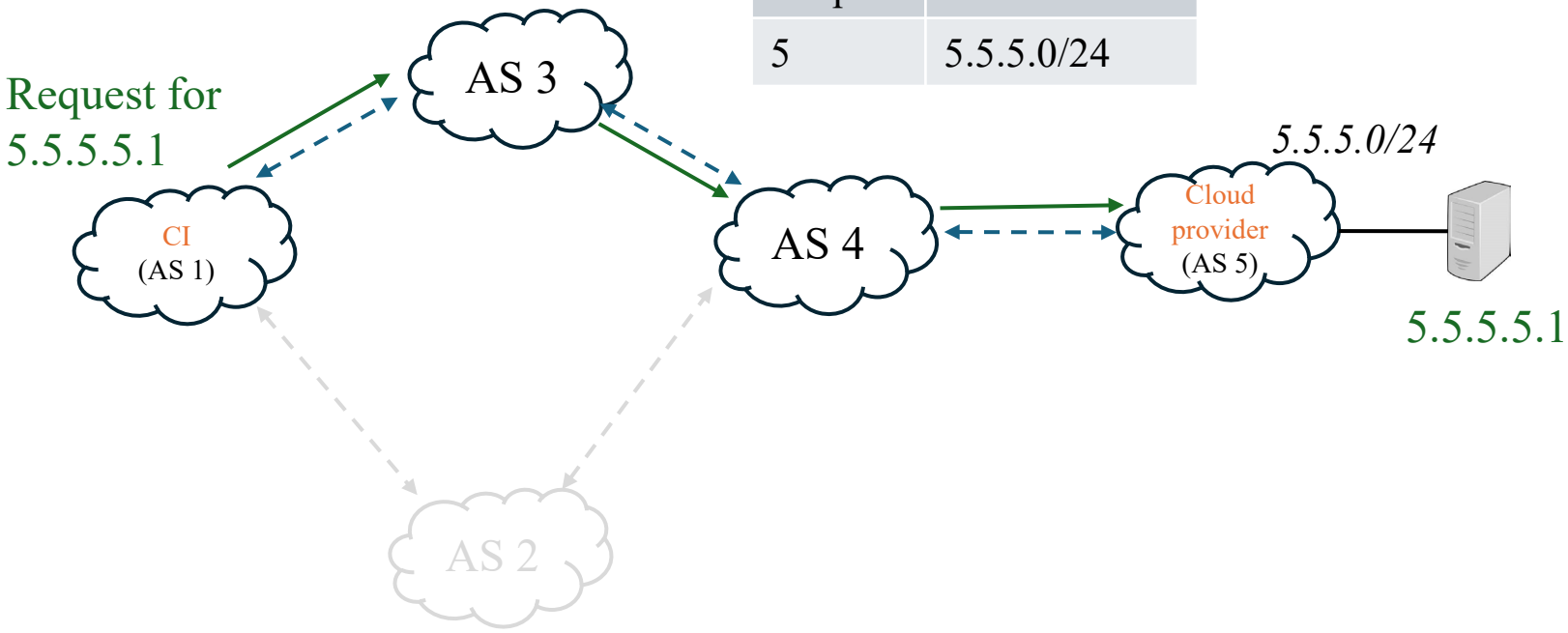
Prefix hijacking and Route Origin Validation

AS 4 routing table	
AS path	Prefix
5	5.5.5.0/24



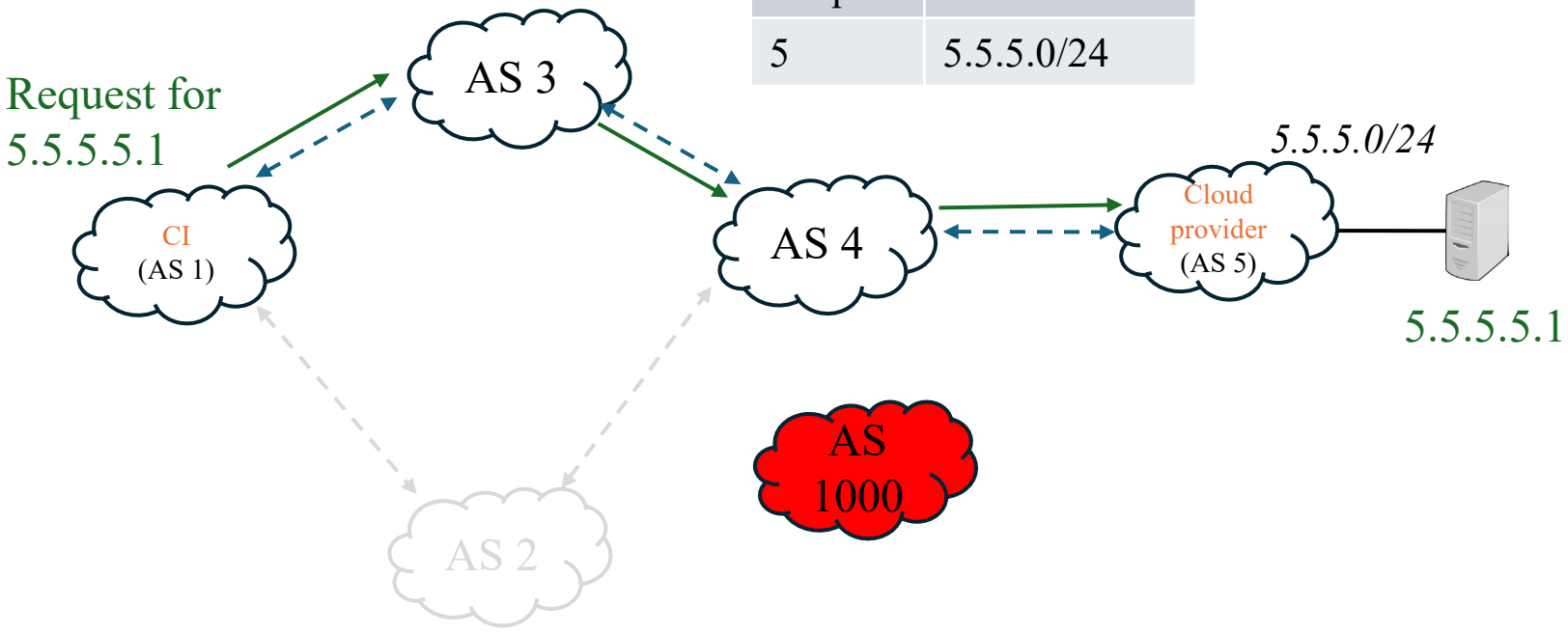
Prefix hijacking and Route Origin Validation

AS 4 routing table	
AS path	Prefix
5	5.5.5.0/24



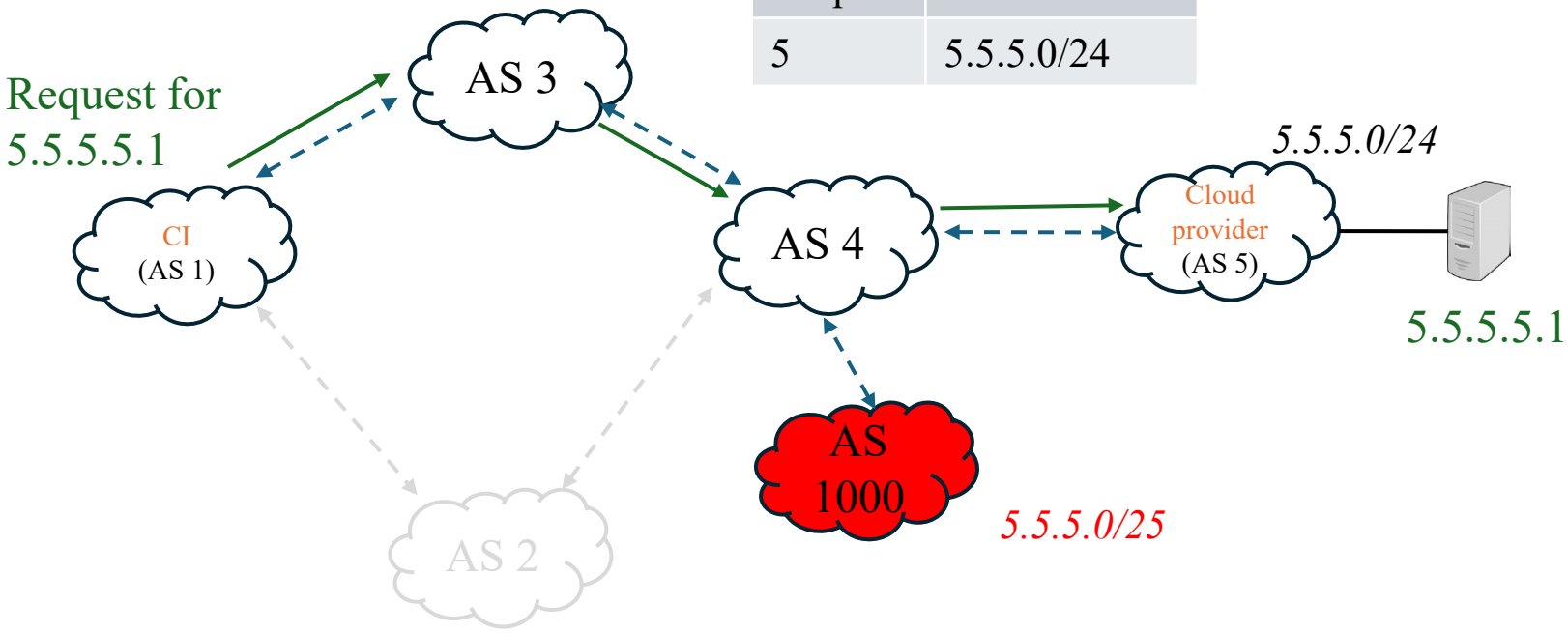
Prefix hijacking and Route Origin Validation

AS 4 routing table	
AS path	Prefix
5	5.5.5.0/24

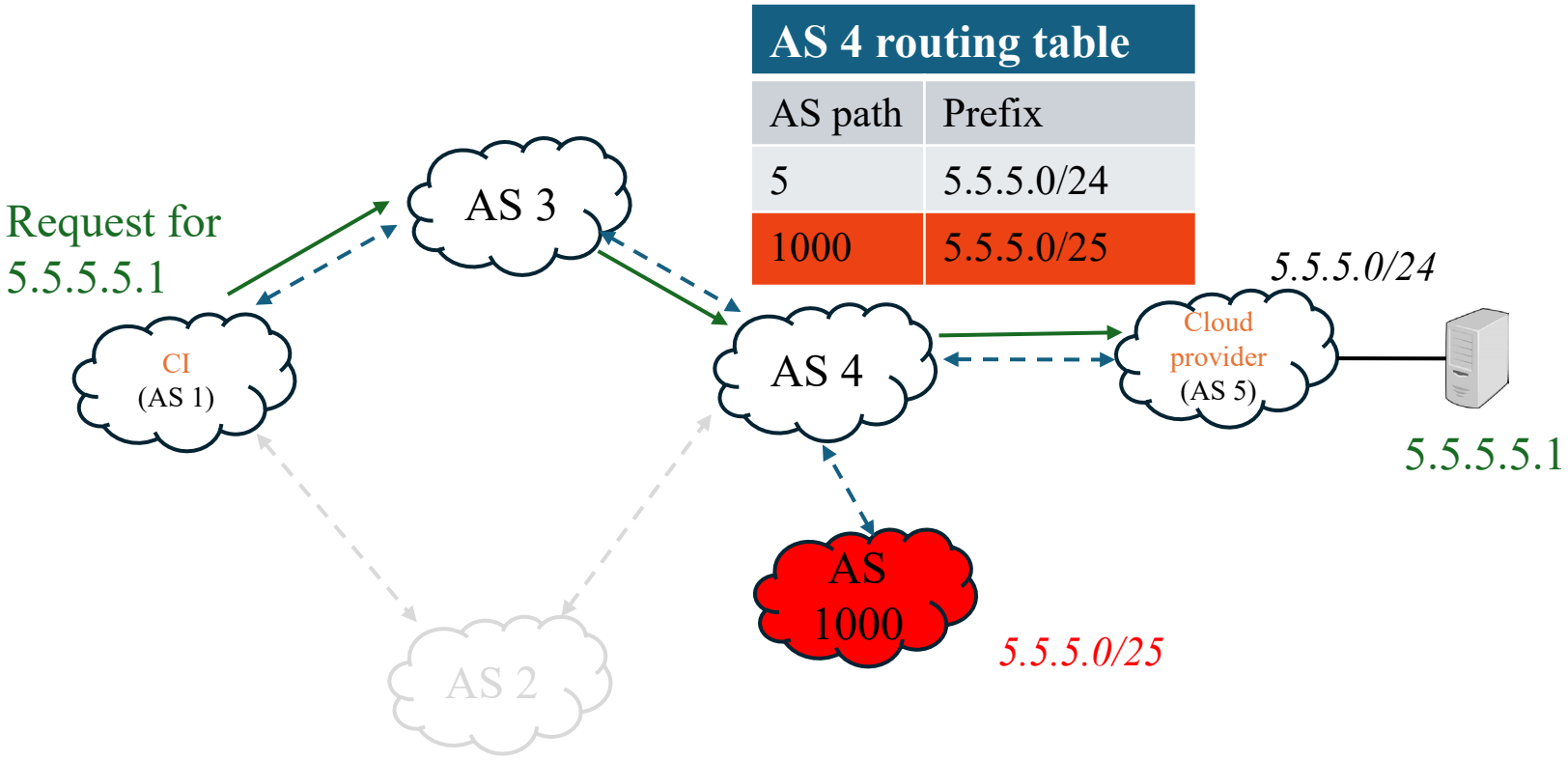


Prefix hijacking and Route Origin Validation

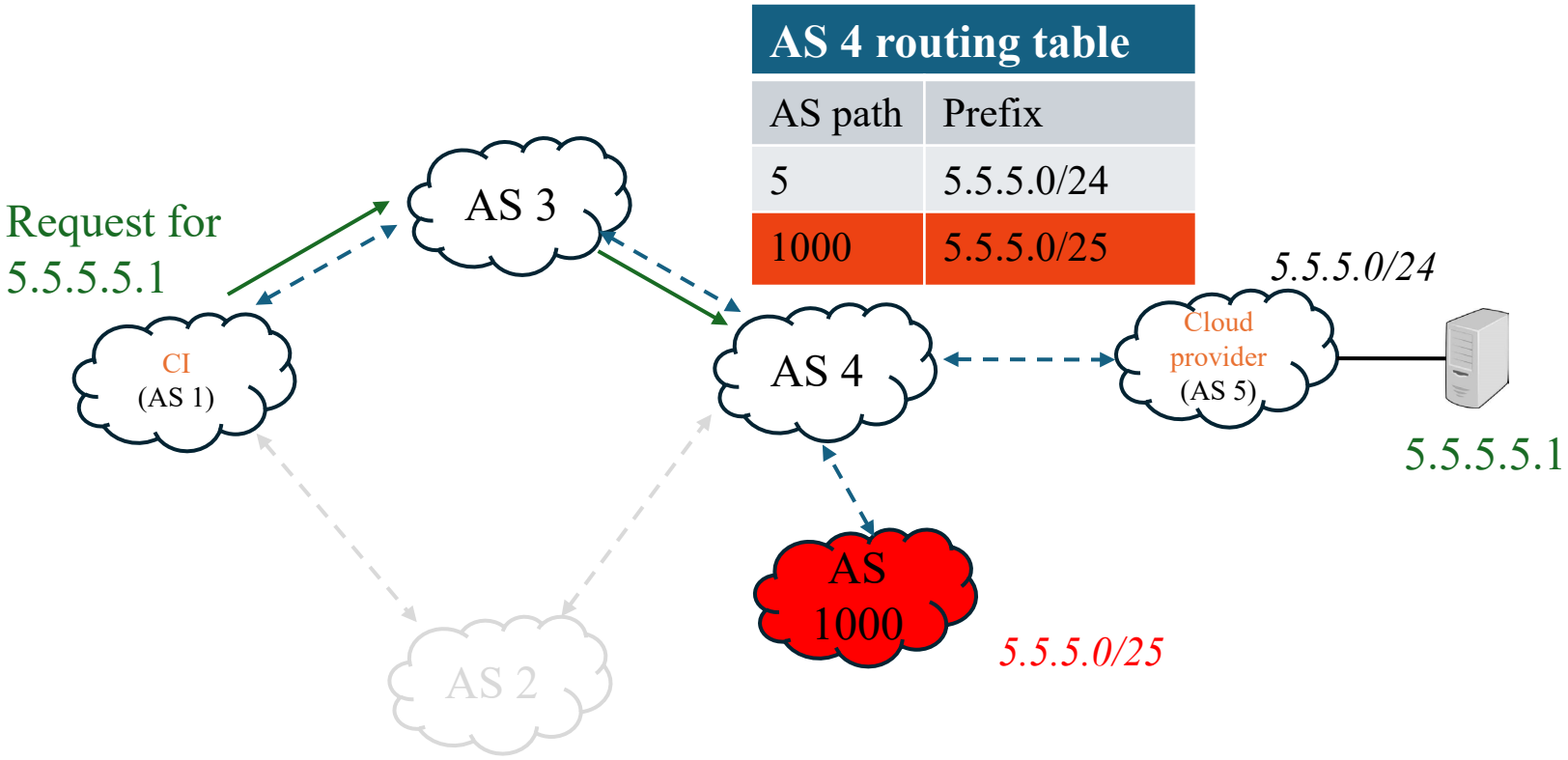
AS 4 routing table	
AS path	Prefix
5	5.5.5.0/24



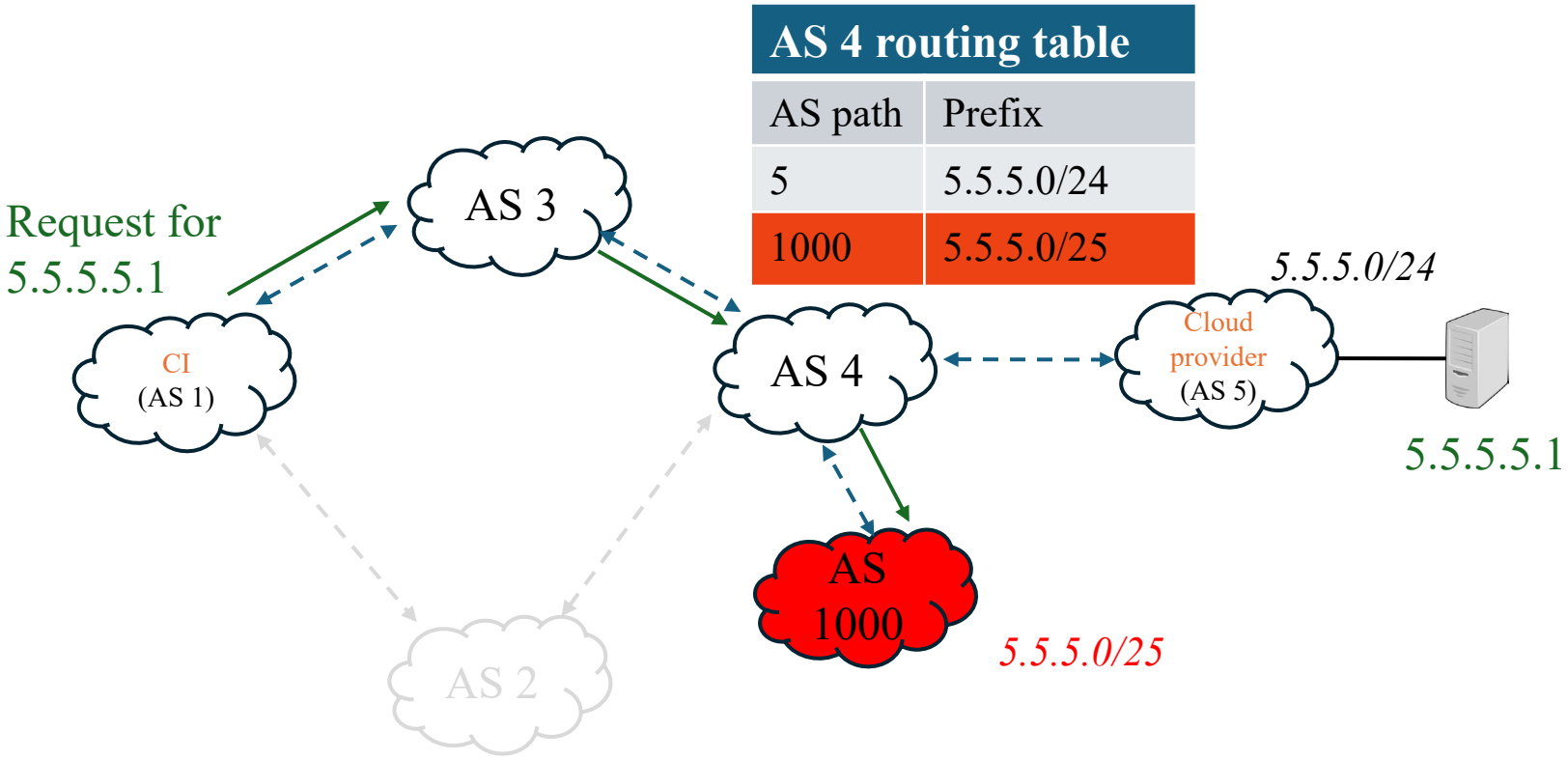
Prefix hijacking and Route Origin Validation



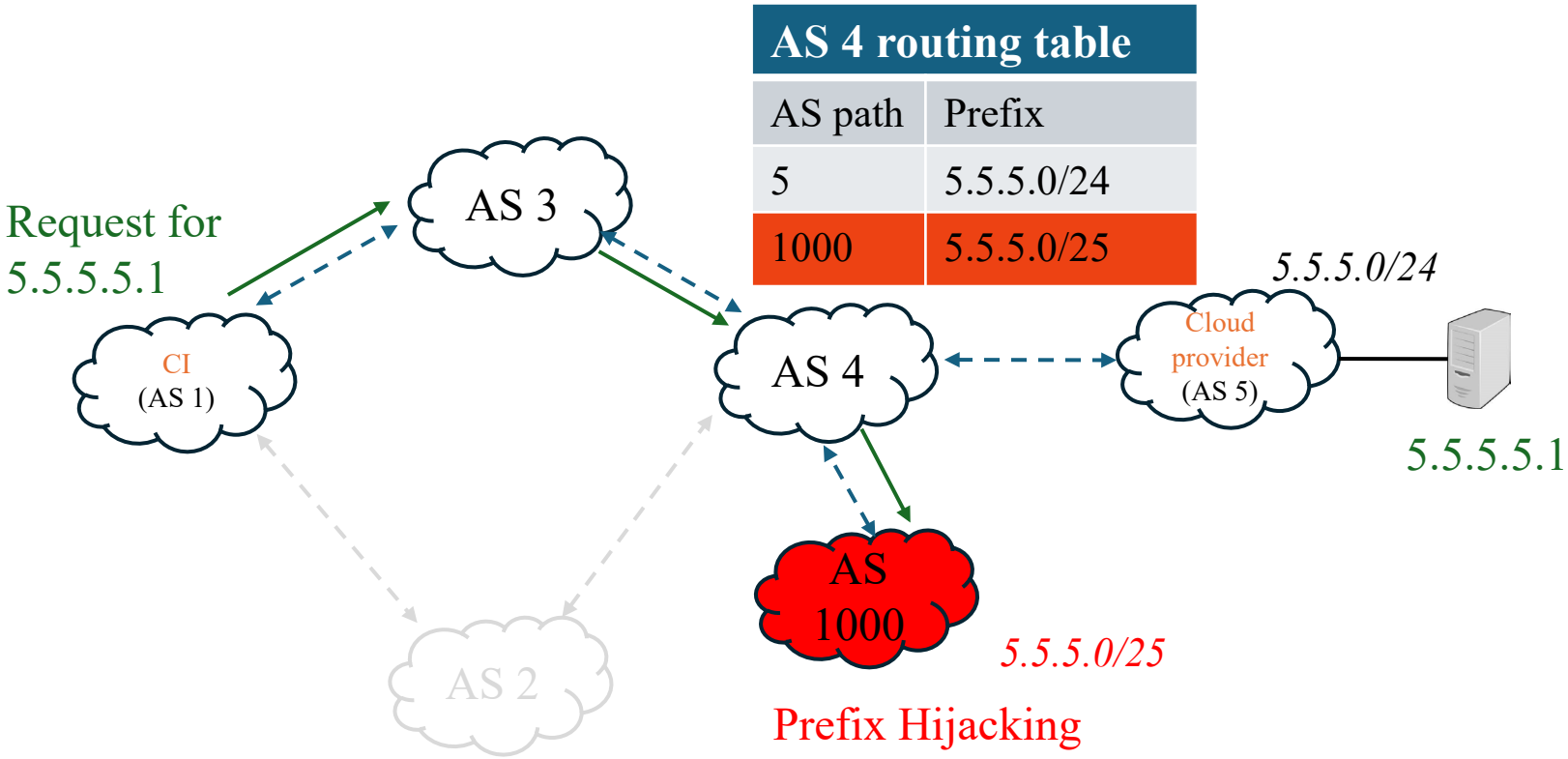
Prefix hijacking and Route Origin Validation



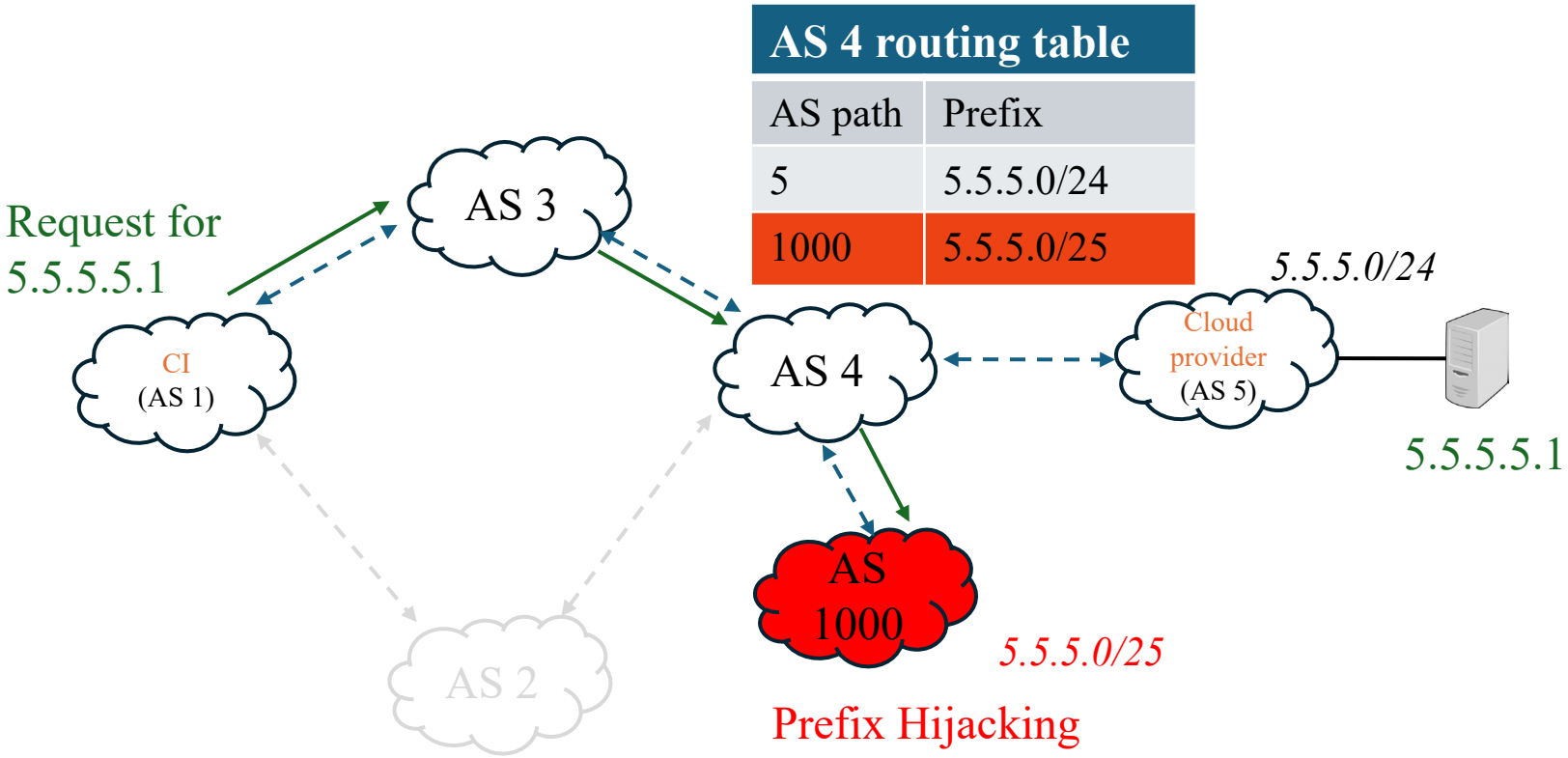
Prefix hijacking and Route Origin Validation



Prefix hijacking and Route Origin Validation

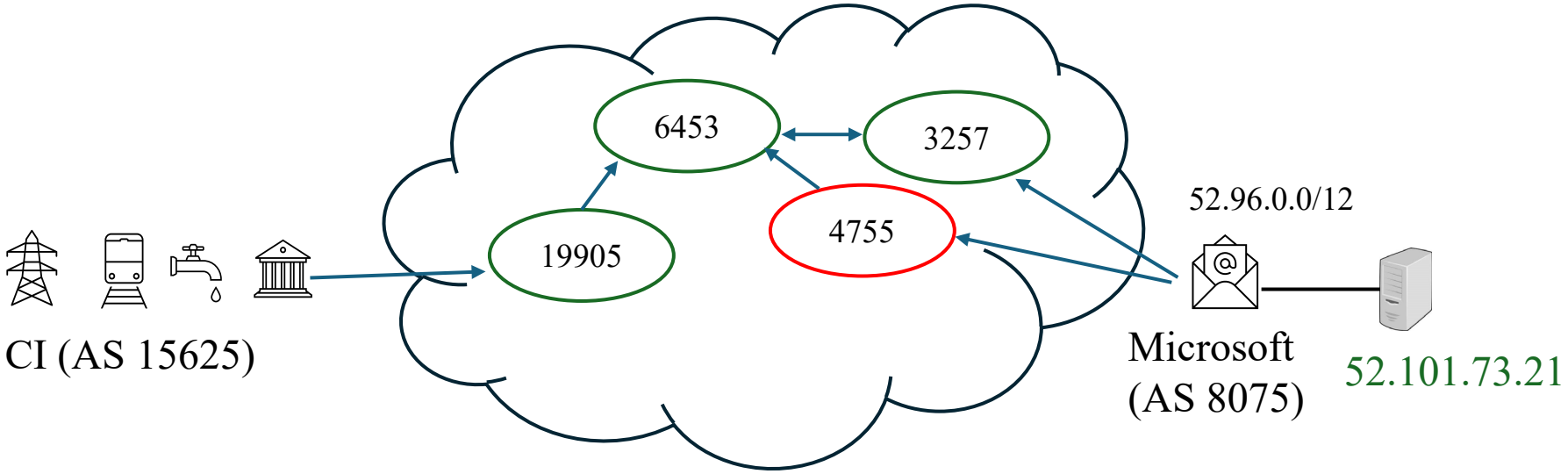


Prefix hijacking and Route Origin Validation

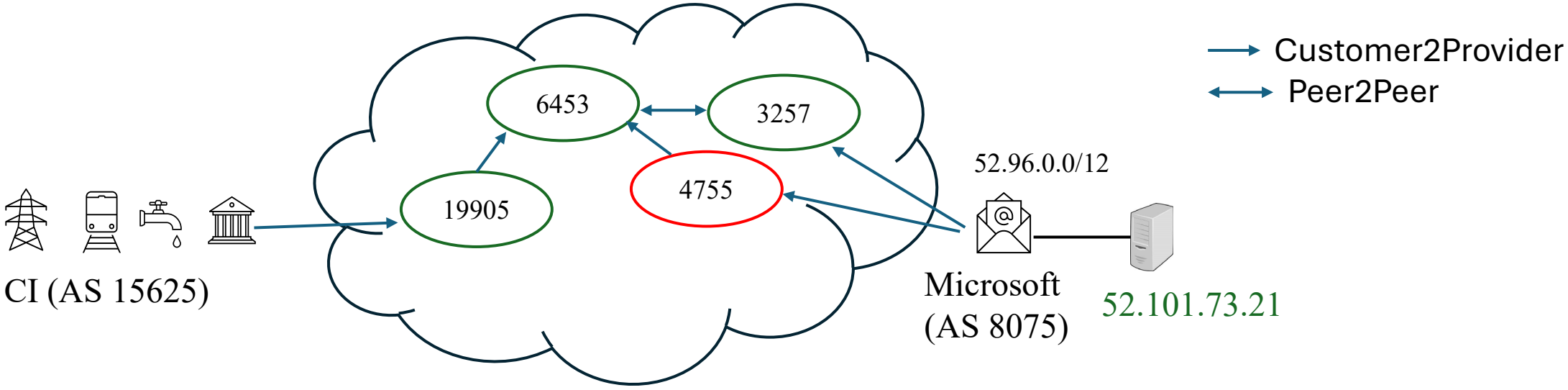


- ROV: A filter to check the list of the prefixes an AS is authorized to announce.
- If AS 4 implemented ROV, it would discard the route 5.5.5.0/25.

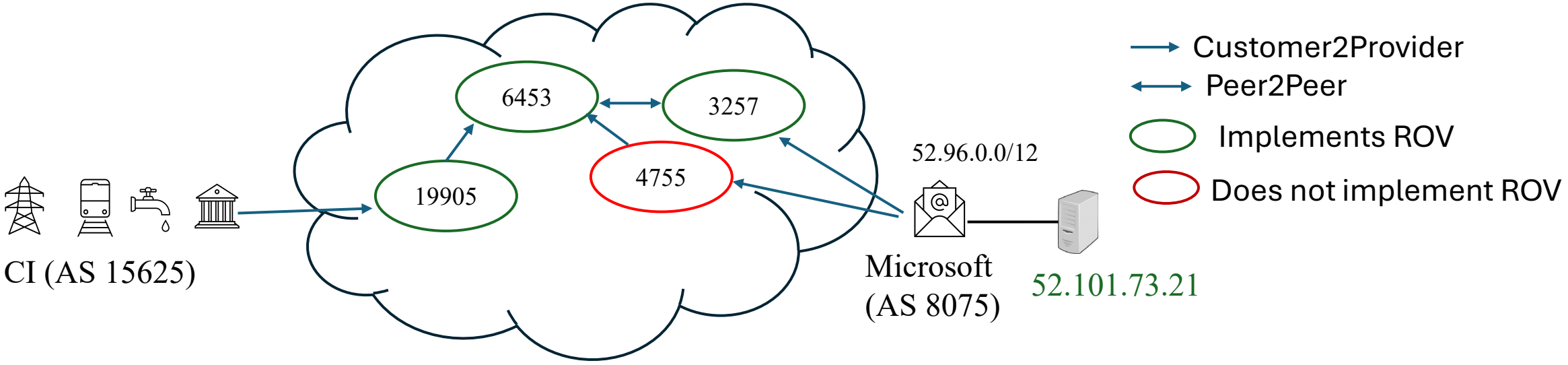
Importance of security insights for CIs



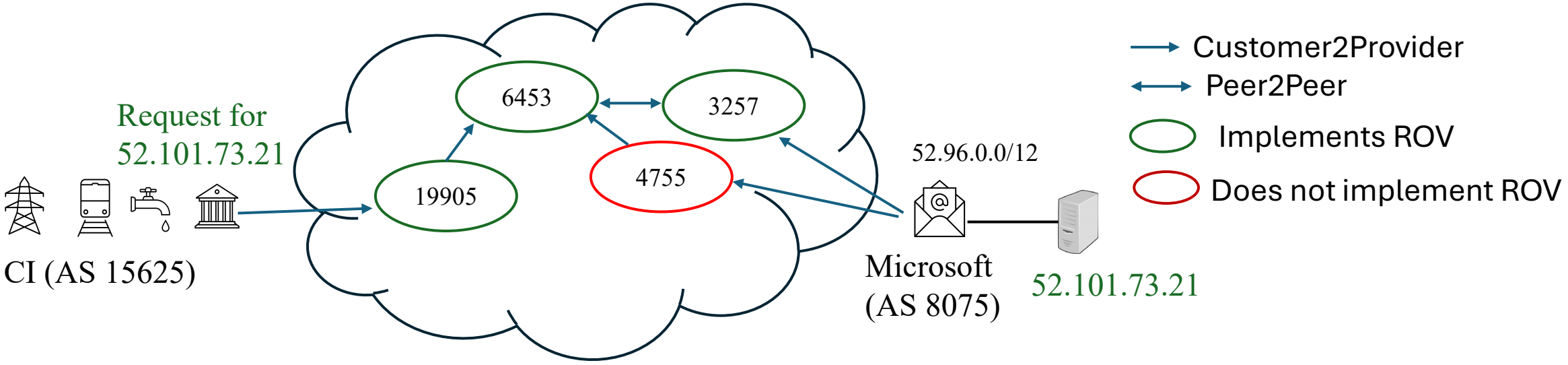
Importance of security insights for CIs



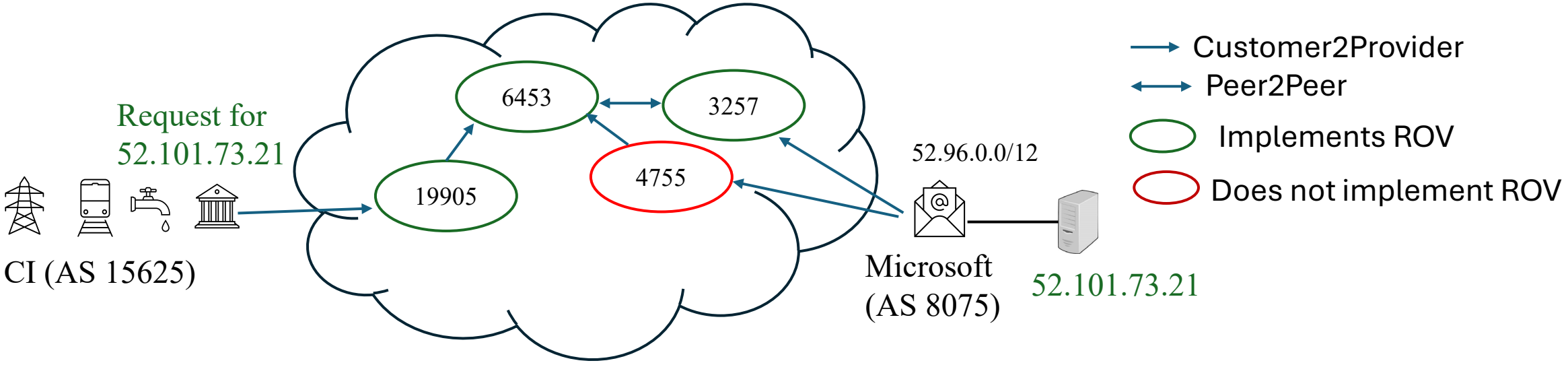
Importance of security insights for CIs



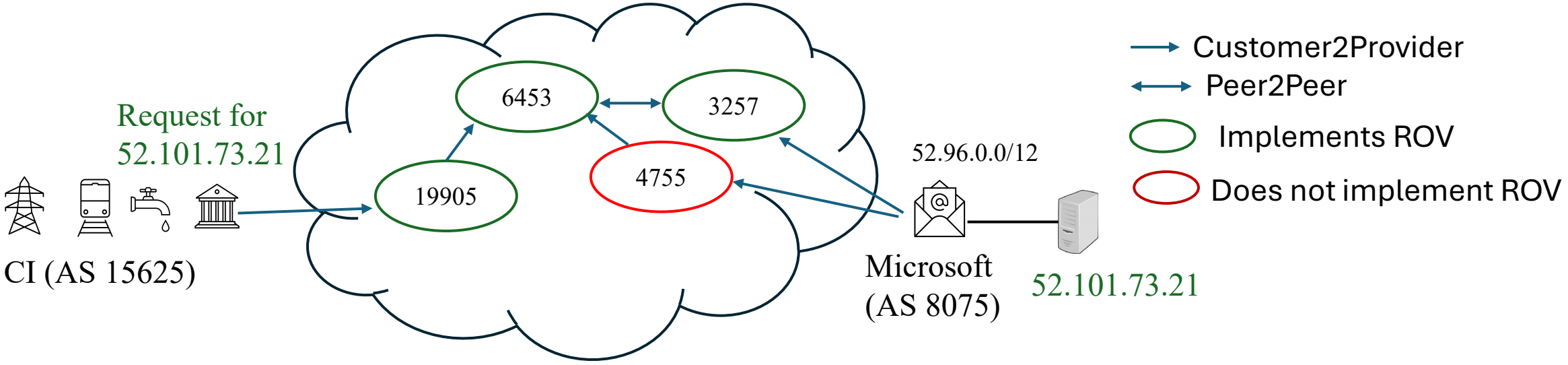
Importance of security insights for CIs



Importance of security insights for CIs

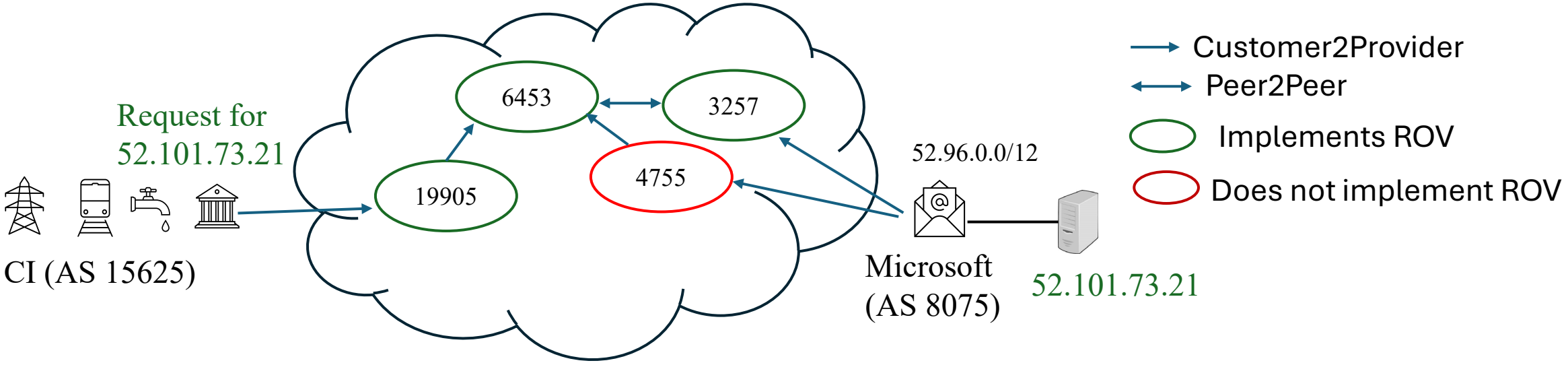


Importance of security insights for CIs



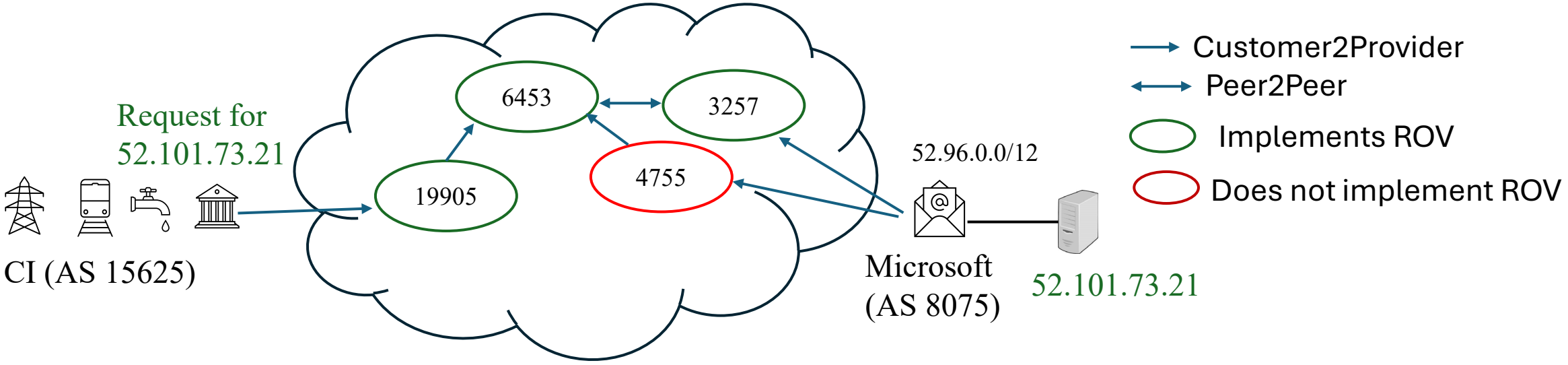
Path1: [15625, 19905, 6453, 3257, 8075]

Importance of security insights for CIs



Path1: [15625, 19905, 6453, 3257, 8075]

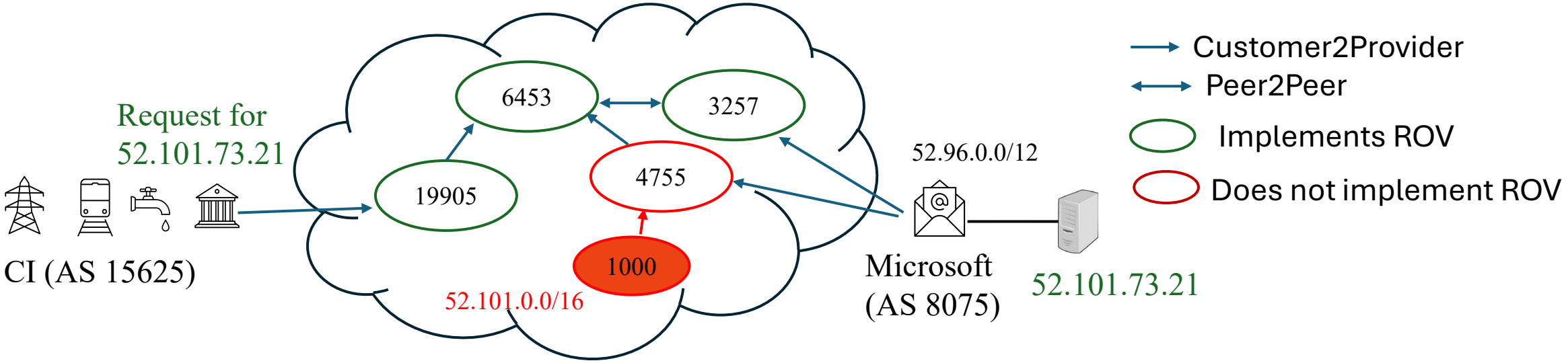
Importance of security insights for CIs



Path1: [15625, 19905, 6453, 3257, 8075]

Path2: [15625, 19905, 6453, 4755, 8075]

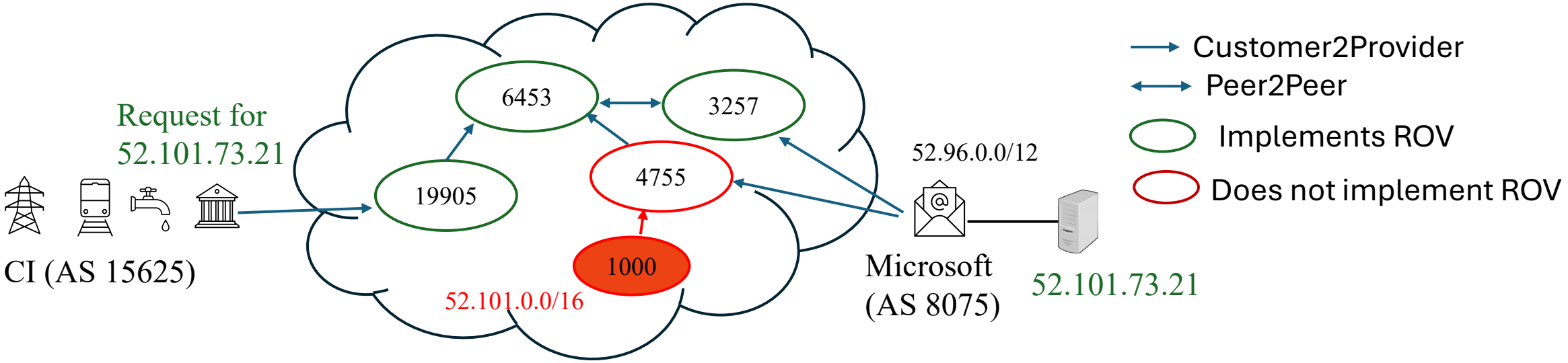
Importance of security insights for CIs



Path1: [15625, 19905, 6453, 3257, 8075]

Path2: [15625, 19905, 6453, 4755, 8075]

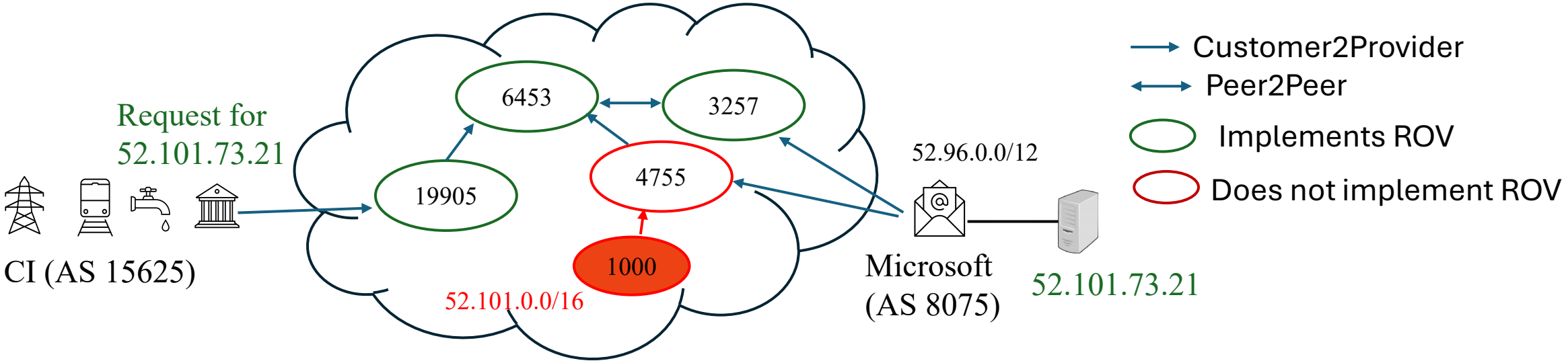
Importance of security insights for CIs



Path1: [15625, 19905, 6453, 3257, 8075]

Path2: [15625, 19905, 6453, 4755, 8075]

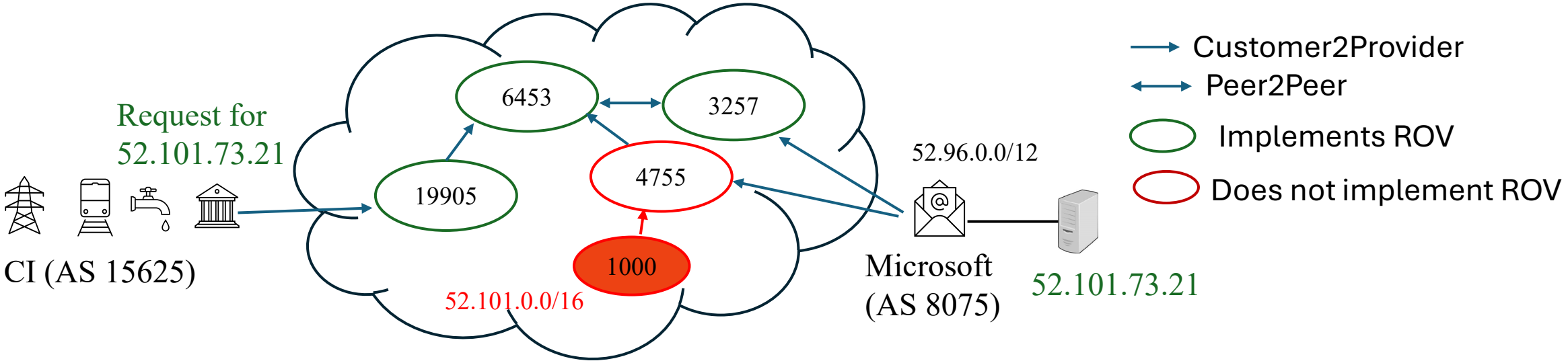
Importance of security insights for CIs



Path1: [15625, 19905, 6453, 3257, 8075]

Path2: [15625, 19905, 6453, 4755, 8075]

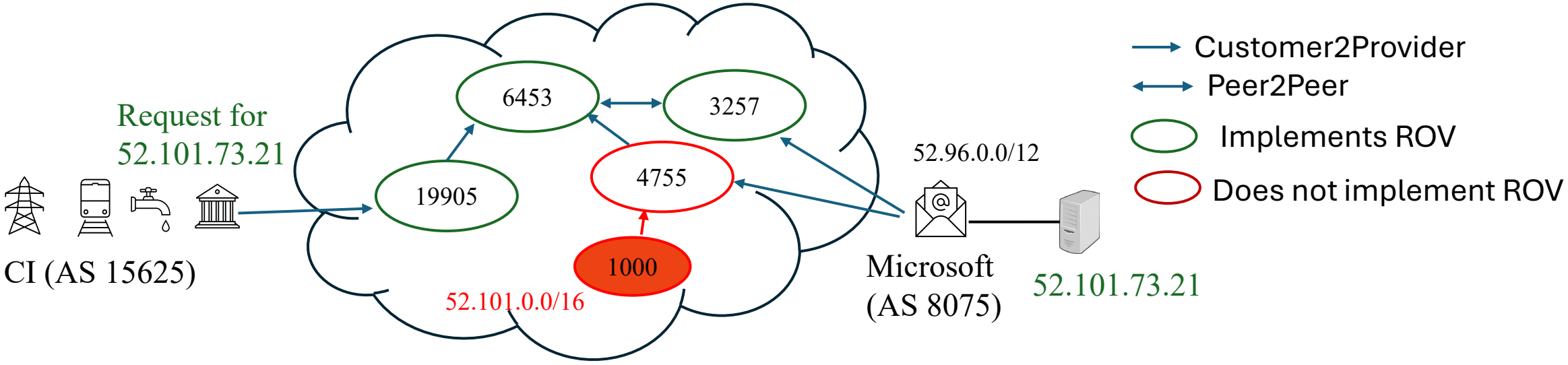
Importance of security insights for CIs



Path1: [15625, 19905, 6453, 3257, 8075]

Path2: [15625, 19905, 6453, 4755, 8075]

Importance of security insights for CIs

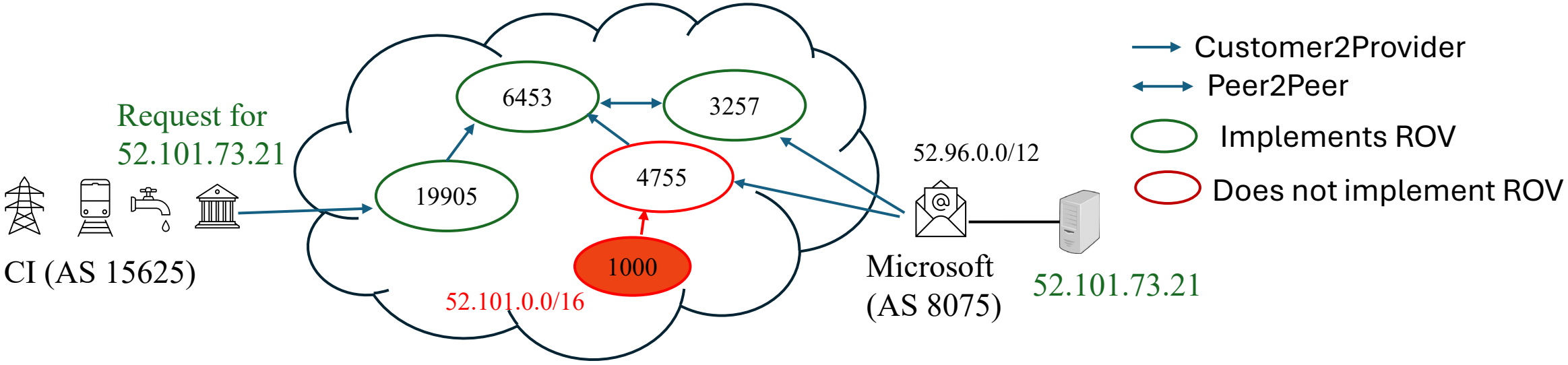


Path1: [15625, 19905, 6453, 3257, 8075]

Path2: [15625, 19905, 6453, 4755, 8075]

*Collateral damage: Path 2 is vulnerable to routing hijacks due to a single AS 4755.

Importance of security insights for CIs



Path1: [15625, 19905, 6453, 3257, 8075]

Path2: [15625, 19905, 6453, 4755, 8075]

*Collateral damage: Path 2 is vulnerable to routing hijacks due to a single AS 4755.

*Yossi Gilad, Avichai Cohen, Amir Herzberg, Michael Schapira, and Haya Shulman. 2016. Are we there yet? On RPKI's deployment and security. Cryptology ePrint Archive (2016)

Research questions

Research questions

i. What is the number of fully and partially ROV-protected paths through which the CI can connect to its cloud provider?

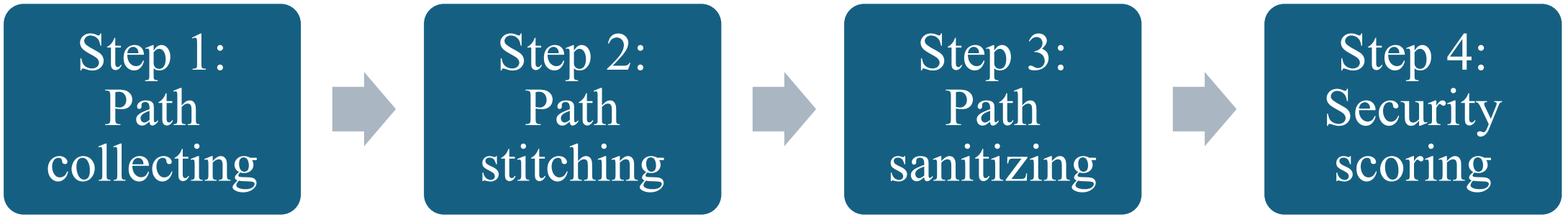
ii. What is the effect of a CI's upstream provider implementing ROV fully on the number of fully ROV-protected paths?

Research questions

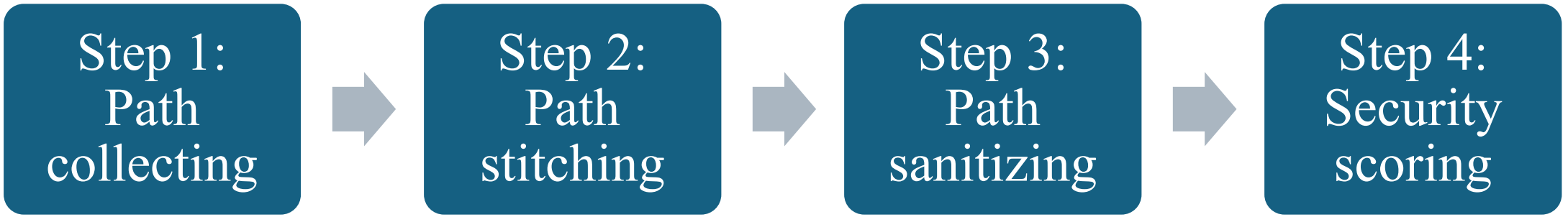
i. What is the number of fully and partially ROV-protected paths through which the CI can connect to its cloud provider?

ii. What is the effect of a CI's upstream provider implementing ROV fully on the number of fully ROV-protected paths?

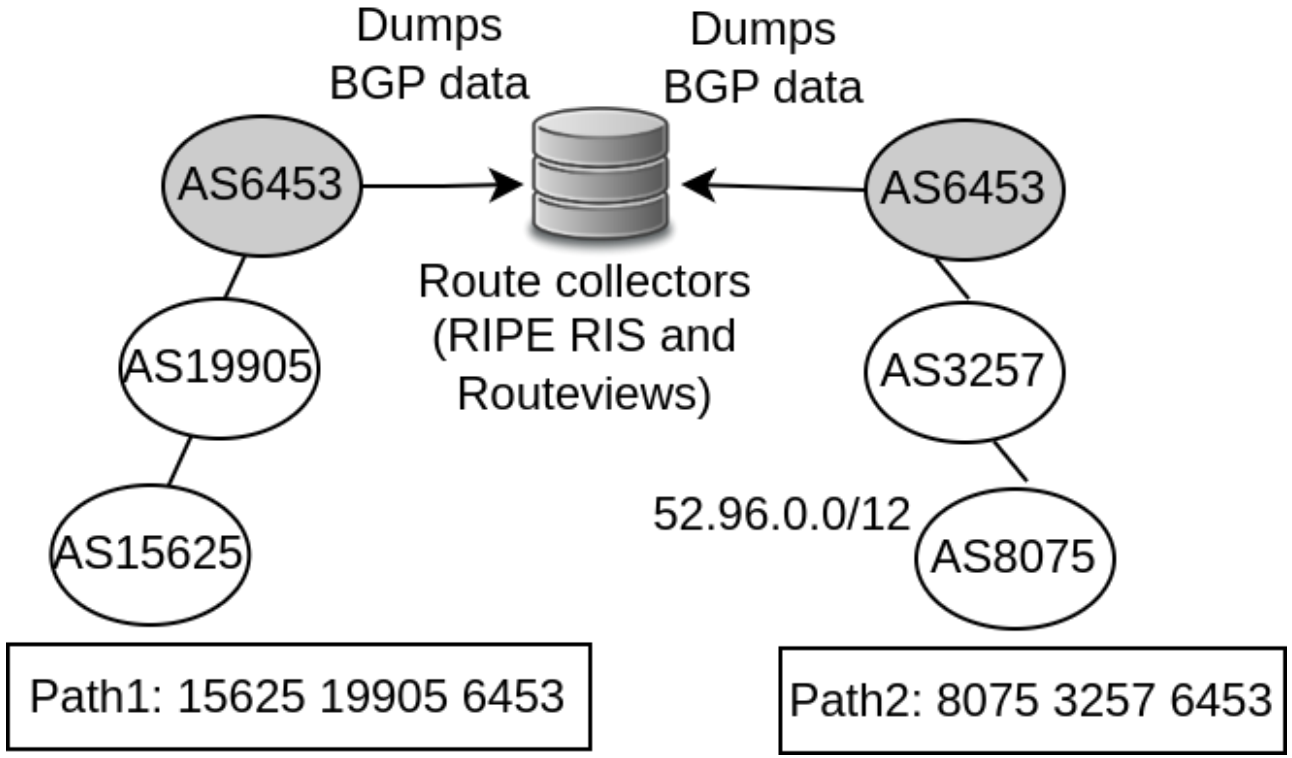
Approach


Step 1: Path collecting
Step 2: Path stitching
Step 3: Path sanitizing
Step 4: Security scoring

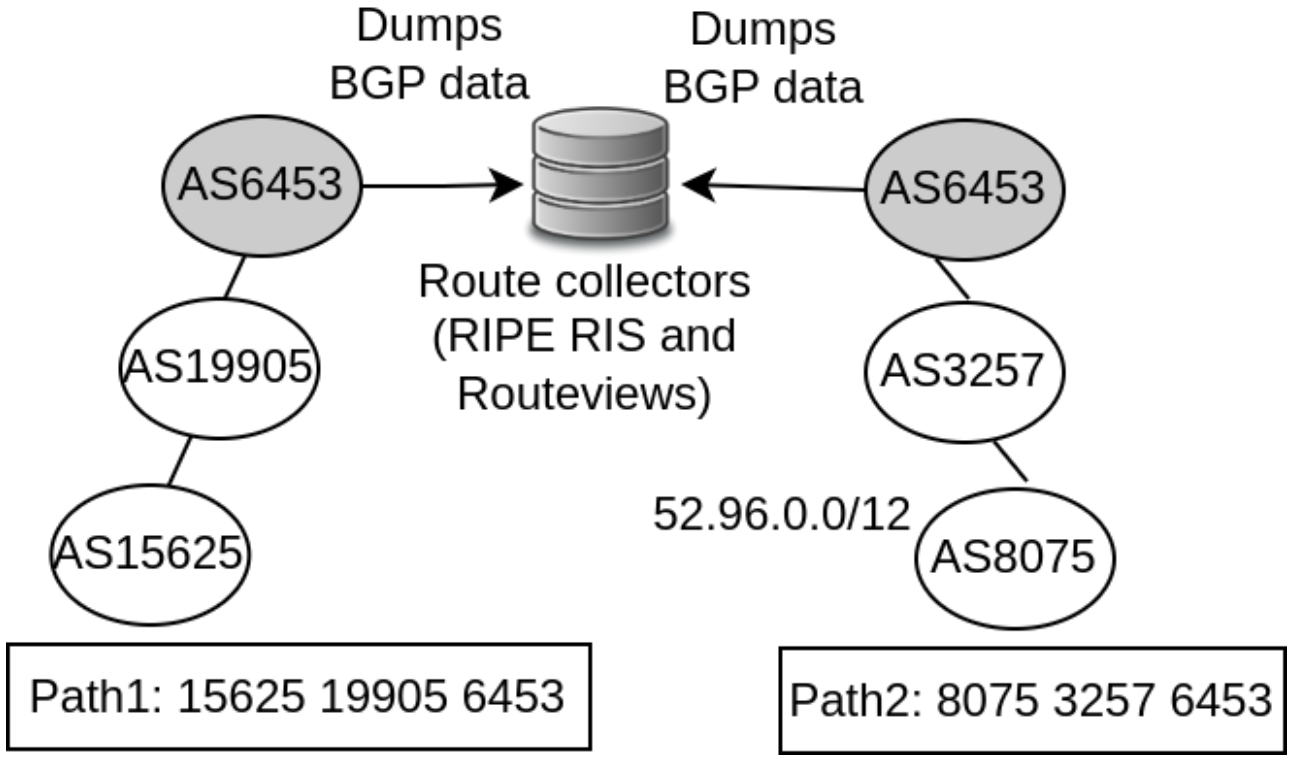
Approach


Step 1: Path collecting
Step 2: Path stitching
Step 3: Path sanitizing
Step 4: Security scoring

Step 1,2: Path collection and stitching



Step 1,2: Path collection and stitching



New path: 15625 19905 **6453** 3257 8075

Step 3: Path sanitizing

Step 3: Path sanitizing

- Find **valid paths** out of "New stitched path"
- Valid paths: prefix of a CI can reach its destination AS and vice versa
- Check Gao-Rexford's model of route export and Valley-free condition

Step 3: Path sanitizing

- Find **valid paths** out of "New stitched path"
- Valid paths: prefix of a CI can reach its destination AS and vice versa
- Check Gao-Rexford's model of route export and Valley-free condition

Step 3: Path sanitizing

- Find **valid paths** out of "New stitched path"
- Valid paths: prefix of a CI can reach its destination AS and vice versa
- Check Gao-Rexford's model of route export and Valley-free condition

Step 3: Path sanitizing

- Find **valid paths** out of "New stitched path"
- Valid paths: prefix of a CI can reach its destination AS and vice versa
- Check Gao-Rexford's model of route export and Valley-free condition

Standard route
export policy

Step 3: Path sanitizing

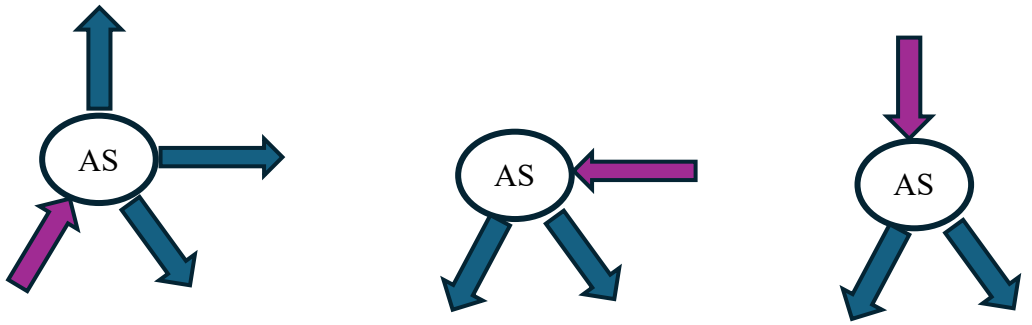
- Find **valid paths** out of "New stitched path"
- Valid paths: prefix of a CI can reach its destination AS and vice versa
- Check Gao-Rexford's model of route export and Valley-free condition

Standard route export policy

providers

peers

customers



Step 3: Path sanitizing

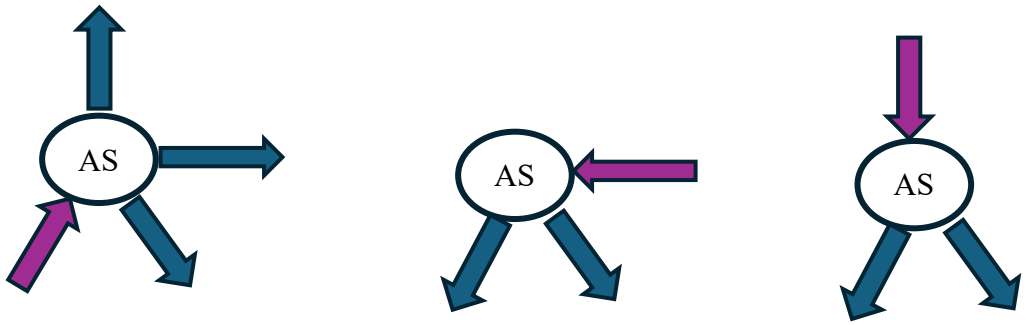
- Find **valid paths** out of "New stitched path"
- Valid paths: prefix of a CI can reach its destination AS and vice versa
- Check Gao-Rexford's model of route export and Valley-free condition

Standard route export policy

providers

peers

customers



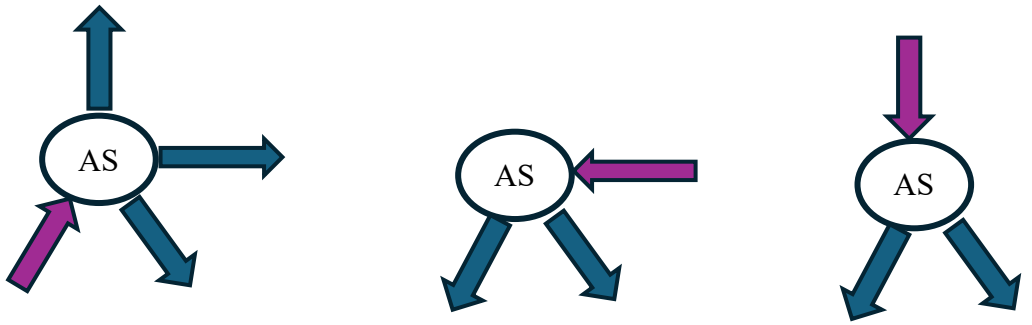
Valley-free condition

Step 3: Path sanitizing

- Find **valid paths** out of "New stitched path"
- Valid paths: prefix of a CI can reach its destination AS and vice versa
- Check Gao-Rexford's model of route export and Valley-free condition

Standard route export policy

providers
peers
customers



Valley-free condition

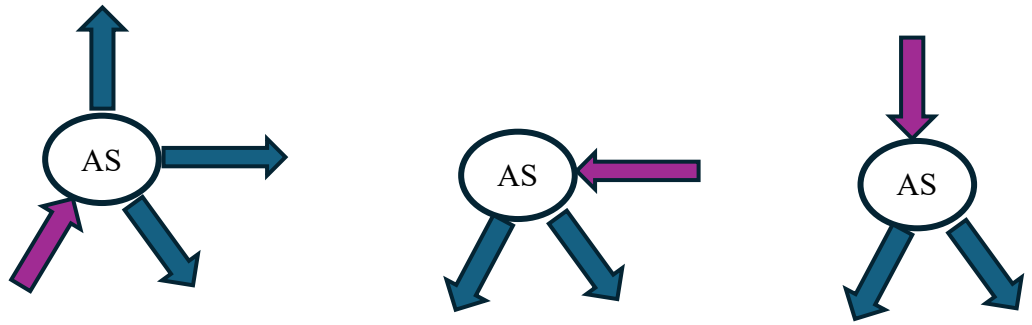
i. at most one P2P link exists in the path
ii. a P2C link not followed by a C2P or P2P link
iii. a P2P link not followed by a C2P link.

Step 3: Path sanitizing

- Find **valid paths** out of "New stitched path"
- Valid paths: prefix of a CI can reach its destination AS and vice versa
- Check Gao-Rexford's model of route export and Valley-free condition

Standard route export policy

providers
peers
customers



Valley-free condition

i. at most one P2P link exists in the path
ii. a P2C link not followed by a C2P or P2P link
iii. a P2P link not followed by a C2P link.

Path *[15625 19905 6453 3257 8075]* has *[C2P, C2P, P2P, P2C]* -> **Valid**

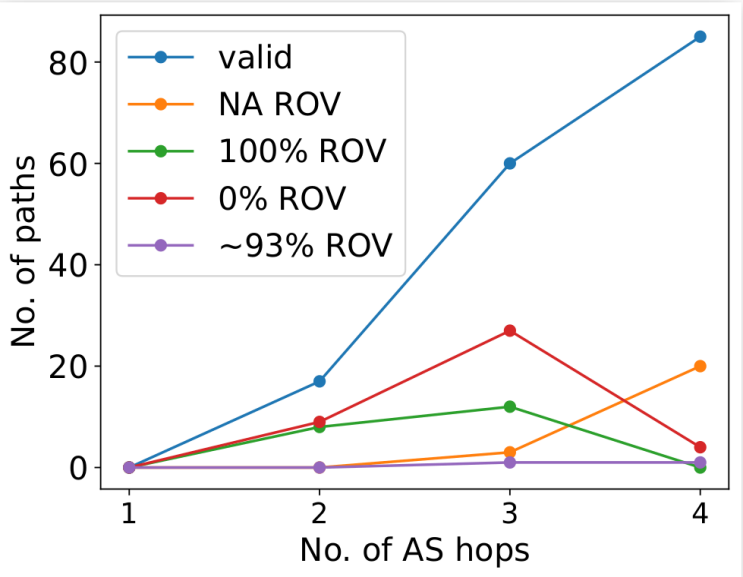
Step 4: Security scoring

- **Use ROV as a metric for security scoring**
- Determine ROV scores of each AS on an AS path using RoVista

Paths	ROV scores of each AS	Path ROV scores
1. *[15625 19905 6453 3257 8075]*	*[0 100 100 100 100]*	**100**
2. *[15625 19905 6453 4755 8075]*	*[0 100 100 0 100]*	**0**
3. *[15625,702,1299,4826,8075]*	*[0 100 100 92.86 100]*	**92.86**
4. *[15625,19905,22822,3491,8075]*	*[0 100 NA 100 100]*	**NA**

Case study in the Netherlands

Four CIs: ING bank, ABN-Amro bank, Vitens (Water supply company), Eneco (Energy supply company)

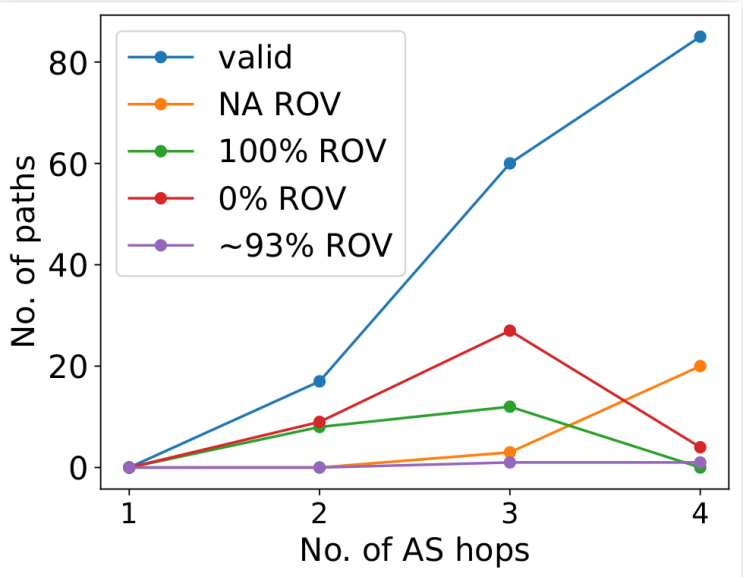


Bank

Multi-homed AS with four providers with a large number of paths. Many ROV-unprotected paths than protected.

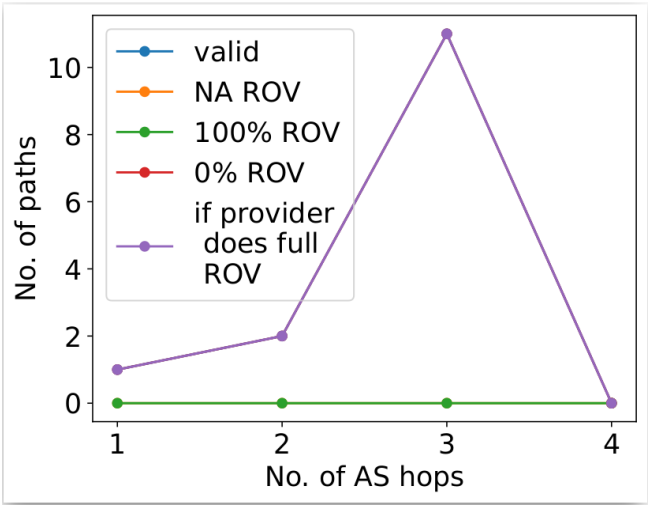
Case study in the Netherlands

Four CIs: ING bank, ABN-Amro bank, Vitens (Water supply company), Eneco (Energy supply company)



Bank

Multi-homed AS with four providers with a large number of paths. Many ROV-unprotected paths than protected.



Energy

Implementing ROV by its provider will result in all its 14 valid paths to be ROV-protected

Group of ASes to forward CI's traffic

CIs	No. of paths with 100% ROV	No. of unique ASes on those paths
Bank1	85	15
Water	13	10
Energy	14	12
Bank2	15	13

Group of ASes to forward CI's traffic

CIs	No. of paths with 100% ROV	No. of unique ASes on those paths
Bank1	85	15
Water	13	10
Energy	14	12
Bank2	15	13

- If 15 ASes form a group to forward CI's traffic, number of ROV-protected paths will increase.
- ASes could also offer such concepts as a value-added service to their customers along with visualizations to provide easy insight into paths.

Group of ASes to forward CI's traffic

CIs	No. of paths with 100% ROV	No. of unique ASes on those paths
Bank1	85	15
Water	13	10
Energy	14	12
Bank2	15	13

- If 15 ASes form a group to forward CI's traffic, number of ROV-protected paths will increase.
- ASes could also offer such concepts as a value-added service to their customers along with visualizations to provide easy insight into paths.

Group of ASes to forward CI's traffic

CIs	No. of paths with 100% ROV	No. of unique ASes on those paths
Bank1	85	15
Water	13	10
Energy	14	12
Bank2	15	13

- If 15 ASes form a group to forward CI's traffic, number of ROV-protected paths will increase.
- ASes could also offer such concepts as a value-added service to their customers along with visualizations to provide easy insight into paths.

Takeaways

Takeaways

- Developed a method to calculate the security status of a path in combination with path-finding
- Implementing ROV fully by upstream providers of CIs will increase the number of fully ROV-protected paths
- Future work: investigating the effects on path-finding using additional geographically diverse route collectors

Takeaways

- Developed a method to calculate the security status of a path in combination with path-finding
- Implementing ROV fully by upstream providers of CIs will increase the number of fully ROV-protected paths
- Future work: investigating the effects on path-finding using additional geographically diverse route collectors

Takeaways

- Developed a method to calculate the security status of a path in combination with path-finding
- Implementing ROV fully by upstream providers of CIs will increase the number of fully ROV-protected paths
- Future work: investigating the effects on path-finding using additional geographically diverse route collectors

Takeaways

- Developed a method to calculate the security status of a path in combination with path-finding
- Implementing ROV fully by upstream providers of CIs will increase the number of fully ROV-protected paths
- Future work: investigating the effects on path-finding using additional geographically diverse route collectors

Thank you!

s.k.khadka@utwente.nl

Takeaways

- Developed a method to calculate the security status of a path in combination with path-finding
- Implementing ROV fully by upstream providers of CIs will increase the number of fully ROV-protected paths
- Future work: investigating the effects on path-finding using additional geographically diverse route collectors

Thank you!

s.k.khadka@utwente.nl

Paper

Source code

APNIC Blog

This work was conducted as part of the project CATRIN (www.catrin.nl) which received funding from the Dutch Research Council (NWO).