





# Blackholing the Internet: A Live Demo

---

 Adam Rapley  
 me@adamrapley.com  
 @admrply  
 [keybase.io/admrply](https://keybase.io/admrply)



# Who am I?

3rd year Ethical Hacking student at Abertay.

Does web things.

Artist/Musician.

Building and Breaking IoT.





# What is BGP

---

- Border Gateway Protocol
- Routing algorithm between ASs
- Advertise prefixes that you manage
  - IP prefix
  - AS-PATH
    - Avoid loops - This is crucial for later in the talk
- Or, y'know... Don't.

# BGP Win Conditions

---

- For the same length prefix
  - Shortest AS-PATH wins
- For different length prefixes
  - The more specific prefix wins.

# ISP Relationships

---

- BT tells Virgin about it's customers and vice versa
- Version tells Sprint about it's customers and vice versa.
- These are shared through BGP UPDATE messages.
- Updates from customers are passed to their upstream provider
- This is all trust based
  - No PKI
  - No validation

# How do we get IP addresses?

---

- ICANN assigns IP blocks to RIRs
  - RIPE in the EU
  - ARIN in the US
- RIRs assign to ISPs
- These IP addresses are NOT assigned to ASNs

# Implementation Errors

---

- Minimal filtering on the upstream edge router
  - Rate limiting
  - Only originating
- No local filtering on networks
  - BGP Propagation
  - Internal network
- As soon as you hit a “backbone AS”, job done.

# Real World Examples

---

- AS 7007
- Spamming unassigned blocks
- YouTube Pakistan
- Hacking Team × Italian Police SpecOps Division
- Bitcoin Stealing



Demo Time!

# Can we MITM this?

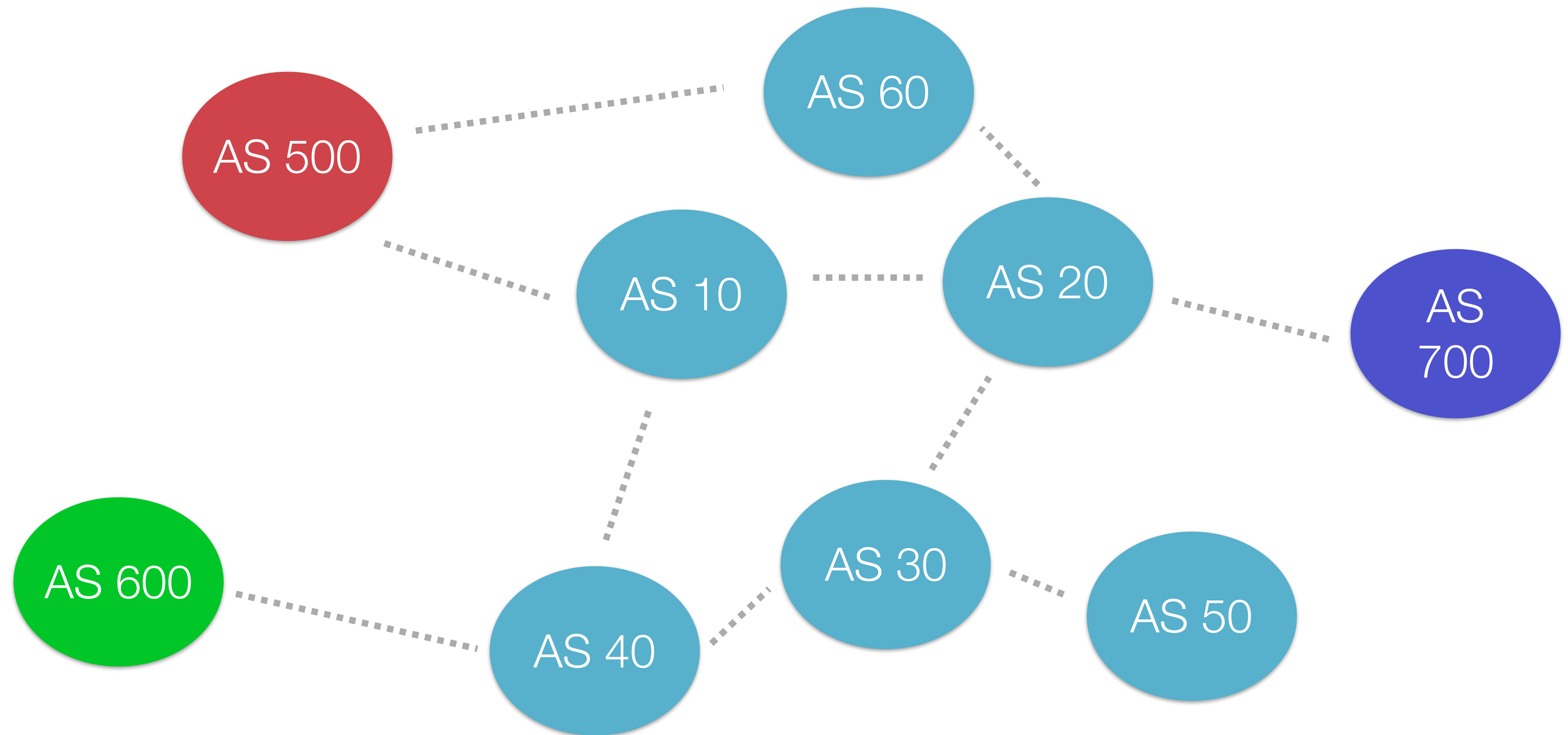
---

- Yes.
- Yes we can.
- Need to serve the real website!
- How do we stop our own next hop router from returning our own traffic
- AS-PATH ASN prefixing



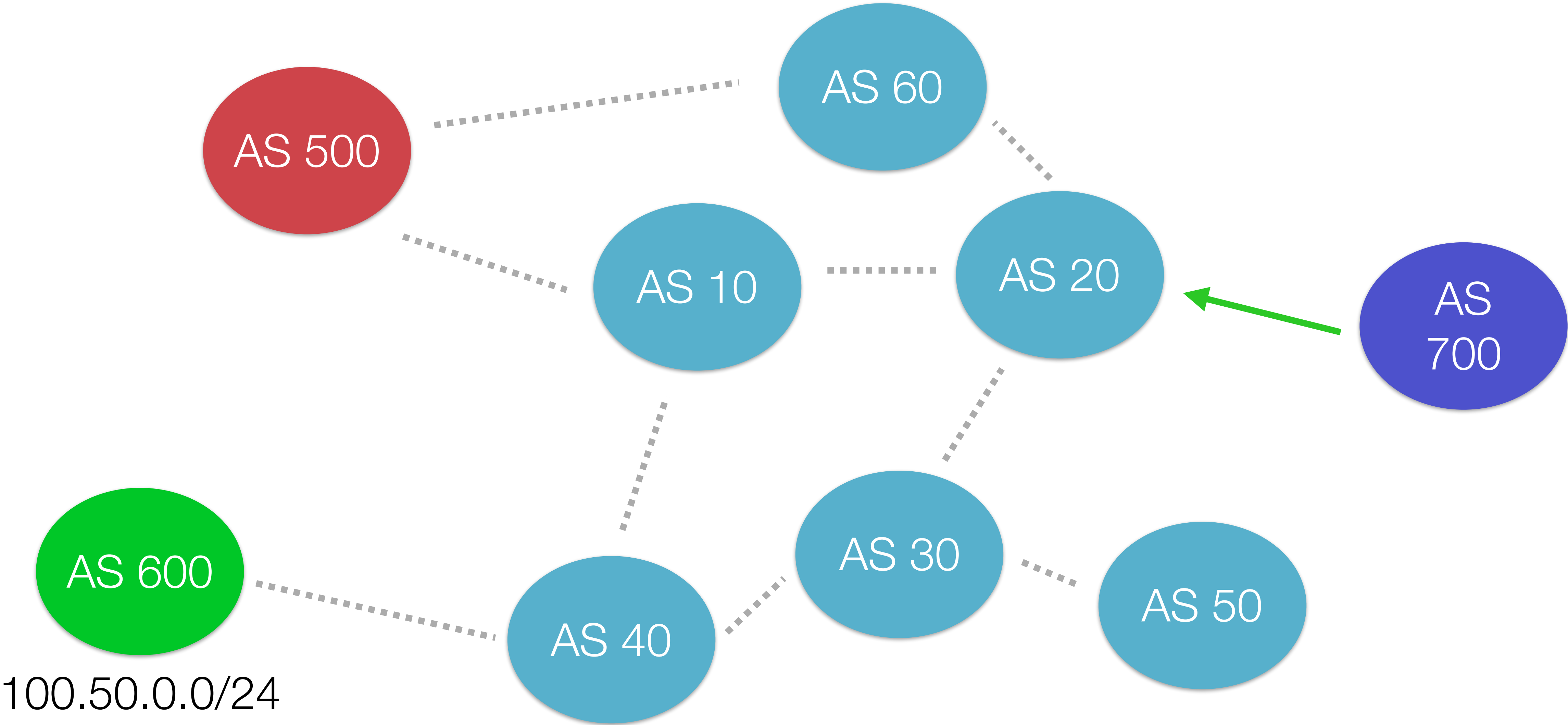
# Keeping the path open

---



# Keeping the path open

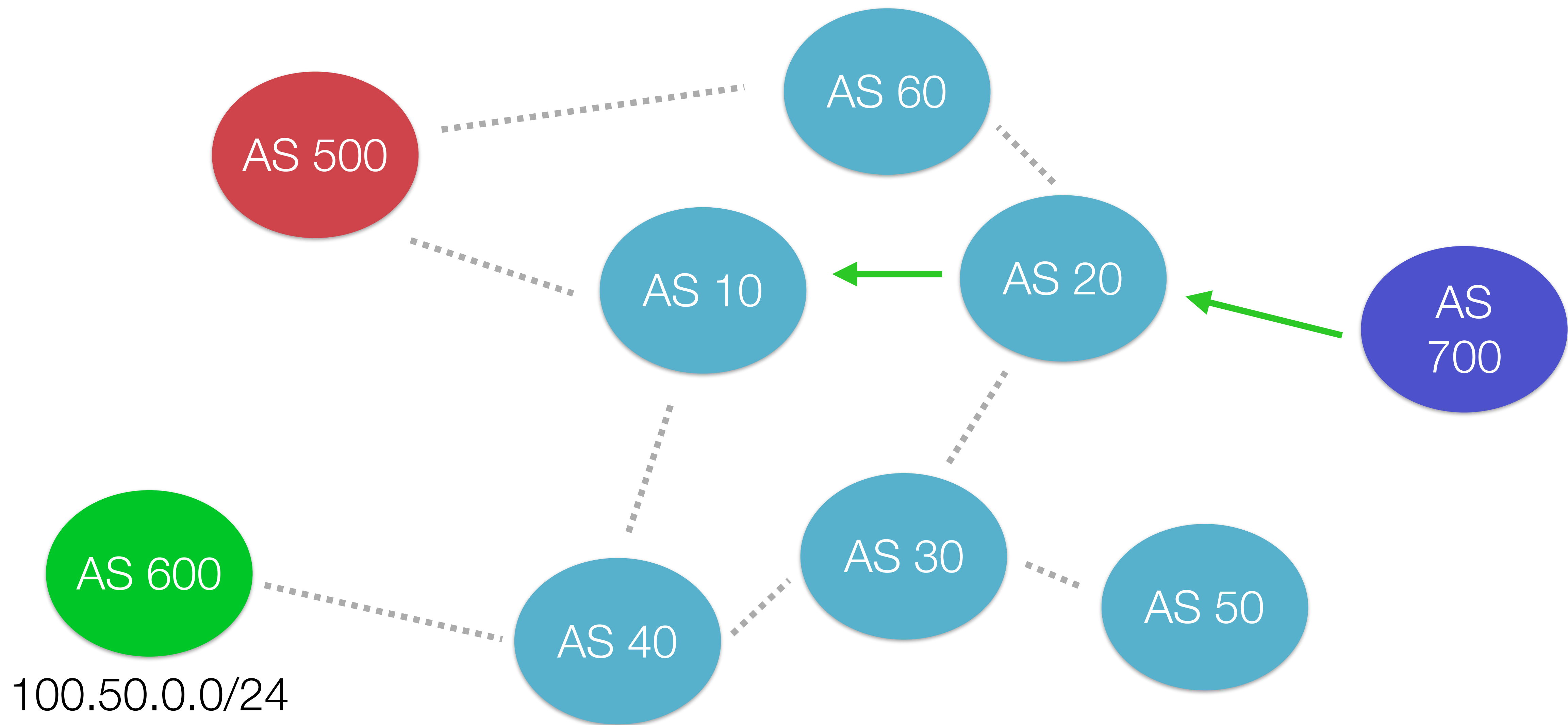
---





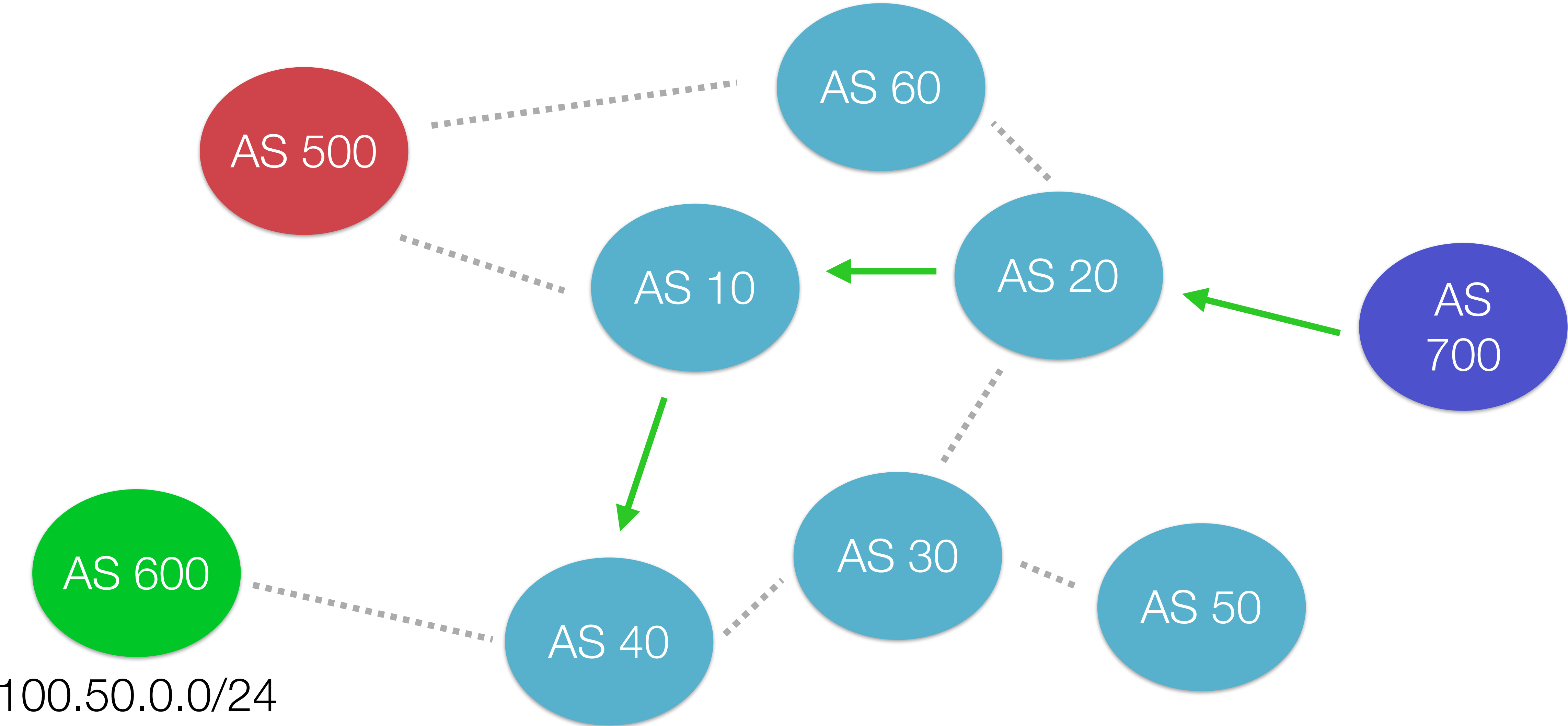
# Keeping the path open

---



# Keeping the path open

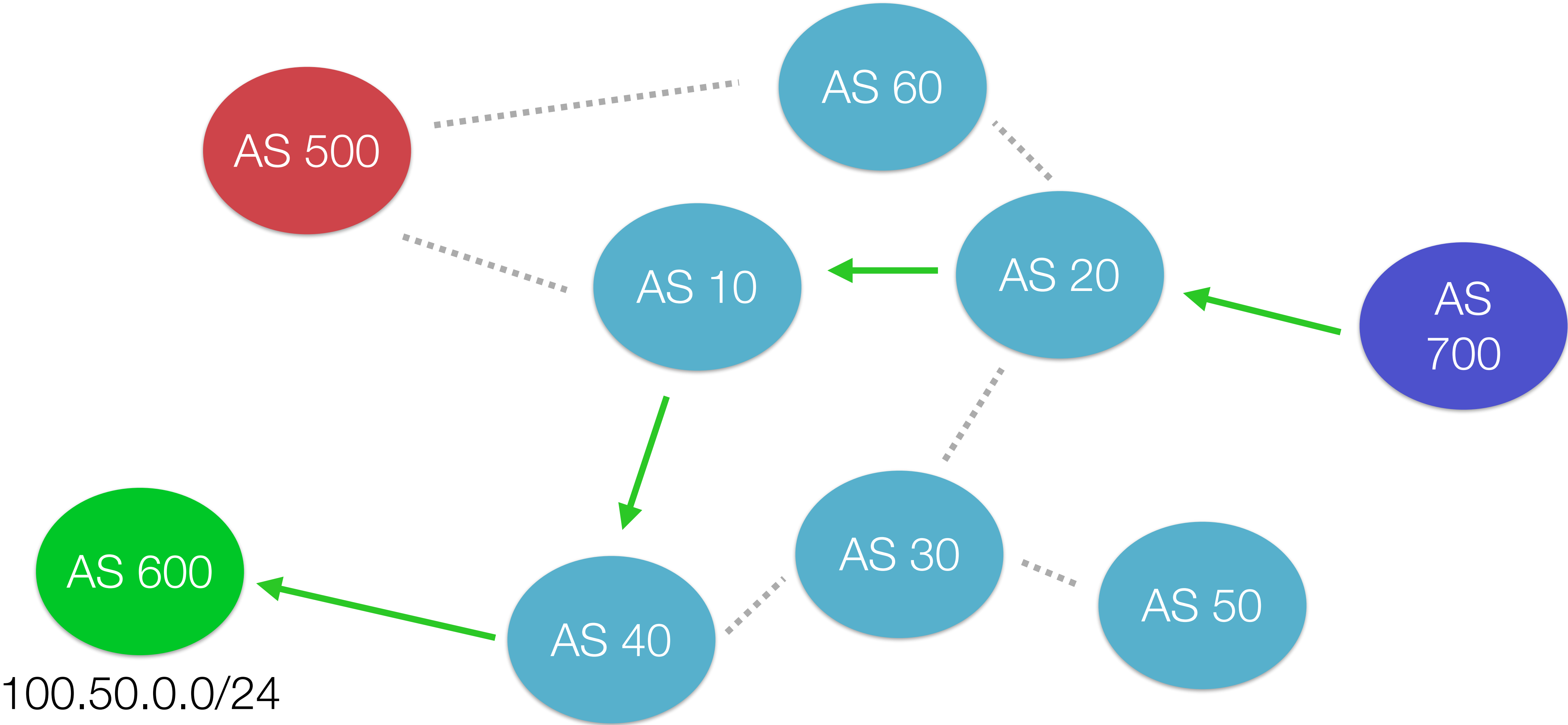
---





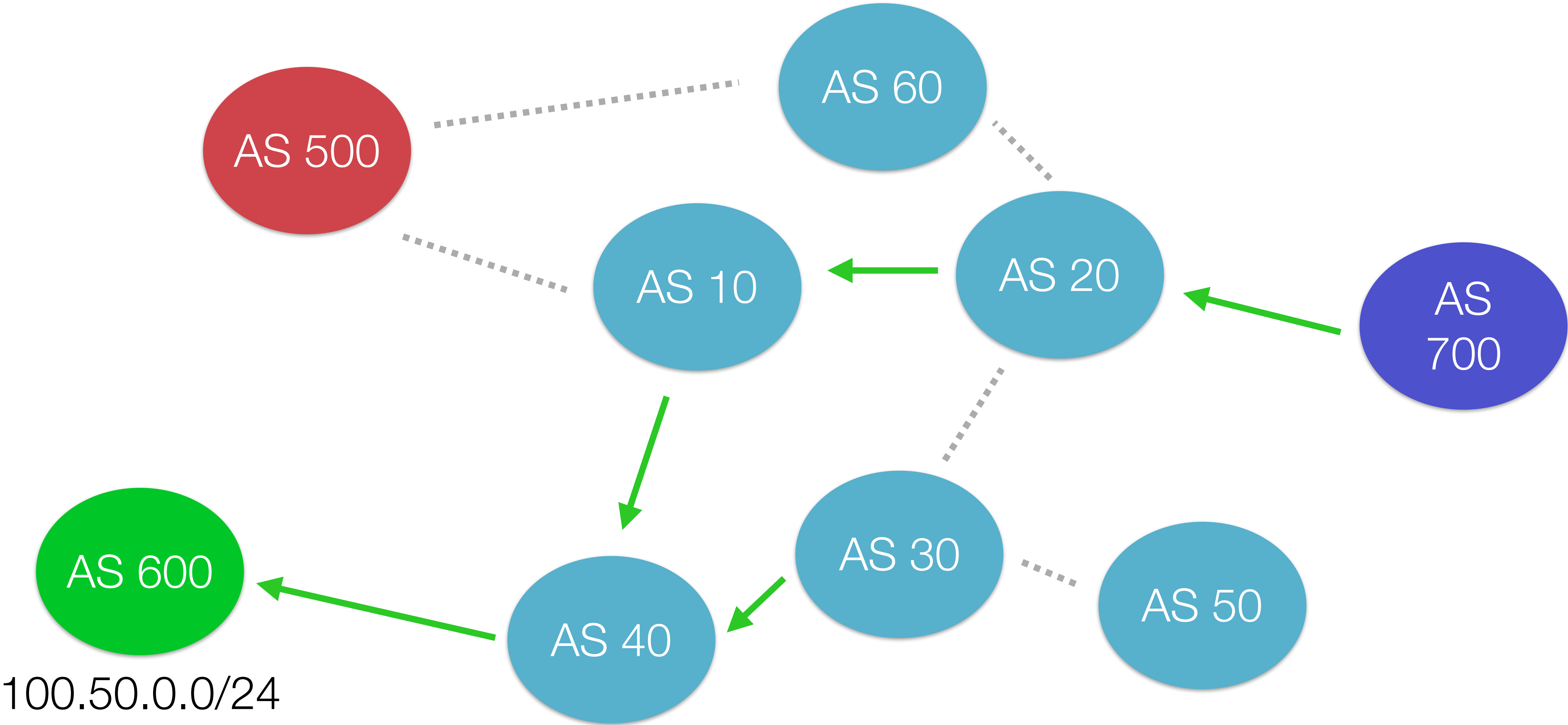
# Keeping the path open

---



# Keeping the path open

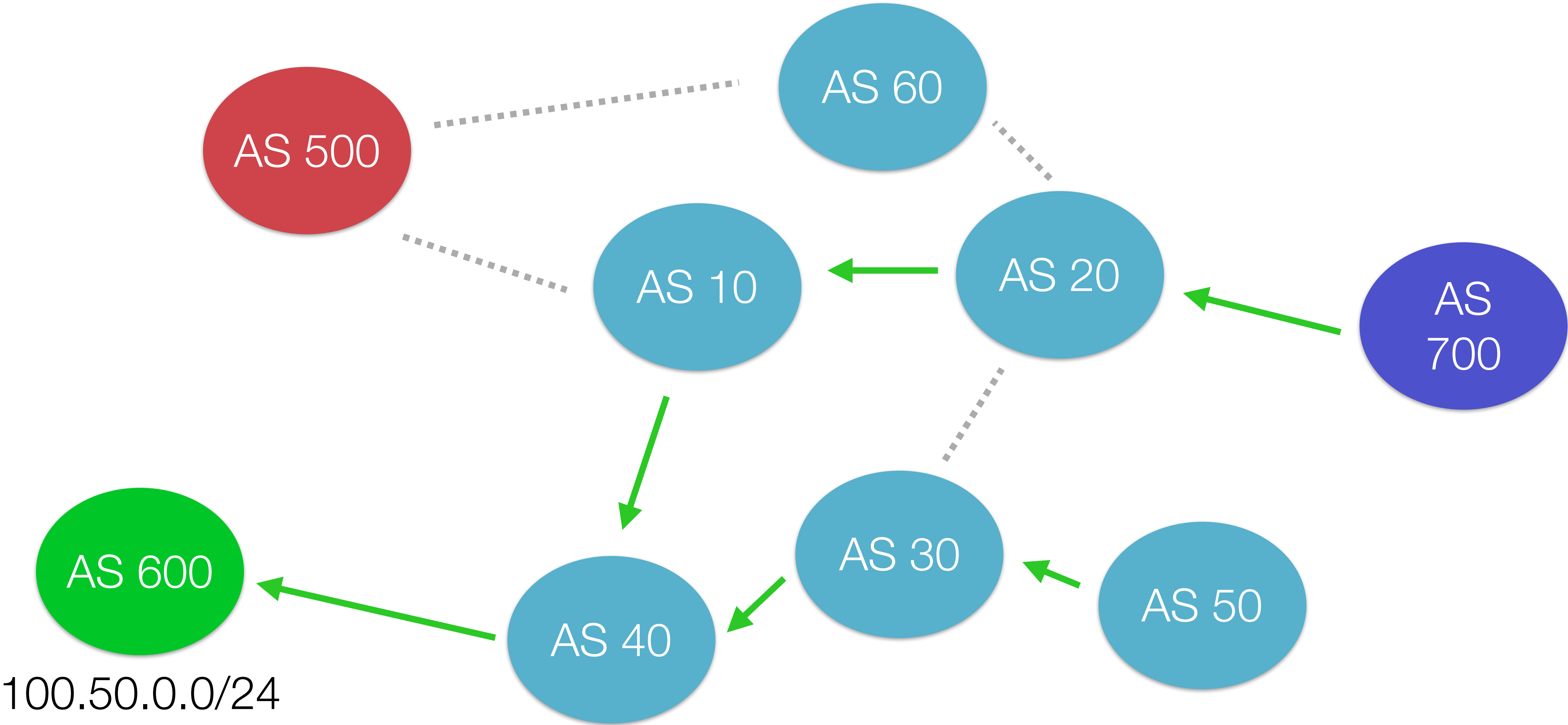
---





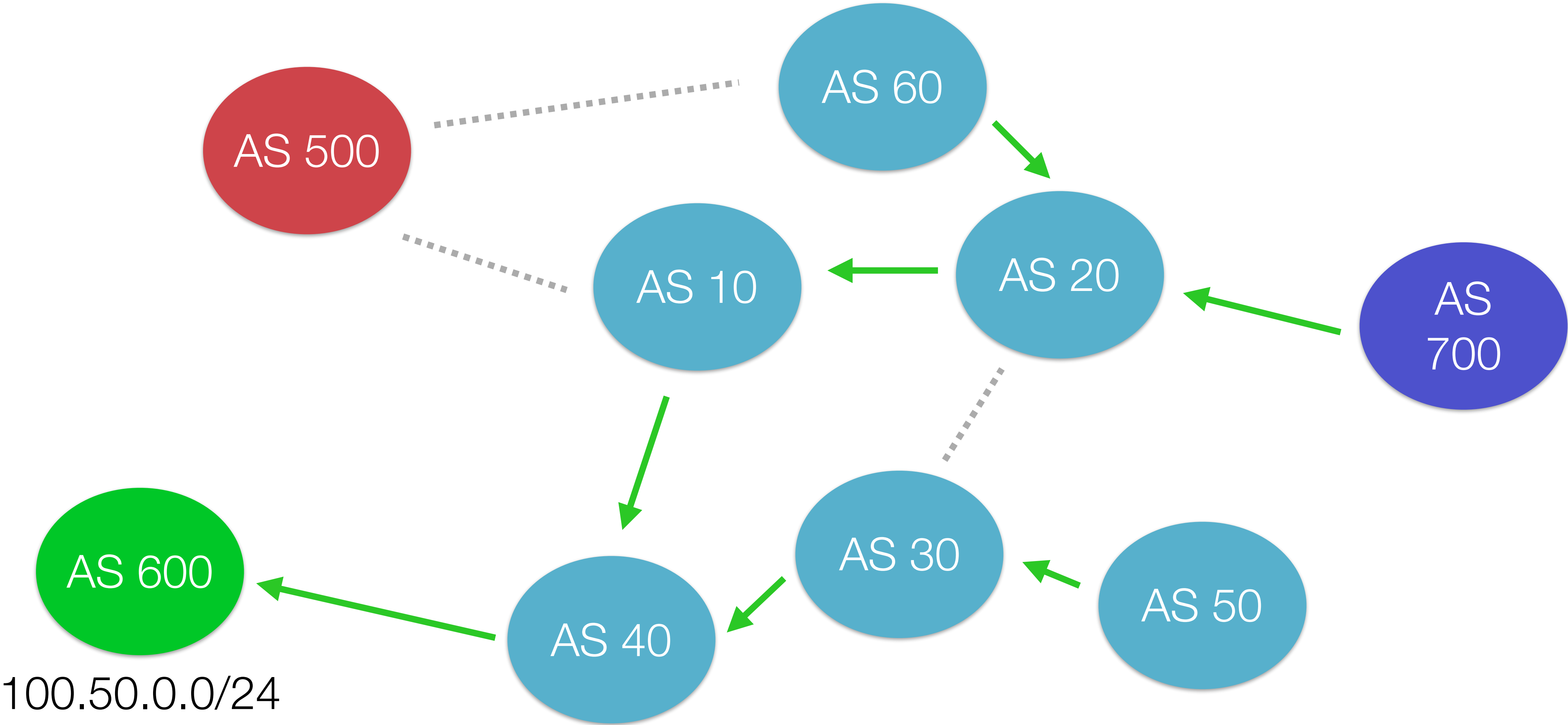
# Keeping the path open

---



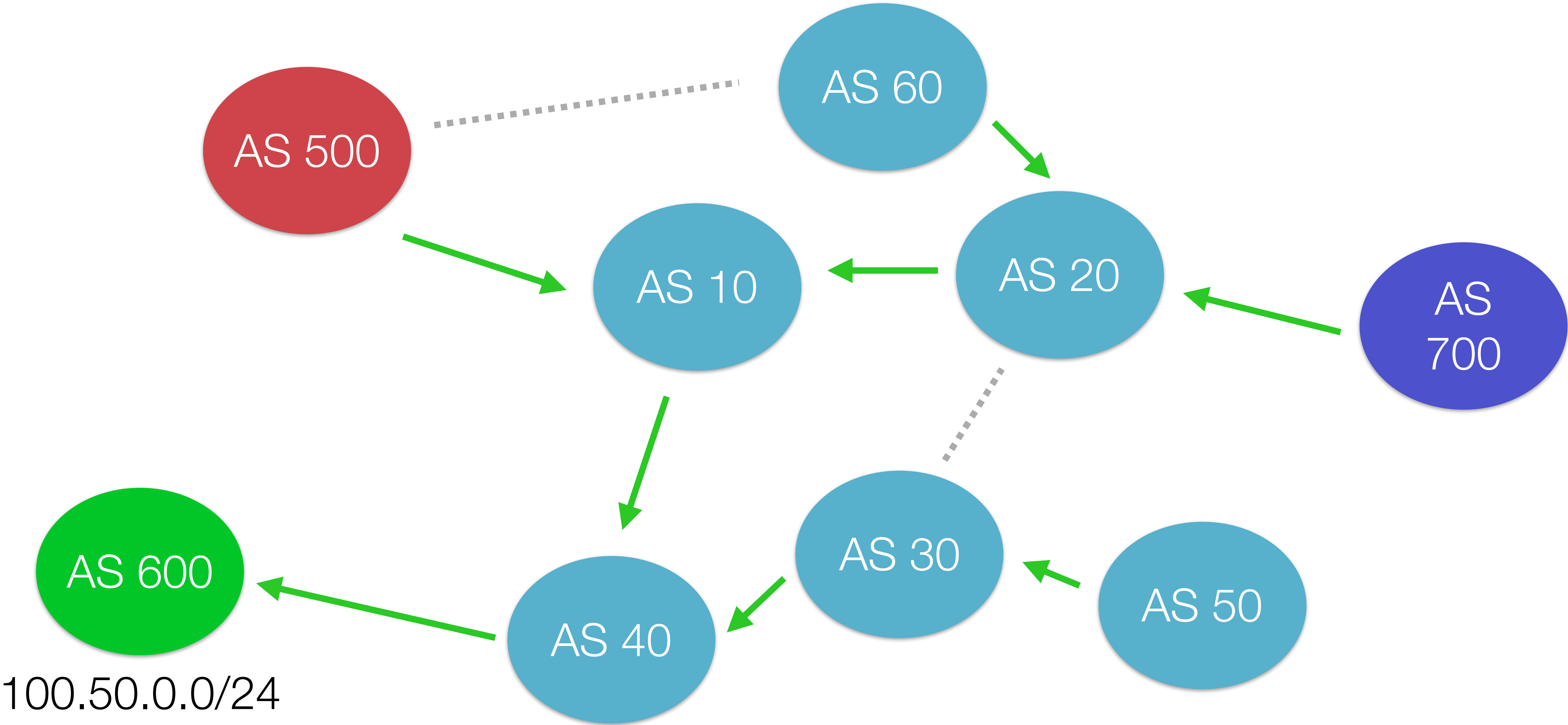
# Keeping the path open

---



# Keeping the path open

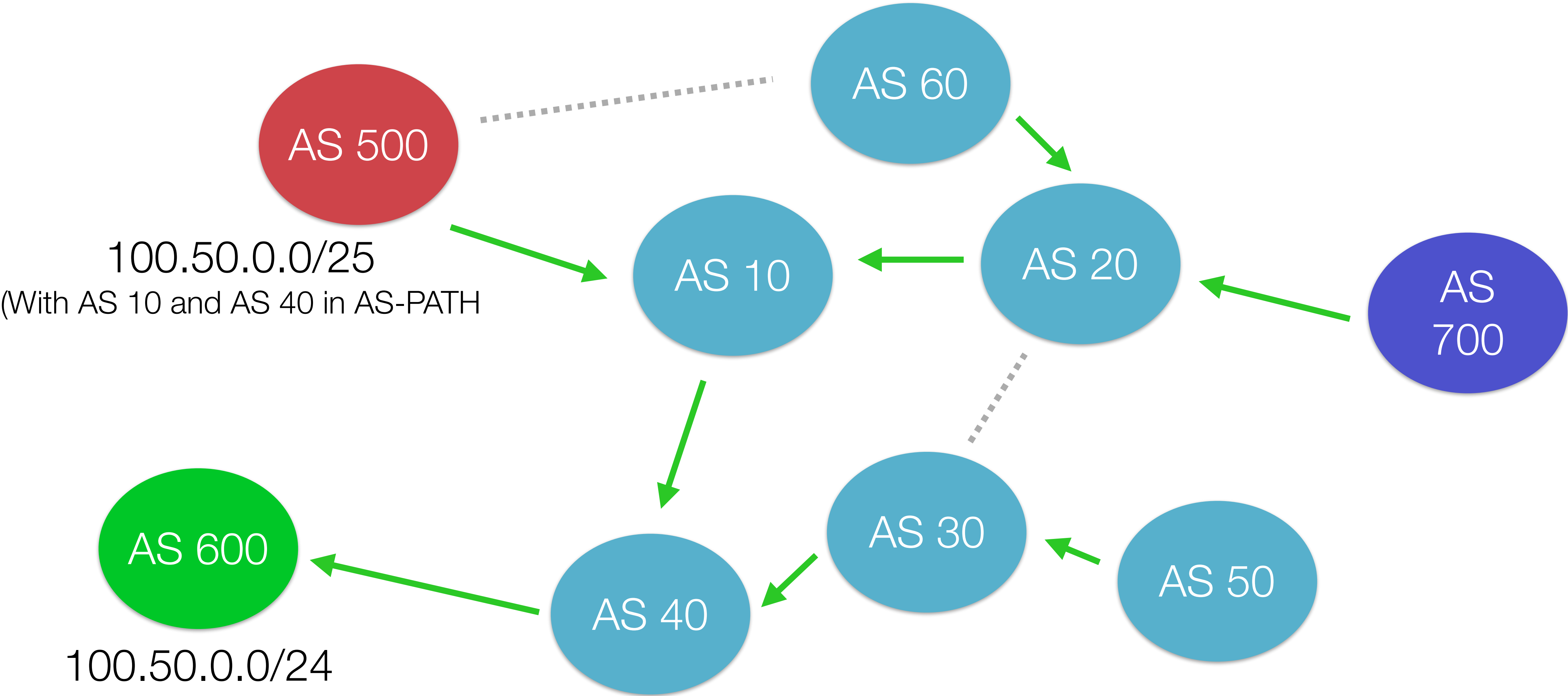
---





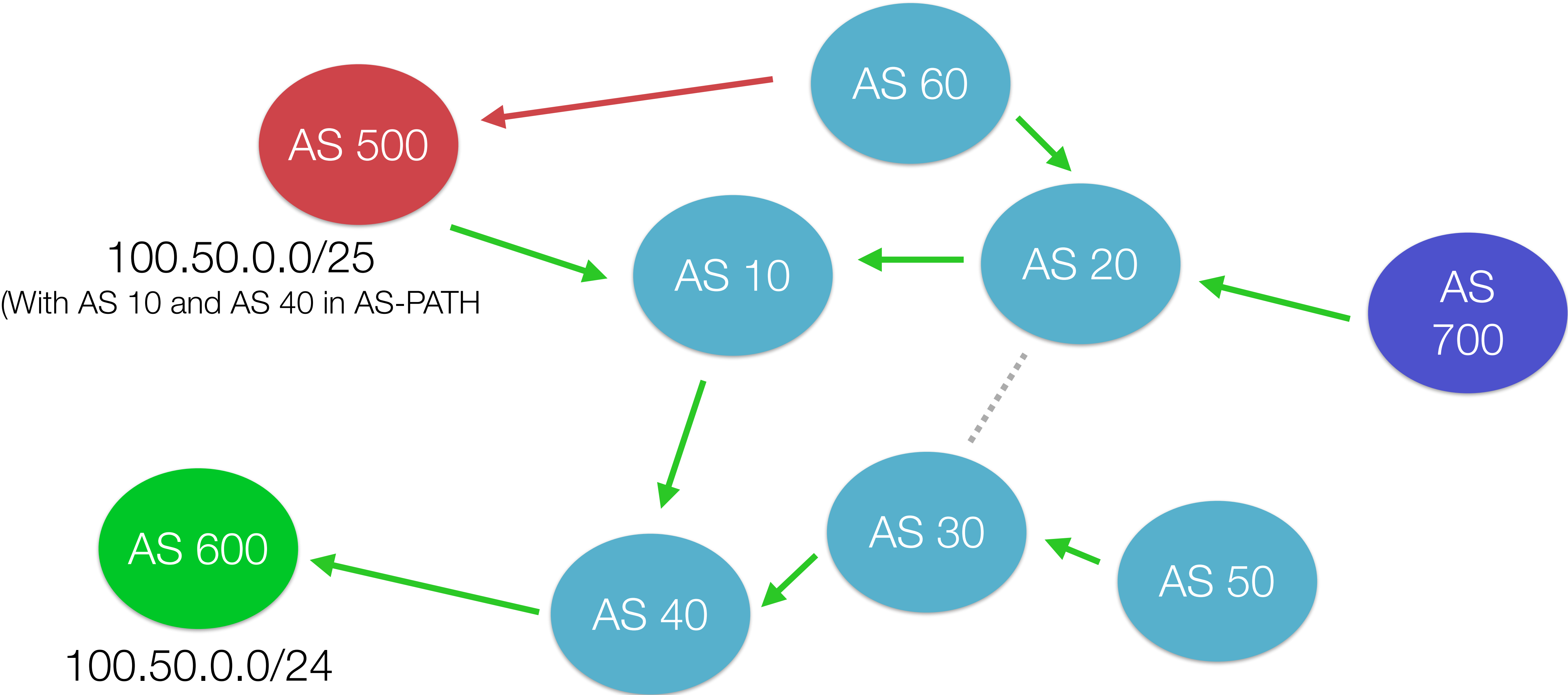
# Keeping the path open

---



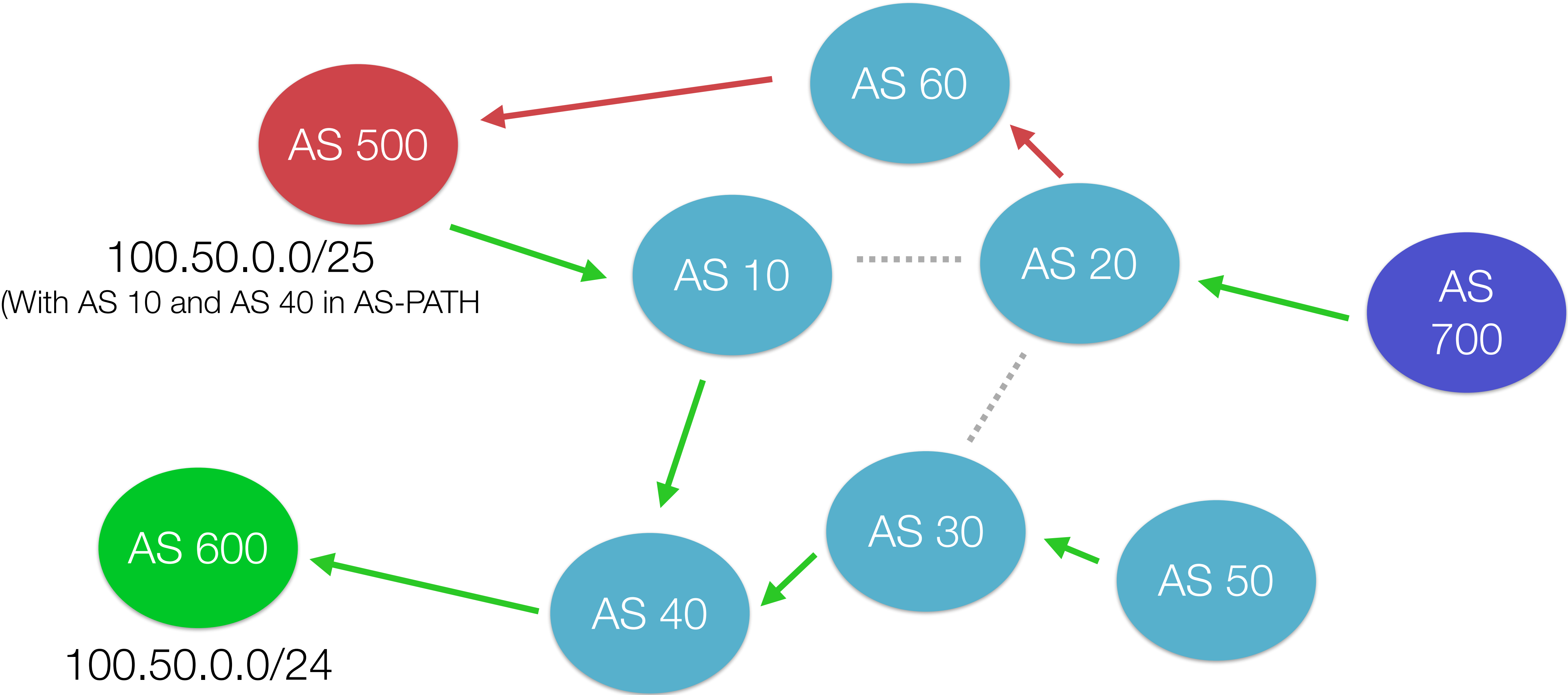
# Keeping the path open

---



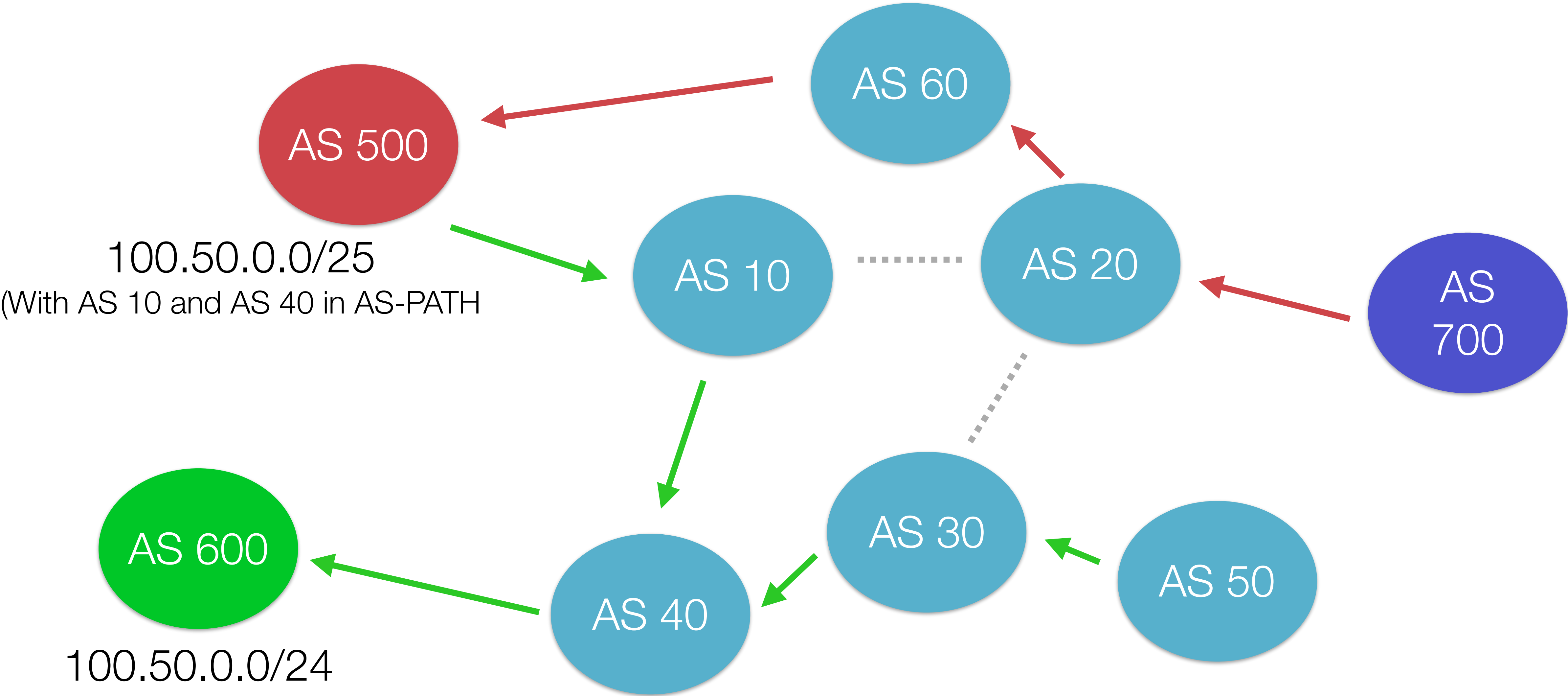
# Keeping the path open

---



# Keeping the path open

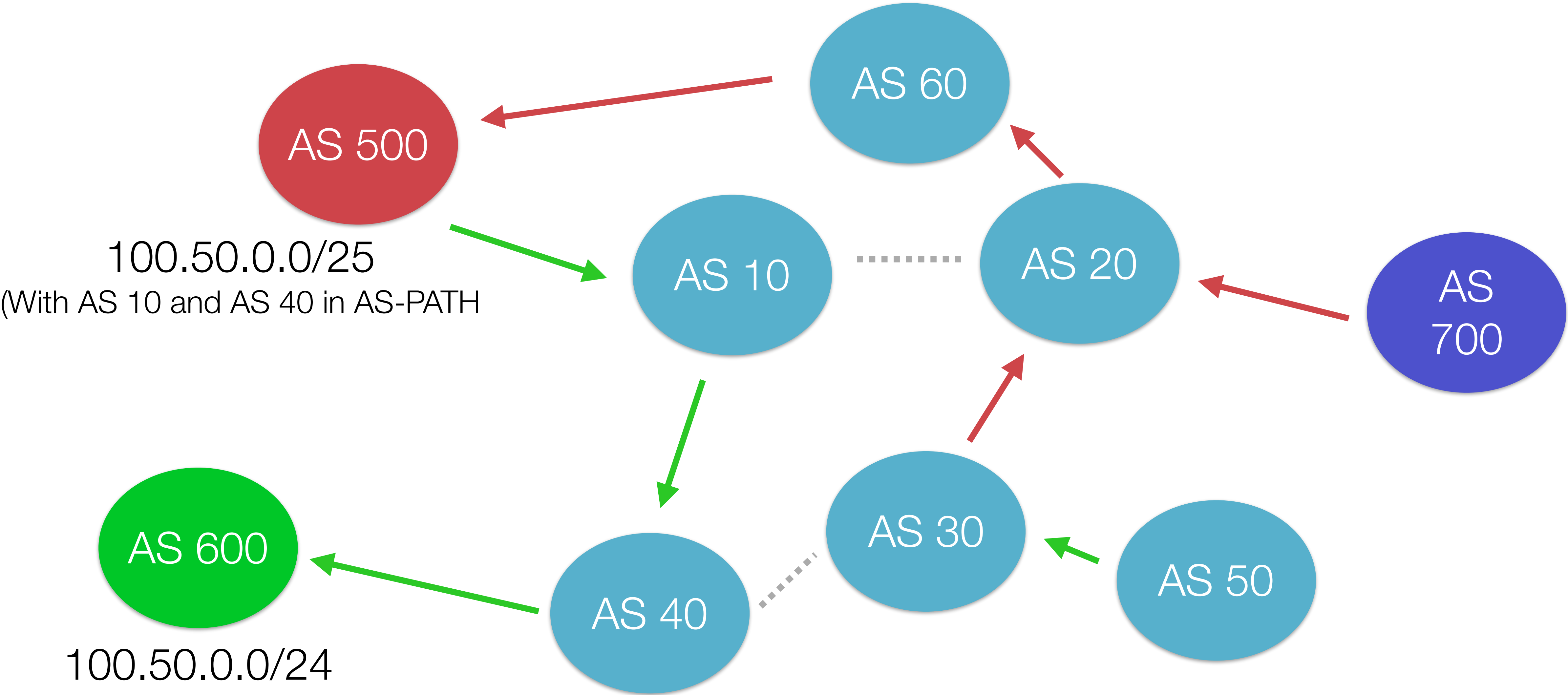
---





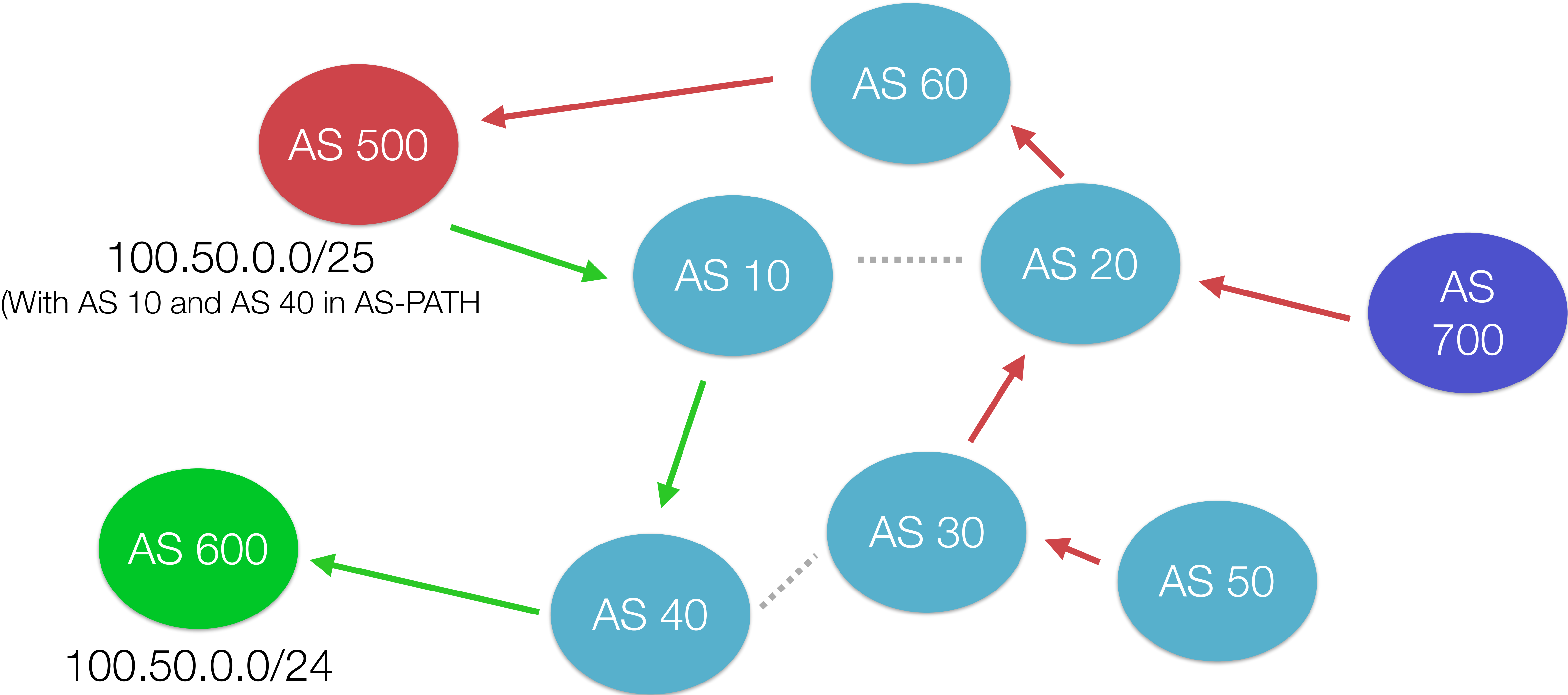
# Keeping the path open

---



# Keeping the path open

---



# Hijacking the AS-PATH

---

- Prepend the AS-PATH with the correct route
  - Right down to the originating AS
  - `set as-path prepend 10 40 600`
- Set a static route towards the correct path
  - `set ip route <10>`

# Mitigations

---

- Know someone at the ISP
- Route Flapping
  - Very ineffective
- Secure alternatives
  - S-BGP
  - psBGP
  - soBGP



# Mitigations for the Mitigations

---

- Uptake
- ...
- IPv6.

Questions?

 Adam Rapley

 me@adamrapley.com

 @admrply

 [keybase.io/admrply](https://keybase.io/admrply)