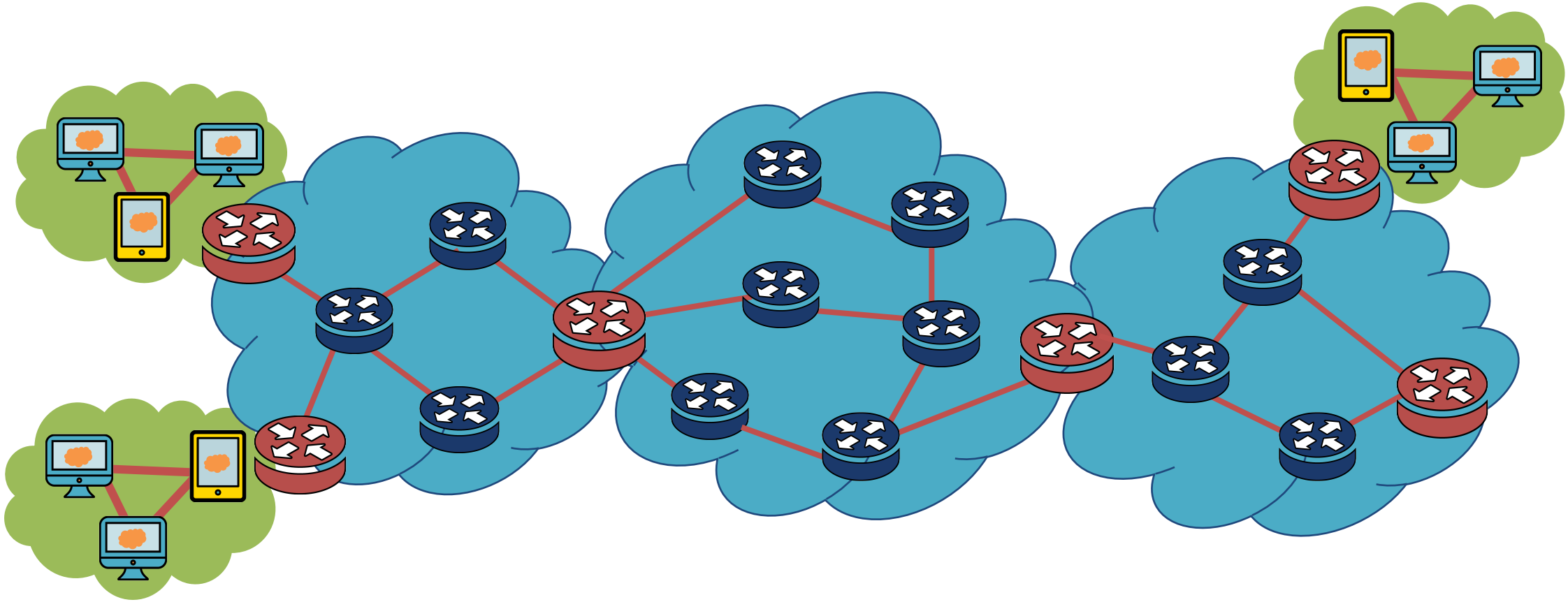
Internet Infrastructure



Internet Infrastructure

- Local and inter-domain routing
- TCP/IP for routing and messaging
- BGP for routing announcements

@ Domain Name System

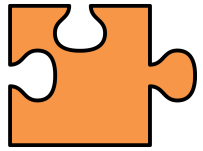
- Find IP address from symbolic name (www.cc.gatech.edu)

Infrastructure Quiz

Match the level to its description

Level:	Descriptions:
3 Tier One	1. A network that purchases all transit from other networks.
2 Tier Two	2. A network that peers some of its network access and purchases some of it.
1 Tier Three	3. A network can reach every other network through peering.

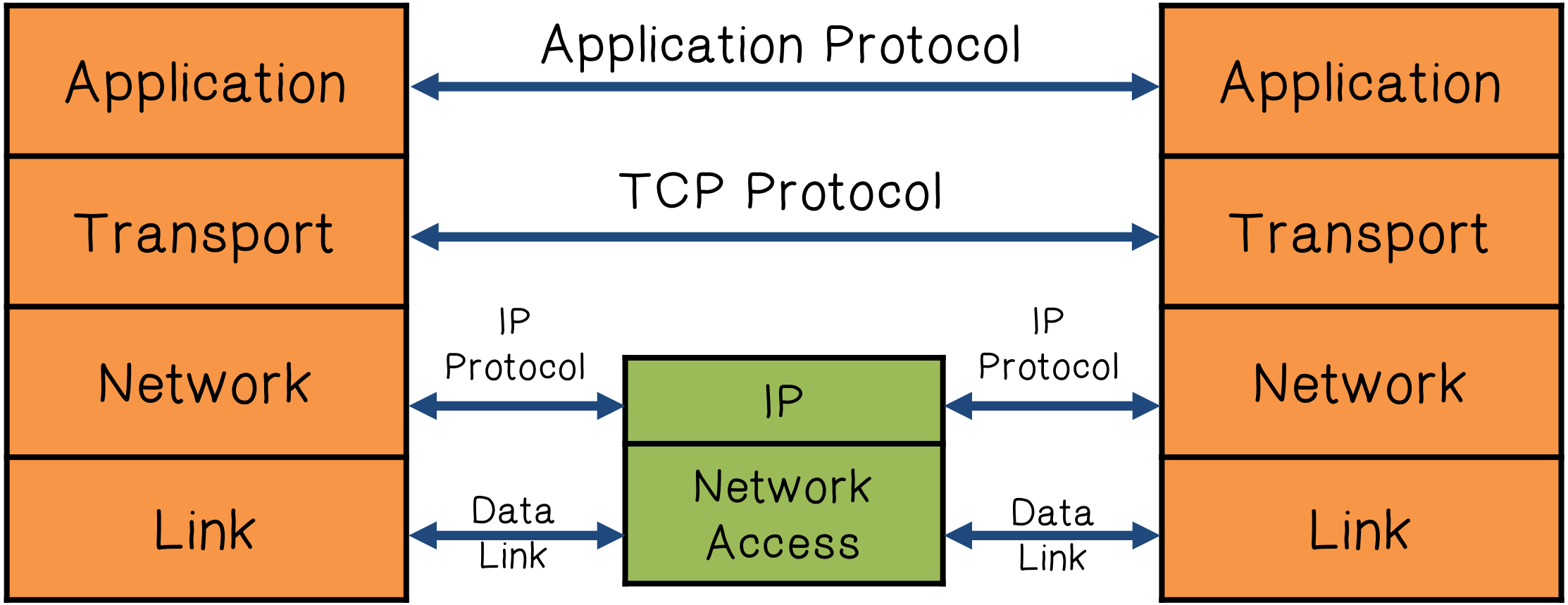
Peering: ISPs connect their networks together. Traffic is allowed to flow across a network in exchange for free access to other networks



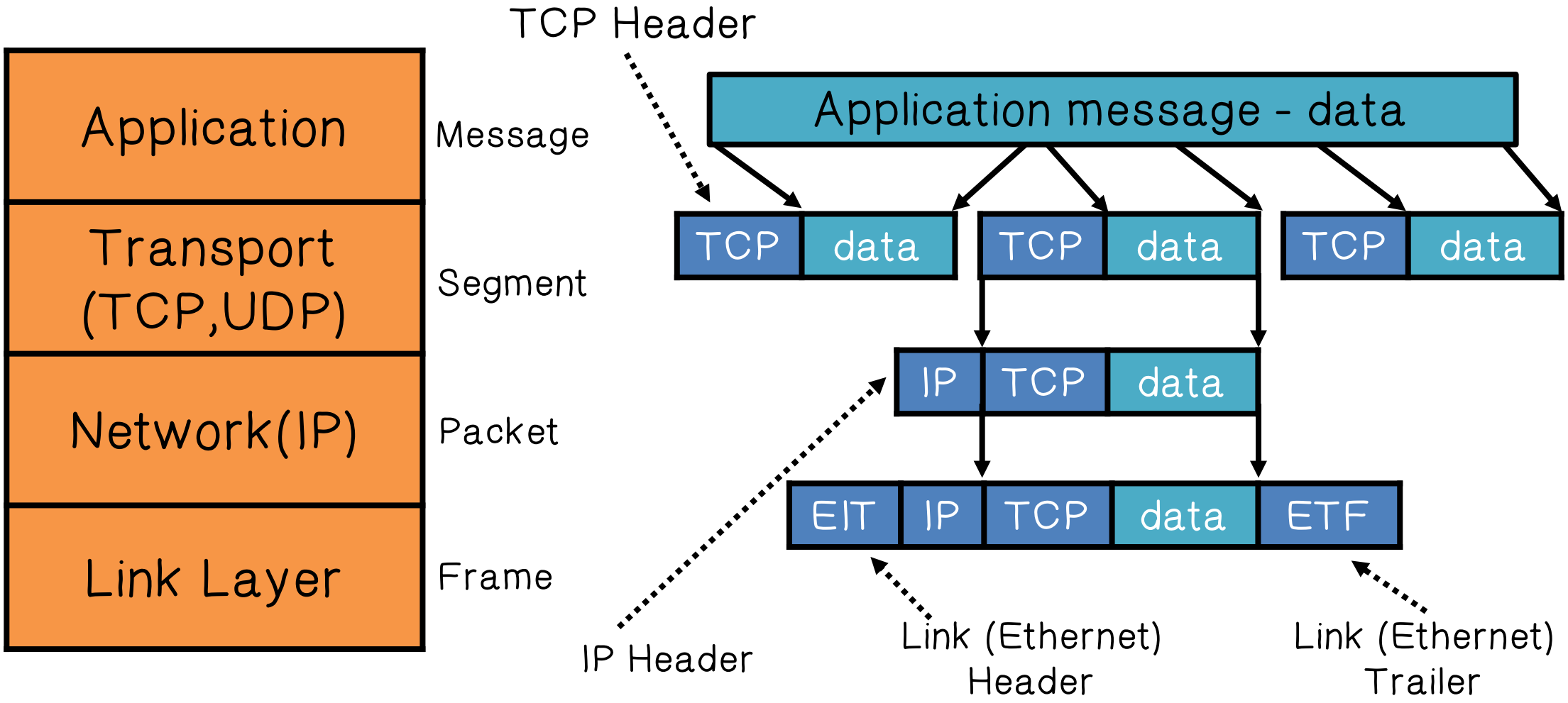
Infrastructure Quiz

NAME	
AT&T	Cogent Communications
CenturyLink	Deutsche Telekom AG
KPN International	Level 3 Communications
NTT Communications (America)	Orange
Sprint	Tata Communications (America)
Telecom Italia Sparkle	Telefonica Global Solutions
Telia Carrier	Verizon Enterprise Solutions
Zayo Group	-----

TCP Protocol Stack



TCP Protocol Stack: Data Formats



Internet Protocol: IP Routing

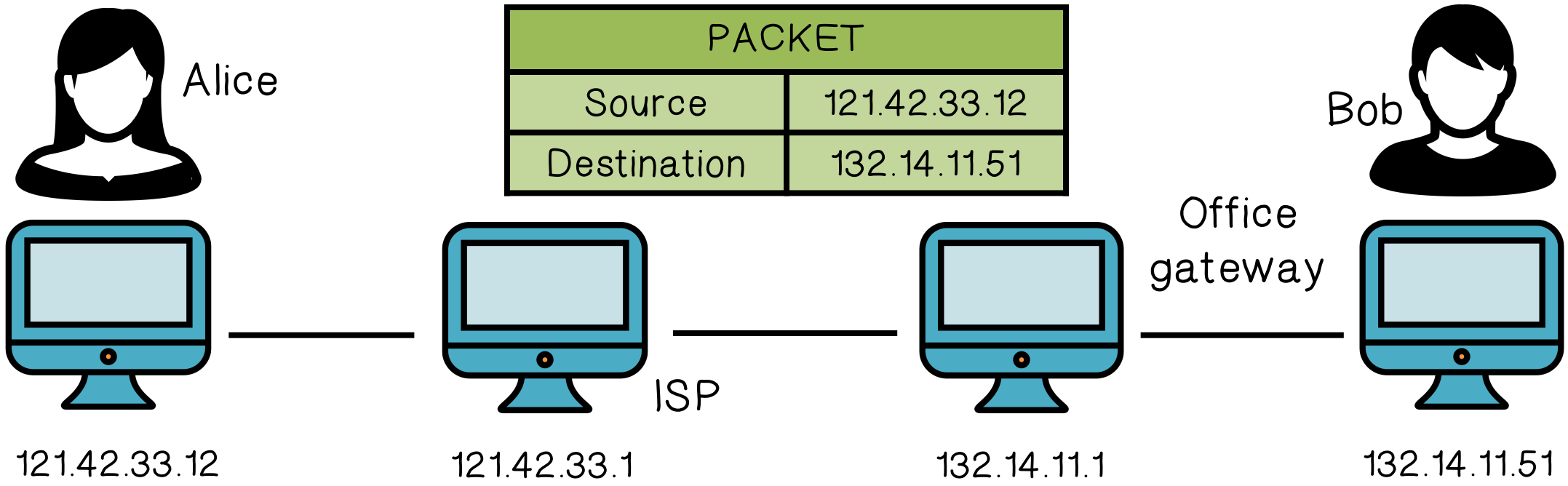
Version	Header Length
Type of Service	
Total Length	
Identification	
Flags	Fragment Offset
Time to Live	
Protocol	
Header Checksum	
Source Address of Originating Host	
Destination Address of Target Host	
Options	
Padding	
IP Data	

Connectionless

- Unreliable
- Best effort

Notes: src and dest ports not parts of IP hdr

Internet Protocol: IP Routing



- Typical route uses several hops
- IP: no ordering or delivery guarantees

IP Protocol Functions (Summary)

Routing

- IP host knows location of router (gateway)
- IP gateway must know route to other networks

Fragmentation and reassembly

- If max-packet-size less than the user-data-size

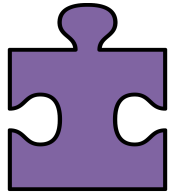
IP Protocol Functions (Summary)

Error reporting

- ICMP packet to source if packet is dropped

TTL field: decremented after every hop

- Packet dropped if TTL=0.
- Prevents infinite loops.



IP Quiz

Select all the true statements about Internet Protocol (IP).

- [ ] IP is a connectionless and reliable protocol.
- [x] IP provides only best effort delivery, it is not guaranteed.
- [x] Due the connectionless nature of IP, data corruption, packet loss, duplication, and out-of-order delivery can occur.

IP Authentication

Client is trusted to embed correct source IP

- Easy to override using raw sockets
- Libnet: a library for formatting raw packets with arbitrary IP headers

The problem: No Source IP authentication

Anyone who owns their machine can send packets with arbitrary source IP, and a response will be sent back to forged source IP

IP Authentication

Client is trusted to embed correct source IP

- Easy to override using raw sockets
- Libnet: a library for formatting raw packets with arbitrary IP headers

The problem: No Source IP authentication

Implications:

- Anonymous DoS attacks;
- Anonymous infection/malware attacks

Transmission Control Protocol

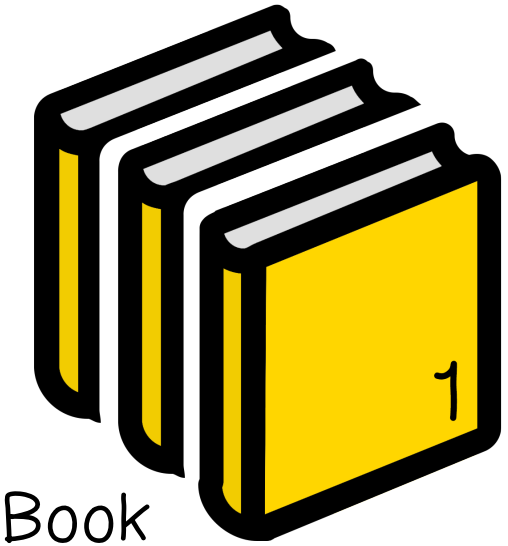
Connection-oriented, preserves order

Book

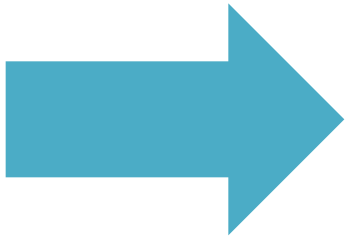
Transmission Control Protocol

Sender :

- Break data into packets
- Attach packet numbers



Book

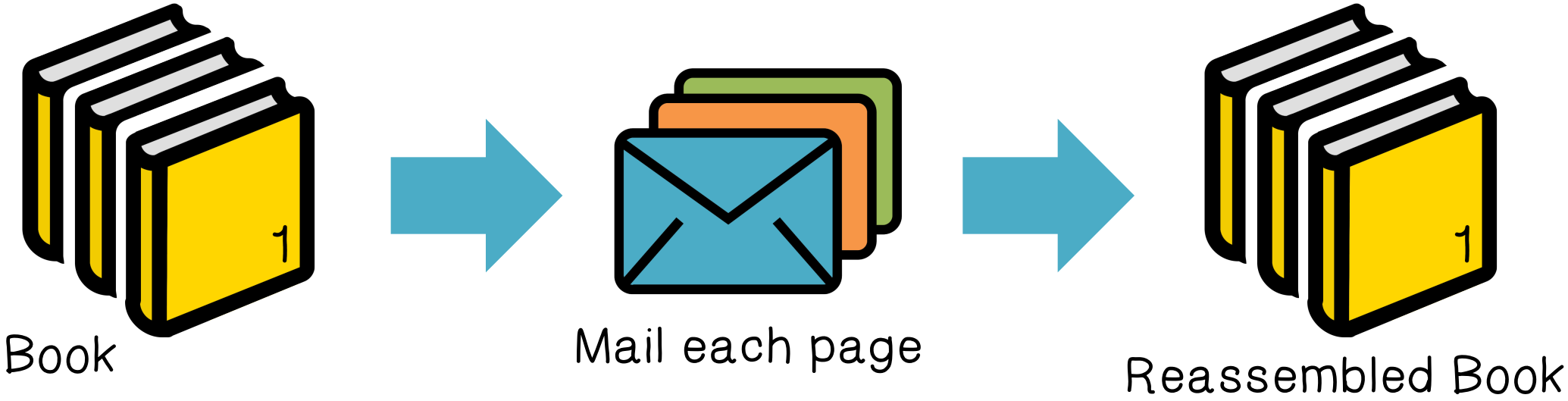


Mail each page

Transmission Control Protocol

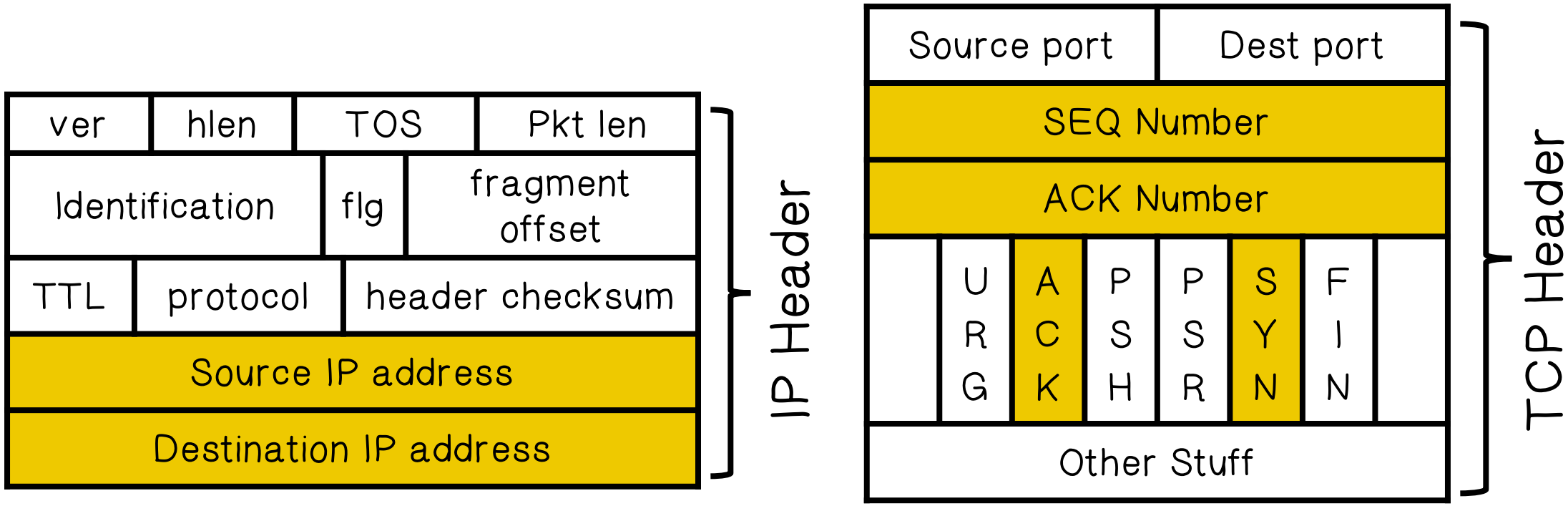
Receiver:

- Acknowledge receipt; lost packets are resent
- Reassemble packets in correct order



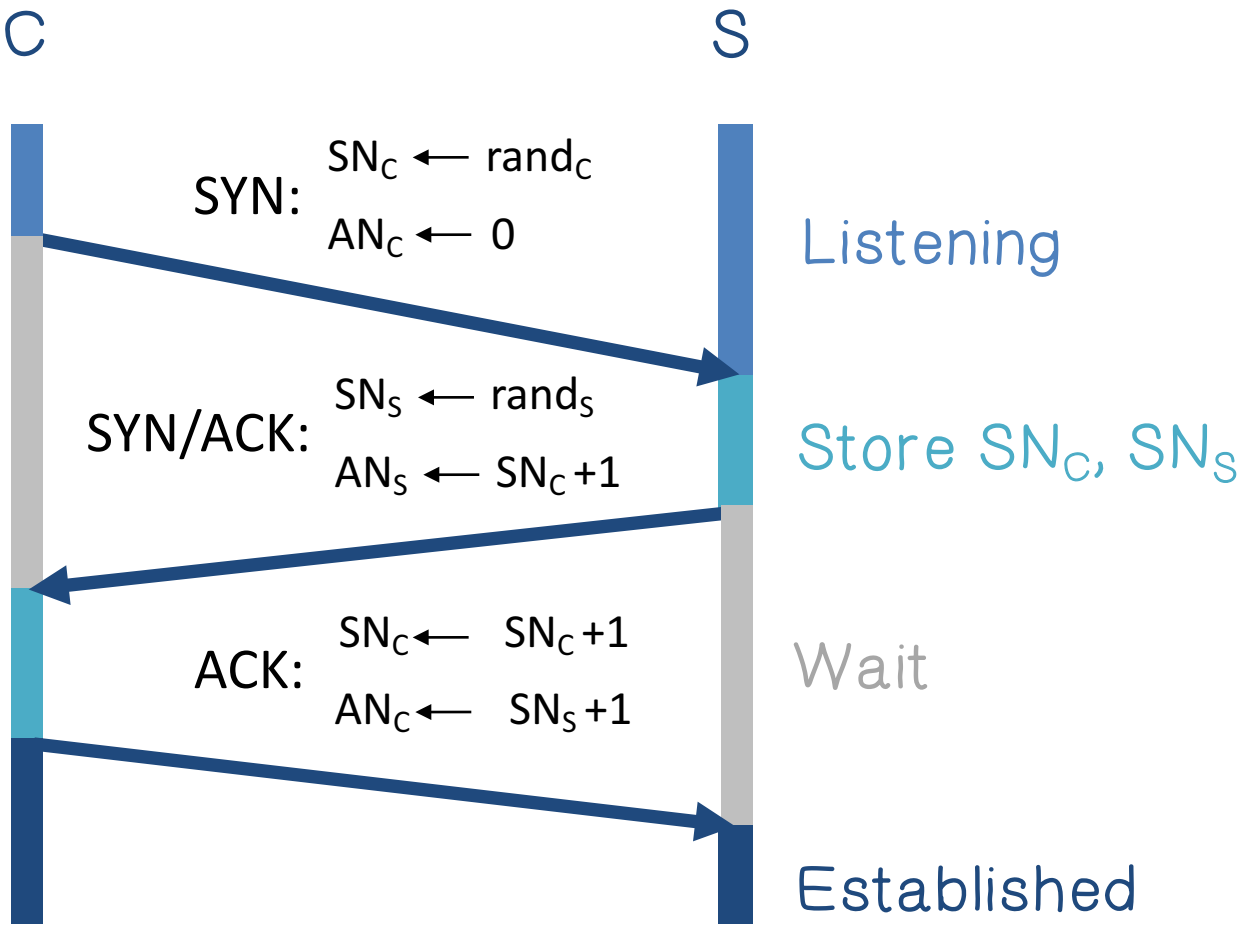
Transmission Control Protocol

TCP Header



Review TCP Handshake

Received packets with SN too far out of window are dropped



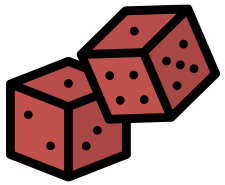
TCP Basic Security Problems

1. Network packets pass by untrusted hosts
   - Eavesdropping, packet sniffing
   - Especially easy when attacker controls a machine close to victim *(e.g. WiFi routers)*
2. TCP state easily obtained by eavesdropping
   - Enables spoofing and session hijacking
3. Denial of Service (DoS) vulnerabilities
   - See DDoS lesson

TCP IP Security Issues Quiz

Select all the true statements:

- [ ] Application layer controls can protect application data, and IP addresses.
- [x] IP information cannot be protected by transport layer controls.
- [x] Network layer controls can protect the data within the packets as well as the IP information for each packet.
- [ ] Data link layer controls can protect connections comprised of multiple links



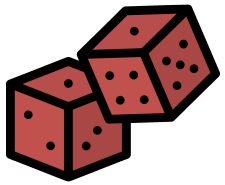
Random Initial Sequence Numbers

Suppose initial seq. numbers (SN_C , SN_S) are predictable:

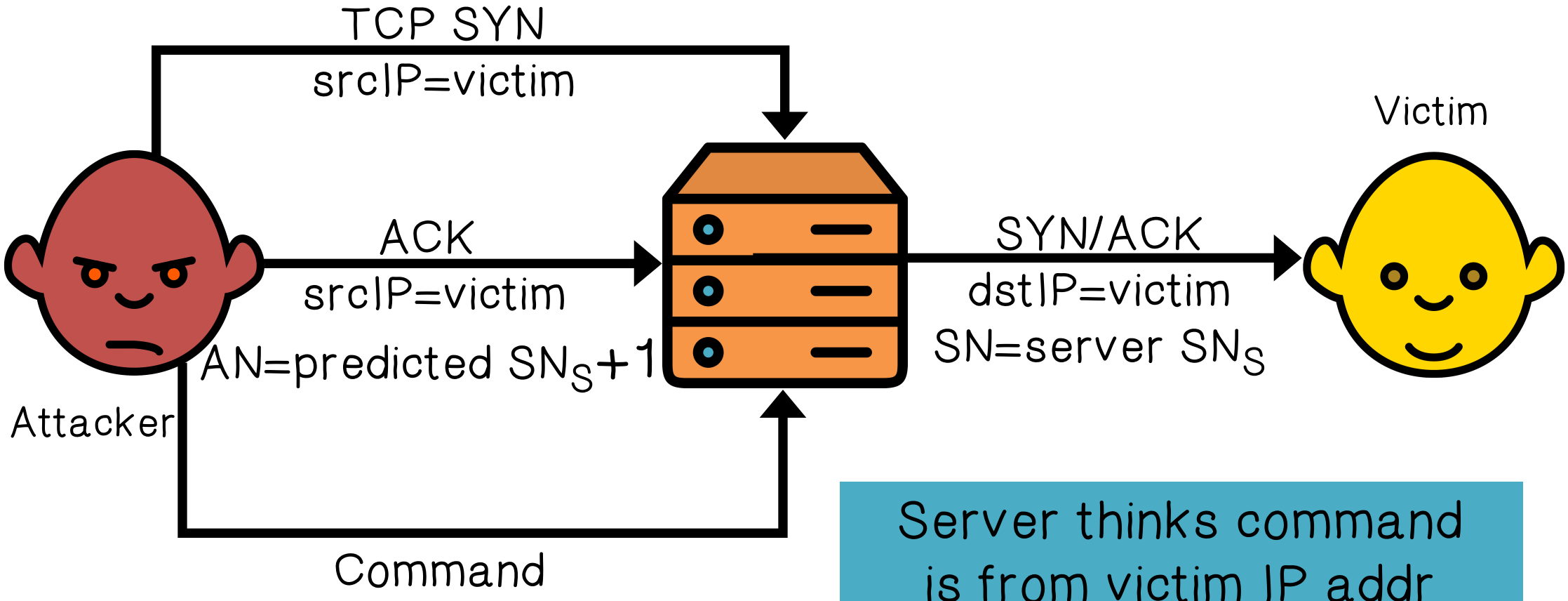
- Attacker can create TCP session on behalf of forged source IP

Breaks IP-based authentication (e.g. SPF, /etc/hosts)

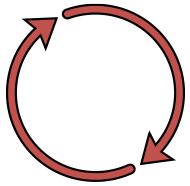
- Random seq. num. do not prevent attack, but make it harder



Random Initial Sequence Numbers



Server thinks command is from victim IP addr



Example DoS Vulnerability: Reset

Attacker sends a Reset packet on an open socket

If correct SN_S then connection will close ⇨ DoS

- Naively, success prob. is 1/232 (32-bit seq. #'s).
  … but, many systems allow for a large window of acceptable seq. #'s. Much higher success probability.
- Attacker can flood with RST packets until one works

Protocols Quiz

Match the protocol with its description:

Protocol:

B Address Resolution Protocol (ARP)

C Open Shortest Path First (OSPF)

A Border Gateway Protocol (BGP)

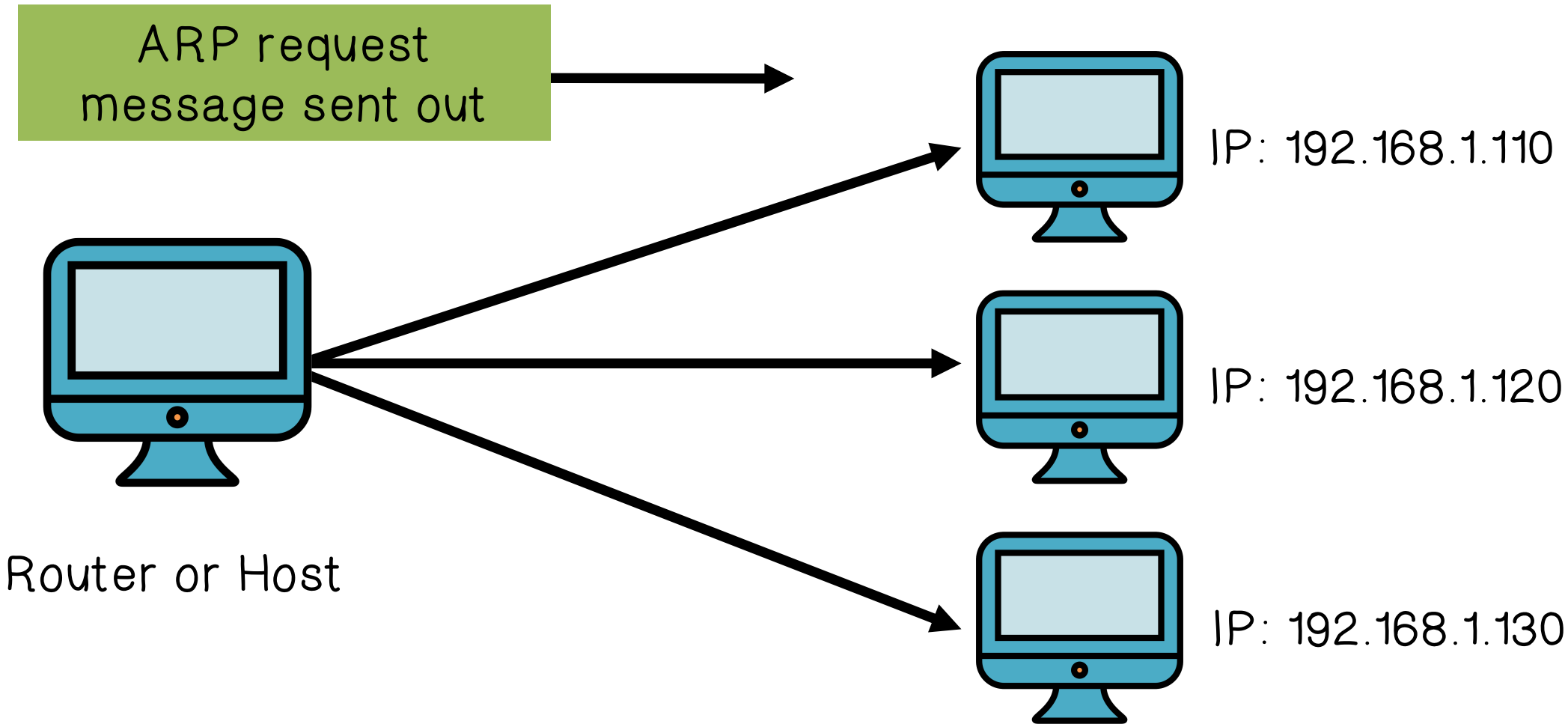
Descriptions:

A. protocol designed to exchange routing and reachability information among autonomous systems (AS)

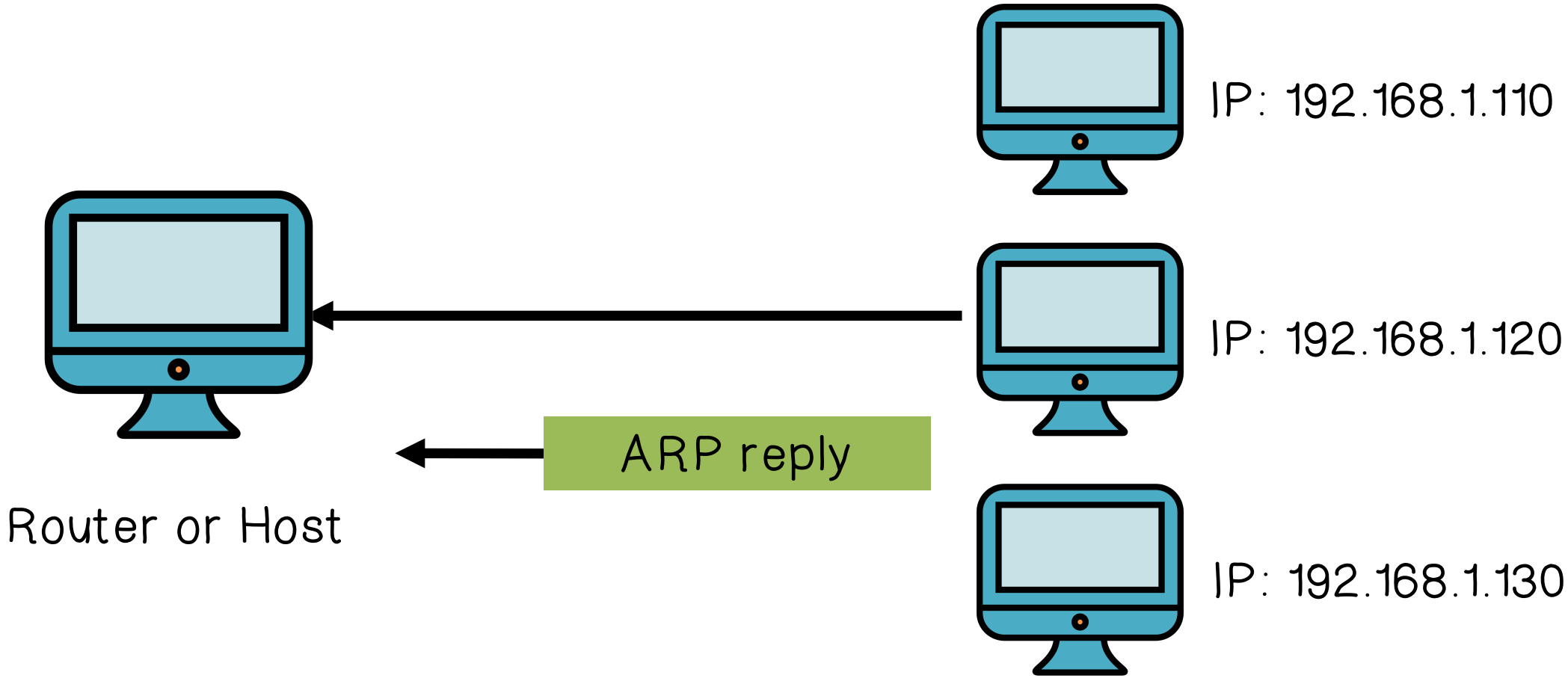
B. protocol designed to map IP network addresses to the hardware addresses used by a data link protocol

C. protocol uses a link state routing algorithm and falls into the group of interior routing protocols

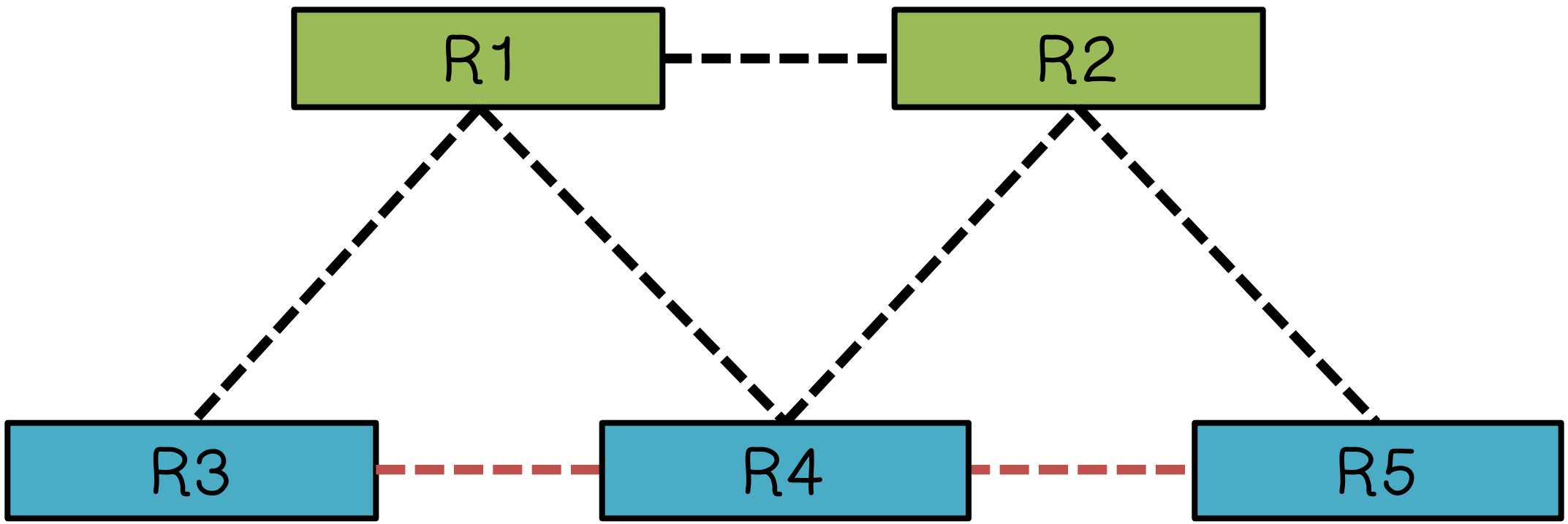
Protocols Quiz



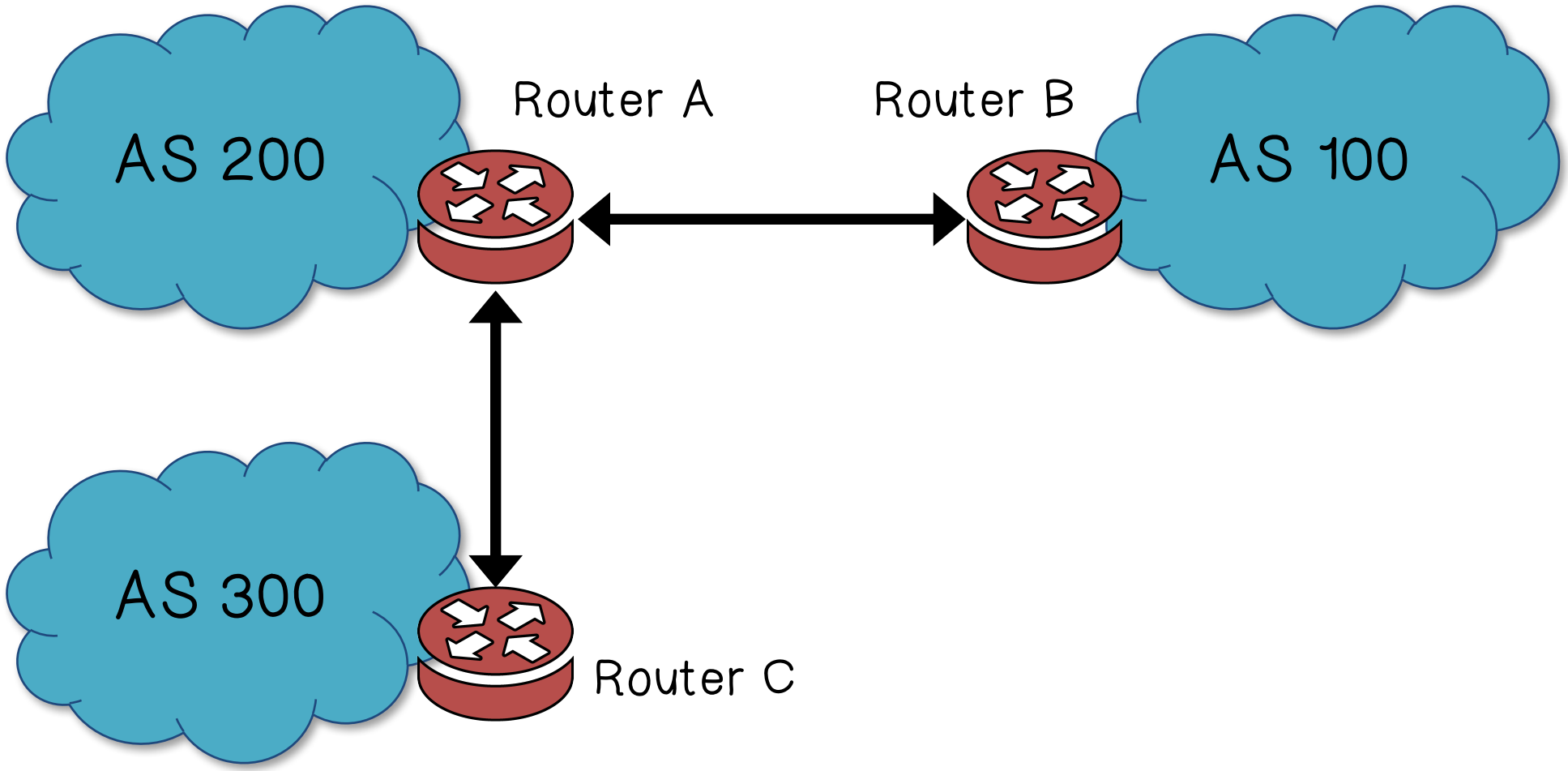
Protocols Quiz



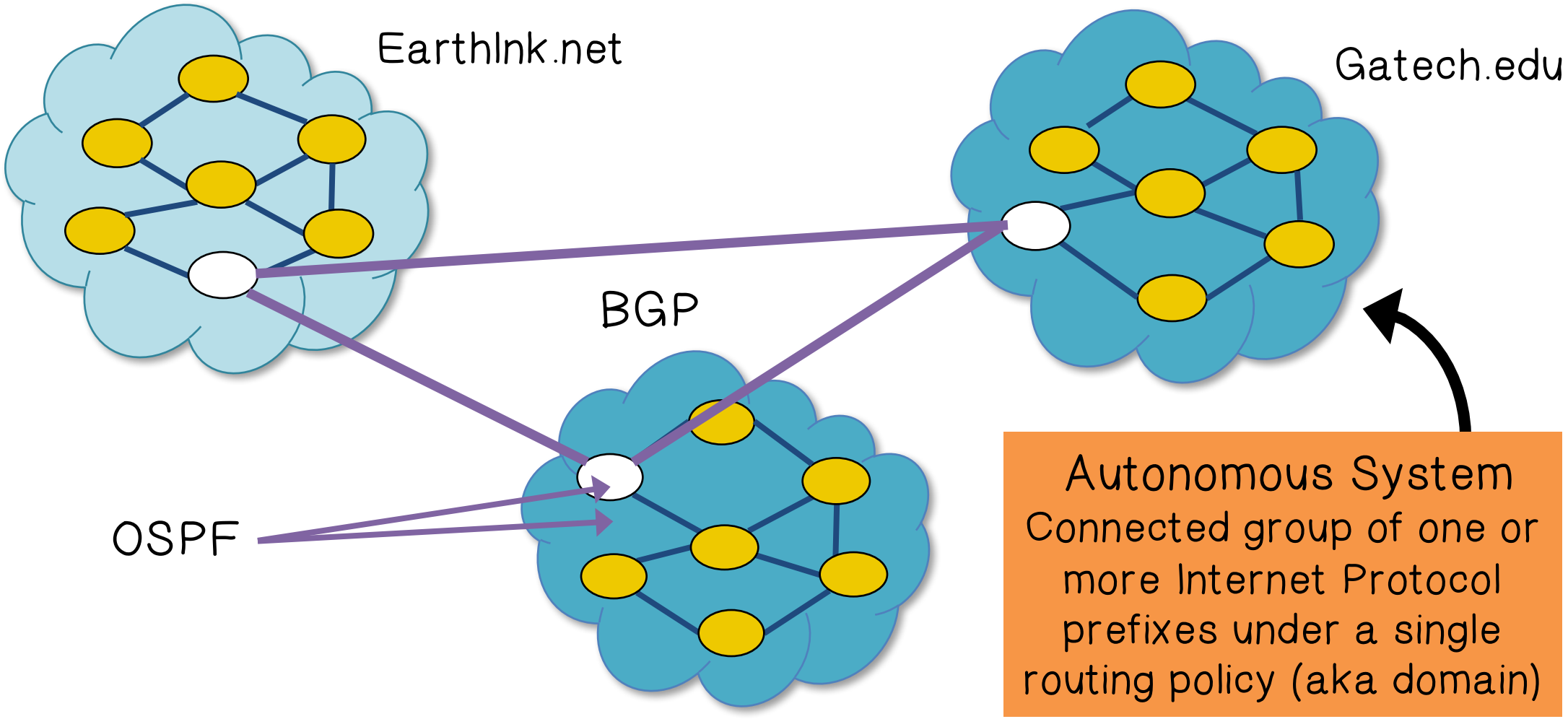
Protocols Quiz



Protocols Quiz



Routing Security: Interdomain Routing



Routing Protocols

ARP (addr resolution protocol): IP addr → eth addr

Security issues: *(local network attacks)*

- Node A can confuse gateway into sending it traffic for Node B
- By proxying traffic, node A can read/inject packets into B's session (e.g. WiFi networks)

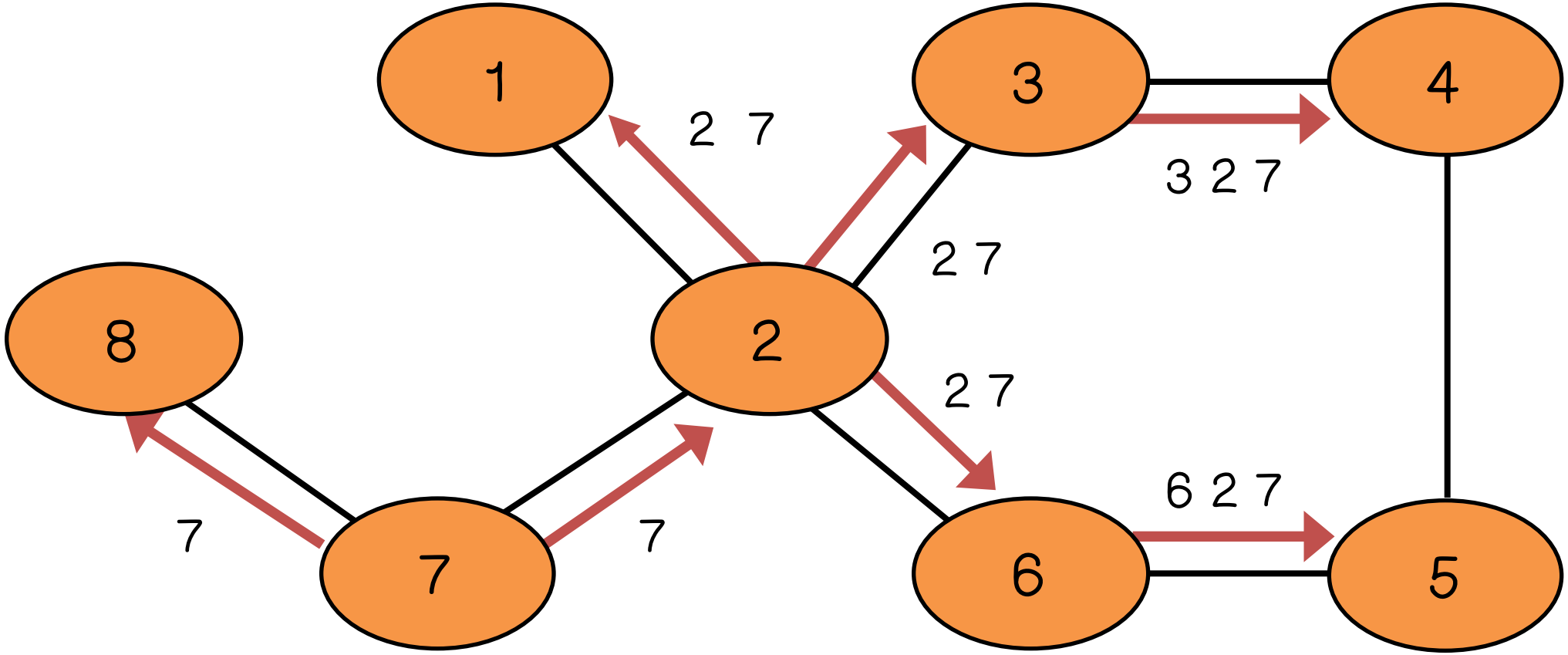
Routing Protocols

BGP: routing between Autonomous Systems

Security issues: *unauthenticated route updates*

- Anyone can cause entire Internet to send traffic for a victim IP to attacker's address
  - Example: Youtube-Pakistan mishap
  - Anyone can hijack route to victim

BGP



[D. Wetherall]

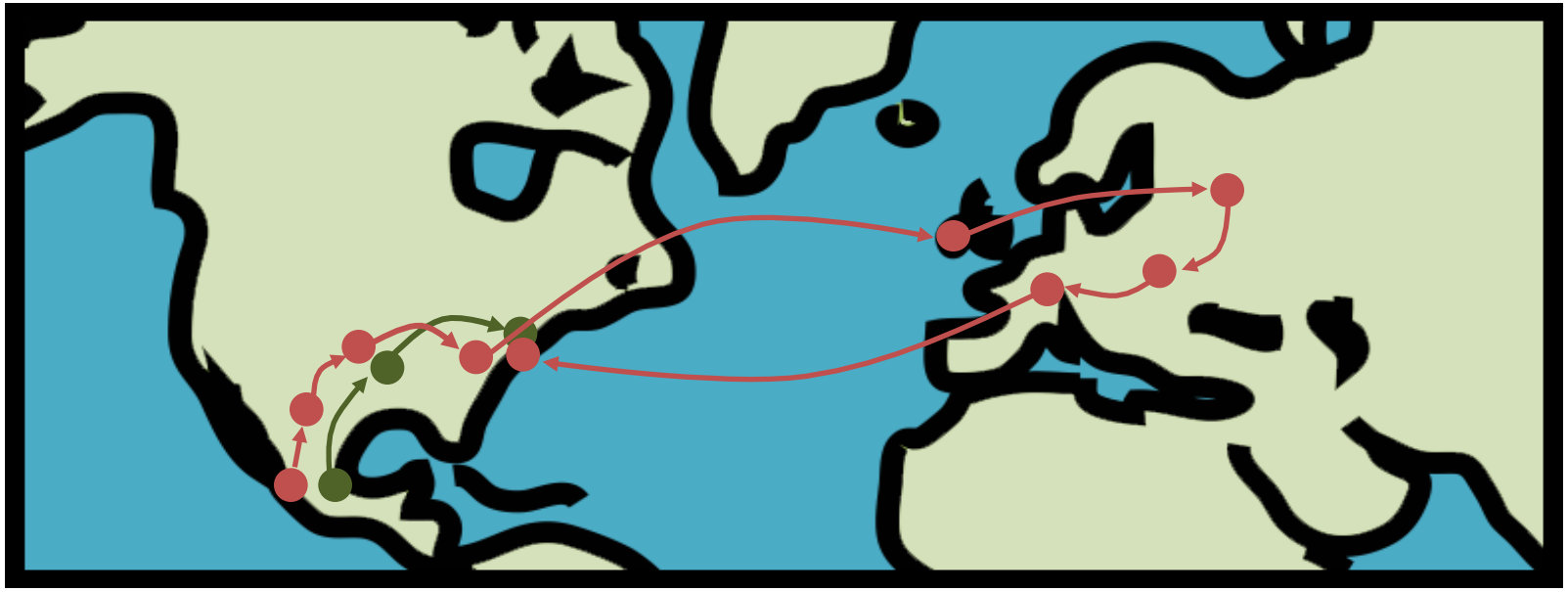
BGP: Security Issues

BGP path attestations are un-authenticated

- *Anyone can inject advertisements* for arbitrary routes
- Advertisement will propagate everywhere
- Used for DoS, spam, and eavesdropping *(details in DDoS lecture)*

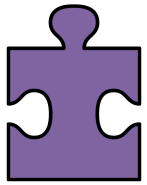
BGP: Example path hijack

Normally: Alestra *(Mexico)* → PCCW *(Texas)* → Qwest *(DC)*



Feb 2013: Guadalajara → Washington DC via Belarus

Person browsing the Web in DC cannot tell by traceroute that HTTP Responses are routed through Moscow



BGP Attacks Quiz

Match the attack to its characteristic:

Attack:

D Denial of Service

E Sniffing

C Routing to Endpoints in Malicious Networks

B Creating Route Instabilities

A Revelation of Network Topologies

Characteristic:

A. Unmasking the AS relationships by hacking the routing table.

B. Not yet used by hackers because damage cannot be contained. It can blowback to the attacker.

C. The first step is to hijack traffic from a legitimate host.

D. Create a false route or kill a legitimate one.

E. The attacker must control a device along the victim's communication path.

BGP: Security Issues

Solutions:

RPKI: AS obtains a certificate (ROA) from regional authority (RIR) and attaches ROA to path advertisement.

- Advertisements without a valid ROA are ignored.
- Defends against a malicious AS (but not a network attacker)

SBGP: sign every hop of a path advertisement

S-BGP Design Overview

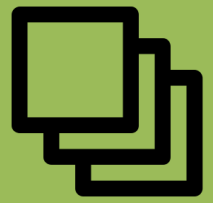
IPsec: secure point-to-point router communication

Public Key Infrastructure: authorization for all S-BGP entities

Attestations: digitally-signed authorizations

- Address: authorization to advertise specified address blocks
- Route: Validation of UPDATEs based on a new path attribute, using PKI certificates and attestations

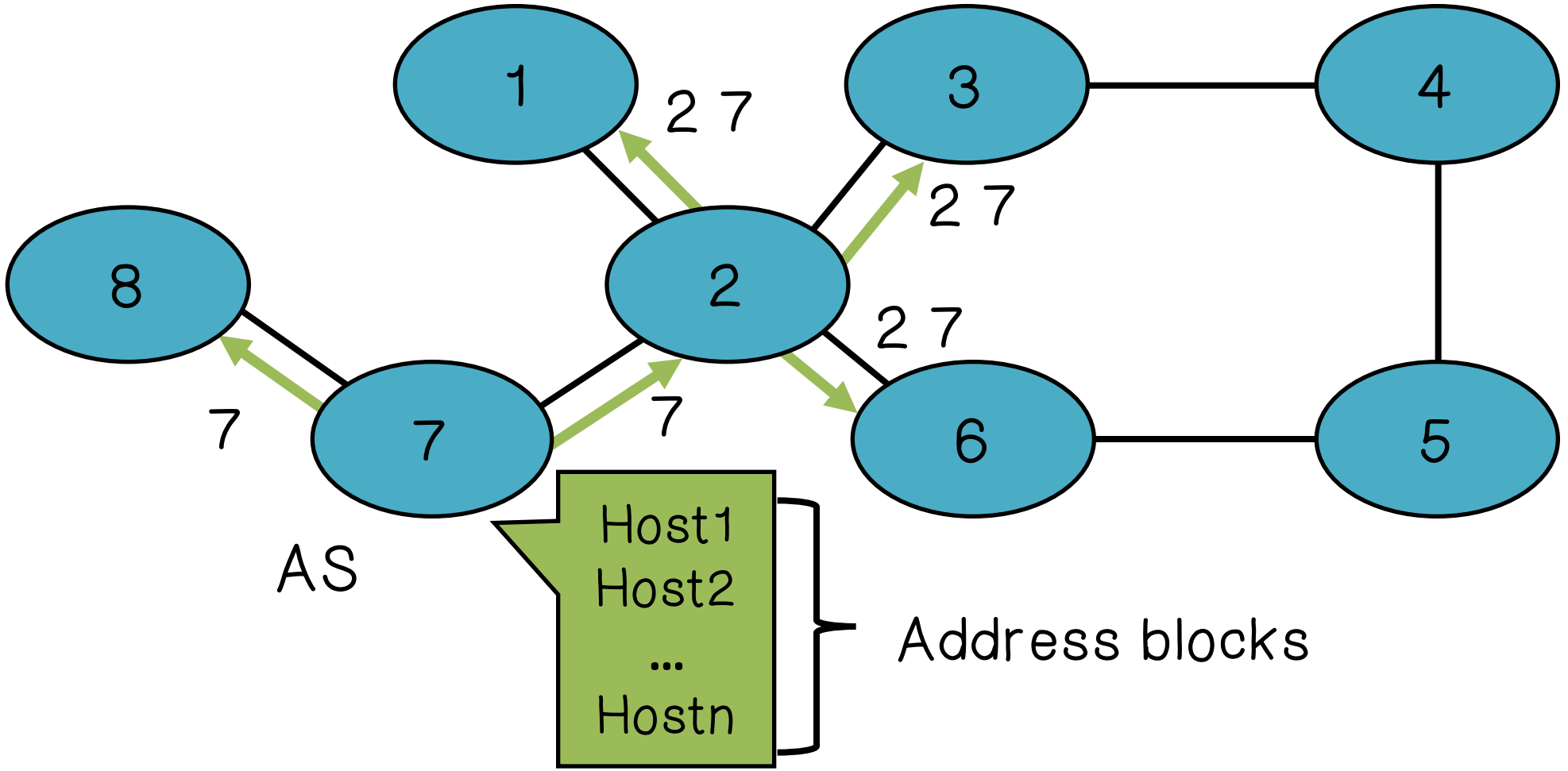
S-BGP Design Overview



Repositories for distribution of certificates, CRLs, and address attestations

Tools for ISPs to manage address attestations, process certificates & CRLs, etc.

S-BGP Design Overview



S-BGP Overview: Address Attestation

Indicates that the final AS listed in the UPDATE is authorized by the owner of those address blocks

Includes identification of:

- owner's certificate
- AS to be advertising the address blocks
- address blocks
- expiration date

S-BGP Overview: Address Attestation

Digitally signed by owner of the address blocks

Used to protect BGP from erroneous UPDATEs *(authenticated but misbehaving or misconfigured BGP speakers)*

S-BGP Overview: Route Attestation

Indicates that the speaker or its AS authorizes the listener's AS to use the route in the UPDATE

Includes identification of:

- AS's or BGP speaker's certificate issued by owner of the AS
- the address blocks and the list of ASes in the UPDATE
- the neighbor
- expiration date

S-BGP Overview: Route Attestation

Digitally signed by owner of the AS *(or BGP speaker)* distributing the UPDATE, traceable to the IANA …

Used to protect BGP from erroneous UPDATEs *(authenticated but misbehaving or misconfigured BGP speakers)*

S-BGP Overview: Route Attestation

To validate a route from AS_n, AS_{n+1} needs:

- address attestation from each organization owning an address block(s) in the NLRI
- address allocation certificate from each organization owning address blocks in the NLRI
- route attestation from every AS along the path (AS_1 to AS_n), where the route attestation for AS_k specifies the NLRI and the path up to that point (AS_1 through As_{k-1})
- certificate for each AS or router along path (AS_1 to AS_n) to check signatures on the route attestations
- all the relevant CRLs must have been checked