Networking and Internet Services(Sockets and Ports)

Presented by
Masoud Bozorgi

Champlain
COLLEGE SAINT-LAMBERT

What is an endpoint?

- An endpoint refers to a process that communicates with the network to which it's connected.
- These are considered "endpoints" because they sit at the ends of communication paths, compared to networking hardware like routers and switches that relay or route the communications.
- An "endpoint" can refer to any interface at which two systems interact. This could be the endpoint for a data stream, an interface on a piece of software, or the terminal point for a communication protocol.

What is a Port?

- A port refers to an endpoint of communication in an operating system. Ports are unique numbers that serve to distinguish communication channels within the Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) services of the Internet Protocol Suite.

- **Port Numbering**: **The Transport layer introduces the concept of "ports" to enable multiple services or processes on a single device to be uniquely addressed**. For example, an HTTP server typically listens on port 80, while an HTTPS server listens on port 443.

- In TCP and UDP communications, port numbers are represented as 16-bit unsigned integers. This means they can have values ranging from 0 to 2^{16}. Port number 0 is reserved and cannot be used, so we have 65535 ports.

Well-known Ports

In computer networking, well-known ports refer to port numbers that are designated and reserved for specific applications or protocols by the Internet Assigned Numbers Authority (IANA). These well-known ports range from 0 to 1023. While there are many well-known ports, here are some of the most commonly recognized and utilized:

```
1023 -> 0000 0011  1111 1111
```

Well-known Ports

FTP:

- Port 20: Data transfer
- Port 21: Command control

SMTP (Simple Mail Transfer Protocol):

Port 25: Used to send emails

DNS (Domain Name System):

Port 53: Resolves domain names to IP addresses

DHCP (Dynamic Host Configuration Protocol):

Port 67 (UDP): DHCP server

Port 68 (UDP): DHCP client

POP3 (Post Office Protocol, Version 3):

Port 110: Used by email clients to retrieve emails

HTTP (Hypertext Transfer Protocol):

Port 80: Standard port for web browsers and web traffic

NTP (Network Time Protocol):

Port 123: Synchronize computer clocks

HTTPS (HTTP Secure):

Port 443: Secure web traffic using SSL/TLS

LDAP (Lightweight Directory Access Protocol):

Port 389: Directory services

LDAPS (Secure LDAP):

Port 636: Secure directory services

Tip

- When you need to serve a web page for personal reasons (let's say you wanted to put a Linux server temporarily on the web to log in remotely), you should use non-standard ports.
- Instead of port 22, put it on 22222 instead, for example.
- Why? Usually, hackers scan your public COMMON ports, like 22.
- If they get an answer, they can identify active processes in the server and the protocol they use. For example, a response from port 20 means the FTP process is up and running, so they can plan an attack based on FTP.

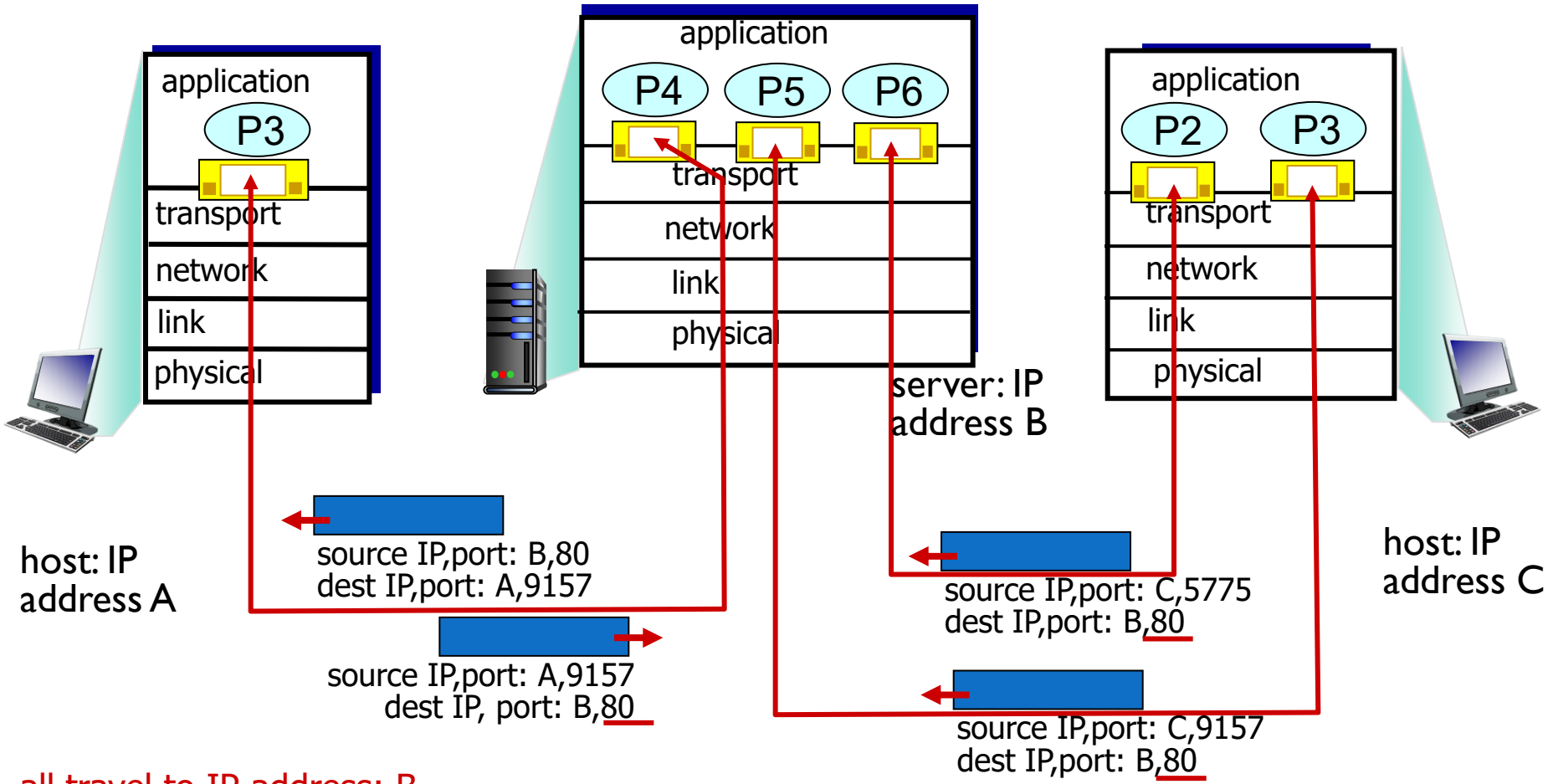
The most common protocols used at the Transport layer in the TCP/IP model

- **TCP** (**Transmission Control Protocol**): Connection-oriented, reliable, and ensures that data packets are delivered in order. It's used for applications where data delivery and order are critical, such as web browsing and file transfer.

- **UDP** (**User Datagram Protocol**): Connectionless and does not guarantee delivery or order of data packets. It's faster and has lower overhead than TCP, making it suitable for applications like streaming media or online gaming where occasional data loss can be tolerated.

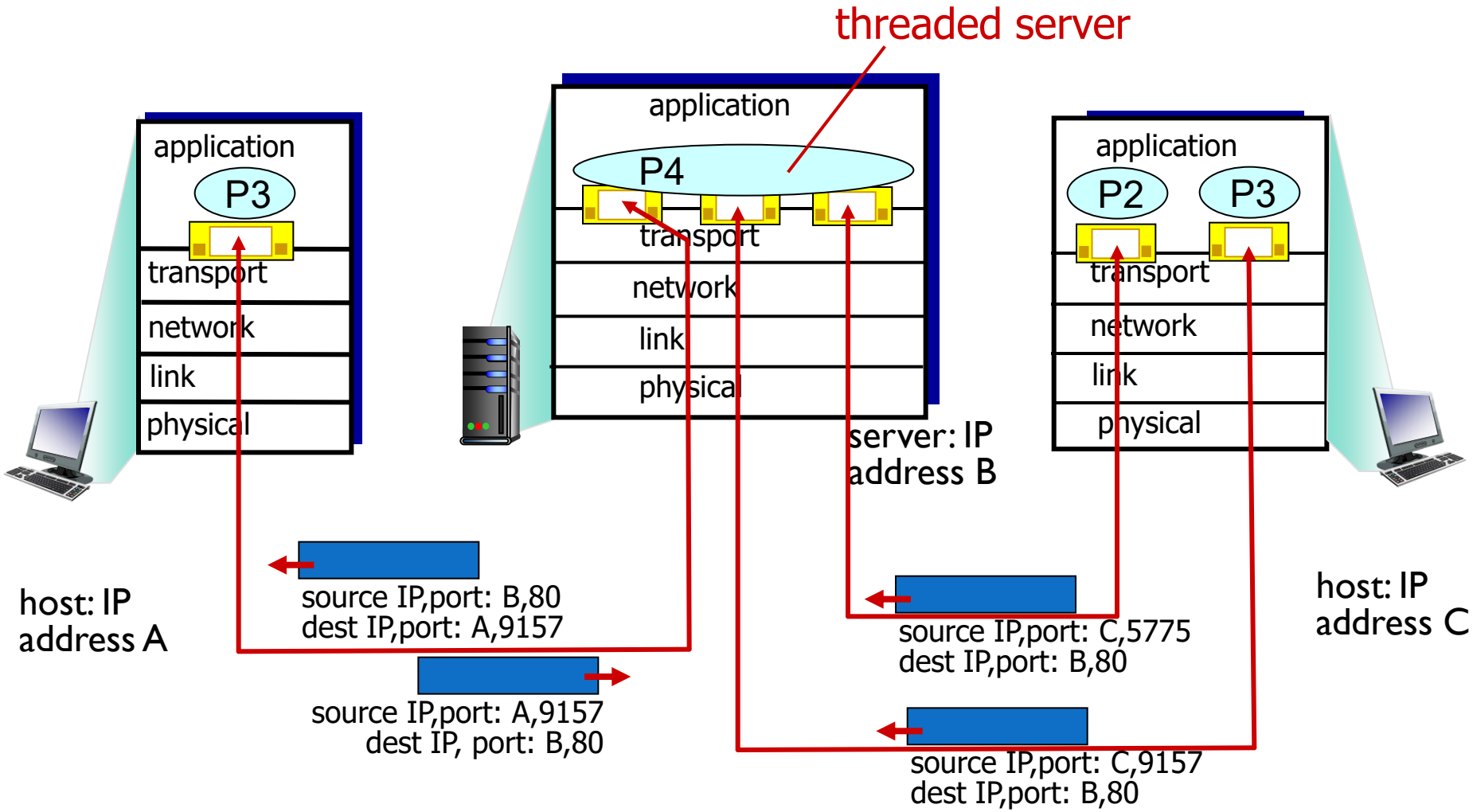
Connection-oriented demux: example

Each TCP is idetified by a 4-tuple: [Source IP, Source Port, Destination IP, Destination Port]

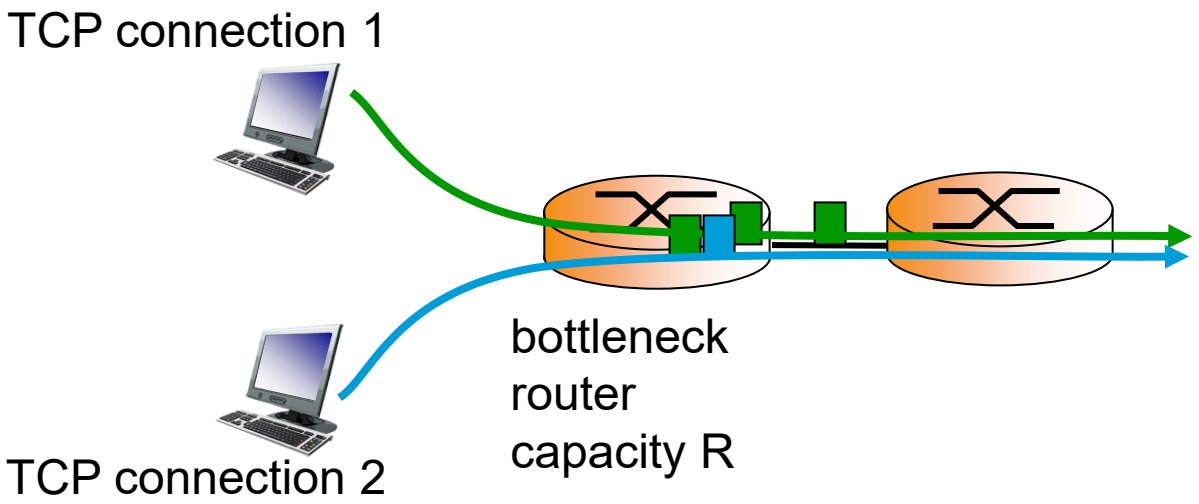


three segments, all travel to IP address: B,
dest port: 80 are demultiplexed to *different* sockets

Connection-oriented demux: example



TCP


TCP connection 1
TCP connection 2
bottleneck
router
capacity R

What is a Socket

- A socket is a software endpoint that establishes bidirectional communication between a server program and one or more client programs. Sockets provide a mechanism for the server and client to send and receive data to and from each other. They serve as the interface for communication in networks, especially in the context of the Internet.

- Here are the key components and concepts associated with sockets:

What is a Socket

- **IP Address**: An IP address represents the location of a device on a network. It can be an IPv4 address (e.g., 192.168.1.1) or an IPv6 address.
- **Port Number**: A port number identifies a specific process or service on a device. It allows multiple services to run on a single device and have their own communication channels. Port numbers range from 0 to 65535.
- **Combination of IP Address and Port**: A socket is defined by the combination of an IP address and a port number. For example, 192.168.1.1:80 would denote port 80 on the device with IP address 192.168.1.1.
- **Protocol**: Most commonly, when we talk about sockets, we're referring to TCP (Transmission Control Protocol) or UDP (User Datagram Protocol) as the underlying transport protocol. TCP is connection-oriented and ensures reliable data transfer, while UDP is connectionless and does not guarantee delivery.

What is a Socket

- **Socket States**: In the context of TCP, sockets can be in various states, such as LISTEN (waiting for a connection), ESTABLISHED (successfully connected), or CLOSED.

- **Socket Programming**: This is a method of creating networked applications. A developer can use APIs provided by the operating system to create, bind, connect, and listen to sockets, enabling applications to communicate over a network.

What is a Socket

Types of Sockets:

- **Stream Sockets**: Use TCP as the transport protocol. They are reliable, connection-oriented, and ensure the data is delivered in the correct order.
- **Datagram Sockets**: Use UDP as the transport protocol. They are connectionless and do not guarantee reliable delivery or order.

What is a Socket

- **Socket Pair**: Every network communication via sockets involves a pair of sockets: one on the client and one on the server side. For instance, when you access a website, your browser creates a socket that connects to a socket on the web server.

In essence, sockets are crucial for network communications, providing a standardized way for applications to exchange data over a network. They abstract much of the complexity of network communications, allowing developers to focus on the logic of their applications.

Connected process

- If a connection is established, usually there is a process that's behind the scene doing the connection.

```
netstat -ano
```

  - Shows the processes in question.
  - Using the task manager we can find the process we obtained from `netstat -ano`

- The `netstat` command is a command-line utility that provides information about network connections, routing tables, interface statistics, masquerade connections, etc. When used on various operating systems, it helps users understand the state of their network connections and services.
- When using the `–ano` flags with `netstat`, here's what they mean:
- - `-a`: This flag displays all active network connections and listening ports.
- - `-n`: This flag shows addresses and port numbers in numerical form, rather than resolving hostnames (which can slow down the output if DNS resolution takes time).
- - `-o`: On platforms that support it (like Windows), this flag displays the associated process identifier (PID) for each connection. This is particularly useful if you want to identify which process or application is responsible for a particular network connection.
- Putting it all together, `netstat –ano` will display all active network connections and listening ports in numerical form, along with the associated process IDs.
- On Windows, for example, if you notice a suspicious or unknown connection, you can use the PID provided by `netstat –ano` to investigate further in Task Manager or another system tool to determine which application or process is creating that connection.

Champlain

COLLEGE SAINT-LAMBERT