university
of
tyumen

school
of advanced
studies

Information Technology - intermediate

Lecture 3
Networking

Fabio Grazioso - *April 2018*

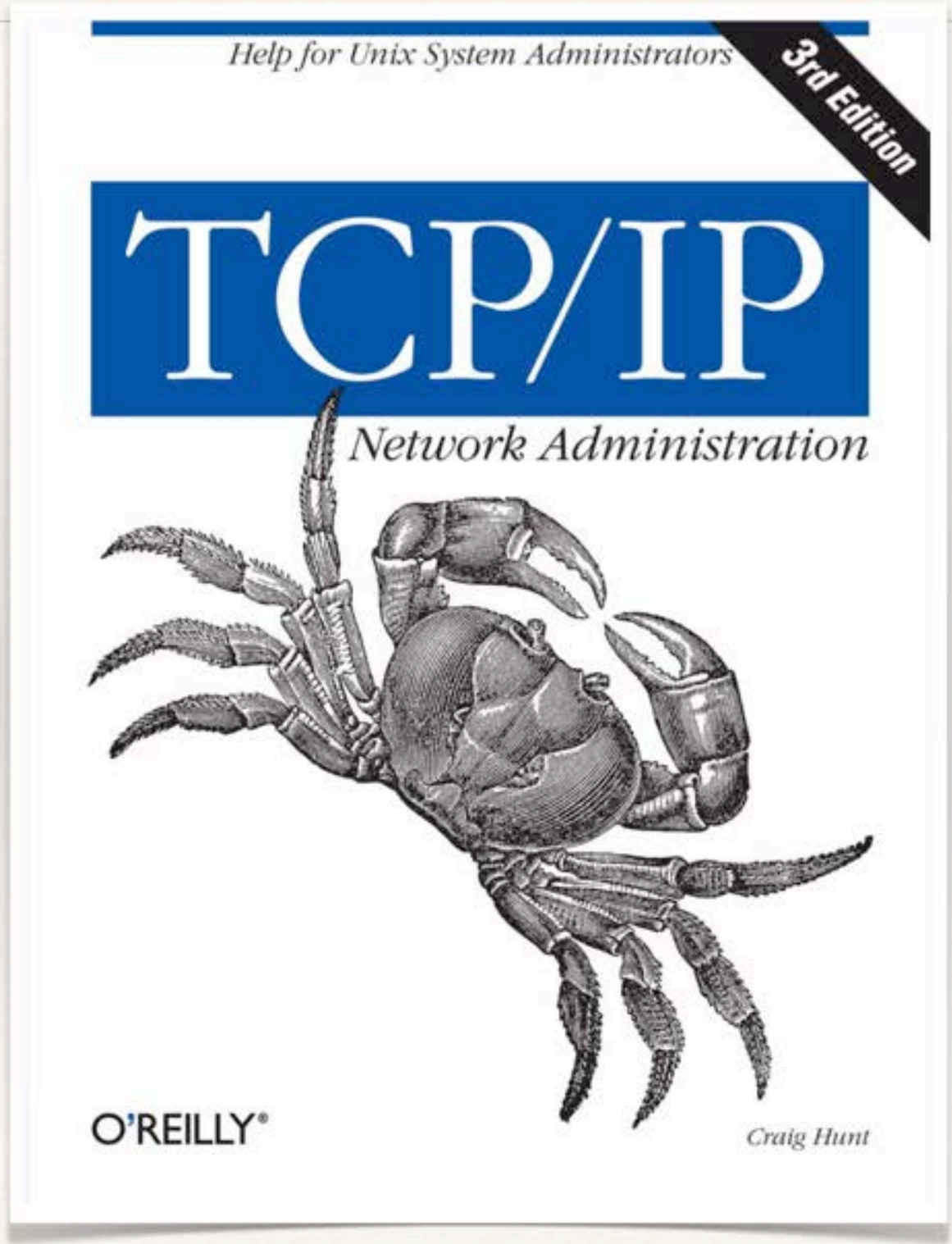
Todays' lecture

Internet

summary of the lecture

- Historical introduction
  - ARPAnet
- Packet switching
- Protocol structure (layers)
- Addresses
- Routing

Textbook


Help for Unix System Administrators
3rd Edition
TCP/IP
Network Administration
O'REILLY®
Craig Hunt

Historical summary

Fault tolerance

- In the early 1960s, American computer scientist Paul Baran developed the concept Distributed Adaptive Message Block Switching with the goal to provide a **fault-tolerant**, efficient routing method for telecommunication messages as part of a research program at the RAND Corporation, funded by the US Department of Defense.
- The new concept found little resonance among network implementers until the independent work of British computer scientist Donald Davies at the National Physical Laboratory (United Kingdom) in 1965. Davies is credited with coining the modern name **packet switching** and inspiring numerous packet switching networks in the decade following, including the incorporation of the concept in the early ARPANET in the United States.

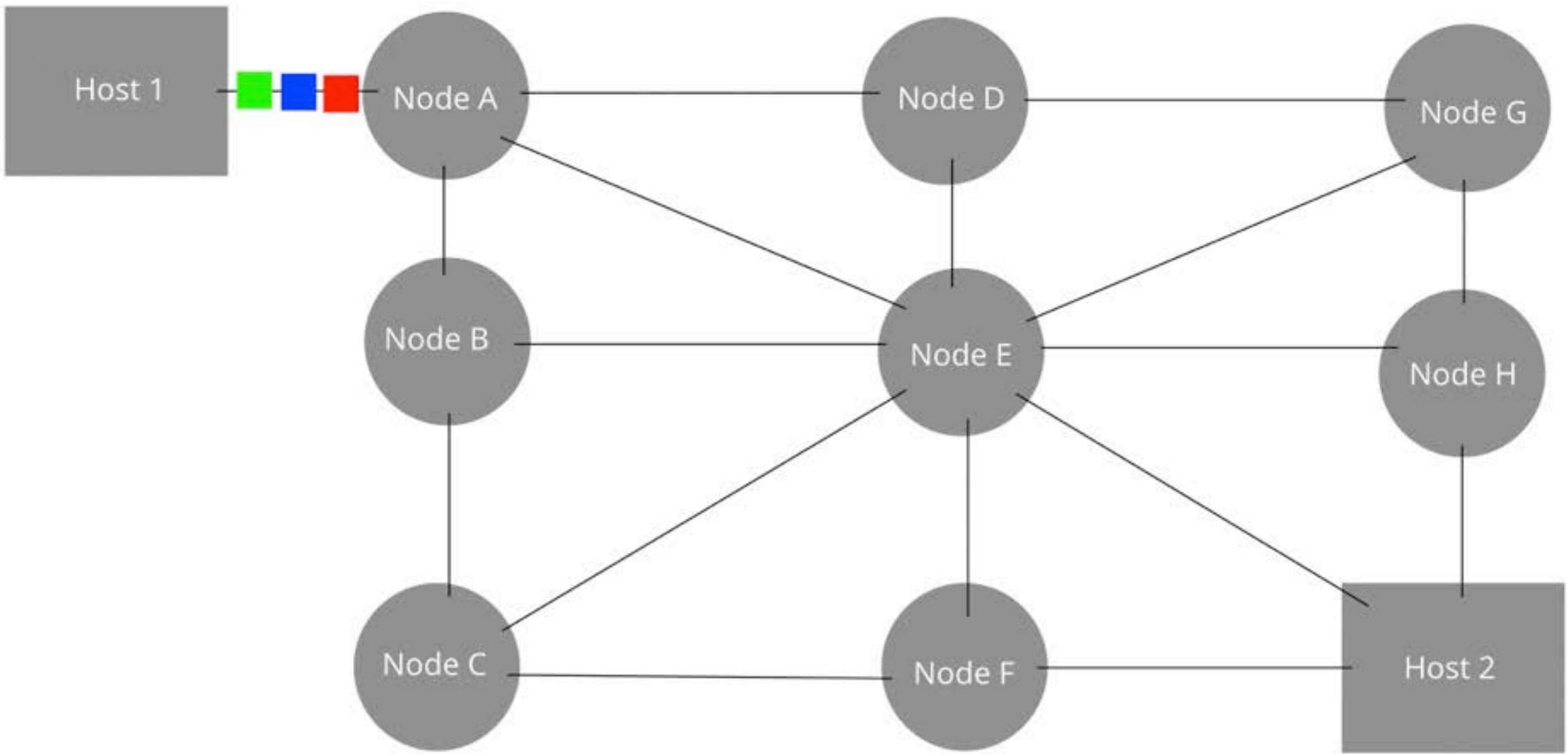
Wikipedia

Packet switching

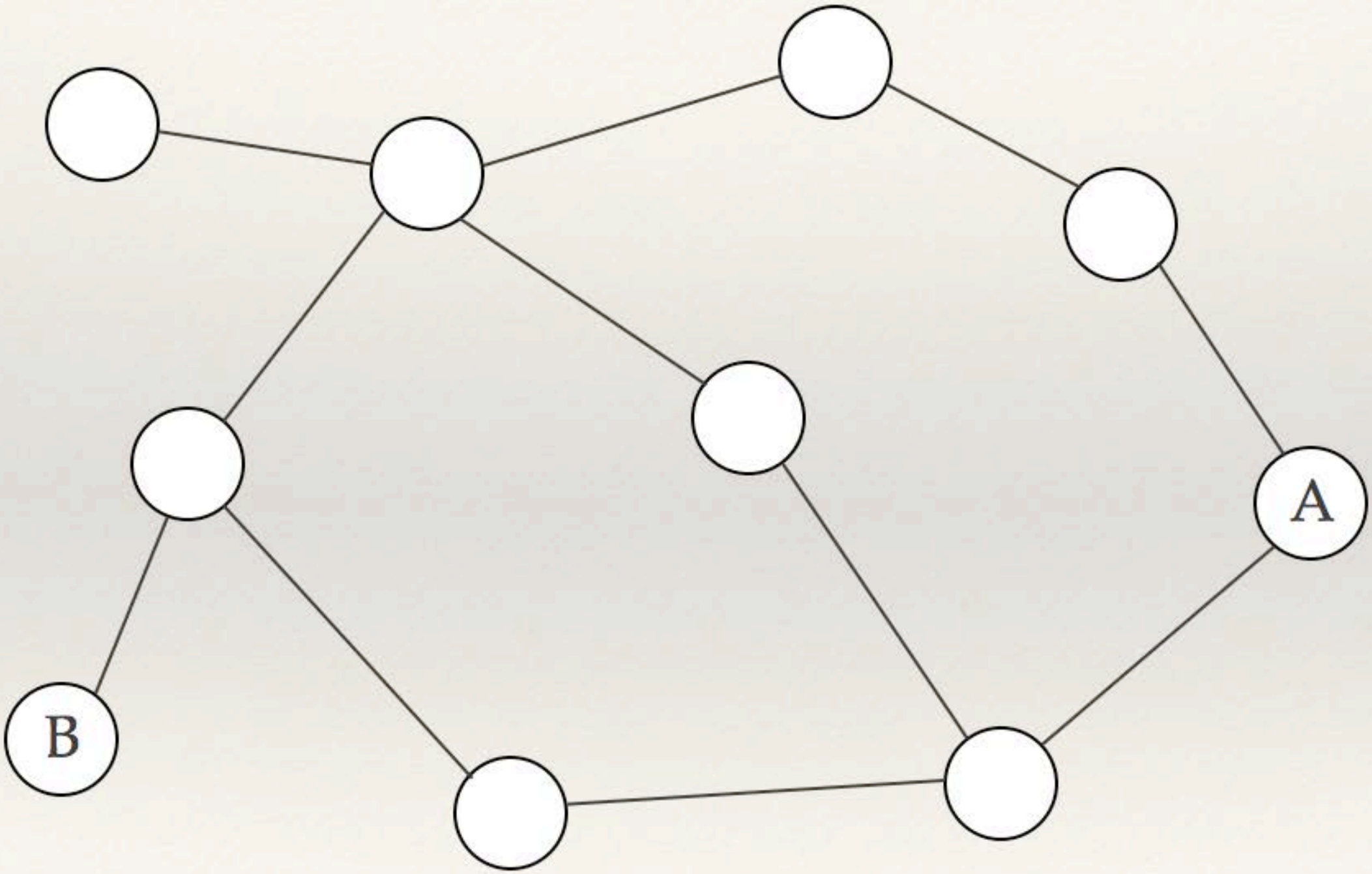
- Packet switching is a method of grouping data which is transmitted over a digital network into packets which are made of a header and a payload. Data in the header is used by networking hardware to direct the packet to its destination where the payload is extracted and used by application software.

Packet switching

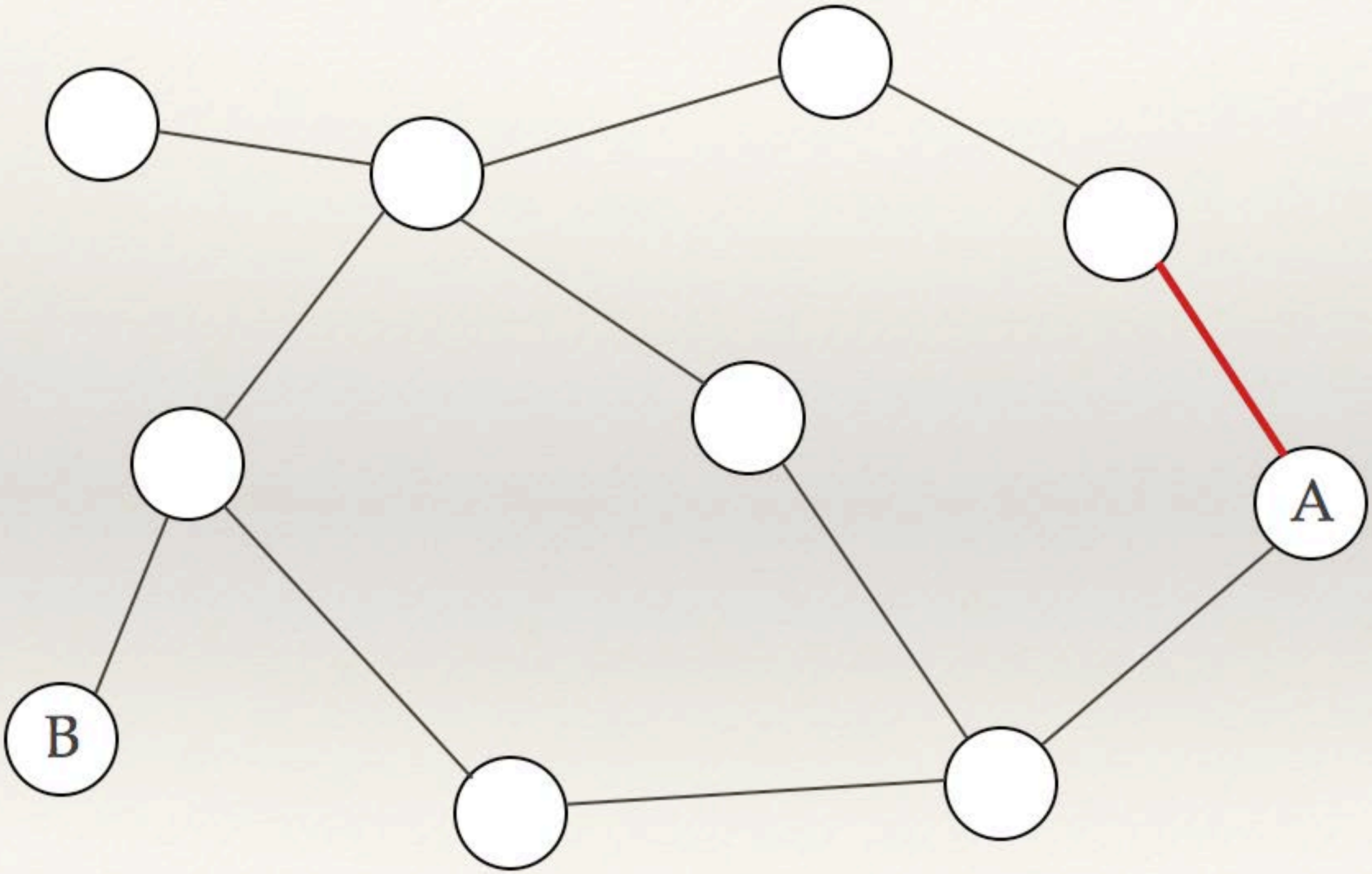
The original message is Green, Blue, Red.



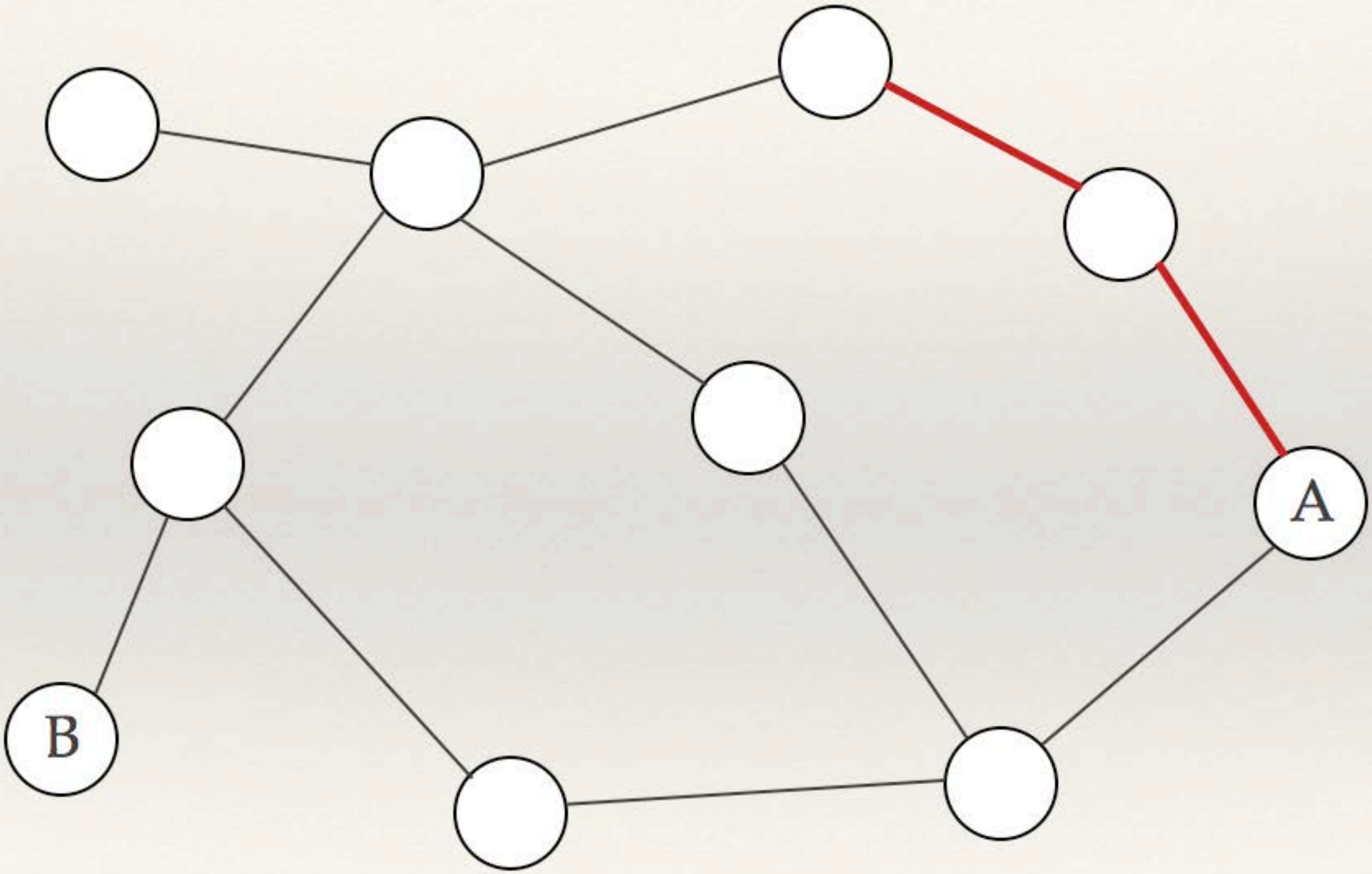
Routing



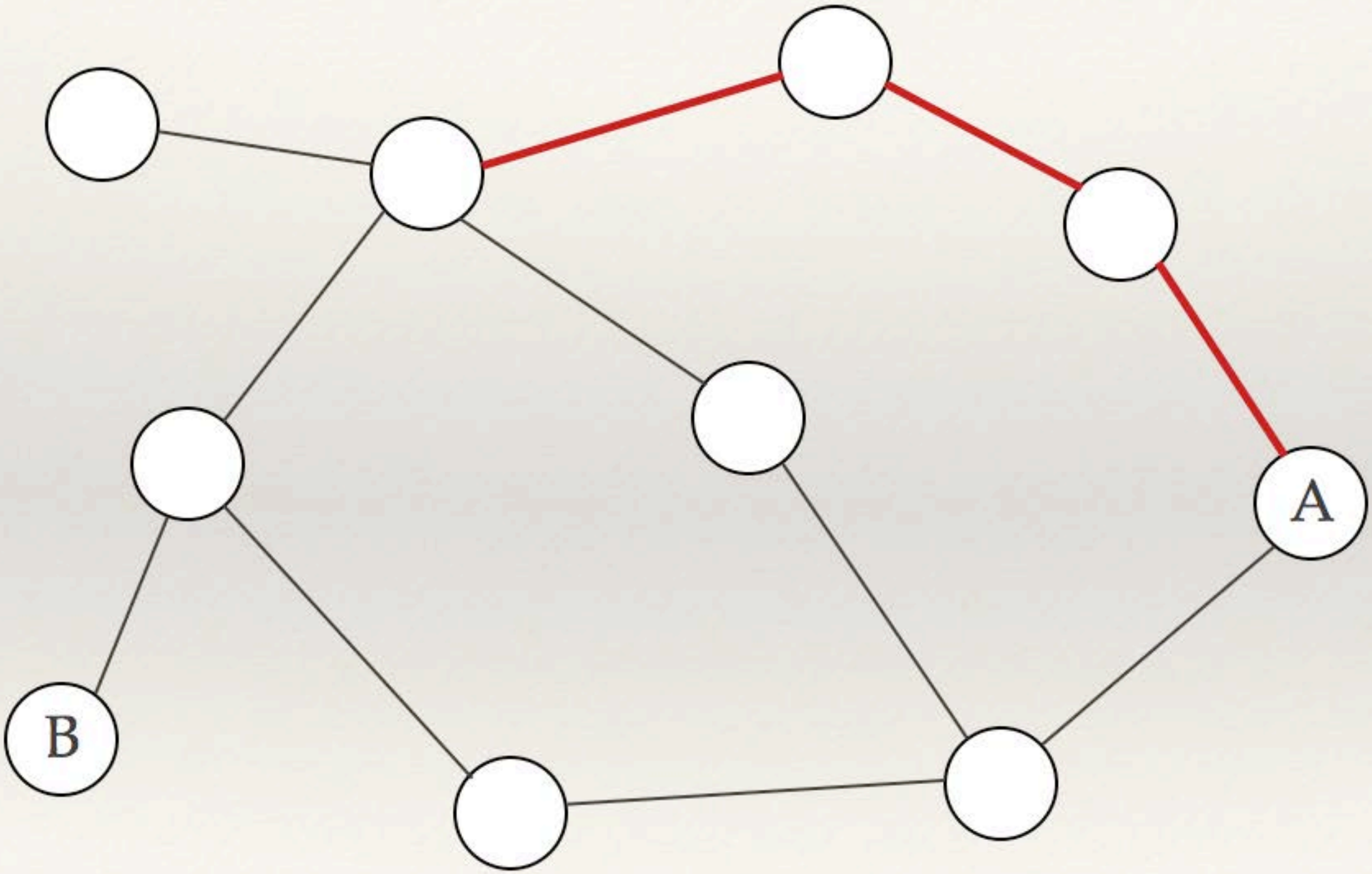
Routing



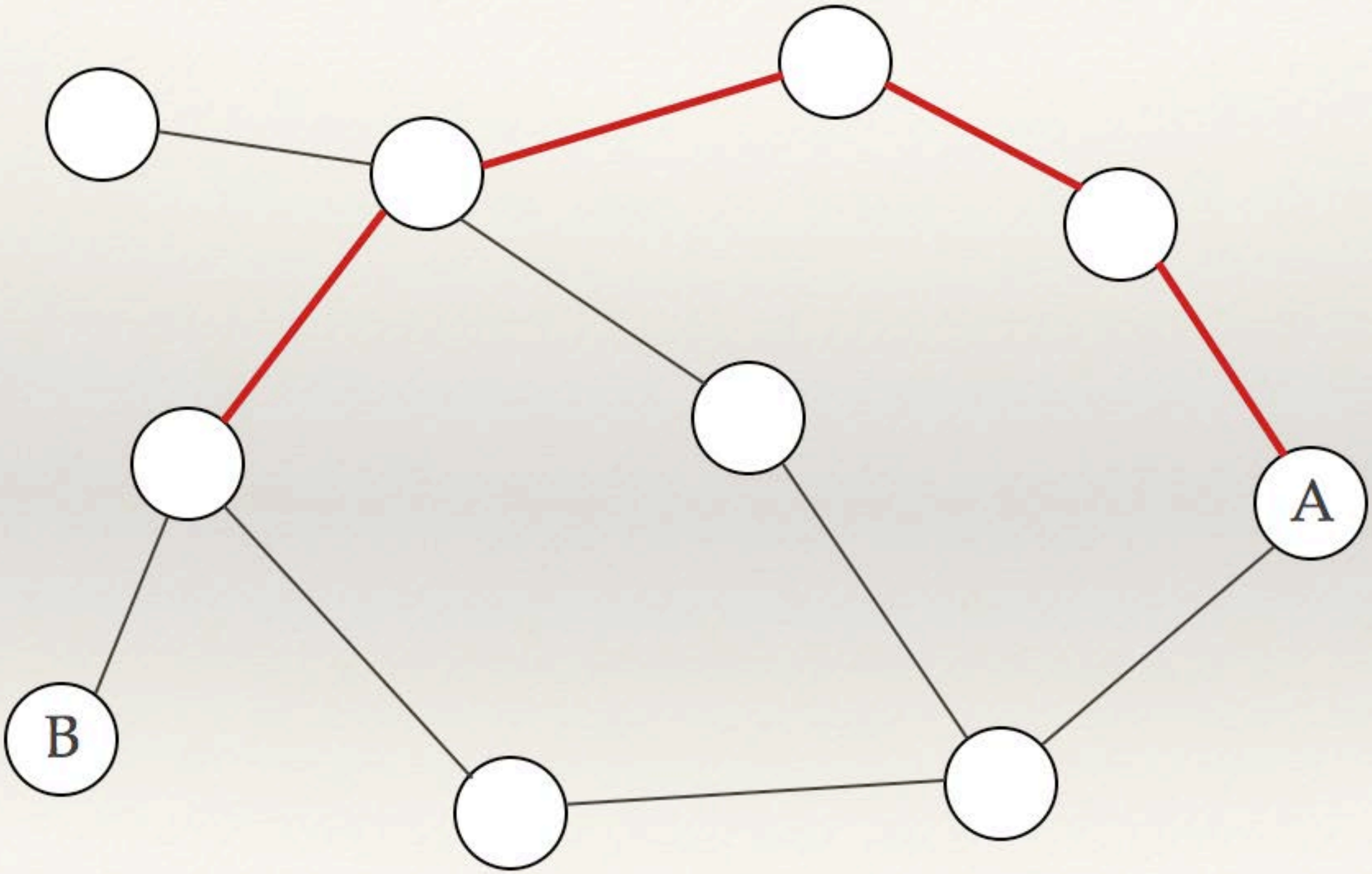
Routing



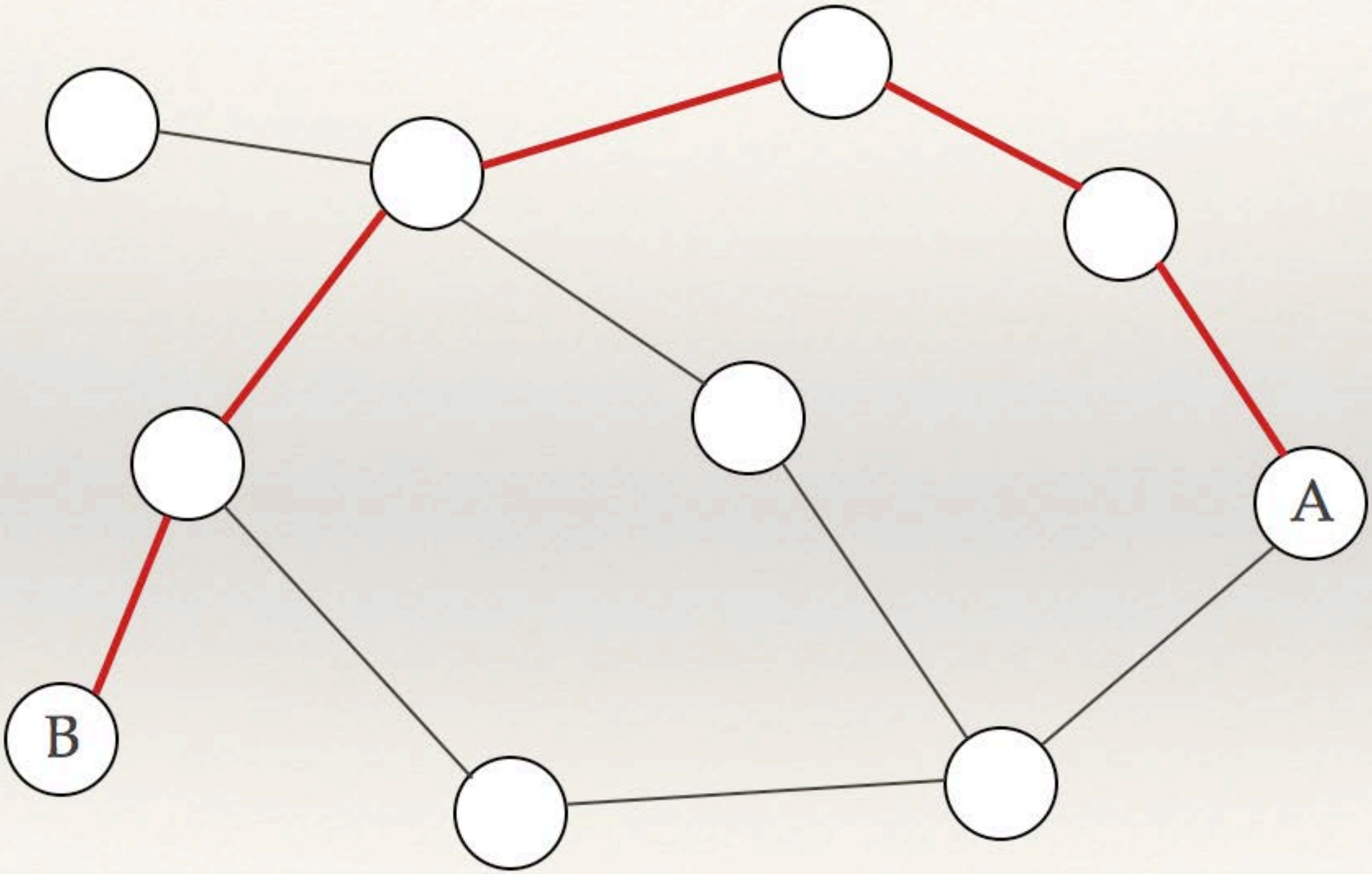
Routing



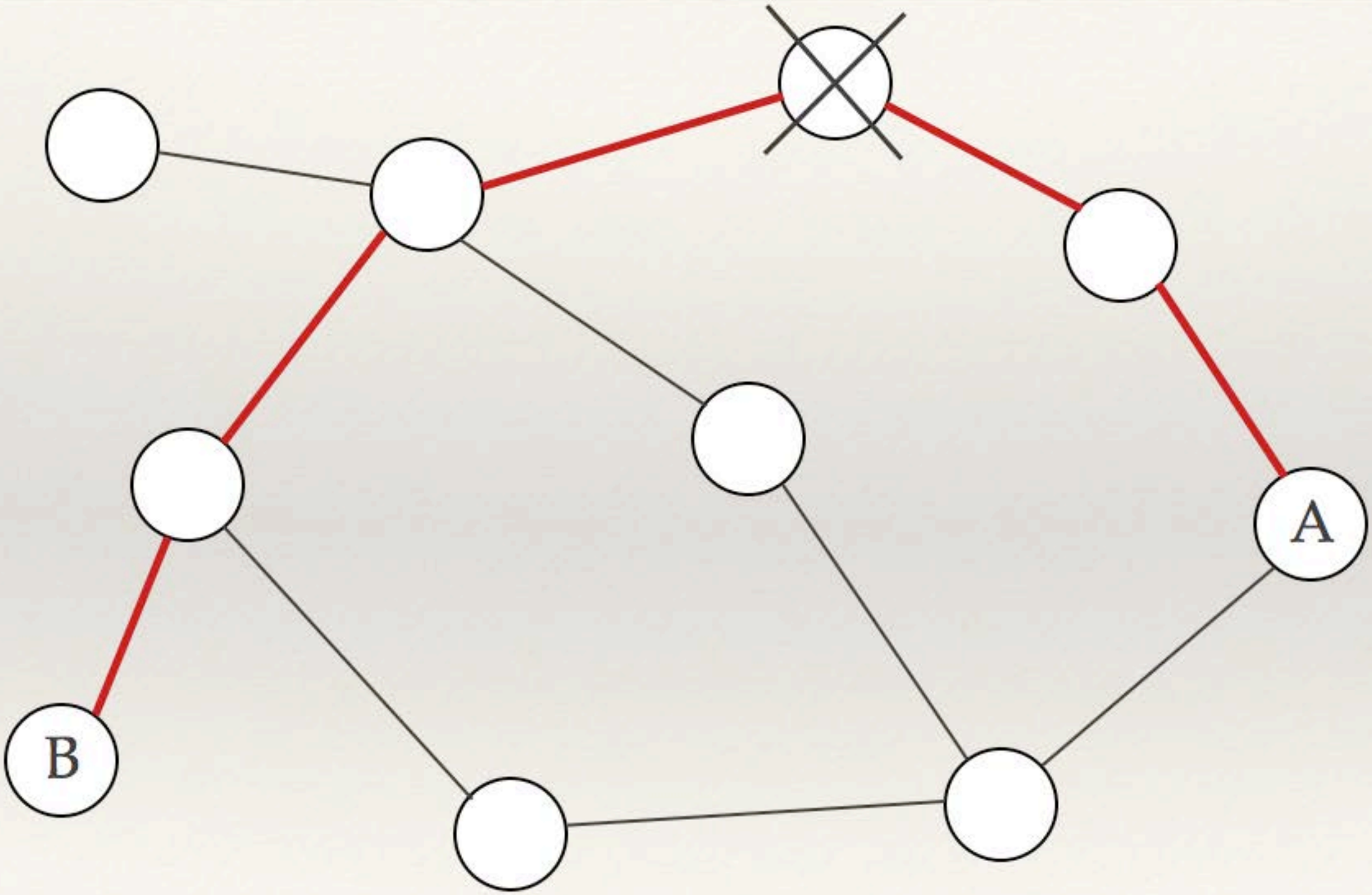
Routing



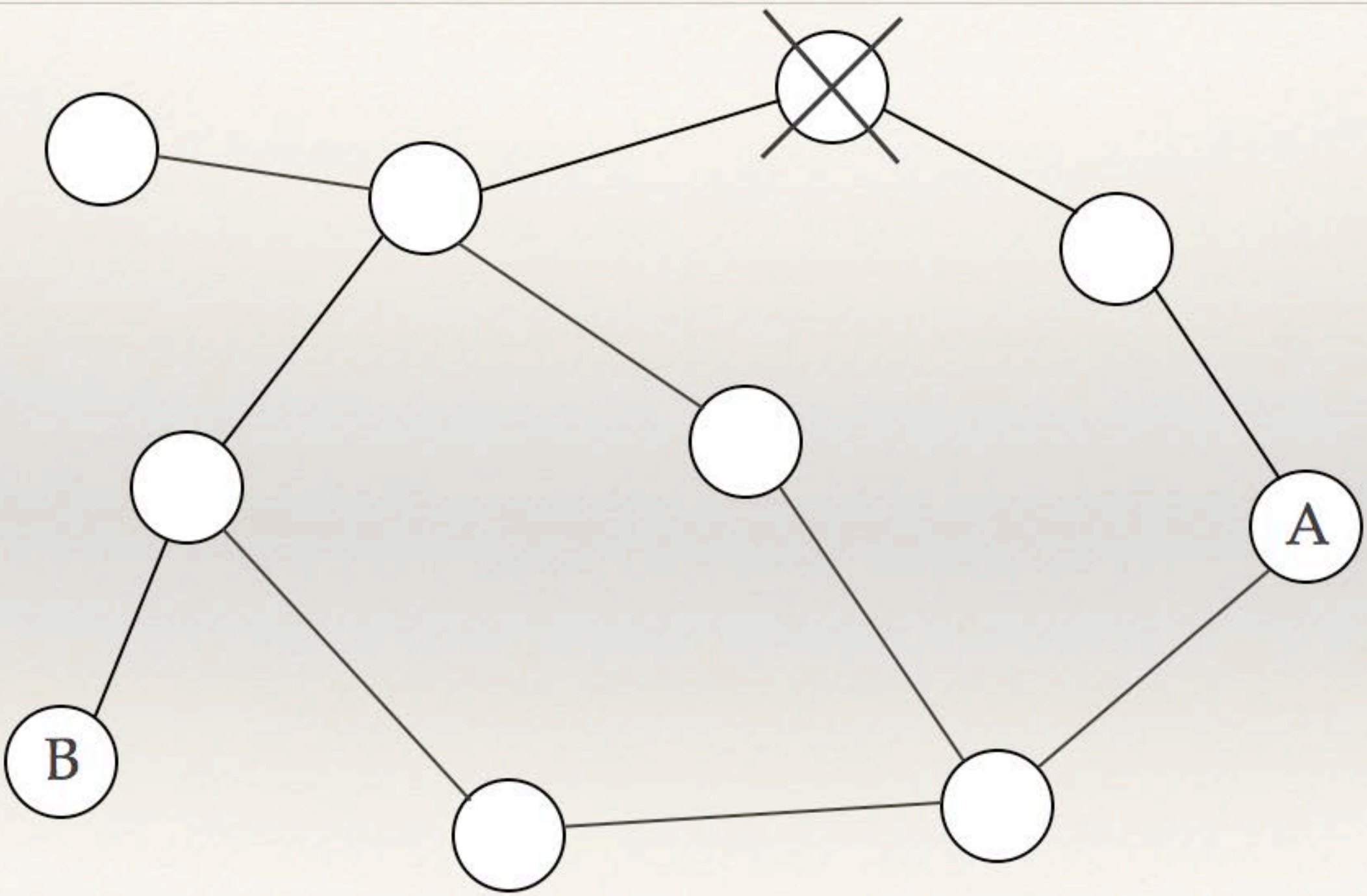
Routing



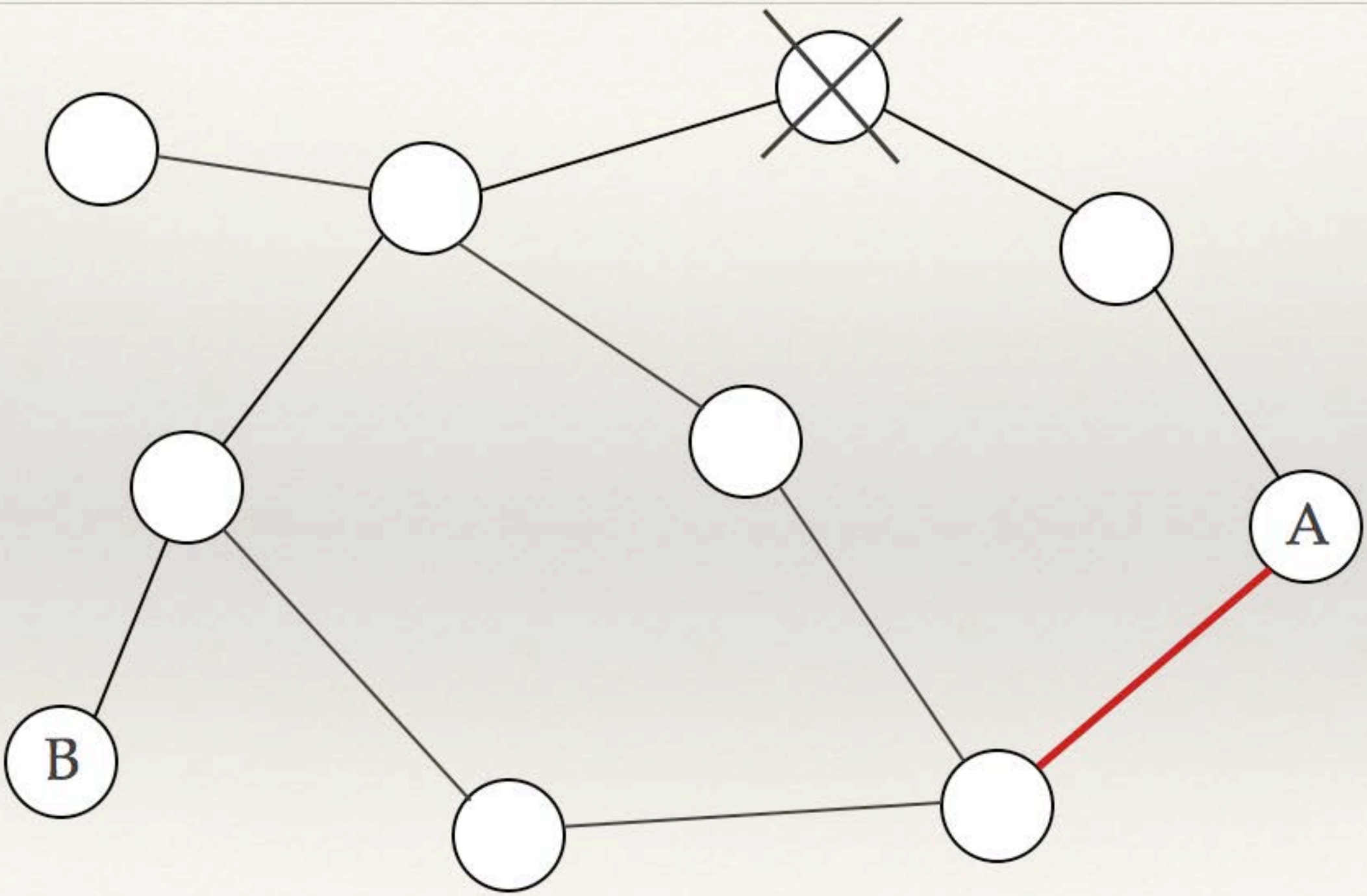
Fault tolerance



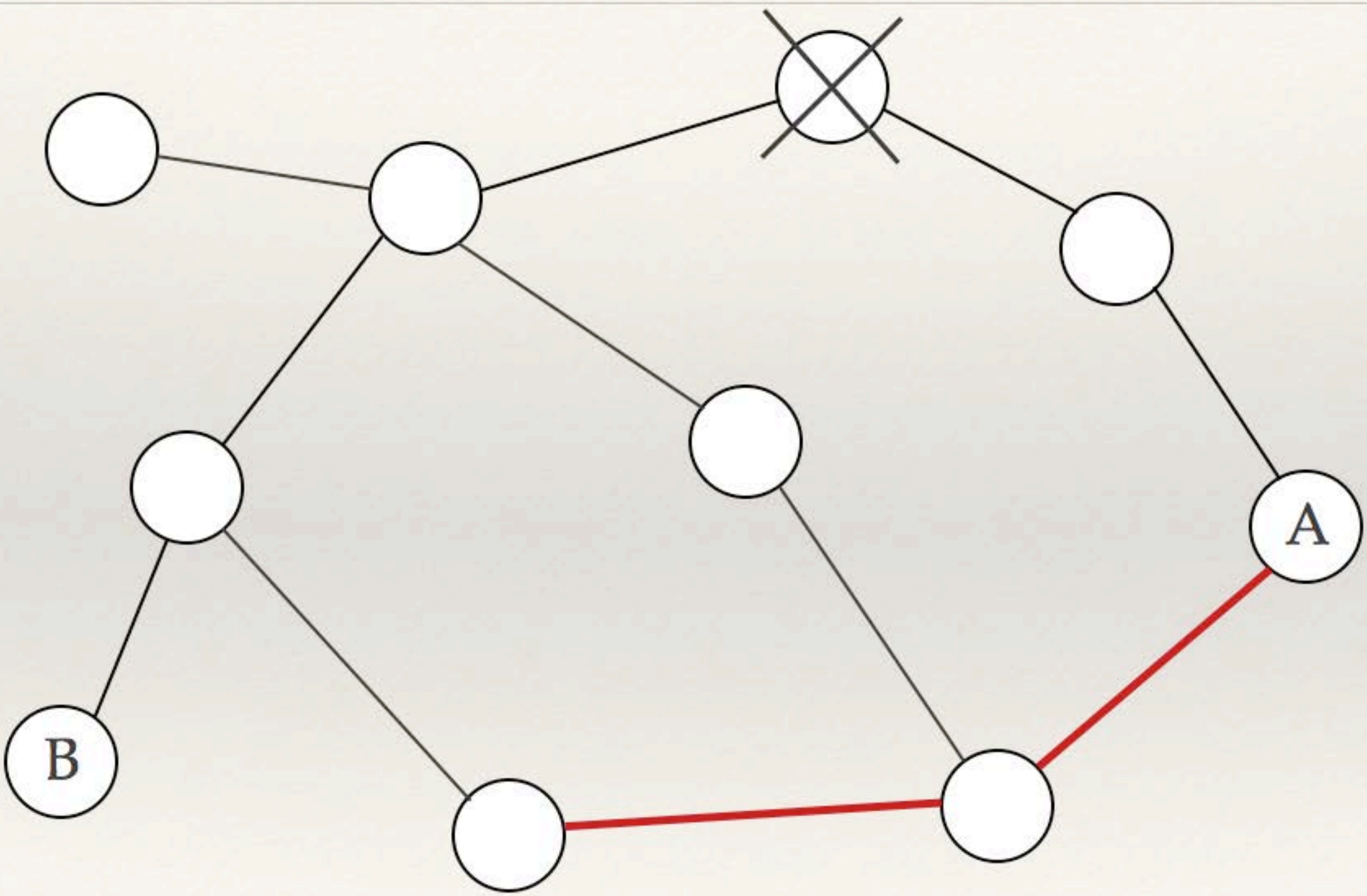
Fault tolerance



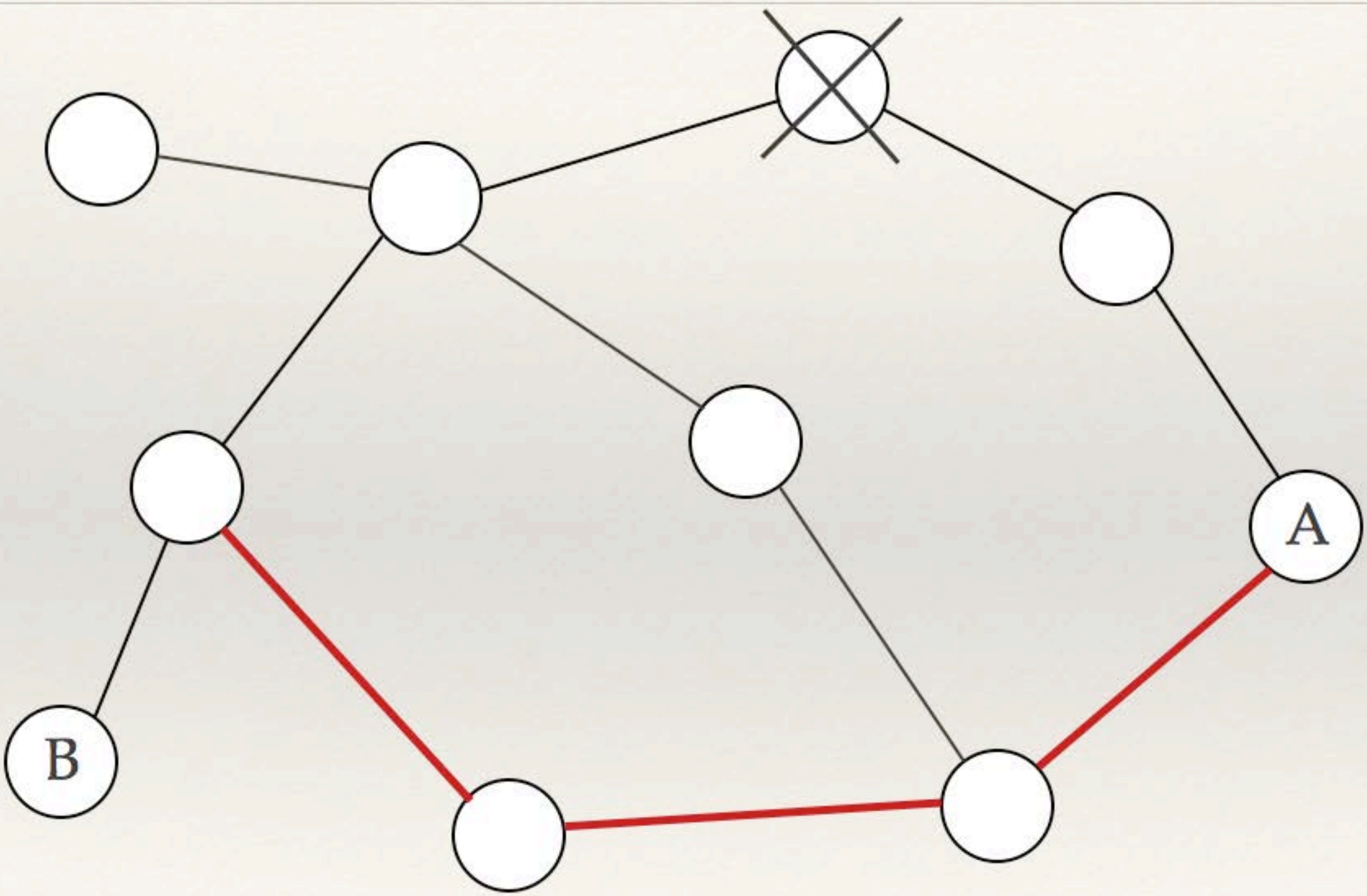
Fault tolerance



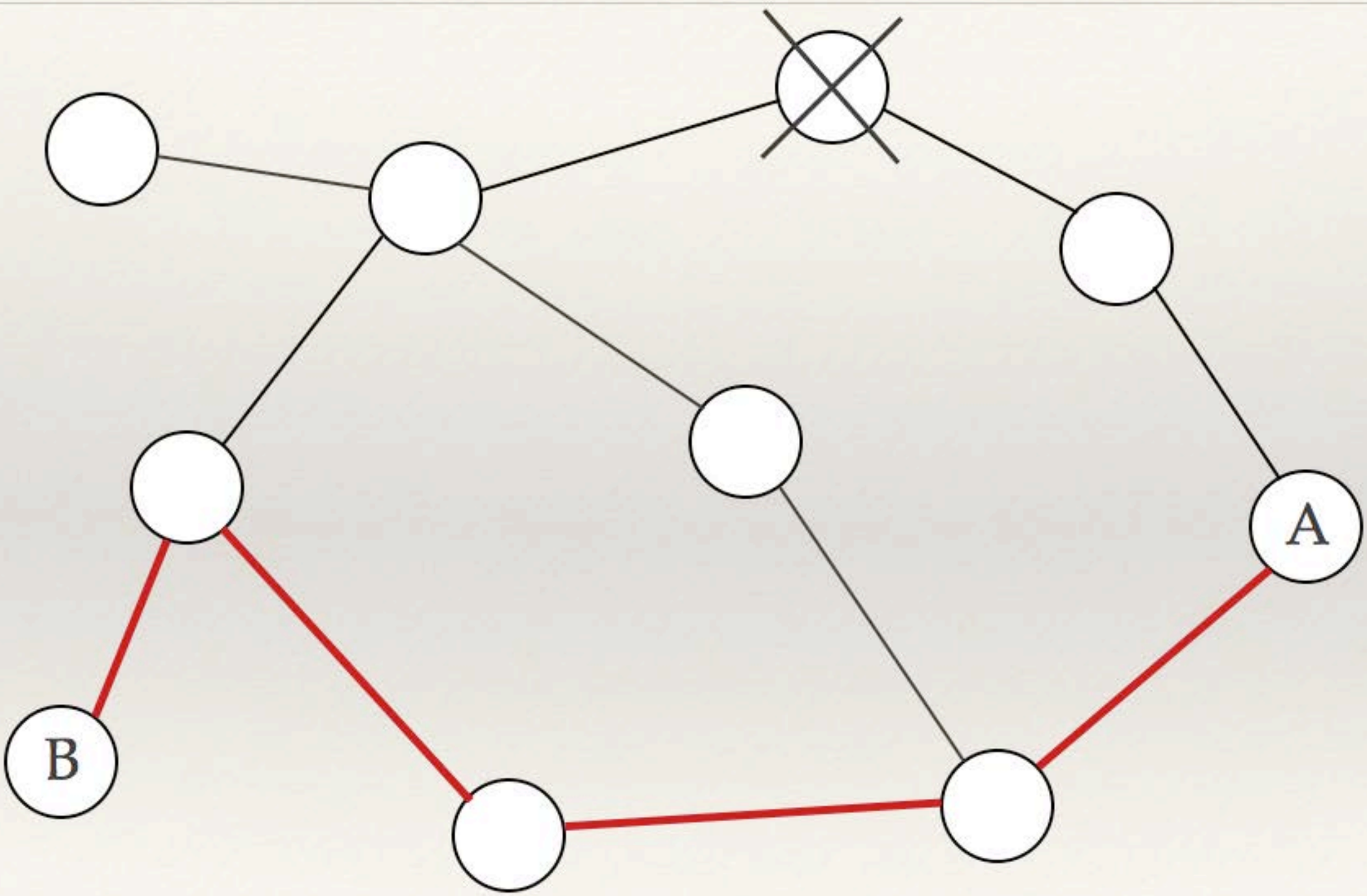
Fault tolerance



Fault tolerance



Fault tolerance



Protocols layers

protocol

protocol | ˈprōdəˌkôl ˈprōdəˌkäl |

noun

1 the official procedure or system of rules governing affairs of state or diplomatic occasions: *protocol forbids the prince from making any public statement in his defense.*

- the accepted or established code of procedure or behavior in any group, organization, or situation: *what is the protocol at a conference if one's neighbor dozes off during the speeches?*

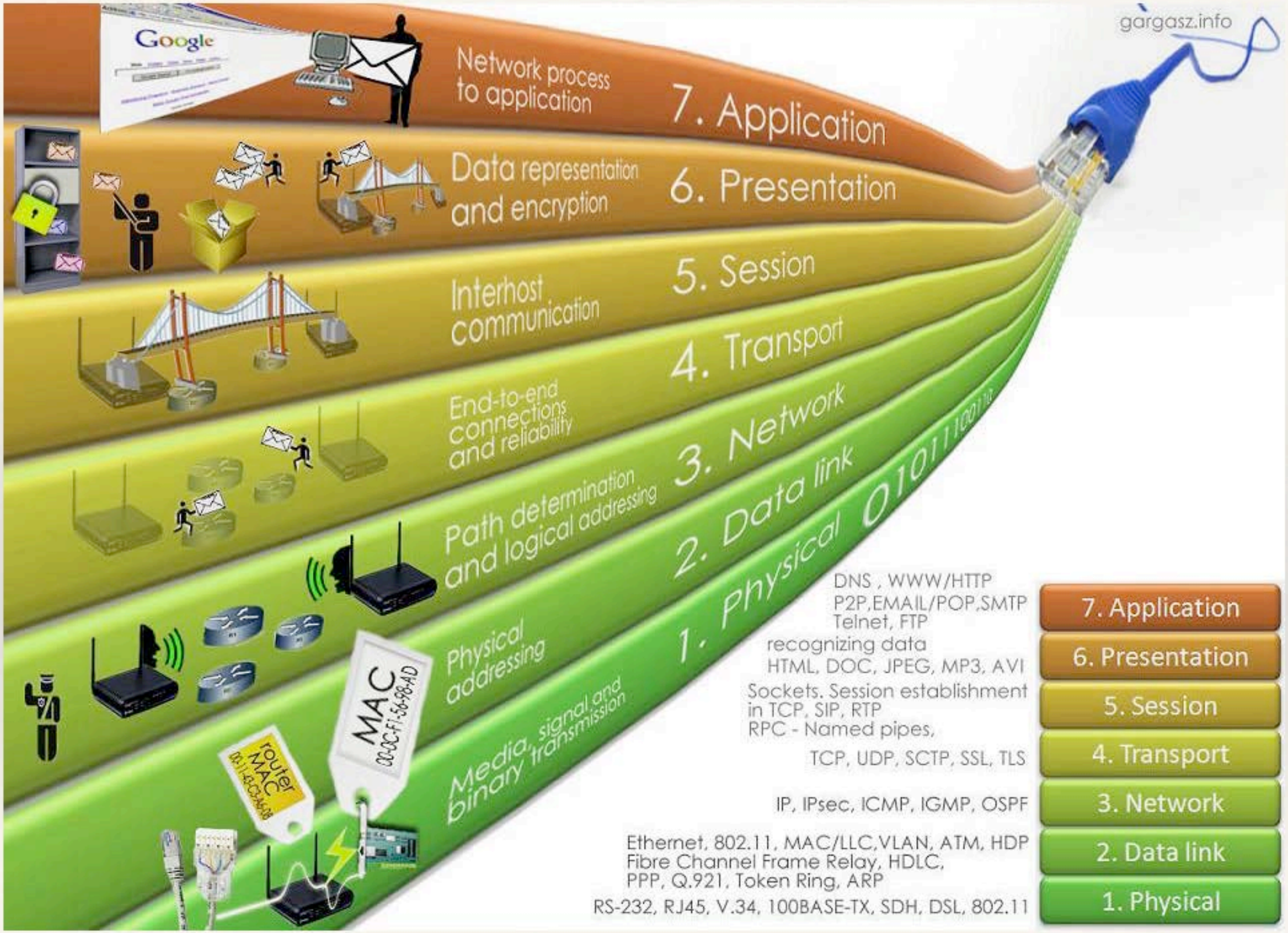
- *Computing* a set of rules governing the exchange or transmission of data between devices.

2 the original draft of a diplomatic document, especially of the terms of a treaty agreed to in conference and signed by the parties.

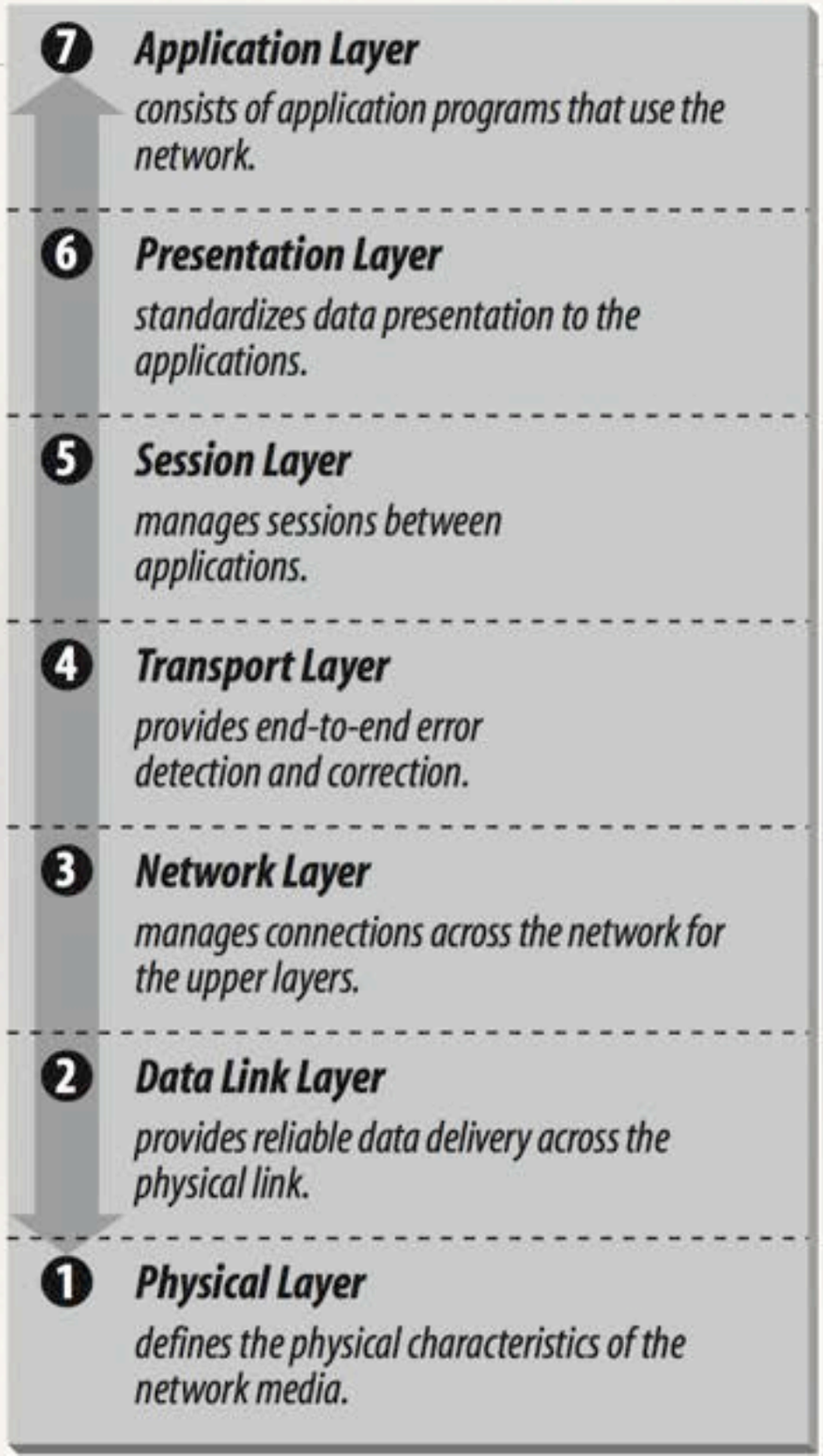
- an amendment or addition to a treaty or convention: *a protocol to the treaty allowed for this Danish referendum.*

3 a formal or official record of scientific experimental observations.

- a procedure for carrying out a scientific experiment or a course of medical treatment.


gargasz.info
Google
Network process to application
7. Application
Data representation and encryption
6. Presentation
Interhost communication
5. Session
End-to-end connections and reliability
4. Transport
Path determination and logical addressing
3. Network
Physical addressing
2. Data link
Media, signal and binary transmission
1. Physical
MAC
00-0C-F1-56-98-AD
router MAC
DNS , WWW/HTTP
P2P,EMAIL/POP,SMTP
Telnet, FTP
recognizing data
HTML, DOC, JPEG, MP3, AVI
Sockets. Session establishment
in TCP, SIP, RTP
RPC - Named pipes,
TCP, UDP, SCTP, SSL, TLS
IP, IPsec, ICMP, IGMP, OSPF
Ethernet, 802.11, MAC/LLC,VLAN, ATM, HDP
Fibre Channel Frame Relay, HDLC,
PPP, Q.921, Token Ring, ARP
RS-232, RJ45, V.34, 100BASE-TX, SDH, DSL, 802.11
7. Application
6. Presentation
5. Session
4. Transport
3. Network
2. Data link
1. Physical

Open Systems Interconnect (OSI) Reference Model

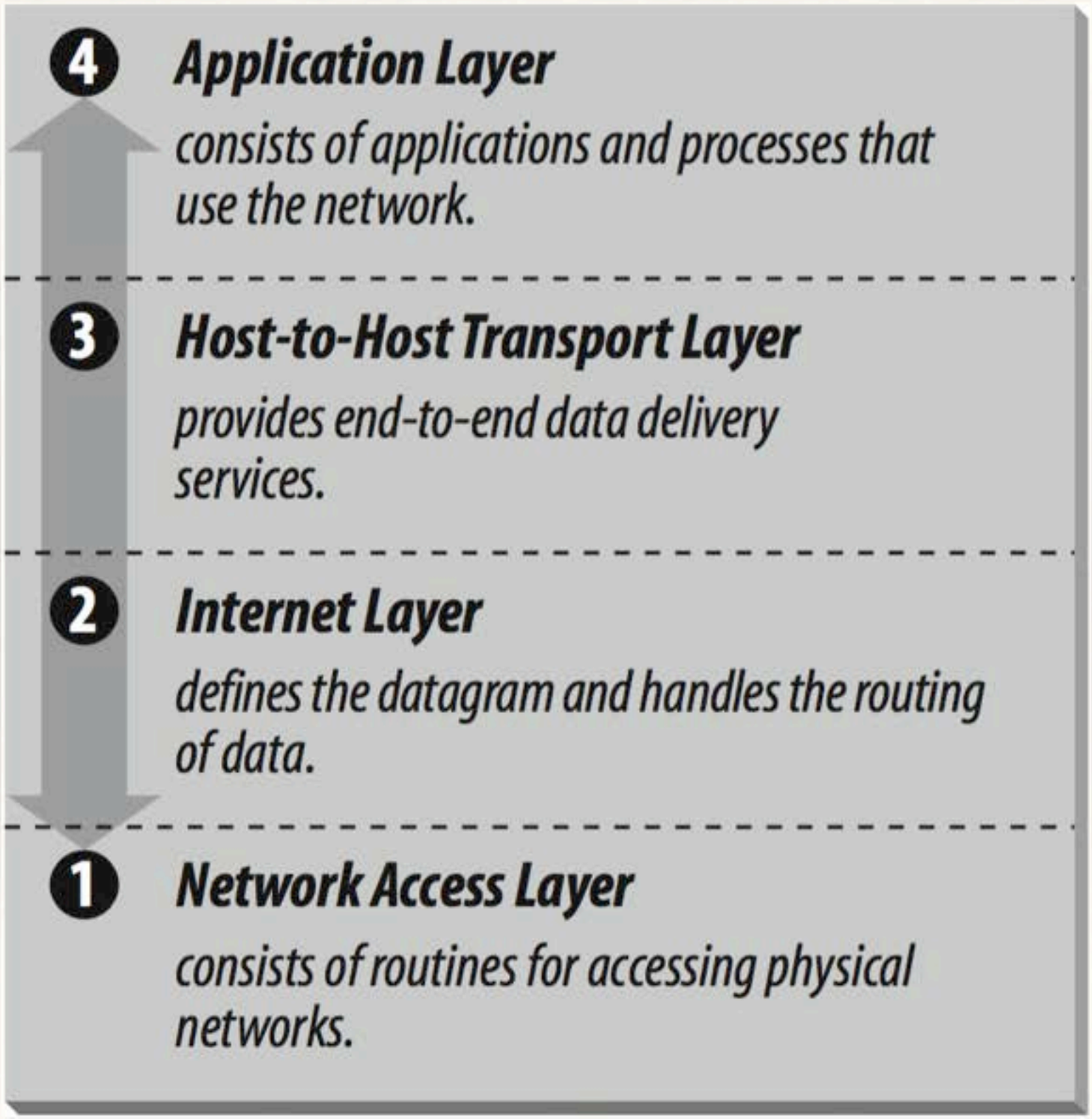


Hunt p7

TCP/IP

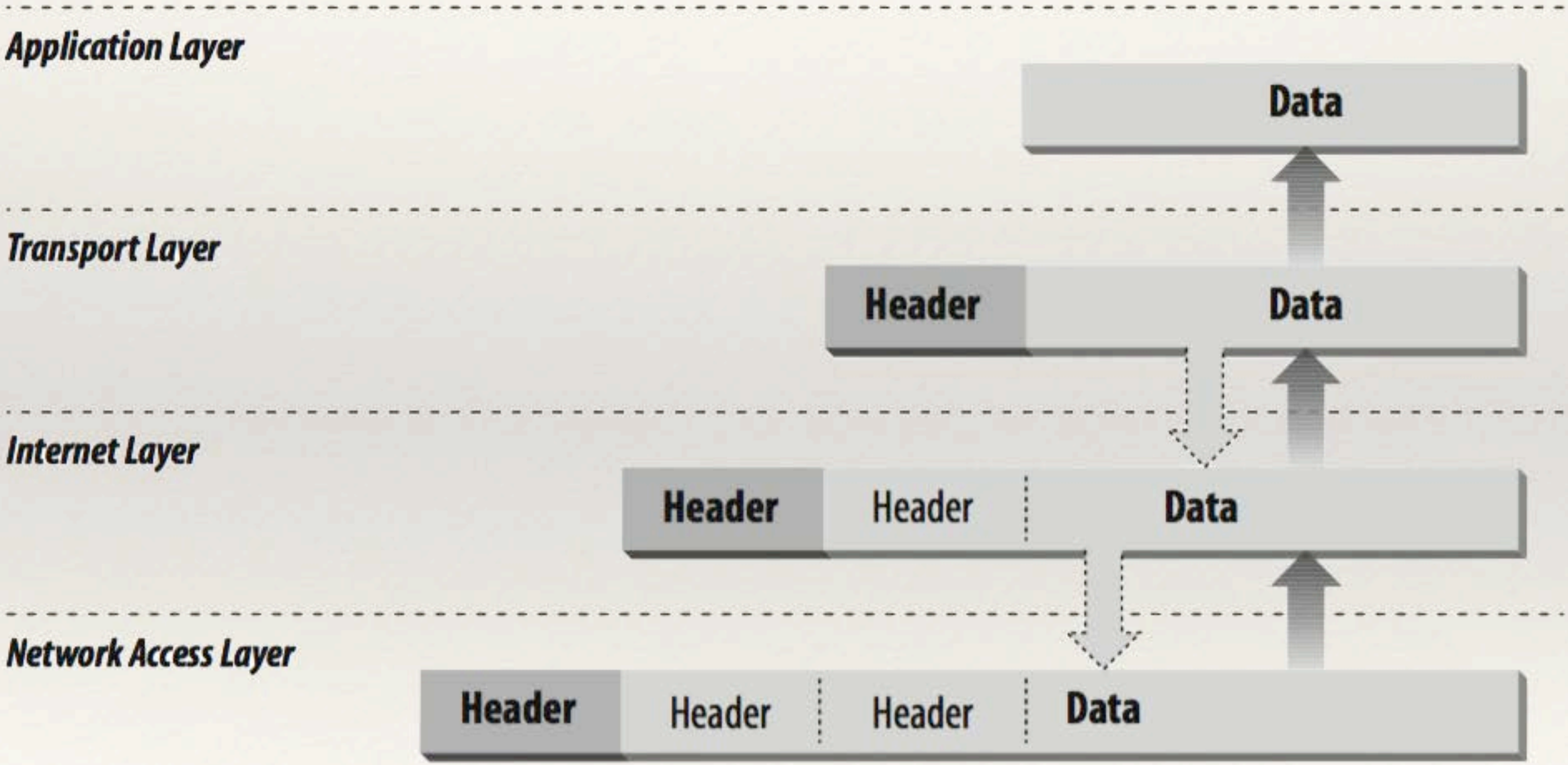
(Transmission Control Protocol /Internet Protocol)

TCP/IP



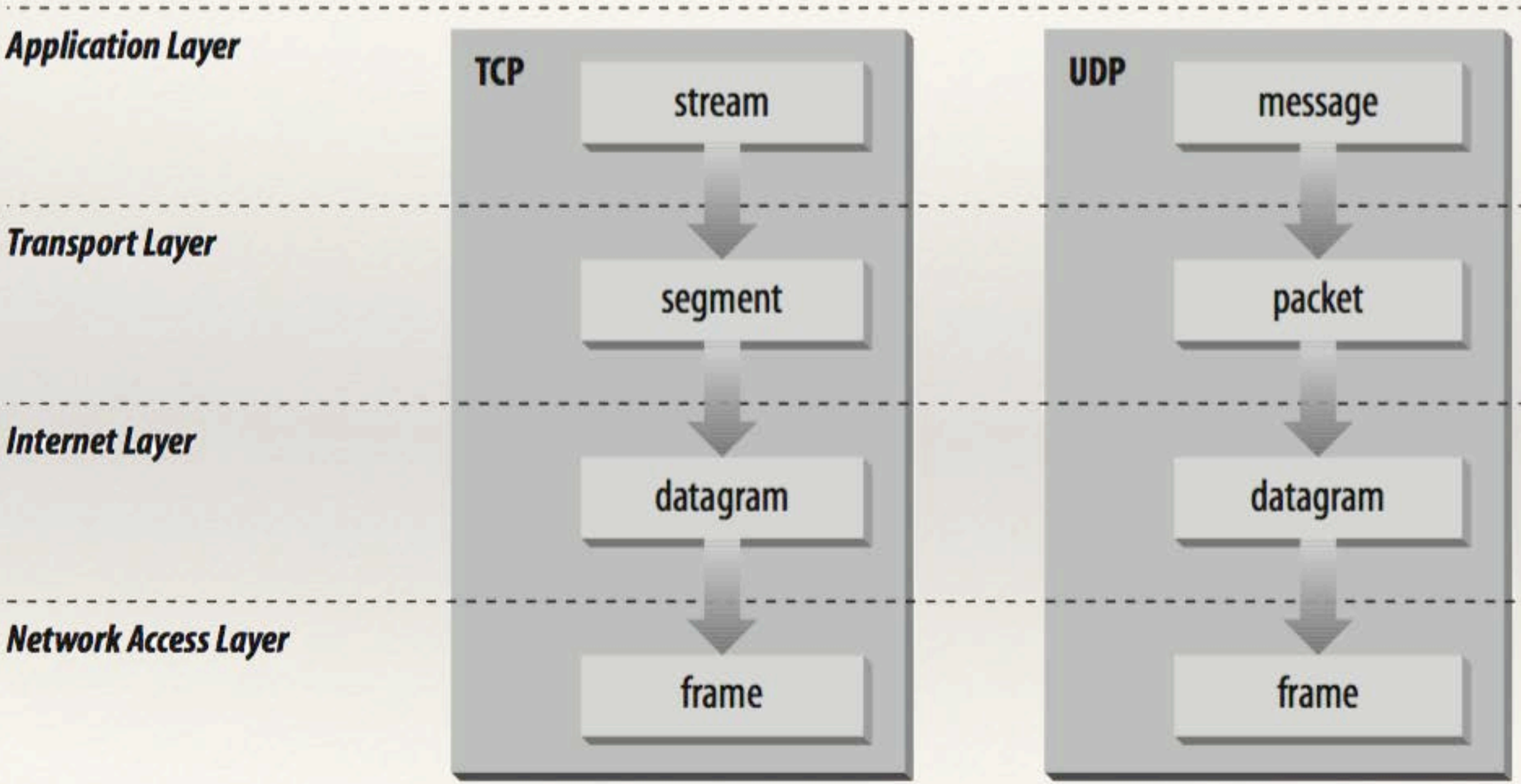
Hunt p10

data encapsulation



Hunt p11

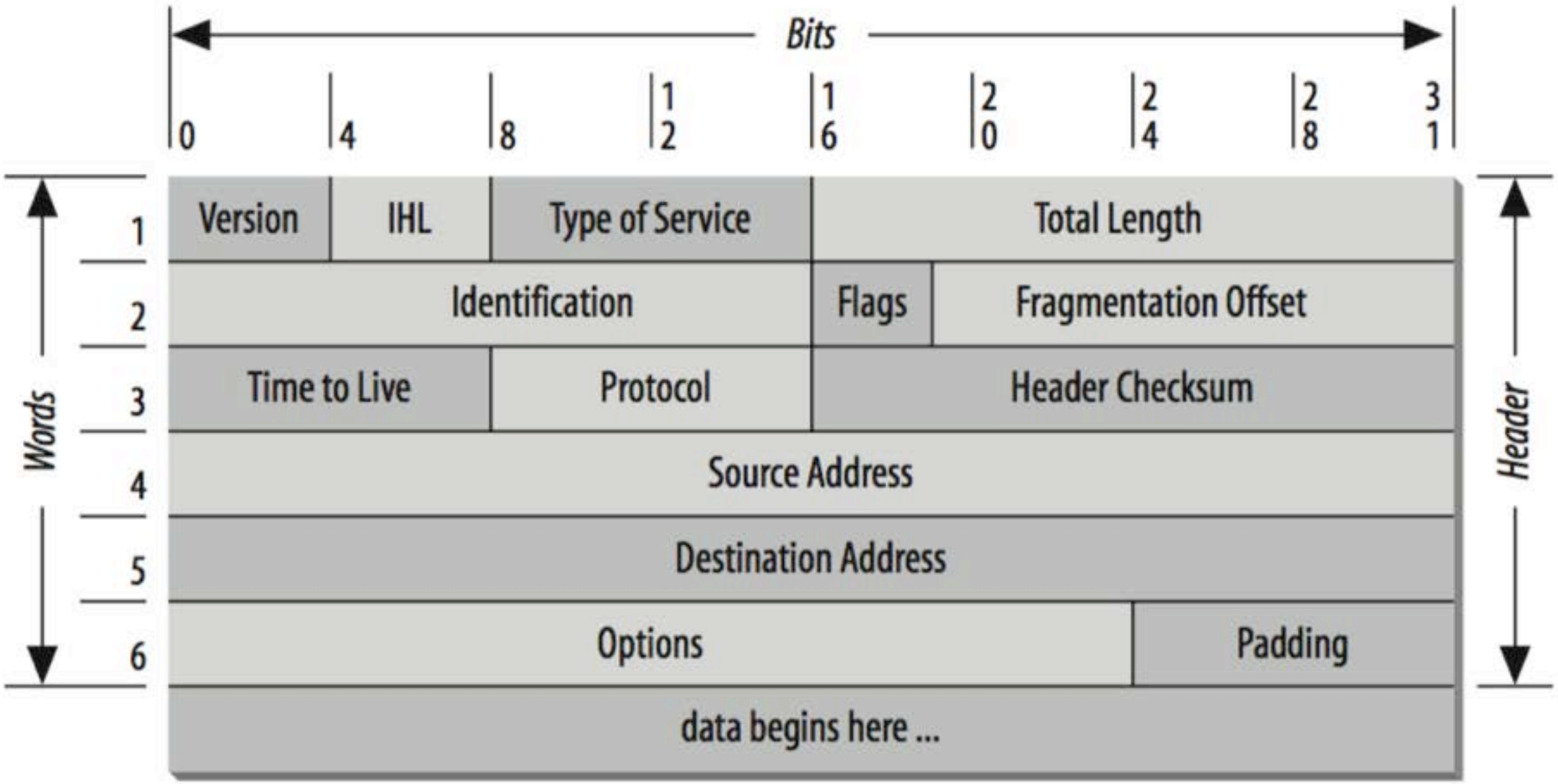
layers



Hunt p11

Packets
(internet layer)

TCP/IP datagram



Hunt p14

Routing

- If the Destination Address is the address of a host on the local network, the packet is delivered directly to the destina- tion. If the Destination Address is not on the local network, the packet is passed to a gateway for delivery.
- Gateways are devices that switch packets between the different physical networks.
- Deciding which gateway to use is called routing. IP makes the routing decision for each individual packet.

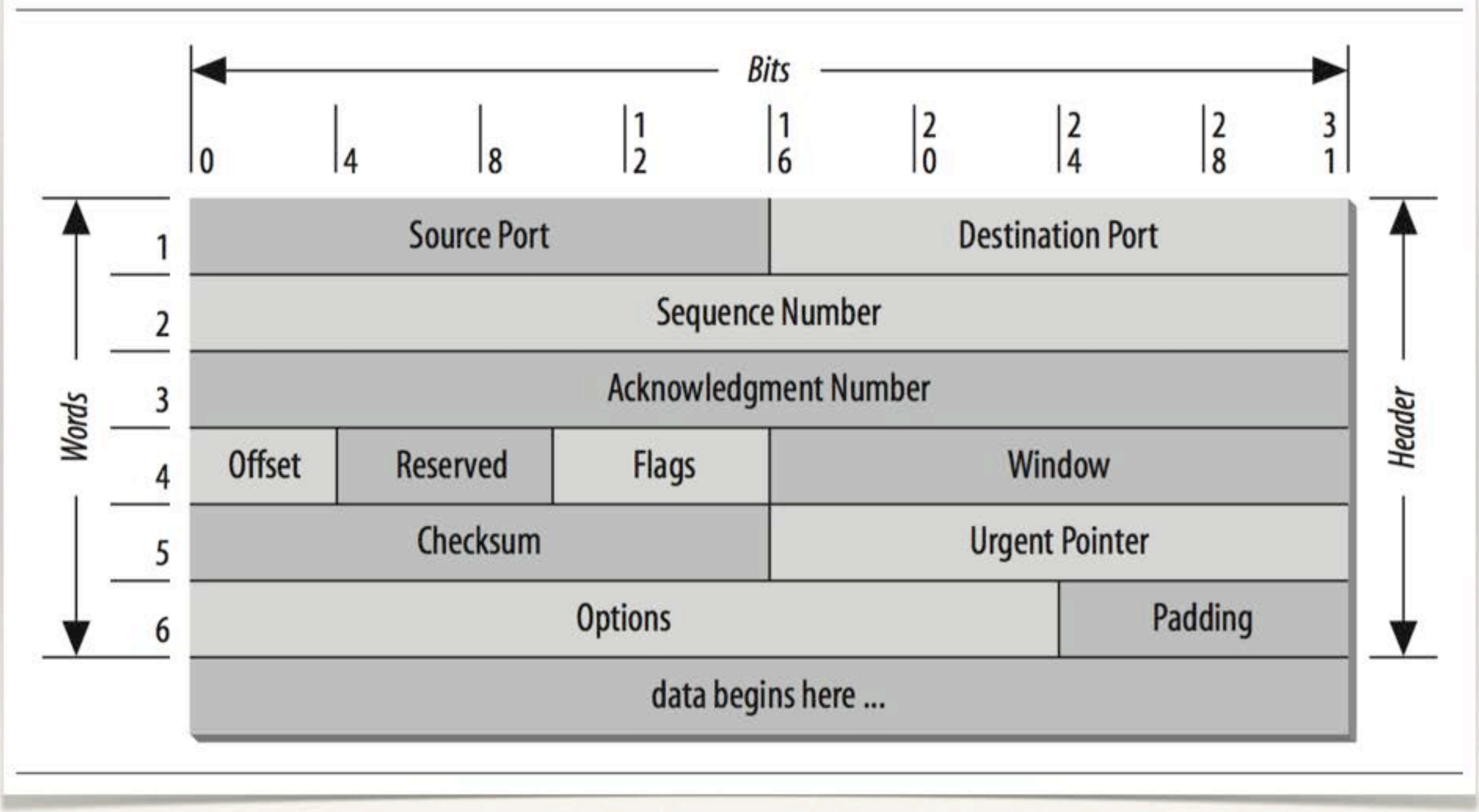
Hunt p14

segments
(transport layer)

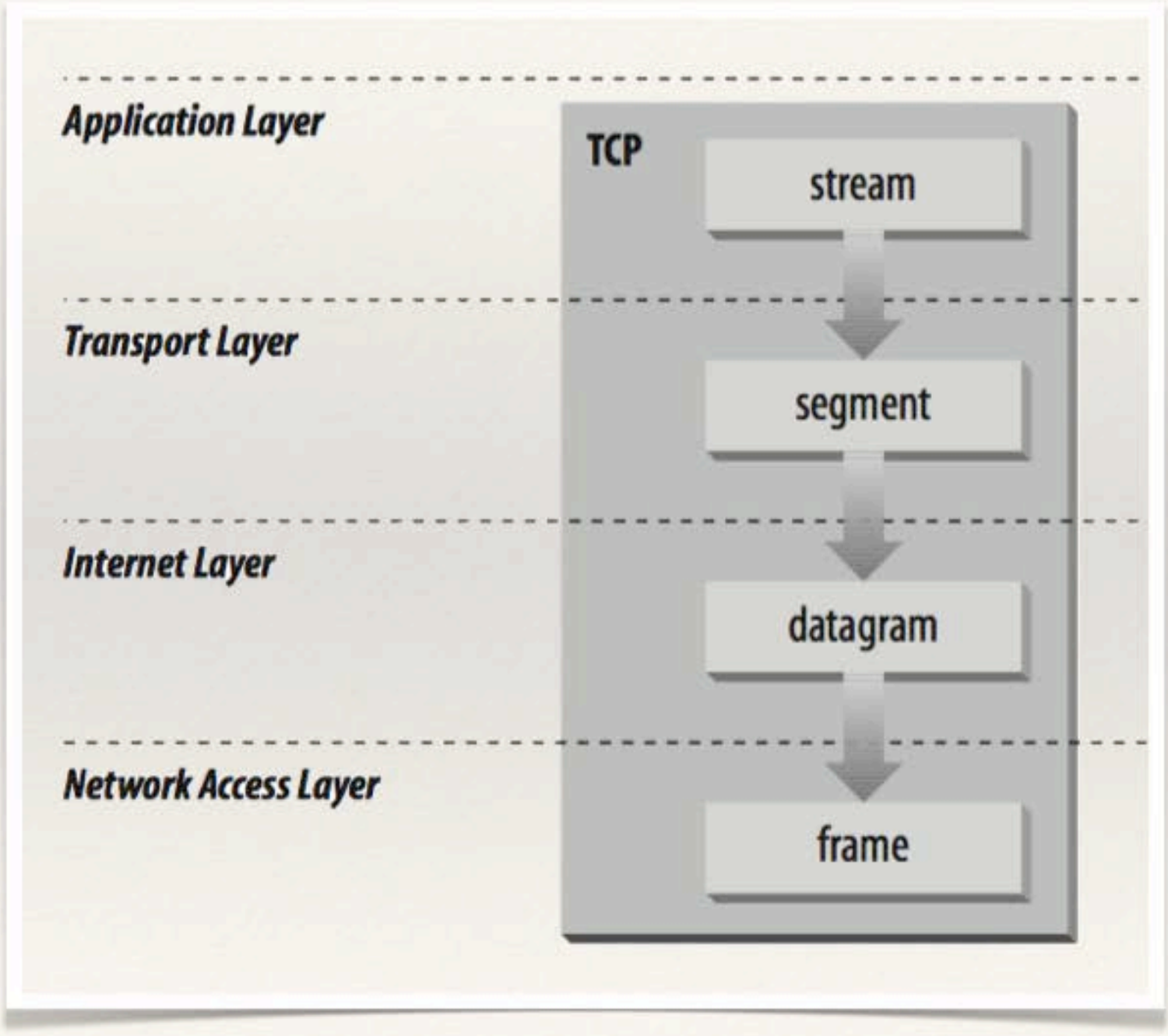
Positive Acknowledgment

- TCP provides **reliability** with a mechanism called **Positive Acknowledgment** with Re- transmission (PAR). Simply stated, a system using PAR sends the data again unless it hears from the remote system that the data arrived OK.
- The unit of data exchanged between cooperating TCP modules is called a **segment** (see next slide). Each segment contains a **checksum** that the recipient uses to verify that the data is undamaged.
  - If the data segment is received undamaged, the receiver sends a positive **acknowledgment** back to the sender.
  - If the data segment is damaged, the receiver discards it. After an appropriate timeout period, the sending TCP module re-transmits any segment for which no positive acknowledgment has been received.

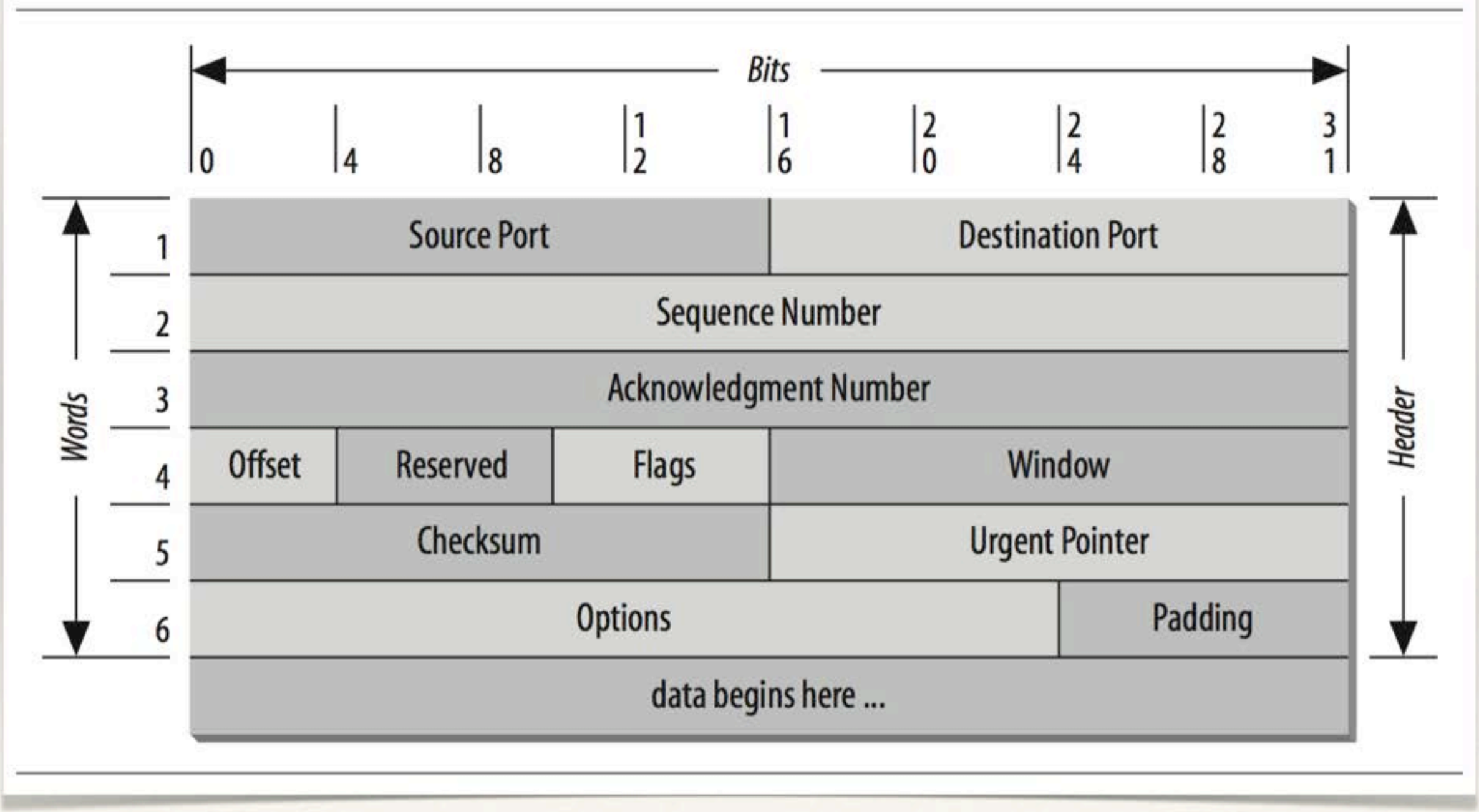
TCP/IP segment



TCP/IP segment



TCP/IP segment



Digression on the checksum

Checksum

- The checksum is a computation based on all the binary values of the message.
- One example of a simple computation for a checksum is to add up the number of 1 bits in the message. For instance, if a binary message consists of 256 bits, and 104 of those are 1s and the remaining 152 are 0s, then the checksum would be 104.
- There are a number of different checksum algorithms including fingerprints, randomization functions and cryptographic functions.
- All those possible computations (algorithms) must have one characteristic: the probability that two different sets of data (segments) give the same checksum must be low.

Fox p351

Checksum

- In other words, the sender computes the checksum, and attaches it to the segment (in the header).
- The receiver computes again the checksum, on the segment he has received.
- If the data has been changed (corrupted) during the transmission, the checksum computed by the receiver is different from the one computed by the sender.
- On the other hand, if the if the checksum computed by the receiver is equal to the one computed by the sender, there is an high probability that the data have not been corrupted during the transmission.

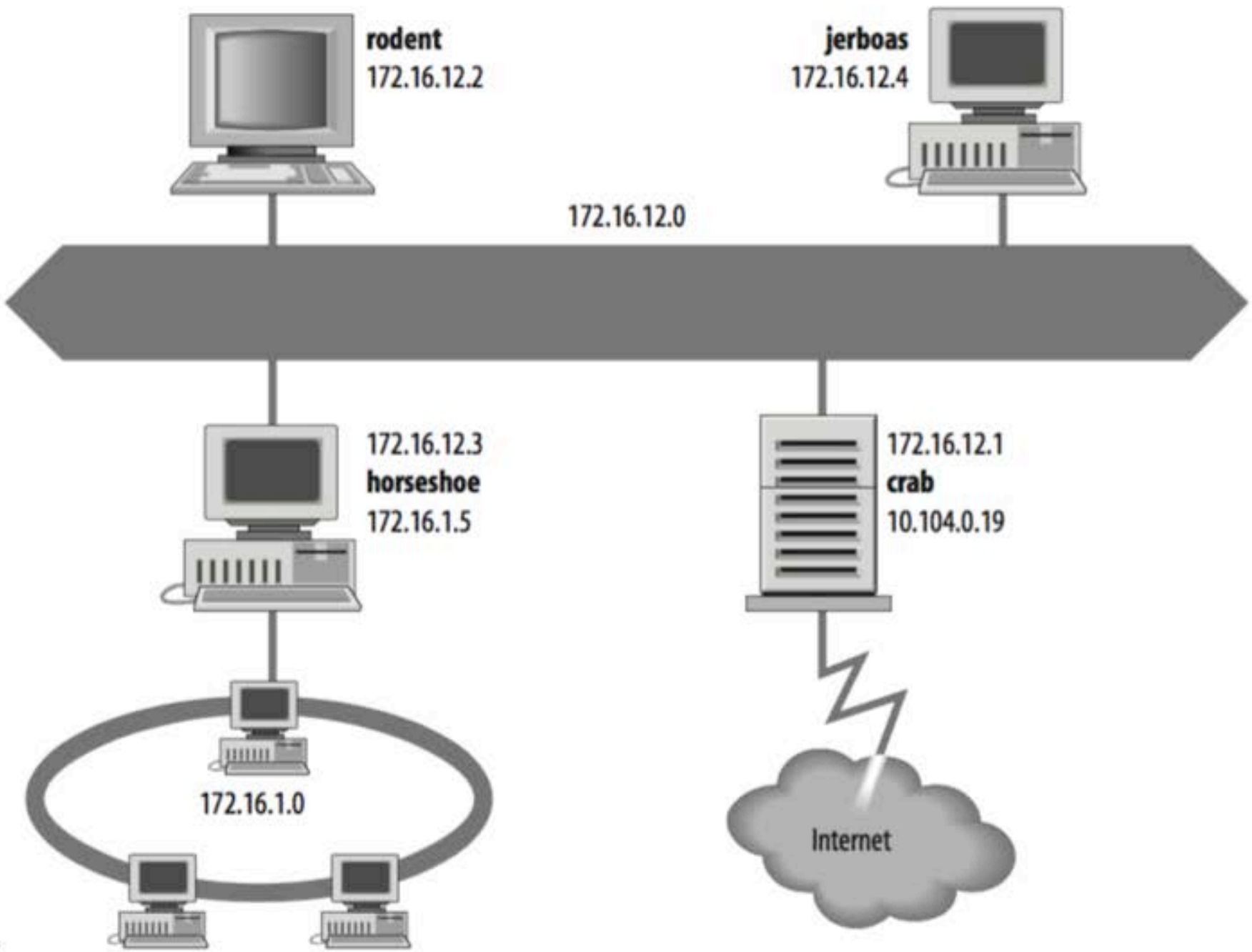
Addresses

The IP Address

- An IP address is a 32-bit value that uniquely identifies every device attached to a TCP/IP network.
- IP addresses are usually written as four decimal numbers separated by dots (periods) in a format called dotted decimal notation.
- Each decimal number represents an 8-bit byte of the 32-bit address, and each of the four numbers is in the range 0–255 (the decimal values possible in a single byte).


Hunt p25

The IP Address



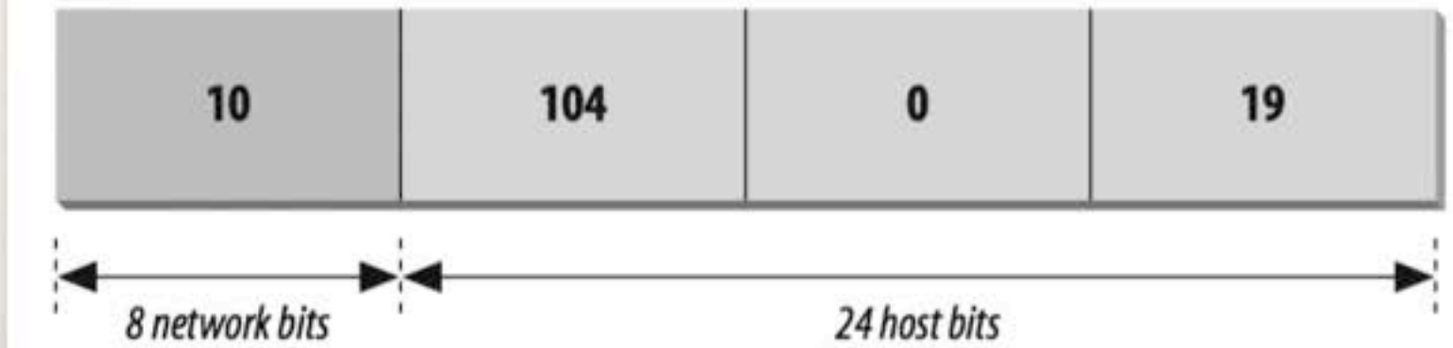
Hunt p25

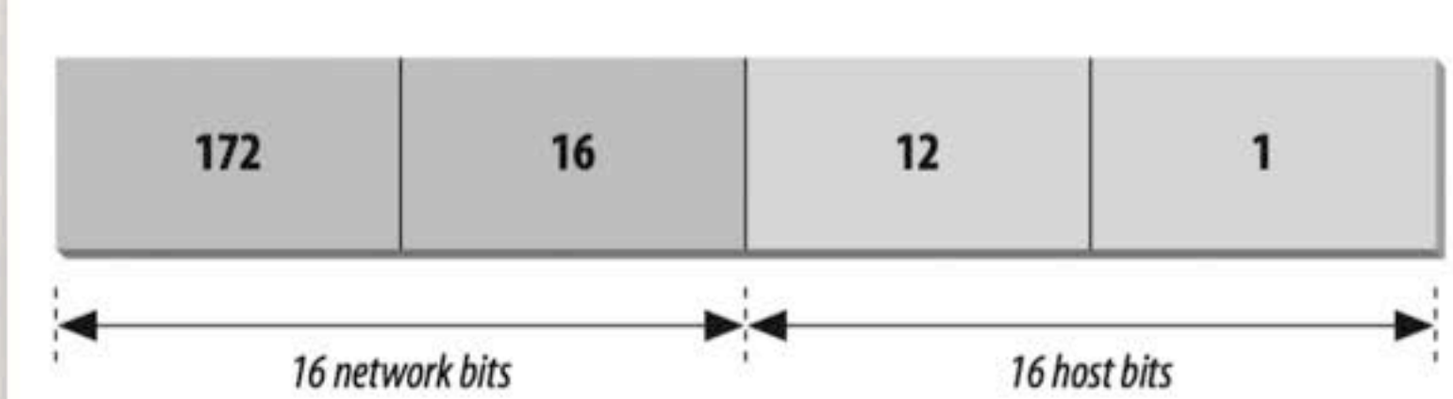
The IP Address

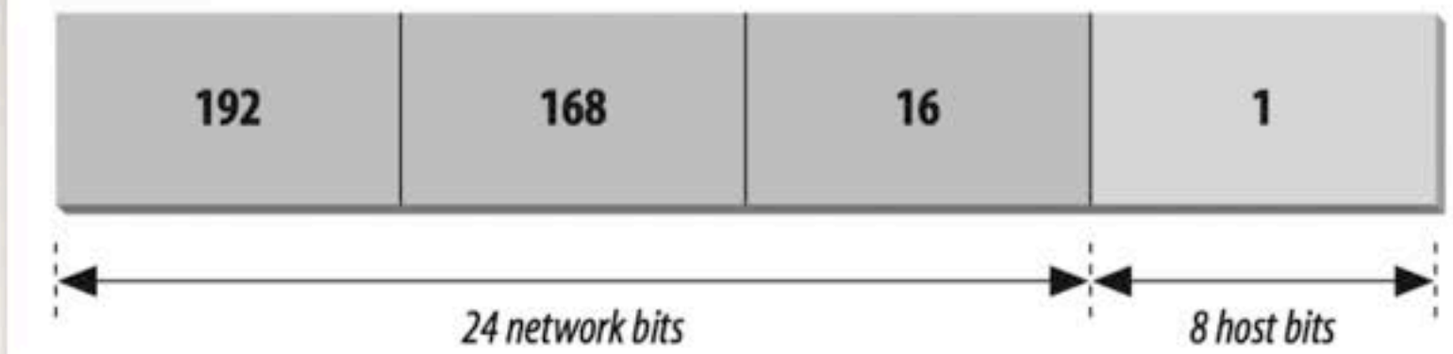
- An IP address contains a **network part** and a **host part.**
- The number of address bits used to identify the **net- work** and the number used to identify the **host** vary according to the **prefix length** of the address.
- The prefix length is determined by the **address bit mask.**
- The address bit mask is interpreted like this:
  - if a bit is **on** in the mask, that corresponding bit in the address is interpreted as a **network bit;**
  - if a bit in the mask is **off,** the corresponding in the address is interpreted as a **host bit.**
- Example:
  - address 172.22.12.4 is given the
  - network mask 255.255.255.0,
  - the first 24 bits (first three bits, i.e. decimal numbers) are the **network number** and
  - the last 8 bits are the **host address.**
  - This tells us that this is the address of **host 4** on network 172.22.12.

Hunt p25

The IP Address

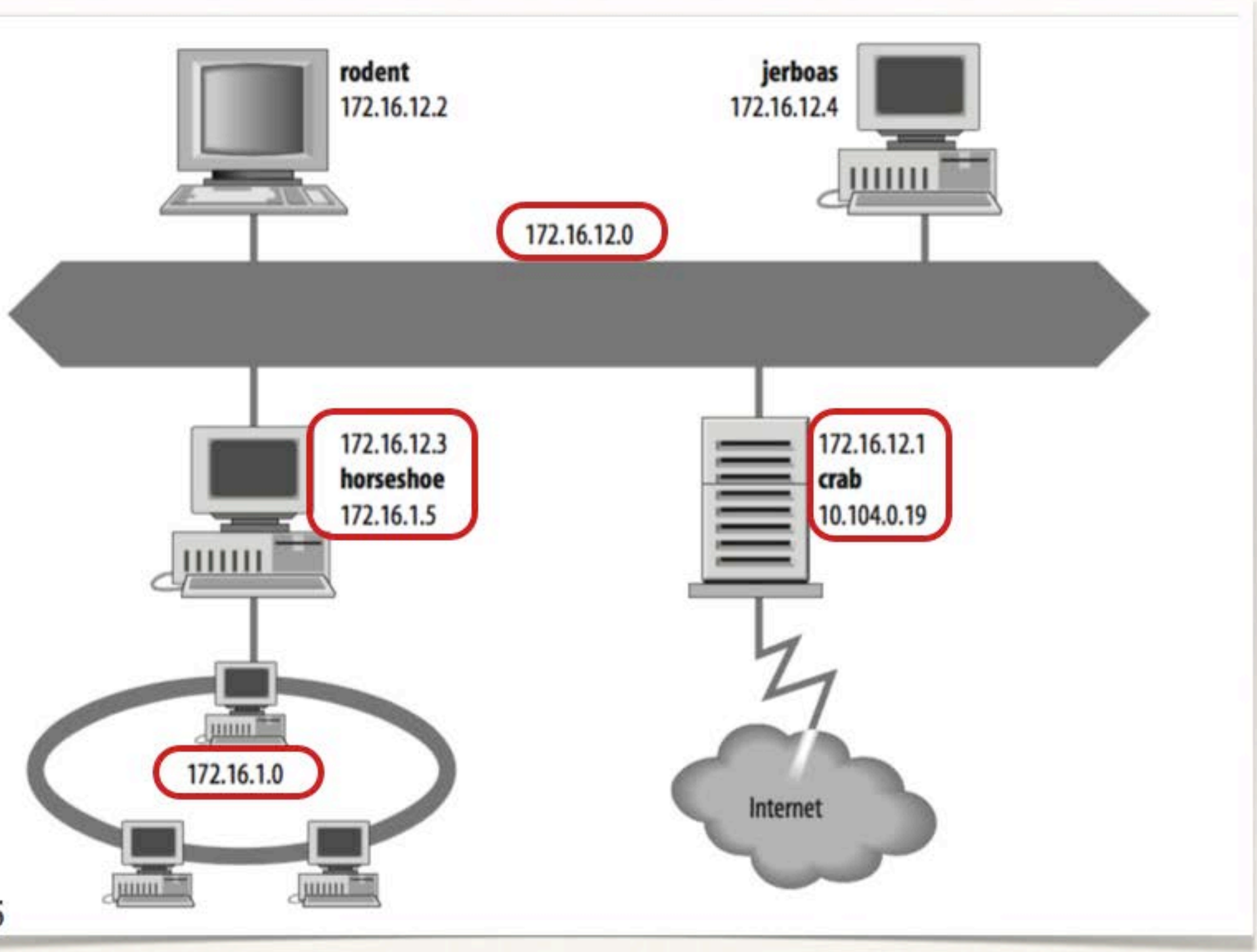






Hunt p31

The IP Address



Hunt p25

Routing

dictionary

route | rōōt rout |

noun

a way or course taken in getting from a starting point to a destination: *the most direct route is via Los Angeles.*

- the line of a road, path, railroad, etc.

- *N. Amer.* a circuit traveled in delivering, selling, or collecting goods.

- a method or process leading to a specified result: *the many routes to a healthier diet will be described.*

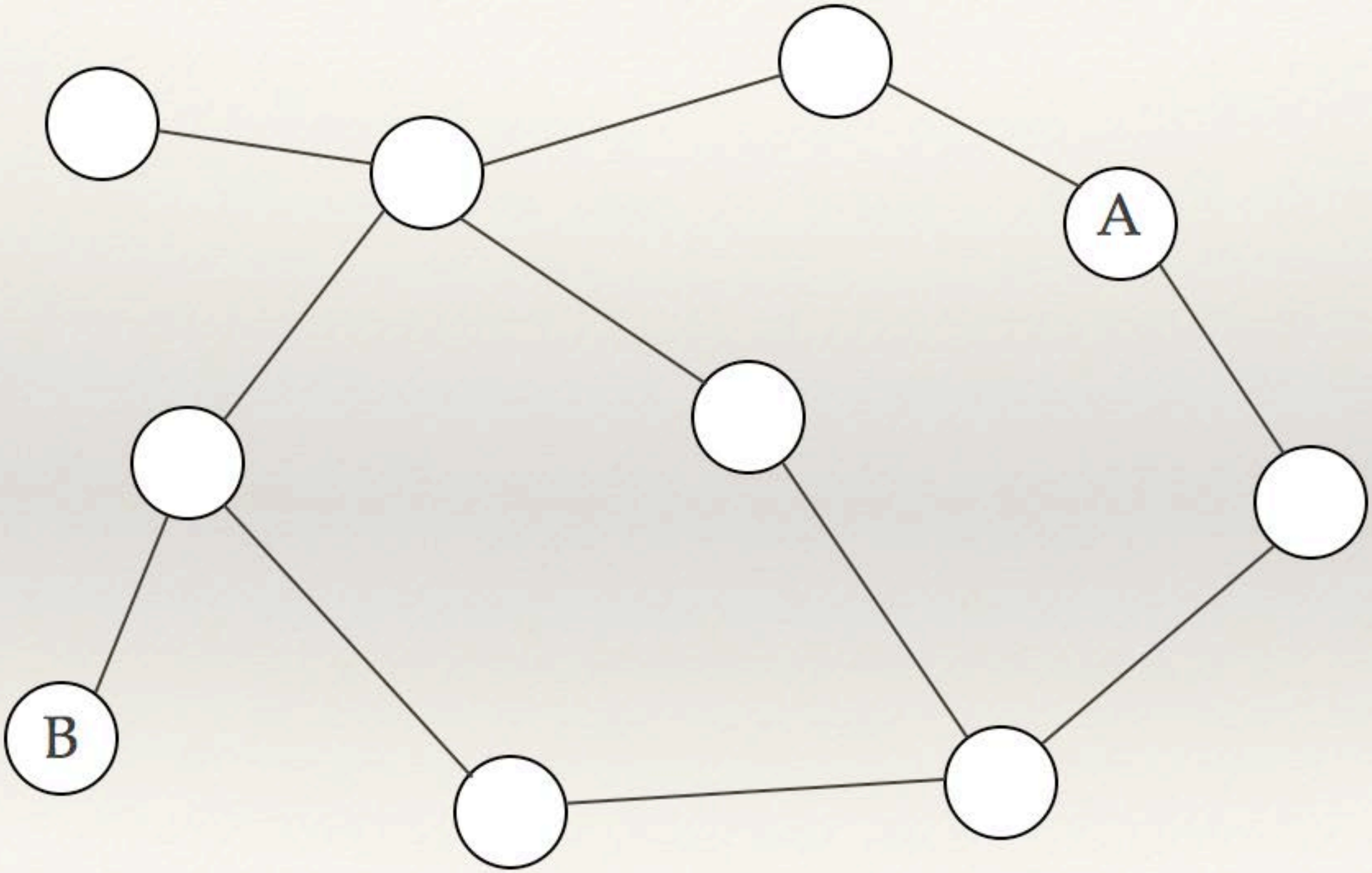
verb (**routes, routing** or *Brit.* **routeing, routed**) *[with obj.]*

send or direct along a specified course: *all lines of communication were routed through Atlanta.*

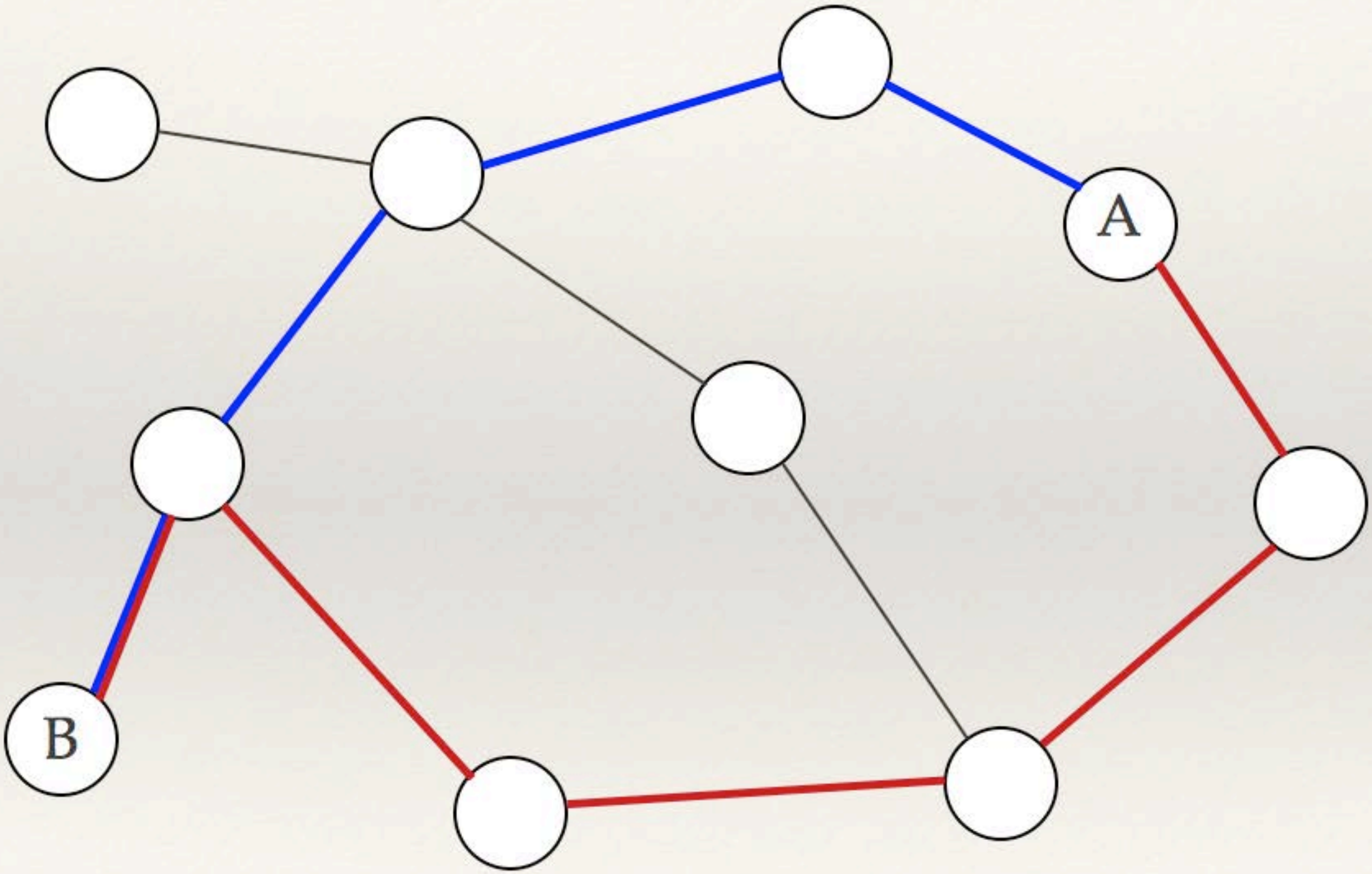
ORIGIN

Middle English: from Old French *rute* **'road,'** from Latin *rupta (via)* **'broken (way),'** feminine past participle of *rumpere* .

Routing



Routing



Old routing architecture

- When the Internet was created, the ARPAnet was the backbone of the network: a central delivery medium to carry long-distance traffic. This central system was called **the core**, and the centrally managed the whole routing architecture.
- Routing information about all of the networks on the Internet was passed into the core gateways. The processed routing information was then passed back out to the external gateways. The core gateways maintained accurate routing information for the entire Internet.
- Major weakness: every route must be processed by the core.
- This routing model does not "scale well".


Hunt p36

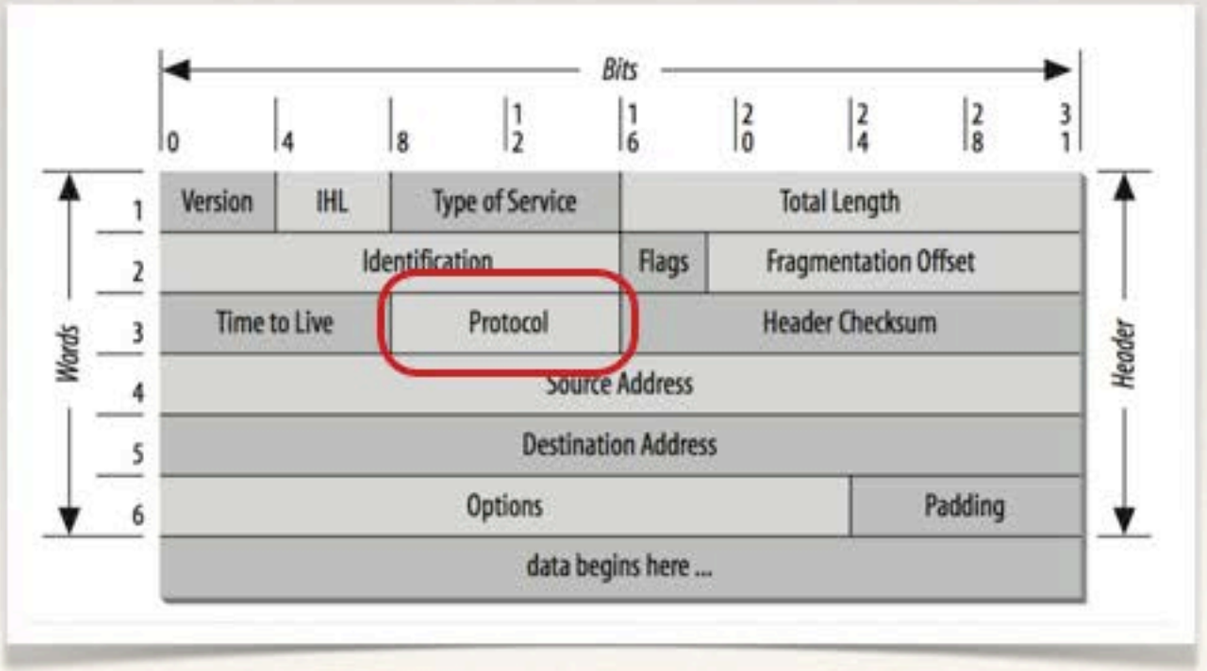
New routing architecture

- The new routing model is based on co-equal collections of **autonomous** systems called routing domains.
- Each routing domain processes the information it receives from other domains.
- This model does not depend on a single core system **to choose the "best" routes**. Each routing domain does this processing for itself; therefore, this model is more expandable.
- Gateways route data between networks, but all network devices, hosts as well as gateways, must make **routing decisions**. For most hosts, the routing decisions are simple:
  - If the destination host is on the **local network**, the data is delivered to the destination host.
  - If the destination host is on a **remote network**, the data is **forwarded** to a **local gateway**.

Hunt p36

Protocols

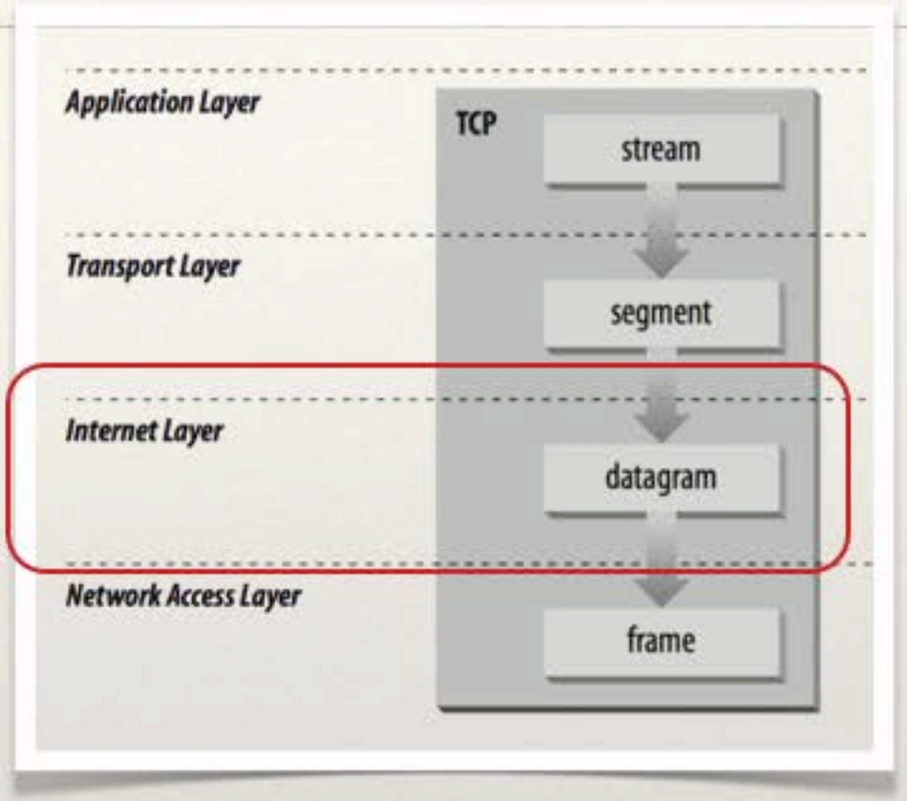
- Once data is routed through the network and delivered to a specific host, it must be delivered to the correct user or process.
- The **protocol number** is a single byte in the third word of the datagram header.

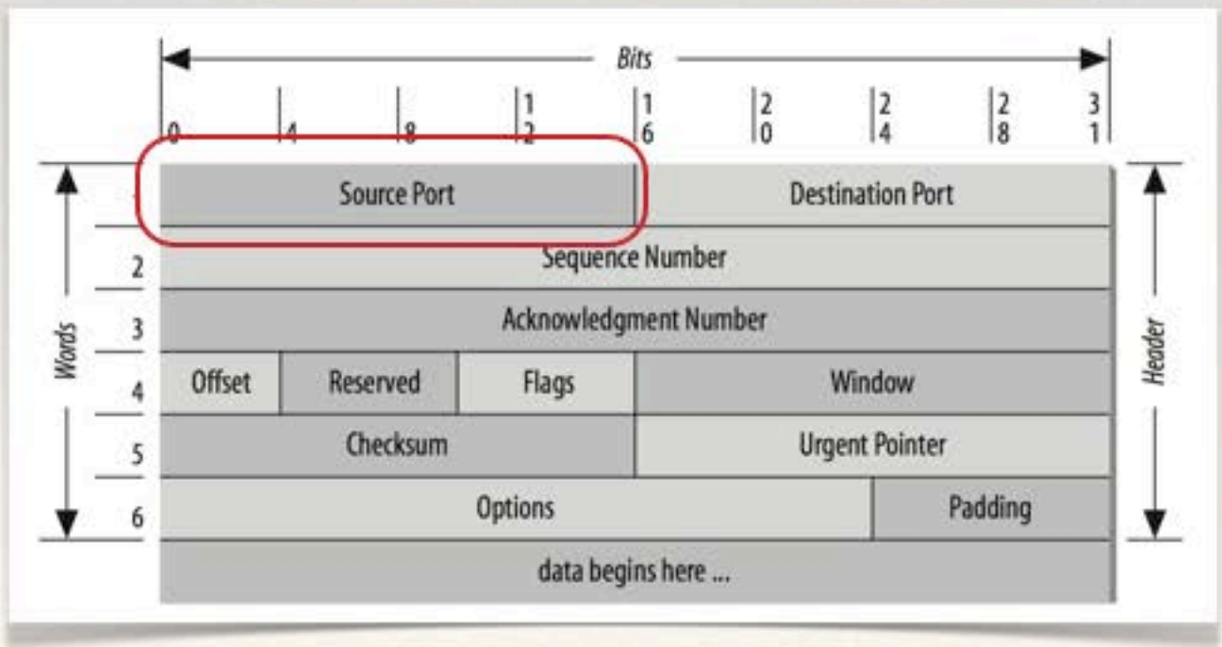


Hunt p44

Ports

- After **IP** (internet protocol) passes incoming data to the **transport protocol**, the transport protocol passes the data to the correct **application process**.
- Application processes are identified by **port numbers**, which are 16-bit values.
- The **source port number**, which identifies the process that sent the data, and the **destination port number**, which identifies the process that will receive the data, are contained in the first header word of each TCP segment and UDP packet.





Hunt p44

Sockets

- Well-known ports are standardized port numbers that enable remote computers to know which port to connect to for a particular network service.
- A second type of port number called a **dynamically allocated port**, which are not pre-assigned; they are assigned to processes when needed.
- The system ensures that it does not assign the same port number to two processes, and that the numbers assigned are *above the range of well-known port numbers*, i.e., above **1024**.
- The **combination** of an IP address and a port number is called a **socket**. A socket uniquely identifies a single network process within the entire Internet. Sometimes the terms "socket" and "port number" are used interchangeably.

Hunt p44

DNS

DNS

- In most cases, **hostnames** and **numeric addresses** can be used interchangeably. A user wishing to see a webpage at IP address 172.16.12.2 can enter:

```
http://172.16.12.2
```

- or use the hostname associated with that address and enter the equivalent command:

```
http://rodent.wrotethebook.com
```

- There are two common methods for translating names into addresses. The **older method** simply looks up the hostname in a table called the host table. The **newer technique** uses a distributed database system called the **Domain Name System (DNS)** to translate names to addresses.
- The old host table system is inadequate for the global Internet for two reasons: **inability to scale** and lack of an **automated update process**.

Hunt p51

DNS

- DNS is a distributed hierarchical system for resolving **hostnames** into **IP addresses**.
- Under DNS, there is no central database with all of the Internet host information. The information is distributed among thousands of **name servers** organized into a **hierarchy** similar to the hierarchy of the OS filesystem.
- DNS has a **root domain** at the top of the domain hierarchy that is served by a group of name servers called the root servers.
- Just as directories in the OS filesystem are found by following a **path** from the **root directory** through subordinate directories to the **target directory**, information about a domain is found by tracing pointers from the root domain through subordinate domains to the target domain.
- Directly under the root domain are the top-level domains. There are two basic types of top-level domains—**geographic** and **organizational**.

Hunt p55

DNS

- Examples of generic top-level domains are:
- organizational

    `com` - Commercial organizations

    `edu` - Educational institutions

    `gov` - Government agencies

    `mil` - Military organizations

    `net` - Network support organizations
- geographic

    `ru` - Russia

    `it` - Italy

    `uk` - United Kingdom

Hunt p55