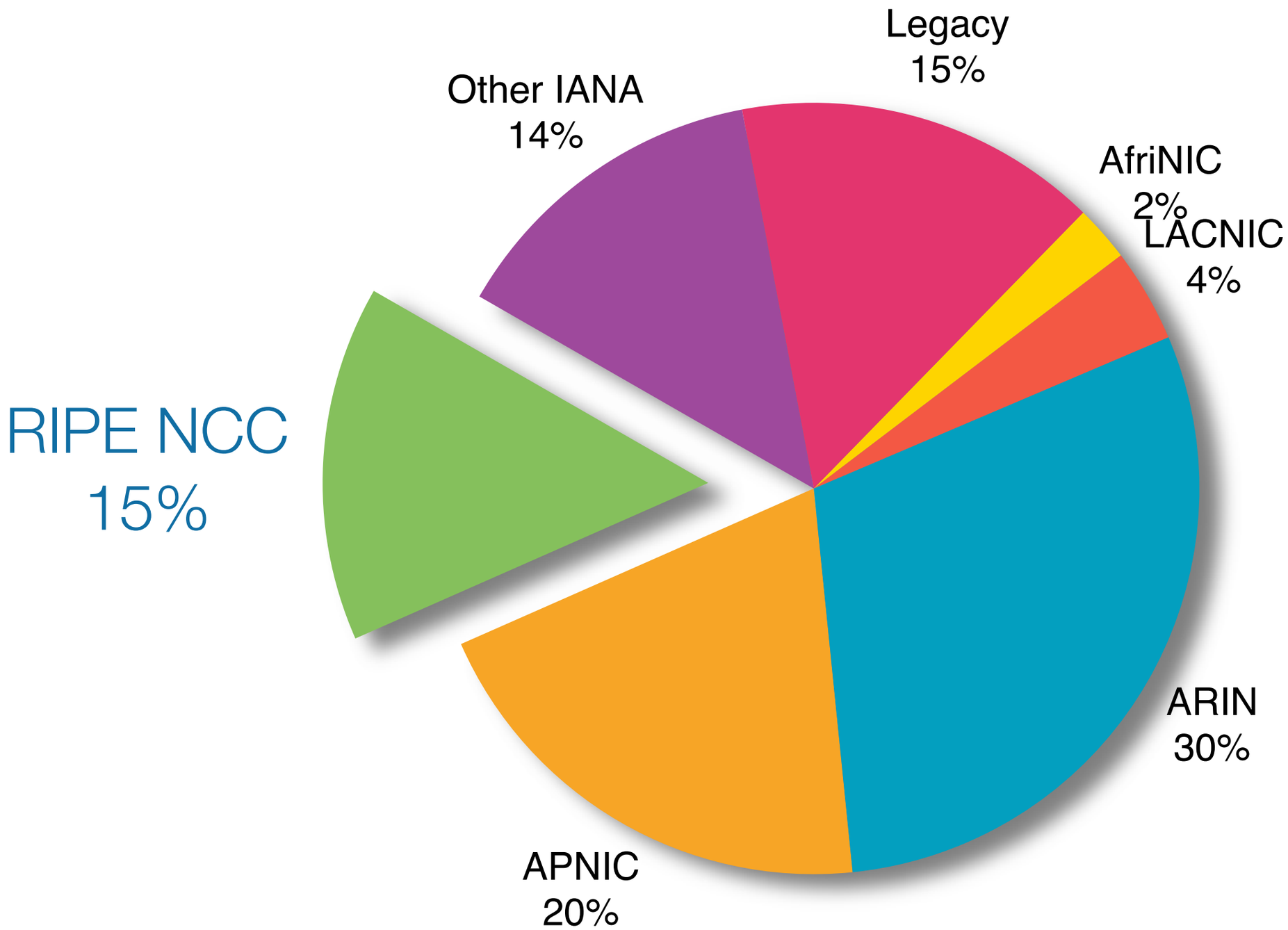
RIPE NCC IPv4 Pool



Marco Hogewoning

IP Hijacking

Securing Internet Routing

Marco Hogewoning
Training Services

Never attribute to malice that which is adequately explained by stupidity.

-- Robert J Hanlon

Why Would You Hijack?

- Sending spam or malware unnoticed
- Intercept traffic to a specific host
- Sell the resources

Two Targets for Hijacking

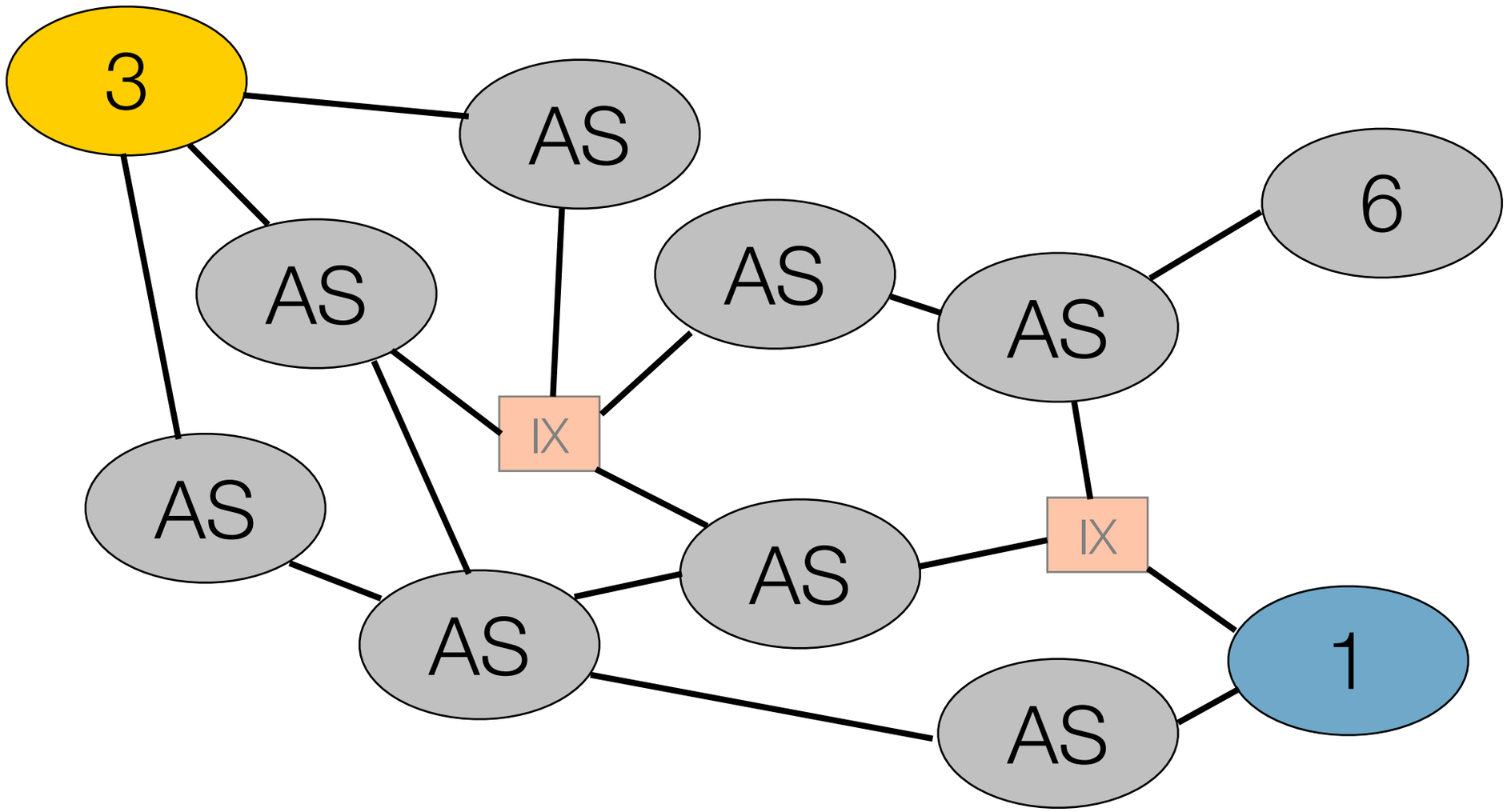
- The Internet routing table
  - Influence how traffic flows by manipulating BGP
- The Internet registry
  - Possibly manipulating BGP filters
  - Hide or change ownership details

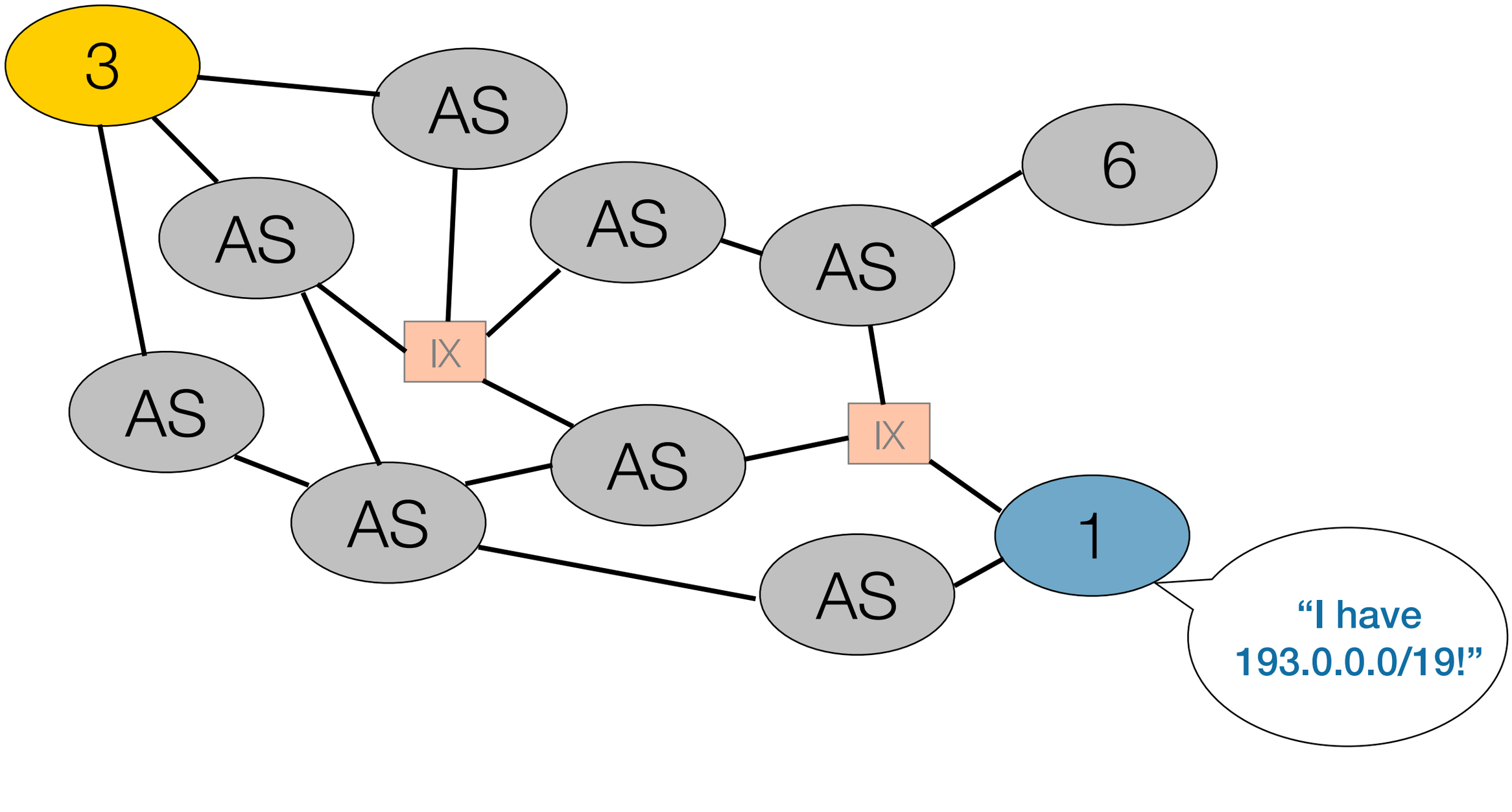
Internet Routing

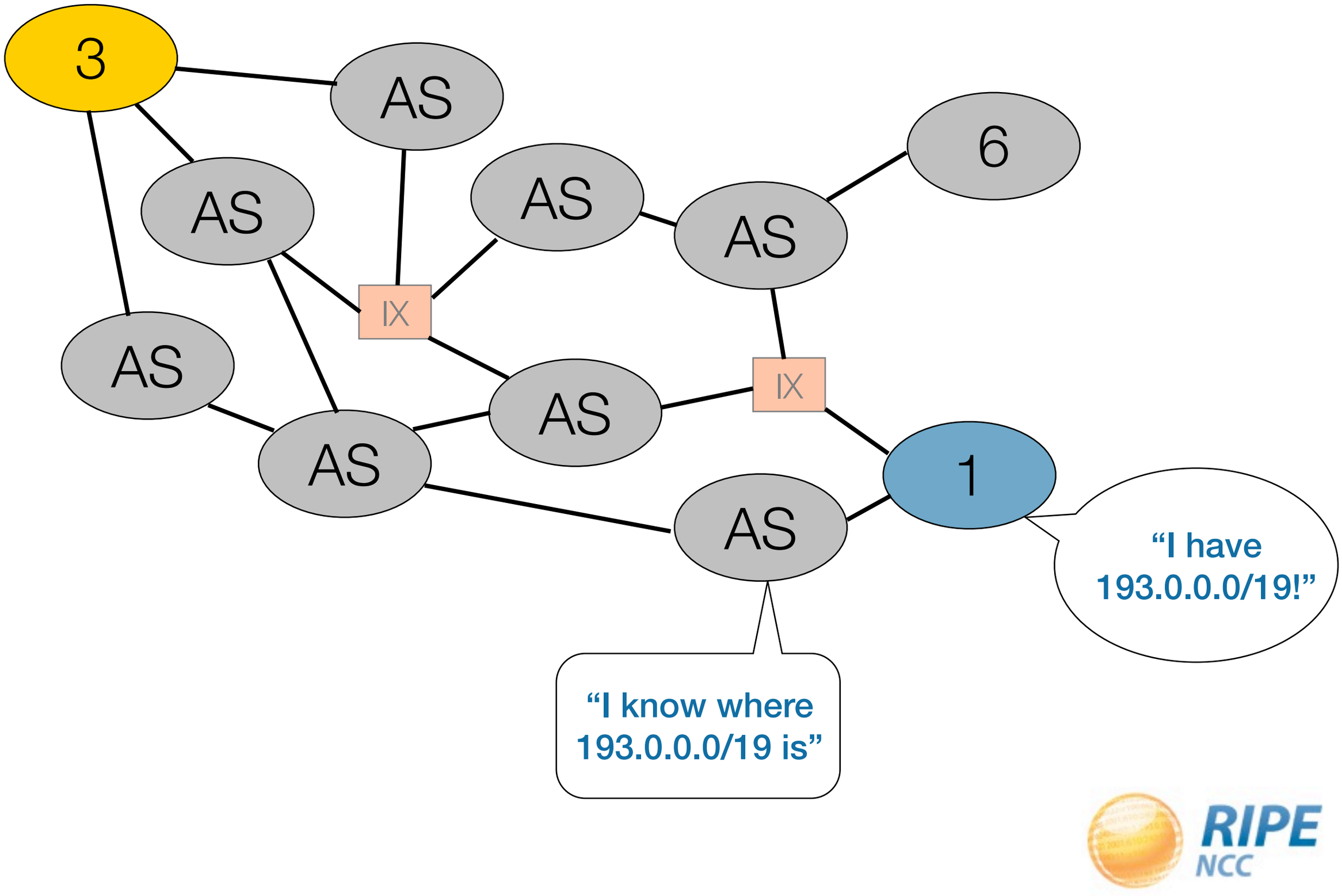
- Non hierarchical
- The internet registries only have limited control
  - It's the operator who decides
  - We can only offer some guidance
- Internet Routing Registry
  - Integrated in the RIPE Database
  - Ties together a prefix and an ASN
- RPKI Certification
  - ROAs couple a prefix and an ASN

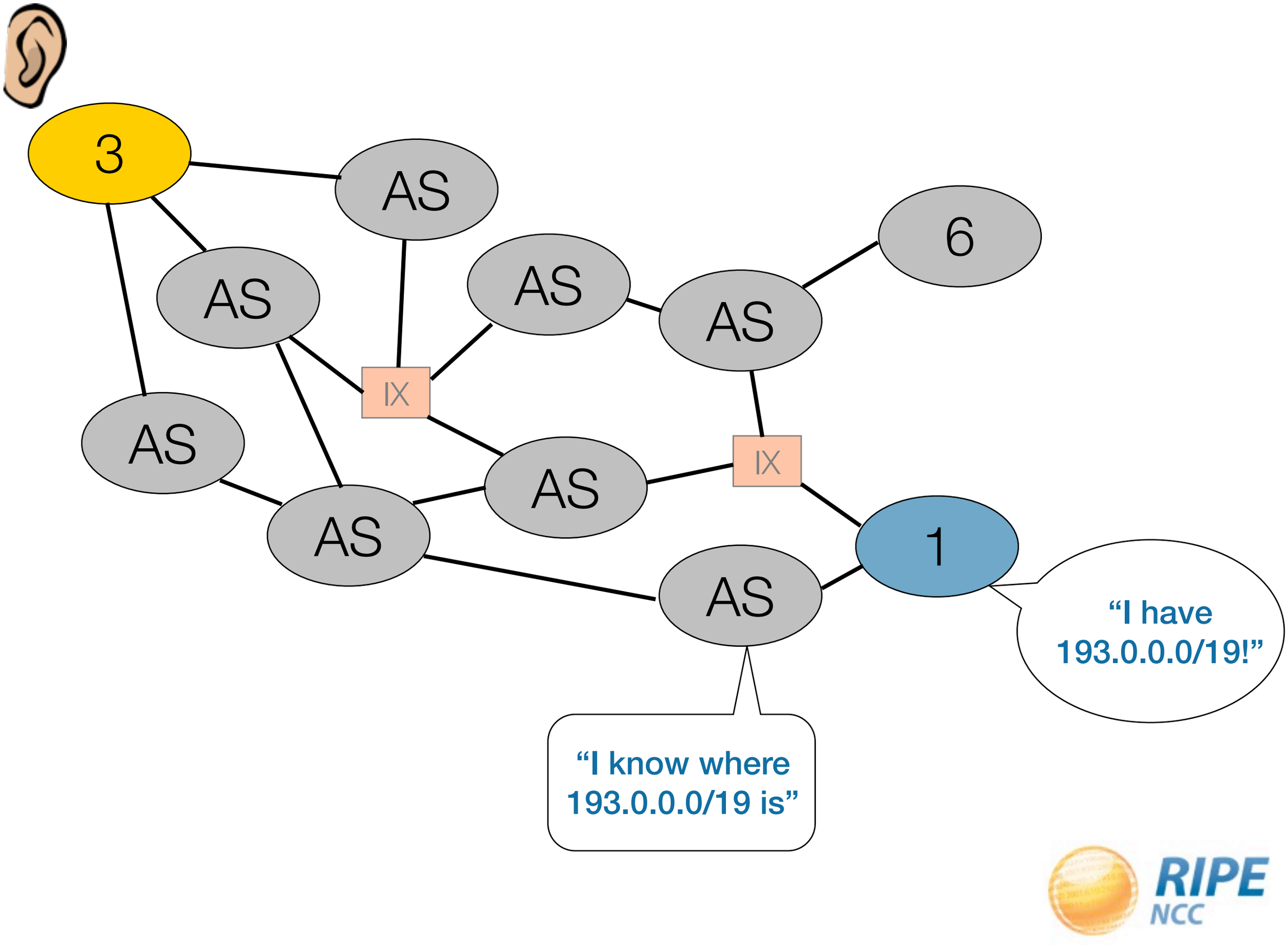
Decision Making in Routing

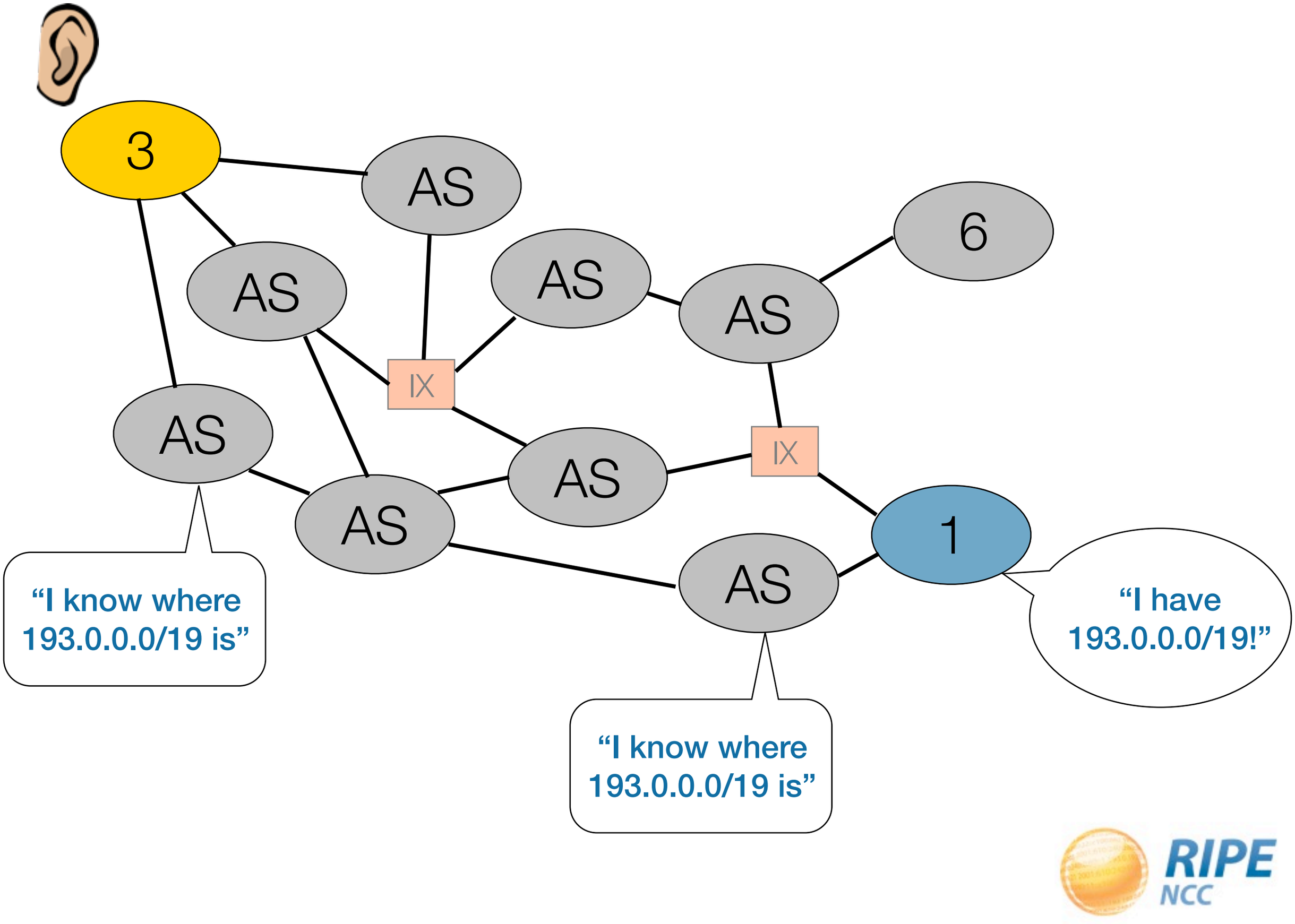
- Unless preferences dictate otherwise, a router will pick the shortest path
- A more specific route will always take preference
- Filtering usually only done at the edge of the Internet
  - Filtering in the core of the Internet is far too complex and costly to achieve
- Most filters are based on IP ranges
  - Input can come from the IRR

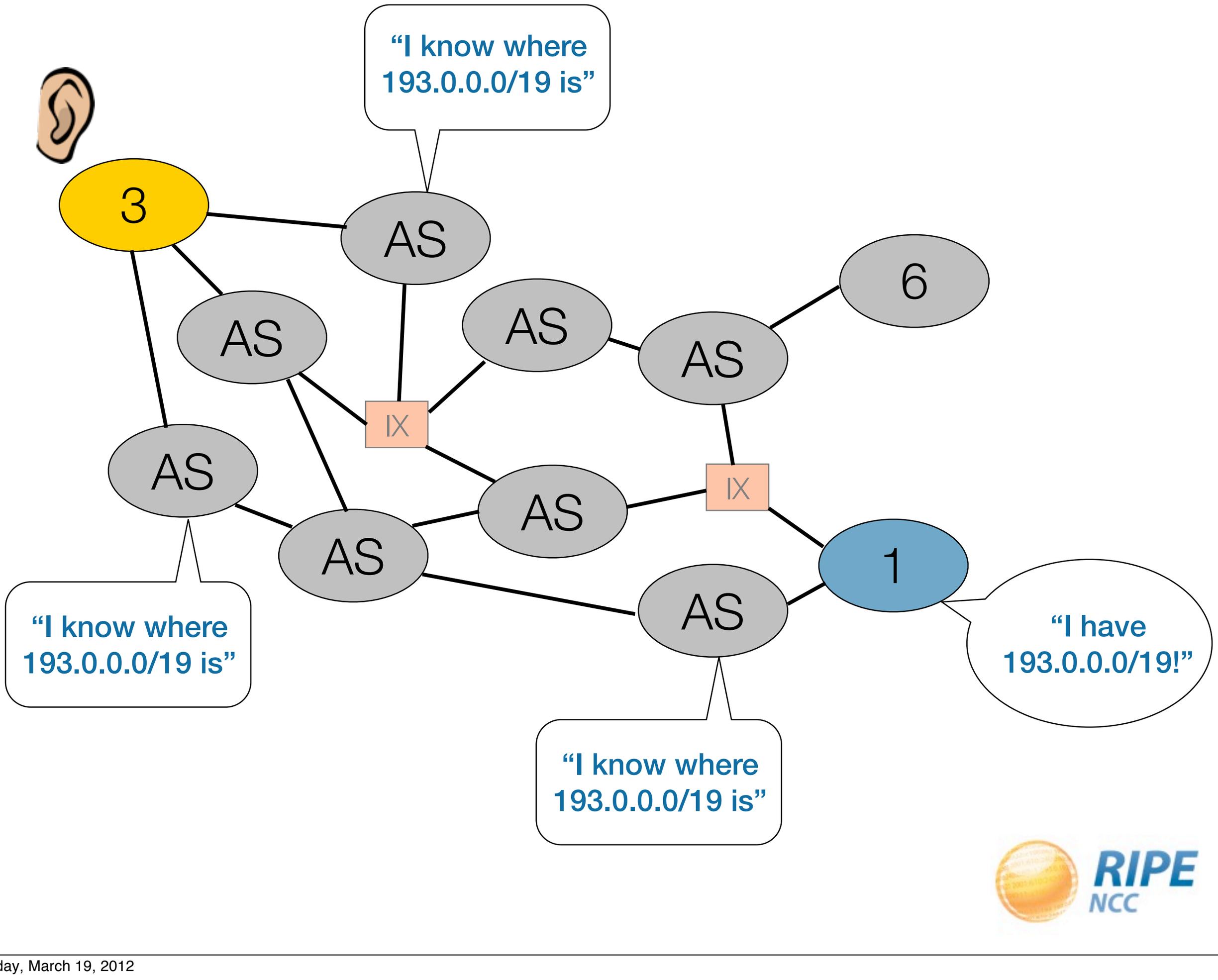

3
AS
AS
AS
AS
6
IX
AS
AS
IX
AS
1
AS

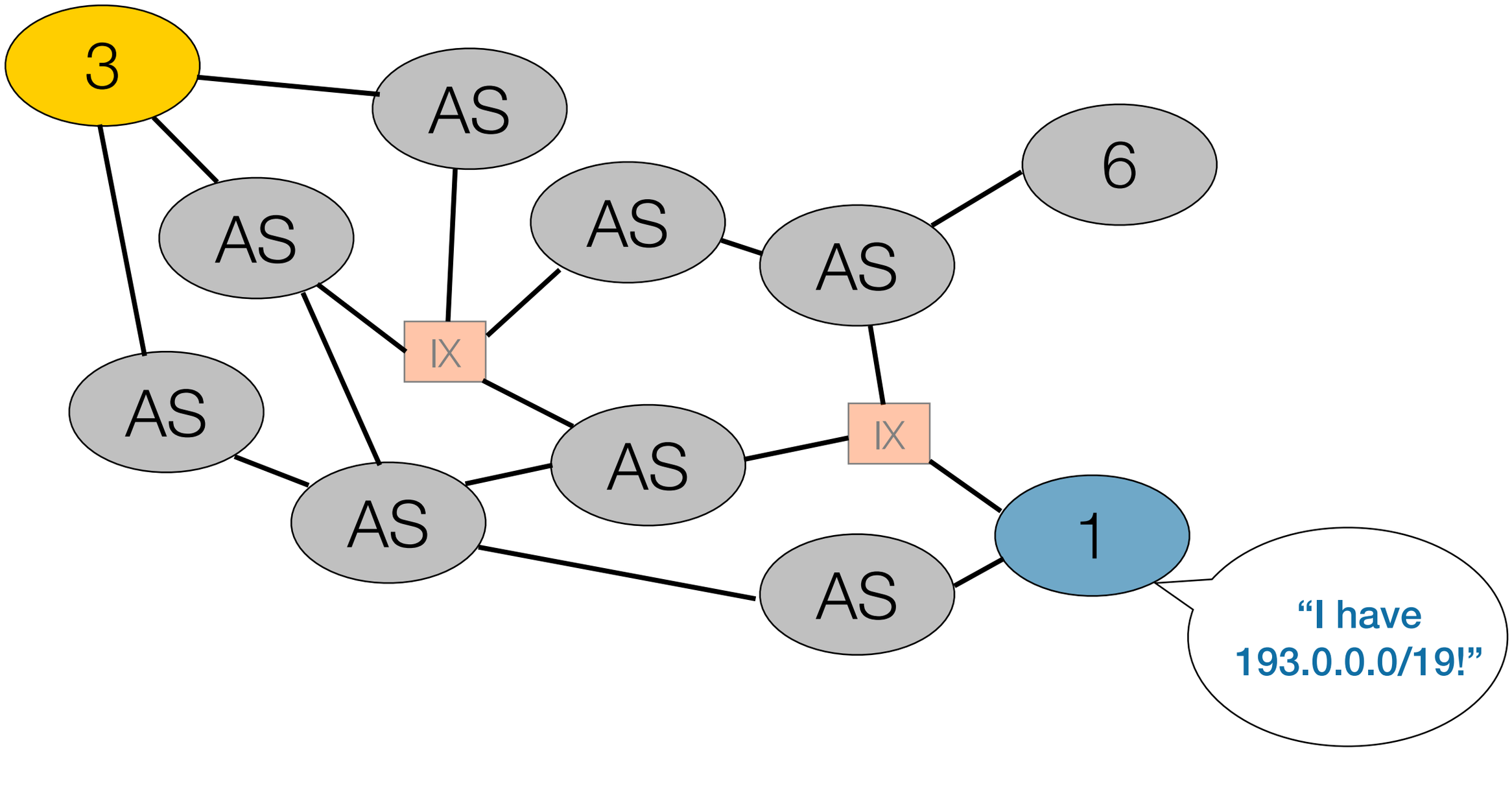

3
AS
AS
AS
AS
6
IX
AS
AS
AS
IX
1
AS
“I have 193.0.0.0/19!”

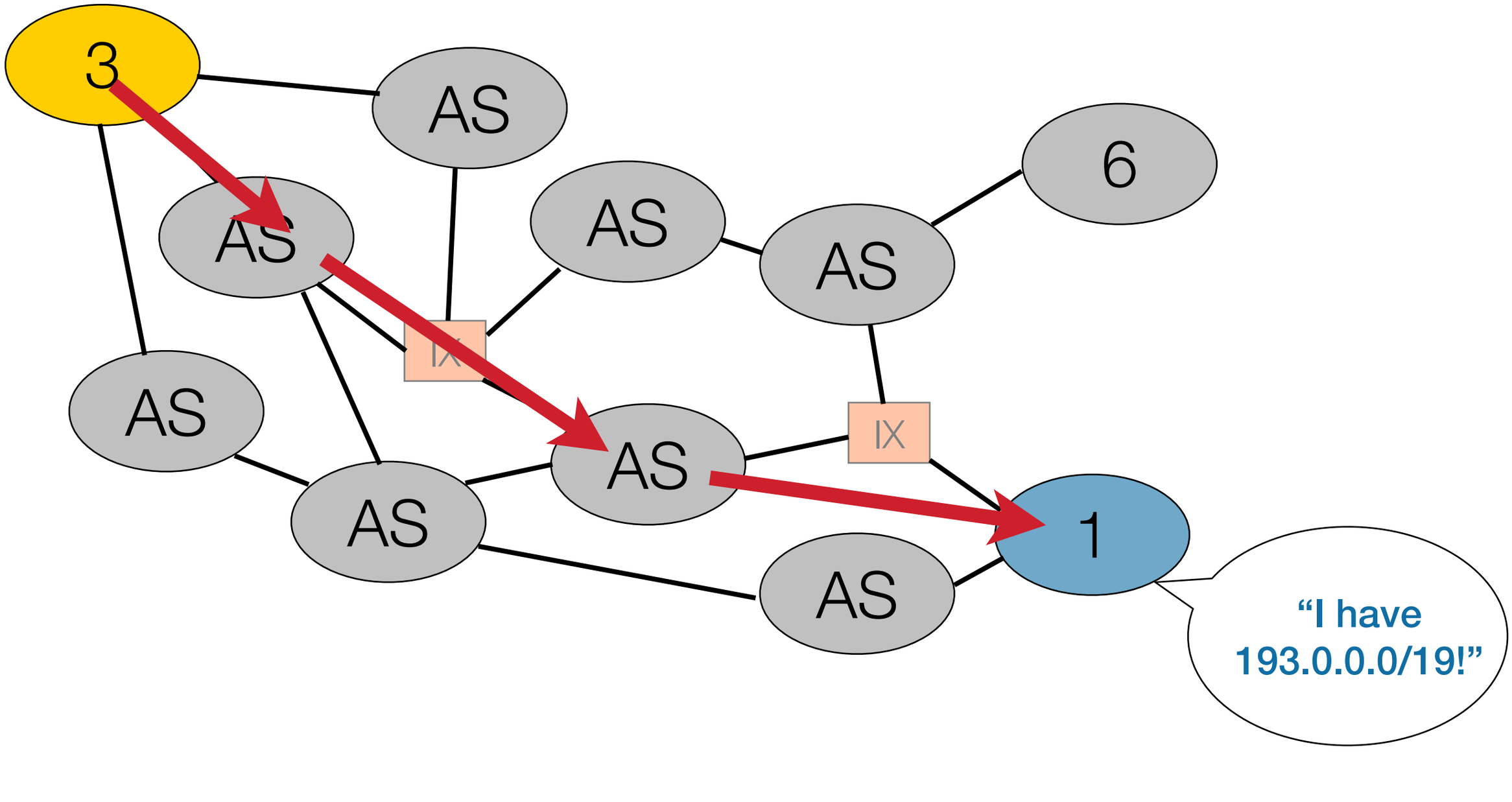

3
AS
AS
AS
AS
6
AS
IX
AS
AS
IX
1
AS
"I have 193.0.0.0/19!"
"I know where 193.0.0.0/19 is"

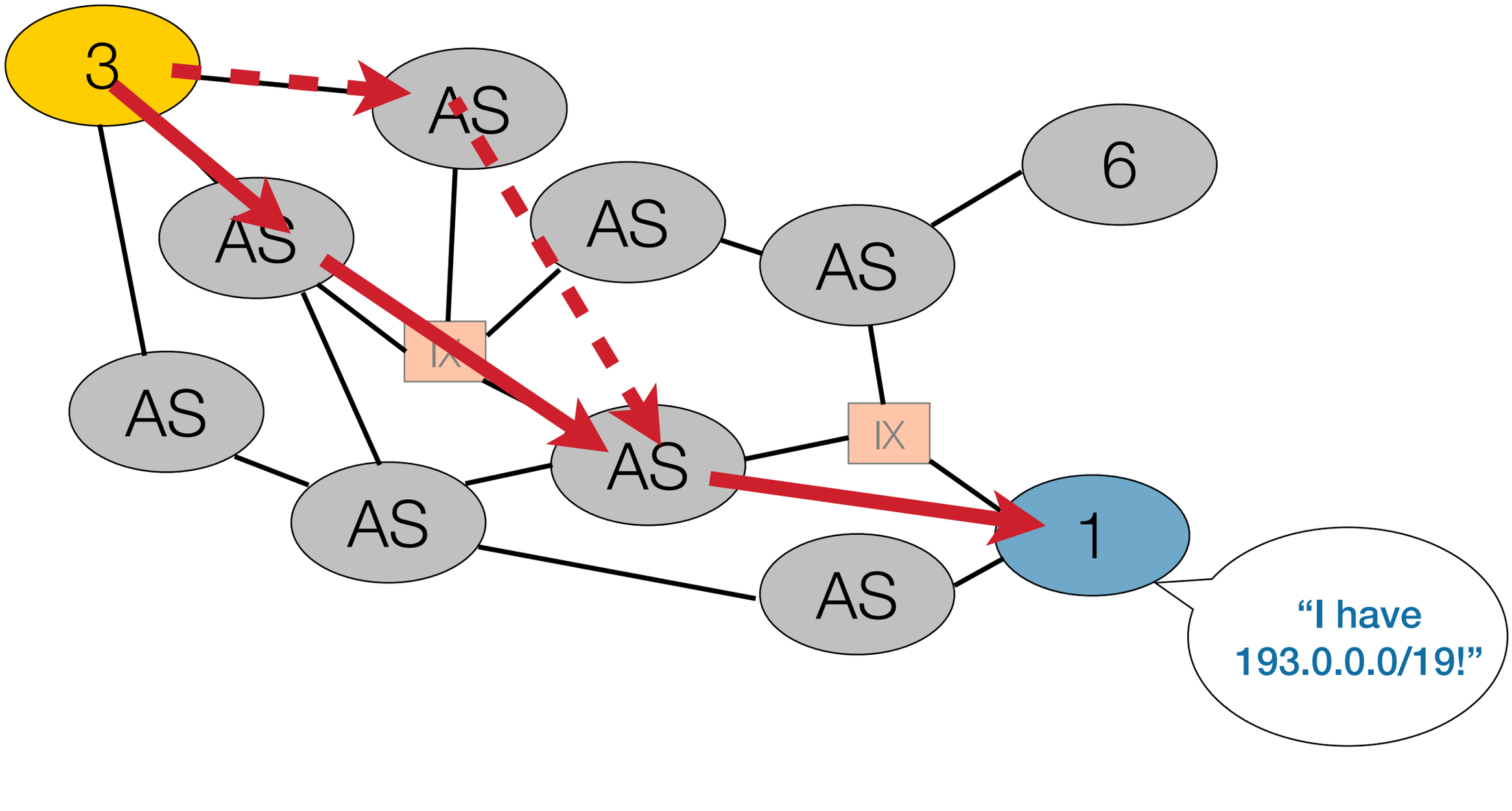

3
AS
AS
AS
AS
6
AS
IX
AS
AS
IX
1
AS
"I have 193.0.0.0/19!"
"I know where 193.0.0.0/19 is"

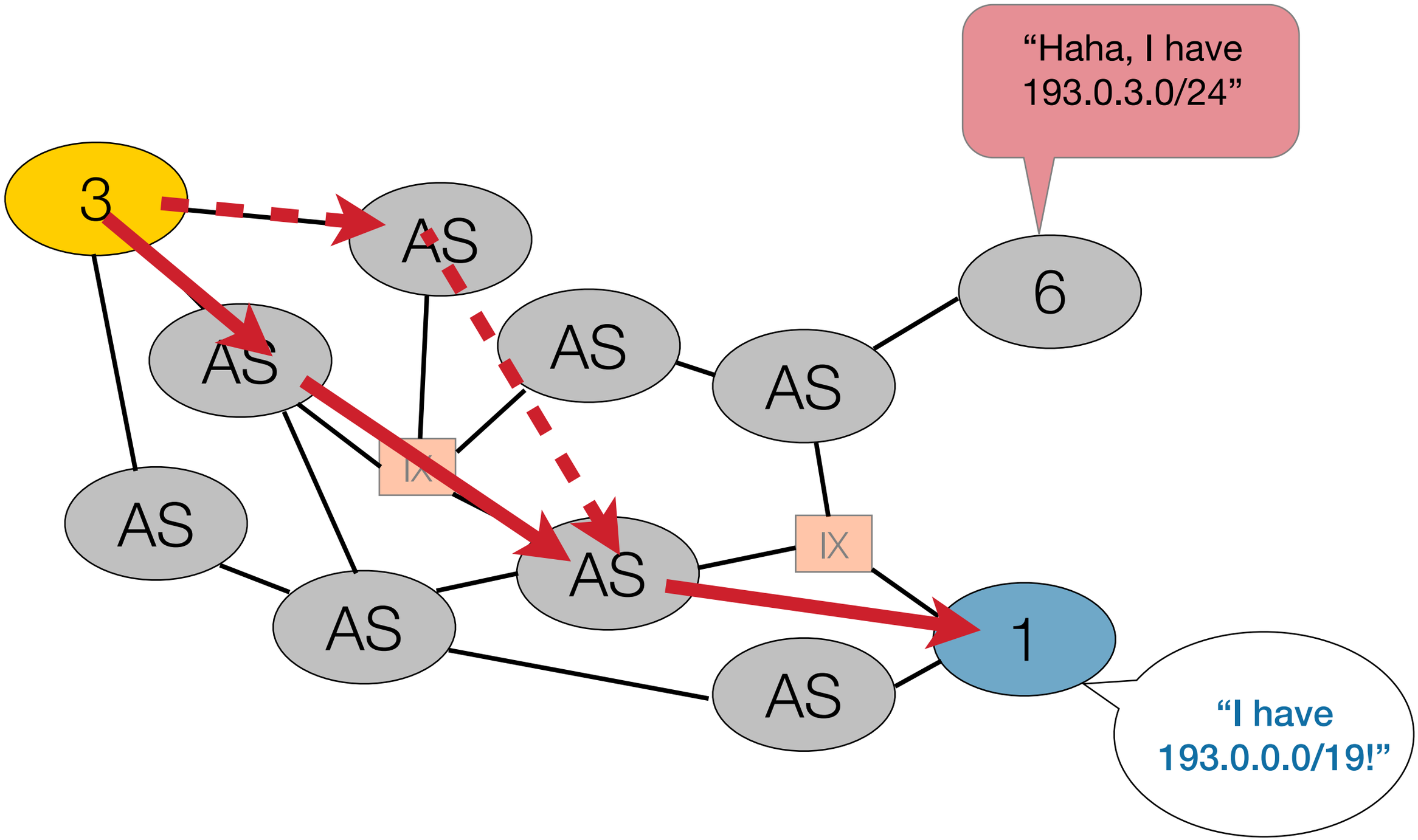

3
AS
AS
AS
AS
6
AS
IX
AS
AS
IX
1
AS
"I know where 193.0.0.0/19 is"
"I know where 193.0.0.0/19 is"
"I have 193.0.0.0/19!"

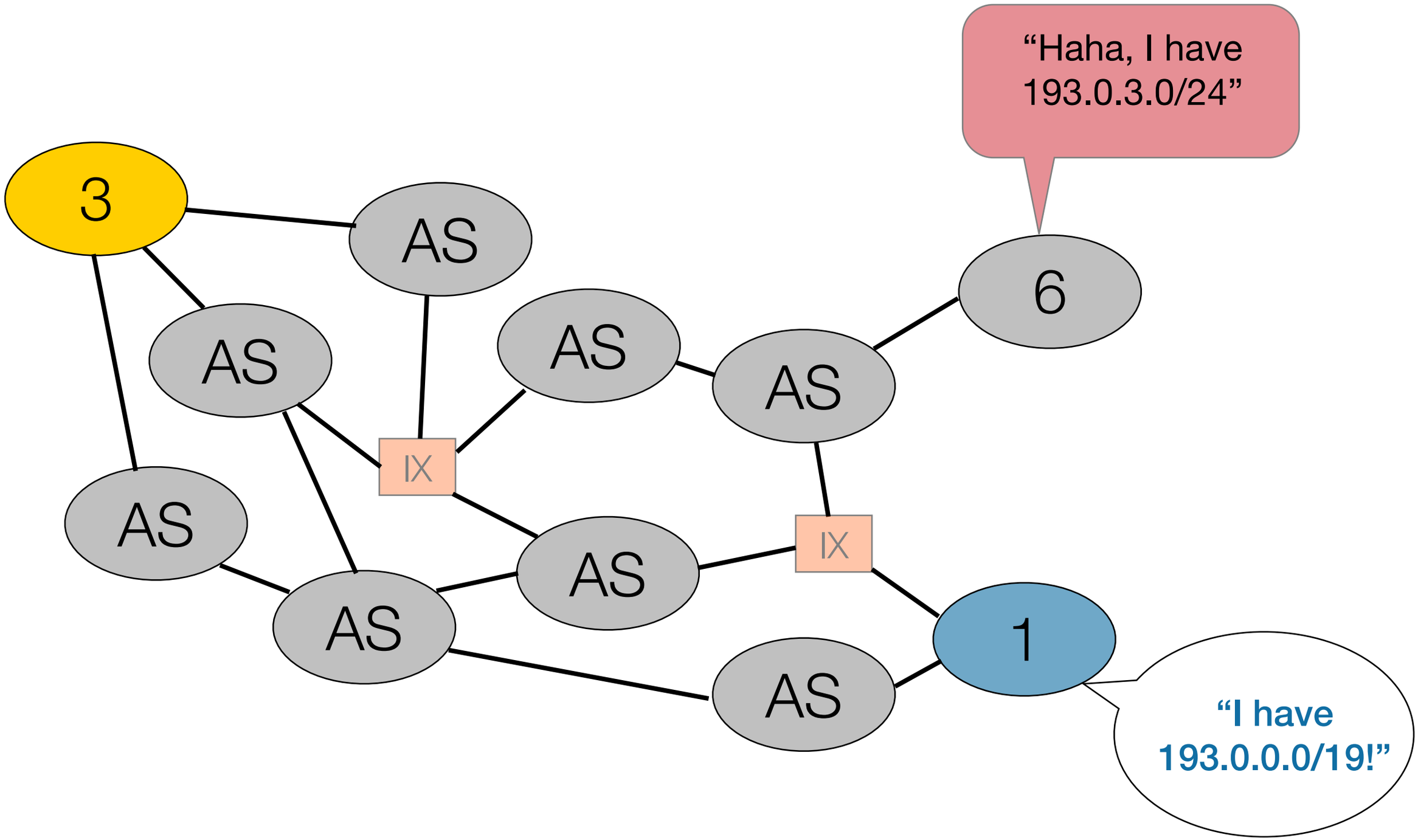

“I know where 193.0.0.0/19 is”
3
AS
AS
AS
AS
6
IX
AS
AS
IX
AS
1
“I know where 193.0.0.0/19 is”
“I know where 193.0.0.0/19 is”
“I have 193.0.0.0/19!”

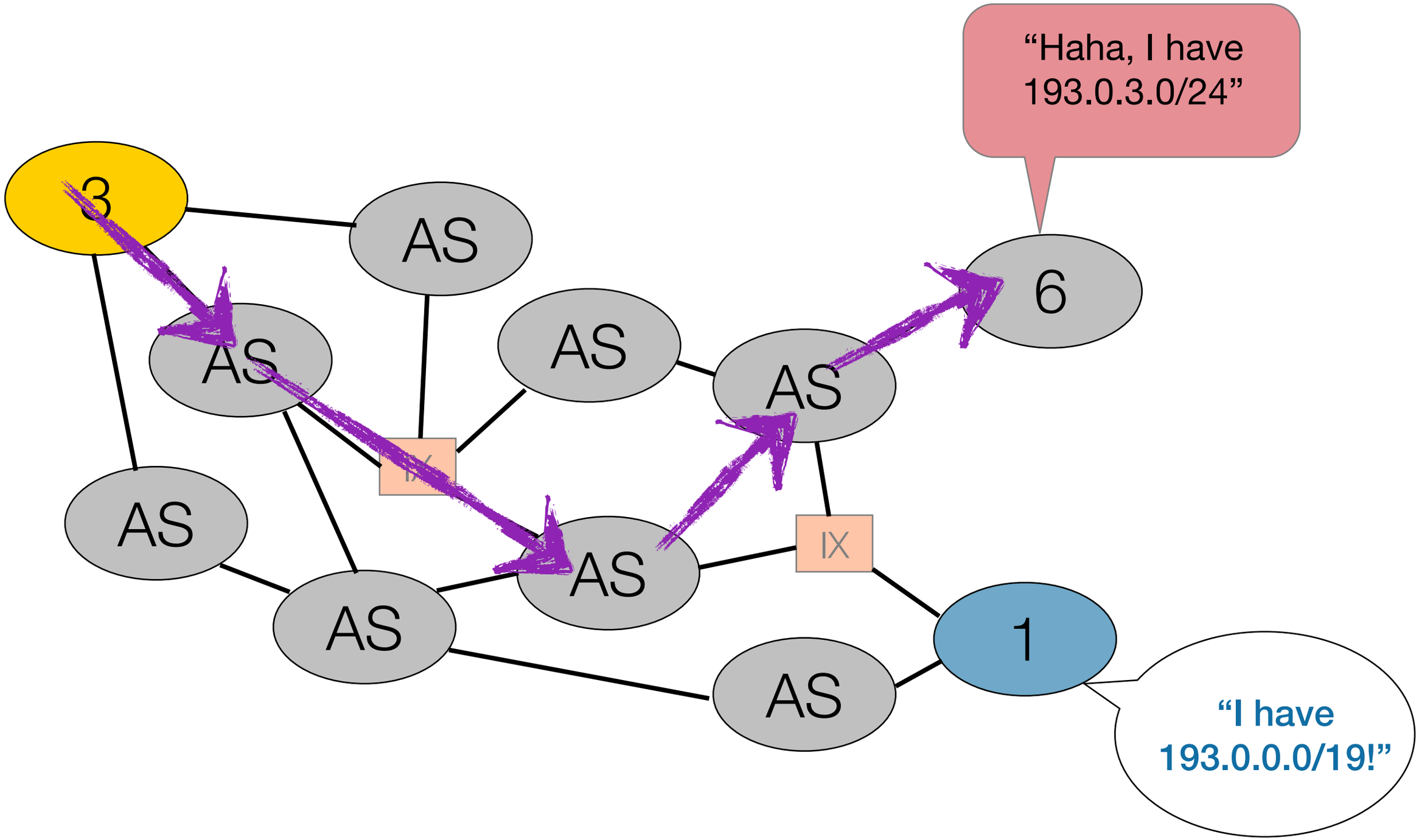

3
AS
AS
AS
AS
6
IX
AS
AS
AS
IX
1
AS
“I have 193.0.0.0/19!”


3
AS
AS
AS
AS
6
IX
AS
AS
IX
AS
1
AS
“I have 193.0.0.0/19!”


3
AS
AS
AS
AS
6
IX
AS
AS
AS
IX
AS
1
“I have
193.0.0.0/19!”


“Haha, I have 193.0.3.0/24”
3
AS
AS
AS
AS
6
IX
AS
AS
AS
IX
1
AS
“I have 193.0.0.0/19!”


“Haha, I have 193.0.3.0/24”
3
AS
AS
AS
AS
6
IX
AS
AS
IX
AS
1
AS
“I have 193.0.0.0/19!”


“Haha, I have 193.0.3.0/24”
3
AS
AS
AS
AS
6
IX
AS
AS
IX
AS
AS
1
“I have 193.0.0.0/19!”

Hijacking in Practice

Hijacking in Order to Spam

- Probably the easiest to do
  - You don't need 100% coverage
  - Probably temporary anyway
  - You don't care about identity or ownership
- Find some space that is not in use
  - Registry can "guide" you to them
- Find an upstream that does not filter
  - Or trusts what you tell them

In Practical Terms

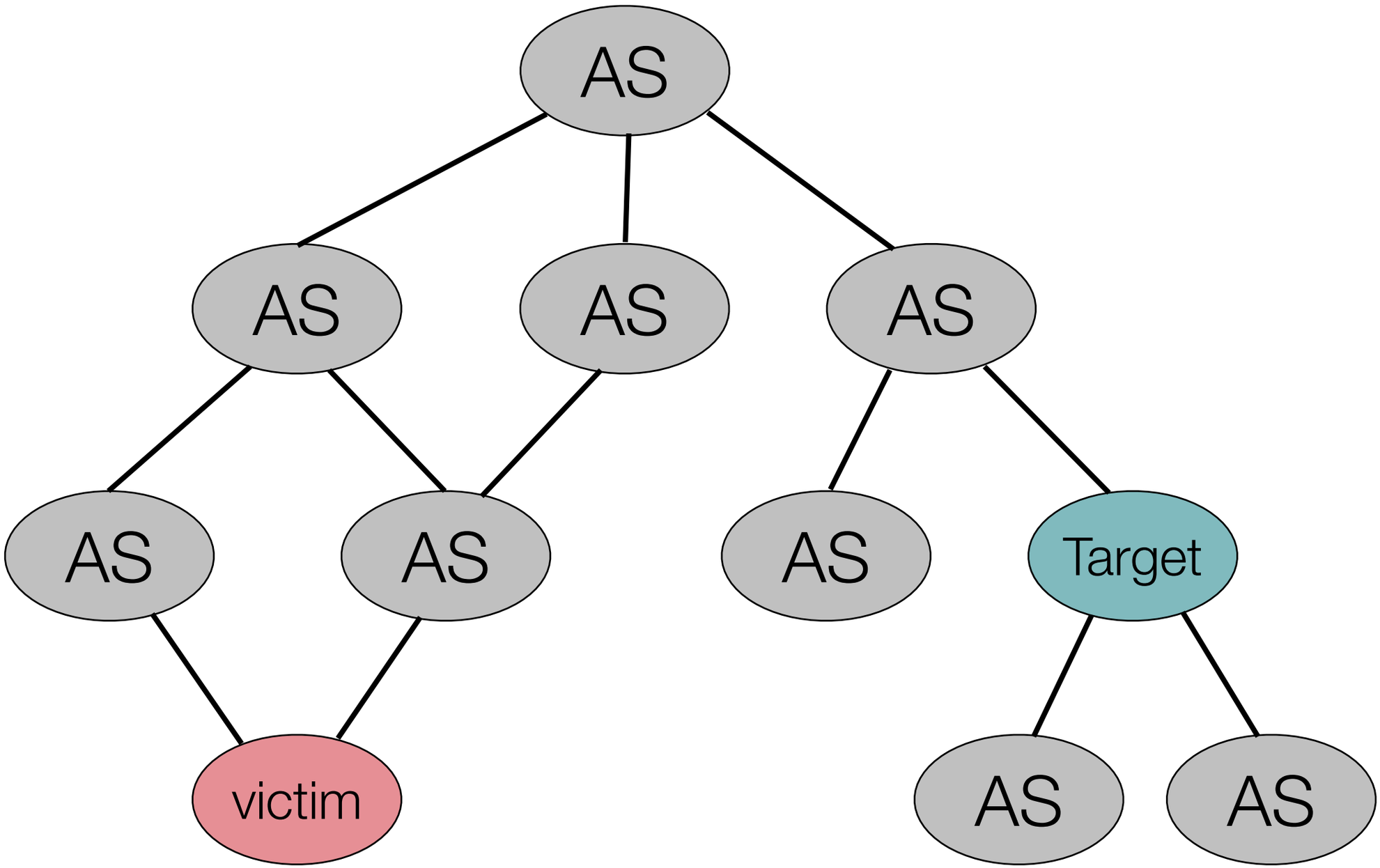
- Look for older registrations or even better, look for something that is not registered at all
- Maybe find an unused ASN to hide behind
- Announce it on the Internet and do your thing

- Role of the registries is very limited
  - We advise people to filter
  - Try to reclaim unannounced space

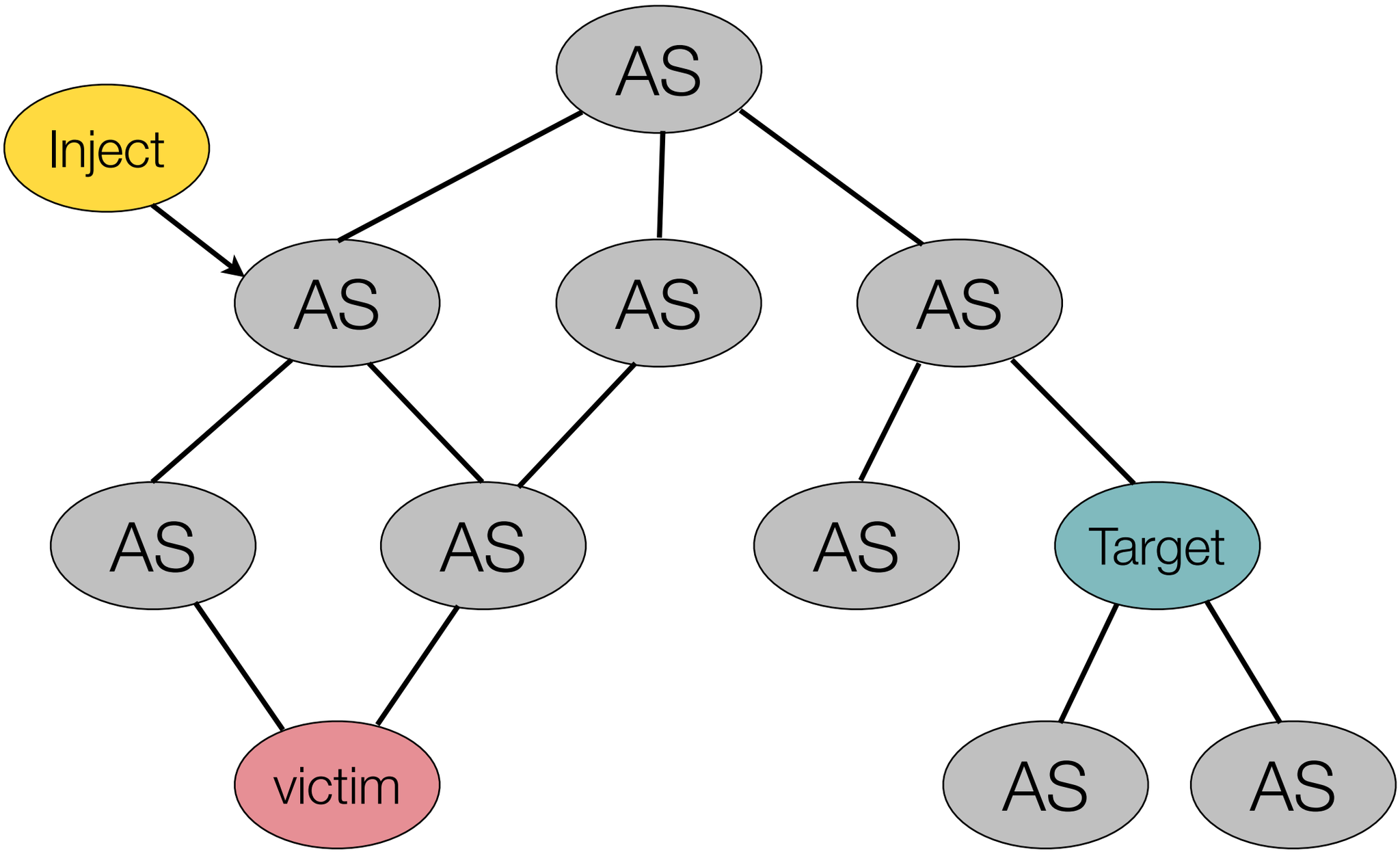
Hijacking to Intercept

- You are targeting space that is in use
  - The owner is much more likely to find out
  - You need to create a shorter or better AS path
- Using a more specific creates a better path
  - Announce only the part you are interested in
- Make sure you don't create a blackhole
- RIPE NCC provides tools that can spot these

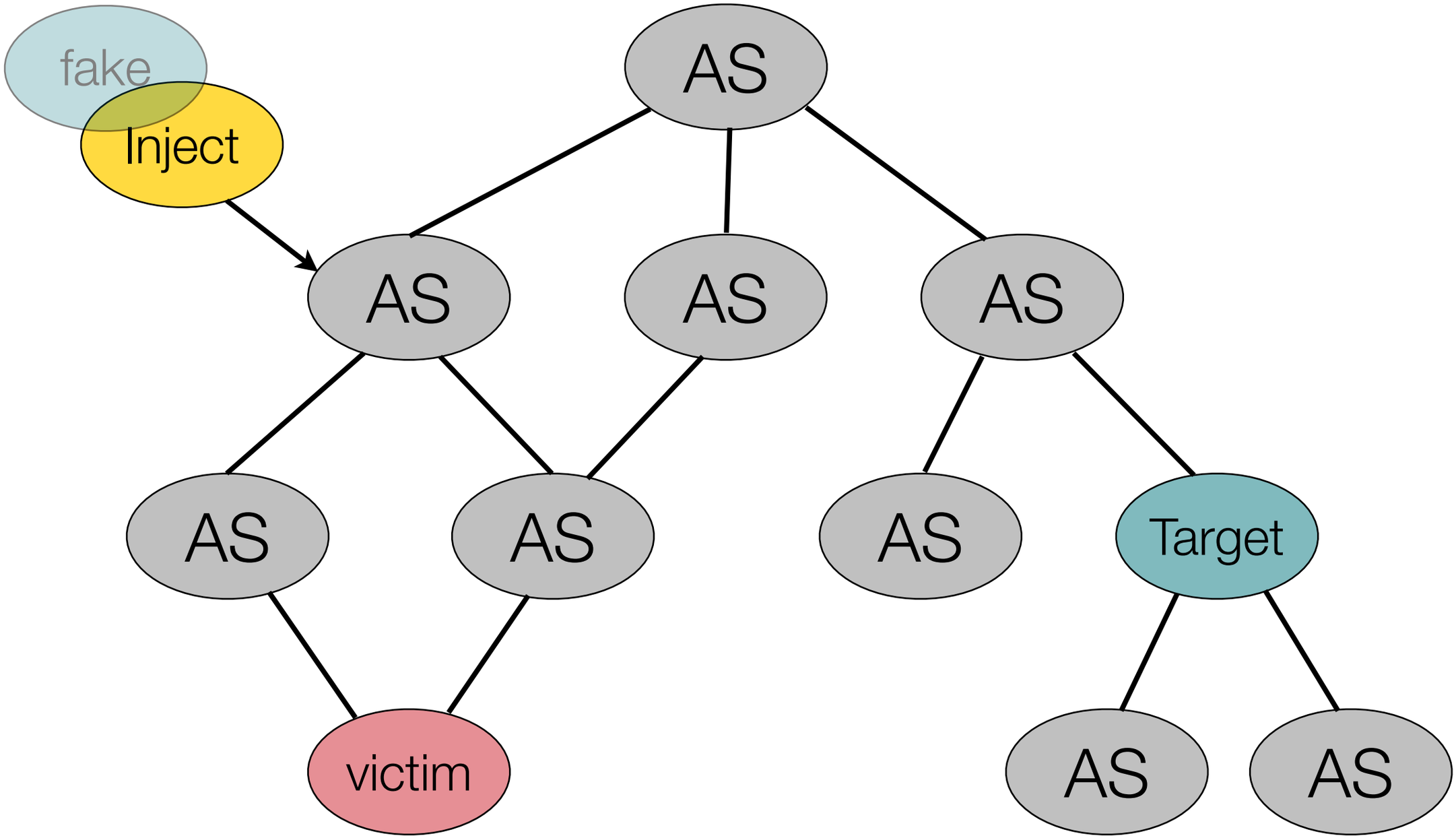
Injecting a Rogue Route



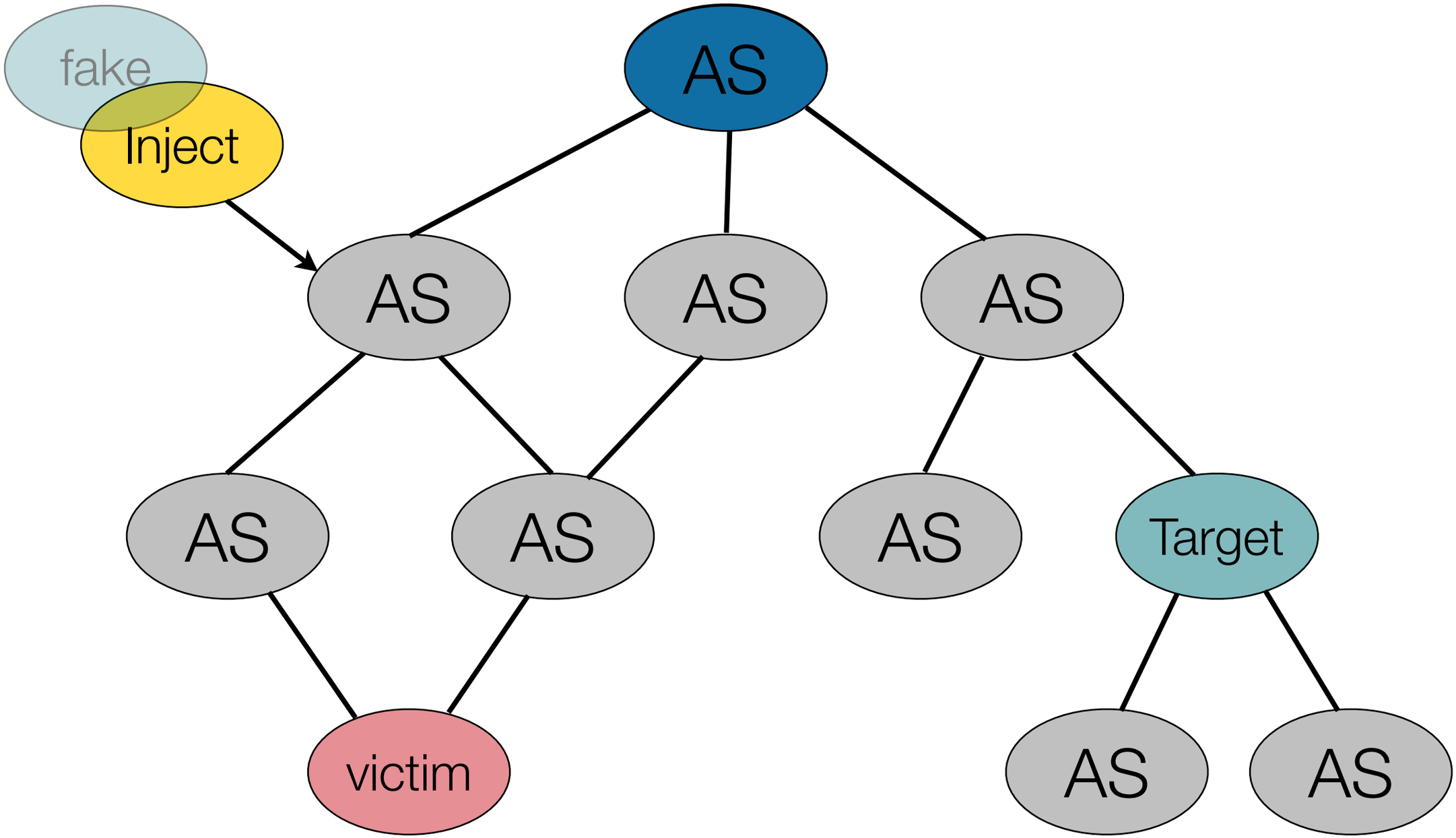
Injecting a Rogue Route



Injecting a Rogue Route



Injecting a Rogue Route

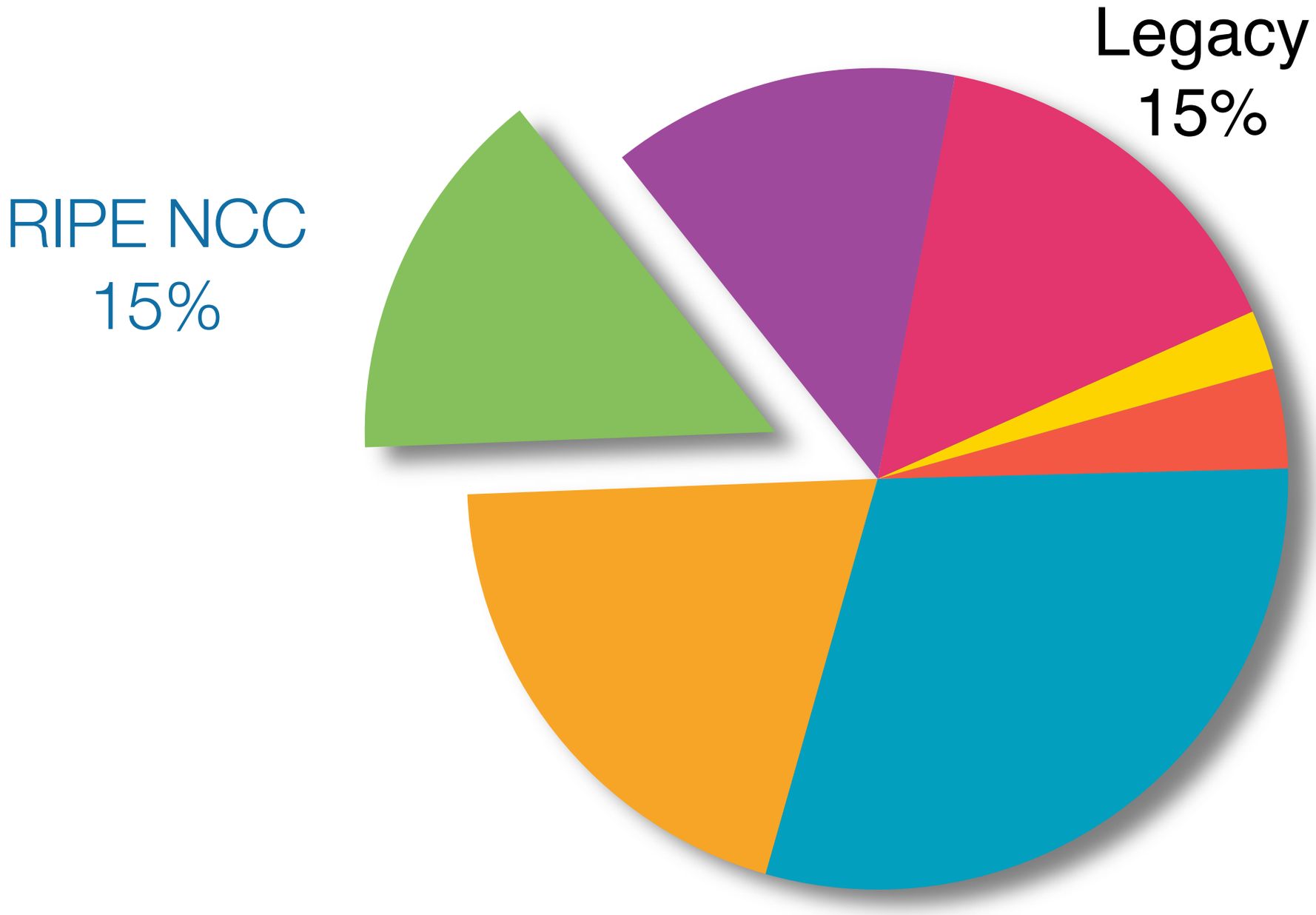


Hijacking With the Intention to Sell

- No need to fiddle with routing
- Unregistered (legacy) space is probably the easiest to target
- Registered space requires you to alter the RIPE Database
- Amount of detail needed probably depends on who is buying it

Protection and Prevention

IPv4 Address Space Covered



Internet Registry

- All assignments and allocations made by the RIPE NCC are protected by us
- Attempts to modify data are monitored and immediately acted upon
- Virtually impossible to steal registered space from the perspective of the Database
- Routing is not depending on registry information

RIPE Database

- Strong protection using MD5 hashed passwords or PGP public/private key pairs
- Only authenticated users can update or change information
- Creation of so called route objects verified by password of both the IP and ASN holders
- It is a public database!

Internet Routing Registry

- Combination of ASN and IP resources
  - "This space is announced by this AS"
- Can be used to setup and maintain filters
  - Used by a number of larger operators
    - Only accept a route from a customer when properly registered
    - Blocks the injection of false routing information
- Use of the IRR is voluntarily

Internet Routing Registry (2)

- Not all address space is covered
- Not everything in the IRR is accurate
  - Stale information can be a problem
  - Manual overrides happen all the time
- It is a distributed system
  - 14 databases that mirror each other
  - Verification and authentication methods vary between those databases

Routing Information Service

- We operate a number of route collectors
  - Thousands of networks feed us their view of the world
  - Provides a global view of the Internet
- Information collected in a central database
  - Provides historic and real time information
  - Information is publicly accessible
- Information can be used to monitor your space
- Can also be used to find unused address blocks

IS Alarms Service

- Tool to monitor the Internet routing table
  - Using RIS as a source
- Track changes in origin or transit AS for a given prefix
- If a rogue route is detected an alarm is raised to the operator either via email or syslog
- Can catch a lot of errors and hijack attempts

Routing Registry Constancy Check

- Compares the IRR and RIS
- Highlights the mismatches in origin AS
- Operator can choose from two options:
  - Fix the IRR to match routing
  - Fix the routing to match the IRR

- Does not prevent or correct any hijacking but improves data quality in the IRR

Certification

- The idea came from the routing community
  - Secure InterDomain Routing (SIDR) WG in IETF
- Route Origination Authorization (ROA)
  - Ties a specific prefix to an ASN
  - “Improved” version of the route object
- Verified by the address holder
  - Registry is the trust anchor
  - Allows for better control compared to IRR

Certification (2)

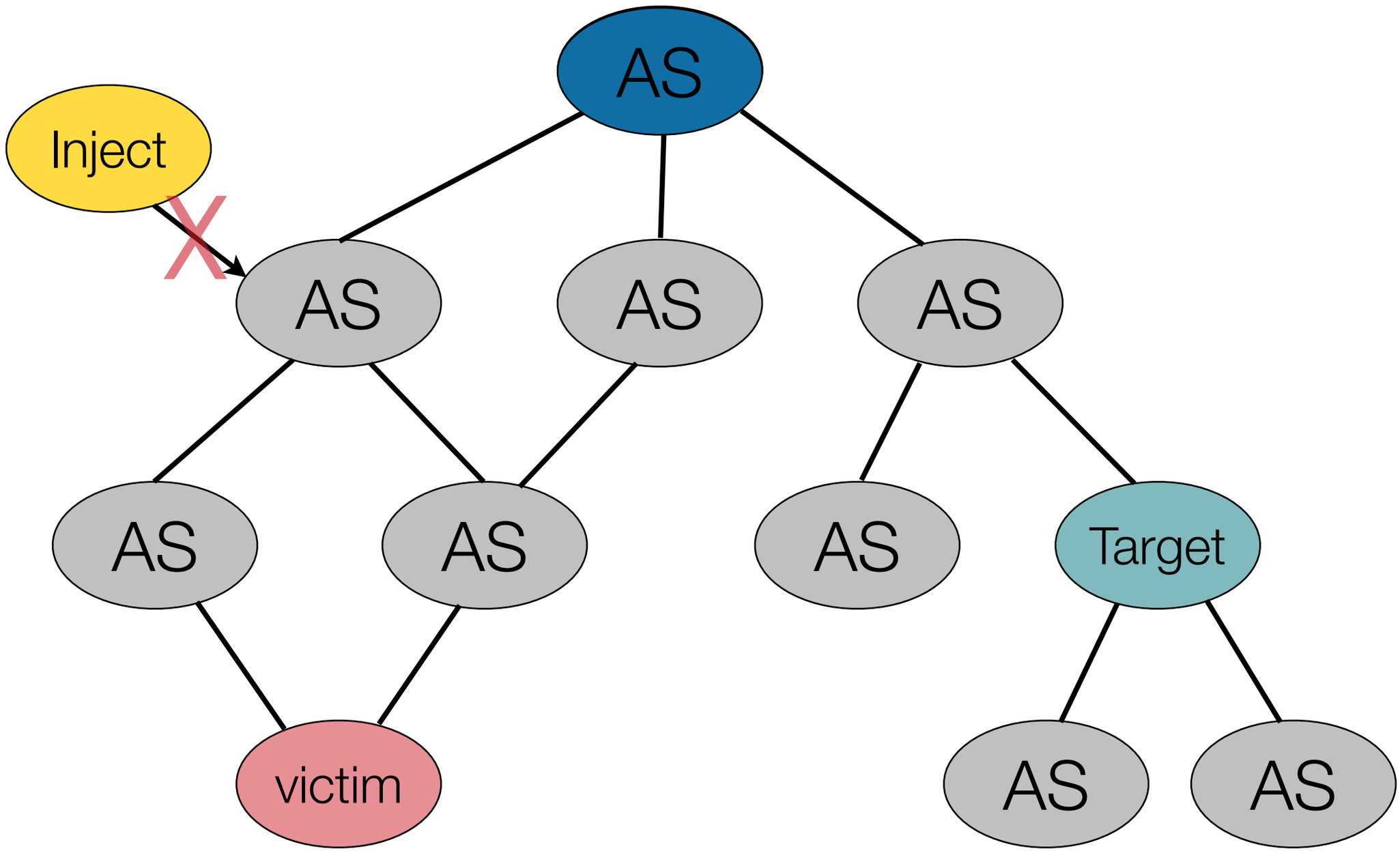
- More and easier integration with the routing layer
  - Compared to the IRR system using the database
- Should have less stale information
  - Turned out to still be error prone
- Use is entirely voluntarily
  - How to handle invalids is up to the operator
- Quality of the RPKI data will influence the speed of adoption amongst operators

Certification (3)

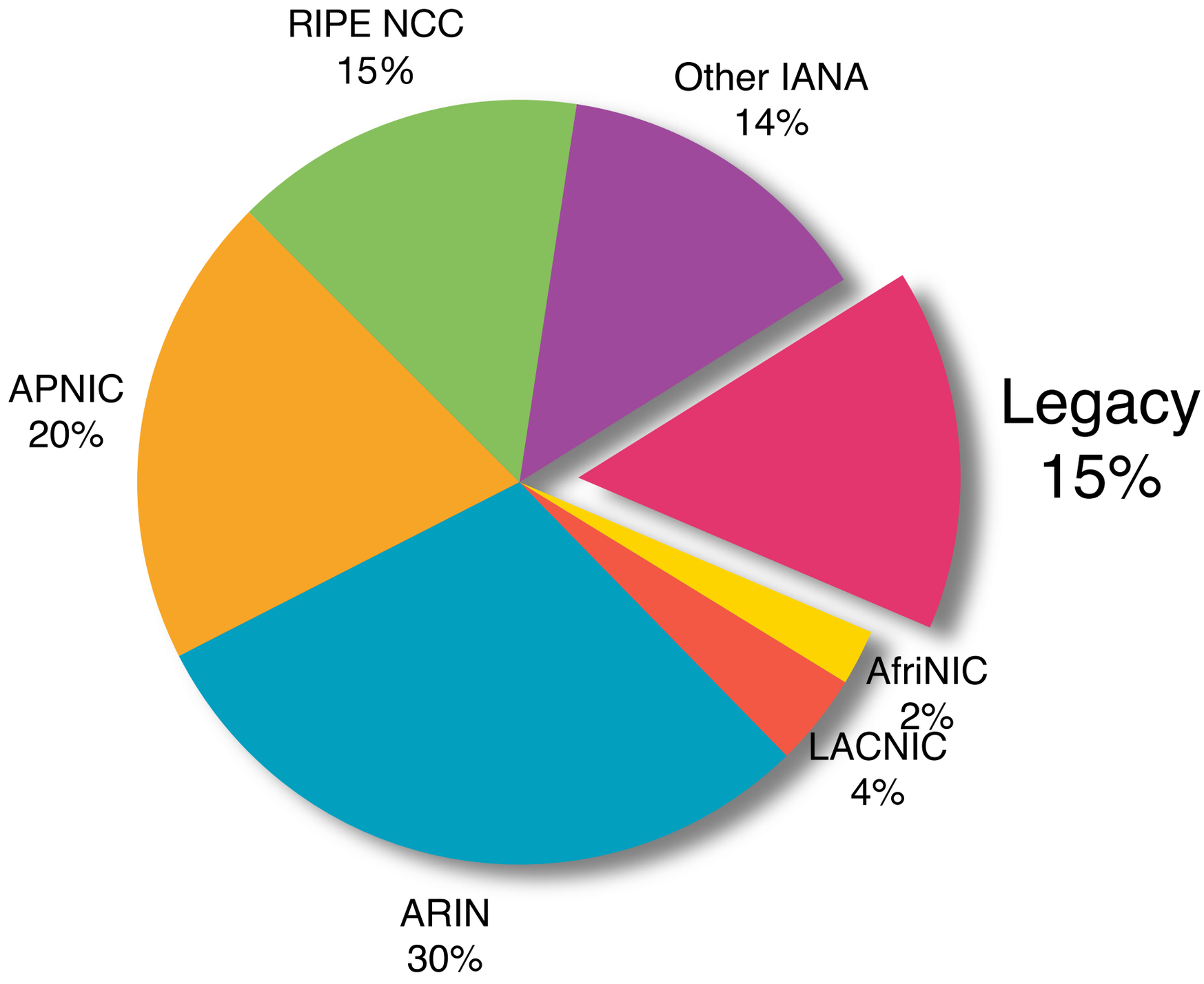
- Current guidelines are to alter preference:
  - Always prefer valid over invalid routes
- Right now can only verify the origin of the route
  - Catches a lot of mistakes
  - “Path validation” added in the future

- Filtering only becomes an option when everybody uses the system correctly

Injecting a Rogue Route



Legacy Is the Easy Victim



Legacy Space

- The most likely target for any form of hijacking or other abuse:
  - Not covered by the registry or stale information
  - Not covered by RPKI
  - More likely to not be used on the Internet

- Project underway to bring these resources into the registry
  - Registration is free of charge

Questions?