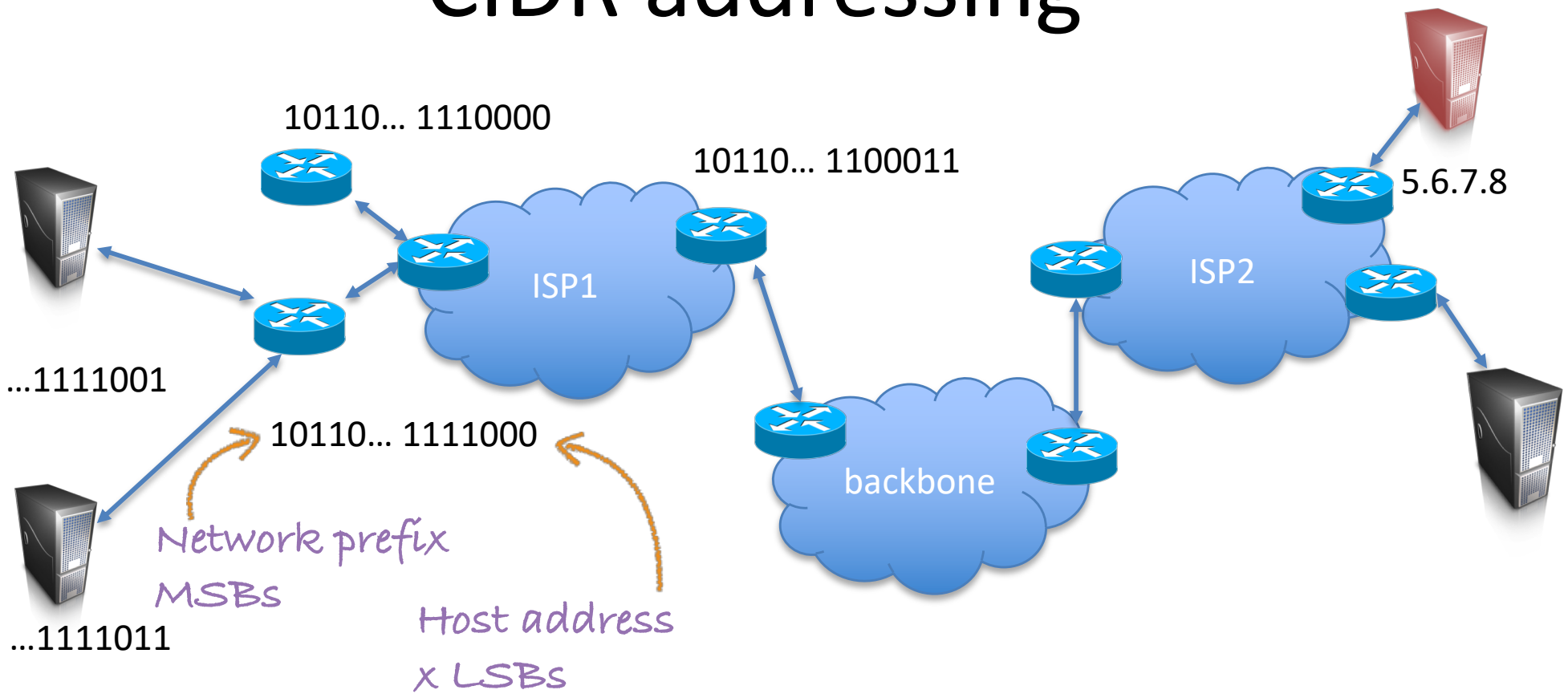
BGP

CS642: Computer Security

CIDR addressing

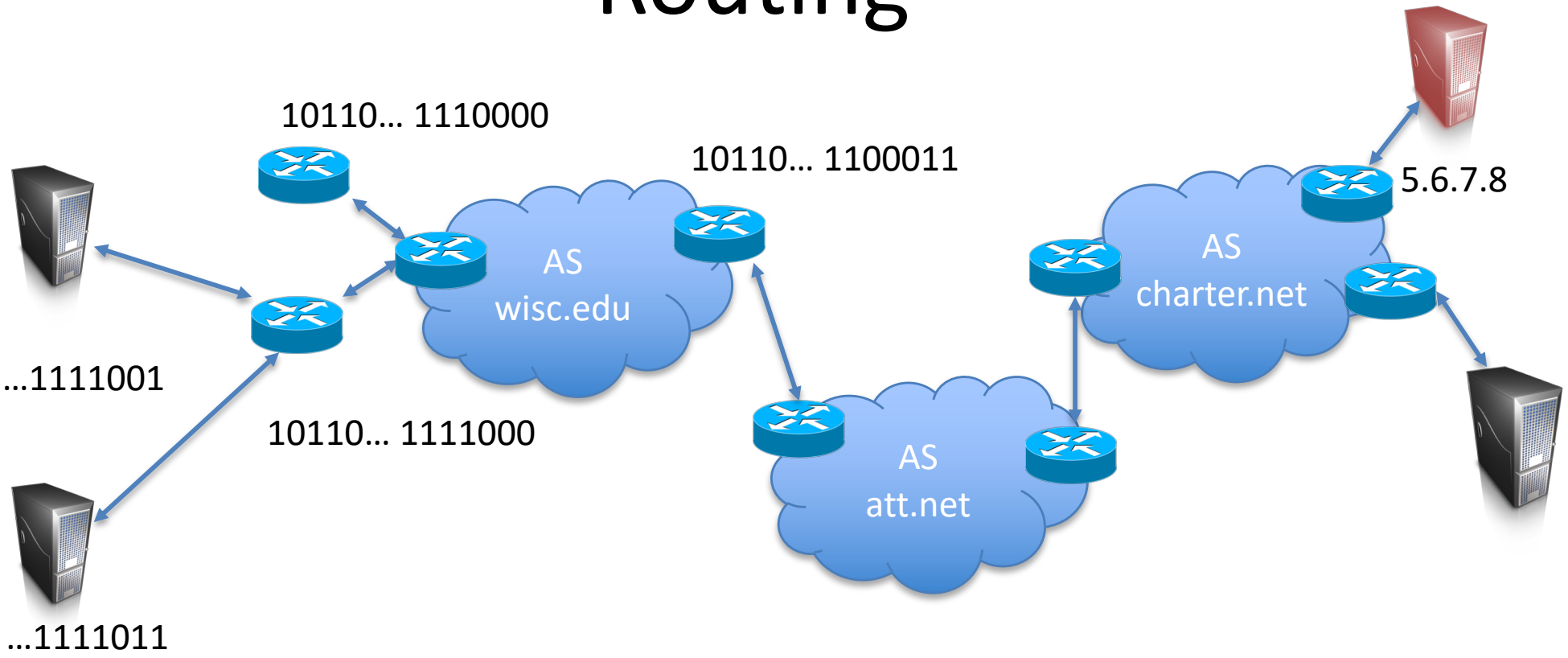


Classless inter-domain routing (CIDR)

Prefixes used to setup hierarchical routing:

- An organization assigned a.b.c.d/x
- It manages addresses prefixed by a.b.c.d/x

Routing



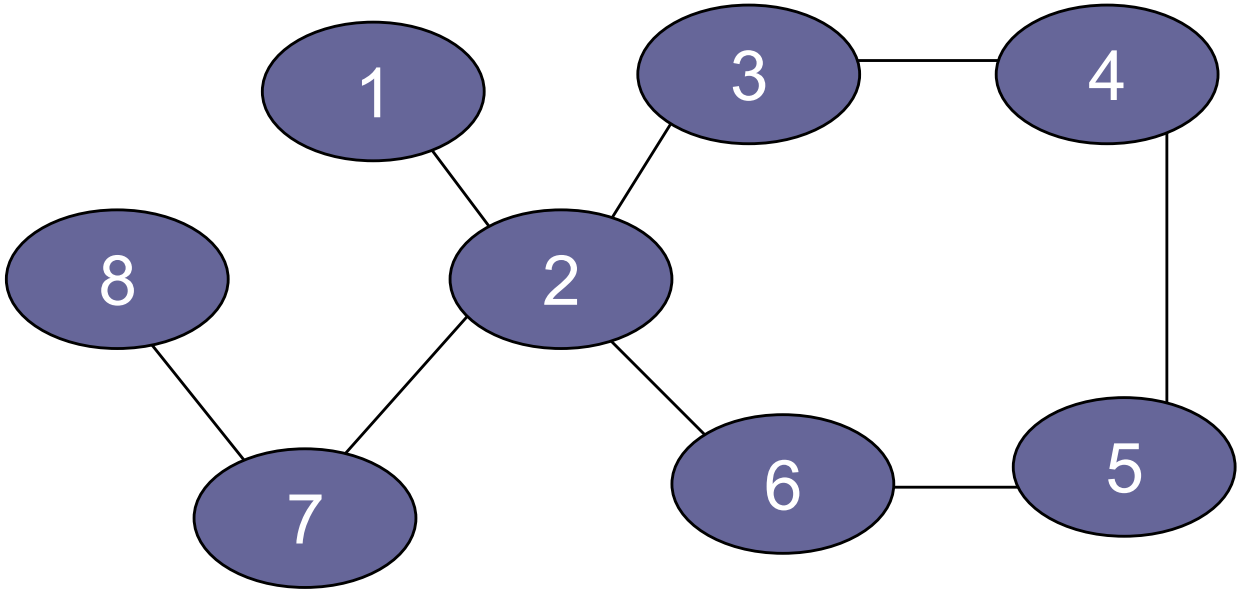
Autonomous systems (AS) are organizational building blocks

- Collection of IP prefixes under single routing policy
- wisc.edu

Within AS, might use RIP (Routing Information Protocol)

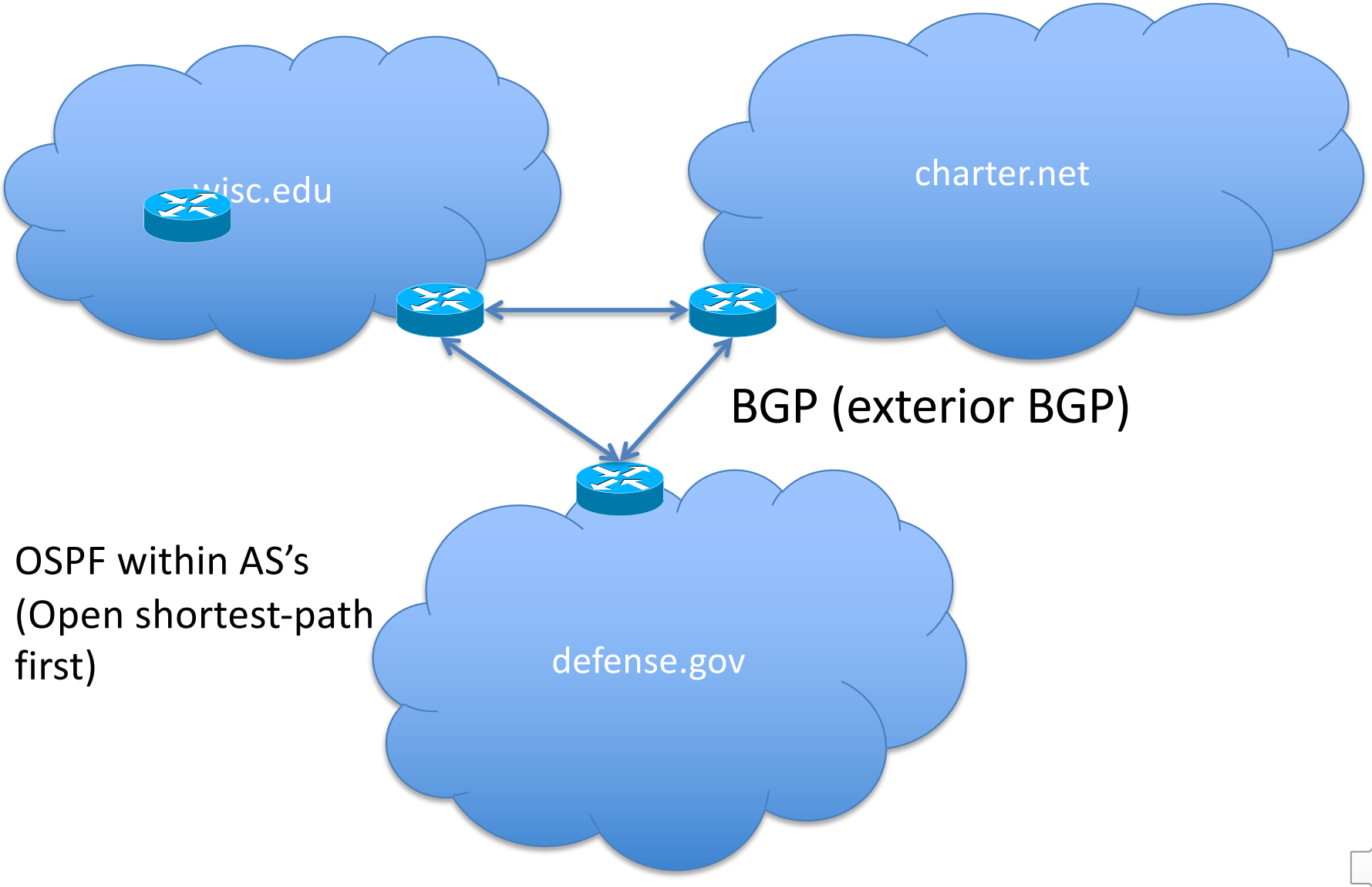
Between AS, use BGP (Border Gateway Protocol)

AS Categories



- **Stub:** connected to only on other AS
- **Multi-homed:** connected to multiple other AS
- **Transit:** routes traffic through it's AS for other AS's

BGP and routing

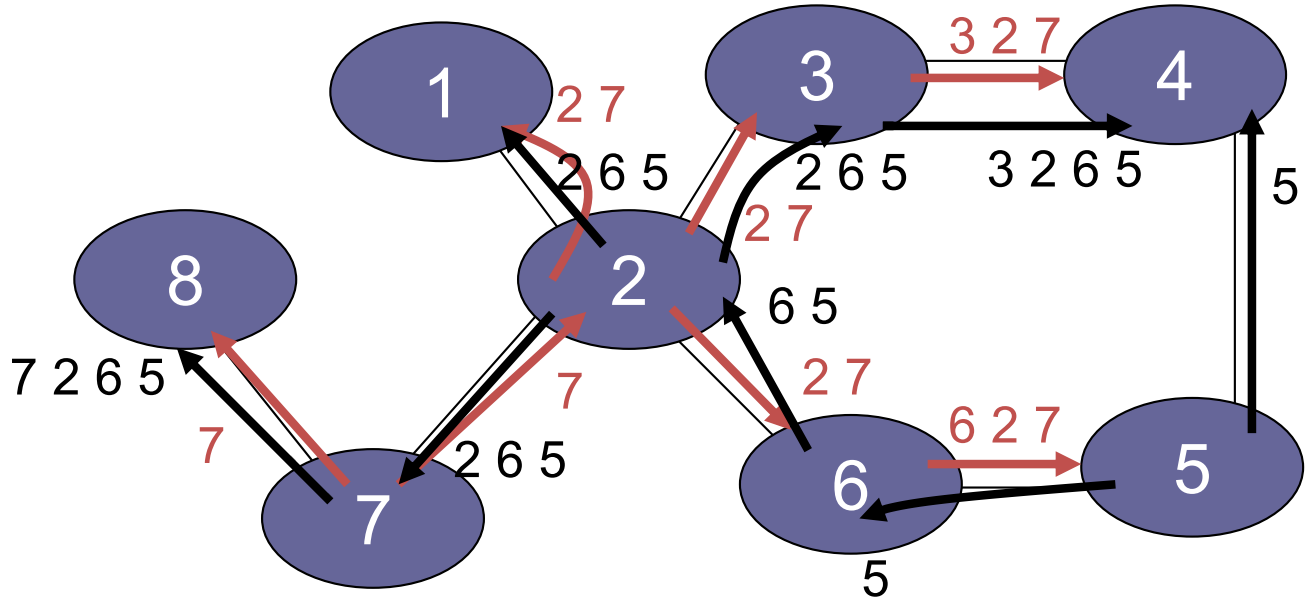


BGP

- Policy-based routing
  - AS can set policy about how to route
    - economic, security, political considerations
- BGP routers use TCP connections to transmit routing information
- Iterative announcement of routes

BGP example

[D. Wetherall]



- 2, 7, 3, 6 are Transit AS
- 8, 1 are Stub AS
- 4,5 multihomed AS
- Algorithm seems to work OK in practice
  - BGP does not respond well to frequent node outages

Routers prefer more specific routes:
128.64.45.0/24 over 128.64.0.0/16

IP hijacking

- BGP unauthenticated
  - Anyone can advertise any routes
  - False routes will be propagated
- This allows IP hijacking
  - AS announces it originates a prefix it shouldn’t
  - AS announces it has shorter path to a prefix
  - AS announces more specific prefix

Malicious or misconfigurations?

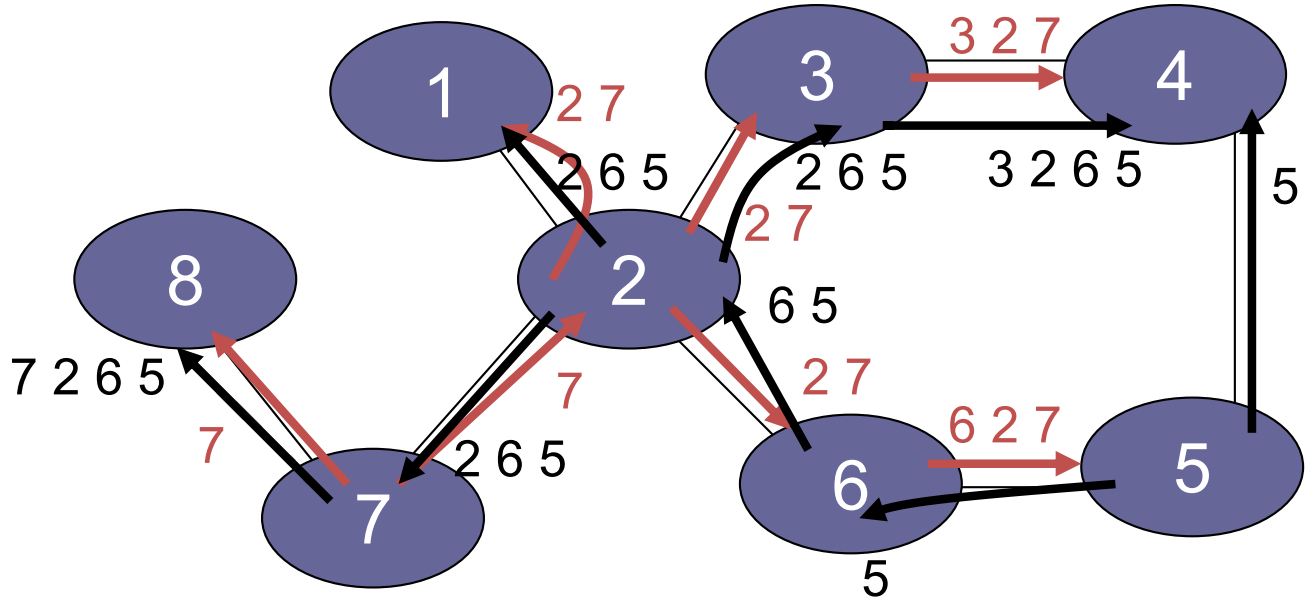
- AS 7007 incident in 1997
  - Florida exchange announces /24 routes for most of the internet go through it
- China Telecom hijacks large chunks of Internet in 2010
  - https://bgpmon.net/chinese-isp-hijacked-10-of-the-internet/
- Causes traffic to flow through announced A

Youtube incident

- Pakistan attempts to block Youtube
  - youtube is 208.65.152.0/22
  - youtube.com = 208.65.153.238
- Pakistan ISP advertises 208.65.153.0/24
  - more specific, prefix hijacking
- Internet thinks youtube.com is in Pakistan
- Outage resolved in 2 hours…

BGPsec

[D. Wetherall]



- Route announcements must be crypographically signed
  - AS can only advertise as itself
  - AS cannot advertise for IP prefixes it does not own
- Requires a public-key infrastructure (PKI)
- Still in development:
  - http://tools.ietf.org/html/draft-lepinski-bgpsec-protocol-00#ref-7

Internet Security

- Recurring themes:
  - Built without any authenticity mechanisms in mind
  - Functionality mechanisms (sequence #’s) become implicit security mechanisms
  - New attempts at backwards-compatible security mechanisms
    - IP -> IPsec
    - DNS -> DNSsec
    - BGP -> BGPsec