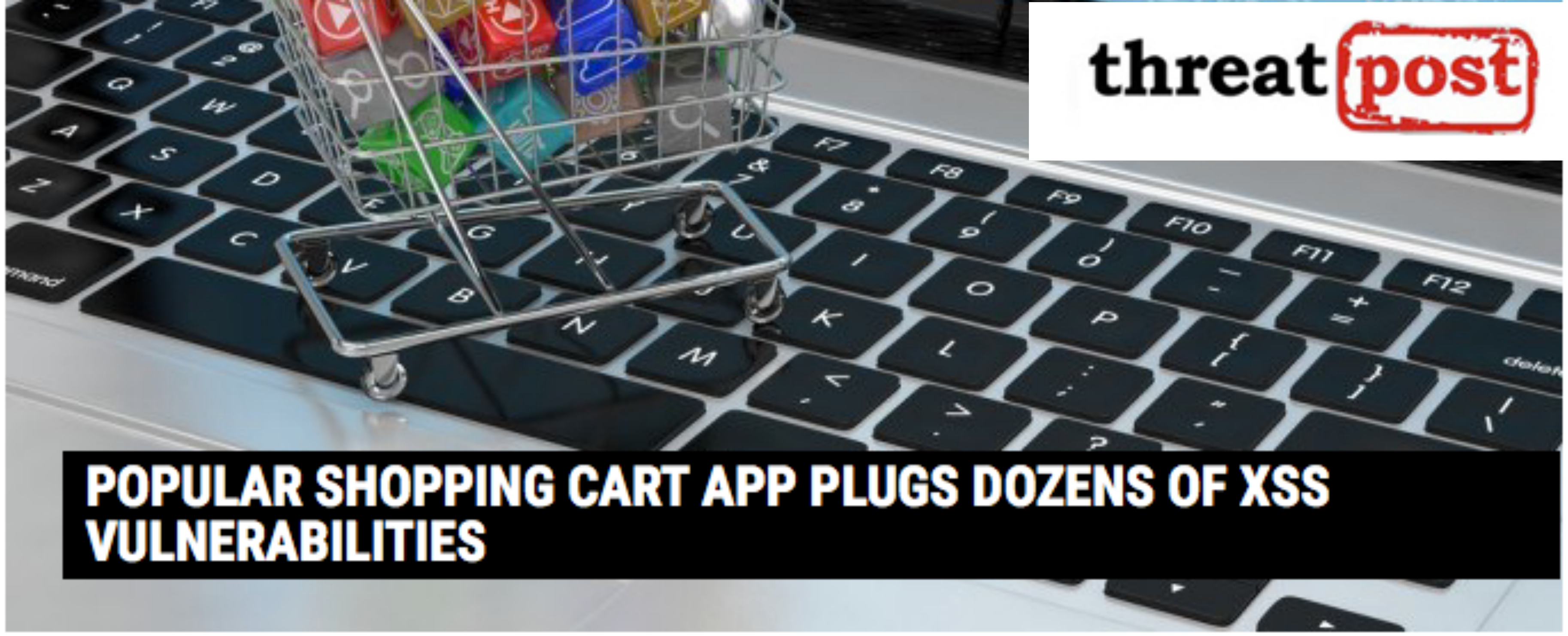
threatpost



POPULAR SHOPPING CART APP PLUGS DOZENS OF XSS VULNERABILITIES

by **Tom Spring** March 28, 2016 , 5:13 pm

Popular open source shopping cart app Zen Cart is warning its users of dozens of cross-site scripting vulnerabilities found in its software. Affected websites, security experts say, risk exposing customers to malware, theft of cookies data and site defacement.

Zen Cart, with an estimated 113,000 active users (according to BuiltWith.com), has told its users they will have to pro-actively install the patch. Affected customers told Threatpost that Zen Cart has notified them of the vulnerability offering

For its part, Trustwave told Threatpost that 50 XSS vulnerabilities were found in the admin section of the Zen Cart software along with one issue in the non-authentication portion of the application.

"We discovered the XSS on Zen Cart in a completely random manner," said Alex Rothacker, senior security researcher at Trustwave. "We have a monthly Hack Friday event where the team goes ahead and picks something and tries to find vulnerabilities. In this case, one team member picked Zen Cart, because it was a popular solution."

network security

cs642

computer security

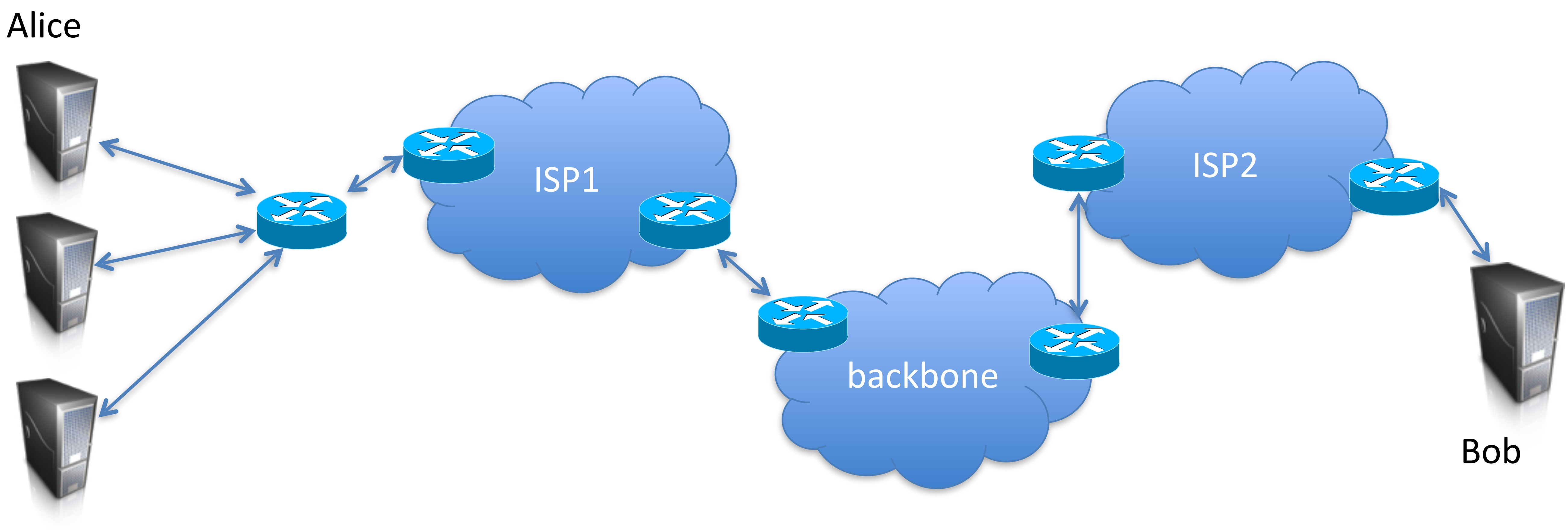
adam everspaugh
ace@cs.wisc.edu

today

* Crypto exercise in-class
* Link layer (in-)security
* IP, TCP (in-)security

crypto
exercise

Internet



Local area network
(LAN)

Ethernet

802.11

Internet

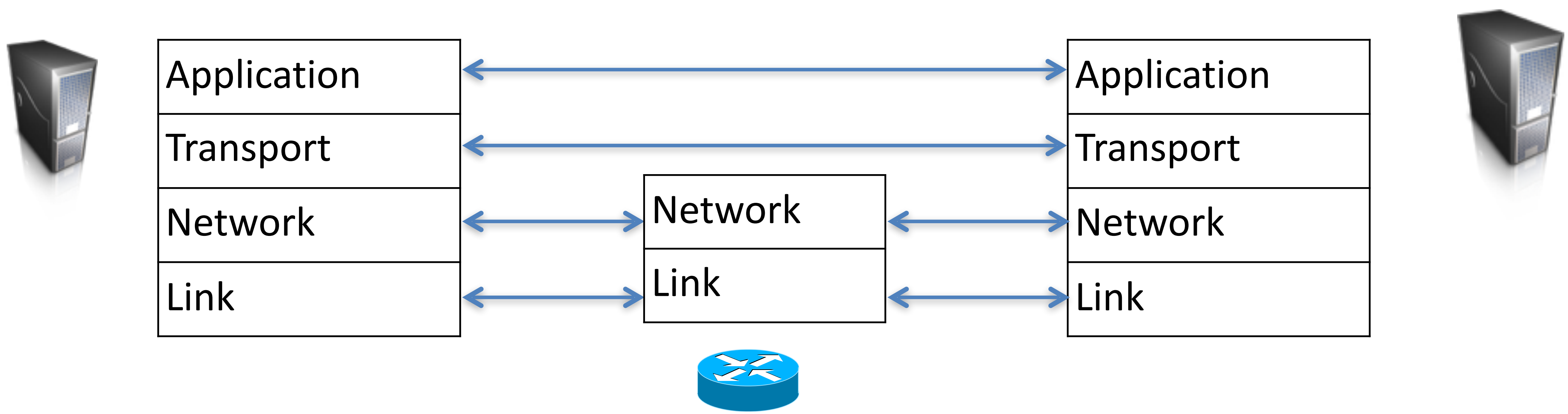
TCP/IP

BGP (border gateway protocol)

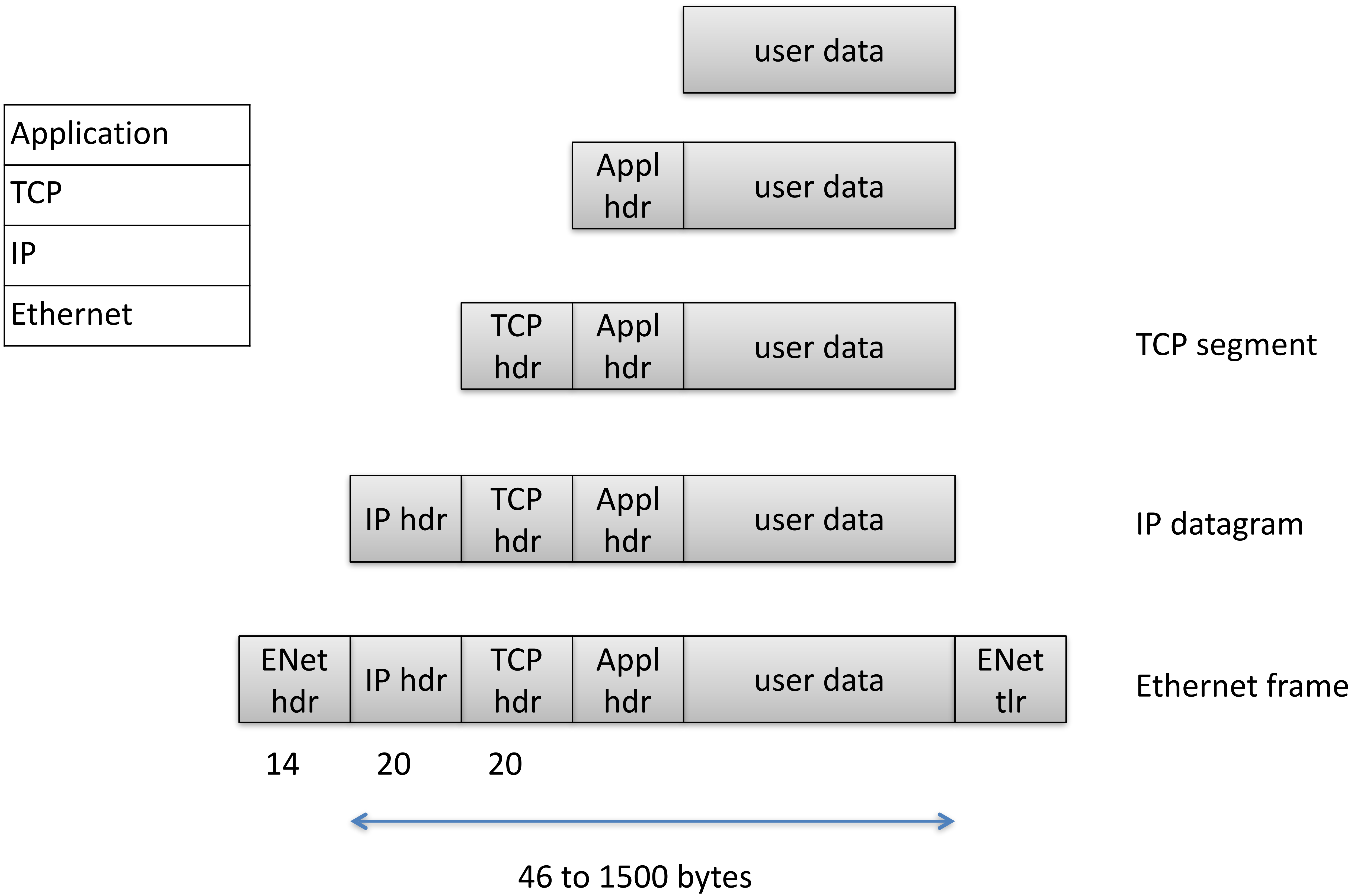
DNS (domain name system)

Internet protocol stack

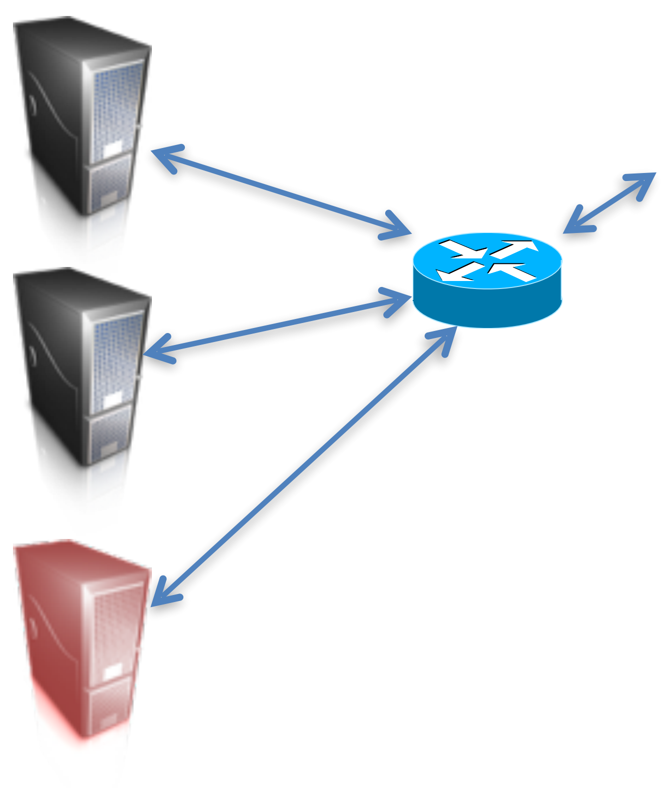
Application	HTTP, FTP, SMTP, SSH, etc.
Transport	TCP, UDP
Network	IP, ICMP, IGMP
Link	802x (802.11, Ethernet)



Internet protocol stack



Address resolution protocol



IP routing:
Figure out where to send
an IP packet based on destination
address.

Link layer and IP must cooperate to
route packets

ARP enables this cooperation by
mapping IPs to MACs

32-bit IP address

ARP ↓

48-bit MAC address

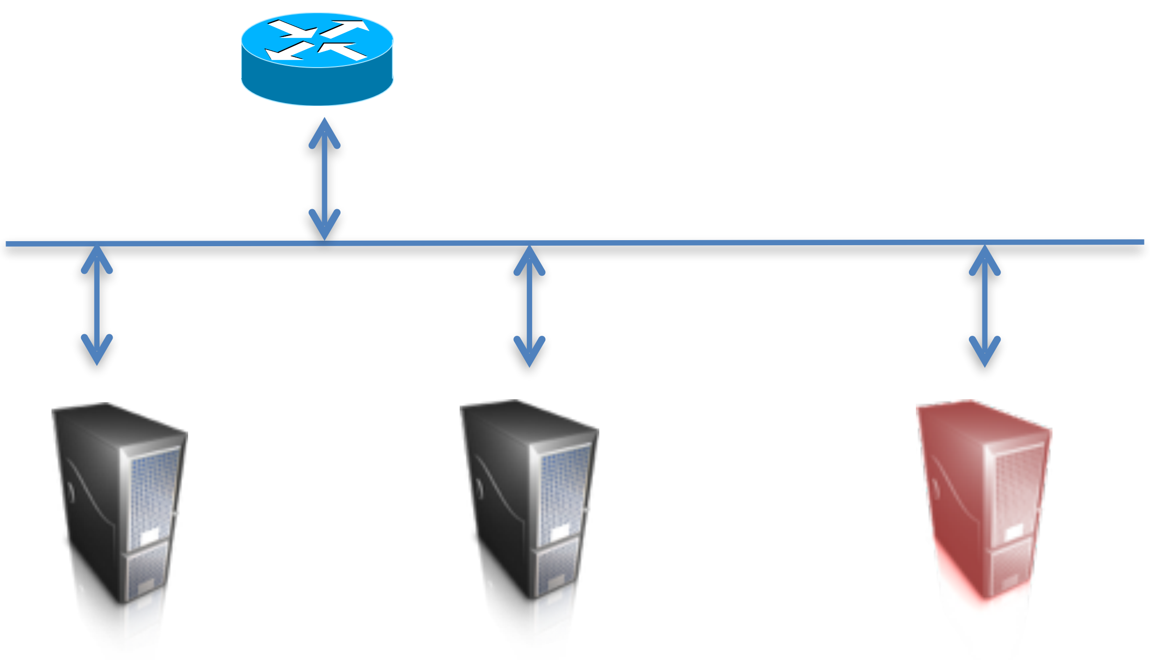
ARP caches

- Hosts maintain cache of ARP data
  - – just a table mapping between IPs and MACs

```
rist@wifi-212:~/work/teaching/642-fall-2011/slides$ arp -a
? (172.16.219.1) at 0:50:56:c0:0:1 on vmnet1 ifscope permanent [ethernet]
? (172.16.219.255) at (incomplete) on vmnet1 ifscope [ethernet]
? (192.168.1.1) at 98:fc:11:91:73:92 on en1 ifscope [ethernet]
? (192.168.1.255) at (incomplete) on en1 ifscope [ethernet]
? (192.168.38.255) at (incomplete) on vmnet8 ifscope [ethernet]
rist@wifi-212:~/work/teaching/642-fall-2011/slides$
```

ARP has no authentication

- Easy to sniff packets on (non-switched) ethernet
- What else can we do?



<u>Easy Denial of Service (DoS):</u>
Send ARP reply associating gateway 192.168.1.1 with a non-used MAC address

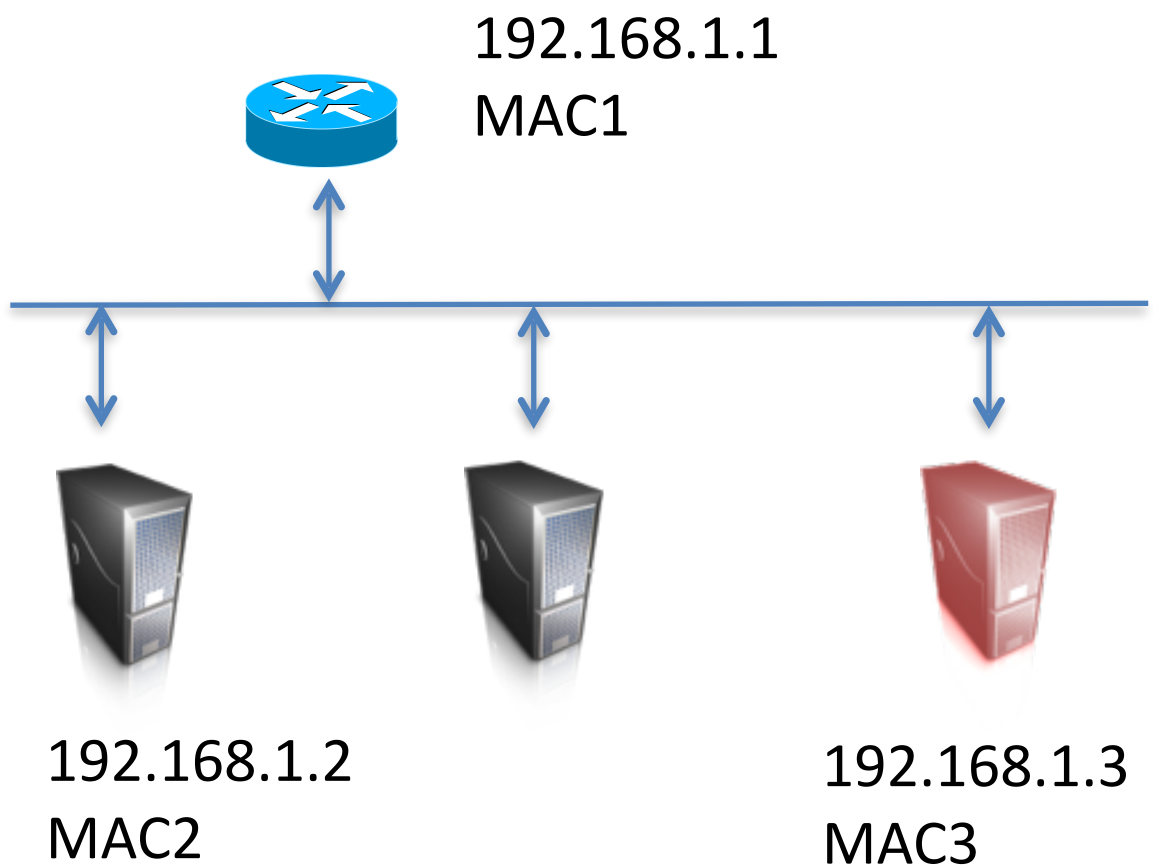
ARP has no authentication

- Easy to sniff packets on (non-switched) ethernet
- What else can we do?

<u>Active Man-in-the-Middle:</u>

ARP reply to MAC2
192.168.1.1 -> MAC3

ARP reply to MAC1
192.168.1.2 -> MAC3



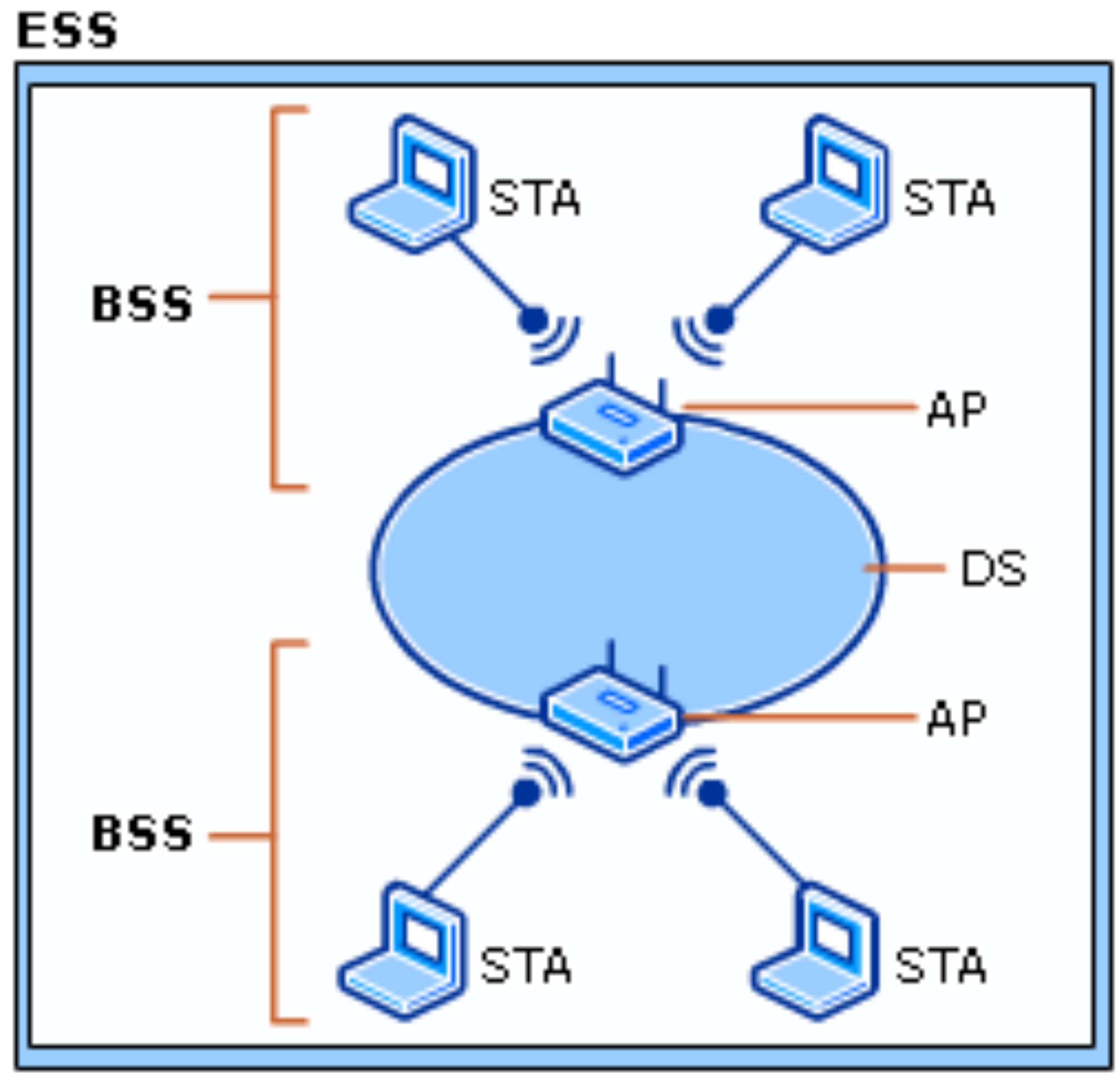
Now traffic “routed” through malicious box

802.11 (wifi)

STA = station
AP = access point

BSS = basic service set
DS = distribution service
ESS = extended service set

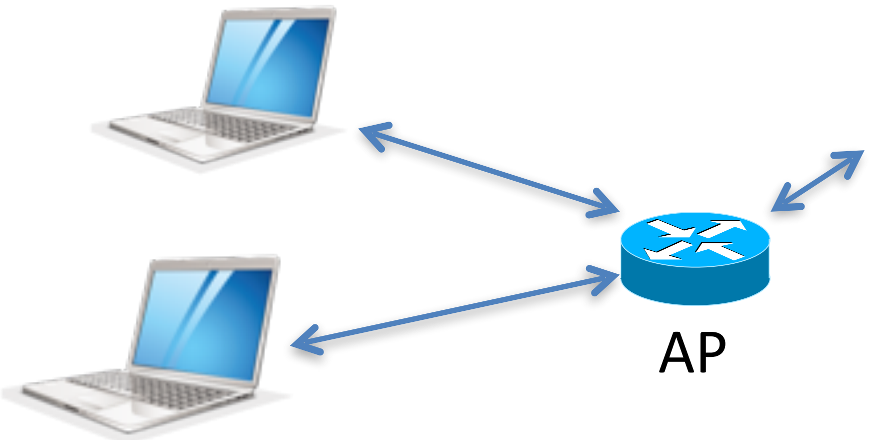
SSID (service set identifier)
identifies the 802.11 network

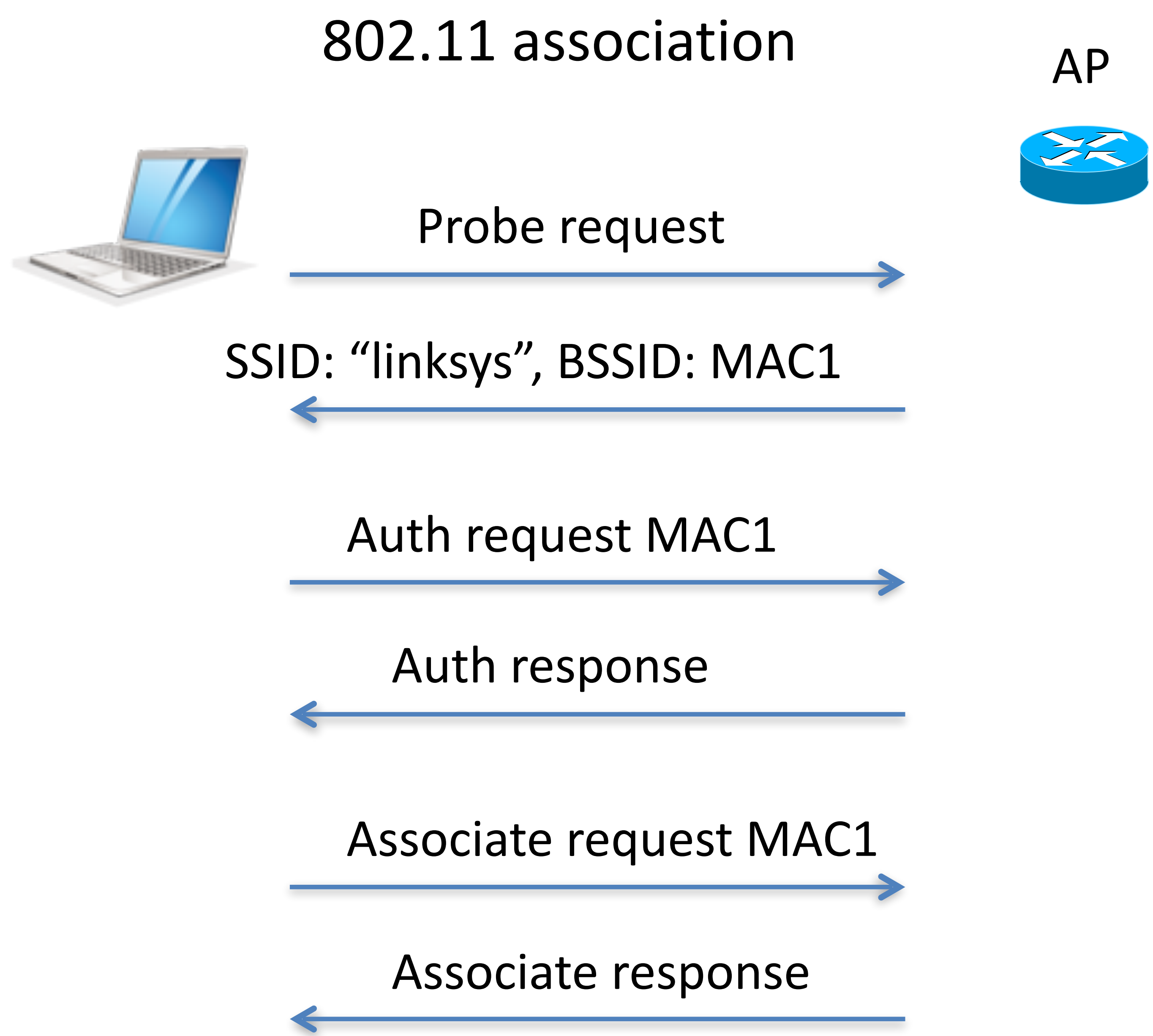


http://technet.microsoft.com/en-us/library/cc757419(WS.10).aspx

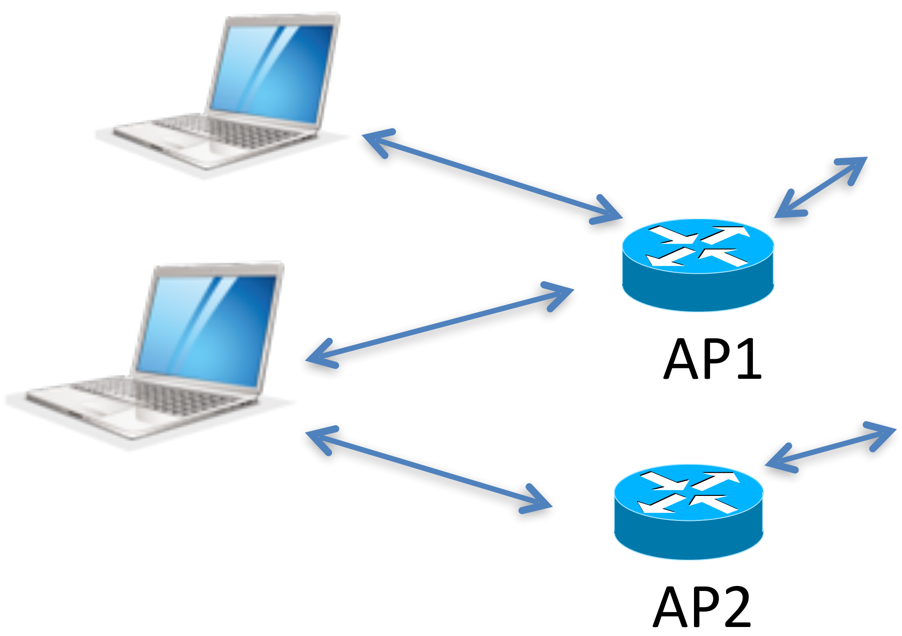
Typical WiFi modes:
Unsecured
Wireless Protected Access (WPA2) - password authenticated, encrypted

802.11 association

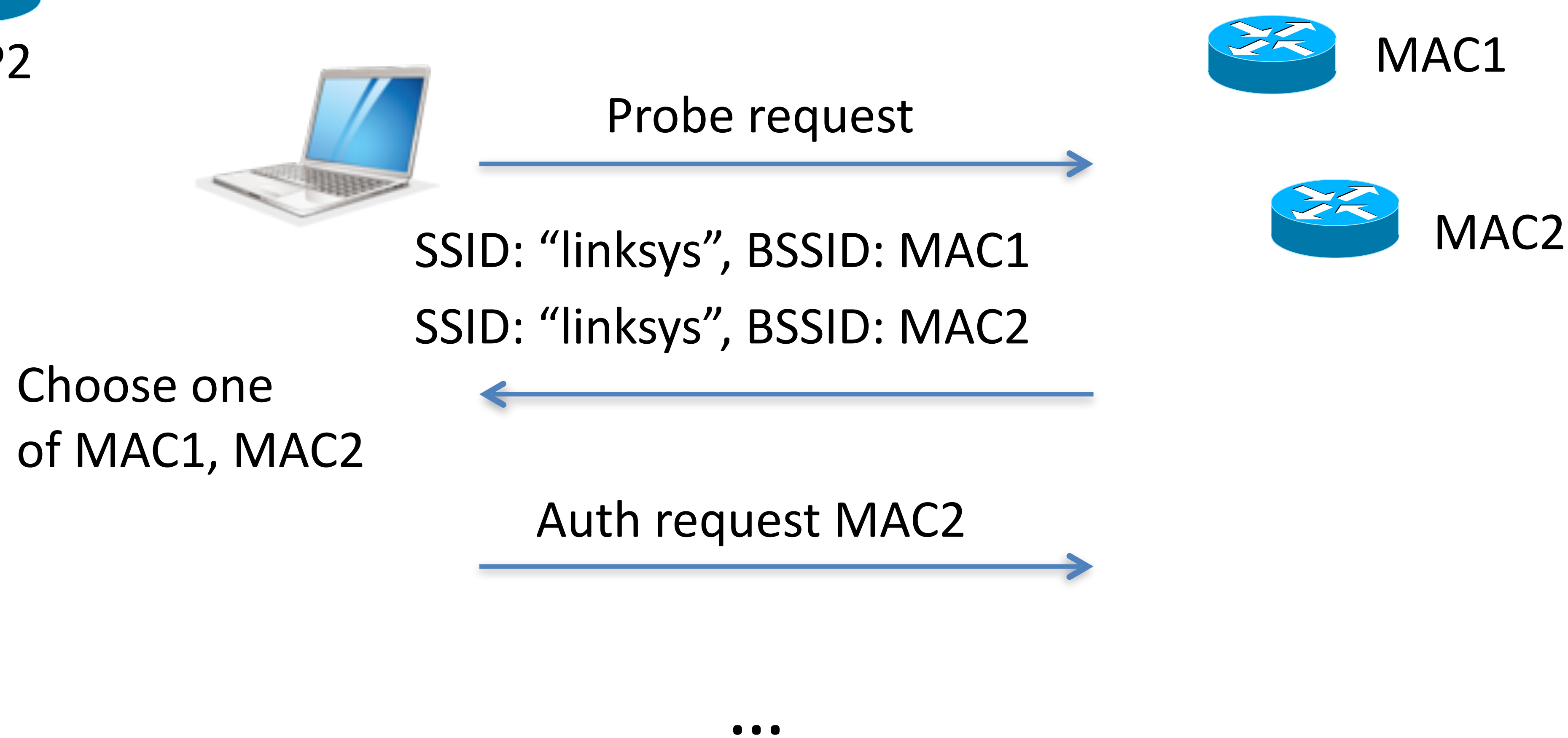




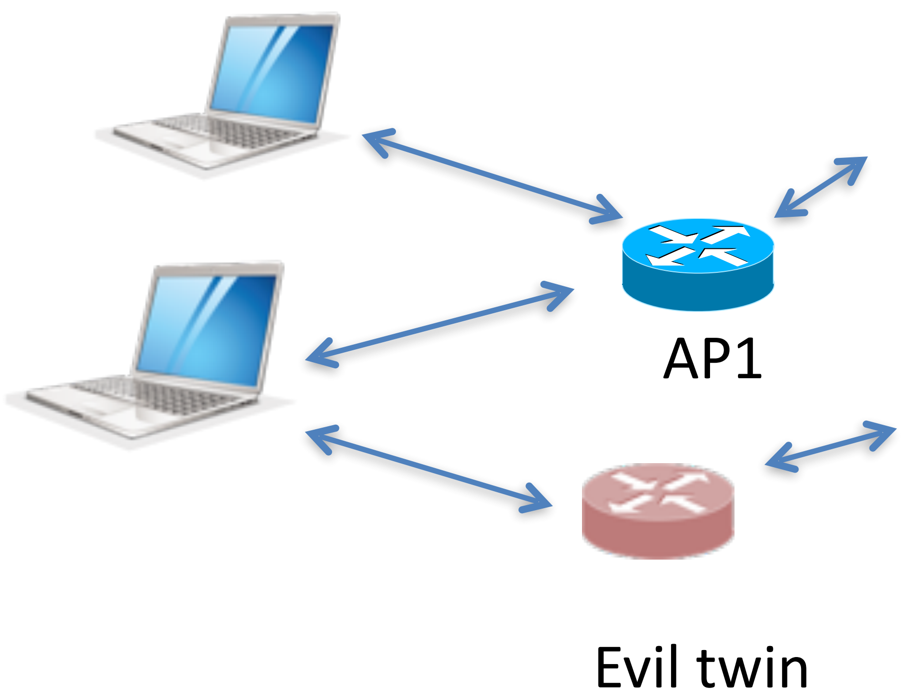
802.11 association



Two APs for same network



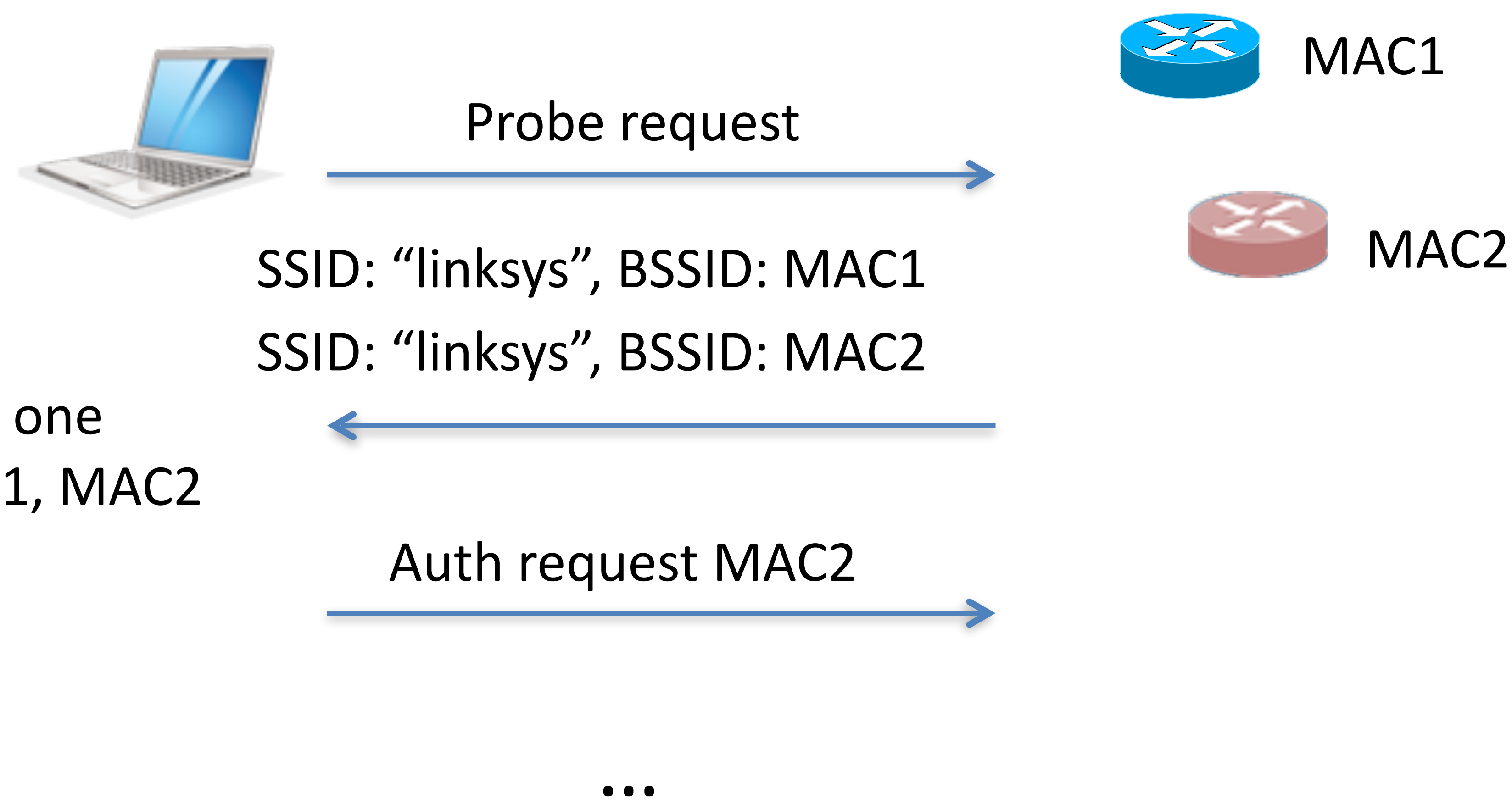
802.11 evil twins



Basic idea:

- Attacker pretends to be an AP to intercept traffic or collect data

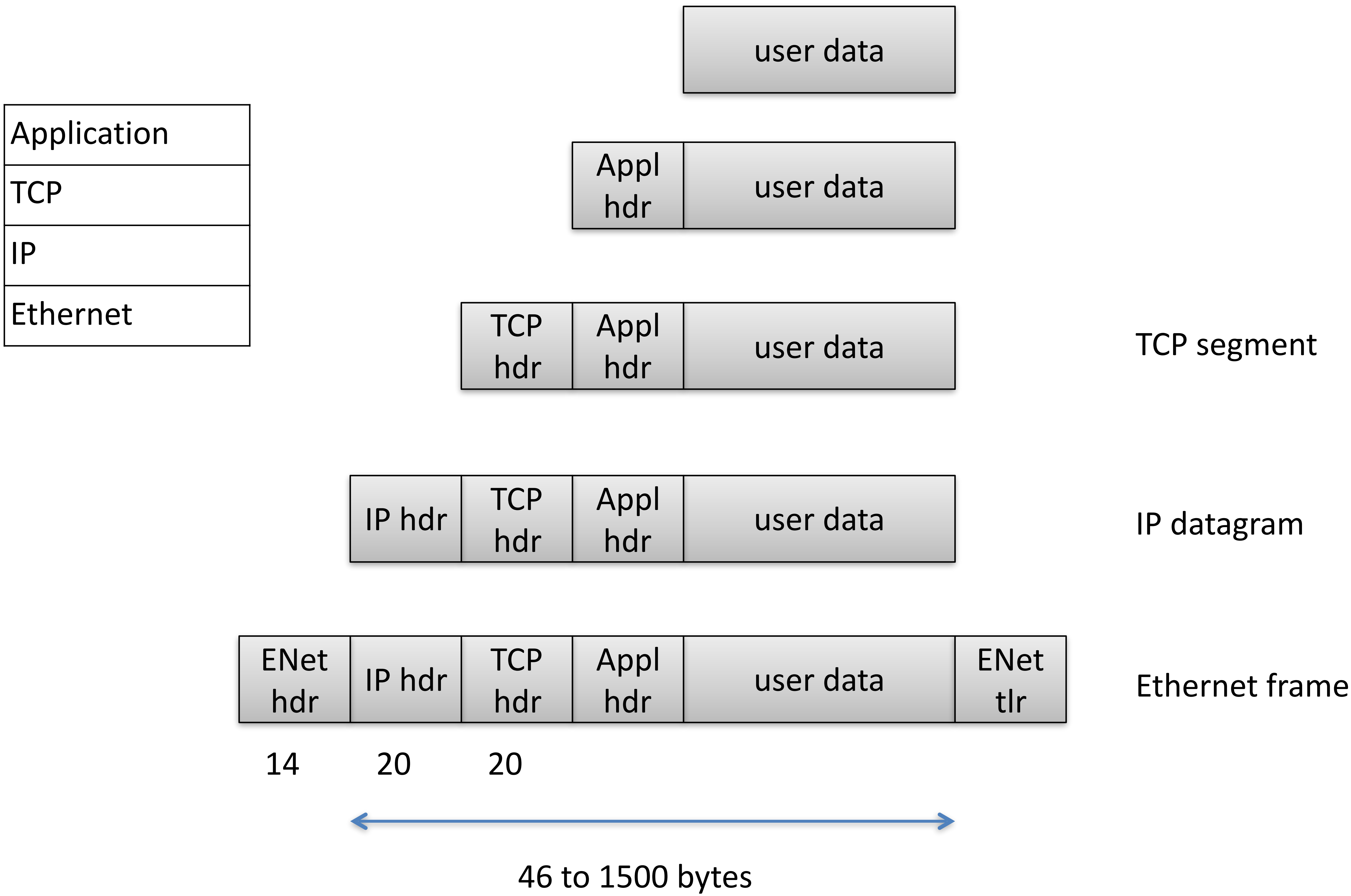
Basic attack: rogue AP



Parrot ARdrone

Drone is a WiFi access point
Uses unsecured 802.11 connection (WiFi)
Controlled from iPad or iPhone with an app
Uses MAC address for security

Internet protocol stack

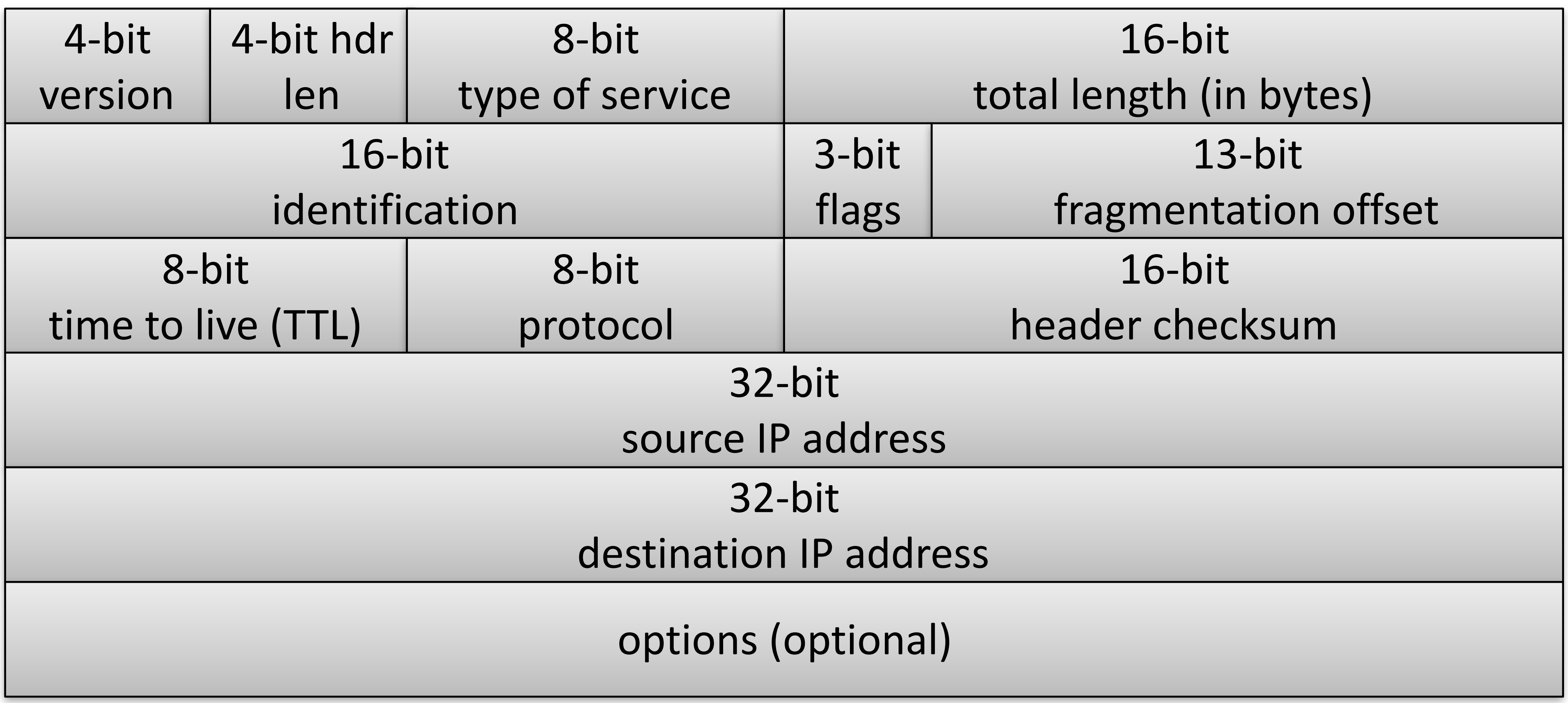


IP protocol (IPv4)

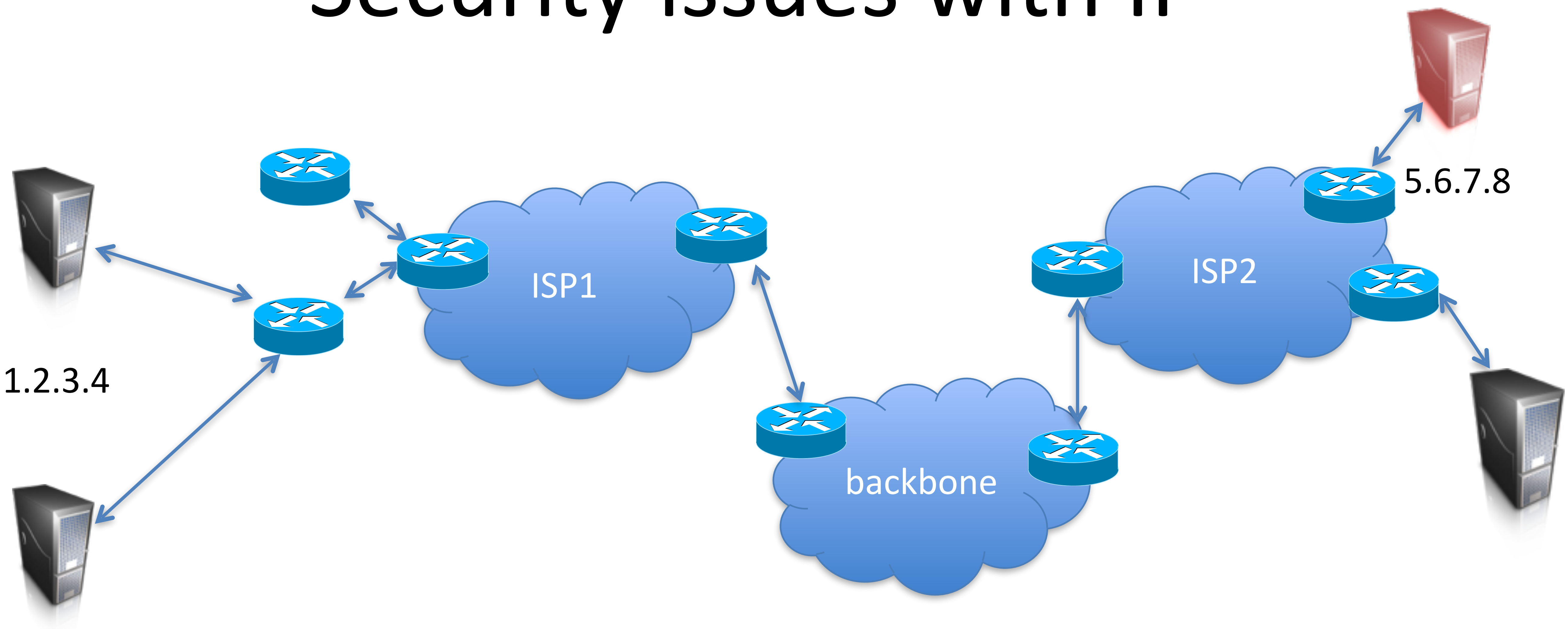
- Connectionless
  - no state
- Unreliable
  - no guarantees
- ICMP (Internet Control Message Protocol)
  - error messages, etc.
  - often used by tools such as ping, traceroute

IPv4

Ethernet frame
containing
IP datagram



Security issues with IP

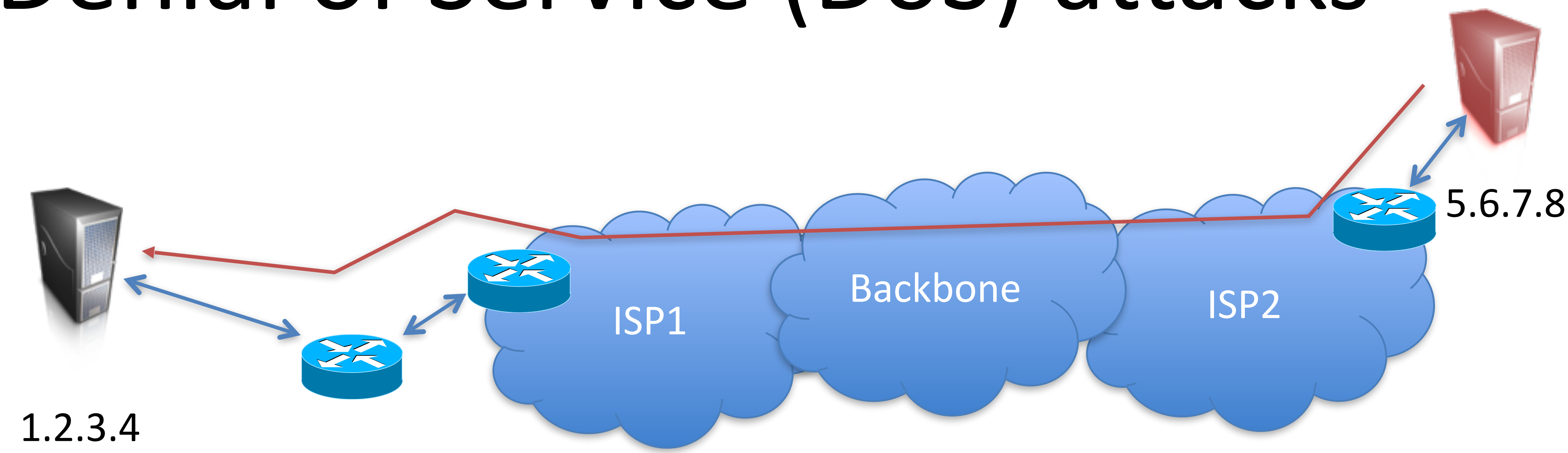


Routing has issues, we'll get to that later

What else?

- No source address authentication in general

Denial of Service (DoS) attacks



Goal: prevent legitimate users from accessing victim (1.2.3.4)

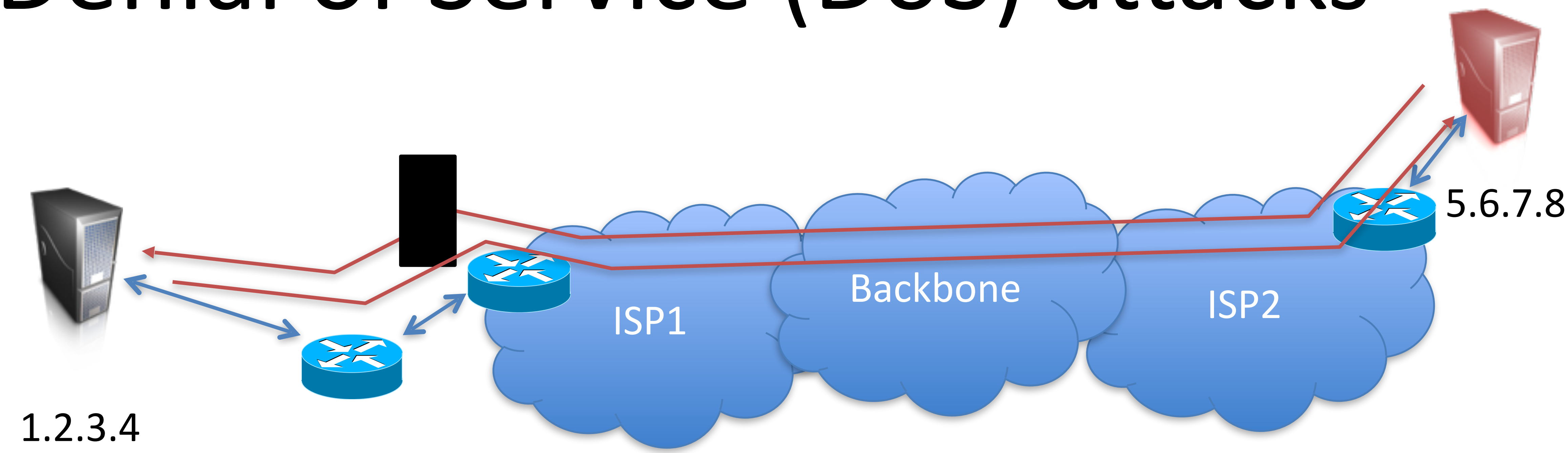
ICMP ping flood

ICMP
(Internet Control Message Protocol)

IP hdr	ICMPh dr	ICMP message

8-bit type	8-bit code	16-bit checksum
4-byte more of header (depends on type)		
message …		

Denial of Service (DoS) attacks

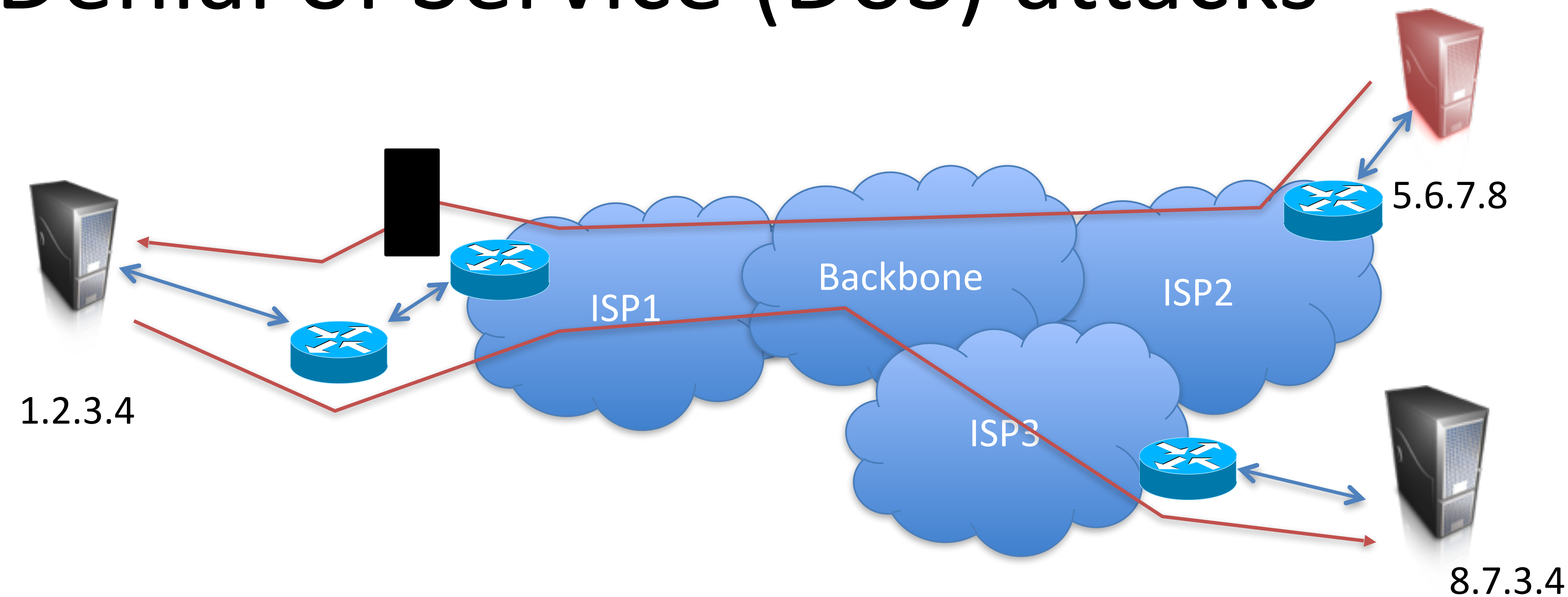


Goal is to prevent legitimate users from accessing victim (1.2.3.4)

ICMP ping flood

- Attacker sends ICMP pings as fast as possible to victim
- When will this work as a DoS? Attacker resources > victim's
- How can this be prevented? Ingress filtering near victim

Denial of Service (DoS) attacks



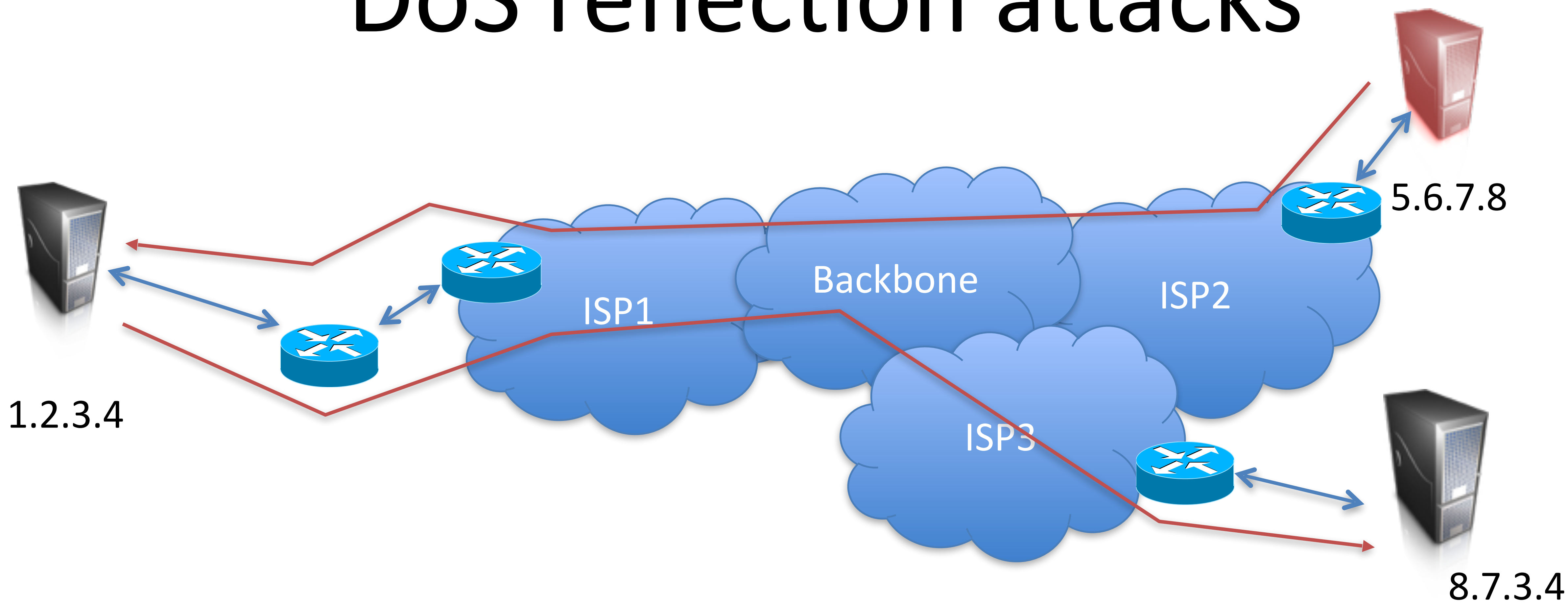
How can attacker avoid ingress filtering?

Attacker can send packet with fake source IP “spoofed” packet
Packet will get routed correctly
Replies will not

Send IP packet with source: 8.7.3.4 dest: 1.2.3.4 from 5.6.7.8

Filter based on source may be incorrect

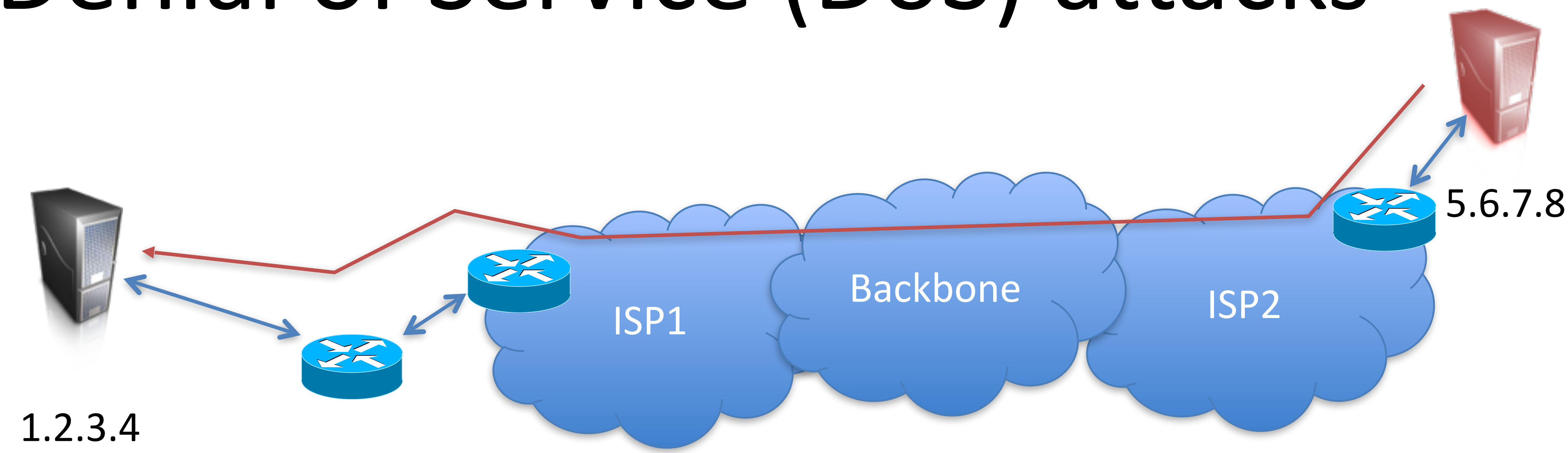
DoS reflection attacks



Note a valid packet sends a reply to 8.7.3.4

- Attacker can bounce an attack against 8.7.3.4 off 1.2.3.4
- "Frame" 1.2.3.4
- Single-packet exploit (1.2.3.4 in foreign country)

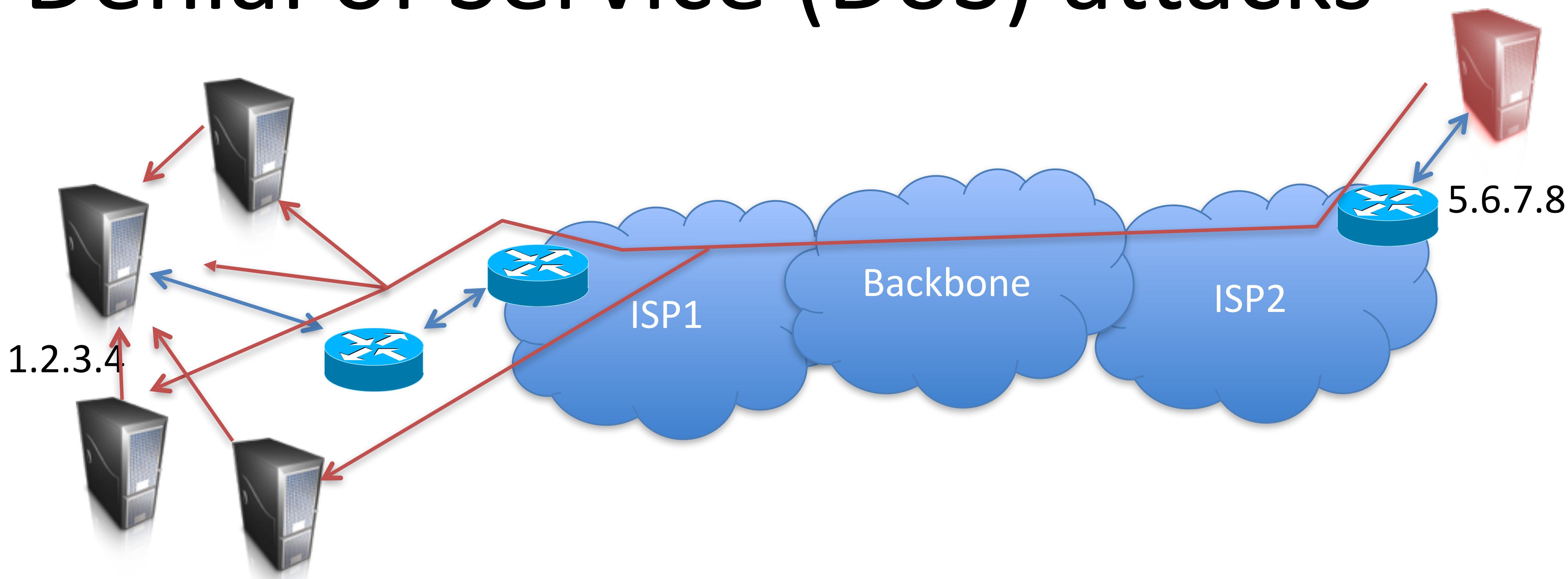
Denial of Service (DoS) attacks



DoS works better when there is ***asymmetry*** between victim and attacker

- Attacker uses few resources to cause victim to consume lots of resources

Denial of Service (DoS) attacks

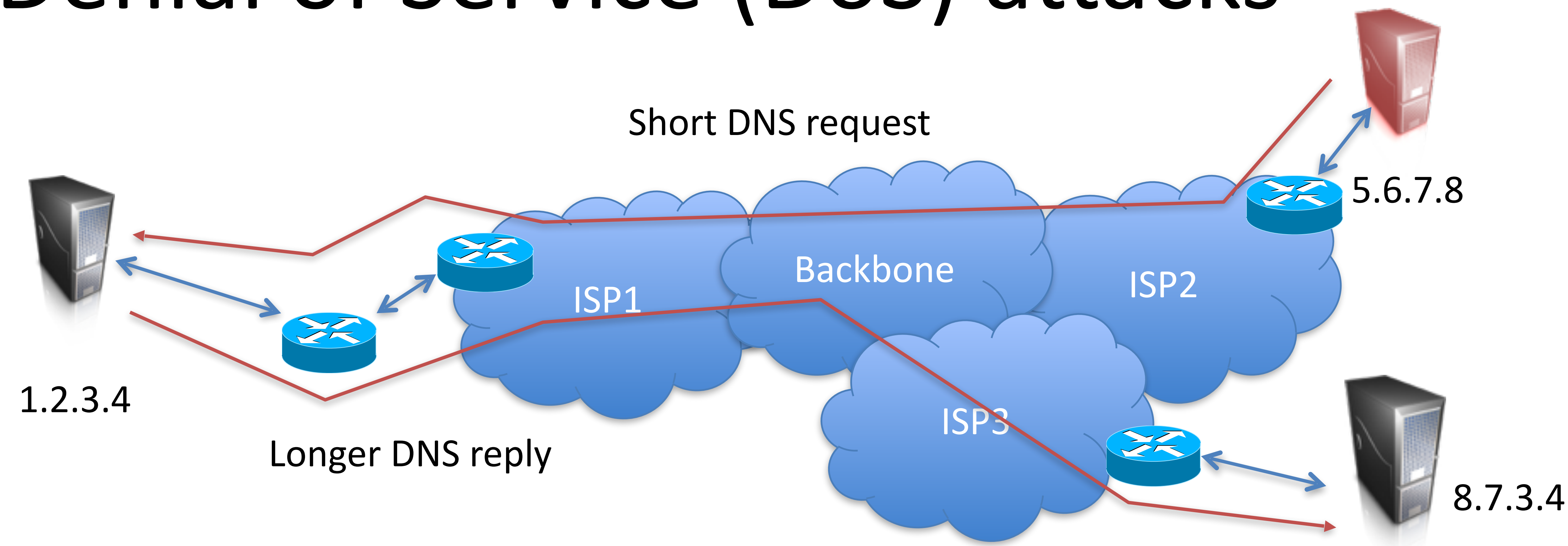


DoS works better when there is ***asymmetry*** between victim and attacker

- Attacker uses few resources to cause victim to consume lots of resources

Old example: Smurf attack
Router allows attacker to send broadcast ICMP ping on network. Attacker spoofs SRC address to be 1.2.3.4

Denial of Service (DoS) attacks



DoS works better when there is ***asymmetry*** between victim and attacker

- Attacker uses few resources to cause victim to consume lots of resources

More recent: DNS reflection attacks

Send DNS request w/ spoofed target IP (~65 byte request)

DNS replies sent to target (~512 byte response)

* In-class exercise
  / Hybrid encryption, digital signatures, PBKDF

* Network Security
  / ARP cache poisoning, MitM, DoS
  / WiFi Evil Twins
  / IP (in-security)

* Exit slips
  / 1 thing you learned
  / 1 thing you didn't understand

recap