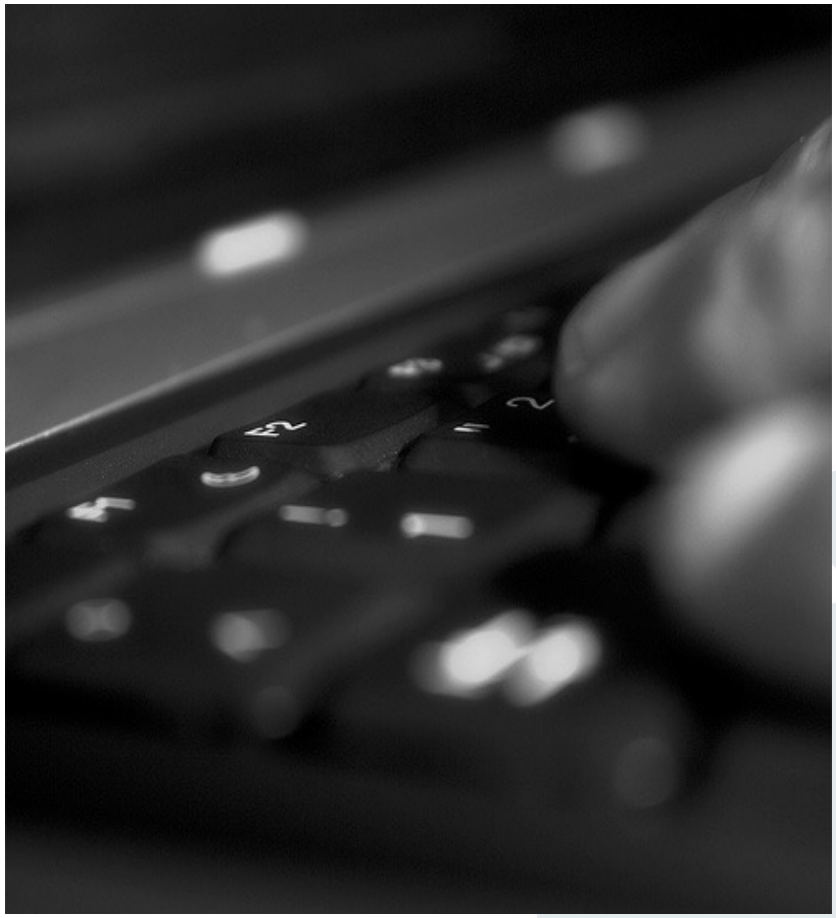
Chair of Mobile Business & Multilateral Security

Mentorium 3
Business Informatics 2 (PWIN)

Communication Systems I & II

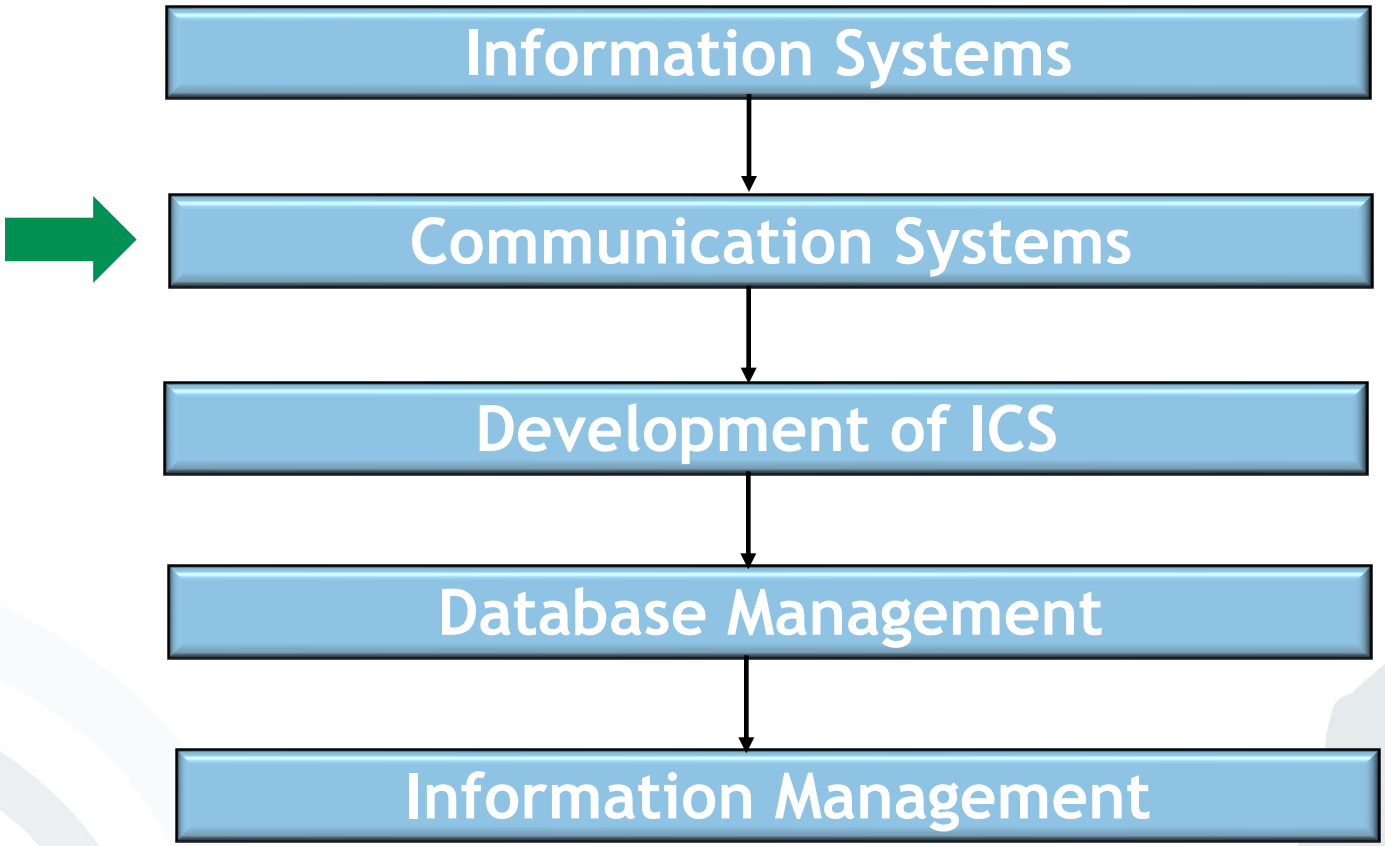
WS 2023

Frédéric Tronnier
www.m-chair.de

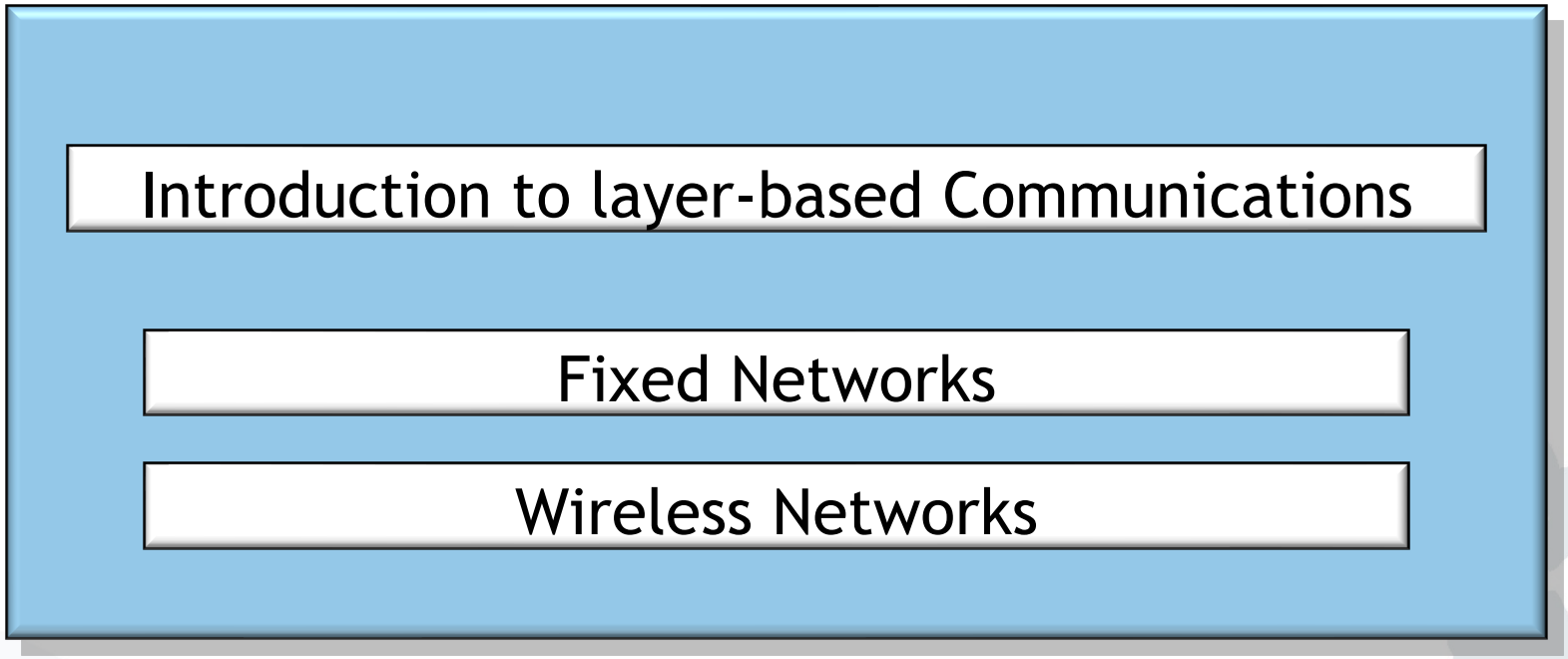


Jenser (Flickr.com)

Components of the Course Business Informatics II (PWIN)



Components of the Course



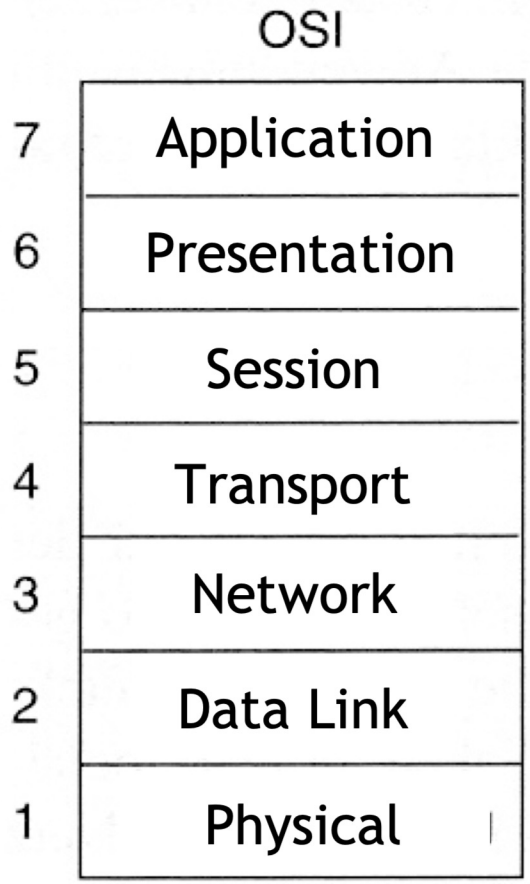
Agenda

- Exercise 1: OSI reference model
- Exercise 2: Fixed Networks
- Exercise 3: Wireless Local Area Networks
- Exercise 4: Bluetooth and NFC

Exercise: TCP vs. UDP

- In which layer are TCP and UDP used? What is the main difference between them?
- Please describe the three way handshake (TCP).
- Should myPlace use TCP or UDP? Why?

Keywords for OSI reference model layers



SMTP, HTTP

Encryption, Compression

Session

TCP (3 way handshake), UDP

Routing, IP address

Frames, MAC

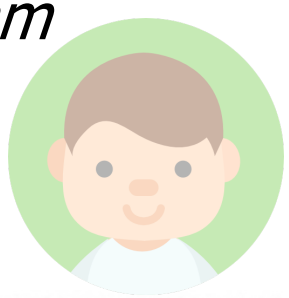
Bits, LAN cable, optical fibre, air

Exercise 2b): Solution

Eva

?

Adam



Application
Presentation
Session
Transport
Network
Data Link
Physical

TCP is used to ensure an ordered and complete transfer of the data. For this it is divided into smaller segments and source and destination are added.

Application
Presentation
Session
Transport
Network
Data Link
Physical

Layer 4: Transport Layer
Transmission Control Protocol (TCP)

- The Transmission Control Protocol (TCP) was especially designed in order to provide a reliable and connection-oriented transportation of a byte-stream (from endpoint to endpoint) through unreliable networks.

- TCP is defined in RFC 793 (September 1981).
- Functions:
  - Data Segmentation
  - Connection Establishment and Termination
  - Error Detection
  - Flow Control

Source: Tanenbaum (2006), p. 573

Layer 4: Transport Layer Transmission Control Protocol (TCP)

- Properties of TCP
  - Reliable
    - Data communication is repeated until the remote station acknowledges the receipt.
  - Connection-oriented
    - Before the actual data transfer begins, during setup of a TCP connection by 3-way handshake, a logical end-to-end connection between sender and receiver is established.
  - Makes it possible to send information directly to an application (ports).

Source: Tanenbaum (2006), p. 573

Layer 4: Transport Layer
User Data Protocol (UDP)

- User Data Protocol (UDP) is a connectionless, insecure transport protocol without assurance whether a data packet has been received by the remote party or not.
- UDP has the advantage of a reduced protocol overhead compared to the Transmission Control Protocol (TCP).
- UDP is used e.g. for the Domain Name System (DNS, sometimes also known as Domain Name Service).

Source: Tanenbaum (2006) p. 573, Holtkamp (2002) p. 40-41

Exercise: TCP vs. UDP

- Please describe the three way handshake (TCP).
- Should myPlace use TCP or UDP? Why?

Exercise: Layer 4: Transport Layer 3-Way Handshake (TCP)

- Example from everyday life – making an appointment via correspondence

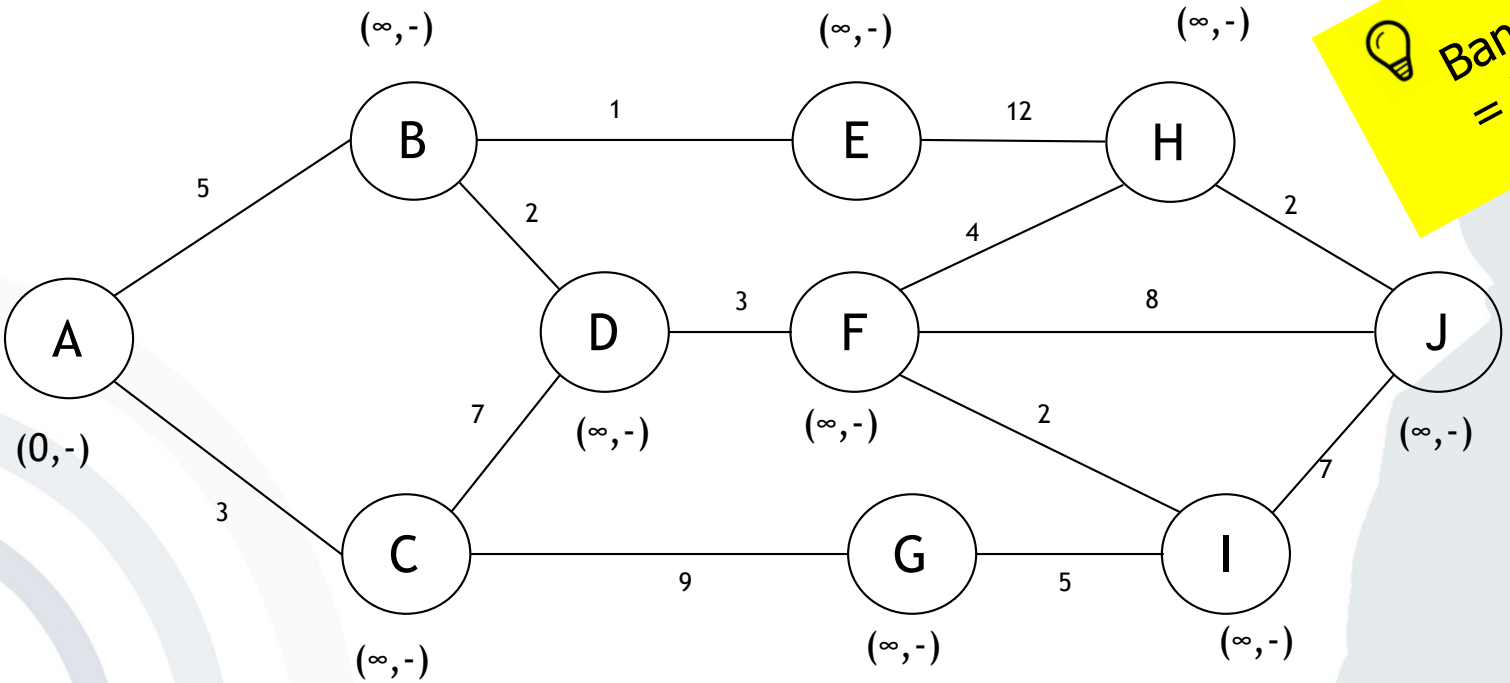
Prof. Rannenberg wants to make an appointment with Prof. König via correspondence.

1. Prof. Rannenberg sends a message to Prof. König to suggest an appointment date.
2. Prof. König confirms the appointment date by sending a message back to Prof. Rannenberg.
3. Prof. Rannenberg sends a message to Prof. König to let him know that he received the confirmation message.

Step 3 is necessary in order for Prof. König to know that Prof. Rannenberg has received the confirmation. Message No. 2 could have gotten lost and then Prof. König would show up alone for the meeting.

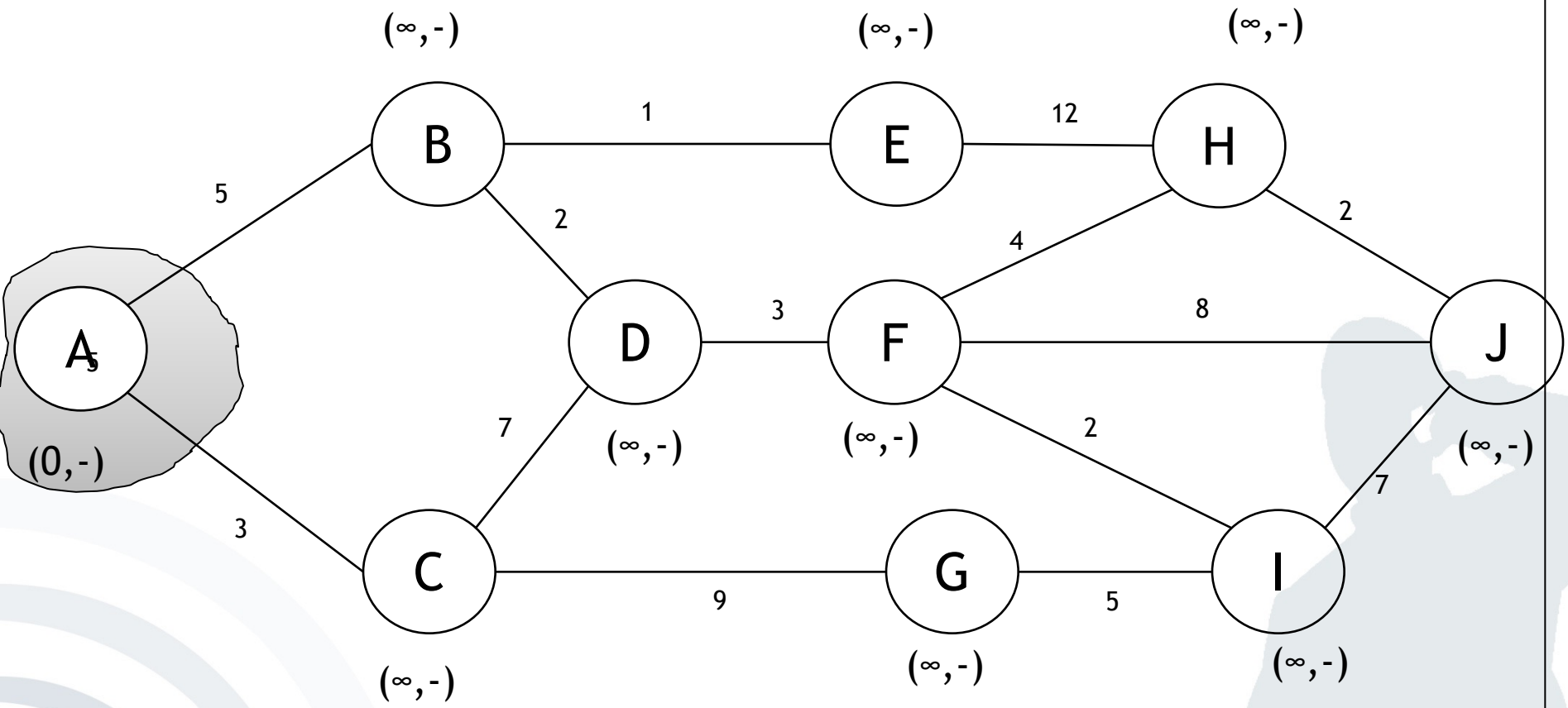
Exercise: Dijkstra Algorithm

- The following graphs shows the various systems a message from a place of interest needs to pass to get to the end user. Please calculate the fastest track. Note that lower case letters denote *system vertices* and the numbers the *bandwidth* of a connection.

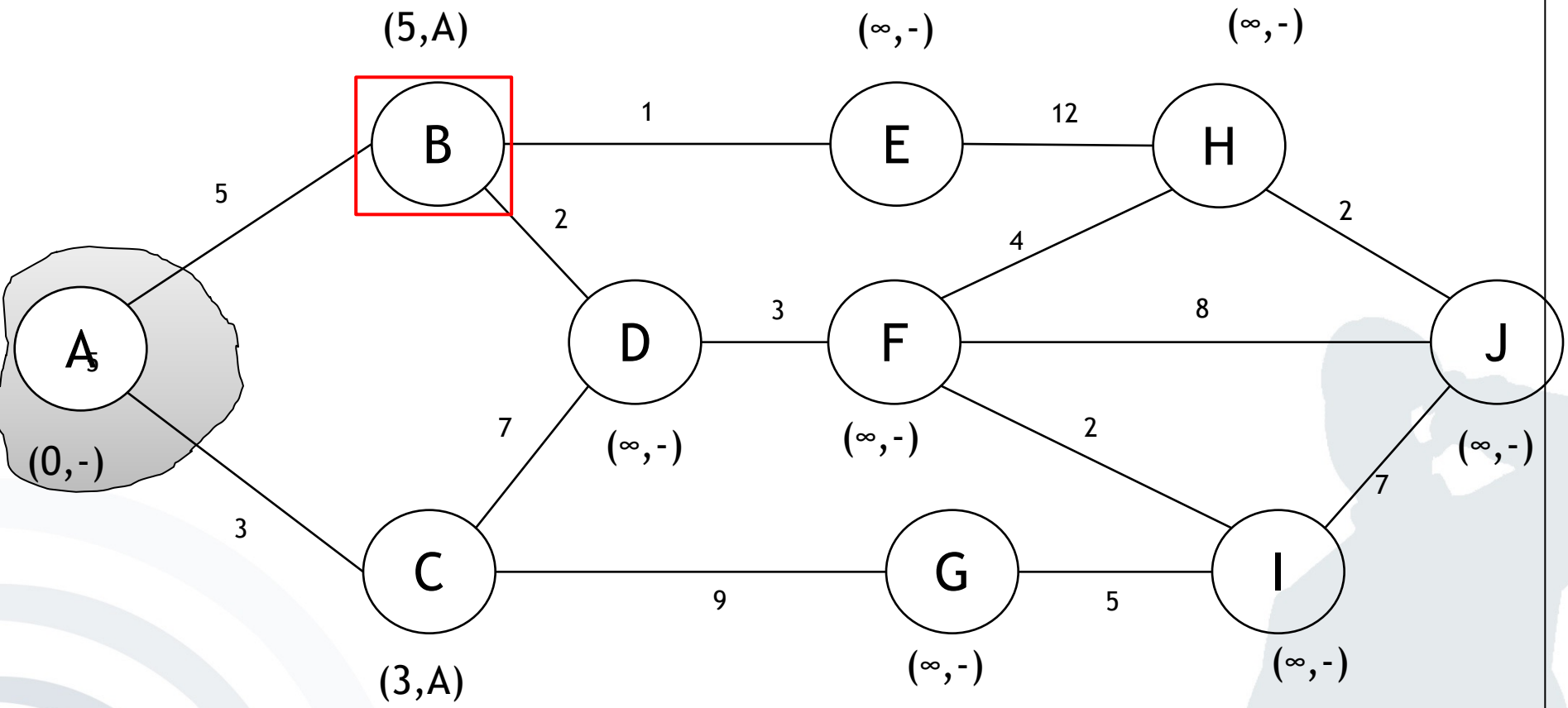


Bandwidth:
= longest path

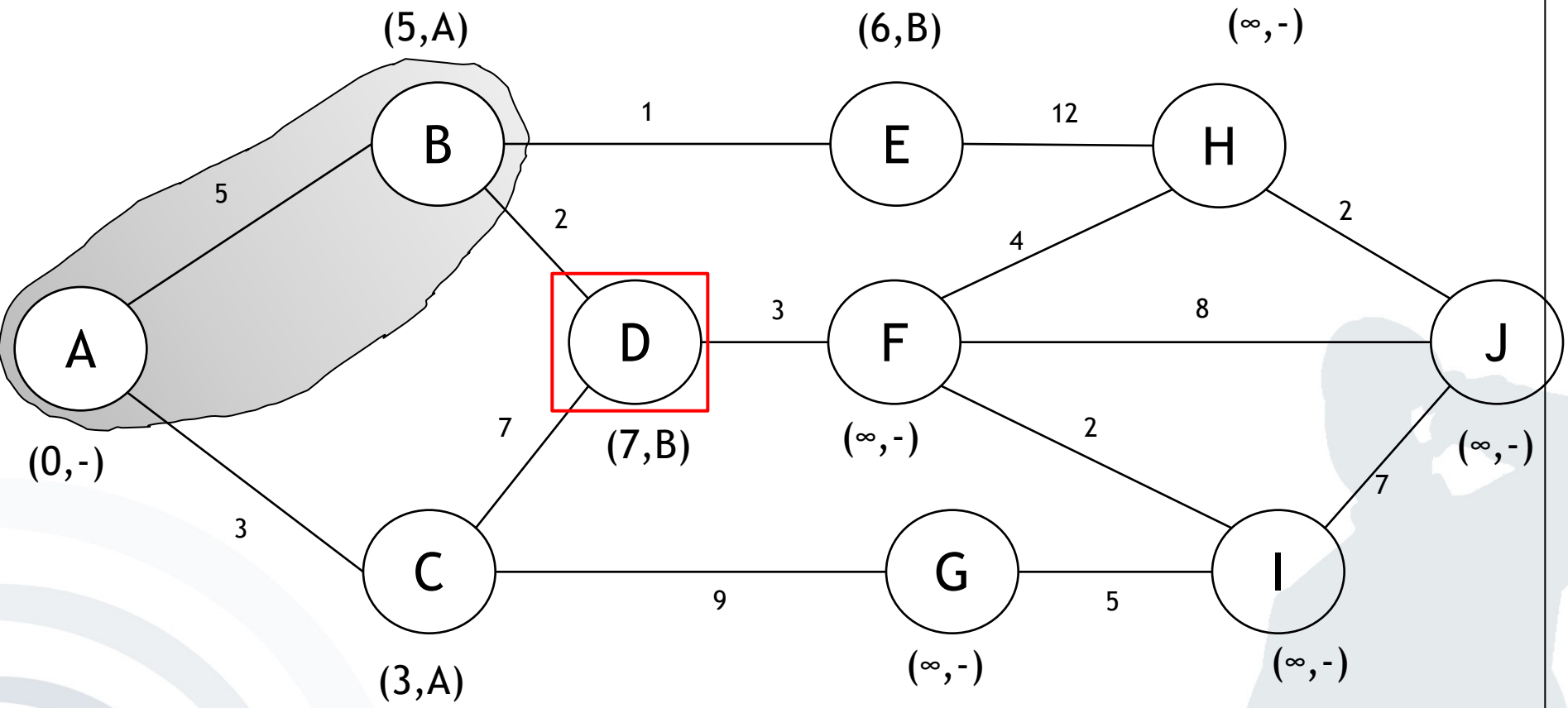
Dijkstra Algorithm



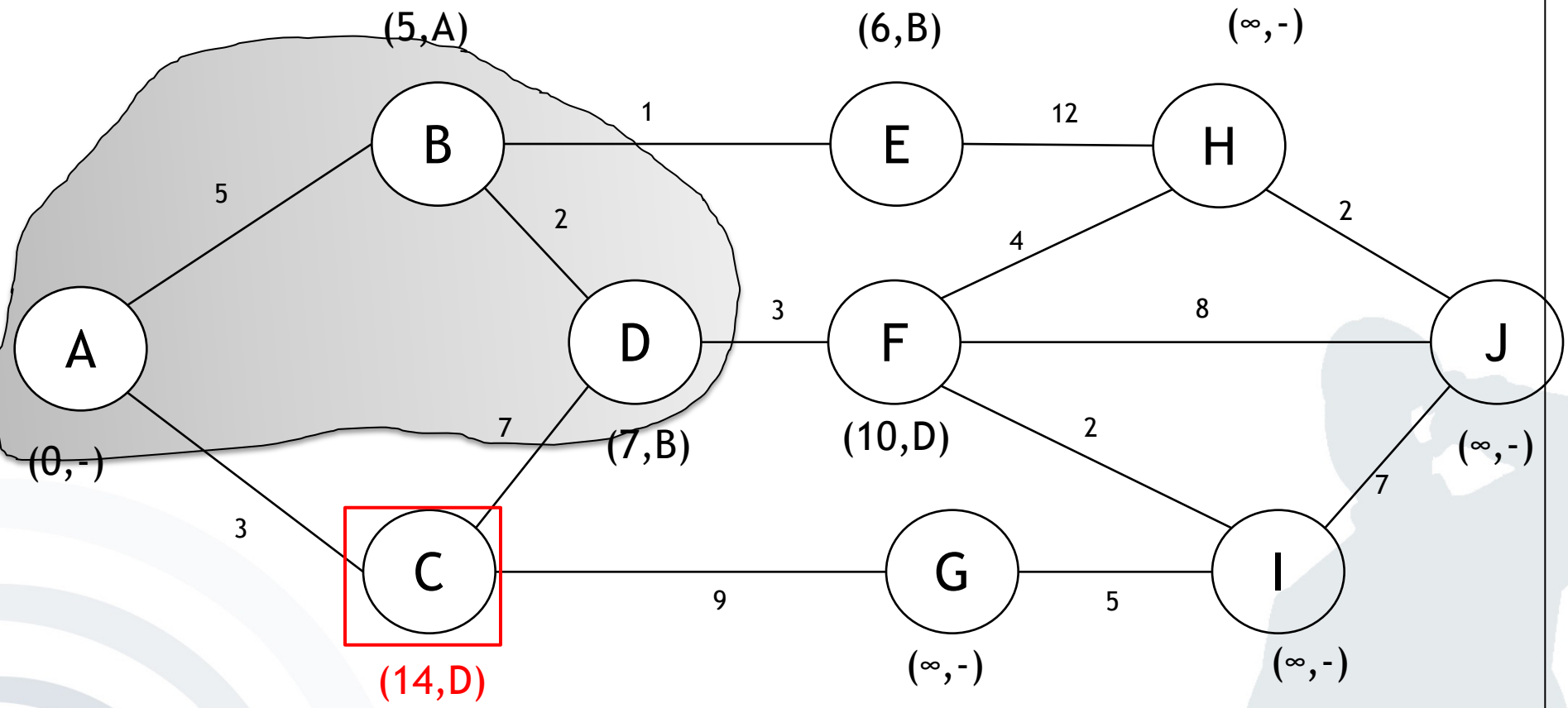
Dijkstra Algorithm



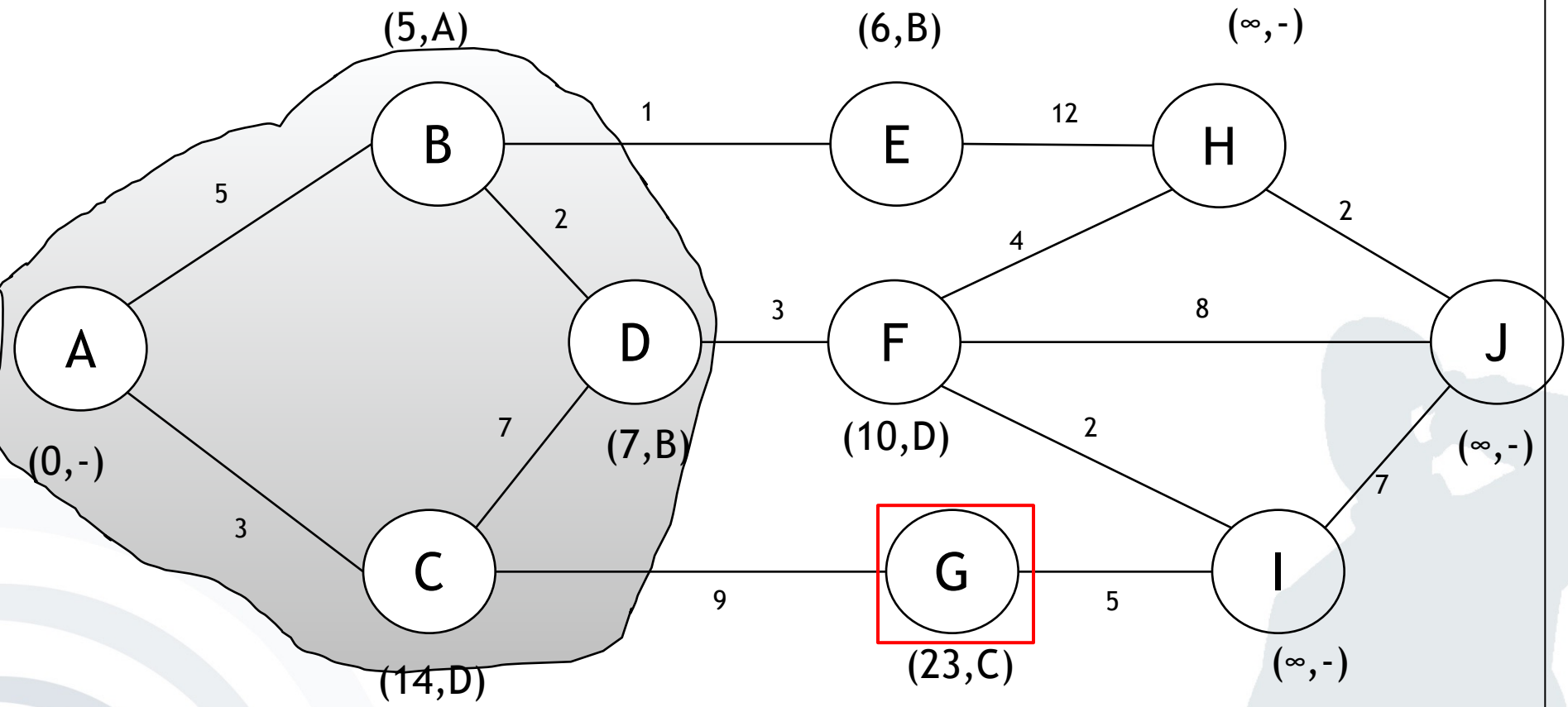
Dijkstra Algorithm



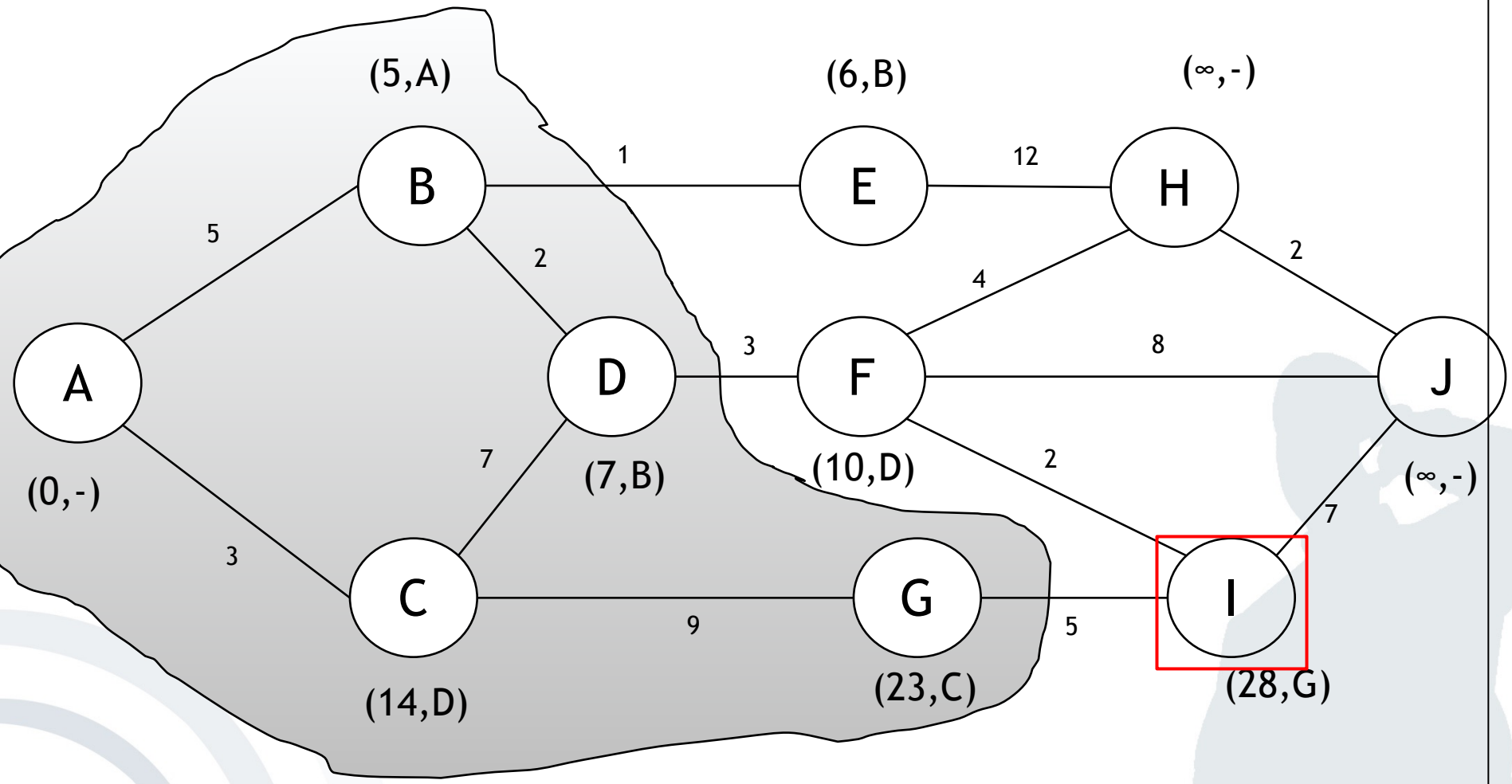
Dijkstra Algorithm



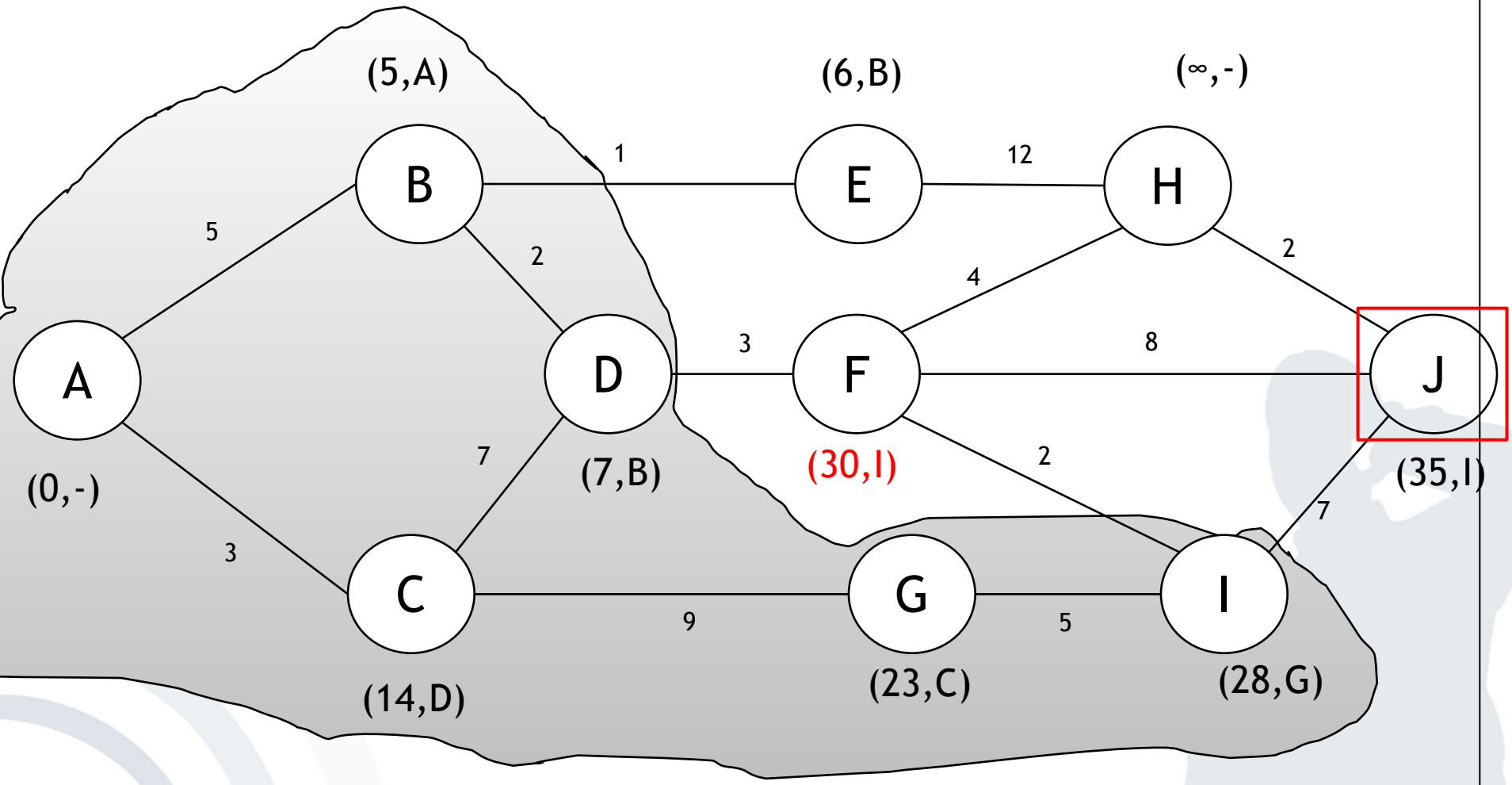
Dijkstra Algorithm



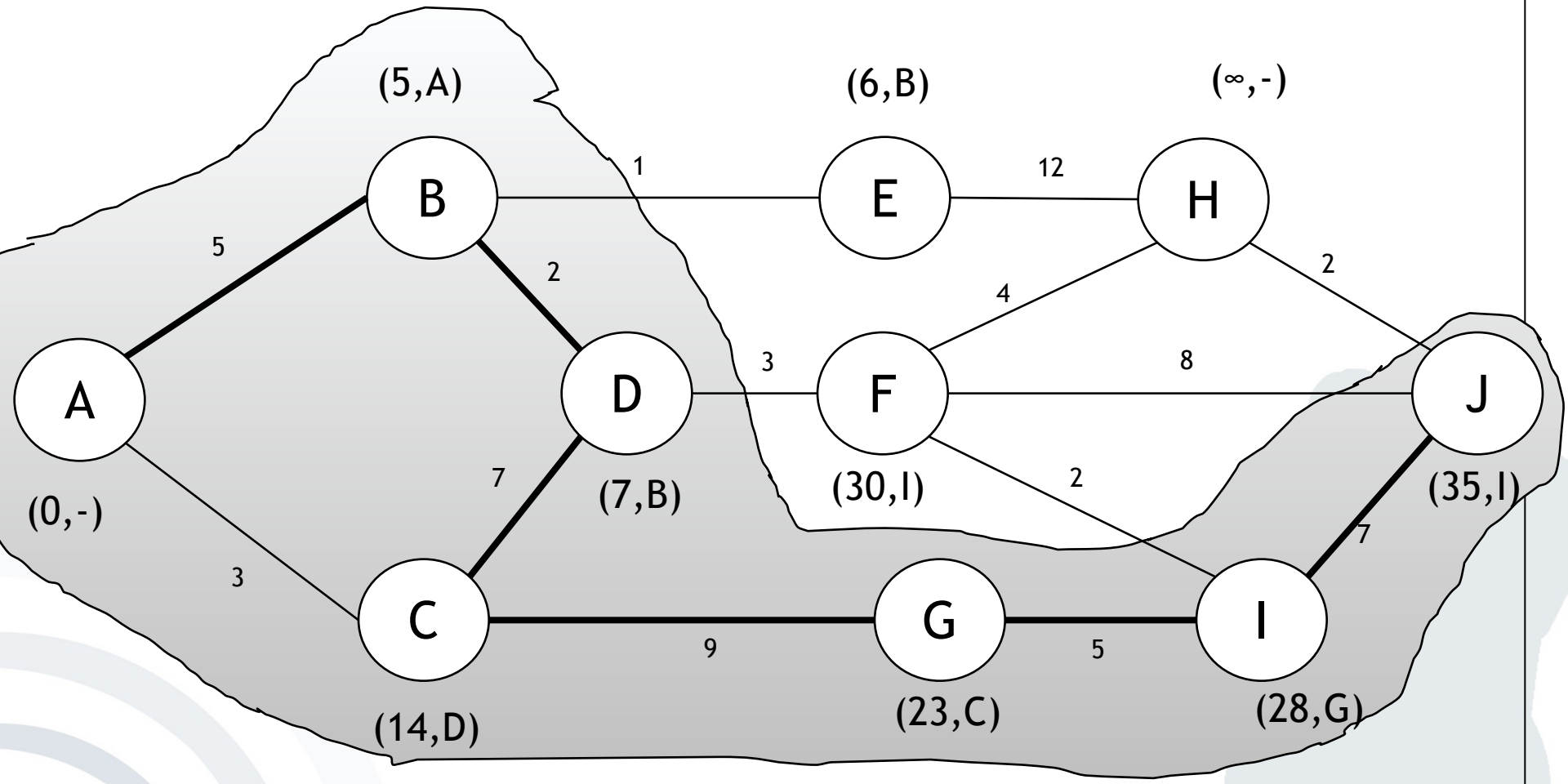
Dijkstra Algorithm



Dijkstra Algorithm



Dijkstra Algorithm



Best path: A → B → D → C → G → I → J

Dijkstra Algorithm - Conclusion

→ Diksta not created to find longest path – Possible that it does not find it

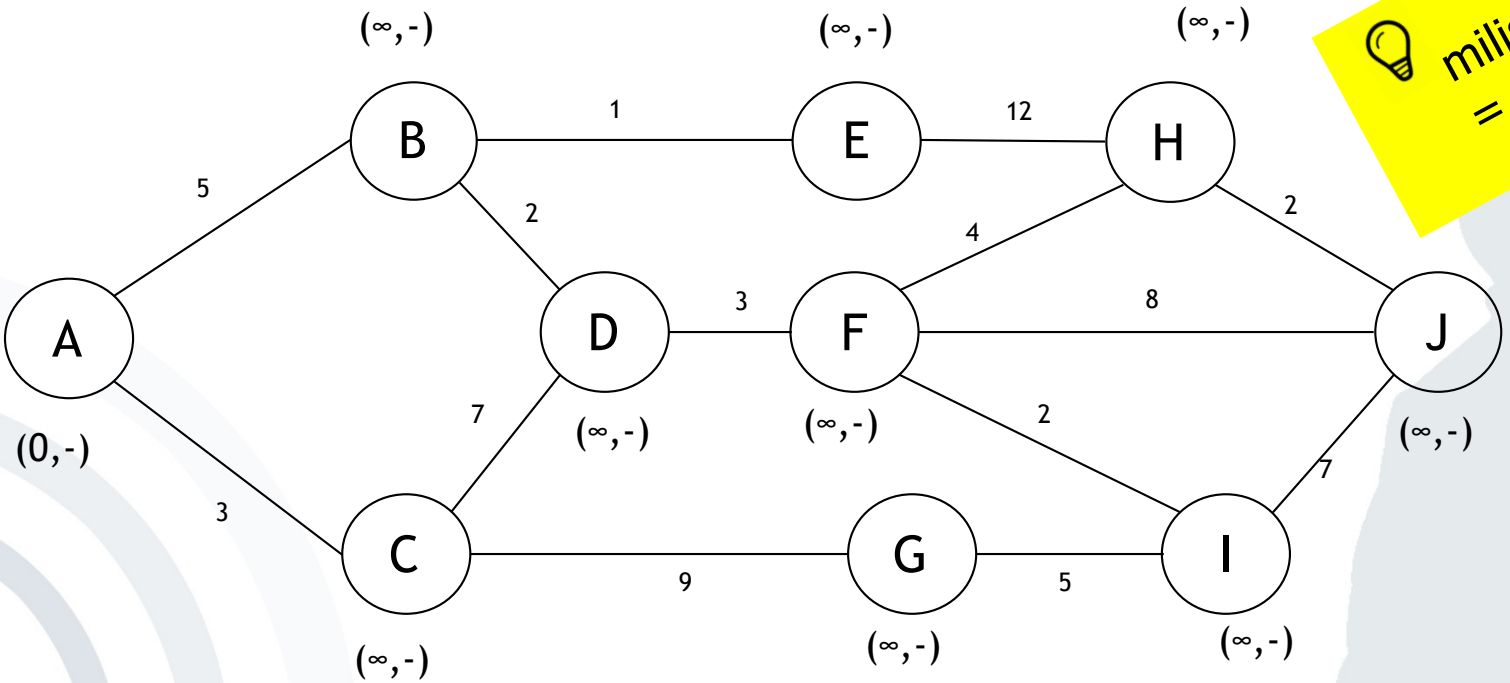
Now try to find the shortest path in the same graph:

Tips:

- Dijkstra only looks at neighbor knots of already visited knots
- Find nearest neighbor and visit it. Recalculate all paths to neighbor knots after each step. Repeat
- Brackets include the total length from starting point and the predecessor knot
- Shortest path can be found by looking at the predecessor knot in brackets, starting from the final knot

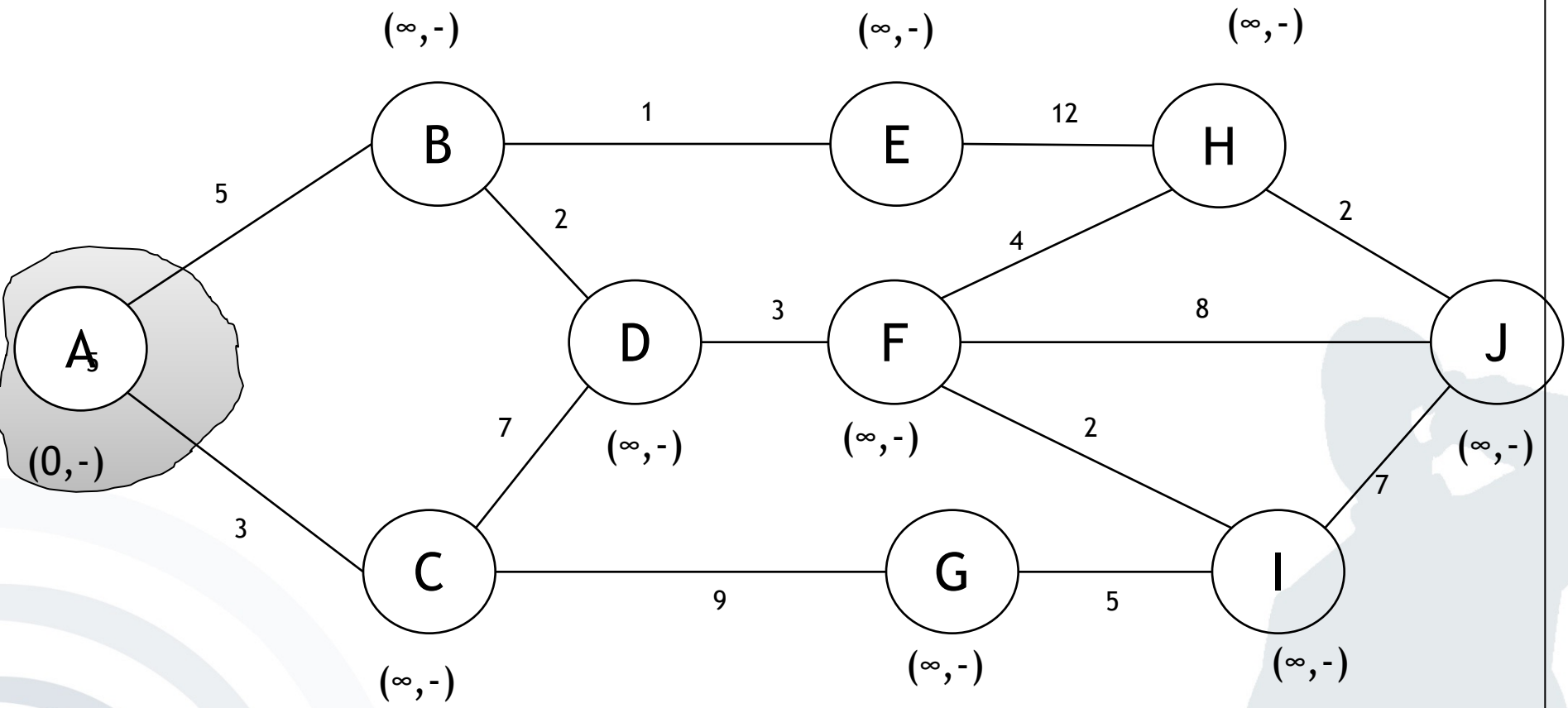
Exercise: Dijkstra Algorithm

- The following graphs shows the various systems a message from a place of interest needs to pass to get to the end user. Please calculate the fastest track. Note that lower case letters denote *system vertices* and the numbers the *miliseconds*.

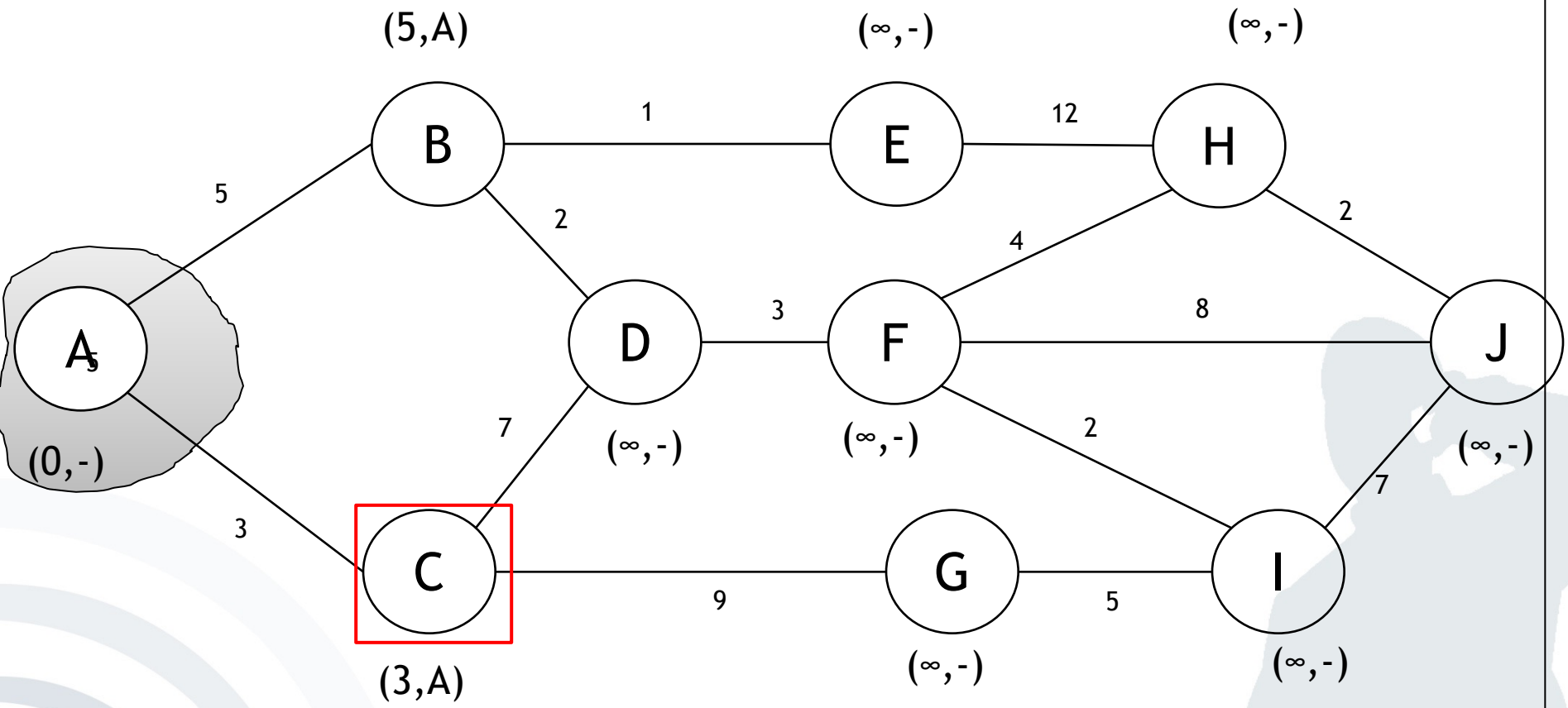


miliseconds:
= shortest path

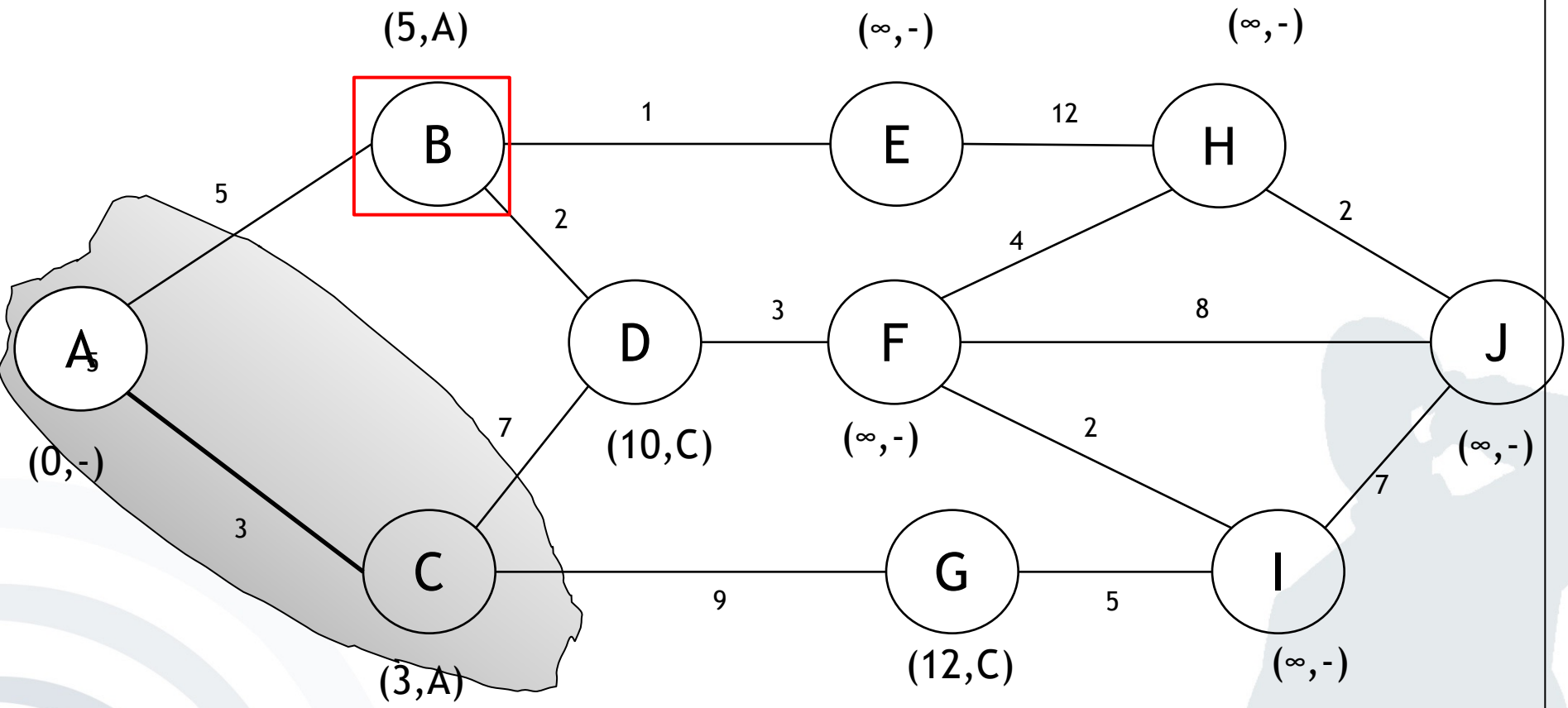
Dijkstra Algorithm



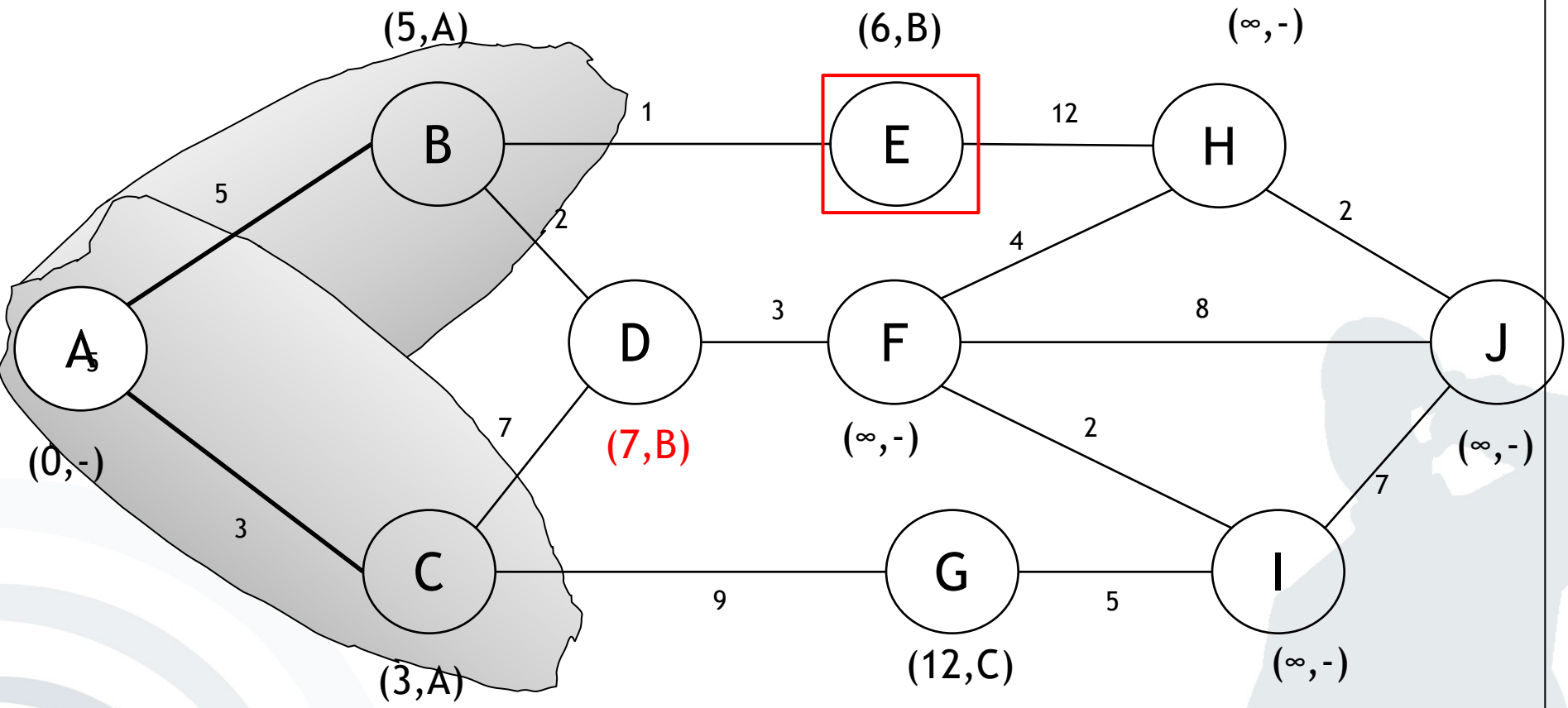
Dijkstra Algorithm



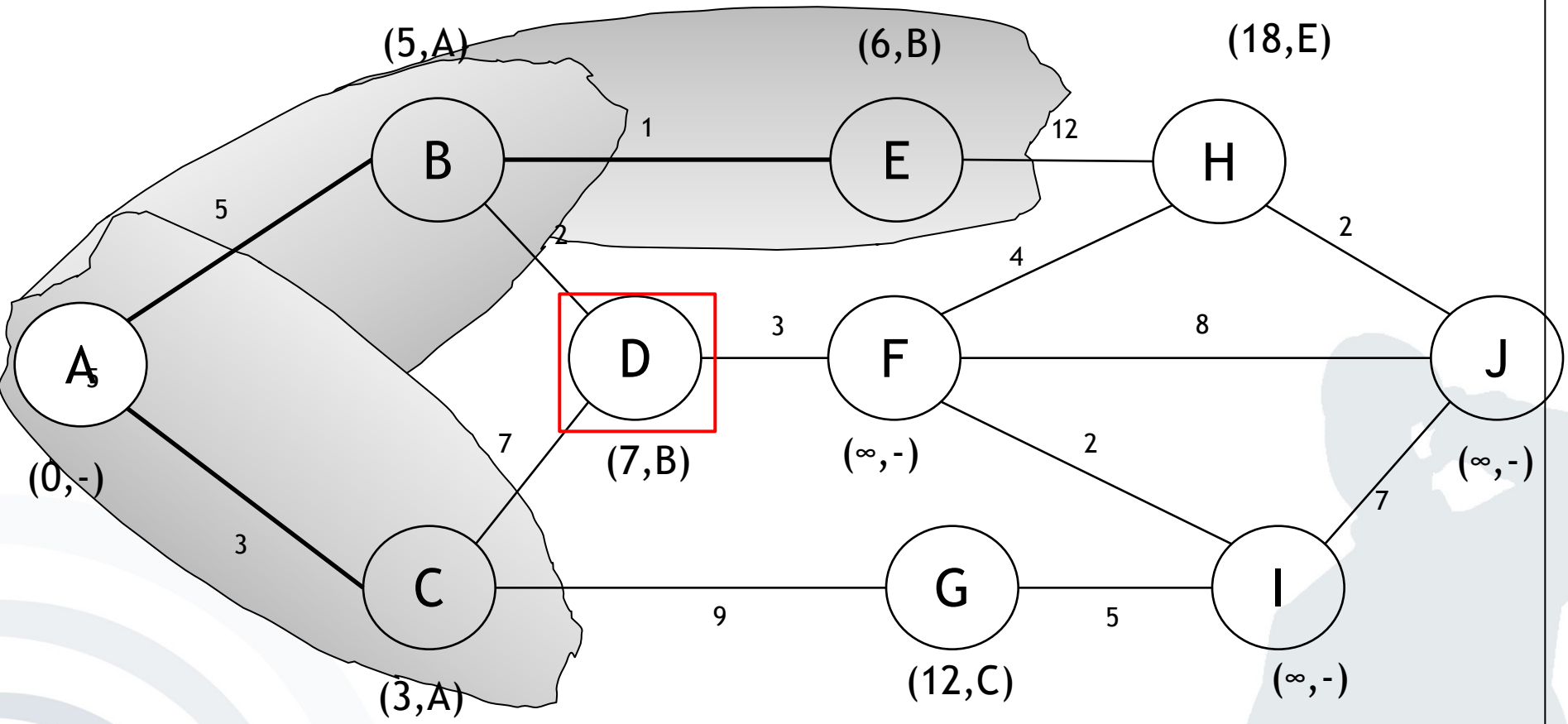
Dijkstra Algorithm



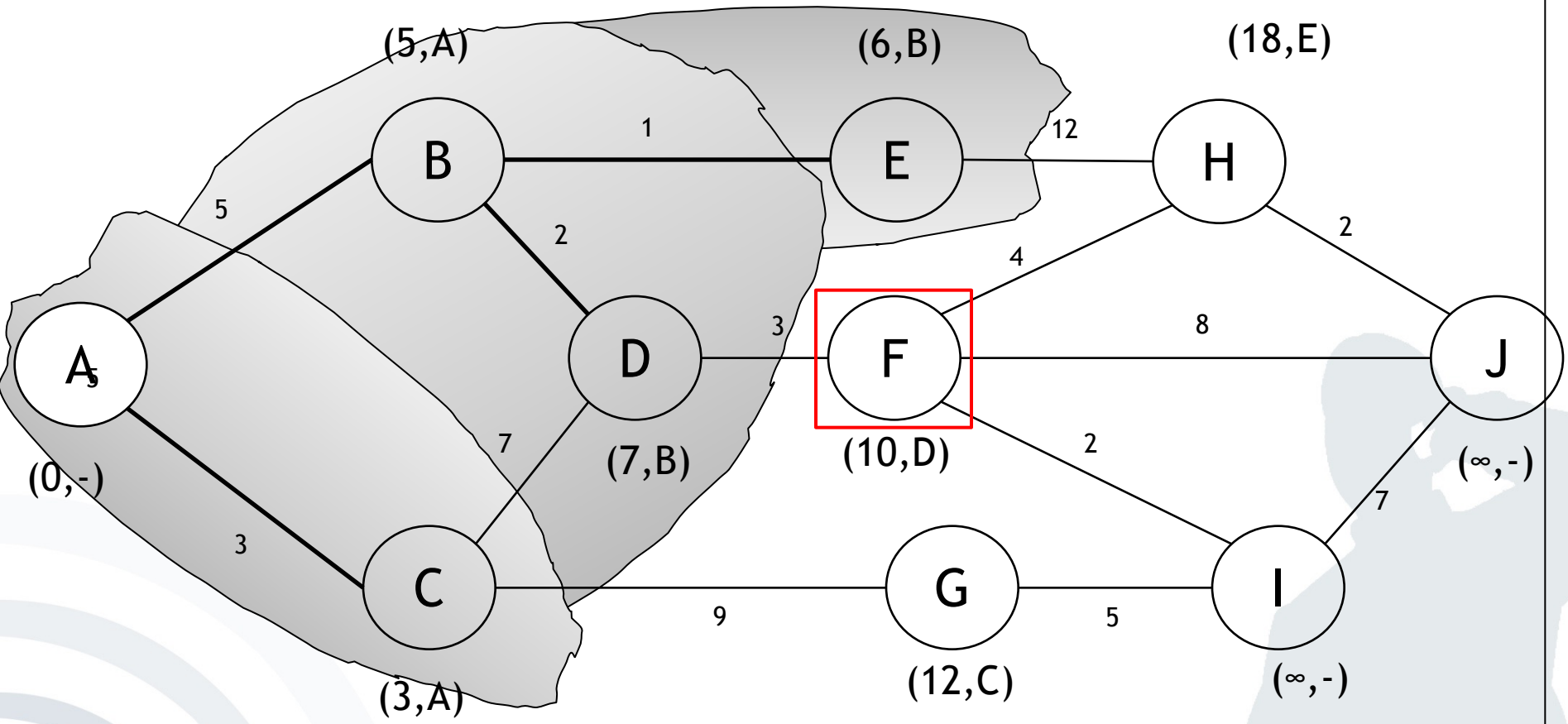
Dijkstra Algorithm



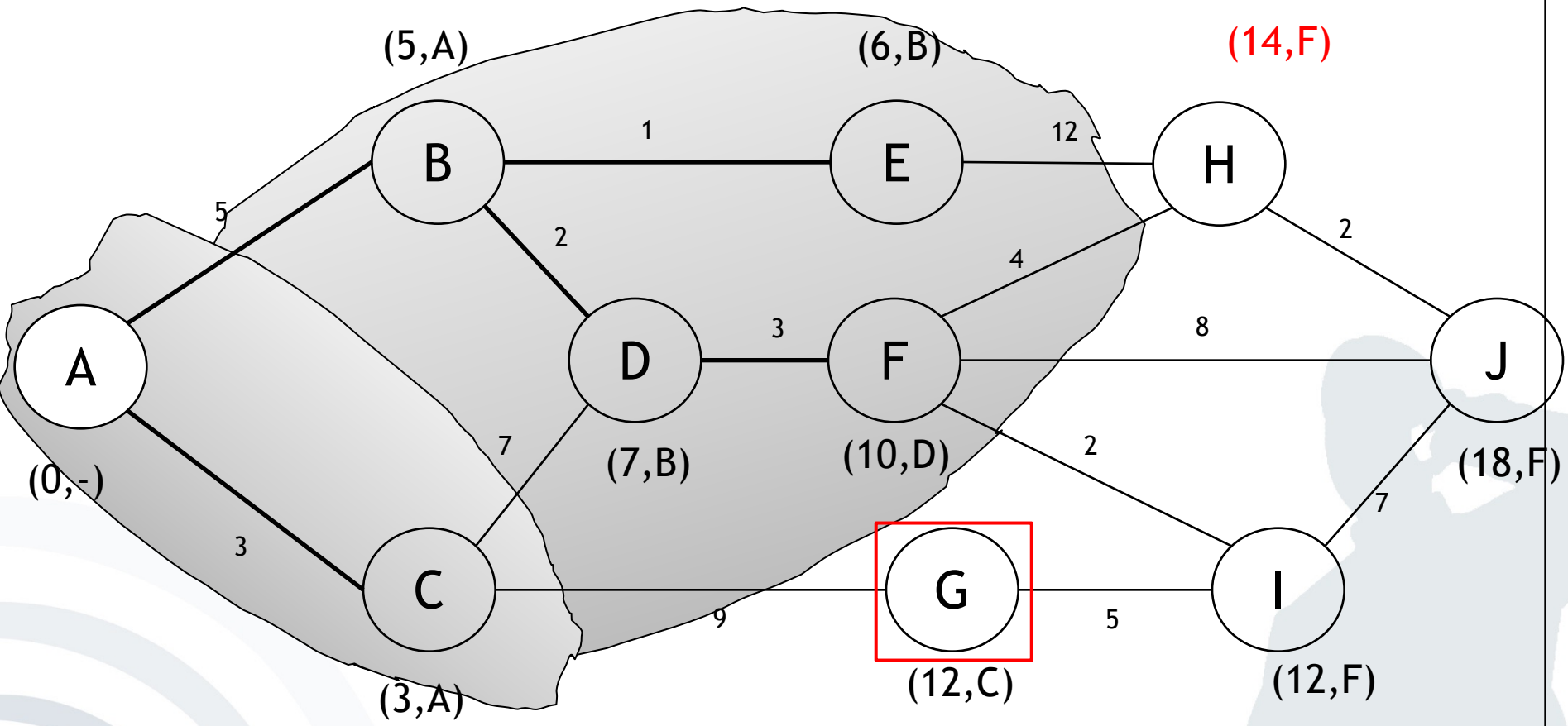
Dijkstra Algorithm



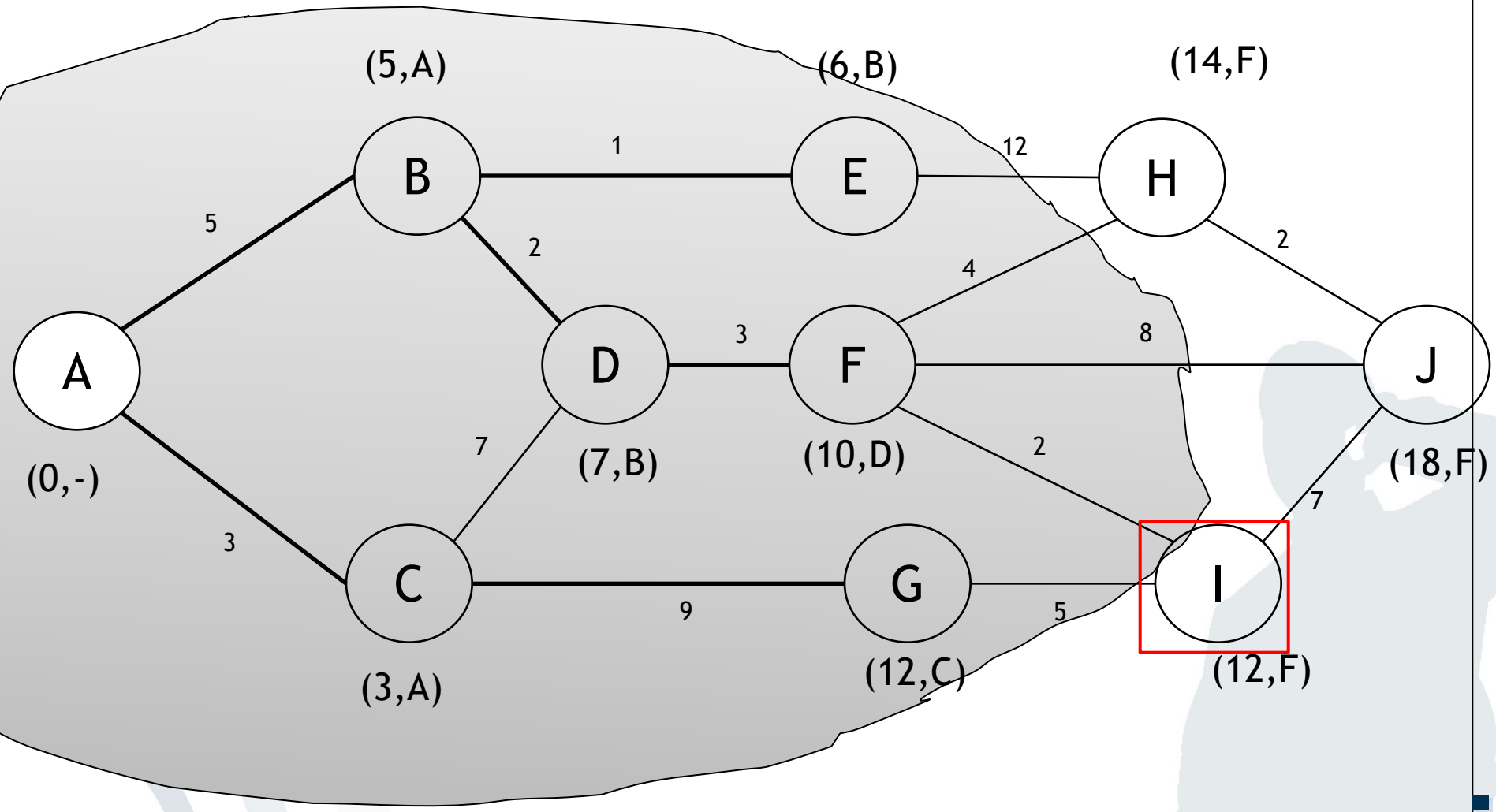
Dijkstra Algorithm



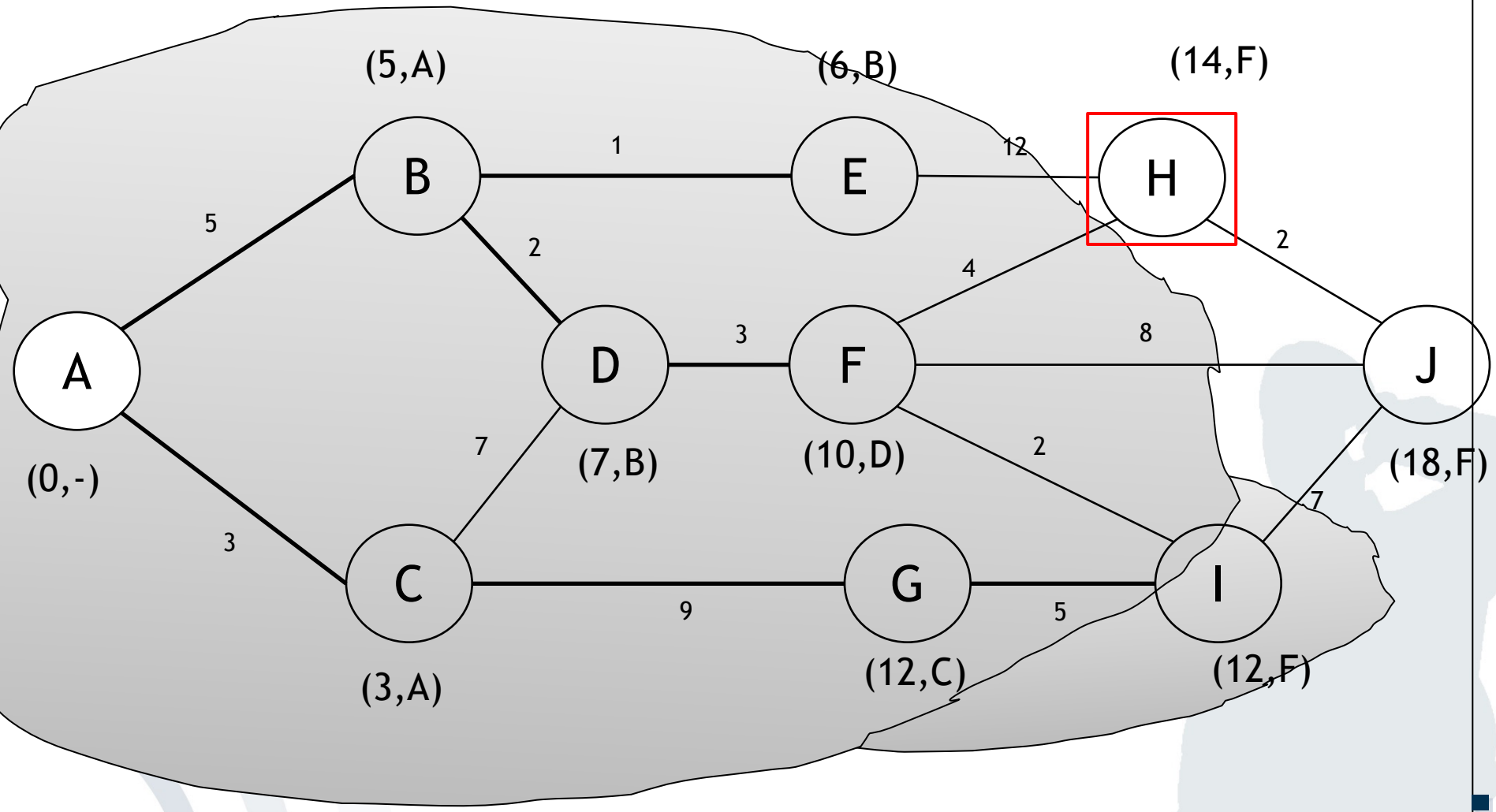
Dijkstra Algorithm



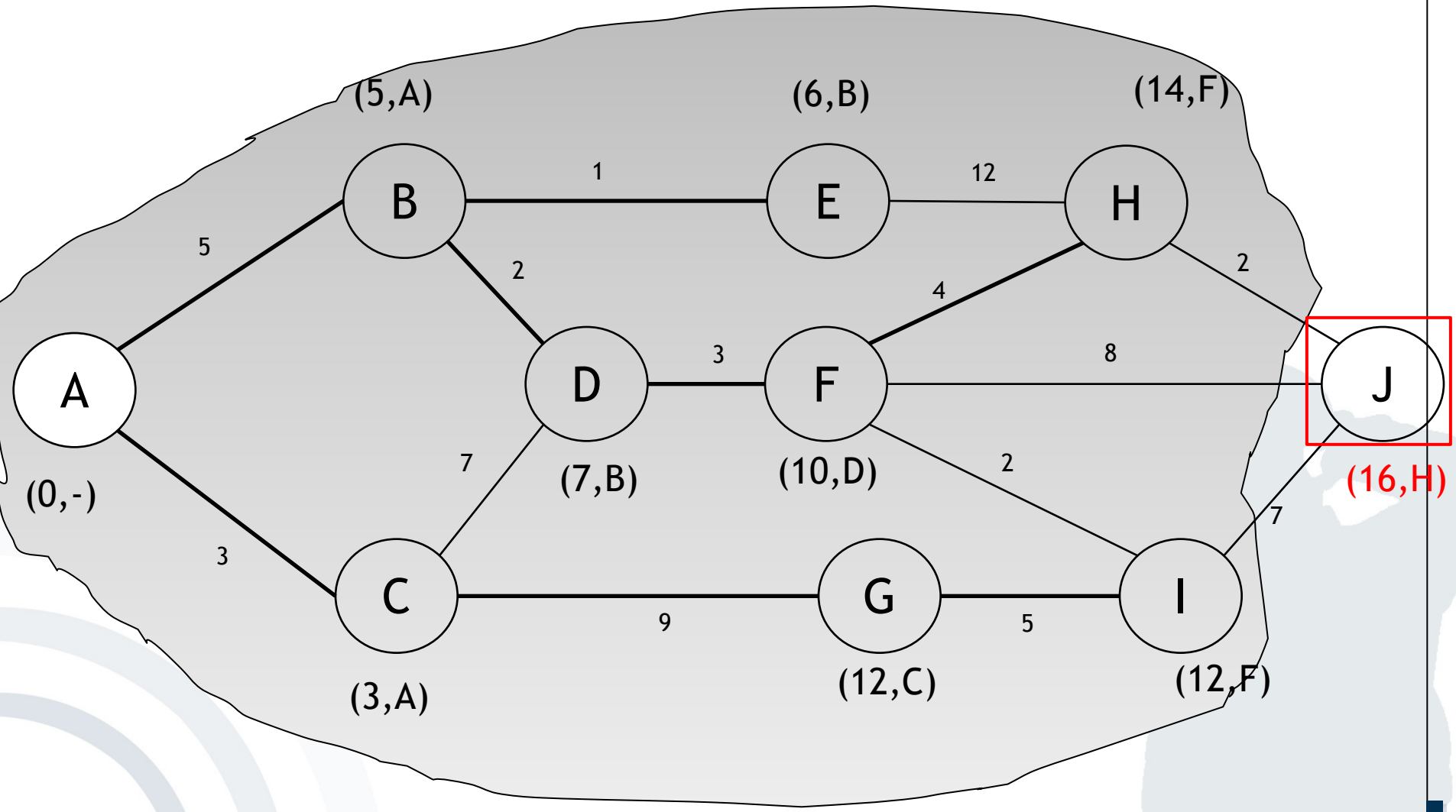
Dijkstra Algorithm



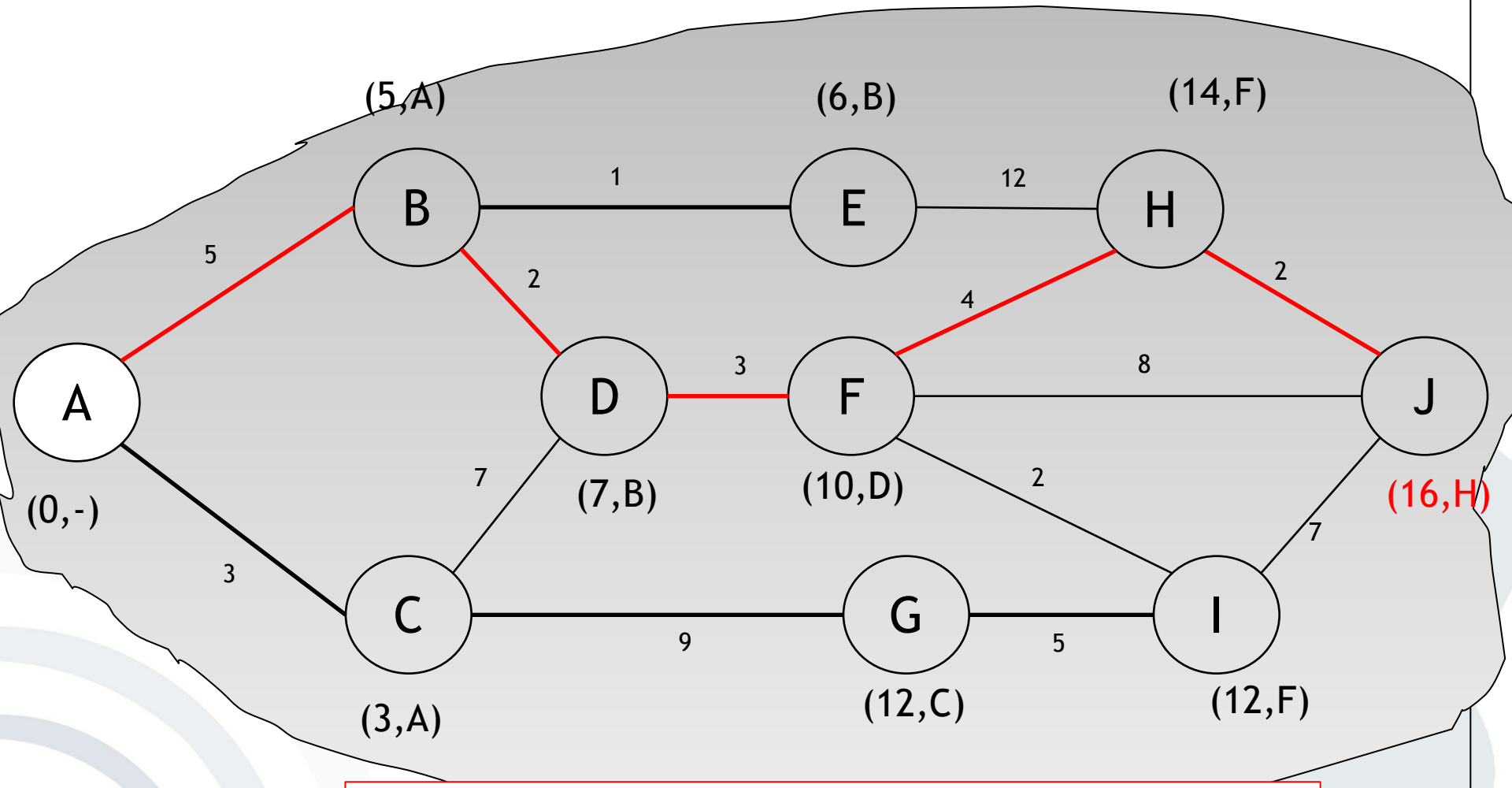
Dijkstra Algorithm



Dijkstra Algorithm



Dijkstra Algorithm



Shortest Path: A → B → D → F → H → J

Exercise: DDoS

Which layer is affected by a Distributed Denial of Service (DDoS) attack?

DDoS: cyber-attack with the objective to disrupt a service by making it (temporarilly) anavailable by flooding it with traffic or requests

Exercise: DDoS

DDoS: attacks are possible on all OSI layers!

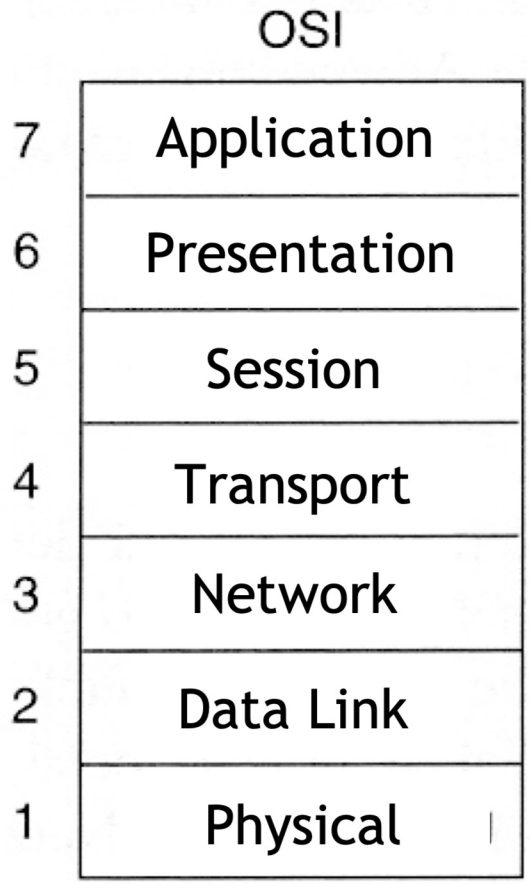
Layer	Examples of Denial of Service Techniques	Potential Impact of DoS Attack	Mitigation Options for Attack Type
Application Layer (7)	PDF GET requests, HTTP GET, HTTP POST, = website forms (login, uploading photo/video, submitting feedback)	Reach resource limits of services Resource starvation	Application monitoring is the practice of monitoring software applications using dedicated set of algorithms, technologies, and approaches to detect zero day and application layer (Layer 7 attacks). Once identified these attacks can be stopped and traced back to a specific source.
Presentation Layer (6)	Malformed SSL Requests – Inspecting SSL encryption packets is resource intensive. Attackers use SSL to tunnel HTTP attacks to target the server	The affected systems could stop accepting SSL connections or automatically restart	Offloading the SSL from the origin infrastructure and inspecting the application traffic for signs of attacks traffic or violations of policy at an applications delivery platform (ADP).
Session (5)	Telnet DDoS-attacker exploits a flaw in a Telnet server software running on the switch, rendering services unavailable	Prevents administrator from performing switch management functions	Check with your hardware provider to determine if there's a version update or patch to mitigate the vulnerability
Transport (4)	SYN Flood, Smurf Attack	Reach bandwidth or connection limits of hosts or networking equipment	DDoS attack blocking, commonly referred to as blackholing, is a method typically used by ISPs to stop a DDoS attack on one of its customers. This approach to block DDoS attacks makes the site in question completely inaccessible to all traffic. Black holding is typically deployed by the ISP to protect other customers on its network from the adverse effects of DDoS attacks such as slow network performance and disrupted service
Network (3)	ICMP Flooding: uses ICMP messages to overload the targeted network's bandwidth	Can affect available network bandwidth and impose extra load on the firewall	Rate-limit ICMP traffic and prevent the attack from impacting bandwidth and firewall performance
Data Link (2)	MAC flooding – inundates the network switch with data packets	Disrupts the usual sender to recipient flow of data - blasting across all ports	Many advances switches can be configured to limit the number of MAC addresses that can be learned on ports connected to end stations; allow discovered MAC addresses to be authenticated against an authentication, authorization and accounting (AAA) server and subsequently filtered
Physical (1)	Physical destruction, obstruction, manipulation, or malfunction of physical assets	Physical assets will become unresponsive and may need to be repaired to increase availability	Practice defense in-depth tactics, use access controls, accountability, and auditing to track and control physical assets

DDoS QUICK GUIDE
https://www.cisa.gov/sites/default/files/publications/DDoS%20Quick%20Guide.pdf

Exercise: IP address vs. MAC address

- What is the difference between an IP and a MAC address?

Keywords for OSI reference model layers



SMTP, HTTP

Encryption, Compression

Session

TCP (3 way handshake), UDP

Routing, IP address

Frames, MAC

Bits, LAN cable, optical fibre, air

IP address vs. MAC address

BASIS FOR COMPARISON	MAC	IP
Full Form	Media Access Control Address.	Internet Protocol Address.
Purpose	It identifies the physical address of a computer on the internet.	It identifies connection of a computer on the internet.
Bits	It is 48 bits (6 bytes) hexadecimal address.	IPv4 is a 32-bit (4 bytes) address, and IPv6 is a 128-bits (16 bytes) address.
Address	MAC address is assigned by the manufacturer of NIC card.	IP address is assigned by the network administrator or Internet Service Provider.

Source: https://techdifferences.com/difference-between-mac-and-ip-address.html

Agenda

- Exercise 1: OSI reference model
- Exercise 2: Fixed Networks
- Exercise 3: Wireless Local Area Networks
- Exercise 4: Bluetooth and NFC

Exercise: Wired Communication

- What are the main challenges in wired communication and why?

Wired Communication

- Wired communication denotes data transmission using physical wires, e.g. for
  - Telephone networks
  - Cable television/Internet access
  - Fiber-optic networks

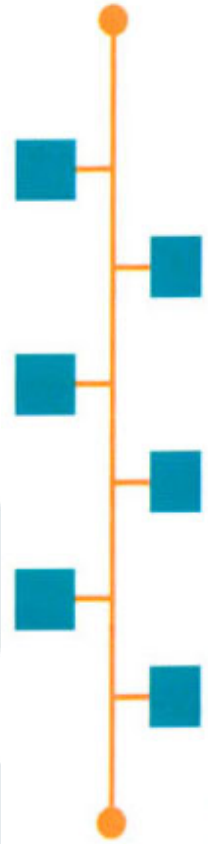
- Main challenges in wired communication
  - Coping with the distance between two endpoints
  - Provision of the appropriate bandwidth

Exercise :Topologies

- Name three different types of topologies and expose their advantages and disadvantages.

Topologies

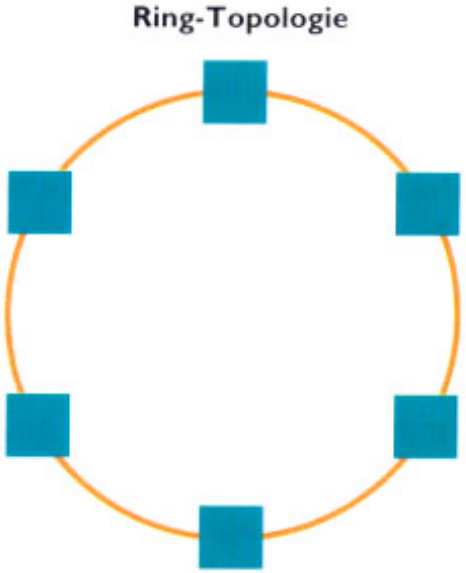
- Bus Topology
  - Low cost
  - Easy and low cost setup and extension
  - Difficult to find errors



Bus-Topologie

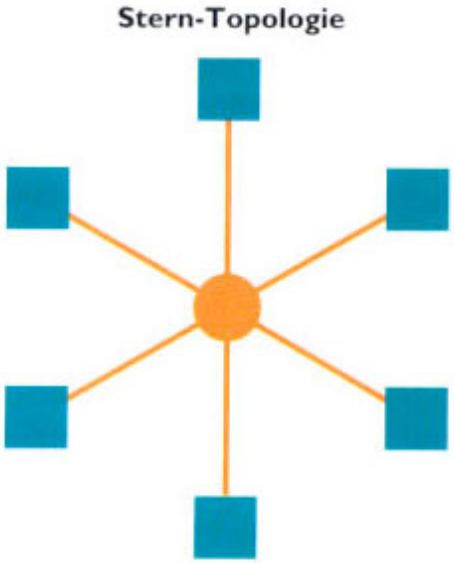
Topologies

- Ring Topology
  - No single point of failure
  - Slow if one way is broken



Topologies

- Star Topology
  - Single point of failure, but only at the central node
  - Easy setup & troubleshooting



Agenda

- Exercise 1: OSI reference model
- Exercise 2: Fixed Networks
- Exercise 3: Wireless Local Area Networks
- Exercise 4: Bluetooth and NFC

Exercise: Wireless Local Area Networks (Wi-Fi)

- Name a secure method for the encryption of Wireless Local Area Networks (Wi-Fi).

- Why is Wi-Fi encryption important? What could be the potential consequences for users failing to enable encryption for their Wi-Fi network?

Wi-Fi

- Wi-Fi Protected Access:
  - WPA is outdated and insecure (e.g. vulnerability to dictionary attacks)
  - WPA3 is secure as it employs Simultaneous Authentication of Equals (SAE)
- Consequences of unsecure Wi-Fi:
  - Data can be extracted
  - Internet access can be used by other for free and illegal activities like file sharing
  - Phone can be misused
  - …

Wi-Fi

- Man-In-The-Middle Attack
  - Attacker between the communication parties and he has the full control of the data traffic
- Eavesdrop and manipulation of data traffic
  - Passwords, data, personal information
- DNS manipulation, malware
  - E.g. Redirect online banking to a phishing site
- Snarfing (fake wlan access point)

Wireless Local Area Networks (Wi-Fi)

- What could be the potential harm if the data communication of the myPlace service is not encrypted?
- Name at least one consequence respectively for the service and the user.

Wi-Fi (myPlace)

- Eavesdropping on communication
- Redirection to a manipulated service is possible
- Mobile user’s perspective:
  - Passwords can be stolen and an attacker can slip into the corresponding identity
- myPlace’s perspective
  - Unsecure services results in public image loss
  - Suit for violating the legal framework

Agenda

- Exercise 1: OSI reference model
- Exercise 2: Fixed Networks
- Exercise 3: Wireless Local Area Networks
- Exercise 4: Bluetooth and NFC

Exercise: Bluetooth and NFC

- What is Bluetooth and what is NFC? Where is the difference between them?

Bluetooth

- Bluetooth is a wireless technology standard for data exchange using small ad-hoc networks called “personal area networks” (PANs)
  - Devices such as laptops, mobile phones, printers, headsets and other periphery-devices can establish a connection.
  - Simple and cheap possibility to set up ad-hoc networks of limited range (up to 10 meters) for spontaneous data exchange
  - Technical specifications for Bluetooth were developed by the Bluetooth Special Interest Group (SIG).
  - Findings were added to the IEEE 802.15 standard.

Source: Wiegleb, M. (2005)

Near Field Communication (NFC)

- NFC is a short-range (< 4 cm) wireless technology
  - Communication mode of a device can be active or passive
  - Magnetic induction between two loop antennas
  - Application domains
    - Mobile payment / mobile wallet
    - Mobile marketing
      (e.g. redemption of digital coupons)
    - Mobile ticketing
    - Access control (e.g. e-Key)
    - Mobile data user exchange
    - ...

Source: techtickerblog.com (2011)

Components of the Course

- Introduction to layer-based Communications ✔
- Fixed Networks ✔
- Wireless Networks ✔

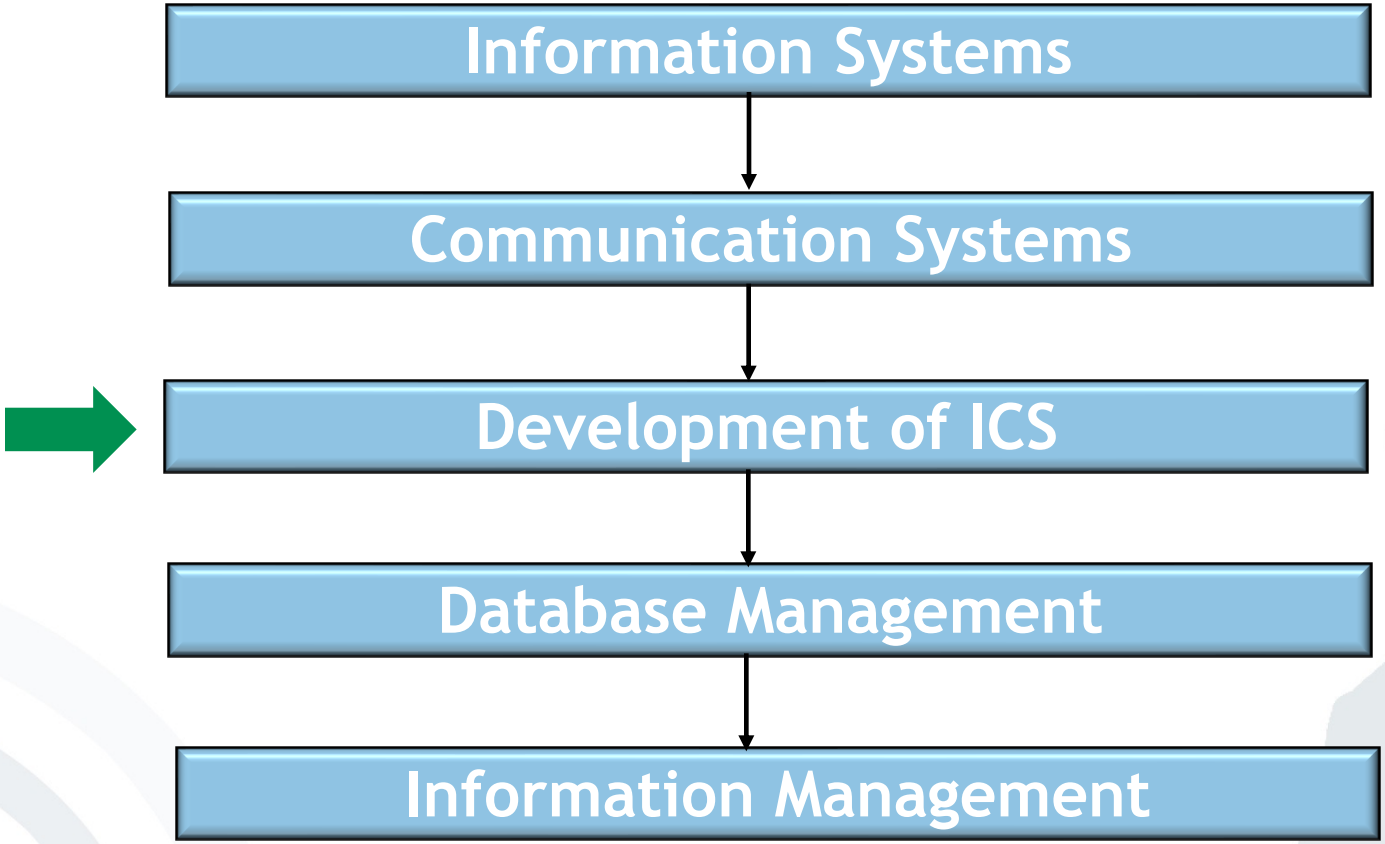
Looking back at Communication Systems I & II

By now you should:

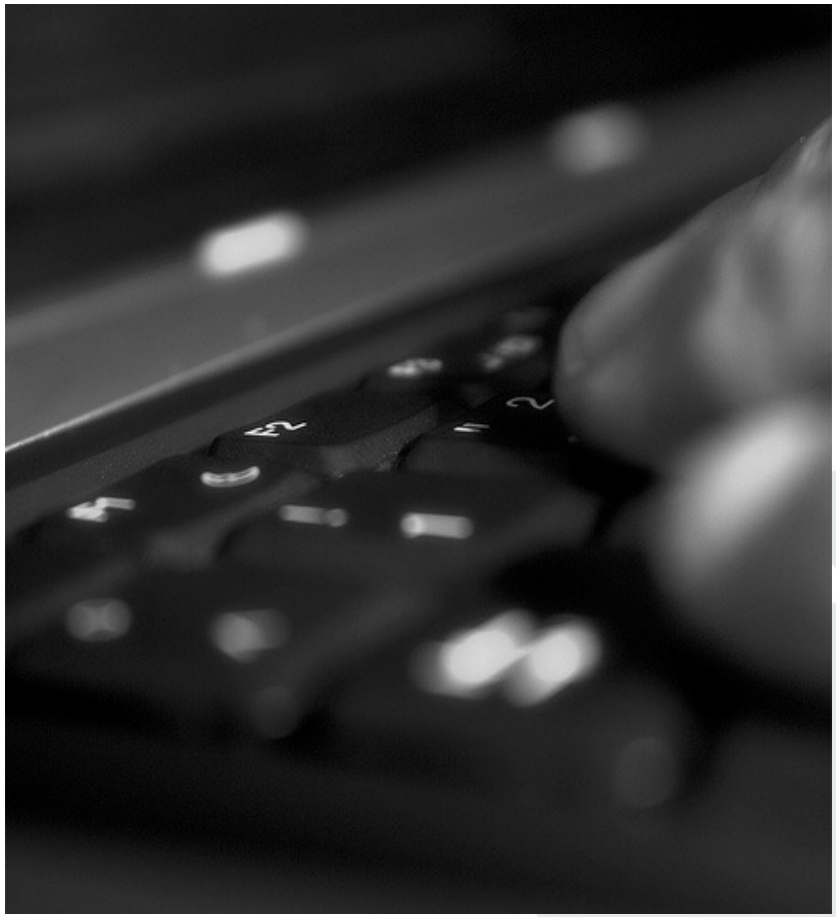
- Know the principles of layer based communication
- Know the layers of the ISO/OSI reference model and their particularities (focus on layer 2, 3, 4 and 7)
- Be able to apply the Dijkstra algorithm
- Understand the principles of fixed Networks
- Understand the principles of wireless communication

→ Apply your knowledge!

Next Mentorium



Thank you!



Jenser (Flickr.com)