Computer Network Security

ECE 4112/6612
CS 4262/6262

Prof. Frank Li

```
* Welcome to CityPower Grid Rerouting *
Authorised Users only!
New users MUST notify Sys/Ops.

login:
```

```
EDITV1 sshnuke
rcr ebx, 1
bsr ecx, ecx
shrd ebx, edi, CL
```

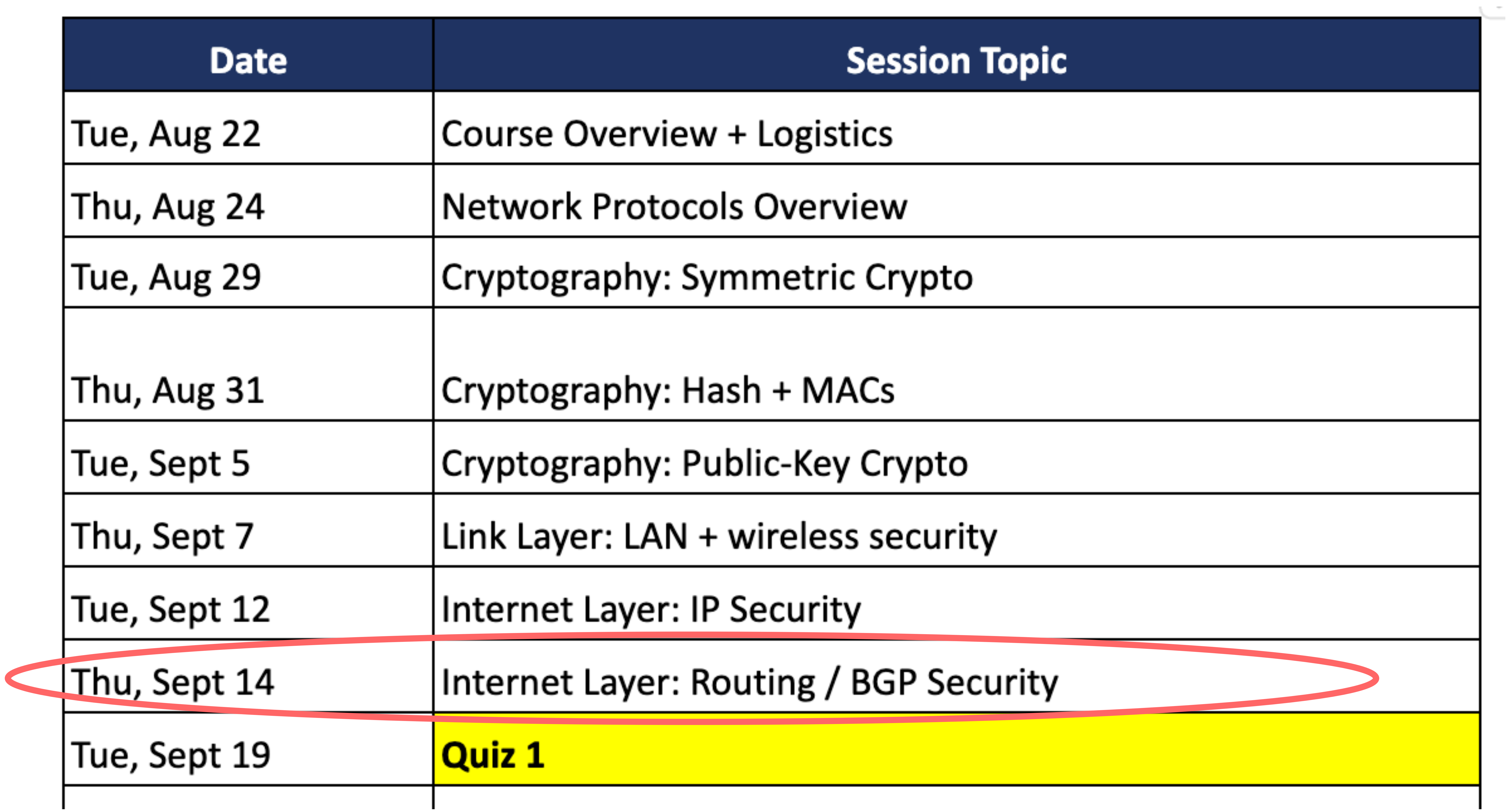
```
80/tcp     open       http
81/tcp     open       hosts2-ns
```

```
# nmap -v -sS -O 10.2.2.2
Starting nmap V. 2.54BETA25
Insufficient responses for TCP sequencing (3), OS detection may be less
accurate
Interesting ports on 10.2.2.2:
(The 1539 ports scanned but not shown below are in state: closed)
Port       State       Service
22/tcp     open        ssh

No exact OS matches for host

Nmap run completed -- 1 IP address (1 host up) scanneds
# sshnuke 10.2.2.2 -rootpw="Z10N0101"
Connecting to 10.2.2.2:ssh ... successful.
Attempting to exploit SSHv1 CRC32 ... successful.
Reseting root password to "Z10N0101".
System open: Access Level <9>
# ssh 10.2.2.2 -l root
root@10.2.2.2's password:
```

Logistics



Date	Session Topic
Tue, Aug 22	Course Overview + Logistics
Thu, Aug 24	Network Protocols Overview
Tue, Aug 29	Cryptography: Symmetric Crypto
Thu, Aug 31	Cryptography: Hash + MACs
Tue, Sept 5	Cryptography: Public-Key Crypto
Thu, Sept 7	Link Layer: LAN + wireless security
Tue, Sept 12	Internet Layer: IP Security
Thu, Sept 14	Internet Layer: Routing / BGP Security
Tue, Sept 19	**Quiz 1**

Logistics

Quiz 1 next Tuesday:

- Open paper notes (no electronic devices, including tablets, laptops, phones)
- One seat between each person (including diagonally)

HW1 solutions posted

Project groups assigned (for those who filled out the survey)

Continuing with Network Layer

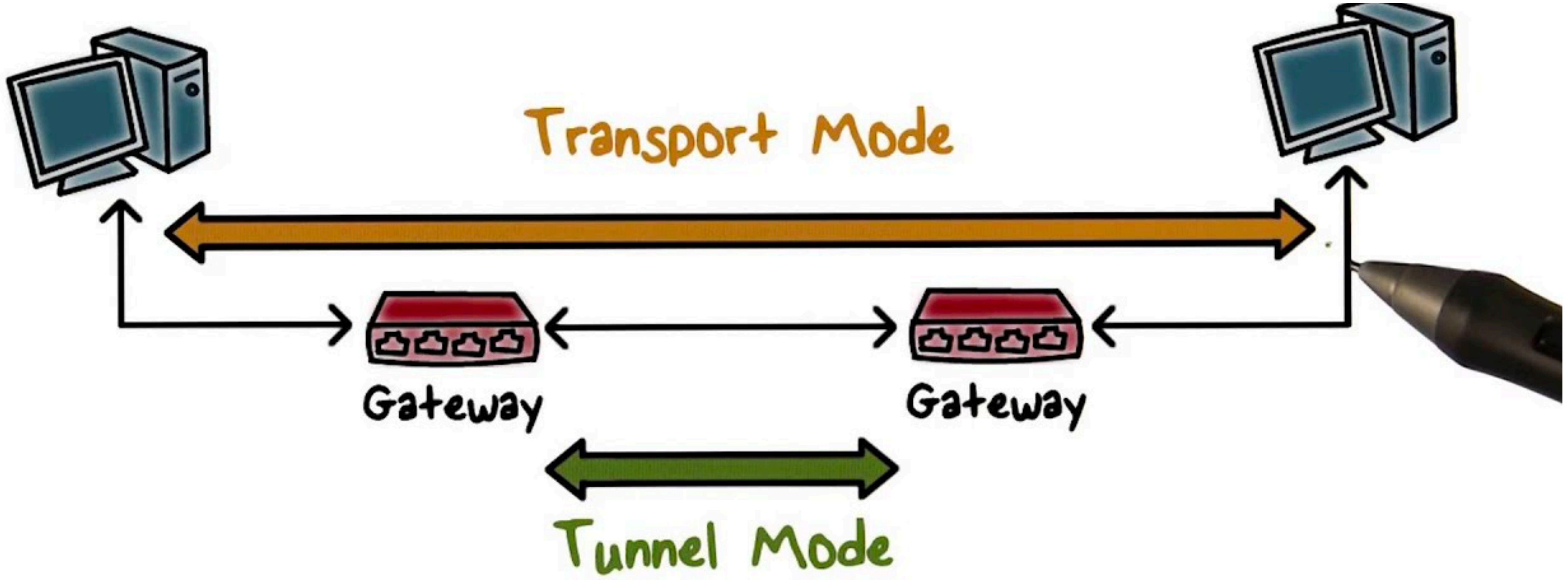
IP Packet Vulnerability #1

IP header + payload is unencrypted (no confidentiality/integrity built in)

IPSec

IPSec: Use encryption/MACs for confidentiality/integrity.

- Requires key exchange/establishment b/w IPSec endpoints
- Adopted in certain situations (e.g., b/w networks of the same company)
- Two IPSec modes:
  - Transport Mode (host <-> host)
  - Tunnel Mode (gateway <-> gateway, VPN-like)



IPSec

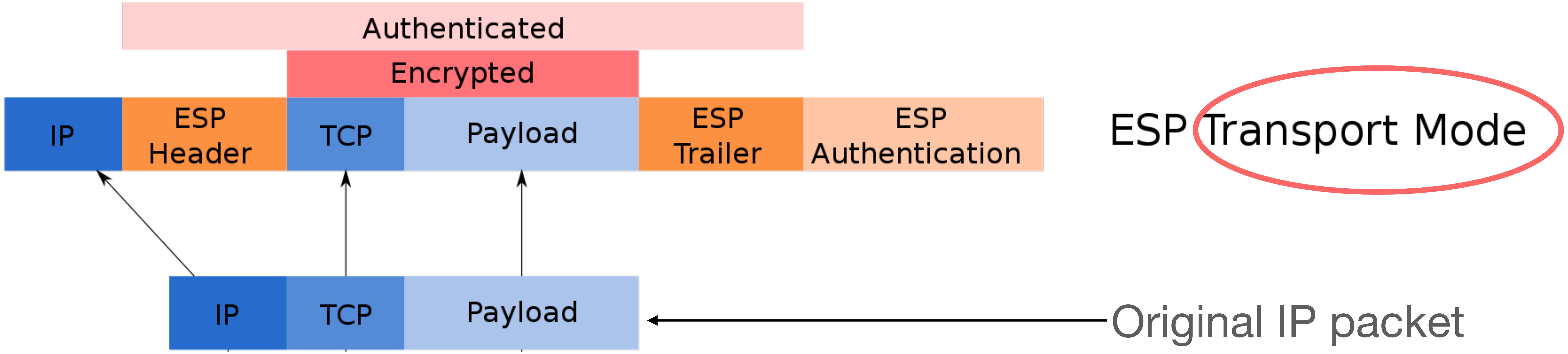
IPSec: Different security functionalities provided.

- **Encapsulating Security Payload (ESP)** functionality provides confidentiality + integrity
- **Authentication Headers (AH)** functionality provides only integrity (not often used)

IPSec

IPSec: Different security functionalities provided.

- **Encapsulating Security Payload (ESP)** functionality provides confidentiality + integrity

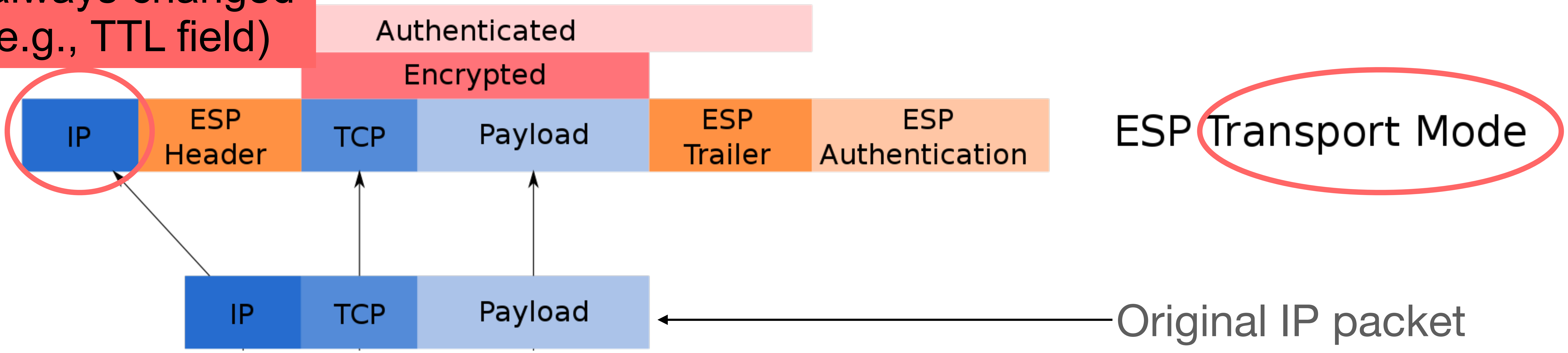


IPSec

IPSec: Different security functionalities provided.

- **Encapsulating Security Payload (ESP)** functionality provides confidentiality + integrity

Why no integrity for IP header?
B/c header always changed each hop (e.g., TTL field)



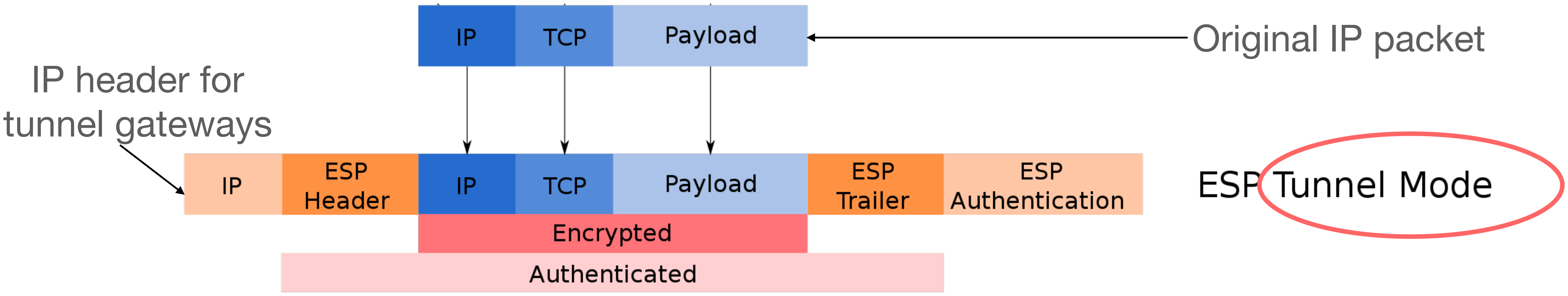
ESP Transport Mode

Original IP packet

IPSec

IPSec: Different security functionalities provided.

- **Encapsulating Security Payload (ESP)** functionality provides confidentiality + integrity



IPSec

Recap:

- Provides confidentiality/integrity for IP packet
- Transport mode gives end-to-end benefits, but no IP header encryption/integrity
- Tunnel mode provides full IP confidentiality/integrity in transit across the Internet, but unencrypted between host and gateway (also requires gateways to be configured)
- In practice, requires host pre-configuration (e.g., public/private keys + certificates + PKI), so most apt for use within an organization/company (e.g., supported by cloud providers like Amazon and Cloudflare)

IPSec in IPv6

- In theory, IPv6 standard says to use **"opportunistic"** IPSec by default
  - Opportunistic: even w/o a global PKI (where we can verify someone else's public key), we can just use the other person's key. As long as there's not active MITM attack, this provides confidentiality/integrity.
  - Hasn't been deployed much in practice yet

IP Packet Vulnerability #2

IP source address can be forged/spoofed.

Defenses:

- **Ingress filtering:** A network should not accept/forward incoming packets where the source IP address is not within the origin network's IP range.
- **Egress filtering:** A network should not send outbound packets where the source IP address is not within the network's IP range.

If all networks did this filtering, spoofing will be largely infeasible. Many do! But not all :(

IP Packet Vulnerability #2

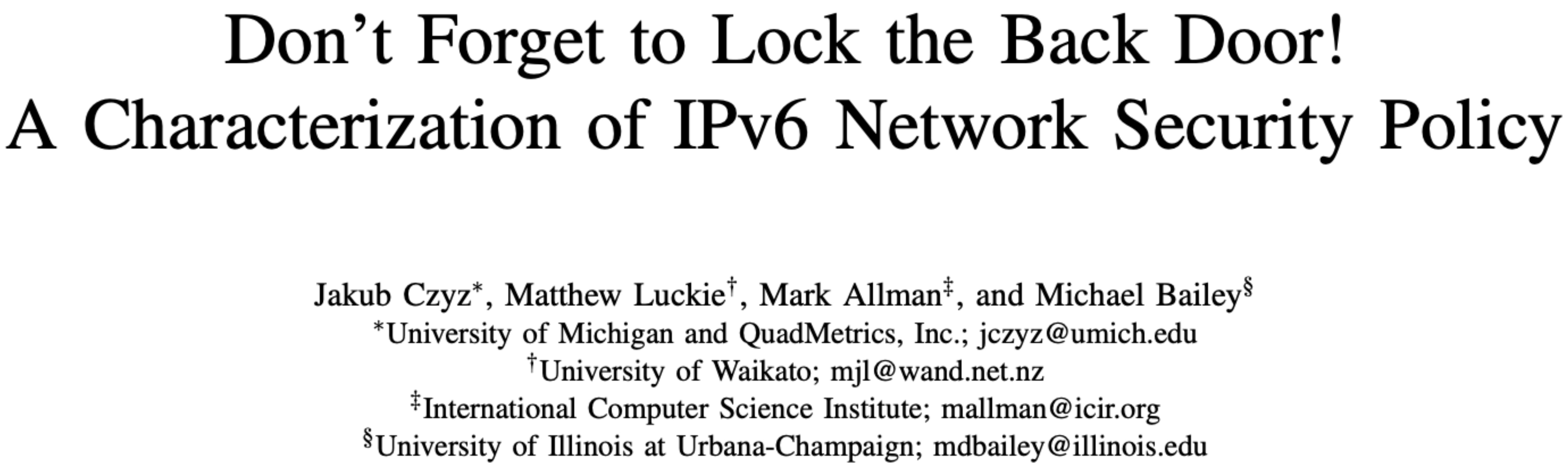
Why isn't ingress/egress filtering universal?

- Filtering may require some work (e.g., implementation, administrative, policy) by a network that doesn't directly benefit it
- Filtering's benefits really arise only if most/all networks implement. This can lead to a lack of incentivies for early adoption
- **But** there's hope. Today ~80% of networks disallow spoofing.

IPv6-Specific Security Issues

IPv6 is a separate protocol + software stack

- IPv6 doesn't need NAT (b/c plenty of addresses for every device). But NAT used to hide IPv4 end hosts. IPv6 networks with NATs may lose this property.
- Instead, a network firewall should be used to protect a network. **But** many networks forget to deploy their IPv4 firewall for IPv6. So IPv6 remains open/ unprotected.



Don’t Forget to Lock the Back Door!
A Characterization of IPv6 Network Security Policy

Jakub Czyz[*], Matthew Luckie[†], Mark Allman[‡], and Michael Bailey[§]
[*]University of Michigan and QuadMetrics, Inc.; jczyz@umich.edu
[†]University of Waikato; mjl@wand.net.nz
[‡]International Computer Science Institute; mallman@icir.org
[§]University of Illinois at Urbana-Champaign; mdbailey@illinois.edu

IPv6-Specific Security Issues

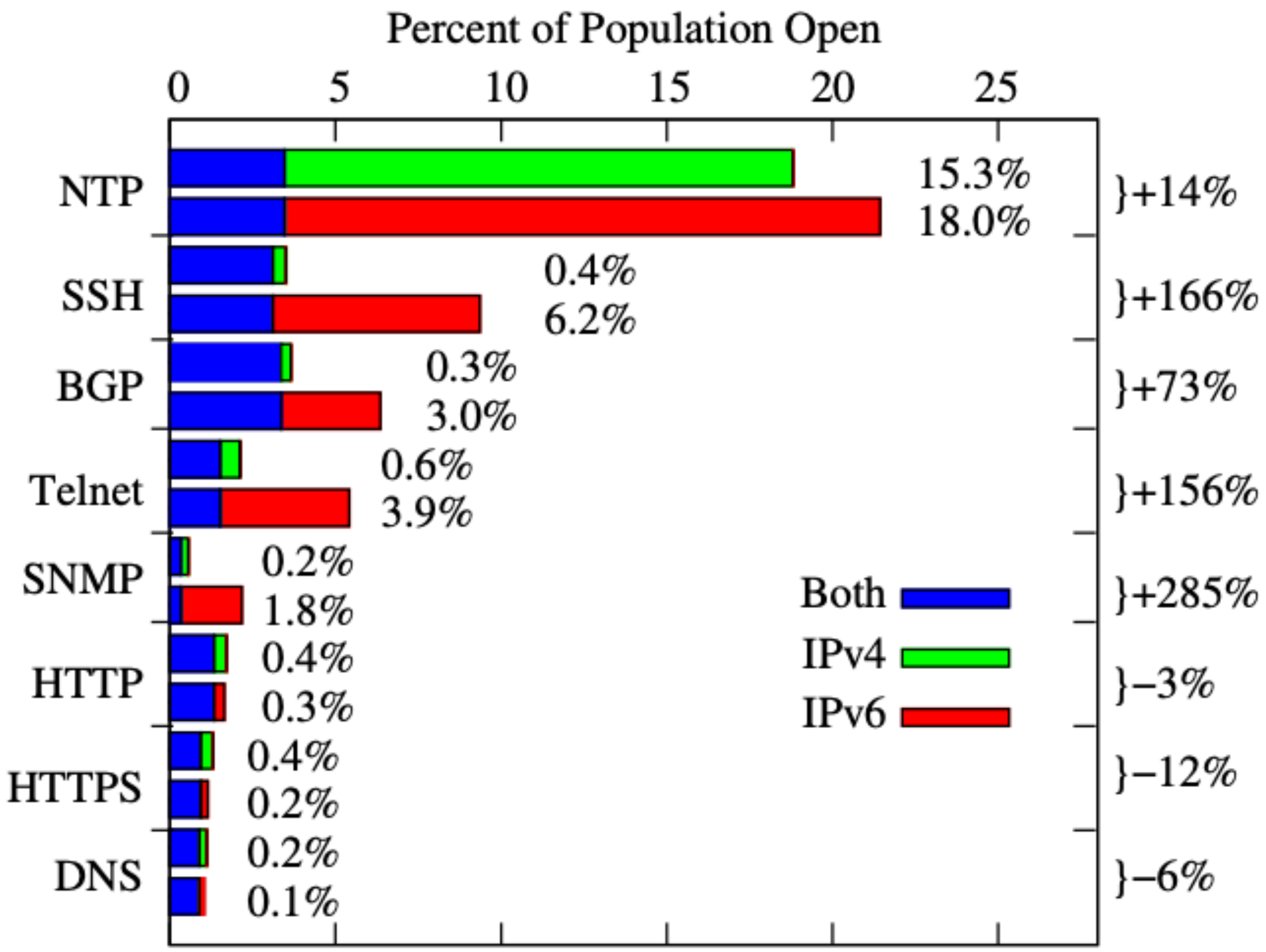
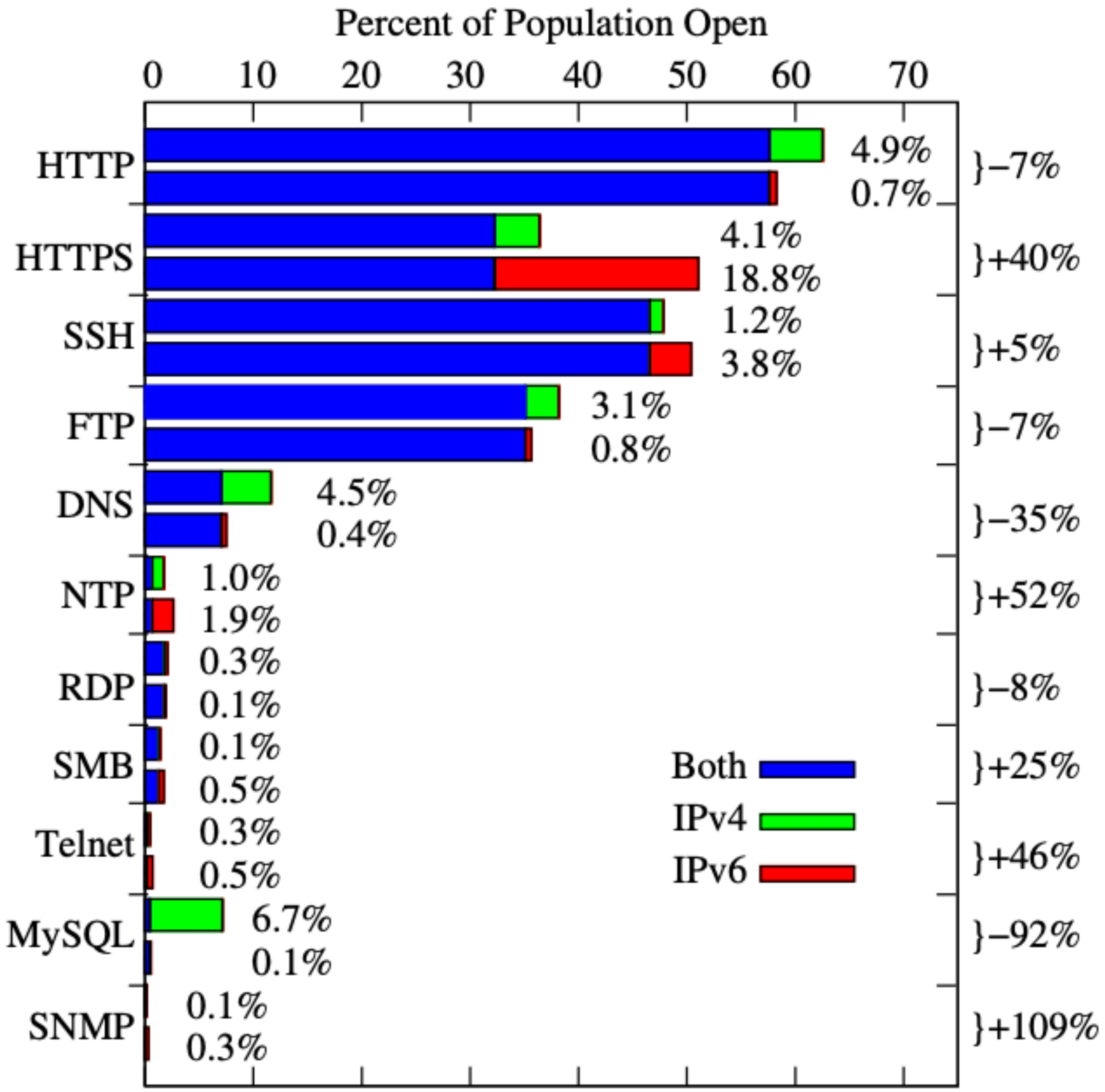


Fig. 1: Percentage of 25K dual-stack routers ($\mathcal{R}_B$) responsive to ping that were open via IPv4 and/or IPv6 for each application tested. For each application, the green bar corresponds to reachability (connection success) over only IPv4, the red bar only IPv6, and the blue bar reachability over both. Beside each bar we report the percentage of hosts tested that were only reachable by IPv4 or IPv6, and beside each application is the percentage difference in reachability over IPv6 compared to IPv4.

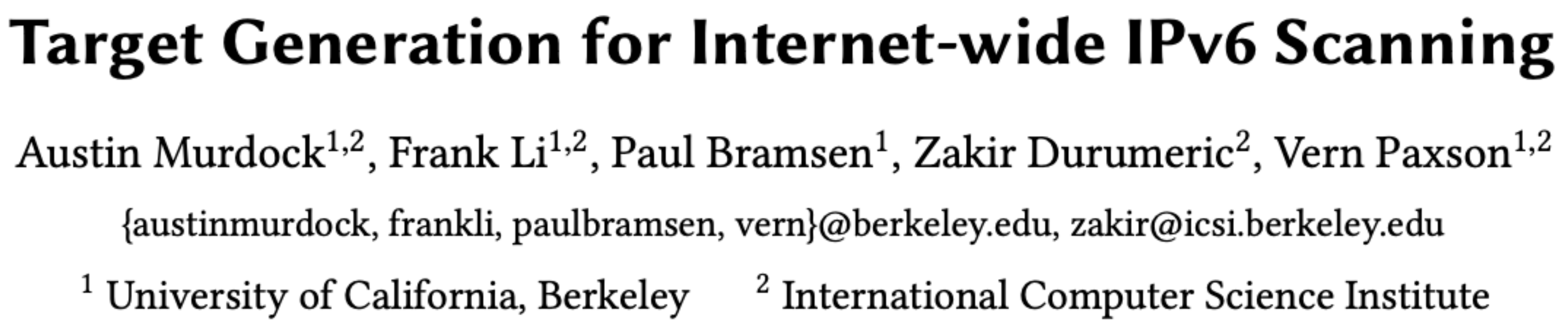


(a) Servers ($\mathcal{S}_B$)

IPv6-Specific Security Issues

IPv6 address space is huge

- Some networks rely on security through obscurity, assuming that IPv6 is too large for attackers to find their host's IPs. Not true! IPs in various dataset, plus active research on ways to predict where active IPv6 addresses are.



Target Generation for Internet-wide IPv6 Scanning

Austin Murdock[1,2], Frank Li[1,2], Paul Bramsen[1], Zakir Durumeric[2], Vern Paxson[1,2]

{austinmurdock, frankli, paulbramsen, vern}@berkeley.edu, zakir@icsi.berkeley.edu

[1] University of California, Berkeley [2] International Computer Science Institute

- Data structures (e.g., tables) tracking all IP addresses can get overly large, leading to resource exhaustion vulnerabilities.
  - For example, most IPv4 LANs are /24s, with only 2^8=256 addresses. An IPv6 LAN may be a /64, with 2^64 = HUGE number of addresses!
  - Any device tracking IP addresses (e.g., routers) need to manage memory carefully.

ICMP

Internet Control Message Protocol (ICMP)

- Simple messages within single IP packets (auxiliary to IP, so network layer)
- Used for network testing, debugging, and diagnostics
  - **Ping:** Test for liveness and communication round-trip time (RTT).
    Send ICMP "Echo" request packet with a message, receiver sends back an ICMP "Echo" response packet with the original message.

ICMP

Internet Control Message Protocol (ICMP)

- Simple messages within single IP packets (thus network layer)
- Used for network testing, debugging, and diagnostics
  - **Diagnostics:** Send ICMP packets indicating an error happened in transit.
    - Time Exceeded: If a router sees that an IP packet's TTL is now 0, it can drop the packet. Often it'll send an ICMP Time Exceeded packet back to the sender.

    - **Unreachable:** If a router gets an IP packet and doesn't know how to deliver it to its destination, it can send an ICMP Destination Unreachable packet to the sender.

ICMP

Internet Control Message Protocol (ICMP)

- Simple messages within single IP packets (thus network layer)
- Used for network testing, debugging, and diagnostics
  - **Traceroute:** Finds the routers in the path to a destination.
    1. Send an ICMP request packet to the destination, with an IP TTL of 1.
    2. First router receives this packet, decrease the TTL, and since the TTL is zero, it can drop the packet, and send back an ICMP Time Exceeded message.
    3. Repeat with a TTL of 2 (to reach the second router), increasing the TTL until you reach the destination.

ICMP

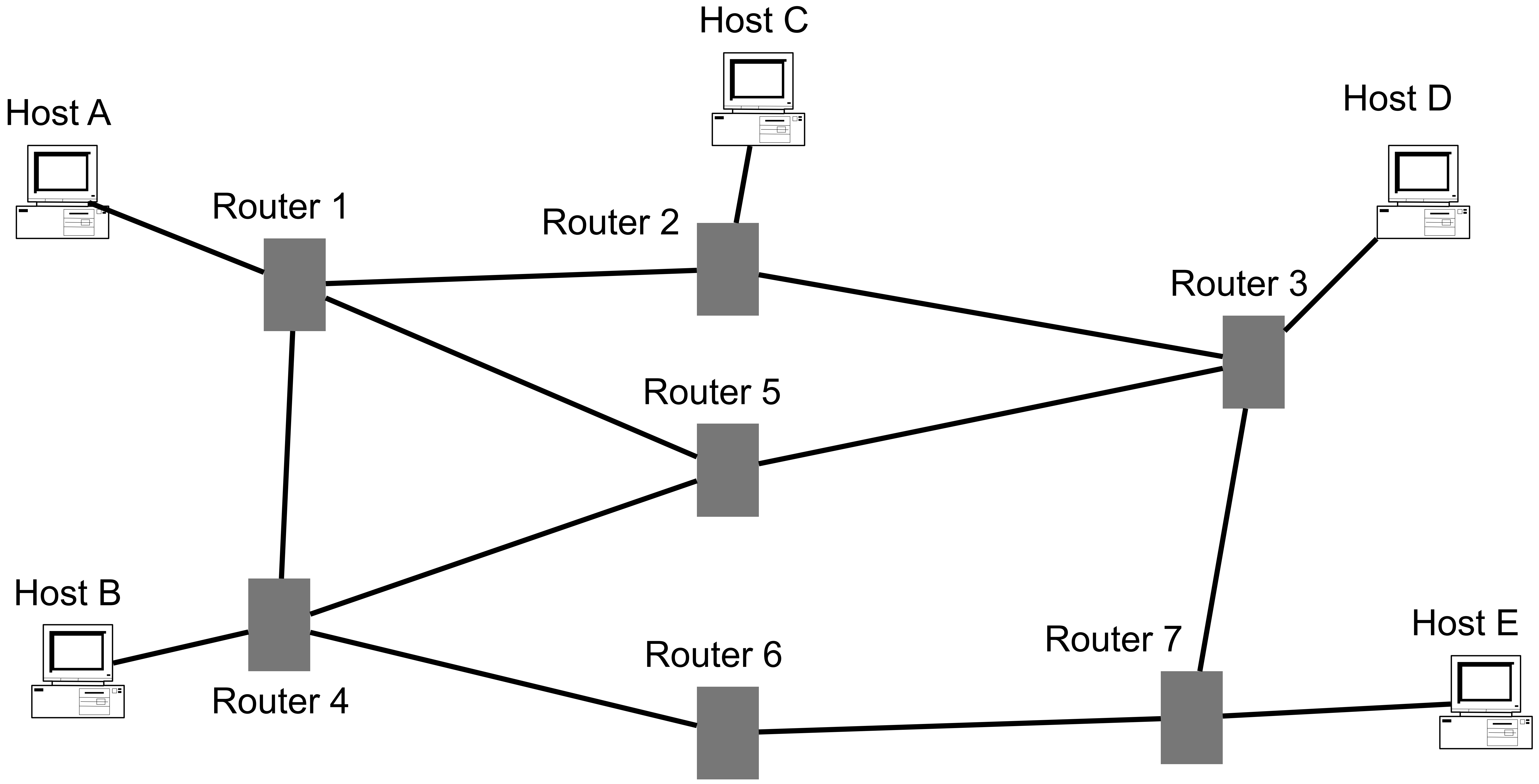
Security issues:

- **Main issue:** Potentially allows for attacker reconnaissance of a network. As a result, many servers/routers/networks disable certain ICMP replies.
- ICMP packets can be used in certain types of attacks, particularly denial-of-service attacks
  - **ICMP floods:** send *tons* of ICMP requests that each need to be serviced, which overloads the server.
  - **ICMP "Ping of Death" + Teardrop Attack:** Historically, a very large packet or a malformed packet could cause network stacks/devices to crash (e.g., due to memory management issues). Less of an issue today though.

Routing

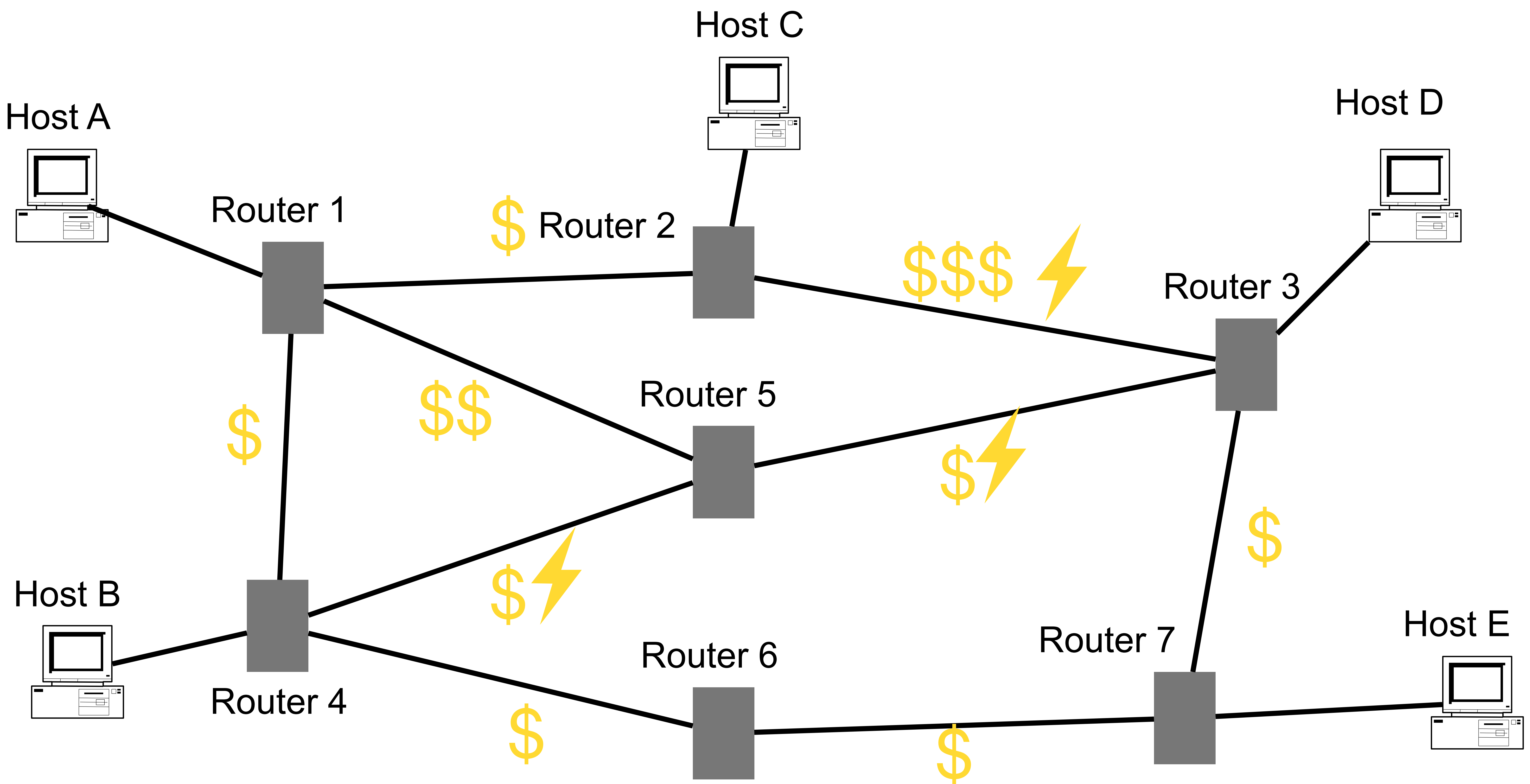
Routing

Host A wants to communicate with Host D. How do you figure out which route to take?



Routing

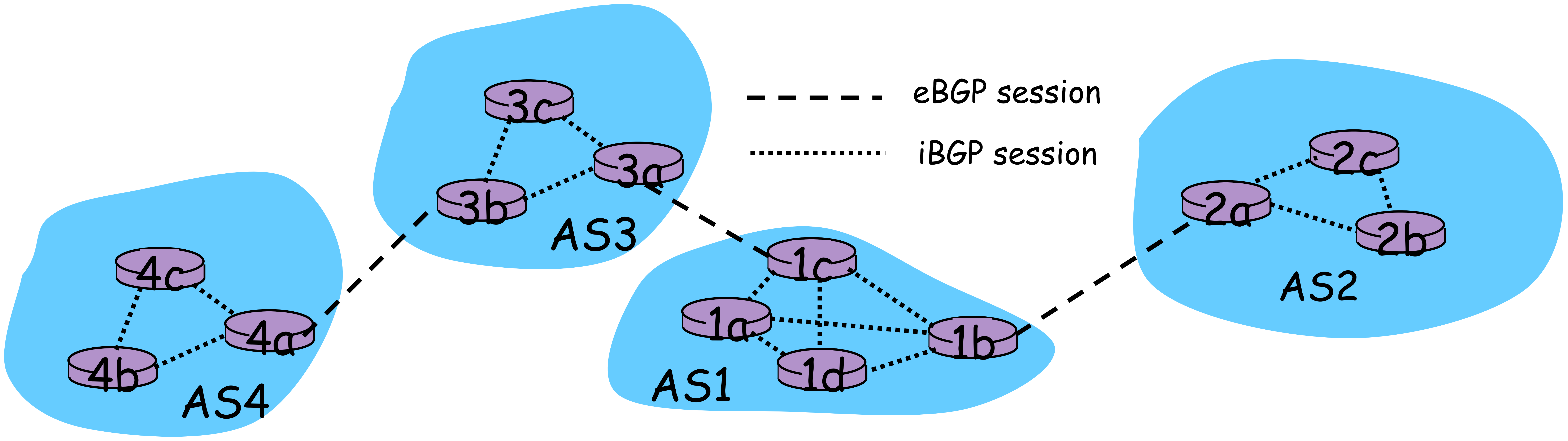
Host A wants to communicate with Host D. How do you figure out which route to take?



Routing via BGP

Border Gateway Protocol (BGP): Allows networks, called Autonomous Systems (AS), to advertise reachability and route attribute information (e.g., which subnets is an AS willing to deliver traffic to). *Note: BGP is a TCP protocol (so application layer), but routing is a network layer task.*

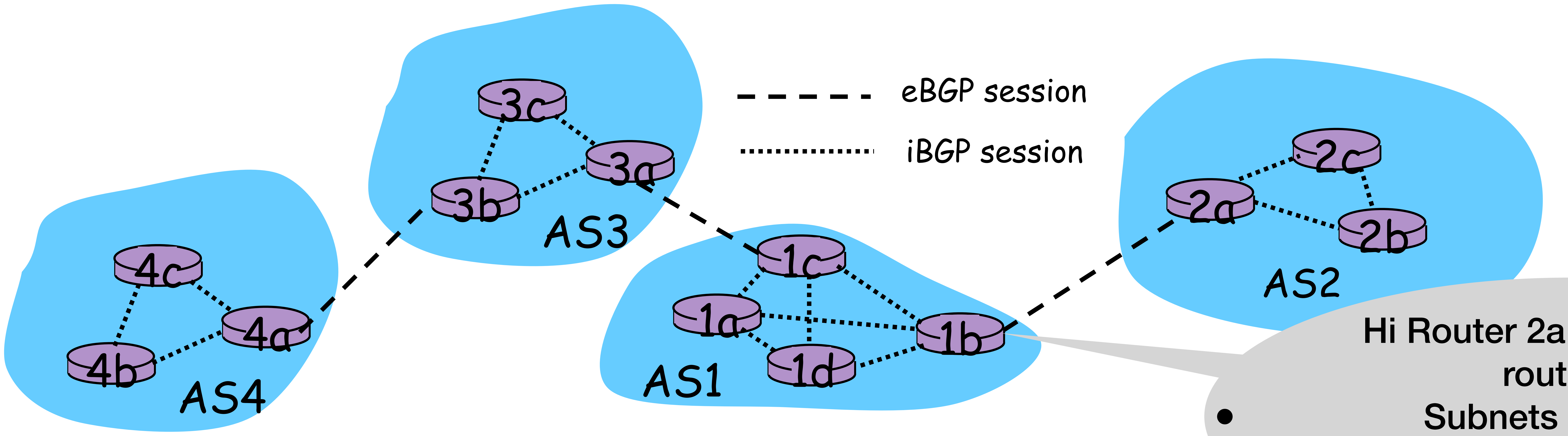
- Within a network/AS, iBGP is run between routers
- Between networks/ASes, eBGP is run between border routers (BGP peers)



Routing via BGP

Border Gateway Protocol (BGP): Allows networks, called Autonomous Systems (AS), to advertise reachability and route attribute information (e.g., which subnets is an AS willing to deliver traffic to). *Note: BGP is a TCP protocol (so application layer), but routing is a network layer task.*

- Within a network/AS, iBGP is run between routers
- Between networks/ASes, eBGP is run between border routers (BGP peers)



Hi Router 2a in AS2, I can route to:

- Subnets X, Y in AS1
- Subnets A, B in AS3
- Subnet M in AS 4

BGP Route/Path Attributes

BGP peers advertise/announce subnet prefixes they can route to, and attributes of those routes. Example attributes:

- AS-PATH: List of ASes along the route (e.g., AS1-> AS3->AS4). Can avoid routing loops by checking this list.
- NEXT-HOP: IP address of the next hop router in the route to a subnet

AS Relationship

BGP peers have policies on which announcements to make and which to accept/decline (often based on business relationships b/w ASes).

- AS1 is a customer of AS2, meaning AS1 pays AS2 to route traffic to/from AS1.
  - AS2 will announce to AS1 all routes that it knows (so that AS1 might route through AS2, paying $).
  - AS2 will announce to all other ASes routes to AS1 (so other ASes might route to AS1 through AS2, again costing AS1 money).
  - AS1 will accept AS2's announced routes, unless it has a cheaper option.
- AS1 and AS3 establish a peering relationship, where they will route each other's traffic for free.
  - AS1 and AS3 will share subnet reachability info with each other based on their business agreement, and both will happily accept each other's advertised routes (b/c free routing)

BGP Route Selection

A router may learn multiple routes to the same subnet/prefix. How to decide which route to select? Simplified decision process (in order of preference):

1. Route preference value (e.g. peering vs $$$)
2. Shortest AS-PATH
3. Closest NEXT-HOP (e.g., round-trip time)
4. Further tie breakers

When routing to a specific IP address, a router finds the most specific subnet/prefix it can route to based on *longest prefix match,* and uses the selected route for that prefix.

Example: Destination = 108.0.1.2

Routing Table:

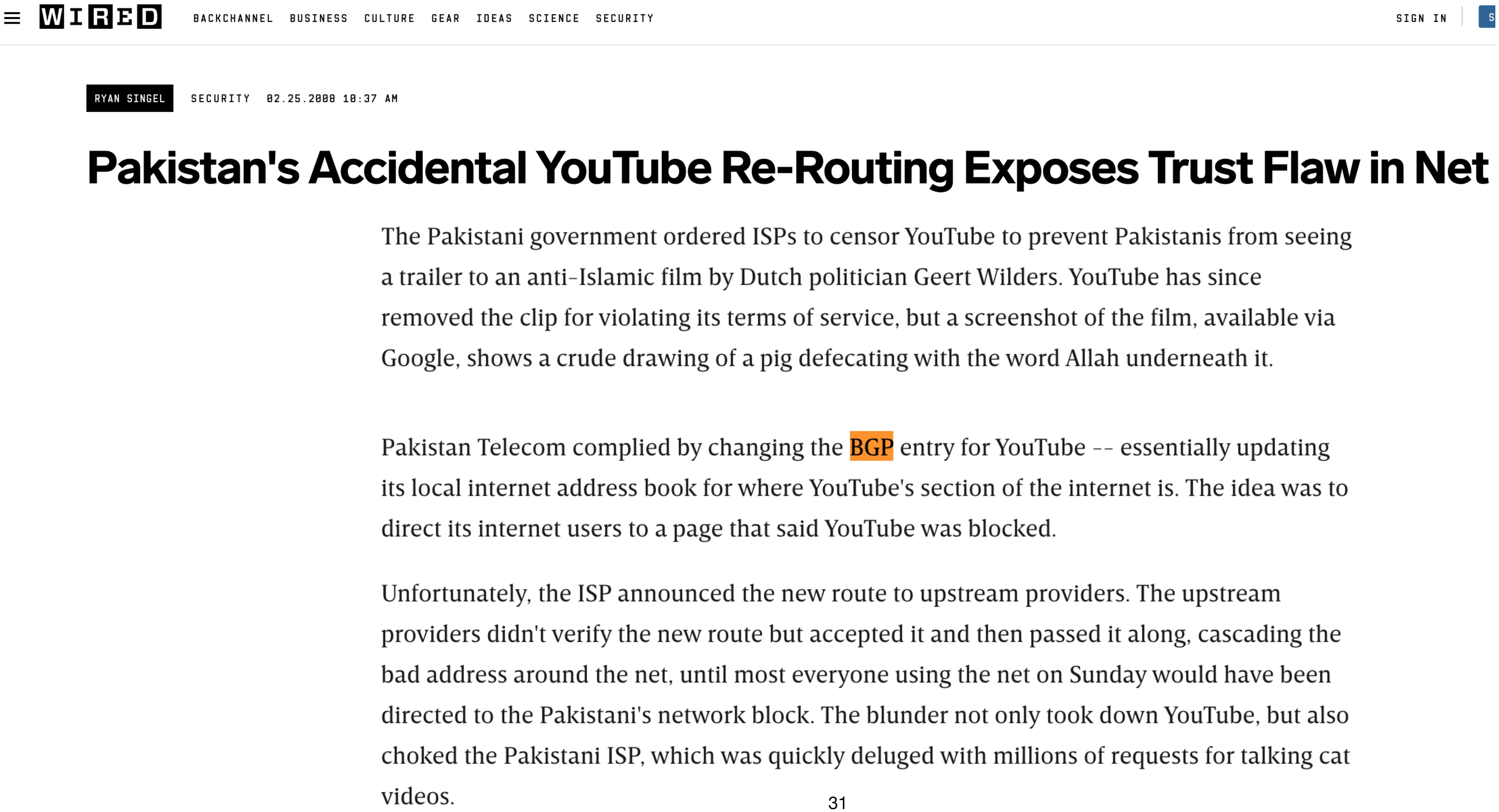
Prefix	**Route AS-PATH**
108.0.0.0/8	AS2, AS17
108.0.1.0/24	AS3, AS18, AS4

BGP Security Issue

An AS can announce (either maliciously or by accident) invalid/incorrect routes, potentially redirecting traffic to a destination. This is called BGP hijacking.

- Requires other ASes to accept the announced route, but this can often happen by announcing a very specific route (e.g., long prefix).

BGP Hijacking



RYAN SINGEL SECURITY 02.25.2008 10:37 AM

Pakistan's Accidental YouTube Re-Routing Exposes Trust Flaw in Net

The Pakistani government ordered ISPs to censor YouTube to prevent Pakistanis from seeing a trailer to an anti-Islamic film by Dutch politician Geert Wilders. YouTube has since removed the clip for violating its terms of service, but a screenshot of the film, available via Google, shows a crude drawing of a pig defecating with the word Allah underneath it.

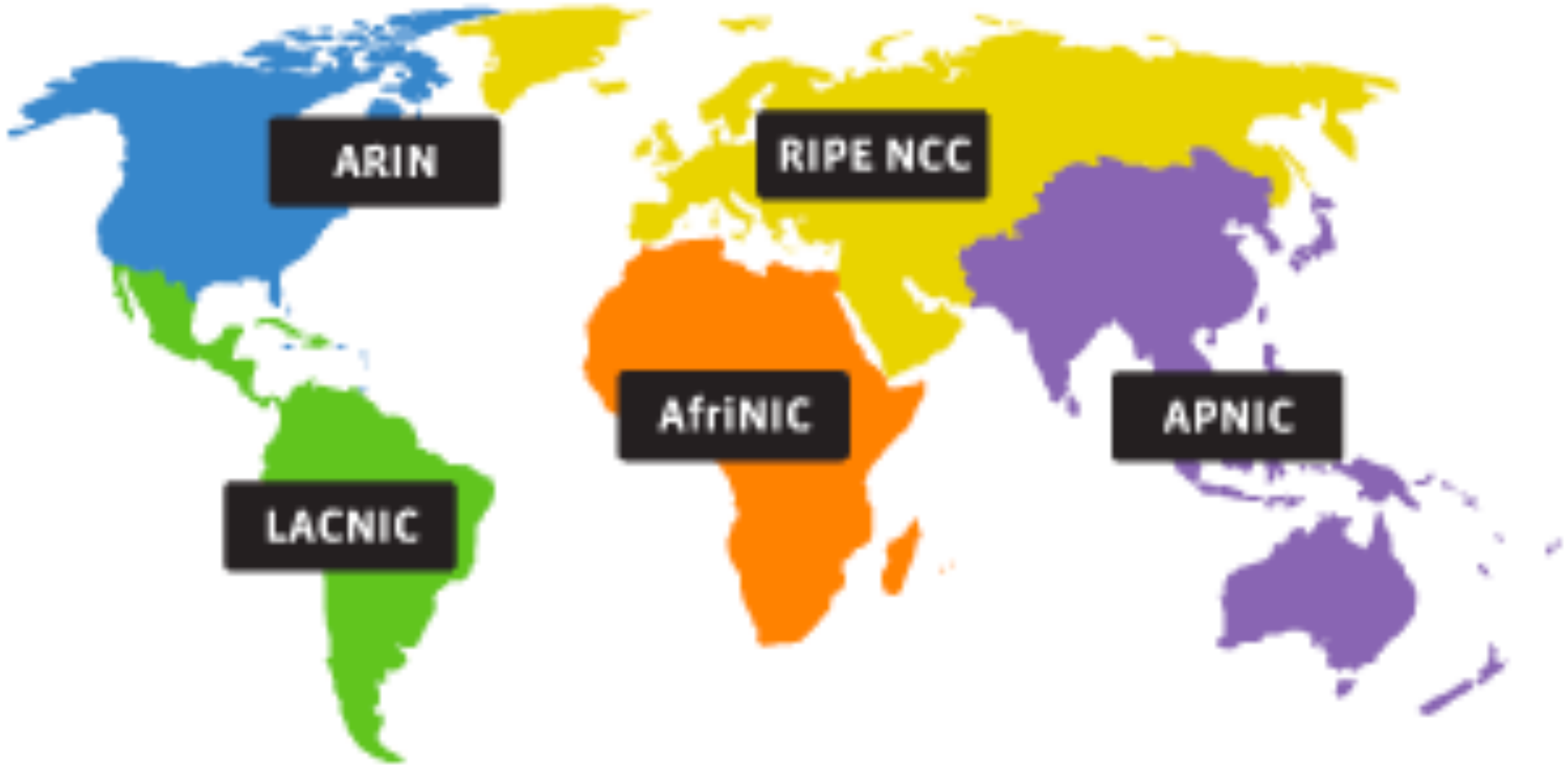
Pakistan Telecom complied by changing the BGP entry for YouTube -- essentially updating its local internet address book for where YouTube's section of the internet is. The idea was to direct its internet users to a page that said YouTube was blocked.

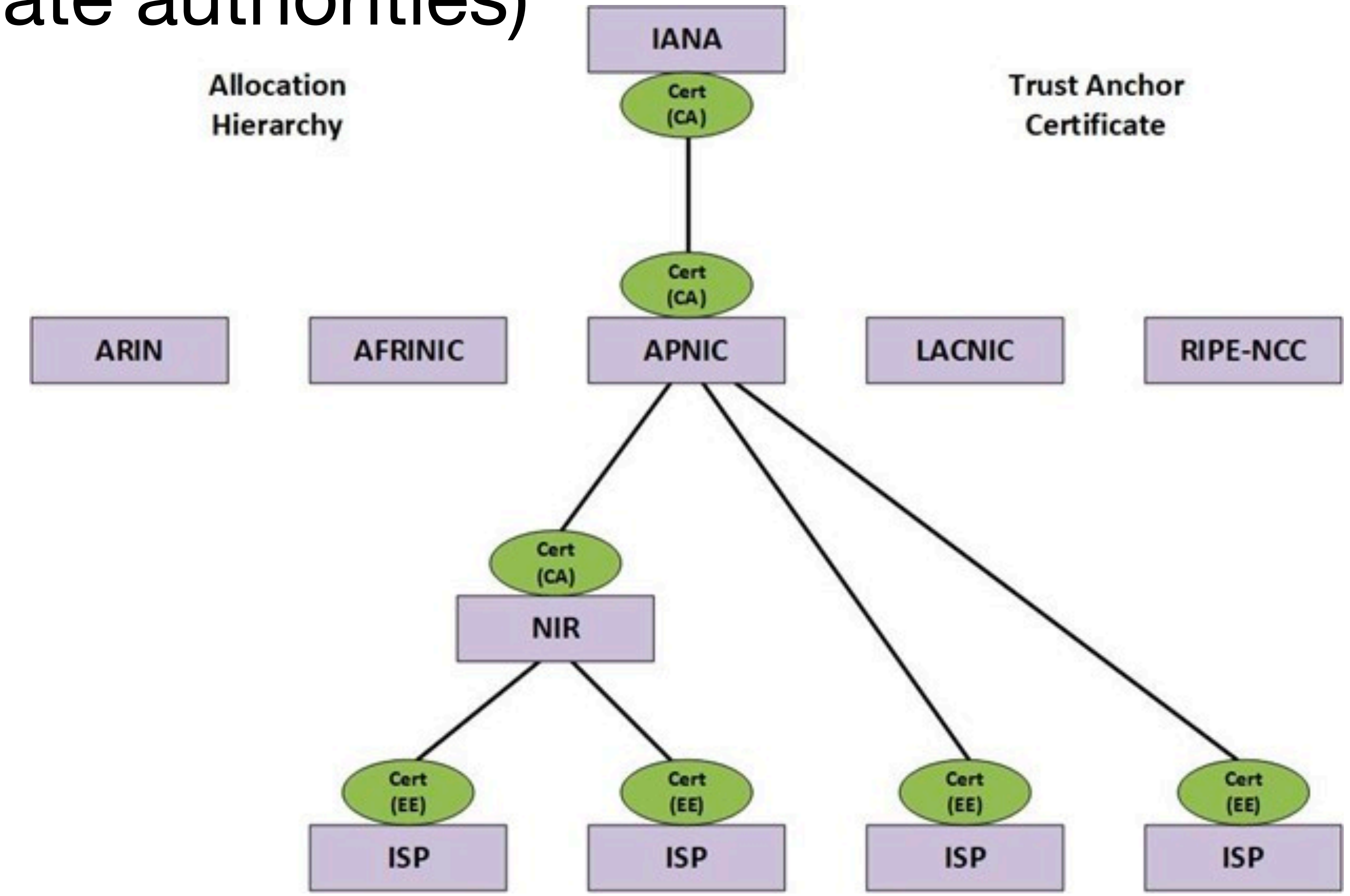
Unfortunately, the ISP announced the new route to upstream providers. The upstream providers didn't verify the new route but accepted it and then passed it along, cascading the bad address around the net, until most everyone using the net on Sunday would have been directed to the Pakistani's network block. The blunder not only took down YouTube, but also choked the Pakistani ISP, which was quickly deluged with millions of requests for talking cat videos.

BGP Defense

Internet Assigned Numbers Authority (IANA) and the 5 Regional Internet Registries (RIR) decide which IP addresses belong to each AS.

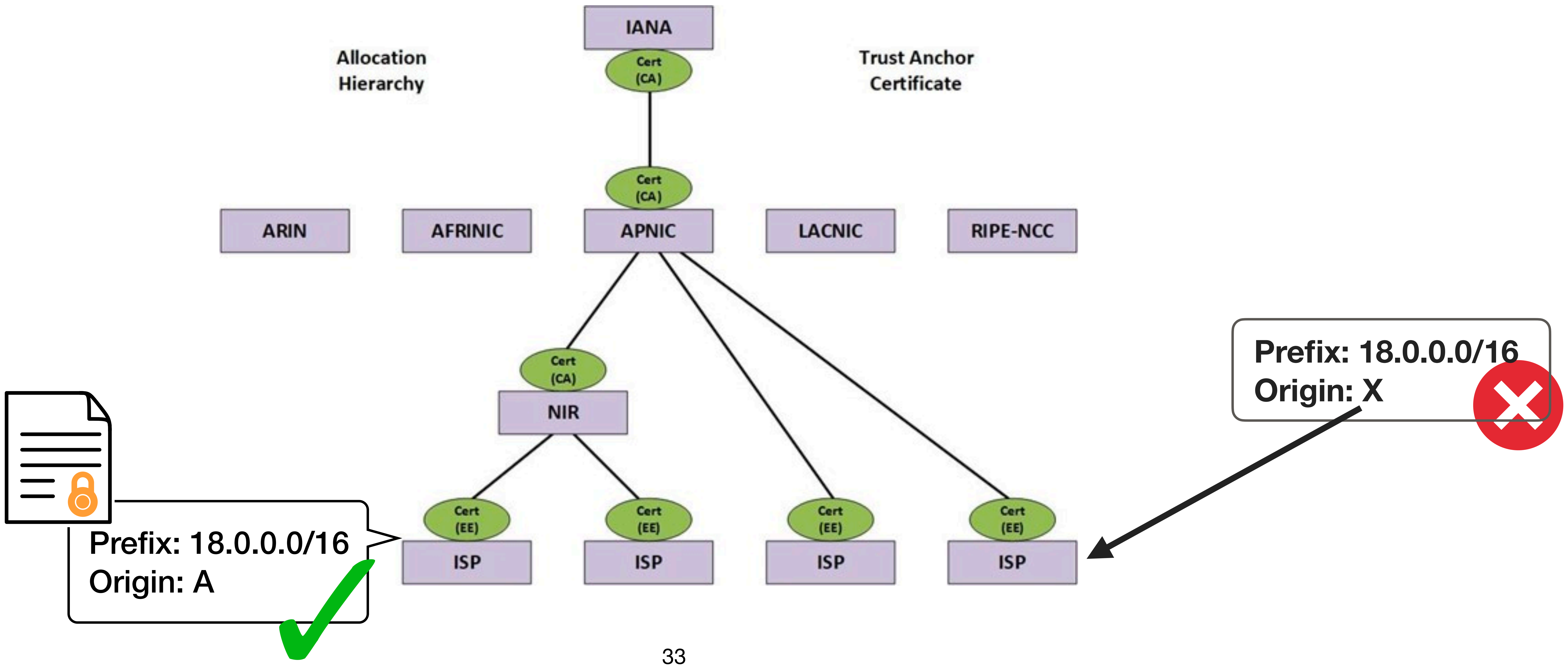
Resource PKI (RPKI): With RPKI, IANA + RIRs + ASes have public-key pairs. RIRs sign certificates for ASes binding AS-owned subnets/prefixes to the AS public keys (i.e., IANA + RIRs = root certificate authorities)





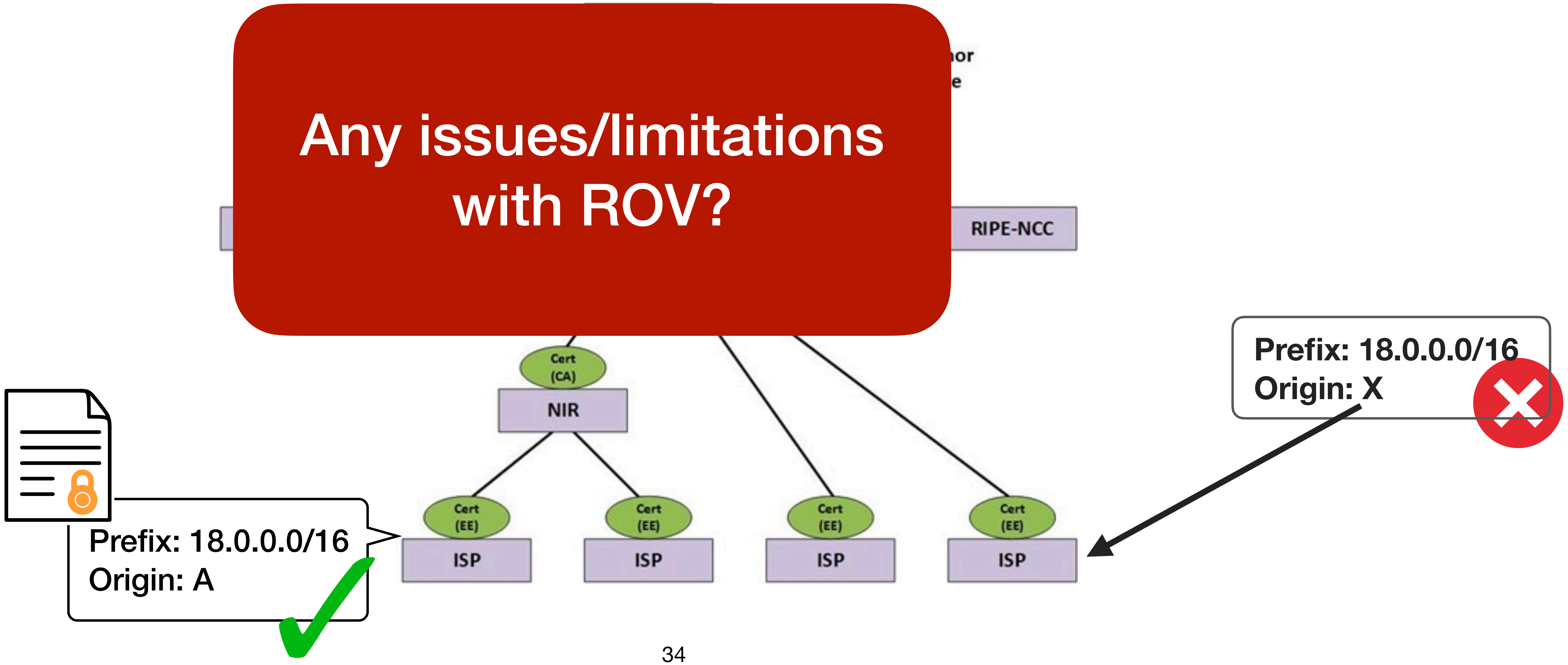
BGP Defense

Route Origin Validation (ROV): ASes can share Route Origin Authorizations (ROAs), signed records of which ASes can originate a route for a prefix. BGP routers can validate that a BGP announcement has a valid origin (i.e., the origin AS in the AS-PATH is allowed to announce the prefix).



BGP Defense

Route Origin Validation (ROV): ASes can share Route Origin Authorizations (ROAs), signed records of which ASes can originate a route for a prefix. BGP routers can validate that a BGP announcement has a valid origin (i.e., the origin AS in the AS-PATH is allowed to announce the prefix).



Any issues/limitations with ROV?

BGP Defense

ROV validates origin AS can announce a BGP route (i.e., it "owns" the IP space being announced).

BUT: the rest of the BGP route is not validated.

Ex: Say AS19 owns IP prefix X, with ROV

AS-Path in benign BGP route for X: AS 24 -> AS 35 -> AS 19

AS-Path in attacker's BGP route for X: **AS 666** -> AS 35 -> AS 19

MITM

BGP Defense

BGPSec: Each AS in the AS-PATH of a BGP route announcement provides a signature indicating that they announced the route to the next AS. This provides integrity over the whole AS-PATH, rather than just the origin AS.

AS-PATH: AS 24 -> AS 35 -> AS 19

BGPsec AS-PATH: AS 24 -> AS 35 -> AS 19

This route sent to AS 35
(Signed by AS 19)

This route sent to AS 24
(Signed by AS 35)

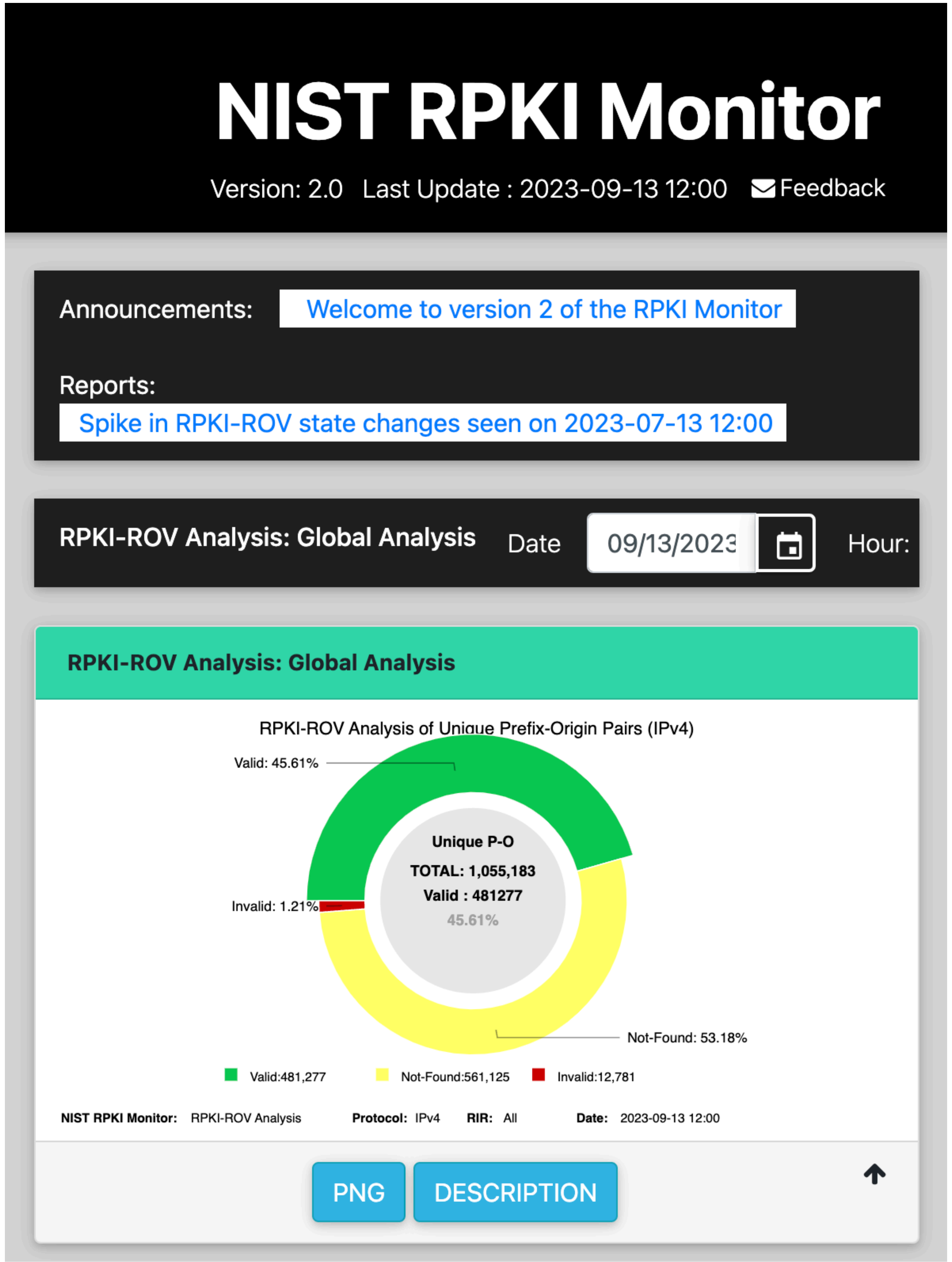
Attacker AS-Path: **AS 666** -> AS 35 -> AS 19

This route sent to AS 35
(Signed by AS 19)

NO SIGNED ROUTE
BY AS 35

BGP Defense

ROV: Adopted by ~45% of routed prefixes



NIST RPKI Monitor

Version: 2.0 Last Update : 2023-09-13 12:00 ✉ Feedback

Announcements: Welcome to version 2 of the RPKI Monitor

Reports:
Spike in RPKI-ROV state changes seen on 2023-07-13 12:00

RPKI-ROV Analysis: Global Analysis Date 09/13/2023 Hour:

RPKI-ROV Analysis: Global Analysis

RPKI-ROV Analysis of Unique Prefix-Origin Pairs (IPv4)

NIST RPKI Monitor: RPKI-ROV Analysis Protocol: IPv4 RIR: All Date: 2023-09-13 12:00

BGP Defense

BGPSec: Very little adoption :(

Why?

- Only works if entire AS path uses it. If not all ASes use it, either need to
  1) not accept/use their routes (not good...)
  2) do not enforce BGPsec (then little value in adopting...)
- Also, doesn't prevent "route leaks". ROV validates origin AS announcements, but neither ROV or BGPsec prevent intermediate AS from propagating a route incorrectly.
- BGPSec entails performance overhead

BGP security is growing in importance, so likely will see developments soon!