QUEEN'S UNIVERSITY BELFAST

Security Issues in Internet Protocols – Part 1

Dr. Sandra Scott-Hayward

CSC3064 Lecture 06

School of Electronics, Electrical Engineering and Computer Science

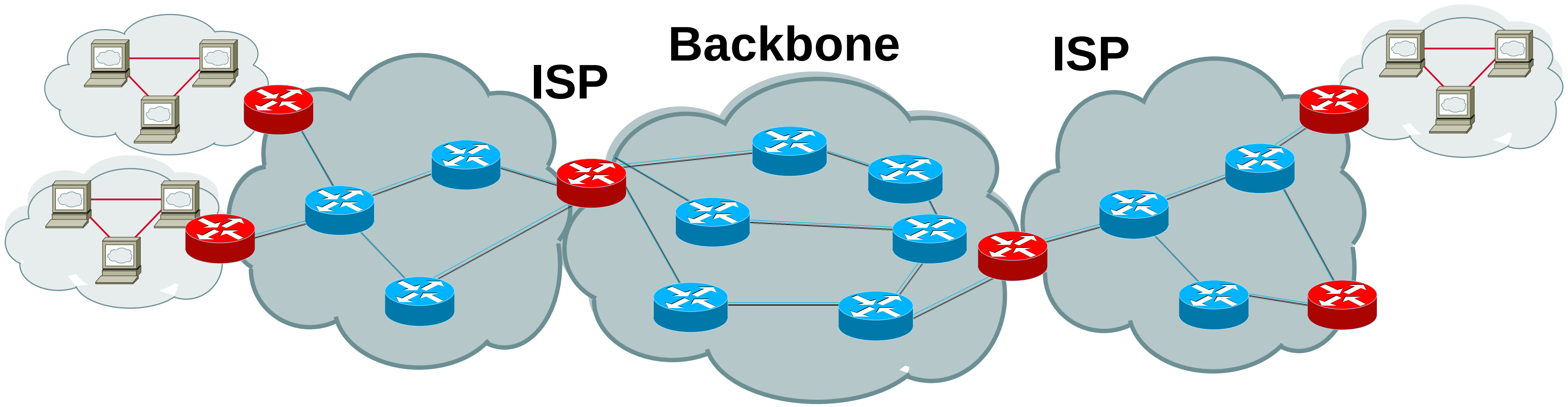
Session Overview

- TCP/IP
- ARP (Address Resolution Protocol)
    - ARP spoofing

References:
Jacobson, Douglas. *Introduction to network security*. CRC Press, 2008.
Schäfer, Günter, and Michael Rossberg. *Security in Fixed and Wireless Networks*. John Wiley & Sons, 2016.
Stallings, William. *Network security essentials: applications and standards*. Pearson Education India, 2007.

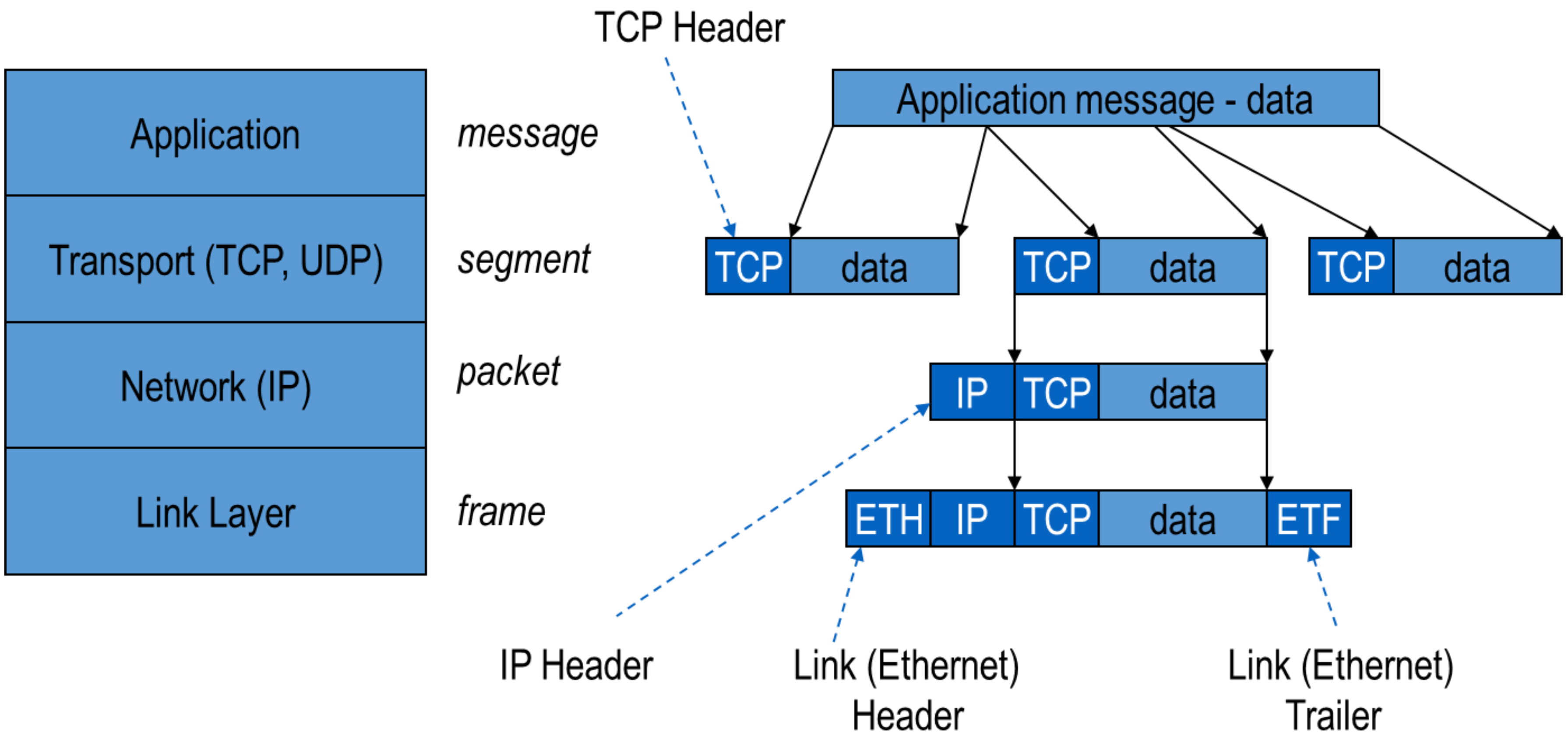
QUEEN'S UNIVERSITY BELFAST

Internet Infrastructure



- Local and inter-domain routing
  - TCP/IP for routing and messaging
  - ARP for address resolution
  - OSPF for inter-AS routing
  - BGP for routing announcements

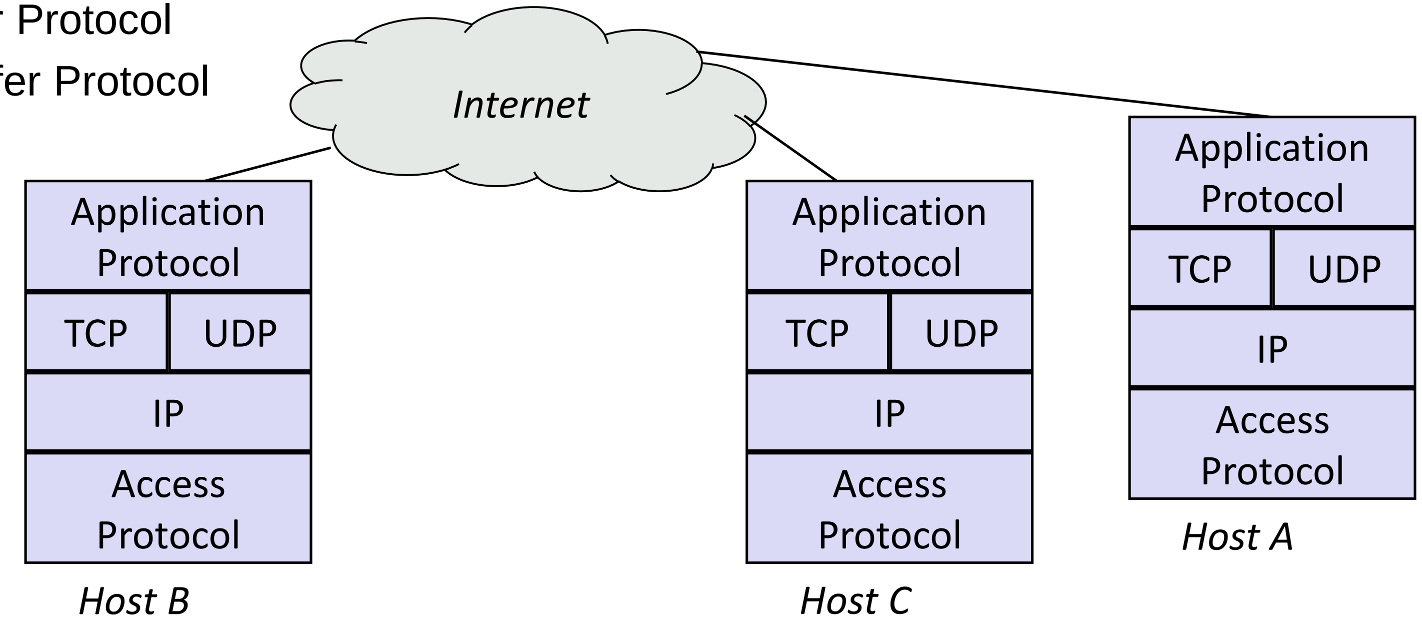
TCP – Data Formats



QUEEN'S UNIVERSITY BELFAST

The TCP/IP Protocol Suite

- *IP (Internet Protocol):* unreliable, connectionless network protocol
- *TCP (Transmission Control Protocol)*: reliable, connection-oriented transport protocol, realized over IP
- *UDP (User Datagram Protocol)*: unreliable, connectionless transport protocol, offers an application interface to IP
- Examples for *application protocols*:
  - HTTP: Hypertext Transfer Protocol
  - SMTP: Simple Mail Transfer Protocol



QUEEN'S UNIVERSITY BELFAST

The IPv4 Packet Format

<table>
<tr><td>Ver.</td><td>IHL</td><td>TOS</td><td colspan="2">Length</td></tr>
<tr><td colspan="3">IP Identification</td><td>Flags</td><td>Fragment Offset</td></tr>
<tr><td colspan="2">TTL</td><td>Protocol</td><td colspan="2">IP Checksum</td></tr>
<tr><td colspan="5">Source Address</td></tr>
<tr><td colspan="5">Destination Address</td></tr>
<tr><td colspan="5">IP Options (if any)</td></tr>
<tr><td colspan="5">TCP / UDP / ... Payload</td></tr>
</table>

- *Version (Ver.):* 4 bits
  - Currently version 4 is widely deployed
  - Version 6 should be deployed … but slow
- *IP header length (IHL):* 4 bits
  - Length of the IP header in 32-bit words
- *Type of service (TOS):* 8 bits
  - This field could be used to indicate the traffic requirements of a packet
  - Now: DCSP and Explicit Congestion (EC) Indication
- *Length:* 16 bits
  - The length of the packet including the header in octets
- *Identification:* 16 bits
  - Used to "uniquely" identify an IP datagram
  - Important for re-assembly of fragmented IP datagrams
- *Flags:* 3 bits
  - Bit 1: do not fragment, Bit 2: datagram fragmented, Bit 3: reserved for future use
- *Fragmentation offset:* 13 bits
  - The position of this packet in the corresponding IP datagram
- *Time to live (TTL):* 8 bits
  - At every processing network node, this field is decremented by one
  - When TTL reaches 0 the packet is discarded to avoid packet looping

The IPv4 Packet Format

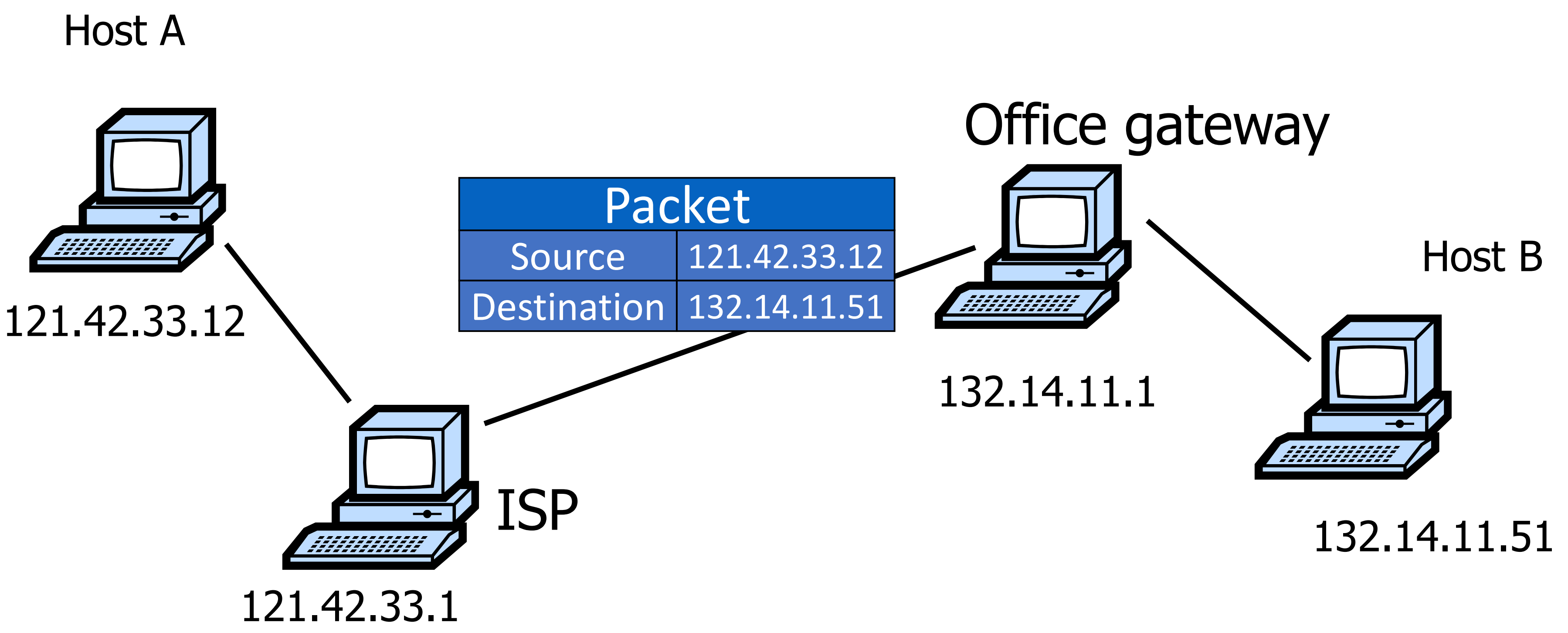
Ver.	IHL	TOS	Length	
IP Identification			Flags	Fragment Offset
TTL		Protocol	IP Checksum	
Source Address				
Destination Address				
IP Options (if any)				
TCP / UDP / ... Payload				

- *Protocol:* 8 bits
  - Indicates the (transport) protocol of the payload
  - Used by the receiving end system to de-multiplex packets among various transport protocols such as TCP, UDP, ...
- *Checksum:* 16 bits
  - Protection against transmission errors
  - As this is not a cryptographic checksum, it can easily be forged
- *Source address:* 32 bits
  - The IP address of the sender of this packet
- *Destination address:* 32 bits
  - The IP address of the intended receiver of this packet
- *IP Options:* variable length
  - An IP header can optionally carry additional information

QUEEN'S UNIVERSITY BELFAST

IP Routing

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



IP Protocol Functions

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

Error reporting

- ICMP packet to source if packet is dropped (e.g. time exceeded/destination unreachable)

TTL field: decremented after every hop

- Packet dropped if TTL=0 (prevents infinite loops)

Issue: No src IP authentication

Client is trusted to embed correct source IP

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

Anyone who owns their machine can send packets with arbitrary source IP

- … response will be sent back to forged source IP

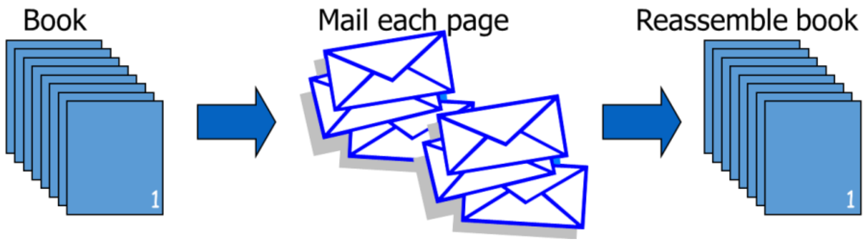
Implications:

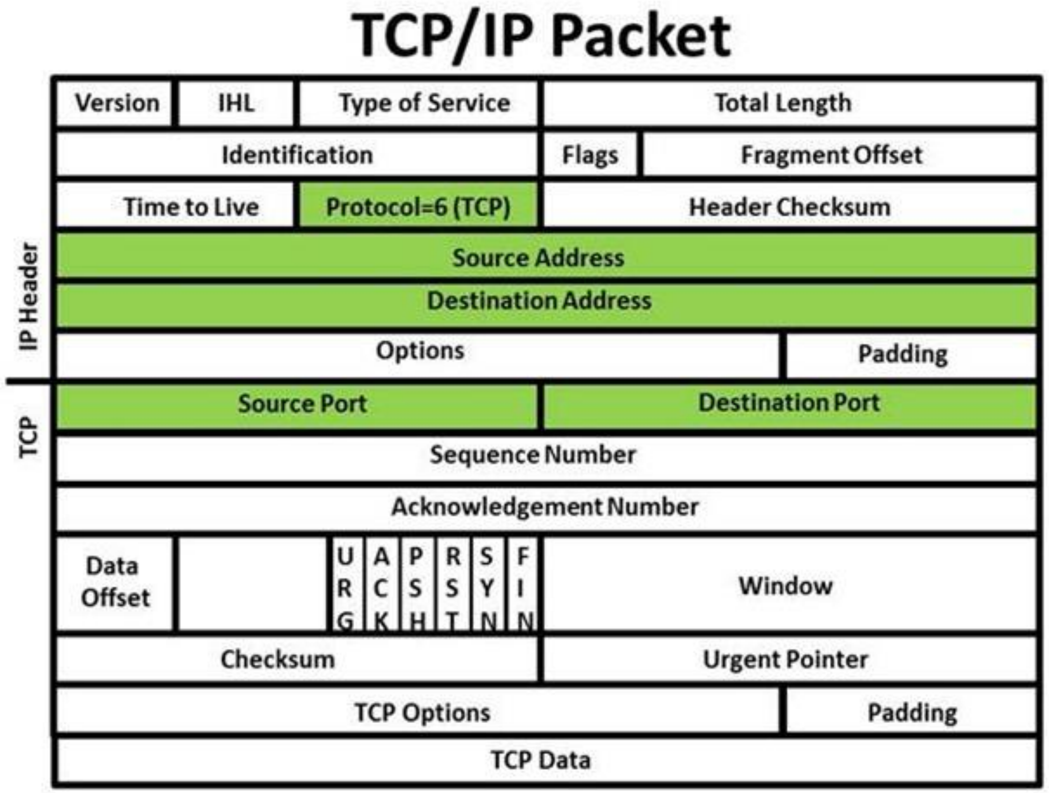
- Anonymous DoS attacks

Transmission Control Protocol

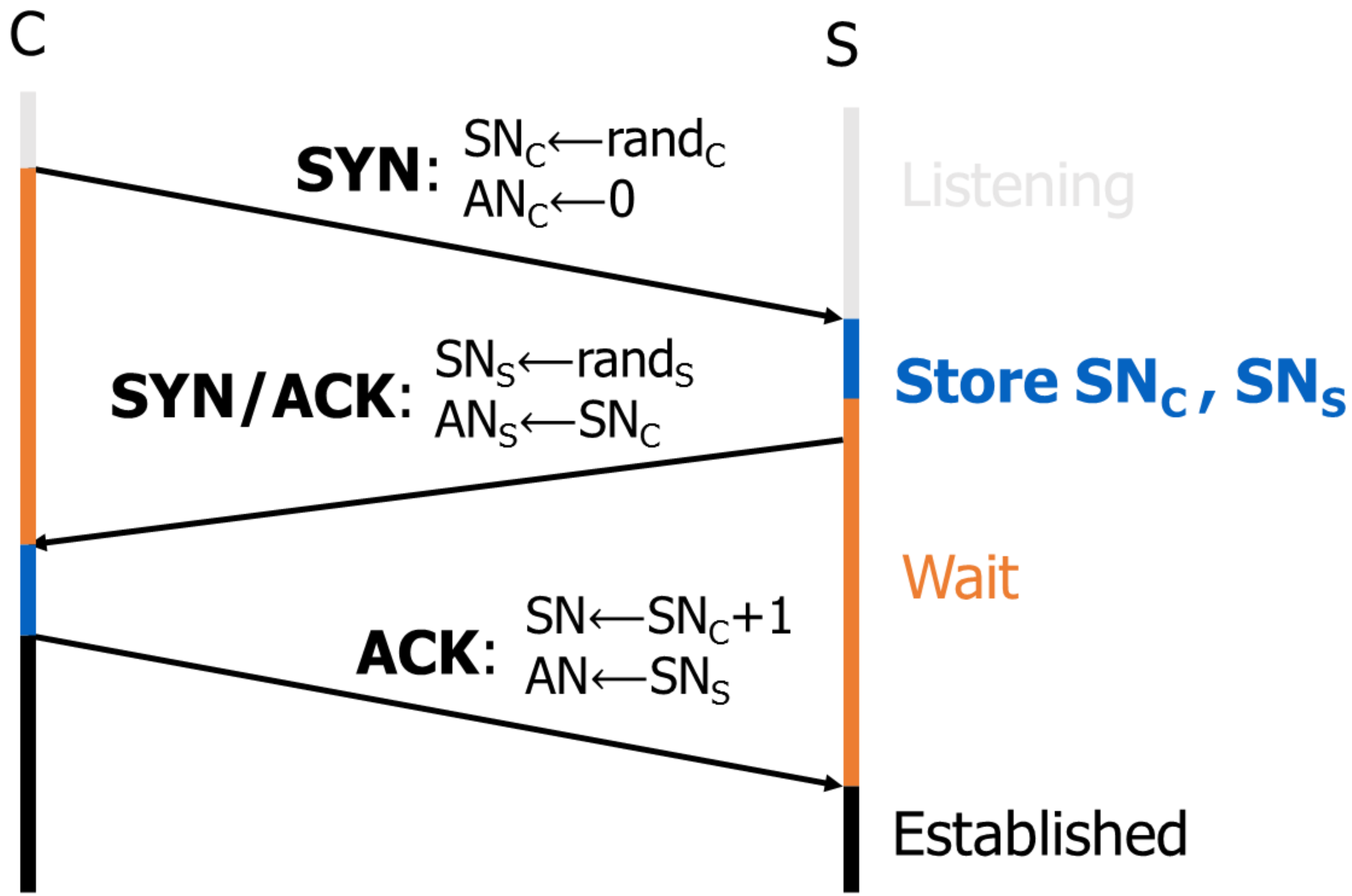
Connection-oriented, preserves order

- Sender
  - Break data into packets
  - Attach packet numbers
- Receiver
  - Acknowledge receipt; lost packets are resent
  - Reassemble packets in correct order





Review: TCP Handshake

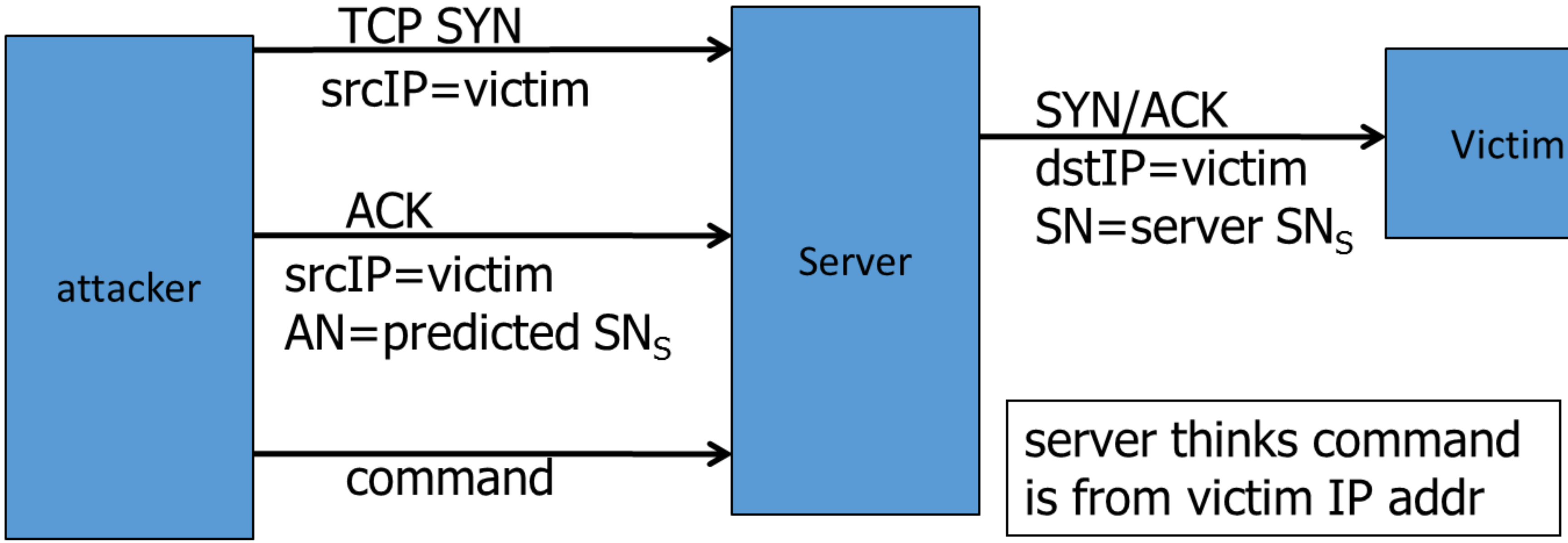


Received packets with SN too far outside the window are dropped

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



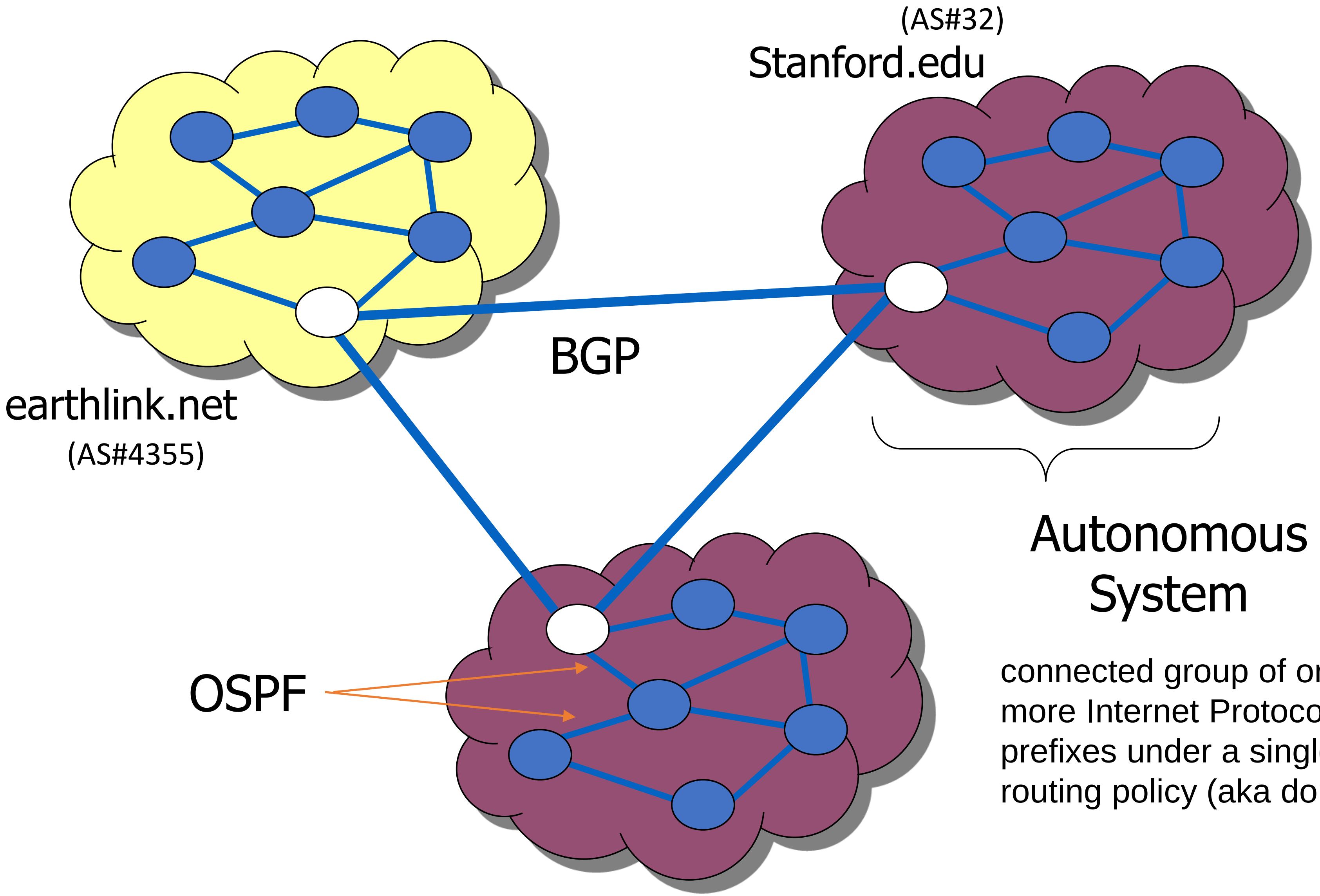
Example DoS Vulnerability: Reset

Attacker sends a Reset packet to an open socket

- If correct SN_S then connection will close $\Rightarrow$ DoS
- Naively, success prob. is $1/2^{32}$ (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

- Most effective against long lived connections, e.g. BGP

Interdomain Routing



connected group of one or more Internet Protocol prefixes under a single routing policy (aka domain)

Routing Protocols

- ARP (address resolution protocol): IP addr ⟶ eth addr

  Security issues: (local network attacks)

  Node A can confuse the 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)

- OSPF: used for routing within an AS

- 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

  Anyone can hijack route to victim

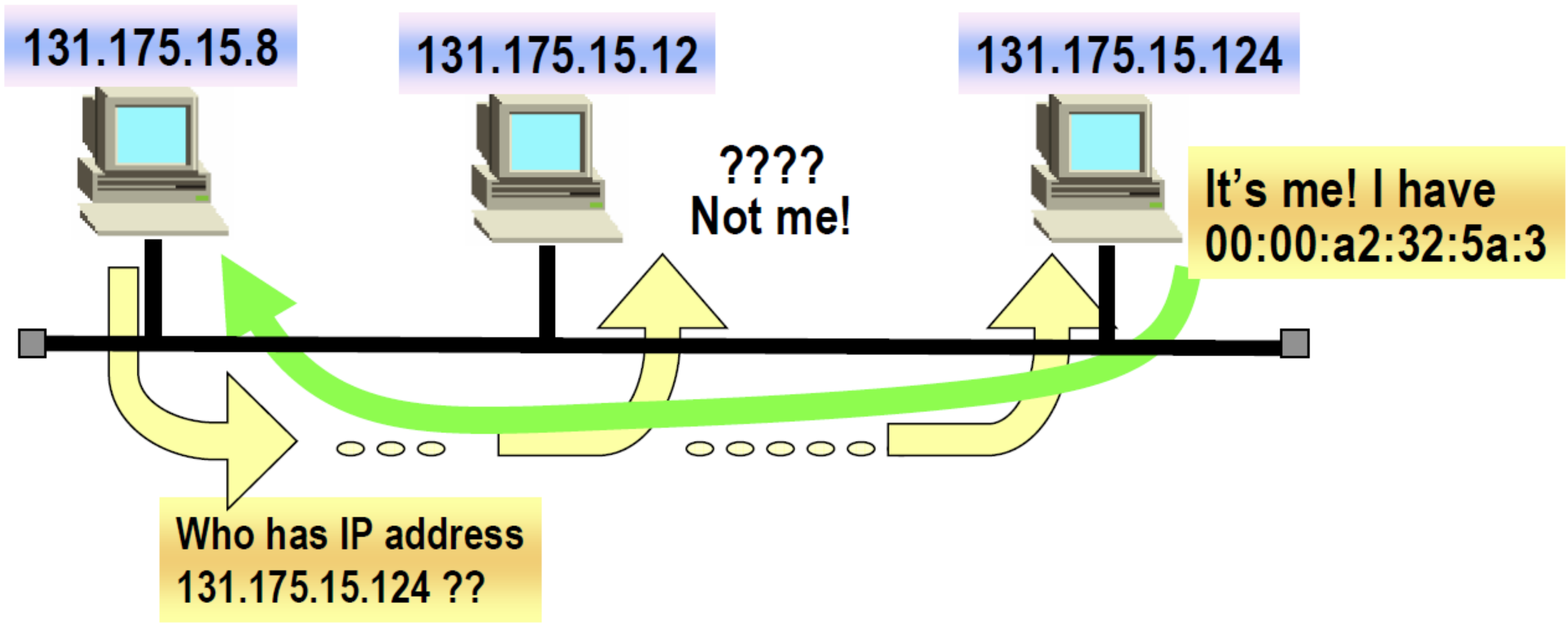
Address Resolution Protocol (ARP)

- Mapping Layer 3 (IP) to Layer 2 (MAC) addresses
- ARP (IPv4), NDP (IPv6)

QUEEN'S UNIVERSITY BELFAST

ARP

- Send broadcast request, Receive unicast response



- Arp cache to avoid arp request for every IP datagram

ARP Request/Reply Encapsulation

- Ethernet Destination Address
  → ff:ff:ff:ff:ff:ff (broadcast) for ARP request
- Ethernet Source Address
  → of ARP requester
- Frame Type
  → ARP request/reply: 0x0806
  → RARP request/reply: 0x8035
  → IP datagram: 0x0800

Protocol de-multiplexing codes!

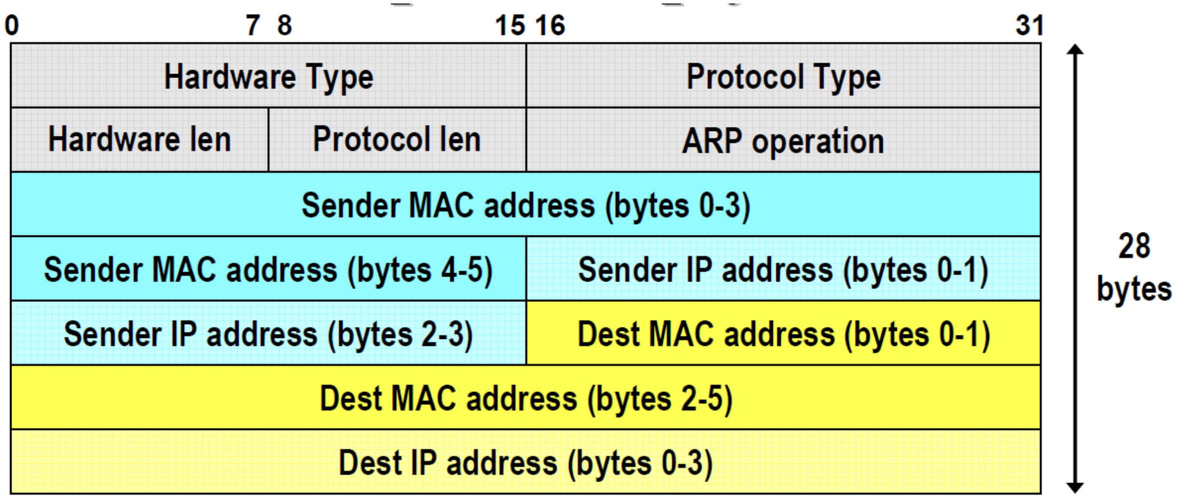
6 bytes	6 bytes	2 bytes	28 bytes (for IP)	4 bytes
Ethernet destination address	Ethernet source address	frame type	ARP Request / Reply	CRC

QUEEN'S UNIVERSITY BELFAST

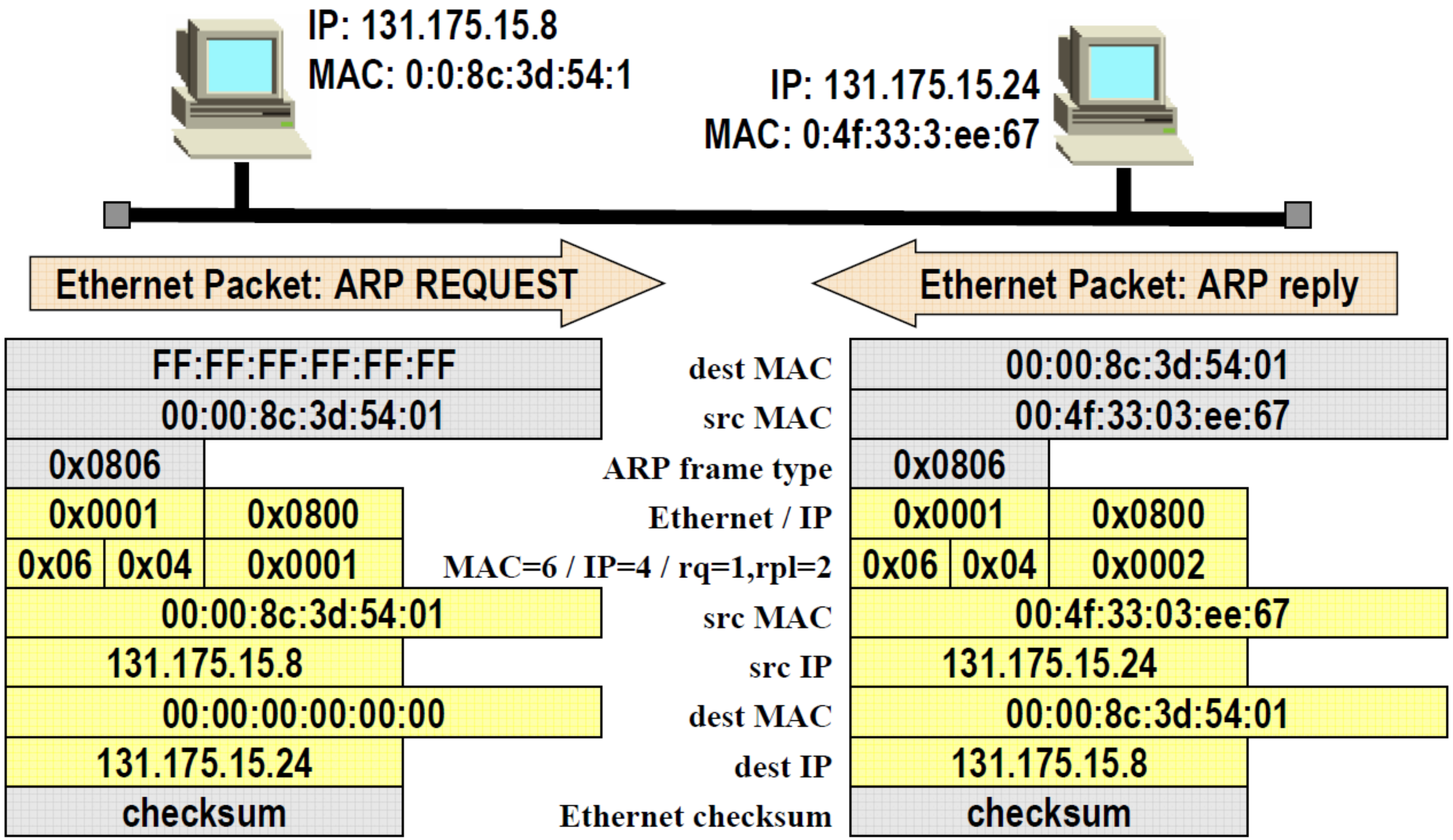
ARP Request/Reply Encapsulation

- Hardware type: 1 for Ethernet
- Protocol type: 0x0800 for IP
- Hardware len: length in bytes of hardware addresses (6 bytes for ethernet)
- Protocol len: length in bytes of logical addresses (4 bytes for IP)
- ARP operation: 1=request; 2=reply; 3/4=RARP req/reply

  → ff:ff:ff:ff:ff:ff (broadcast) for ARP request



Sample ARP Request/Reply



QUEEN'S UNIVERSITY BELFAST

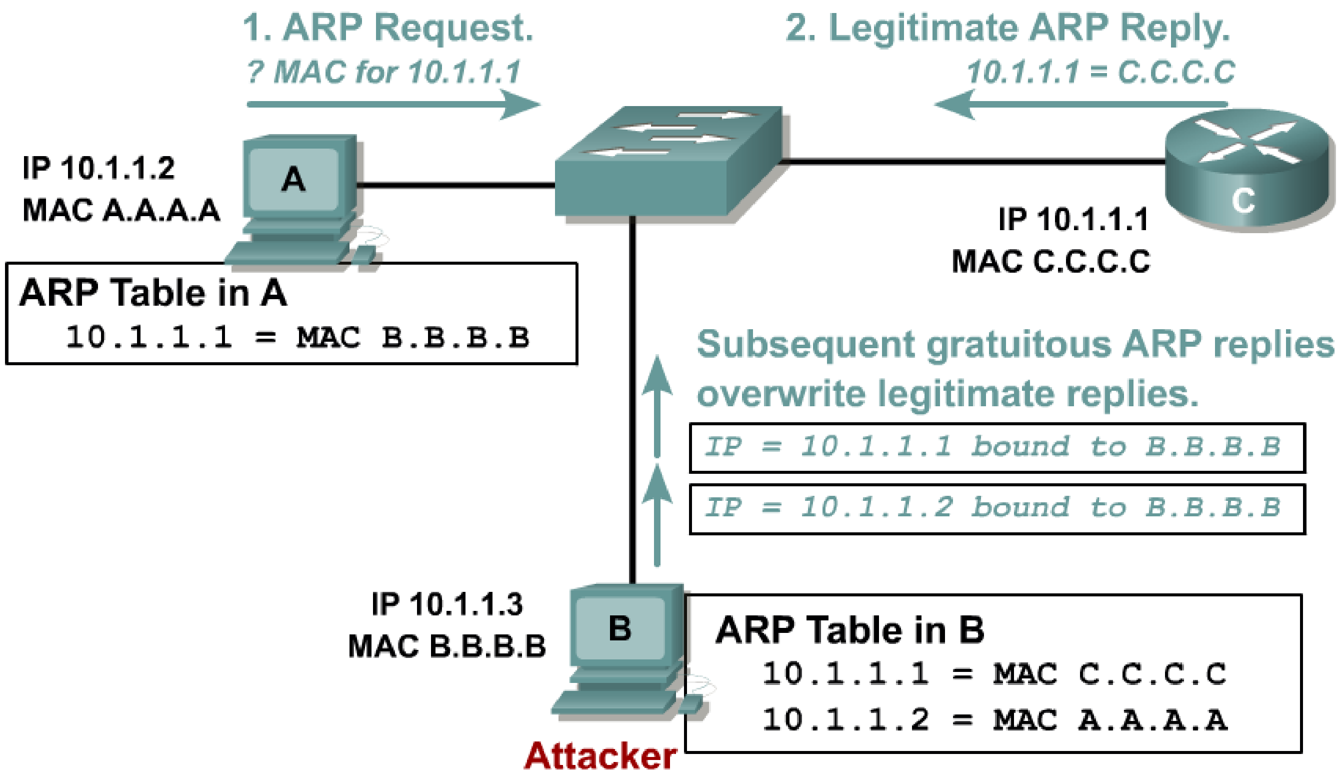
ARP Security Issues

- Stateless protocol – each request or reply treated independently so information from gratuitous ARP replies accepted
- No mechanism to authenticate the sender of an ARP request/reply message or to check integrity or validity of provided information so poisoning host's ARP cache with false IP-MAC address mapping is relatively easy … craft an ARP request/reply message with a false SPA field (IP address)

ARP Spoofing

- Gratuitous request with victim's SPA and TPA and own SHA
- Gratuitous reply with victim's SPA and own TPA
- Reply to request with victim's SPA and own TPA

Note: Limited to broadcast domain



SPA (Sender Protocol Address)= Src IP, THA (Target Hardware Address) = Dst MAC

QUEEN'S UNIVERSITY BELFAST

Approaches to mitigate ARP spoofing/poisoning

- S-ARP for cryptographic protection
  - relies on each node having a public/private key pair
  - Digital signature field added to ARP packet format => message integrity
  - reliance on PKI/CA is impractical
- Dynamic ARP inspection (DAI)
  - Cisco proprietary - implemented in Ethernet switches and checks ARP packets against a trusted database of IP-MAC address mappings – challenge to establish and maintain the database
- Arpwatch monitoring tool

QUEEN'S UNIVERSITY BELFAST

Summary

Core protocols not designed for security

- Eavesdropping, packet injection, route stealing etc.
- Patched over time to prevent basic attacks (e.g. random TCP SN)
- More secure variants exist:
  - ARP $\longrightarrow$ S-ARP

Questions?

Next Session: Security Issues in Internet Protocols – Part 2

Tuesday, 29 January 2019

QUEEN'S UNIVERSITY BELFAST