FIT5191: Network Protocols

2019 update
Teaching material for this unit is based on the following sources:

- Related standards
- J. F. Kurose, K. W. Ross: Computer Networking. A Top-down approach, 7th ed., 2017, Pearson
- J. FitzGerald, A. Dennis, A. Durcikova : Business Data Communications and Networking, 12th ed., 2014, John Wiley & Sons
- B. Forouzan: TCP/IP Protocol Suite, 4th ed., 2009, McGraw-Hill
- Internet resources, e.g. Wikipedia

Lecture 1: Overview of the Internet Structures and Protocols

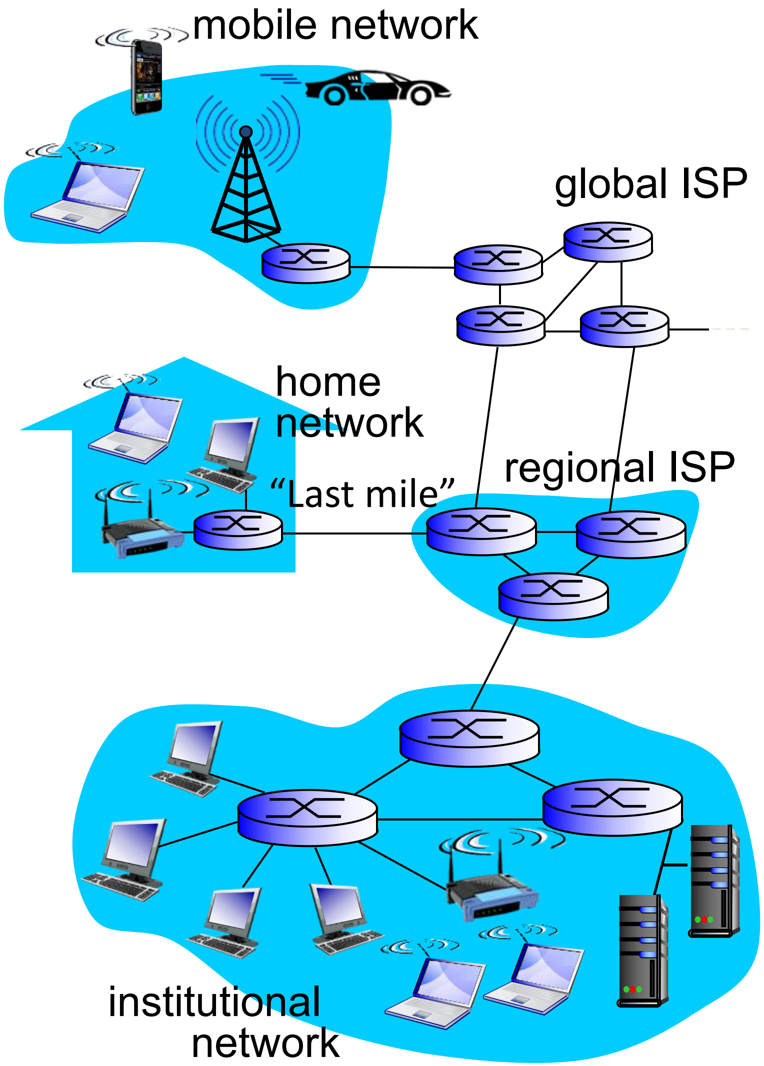
Acknowledgement: Slides for this lecture are based on materials from:

- *Computer Networking: A Top Down Approach,* J. Kurose, K. Ross, 7th ed., 2017, Addison-Wesley, Chapter 1
- *Business Data Communications and Networking,* J. Fitzgerald, A. Dennis, 12th ed., 2014, John Wiley & Sons, Chapter 1
- Internet resources

Lecture 1: Contents

- The structure of the Internet
- Internet protocol suite aka TCP/IP model
- Moving messages through the Internet model layers
- Short descriptions of the protocols from the Internet protocol suite

The Internet: Network of Autonomous Systems



- The Internet is a network of interconnected **autonomous** computer networks that use the standard **Internet Protocol Suite – TCP/IP**
- Typical examples of the autonomous networks include
  - Home networks
  - Company networks
  - Mobile networks
- Hierarchical **Internet Service Providers** (ISPs) span the autonomous networks with **routing computers (routers)**

The Services Distributed over the Internet

- The most fundamental **services distributed over the Internet** are:
  - World Wide Web – Interconnection of **Web servers**
  - Email – distributed by **mail servers**
  - Instant message networks, e.g. Skype
  - Movies/videos – content delivery networks
  - IoT, the Internet of Things, what about?

- The Internet is to be distinguished from the **Wide Area Networks** that provide networking for companies

Internet protocols

- The internet communication layers are described in **RFC 1122** (Request For Comments) and related documents published by the **Internet Engineering Task Force**
- The internet protocols described in the Requests for Comments (RFCs) form the **Internet protocol suite** aka **TCP/IP model**
- All computer connected to the Internet must use the Internet protocol standards as described in RFCs
- In RFC 1122 two basic definitions are (quote):
  - A **host computer**, or simply **"host,"** is the ultimate consumer of communication services.
  - The networks are interconnected using **packet-switching** computers called **"gateways" or "IP routers"**

Three Addressing Systems: appl, IP

Sending packets through the Internet is based on **three addressing systems**:

1. The **application layer addresses,**
   - e.g. www.baidu.com typically used by web browsers to communicate with the web servers
   - e.g. app@monash.edu used by mail servers
2. The **IP addresses**, e.g.

   IPv4: from 130.194.11.149 (src) **to** 103.235.46.39 (dst)

   IPv6: from 2001:388:608c:2c52:d04d:a361:4d1c:c8ac (src)

   to 2001:388:608c:2c52:d04d:a361:1d1d:181c (dst)

   Used to identify the **sender/source** and the **final destination** of a packet in the **multi-hop** structure of the internet

Three Addressing Systems: MAC

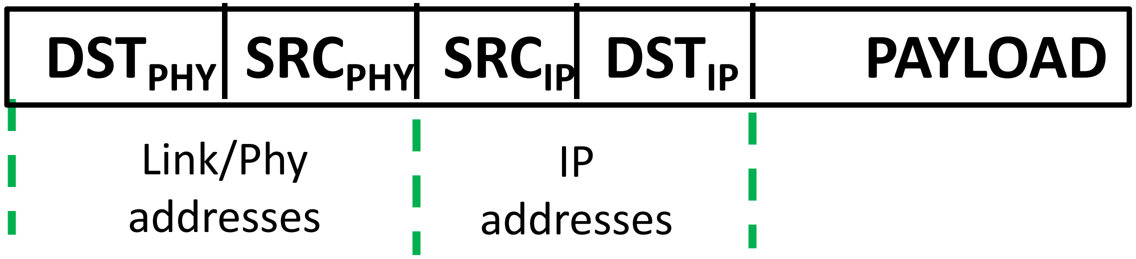
3. **The Link/MAC/Physical (PHY) addresses**

   e.g. **from:** D0-67-E5-3D-05-97 **to:** D0-67-E5-3D-1A-BA

   used to send the packet between **two logically adjacent computers**, e.g.

   - a host in a LAN/subnet and its gateway/router
   - routers forming the **single hop**.

A typical addressing part of the Internet packet might look like:



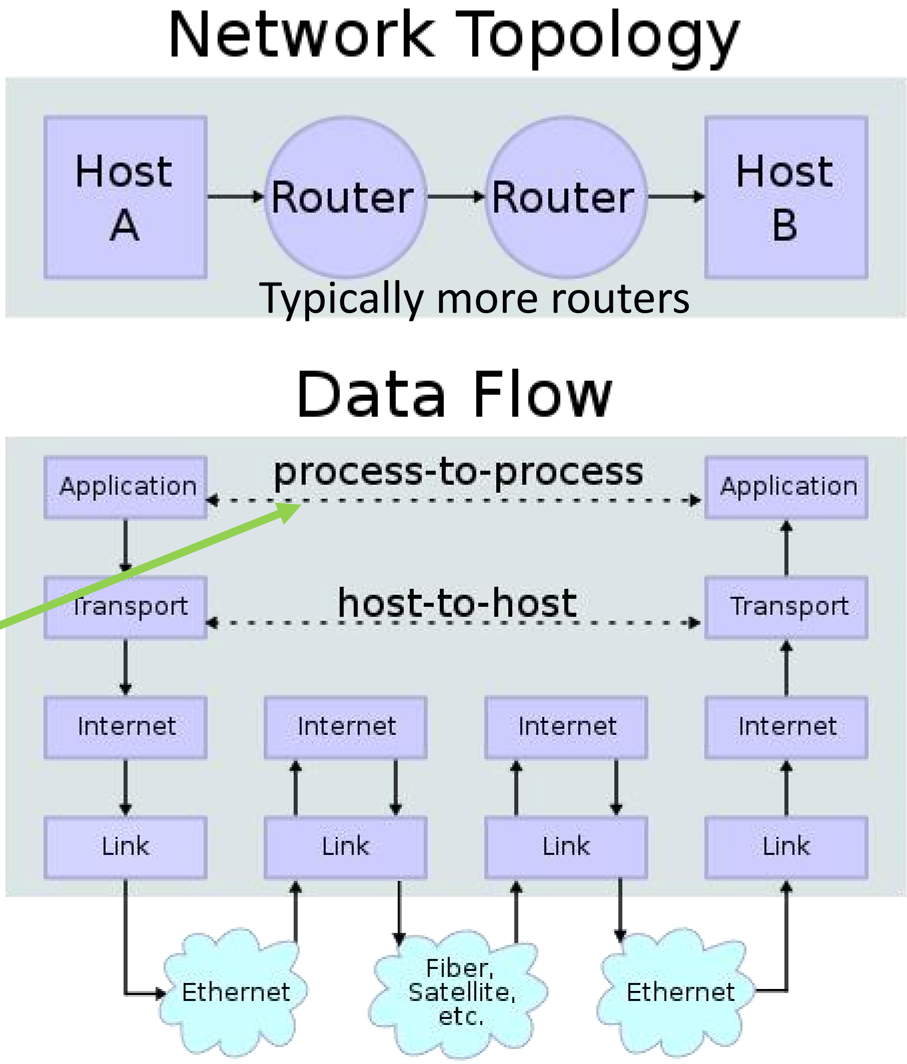
DST_{PHY} SRC_{PHY} SRC_{IP} DST_{IP} PAYLOAD

Link/Phy addresses

IP addresses

Moving messages through layers (**Application**)

- Two Internet **host computers** communicate across local network boundaries constituted by their internetworking (or border) routers.
- The **application** on each host executes read and write operations as if the **processes** were directly connected to each other by a data pipe.
- Detail of the communication is hidden from each application process.



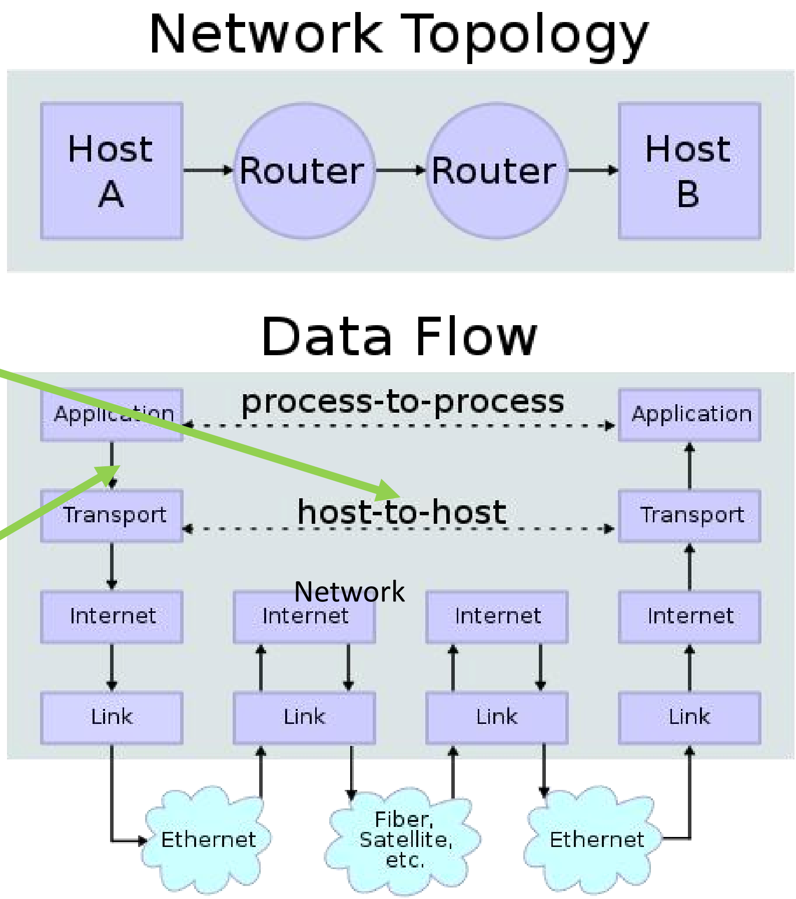
From Wikipedia

Moving messages through layers (**Transport**)

The Transport Layer establishes **host-to-host** connectivity, and handles:

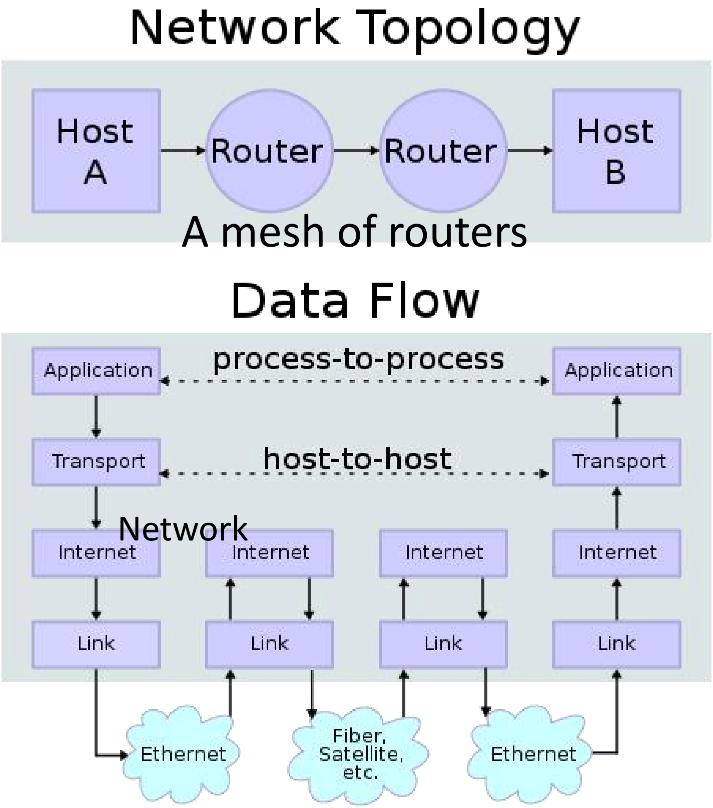
- the details of data transmission that are independent of the structure of user data (e.g. photo, text, …)
- the logistics of exchanging information for any particular specific purpose.

The Transport layer communicate with an application software using **ports** (part of the sockets)



Moving messages through layers (**Network**)

- The Internet (or Network) Layer provides an unreliable **packet** or datagram transmission facility between hosts located on potentially different IP networks
- It forwards the Transport Layer **segments** to an appropriate **next-hop** router for further relaying to its destination
- Note that the **Routers** do not need the Transport and Application layers.
- A router checks the destination **IP address** to decide where to send the packet.



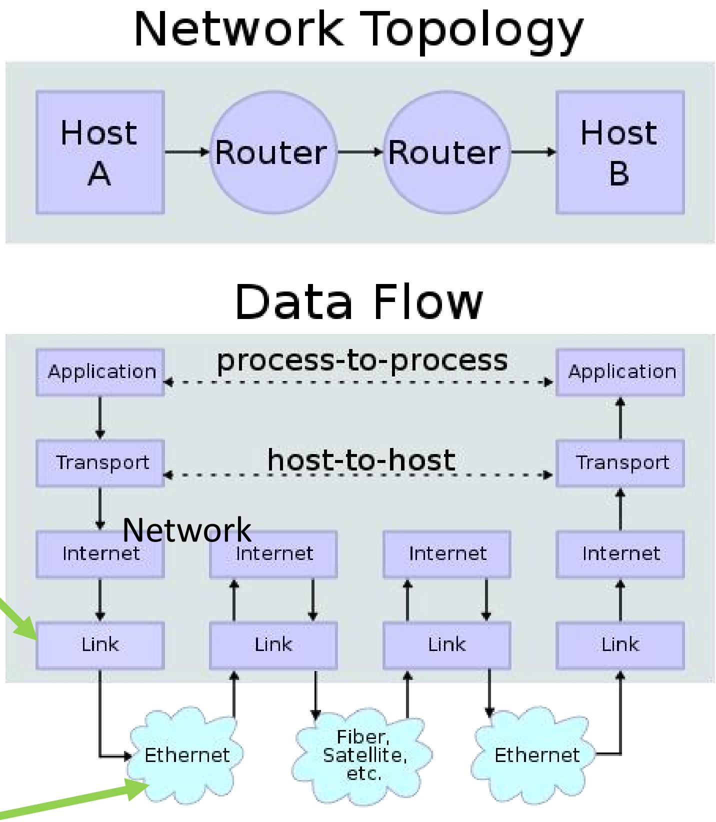
Moving messages through layers (**Link**)

- The lowest layer in the Internet Protocol Suite is the **Link Layer**.
- The link layer describes the functions of the local link, i.e. the network segment connecting two neighbouring hosts or routers.

This involves interacting with

- the hardware-specific functions of network interfaces and
- specific transmission technologies, e.g., 802.3 Ethernet, 802.11 WLAN, …

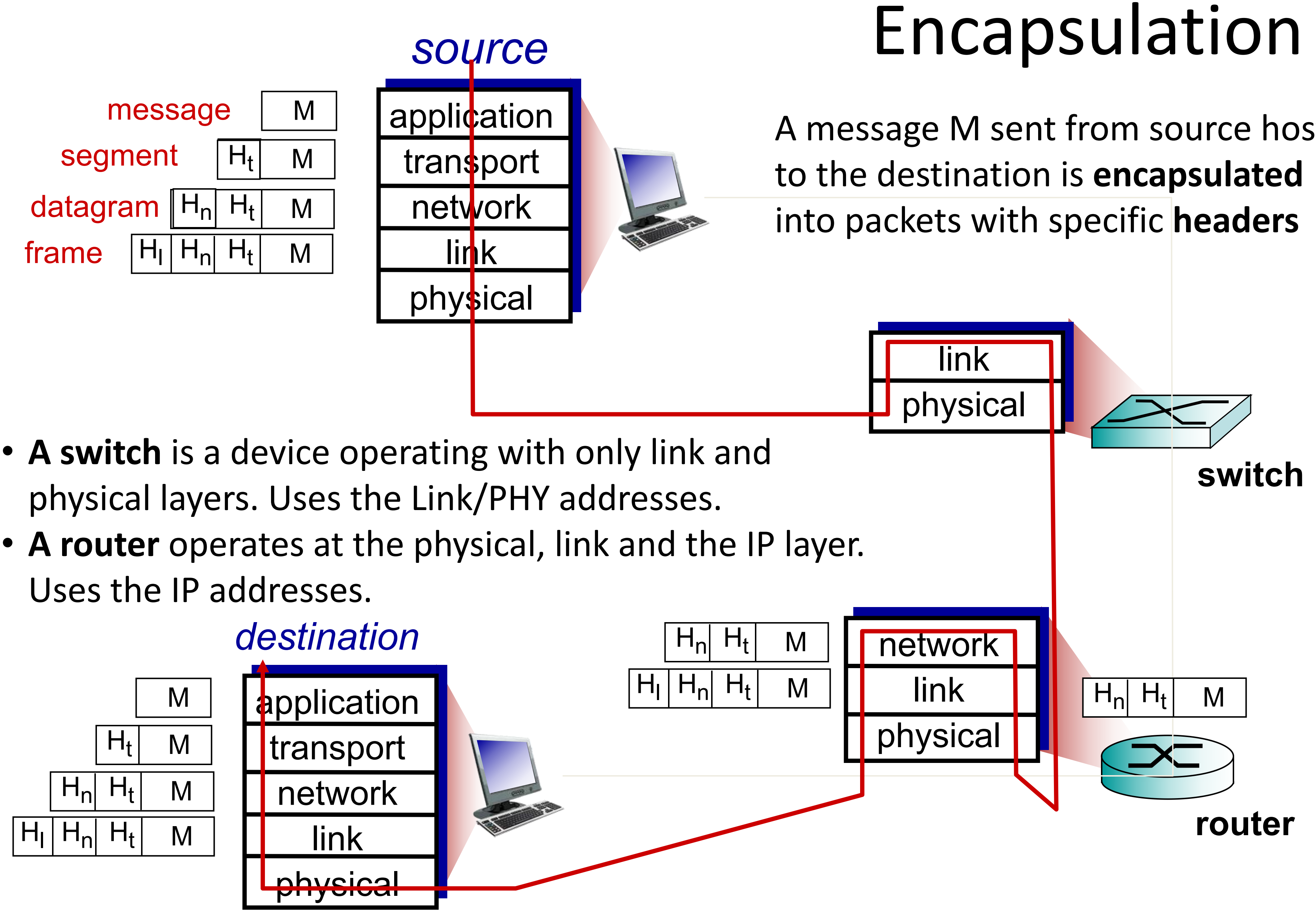
The “new” Link/Phy destination address is required between all link segments of the network



Encapsulation

A message M sent from source host to the destination is **encapsulated** into packets with specific **headers**

- **A switch** is a device operating with only link and physical layers. Uses the Link/PHY addresses.
- **A router** operates at the physical, link and the IP layer. Uses the IP addresses.



Wait!

Layer 2: Link Layer Protocols

Ethernet standardized by **IEEE 802.3**

- is a family of computer networking technologies for **local area networks** (LANs) and metropolitan area networks (MANs).
- It is a prime **data link layer protocol** that over time has replaced all competing wired LAN technologies.

ARP – **Address Resolution Protocol** defined by RFC 826 , 5494

- is a protocol used for resolution of **network layer** (IP) addresses into **link layer** addresses, a critical function in multiple-access networks.

NDP – The **Neighbor Discovery Protocol** defined by RFC 4861

- is the ARP replacement for IPv6.
- IPv6 nodes on the same link use NDP to discover each other's presence, to determine each other's link-layer addresses, to find routers, and to maintain reachability information about the paths to active neighbours.

Layer 2: Link Layer Protocols (cont.)

OSPF – **Open Shortest Path First** RFC 2328 (IPv4), RFC 5340 (IPv6)

- is a routing protocol for IP networks.
- It uses a **link state routing algorithm** and falls into the group of **interior** routing protocols, operating within a **single autonomous system** (AS).

PPP RFC 1661– **Point-to-Point Protocol**

- is **a link protocol** used to establish a direct connection between two nodes.
- It can provide connection **authentication**, transmission **encryption** and **compression.**
- RFC 2516 describes **Point-to-Point Protocol over Ethernet** (PPPoE) as a method for transmitting PPP frames over Ethernet that is often used by ISPs with **DSL** (Digital Subscriber Line) and **FTTP** (Fibre To The Premisses) connections.

Layer 2: Link Layer Protocols: L2TP

L2TP – **Layer 2 Tunnelling Protocol** RFC 3931 (v3)

- is a tunnelling protocol used to support **virtual private networks** (VPNs) or as part of the delivery of services by ISPs.
- The entire L2TP packet, including **payload and L2TP header**, is sent within a User Datagram Protocol (UDP) datagram.
- It is common to carry PPP sessions within an L2TP tunnel.
- L2TP does not provide confidentiality or strong authentication by itself.
- **IPsec** is often used to secure L2TP packets by providing confidentiality, authentication and integrity.
- The combination of these two protocols is generally known as L2TP/IPsec

Layer 3: Internet/Network Layer Protocols

IP – The **Internet Protocol** RFC 791 (IPv4), RFC8200 (IPv6)

- is the principal communications protocol in the Internet protocol suite for relaying datagrams/packets across network boundaries.

ICMP, **ICMPv6** – **The Internet Control Message Protocol**

- defined in RFC 792.
- ICMP messages are typically used for **diagnostic** or **control** purposes or are generated in response to **errors** in IP operations.
- ICMP errors are directed to the source IP address of the originating packet.

Layer 3. cont.

IPsec – Internet Protocol Security (IPsec)

- is a protocol suite for **securing** Internet Protocol (IP) communications by **authenticating** and **encrypting** each IP packet of a communication session.
- IPsec includes protocols for establishing **mutual authentication** RFC 4302 between agents at the beginning of the session and negotiation of **cryptographic keys** to be used during the session RFC 8221.

MPLS – Multi-Protocol Label Switching protocol RFC 3031

- is designed to sent packets (IP packet in particular) based on addresses called labels assigned when the packet enters the network.
- Routers which support MPLS are called Label Switching Routers (LSR).

Layer 4: Transport Layer Protocols

TCP – **Transmission Control Protocol,** RFC 793, …

- A fundamental protocol from the TCP/IP suite. Provides a **host-to-host connectivity** at the Transport Layer of the Internet model.

UDP – The **User Datagram Protocol,** RFC 768

- A simple connectionless transport layer protocol without a handshaking dialogue

RSVP – **Resource Reservation Protocol,** RFC 2205

- operates over an IPv4 or IPv6 Internet Layer and provides receiver-initiated setup of **resource reservations** for **multicast** or **unicast** data flows with scaling and robustness.
- It does not transport application data but is similar to a control protocol, like ICMP

Layer 4: Transport Layer Protocols (cont.)

SCTP – Stream Control Transmission Protocol (**SCTP**) is a transport-layer protocol, serving in a similar role to the popular protocols TCP and UDP, RFC 4960.

TLS – The Transport Layer Security, RFC 5246 (v1.2)

- is a cryptographic protocol designed to encrypt the data of network connections in the application layer
- It uses X.509 certificates to **authenticate** the communicating party using **asymmetric** cryptography, and to negotiate a **symmetric** session key.
- This session key is then used to encrypt data flowing between the parties.
- Several versions of the protocols (TLS and SSL) are in widespread use in applications such as web browsing, electronic mail, instant messaging, and voice-over-IP (VoIP).

Layer 5: Application Layer Protocols

HTTP – Hypertext Transfer Protocol, RFC 7540 (v2, 05/2015)

- is an application protocol for distributed, collaborative, hypermedia information systems.
- HTTP is the foundation of data communication for the World Wide Web.

Email protocols

SMTP – Simple Mail Transfer Protocol, RFC 5321 (2008)

- originates from RFC 821 (1982)
- is an Internet standard for electronic mail (e-mail) transmission.
- SMTP **Extension** for Transmission of Large and Binary **MIME** (Multipurpose Internet Mail Extensions) Messages is described in RFC 3030.

Application Layer: more Email Protocols

IMAP – **Internet Message Access Protocol**, RFC 3501 (IMAP4rev1)

- is a protocol for **email retrieval and storage**.
- IMAP allows an **e-mail client** to access e-mail on a **remote mail server.**

POP – **Post Office Protocol,** RFC 1939 (POP3)

- is a protocol used by local e-mail clients to retrieve e-mail from a remote server over a TCP/IP connection.
- Current specification is updated with an extension mechanism (RFC 2449) and an authentication mechanism (RFC 1734)

➢ IMAP and POP3 are supported by all modern **e-mail clients and servers**, and are the two most prevalent Internet standard protocols for e-mail retrieval.

Application Layer Protocols: DHCP and DNS

DHCP – The **Dynamic Host Configuration Protocol,** RFC 2131 (IPv4)

- is used on IP networks to dynamically distribute network configuration parameters, such as IP addresses.
- DHCPv6 , (RFC 3315, 2003) and its numerous updates are designed to be used on IPv6 networks.

DNS **Domain Name System** RFC 1034 , RFC 1035 , …

- is a hierarchical distributed **naming system** for computers, services, or any resource connected to the Internet or a private network.
- It **translates domain names to the numerical IP addresses** needed for the purpose of computer services and devices worldwide.
- DNS is an essential component of the functionality of most Internet services because it is the Internet's primary directory service.

More Application Layer Protocols

NTP – **Network Time Protocol** RFC 5905 (v4)

- is a networking protocol for **clock synchronization** between computer systems over packet-switched networks.
- NTP is intended to synchronize all participating computers to within a few milliseconds of Coordinated Universal Time (UTC).

SNMP – **Simple Network Management Protocol** RFC 3411 – 3418, 6353

- is an Internet-standard protocol for managing devices on IP networks.

FTP – **File Transfer Protocol**, RFC 959

- is a standard network protocol used to transfer computer files from one host to another over a TCP-based network

SSH – **Secure Shell**, RFC 4253

- is a cryptographic (encrypted) network protocol for initiating text-based shell sessions on remote machines in a secure way.

Application Layer Routing Protocols

BGP – **Border Gateway Protocol**, RFC 4271 (BGP4)

- is a standardized **exterior gateway protocol** designed to exchange routing and reachability information between **Autonomous Systems** (AS) on the Internet.

RIP – **Routing Information Protocol,**

- Is an interior gateway protocol designed to be used **inside** Autonomous Systems
- It employs the **hop count** as a routing metric.
- For RIP v2: RFC2453
- For RIPng: RFC 2080

Application Layer Multimedia Protocols

RTP – The **Real-time Transport Protocol,** RFC 3550

- is a network protocol for delivering **audio and video over IP** networks.
- RTP is used extensively in communication and entertainment systems that involve streaming media, such as telephony, video teleconference applications, television services and web-based push-to-talk features.
- RTP is used in conjunction with the RTP Control Protocol (RTCP).
- RTP carries the media streams (e.g., audio and video) and RTCP is used to monitor transmission statistics and quality of service (QoS) and aids synchronization of multiple streams.
- RTP is one of the technical foundations of Voice over IP (VoIP) and streaming services.

LLDP and LLMNR

LLDP – Link Layer Discovery Protocol, IEEE 802.1AB

- is a vendor-neutral **link layer protocol** in the Internet Protocol Suite used by network devices for advertising their identity, capabilities, and neighbours on an IEEE 802 local area network, principally wired **Ethernet**.
- The protocol is formally referred to by the IEEE as *Station and Media Access Control Connectivity Discovery*

LLMNR – Link-Local Multicast Name Resolution, RFC 4795

- is a protocol based on the Domain Name System (DNS) packet format that allows both IPv4 and IPv6 hosts to perform name resolution for hosts on the same local link.
- It is included in all recent Microsoft Windows including Windows 7 and Windows 10.

SSDP

SSDP – Simple Service Discovery Protocol

- is a network protocol based on the Internet Protocol Suite for advertisement and discovery of network services and presence information.
- It accomplishes this without assistance of server-based configuration mechanisms, such as DHCP, or DNS, and without special static configuration of a network host.
- SSDP is the basis of the discovery protocol of **Universal Plug and Play** (UPnP) and is intended for use in residential or small office environments.
- SSDP was incorporated into the UPnP protocol stack, and a description of the final implementation is included in UPnP standards documents of the Open Connectivity Foundation