Computer Networks
(Intensive Learning Experience)

July 03, 2018

Dr. Ram P Rustagi
Dept of CSE
KSIT, Bangalore
rprustagi@ksit.edu.in
http://www.rprustagi.com

Executive Summary

- Why ILE
  - Covering employability gap
- Network Technology Topics
  - DNS, Packet forwarding/routing
    - In routers and switches
  - ICMP, ARP, Path MTU
  - HTTP, SSH, FTP, Telnet
  - IP, IPv6, TCP, UDP
- Tools for learning and experience
  - nc, wget, telnet, wireshark, tcpdump
  - ip (iproute2 package) commands
  - Cisco packet tracer, GNS3 simulator

Sources

- iproute2 package
  - lartc.org/howto/lartc.iproute2.explore.html
- wireshark: www.wireshark.org
- nc: netcat.sourceforge.net/
- Cisco Packet Tracer: Cisco Network Academcy
- GNS3: www.gns3.net/download/
- Learning Linux:
  - https://www.edx.org/course/introduction-linux-linuxfoundationx-lfs101x-1
- ACS : http://acc.digital
- Github: github.com/rprustagi
- ELNT: http://rprustagi.com/ELNT/Experiential-Learning.html

NETWORK

Acronym

- **N**ovel
- **E**xperience of
- **T**heoretical,
- **W**orking,
- **O**perational, and
- **R**ealized
- **K**nowledge

Why ILE ?

- Employability gap
  - As per industry, gap >80% or even >90%
  - Poor performance during placement
  - Lack of knowledge to carry out required work
  - Lack of practical hands-on experience in college
- Approach for experience network technology
  - Consider a simple everyday case study
    - Consider various scenarios, constraints
    - Should be doable in the lab
    - Using only open source software
  - Discuss commonly asked placement questions
- Expectation:
  - Confidence with knowledge of how network works

Every Day Case Study

- Example case study: Using a browser on your laptop
- Question:
  - What happens internally when you type in `google.com` in your browser?"
  - What kind of network activity takes place in n/w
    - laptop, gateway, other network elements
  - Map Browser interaction to TCP/IP stack/layers
  - Protocols/addressing at each layer
    - IP addressing, subnetting, supernetting
  - What is TCP? Its working and handshaking.
  - Web Security

General N/W Insights

- HTTP protocol
  - request and response structure
  - role of headers
  - authentication
    - password fields
    - .htaccess, other protection
  - multi-site hosting
  - persistent vs non-persistent questions
  - session mgmt
    - cookies, URL rewriting, hidden fields
  - proxies: forward and reverse
- HTTPS: certificate mgmt

General N/W Queries

- What is subnetting?
  - How to divide various networks using subnet?
  - How many systems in particular subnet.
  - What subnet to be used for given setup
  - Masking the IP address
- Explain TCP flow control and congestion control
- How to know if a website is fake or not?
- For a given scenario, how to choose protocol
  - When to use UDP or TCP?

N/W Programming Challenges

- Difference between port and socket?
  - What is socket programming
    - what bind(), listen() do for server
  - Write a simple tcp server (pseudocode only)
  - Explain TCP handshake
- Is TCP reliable?
- Difference between various network elements
  - hub, repeater, switch, bridge, routers, gateways etc.
- HTTP return codes
  - (*) HTTP logs
- Concept of CDN (Akamai)

General N/W Misnomers

– Forwarding vs Routing
- What are various delays:
  – Propagation, Transmission, Queuing, Processing
- Address types:
  – Unicast, Multicast, Broadcast, Anycast

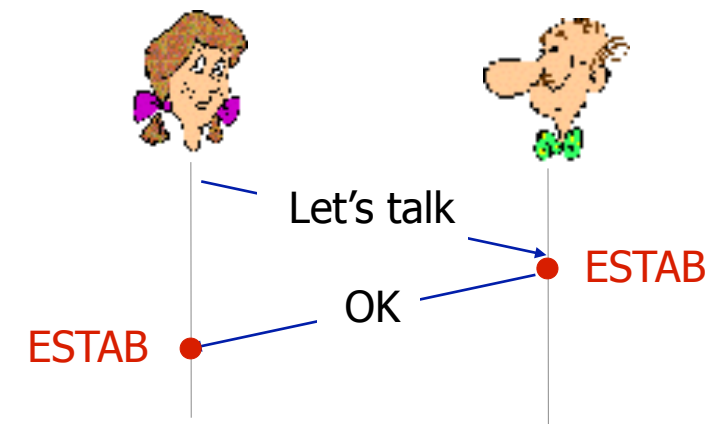
– Public IP address vs. Private IP address
- Error handling
  – Error Correction vs Error Detection
  – Parity bits, CRC, internet checksum

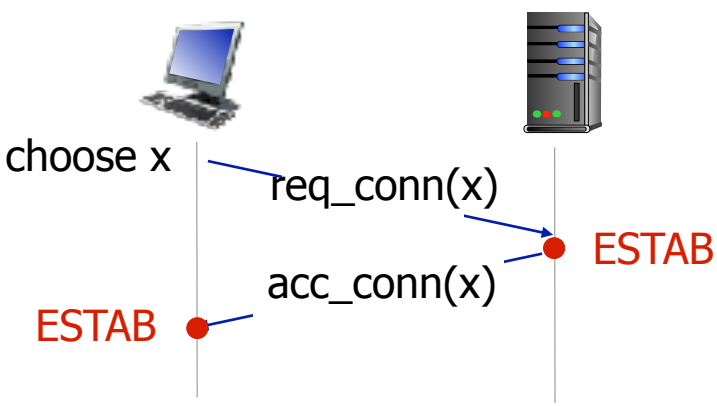
General N/W Operations

- If you want to isolate 2 systems in the same network, how would you do it?
- Explain the workings of DHCP and IP assignment
- After TCP connection opened, server goes down. What happens?
- Difference between forward and reverse proxy
- Difference between Router and multi-homed host
- P2P network vs Client server network
- Communication types:
  – Simples, half duplex, full duplex

Basis of TCP Handshake

2-way handshake:





Source: Kurose, Ross: Computer Networking, A Top Down Approach

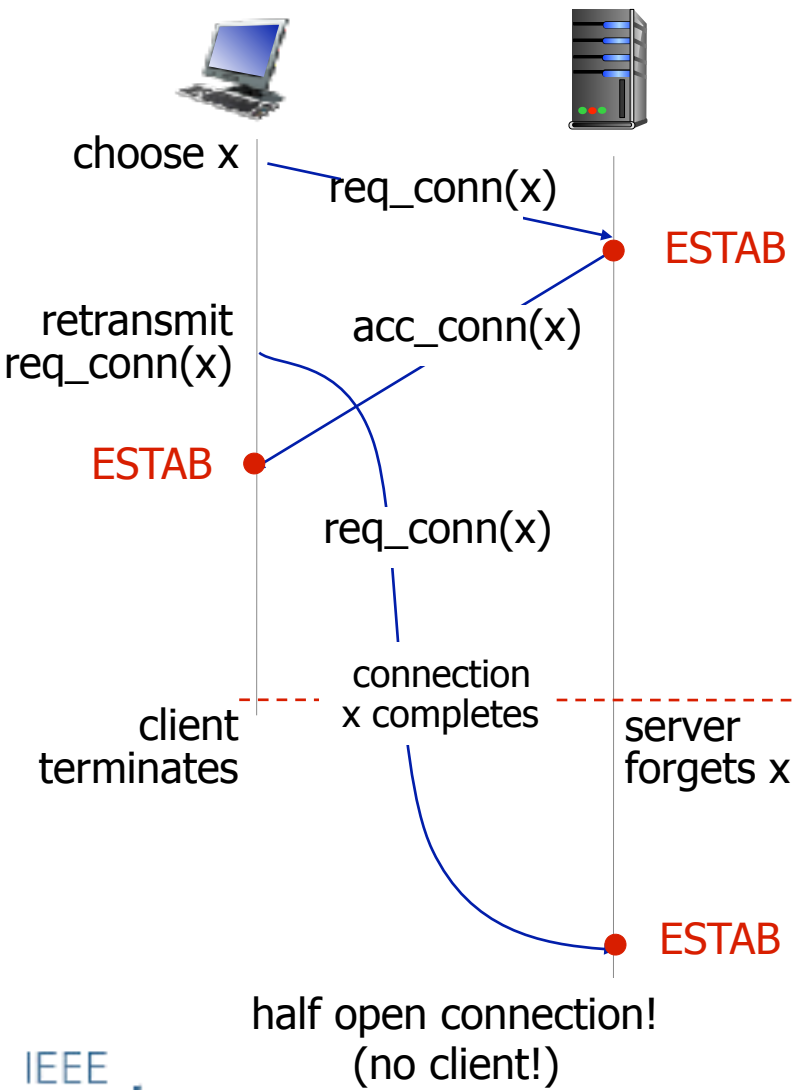
Q: will 2-way handshake always work in network?

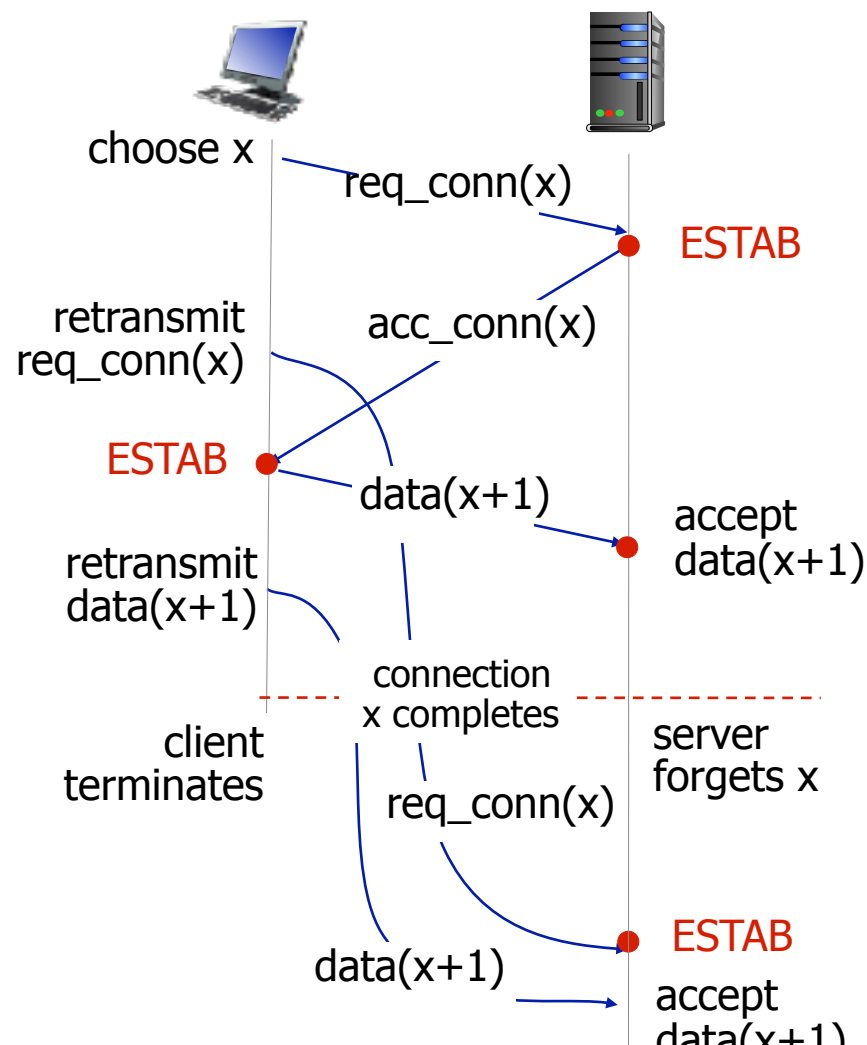
- variable delays
- retransmitted messages (e.g. req_conn(x)) due to message loss
- message reordering
- can't "see" other side

Basis of TCP Handshake

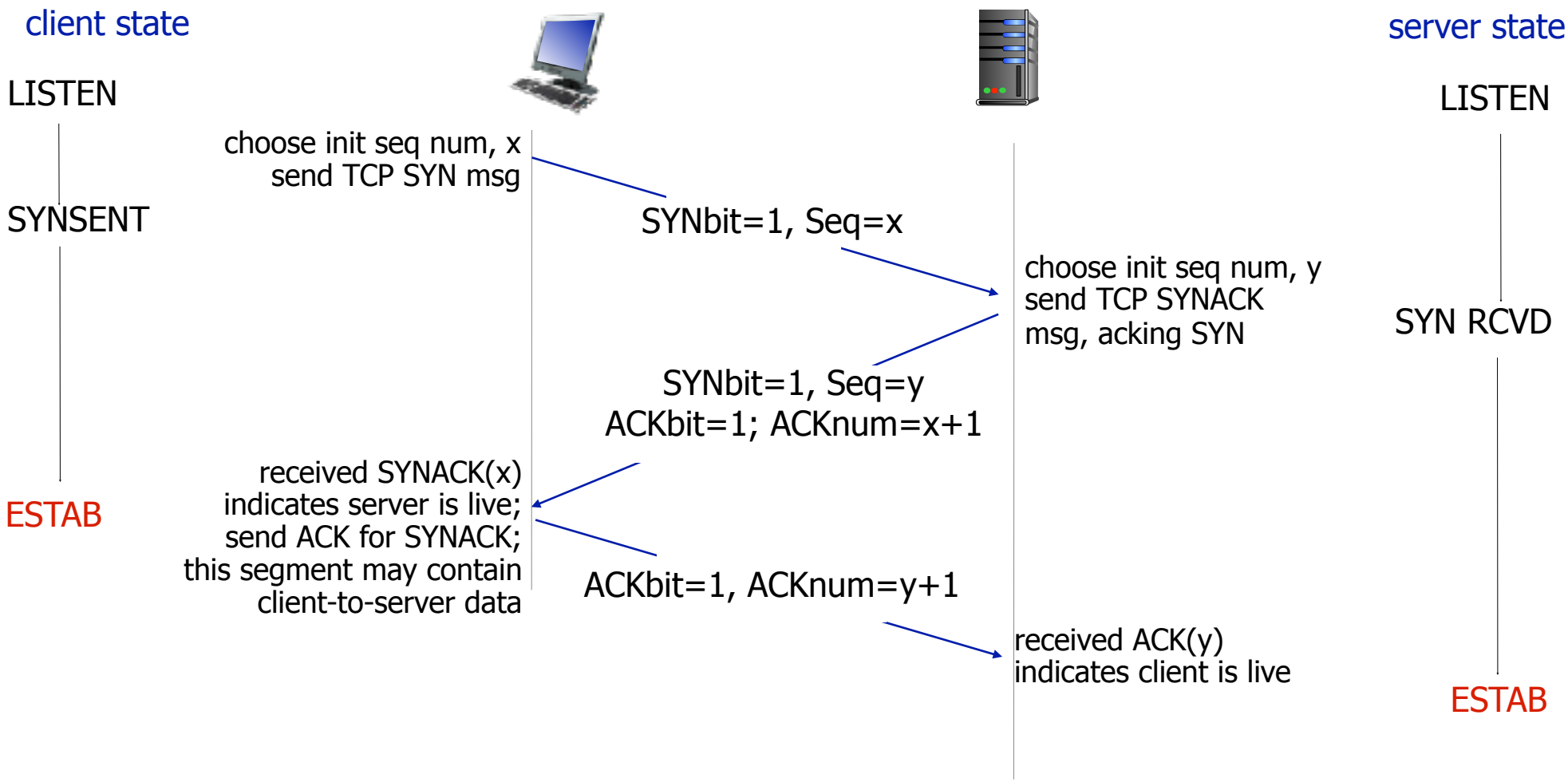
Source: Kurose, Ross: Computer Networking, A Top Down Approach

2-way handshake failure scenarios:



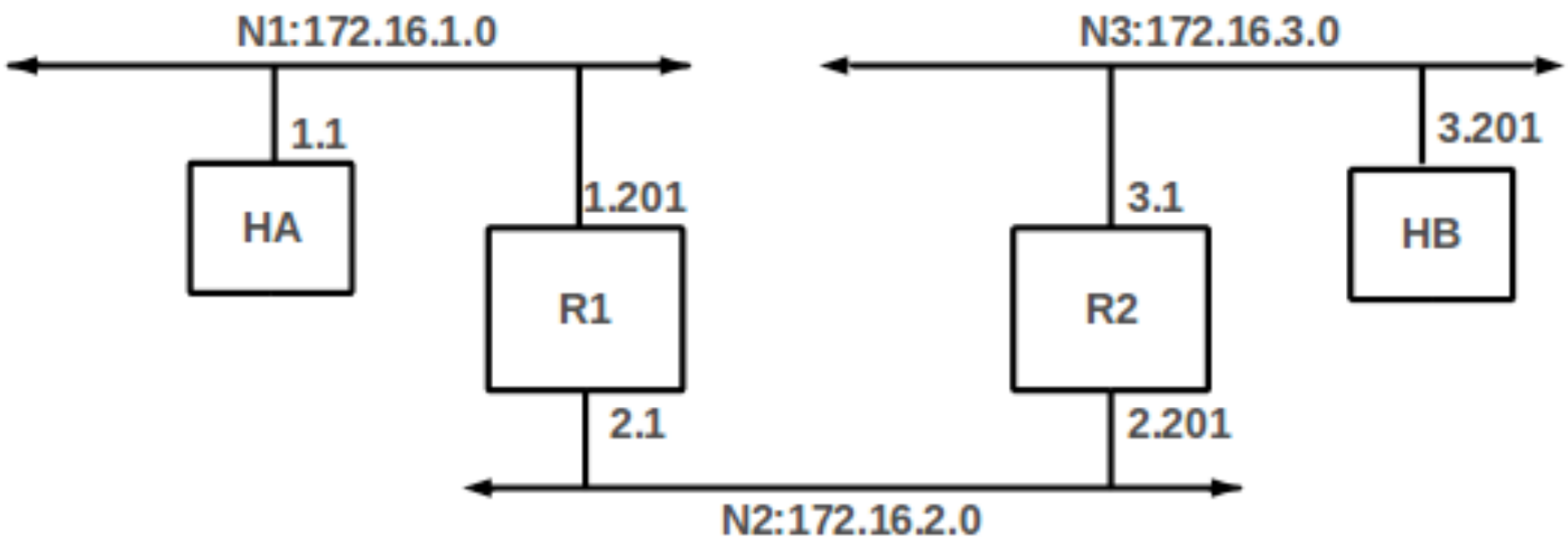


TCP 3-Way Handshake

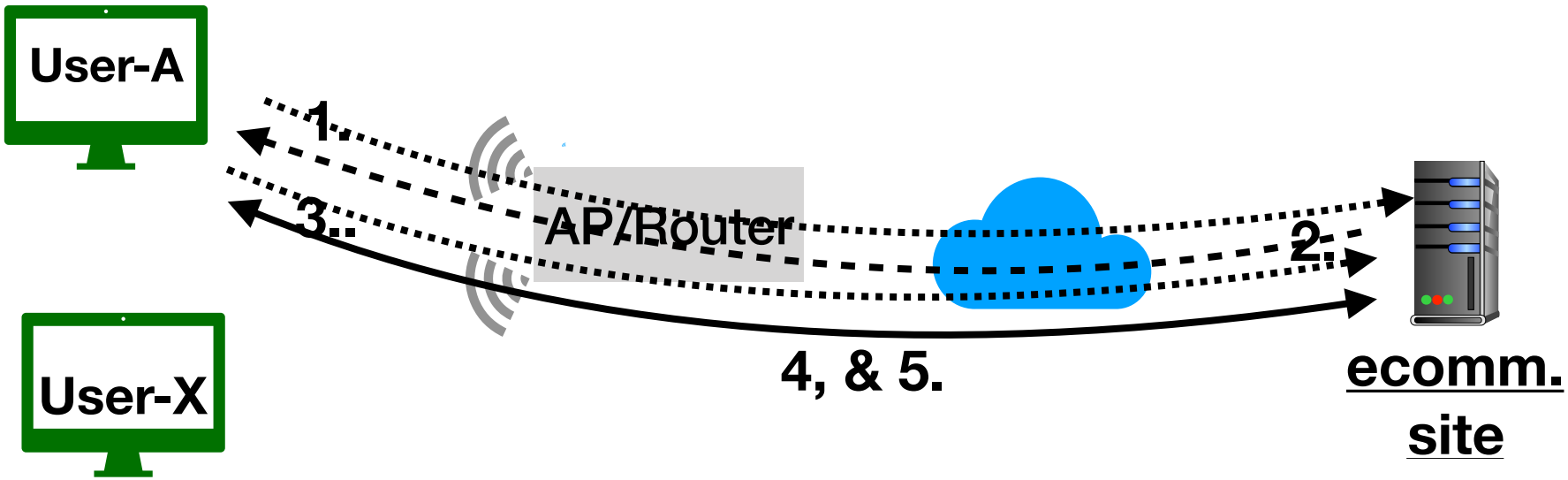


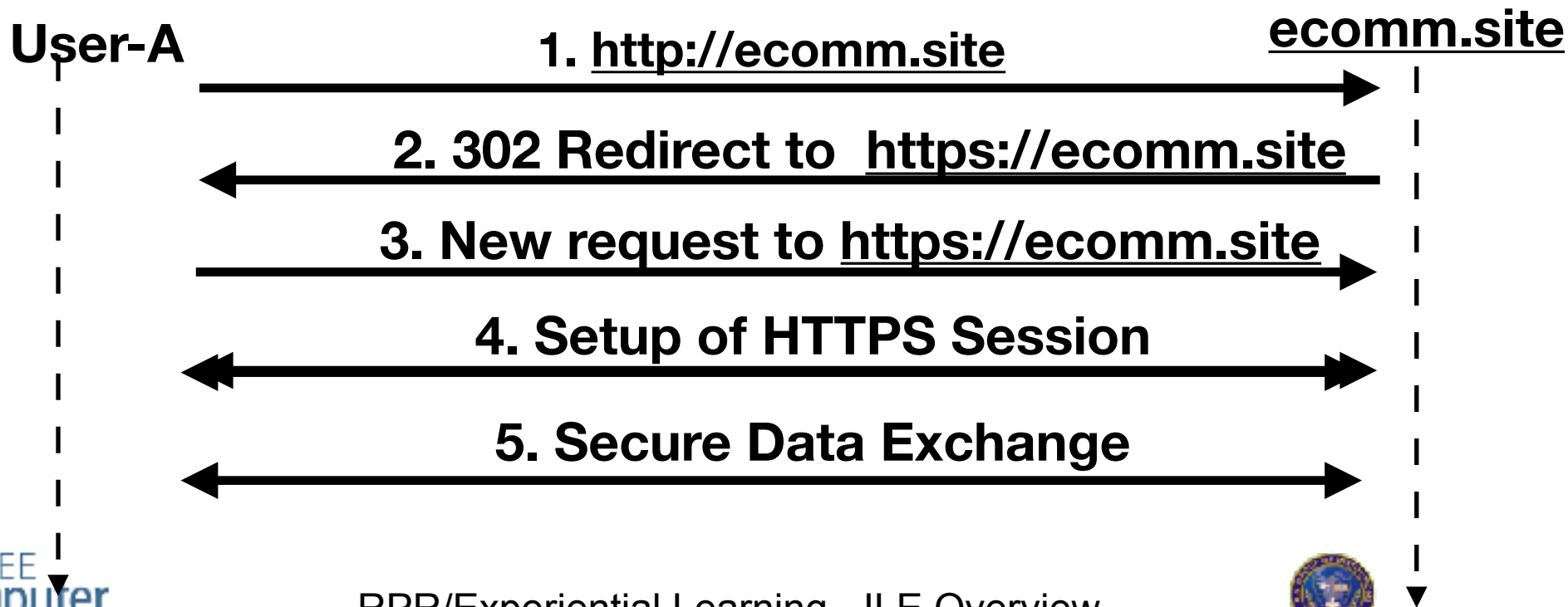
Source: Kurose, Ross: Computer Networking, A Top Down Approach

Hands-On IPv4 Routing

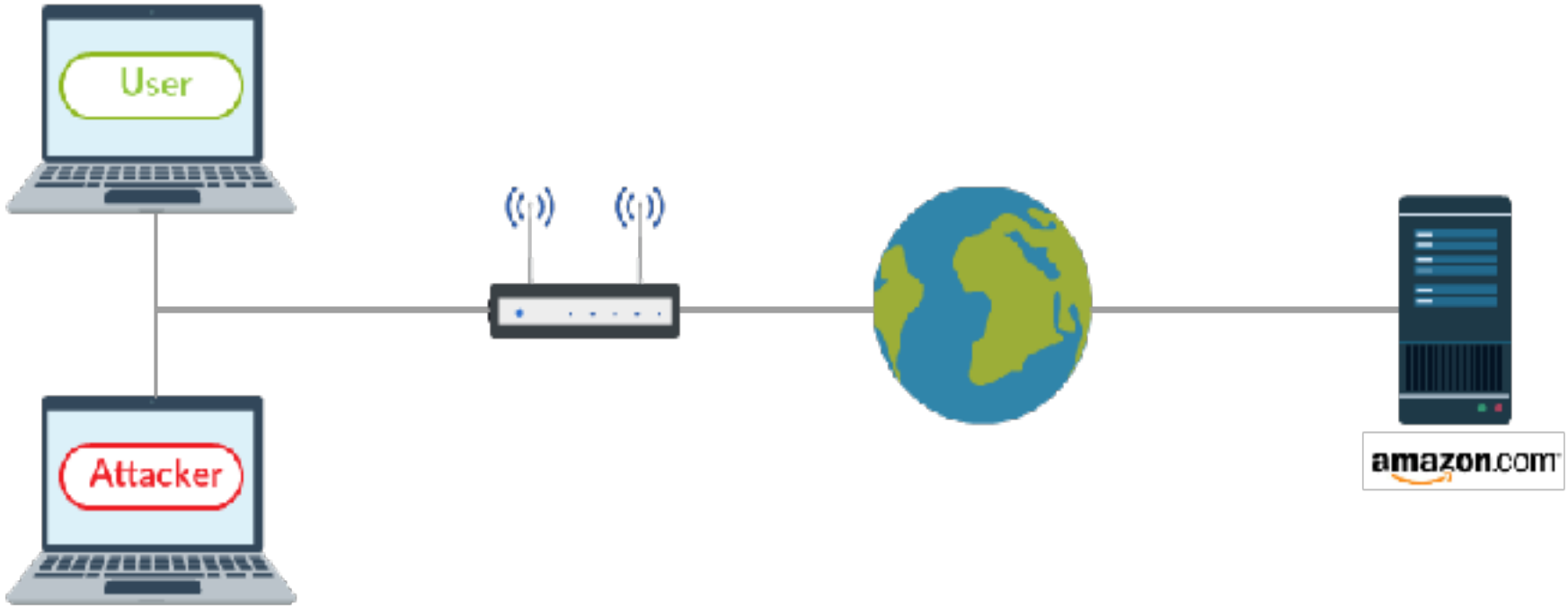


Typical E-commerce Traffic Setup



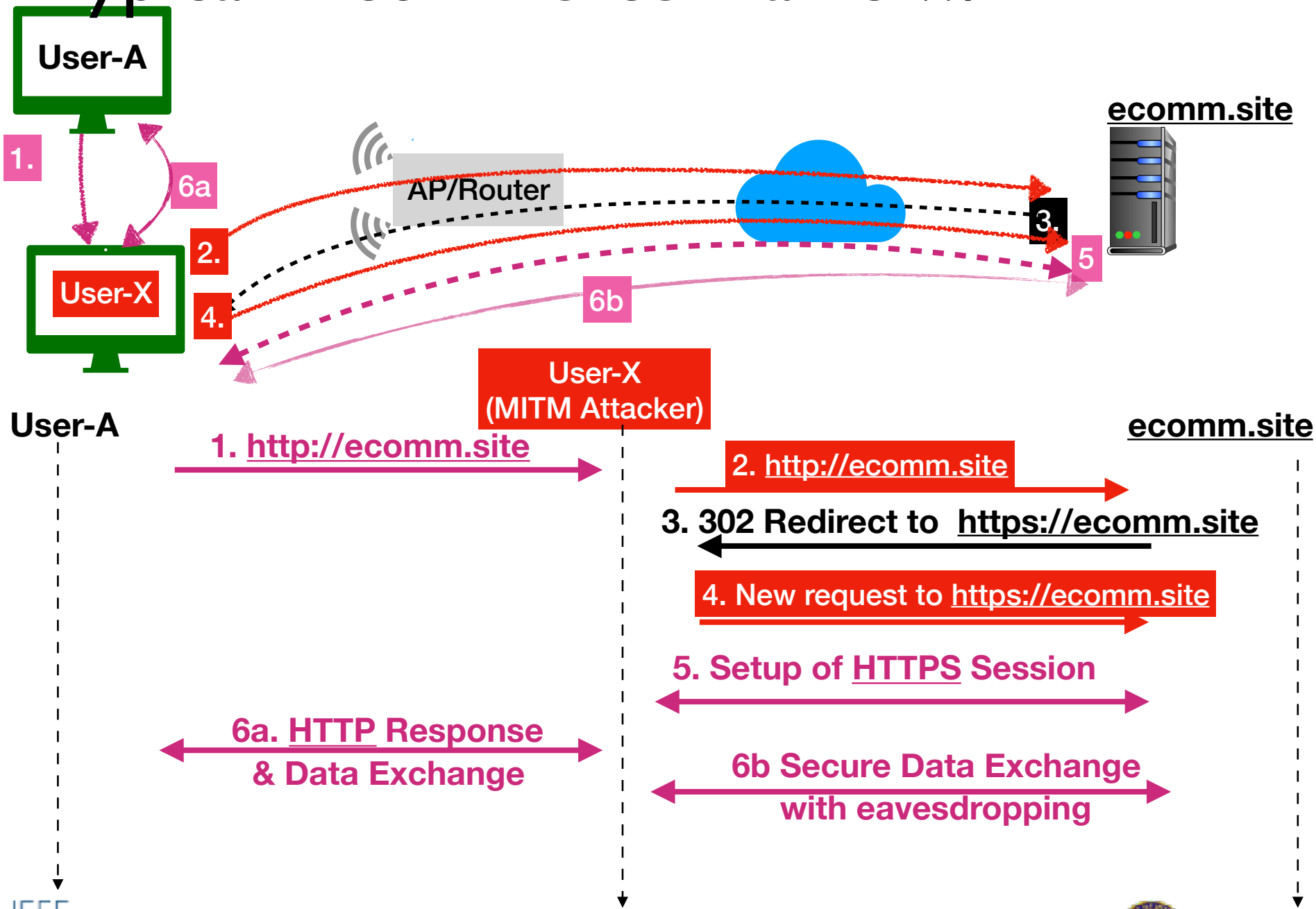


Typical E-commerce Traffic with MITM



- Typical Usage: User enters ecomm.site
- MITM attacker hijacks the URLs and changes n/w settings
- All the back and forth traffic goes via attackr.
- Gets the web page displayed
- Proceeds with transaction

Typical E-commerce Traffic w/ MITM



The Web Today

- Total num of hostnames and active sites (June 2018)
  - src: **http://news.netcraft.com/archives/category/web-server-survey/**
  - Number of sitenames and active sites
    - Sitenames: 1.6+B, Active sites: 177+M
  - Web server vendors
    - June 2018: Apache: 25% , MS IIS : 32%, Nginx: 23%
  - Web Clients: GUI browsers, text browsers
- Communication protocols
  - HTTP, HTTPS
  - Extension of HTTP: WebDAV, CarDAV, CalDAV…

Analogy - Travel to a new place

- Life in getting to new place (e.g. tourism)
  - Identify the tourist location address
    - What is internet similarity?
  - Take a cab to go to airport
    - What is corresponding equivalent in network?
  - Take the appropriate flight
    - Similarity in internet?
    - May need to go over multiple hops
  - Take local transport from last hop
    - Similarity in network?
- Is return path same?

Analogy - Travel to a new place

- Unforeseen challenges
  - Cab break down
  - Traffic jam
  - Airport strike
  - Smaller airplane than initially planned
    - Family members split?
  - Get into the wrong airplane
  - Destination closed

Packet in Internet

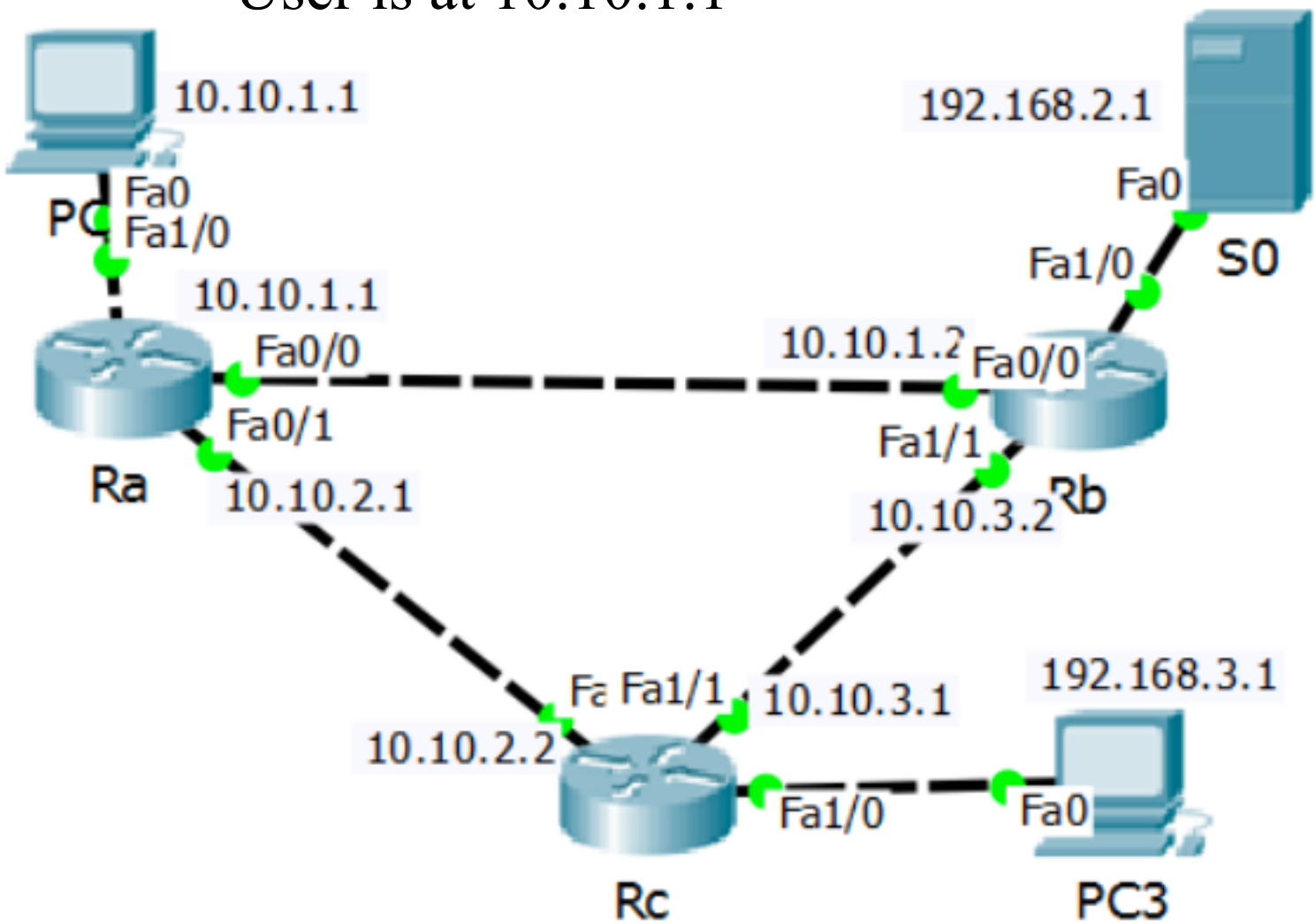
- Case 1:
  - Consider the following daily life example
- PC is powered up
  - (Assuming no network activity is launched in background)
  - Web Browser is opened
  - user types the URL www.google.com
- What happens
  - which is the first packet that goes out

Packet in Internet : Web Access

- Case 1 Steps
  - ARP exchange
  - DNS exchange
  - Web Exchange
  - HTTP Redirect, embedded URLs
    - DNS Again
- Other related steps whenever applicable
  - NAT
    - DNAT/SNAT
  - Proxies, Firewalls
  - HTTPS

Exercise Case 1: N/W diagram

DNS Server: 192.168.3.1
DNS Entry: www.ieee.org = 192.168.2.1
User is at 10.10.1.1



Exercise Case 1 :Worksheet

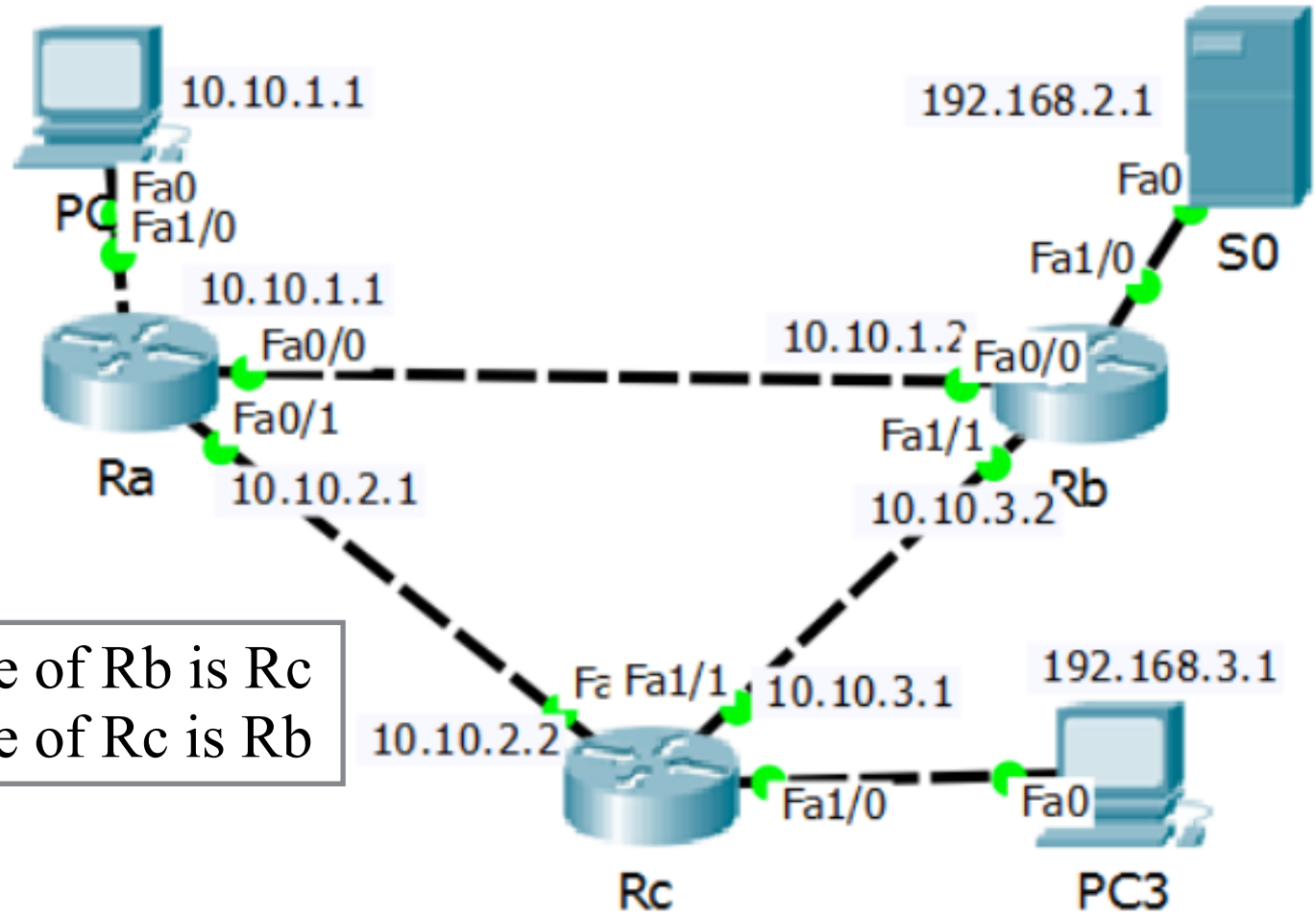
S.No	N/W Link	Src MAC	Dst MAC	Src/ Sender IP	Dest/ Receiver IP	Protocol Type
1	A->Ra	M_A				ARP Request
:						

Every Day Case Study…

- Variations in setup
- Variation 1: DNS not configured or down
- Variation 2: Default GW not configured/down
- Variation 3: Using DHCP
- Variation 4: Browser configured with proxy
- Variation 5: Other configurations
  - HTTPS URL accessed with IP Address
  - NAT, MTU changes/fragmentation, ACLs
  - Router subnet is different than yours
    - Hacker acting as MITM for router
  - (Google) Server is too busy, (or not running)
    - Server failover happens

Packet In Internet: TTL

- Case 2:
  - How do you prevent packet looping for ever



Default Route of Rb is Rc
Default Route of Rc is Rb

Packet in Internet: TTL/Traceroute

- Case 3:
  - Traceroute on Microsoft Windows
  - Traceroute on Linux

Packet in Internet: Server Application stopped

- Case 4:
  - TCP based server application
  - UDP based server application

Packet in Internet: PMTU Discovery

- Case 5:
  - What happens when one link in the path has smaller MTU
  - analogy:
    - got a smaller plane and all member of groups can't travel together

Packet in Internet: IP Fragmentation

- Case 6:
  - What happens when one link in the path has smaller MTU and Don't fragment bit is set
  - Analogy:
    - plane is smaller and group needs to travel together

Thank You