École Pour l'Informatique et les Techniques Avancées – EPITA

BSc L1 – 27 April 2024

Course: Introduction to Computer Networks

Course instructor: M Salman Nadeem

mohammad-salman.nadeem@epita.fr

Introduction to Computer Networks

Course schedule (tentative)

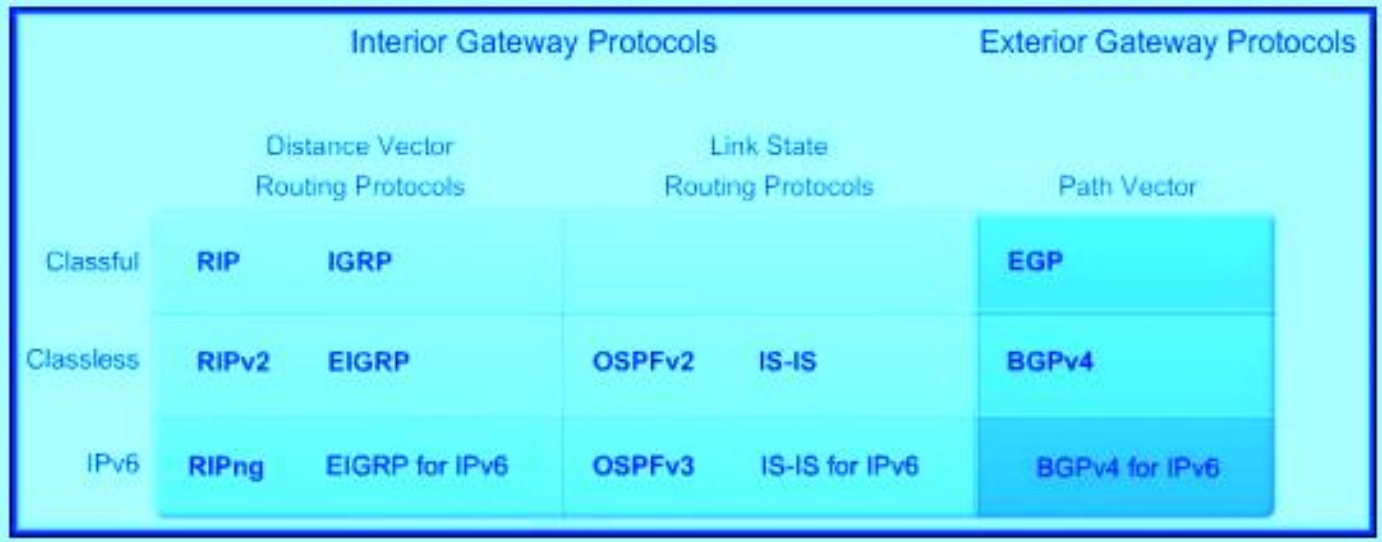
Date & Time	No.	Topics	Duration (hours)
Fri 19/04/24 – 10:00–13:00	1	Primer, Network protocols, types, topology, architecture	3
Fri 26/04/24 – 10:00–13:00	2	Network models, TCP/IP model, Packet switching	3
Sat 27/04/24 – 10:00–13:00	3	Physical Layer (Function, Signals, Modulation, Multiplexing, Transmission media & Hardware, Optical networks)	3
Sat 27/04/24 – 14:00–17:00	4	Data Link Layer (Function, Framing, Protocols, Flow control, Access control, Error correction, Hardware)	3
Fri 03/05/24 – 14:30–17:30	5	Network Layer (Function, IP addressing and subnets)	3
Sat 04/05/24 – 10:00–13:00	**6**	**Network Layer (Routing algorithms and protocols), Internet Control Message Protocol**	**3**
Fri 17/05/24 – 14:00–17:00	7	Network Layer (IGP & EGP), Autonomous System, Border Gateway Protocol	3
Fri 18/05/24 – 14:00–17:00	8	Transport Layer (Function, Flow and congestion controls, Protocols)	3
Fri 24/05/24 – 10:00–13:00	9	Application Layer (Function, Protocols)	3

Lecture 6 Outline

- **Network Layer (TCP/IP)**
  - **Routing protocol (RIP)**
    - **RIP operation**
    - **RIP v1 & v2**
    - **Class exercise 9**
  - Open Shortest Path First (OSPF)
    - Operations
    - Shortest Path Algorithm (Dijkstra)
    - Router types
    - Subdivided areas
    - Class exercise 10
- **Internet Control Message Protocol (ICMP)**
  - **Implementation**
  - **Header**
  - **Use cases**
  - **Class exercise 11**

Routing protocol

- RIPv1 (Routing Information Protocol): Distance Vector, Classful Routing Protocol
  - RIP use UDP on port 520
  - Uses hop count (i.e., Distance) as its only metric for path selection; Vector: direction



	Interior Gateway Protocols				Exterior Gateway Protocols
	Distance Vector Routing Protocols		Link State Routing Protocols		Path Vector
Classful	RIP	IGRP			EGP
Classless	RIPv2	EIGRP	OSPFv2	IS-IS	BGPv4
IPv6	RIPng	EIGRP for IPv6	OSPFv3	IS-IS for IPv6	BGPv4 for IPv6

Routing protocol (Cont.)

- RIP evolved from the Xerox Network System (NS) in the late 1970's
  - In 1988, it was standardized under RFC 1058
- Why learn RIP?
  - Still in use today (mostly V2)
  - Help understand fundamental concepts and comparisons of protocols such as classful (RIPv1) and classless (RIPv2)
  - IPv6 form of RIP: RIPng (next generation)

RIP Operation

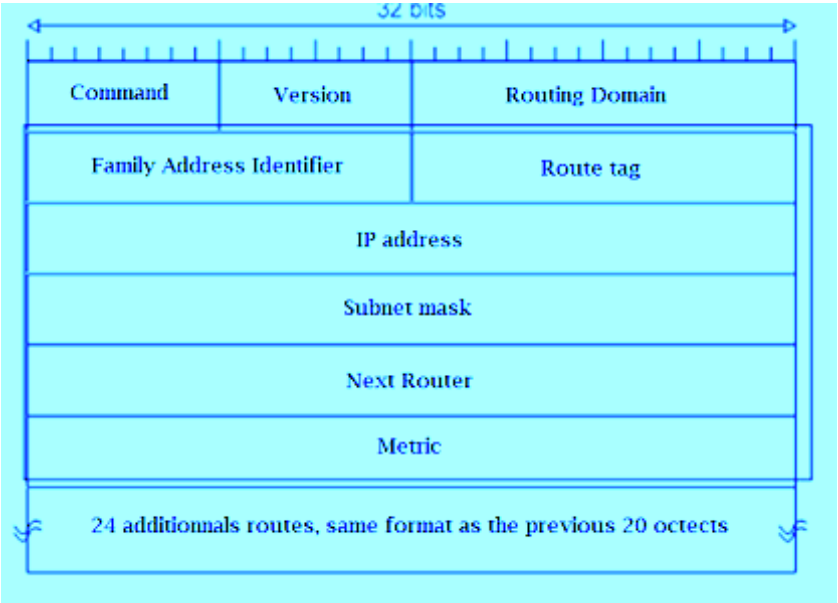
1. On Start-up:
   - Each RIP-configured interface broadcasts a request message, asking any RIP neighbors to send their complete routing table
2. Each RIP neighbor responds with the information
3. The requesting router evaluates each route
   - If it's a new route, it gets added to the routing table
   - If it's already in the routing table and has a better hop count (lower), the routing table is updated
   - If there are no changes, it is ignored
4. The requesting router then sends a triggered update out all interfaces that contains its routing table

IP address classes & classful routing

- RIPv1 is a classful routing protocol – and therefore does not send subnet mask information in the update
- The router determines the subnet mask
  - Uses the subnet mask configured on a local interface
  - Or applies the default, classful subnet mask
- Because of this limitation, RIPv1 networks cannot be separated, nor can they implement VLSM

RIPv2 Protocol

- RIPv2 (RFC 2453) is compatible with RIPv1
- Subnet Mask applied on corresponding IP
- Routing at Hops: Next Hop IP Address tells which destination will be sent to the receiver routing table
  - If this field value is '0', the RIP message sender's address is considered (use of multiple protocols on, a single router)



RIPv2 benefits/downsides

- Benefits
  - Widespread use and implemented on every routing equipment
  - Handle subnet (Classless)
  - Handle router authentication (MD5, uses Authentication keys – password)
  - User friendly
- Downsides
  - Metric (hop count)
  - Limited to 15 hops
  - Slow convergence (the 'state' of a set of routers that have the same topological information)

Display RIP Configuration

- Display information about the routing protocol used on each interface

```
Router#show ip protocols
```

- Display RIP routes:

```
Router#show ip route rip
     165.132.0.0/16 is variably subnetted, 3 subnets, 3 masks
R    192.168.2.0/24 [120/1] via 192.168.1.2, 00:00:25, Serial2/0
```

RIPv2 Configuration

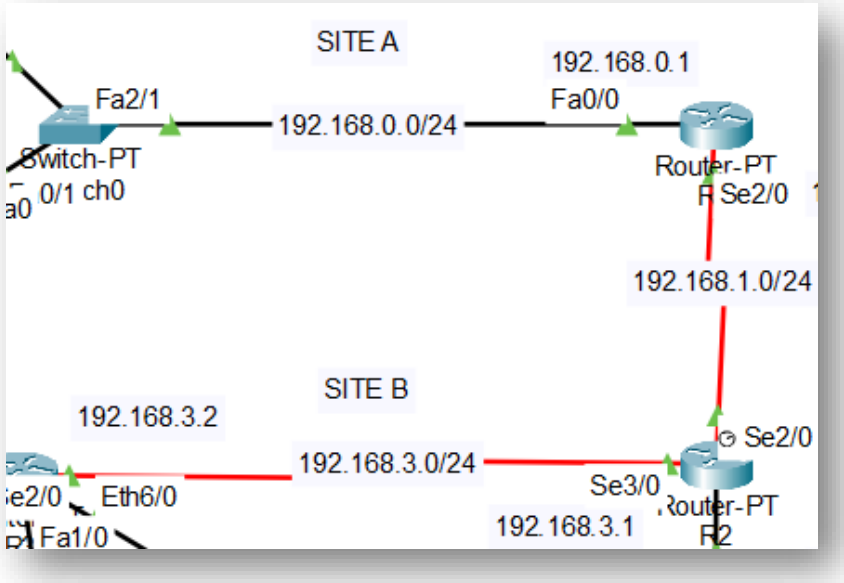
- By default the router sends RIPv1 and can receive both versions
  - Config:
    1. Conf t
    2. Router rip
    3. Version 2 //To define version RIPv2
    4. Network x.x.x.x
    5. exit
- To use RIP only on a specified interface:

```
lab1-ro1841-1(config-if)#ip rip send version 2

lab1-ro1841-1(config-if)#ip rip receive version 2
```

Exercise 9: Practical work

- Using your last cisco packet tracer file:
  1. Implement RIPv2 on all interfaces of 3 central routers
  2. Verify using PING and TRACERT/TRACEROUTE



Save your cpt file with your 'First_Last name'

Deadline: See 'Teams' Assignment section

Lecture 6 Outline

- Network Layer (TCP/IP)
  - Routing protocol (RIP)
    - RIP operation
    - RIP v1 & v2
    - Class exercise 8
  - **Open Shortest Path First (OSPF)**
    - **Operations**
    - **Shortest Path Algorithm (Dijkstra)**
    - **Router types**
    - **Subdivided areas**
    - **Class exercise 9**
- **Internet Control Message Protocol (ICMP)**
  - **Implementation**
  - **Header**
  - **Use cases**
  - **Class exercise 11**

OSPF (Open Shortest Path First)

- Most widely used Interior Gateway Protocol (IGP)
- Supports Classless Inter-Domain Routing (CIDR)
- Used by Internet Gateways & Routers
- Uses Link State Routing (LSR) algorithm
  - Can create a complete view/map or topology of the network by gathering information from all other routers
  - Find Shortest Path First (SPF) using Dijkstra's algorithm
  - Link-state routing protocols do not use periodic updates After the network has converged, a link-state update is only sent when there is a change in the topology

OSPF Operations

Tree

- Routers collect LS (Link State) information, LSA
- Network connection map (Tree) is formed

SPT

- LS routing algorithm forms loop-free Shortest path tree (SPT) to all destination nodes (Dijkstra's algorithm)

Gateway

- Routers update their routing tables (OSPF db description)
- Process gets repeated upon every change detection (multicast: *HELLO procedure*)

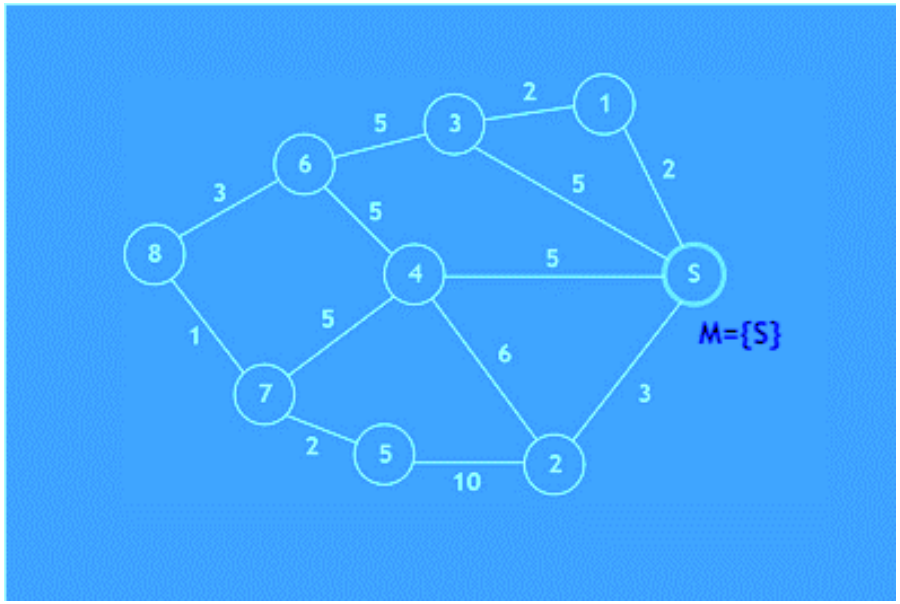
Link cost factors

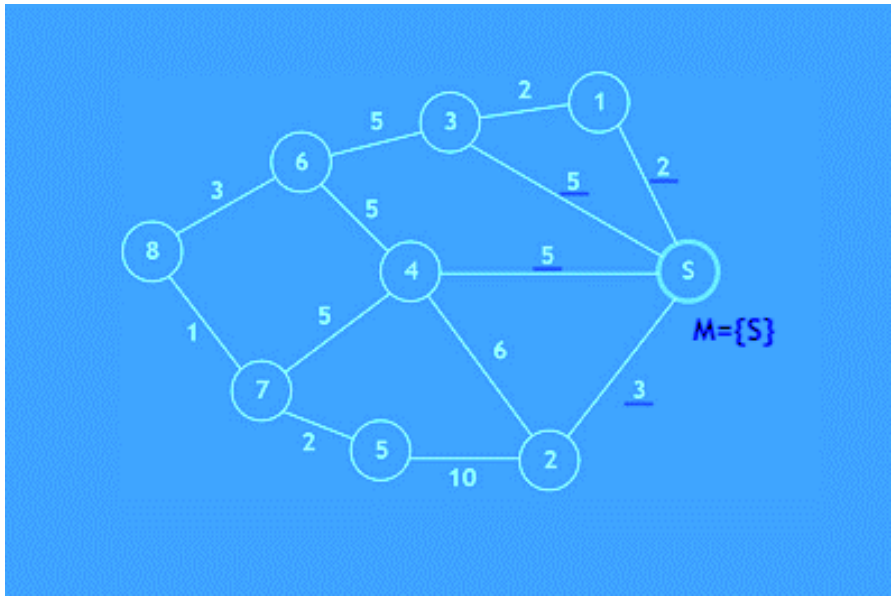
- Throughput [bits/s, packets/s]
- Distance of a router
- RTT (Round-Trip Time) [s]
- Number of hops (routers/switches) to reach destination [hops]
- Availability [unitless]
- Reliability [unitless]
- …

Shortest Path Algorithm (Dijkstra)

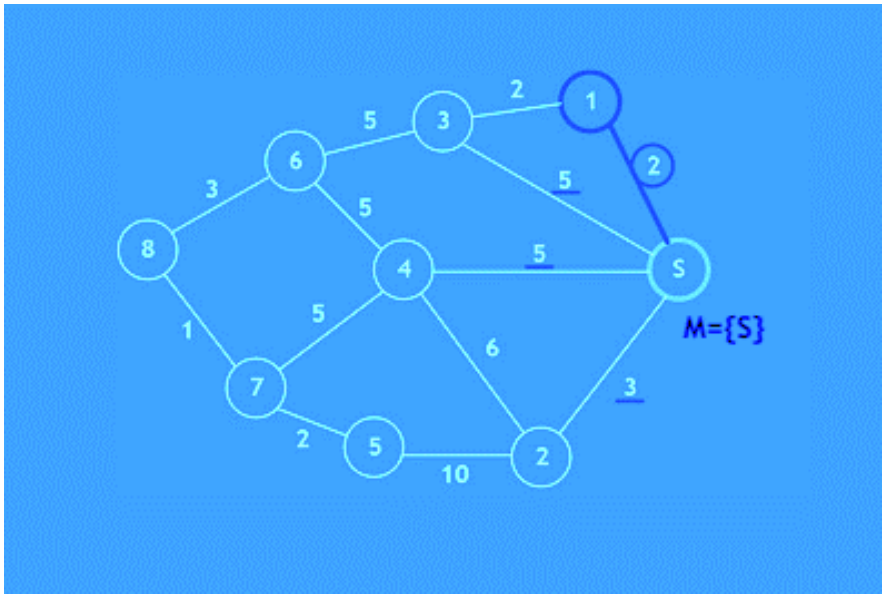
1. M is the set of nodes connected to the SPT
2. Initially M includes only the Source node (S)
3. Find the least cost route (by adding up link cost values on the routing path) from S to node X (that is not in set M yet), using nodes that exist in M as intermediate nodes
4. Add node X to set M
5. Record the least cost route from S to X
6. Repeat steps 3 to 5 until all nodes are in set M

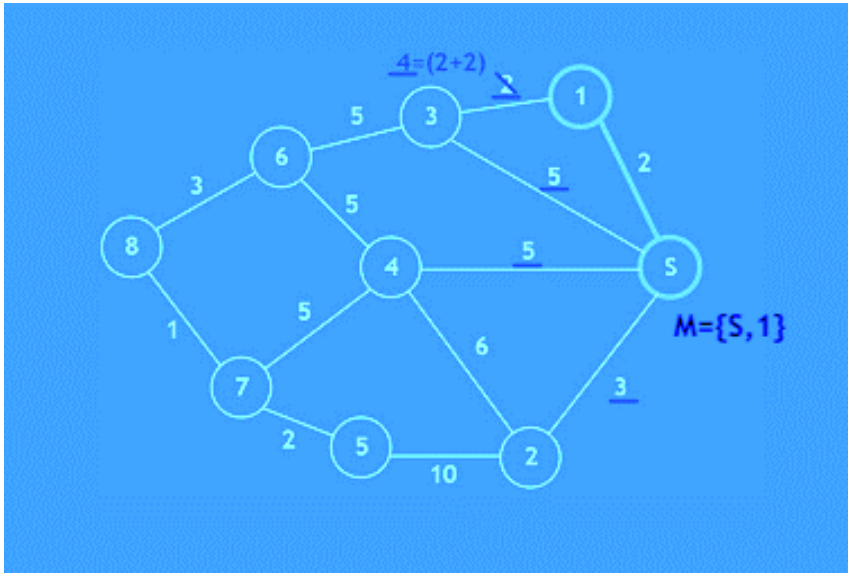
Shortest Path Algorithm (Dijkstra) – example



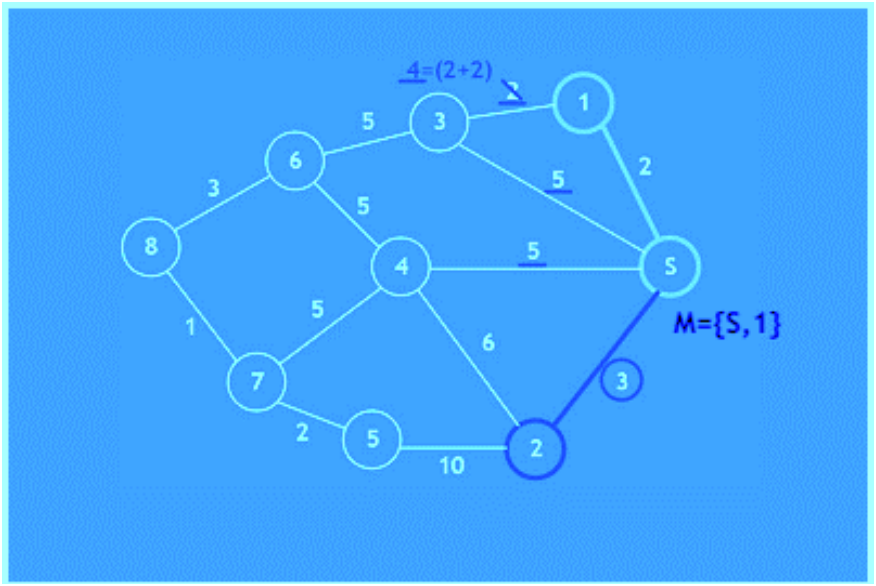


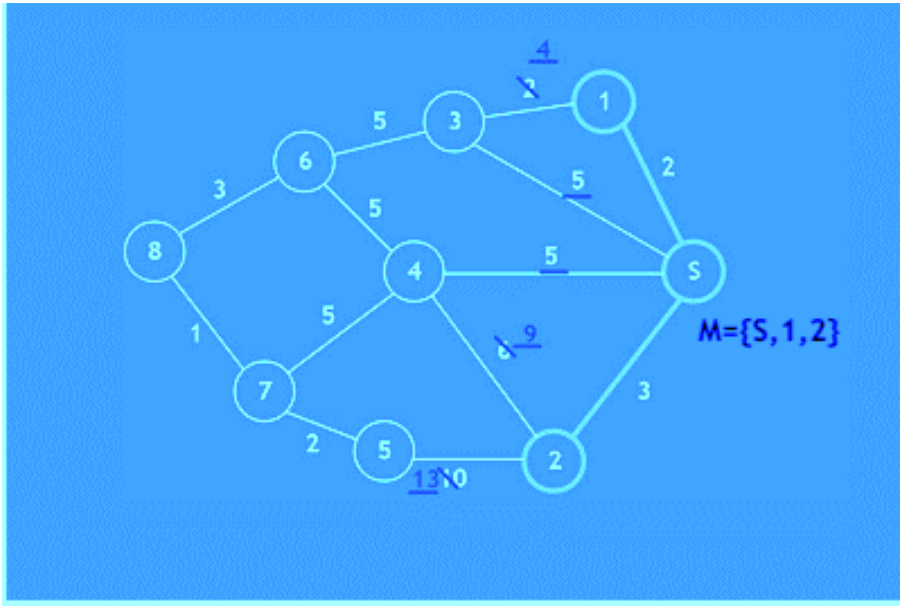
Shortest Path Algorithm (Dijkstra) – example (Cont.)



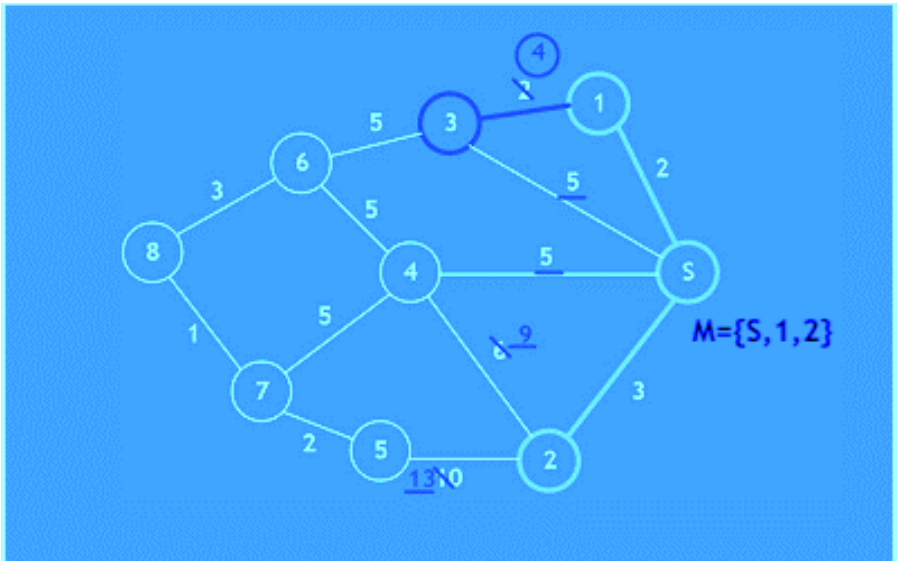


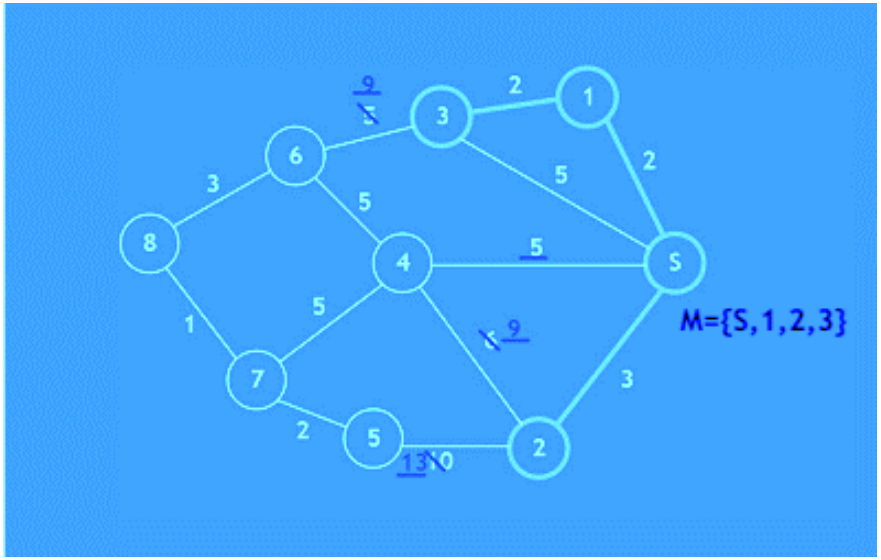
Shortest Path Algorithm (Dijkstra) – example (Cont.)



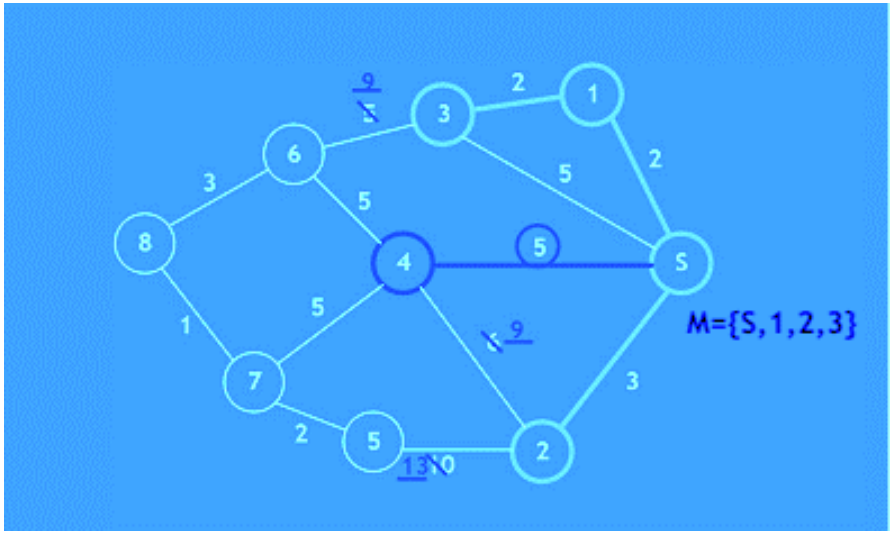


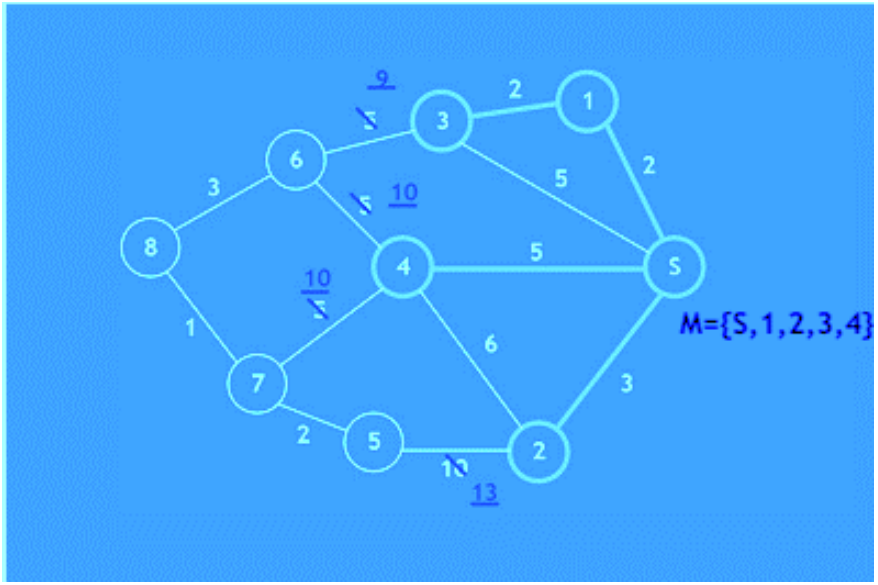
Shortest Path Algorithm (Dijkstra) – example (Cont.)



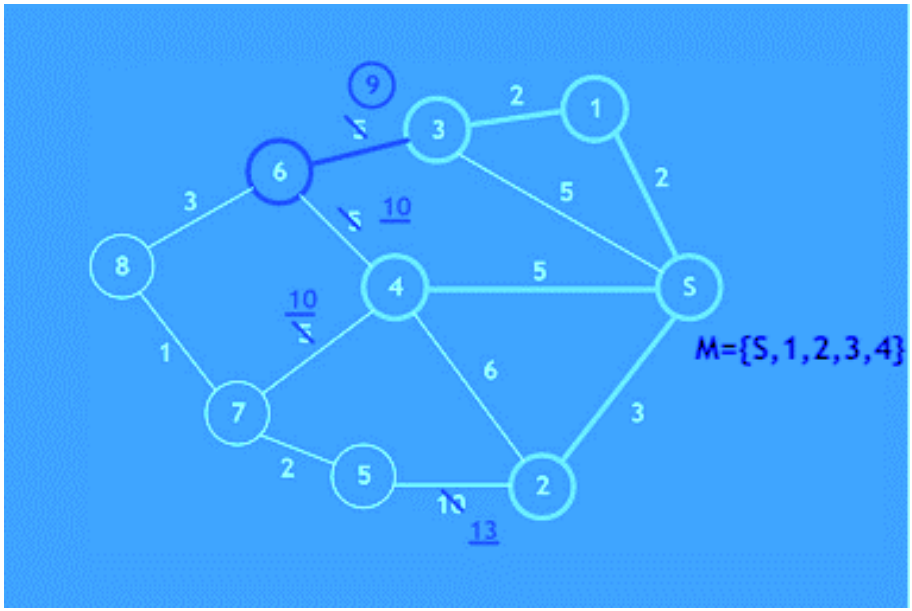


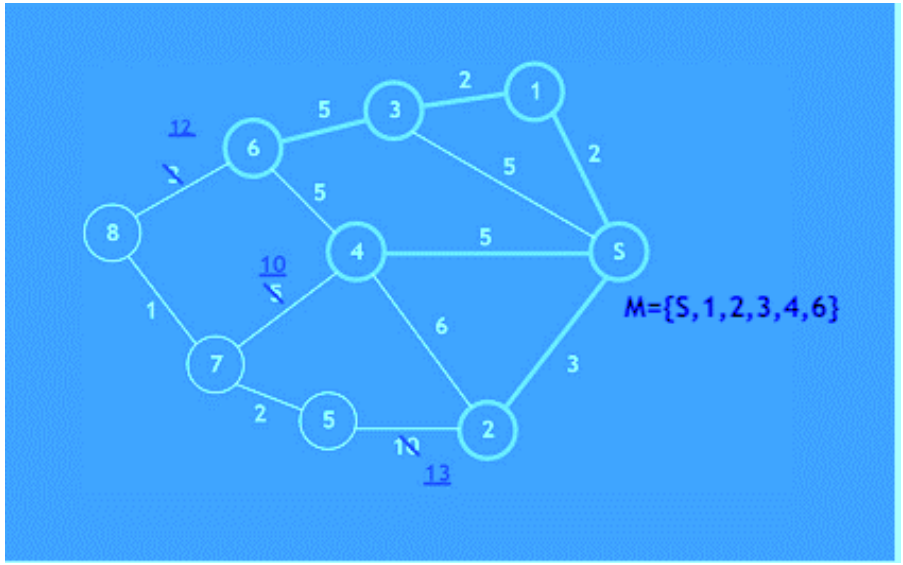
Shortest Path Algorithm (Dijkstra) – example (Cont.)



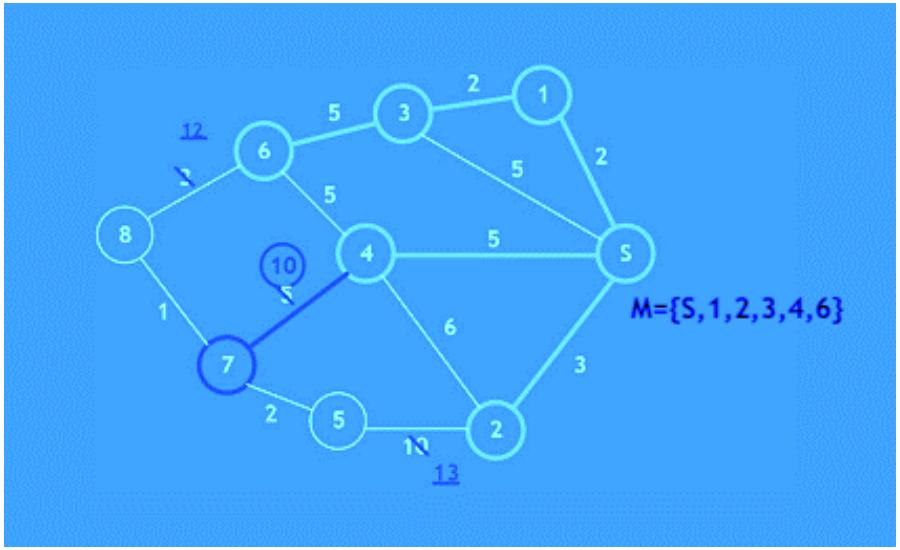


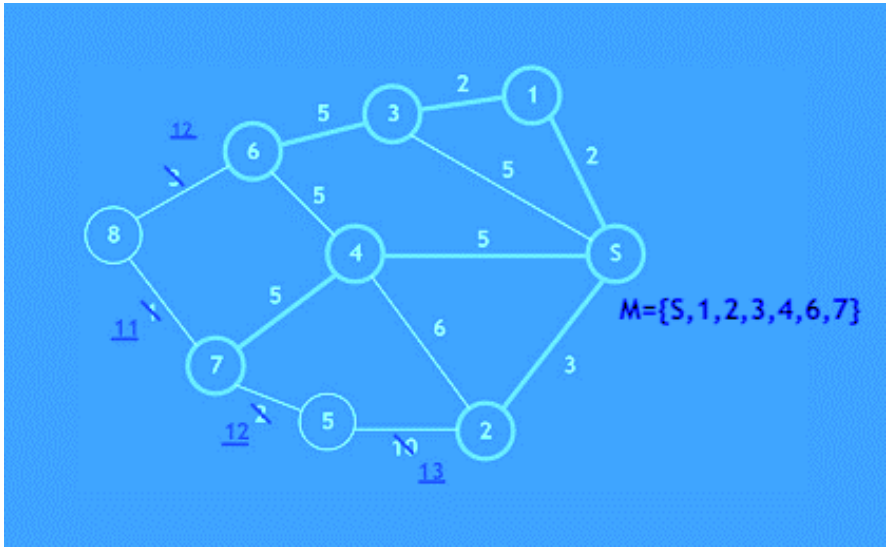
Shortest Path Algorithm (Dijkstra) – example (Cont.)



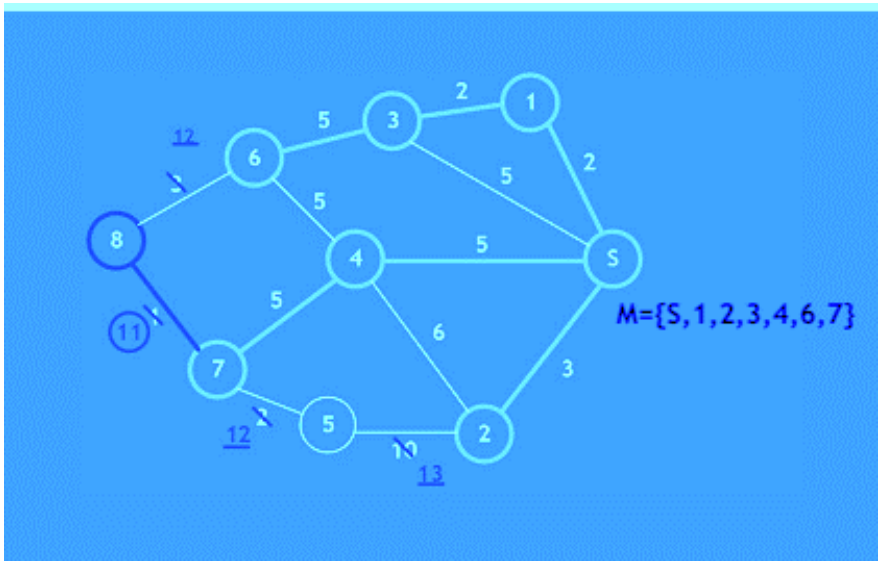


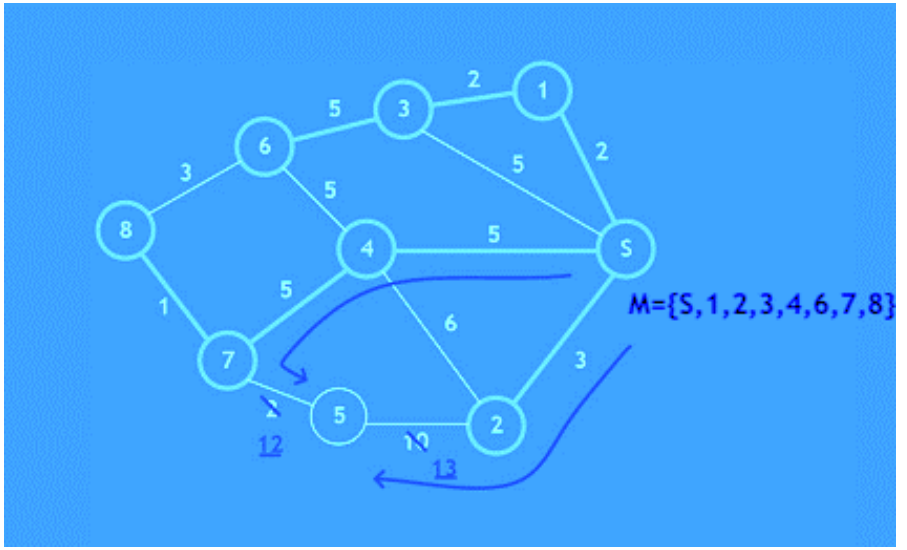
Shortest Path Algorithm (Dijkstra) – example (Cont.)



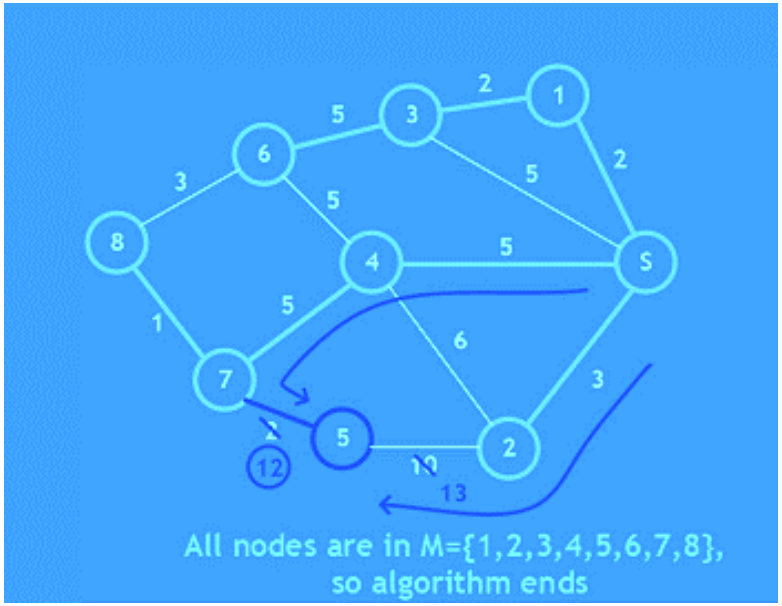


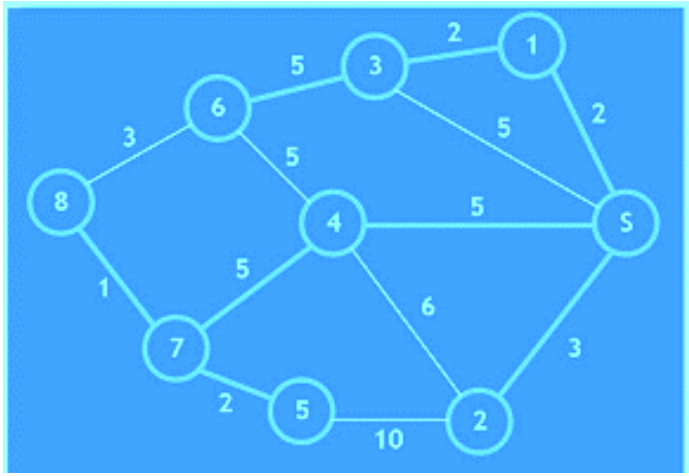
Shortest Path Algorithm (Dijkstra) – example (Cont.)





Shortest Path Algorithm (Dijkstra) – example (Cont.)





From	To	Route
S	1	S → 1
	2	S → 2
	3	S → 1 → 3
	4	S → 4
	5	S → 4 → 7 → 5
	6	S → 1 → 3 → 6
	7	S → 4 → 7
	8	S → 4 → 7 → 8

OSPF subdivided areas

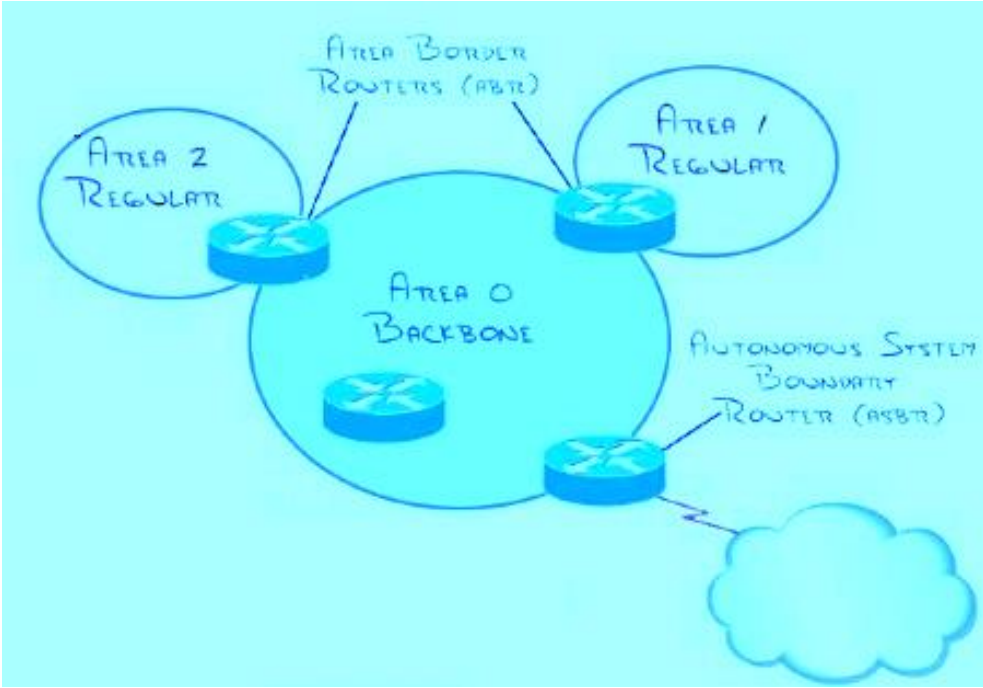
- An OSPF network can be structured, or subdivided, into routing **areas** (logical groupings of hosts and networks)
  - Division is carried out per Administration & Management requirements to:
    - Simplify administration (Traffic Engineering – TE)
    - Optimize traffic & resource utilization (Quality of service – QoS)
    - Enhance security
    - Enable faster routing updates
  - Areas are identified by 32-bit numbers (expressed in decimal/dot-decimal notation)
    - **Area 0 (zero)**, or 0.0.0.0, by convention represents the core or backbone area of an OSPF network
    - Additional areas must have a connection to the OSPF backbone area

ⓘ Always configure in order: **start by configuring Area 0 first,** then Area 1 and so on…

OSPF Router Types

- IR (Internal Router):
  - All routing interfaces belong to the same network area
- ABR (Area Border Router):
  - Connects subarea networks to the backbone network
  - Maintains separate link-state databases for each area it serves + summarized routes for all areas in the network
- BR (Backbone Router):
  - Connects to the backbone network
- ASBR (Autonomous System Boundary Router):
  - Connects between AS's using multiple routing protocols

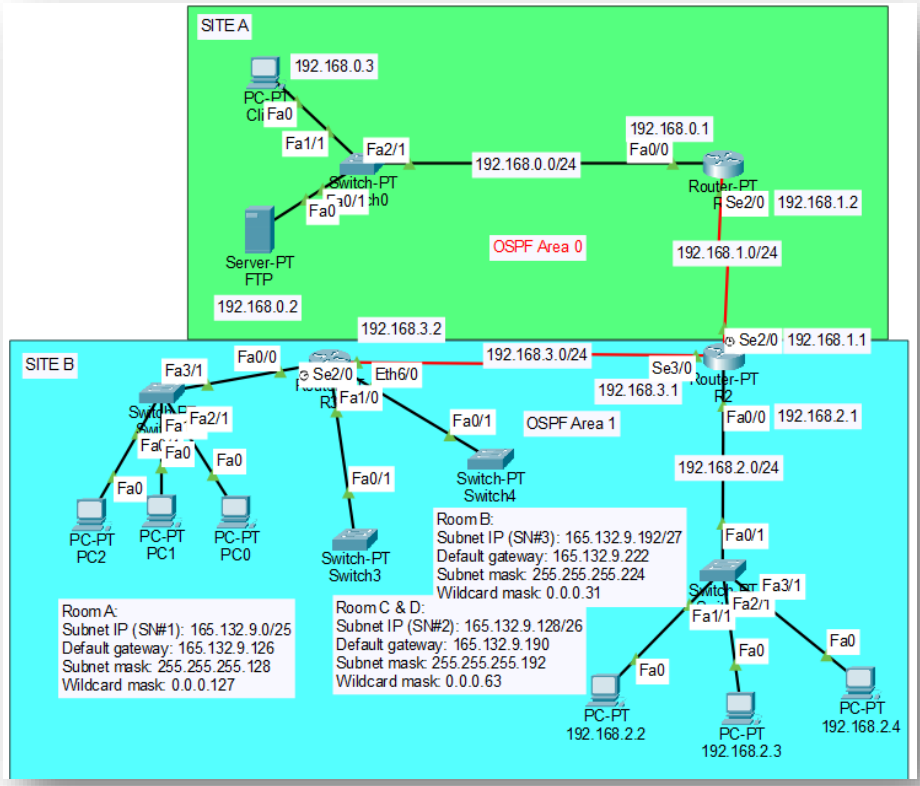
Other Routers: DR (Designated router) and BDR (Backup designated router). DR has the responsibility to share 'Summary link states' with other areas. BDR serves for load-balancing



Devices/routers & Areas

Exercise 10: Practical work

- Using your last cisco packet tracer file:
  1. Remove RIPv2 on all interfaces of 3 central routers
     1. Conf t
     2. no router rip
  2. Configure OSPF:
     Divide in 2 areas:
     Area 0: R1, R2 (int Se2/0)
     Area 1: R2 (int Se3/0, Fa0/0), R3
     1. Conf t
     2. Router ospf 1 //1 is the process id
     3. Network X.X.X.X wildcard (e.g., 0.0.0.255) area 0 //wildcard is the opposite of subnet mask



Verify using PING and TRACERT/TRACEROUTE

Deadline: See 'Teams' Assignment section

Lecture 6 Outline

- **Network Layer (TCP/IP)**
  - Routing protocol (RIP)
    - RIP operation
    - RIP v1 & v2
    - Class exercise 8
  - Open Shortest Path First (OSPF)
    - Operations
    - Shortest Path Algorithm (Dijkstra)
    - Router types
    - Subdivided areas
    - Class exercise 9
- **Internet Control Message Protocol (ICMP)**
  - **Implementation**
  - **Header**
  - **Use cases**
  - **Class exercise 11**

Internet Control Message Protocol (ICMP)

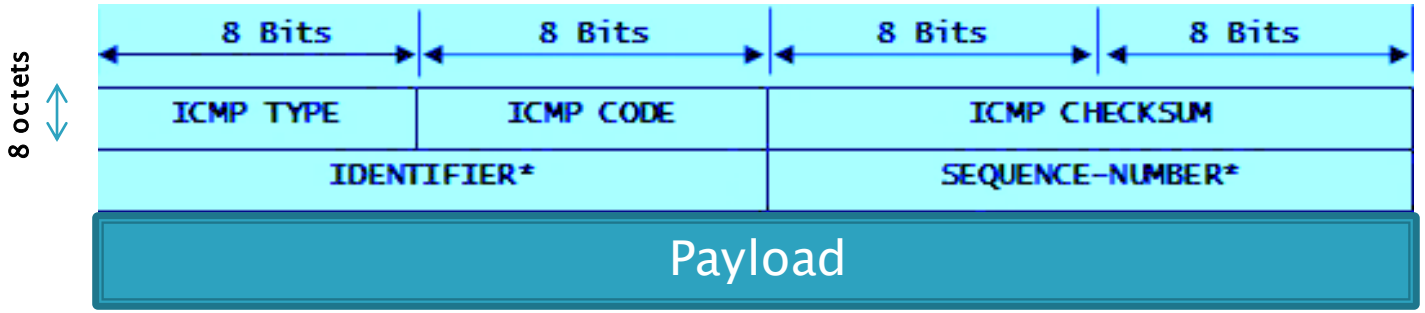
- If an intermediary device fails, or if a destination device is disconnected from the network, data cannot be delivered
  - The IP basic design does not notify the sender (reliably) that a data transmission has failed
- ICMP is a part of TCP/IP protocol stack that was specified in RFC 792 (IPv4)
  - Used to send error messages (not application data) and operational information (indicating success or failure) when communicating with another IP address e.g., IP status, error messages between hosts and routers, …
  - Uses IP protocol to route its messages between hosts

Internet Control Message Protocol (ICMP) (cont.)

- Needs to be implemented with IP
  - Remember, IP is just a packet delivery system:
    - Transmits and routes datagrams from source to destination through a series of interconnected networks
    - It has a checksum in the IP header to detect lost bits
      - No error detection on the datagram payload though
    - Has no native mechanism for source host notification
  - This is where ICMP comes in:
    - It is used to report IP errors to the source host
- ICMP Message types:
  - 8: Echo, 0: Echo reply (i.e., PING)
  - 3: Destination unreachable
  - …

→ Complete reference:
https://www.iana.org/assignments/icmp-parameters/icmp-parameters.xhtml

ICMP Header (1 /2)



* Not part of ICMP: Can be used arbitrarily by the user

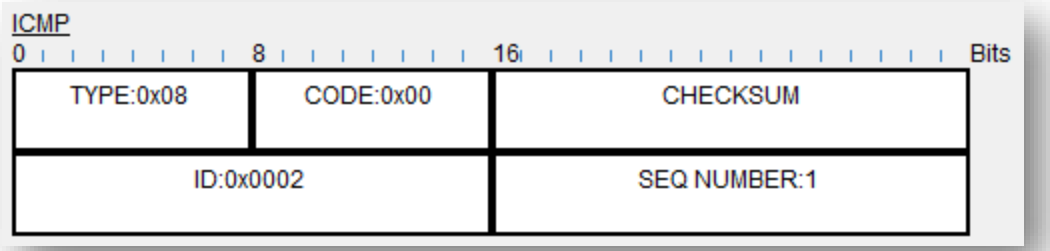
- Beside reporting delivery errors back to the source of the packet
  - It does not correct the encountered network problem; it merely reports the problem
  - It does not propagate information about network changes to routers
  - The status of the delivered packet gets reported only to the source device

ICMP Header (2/2)

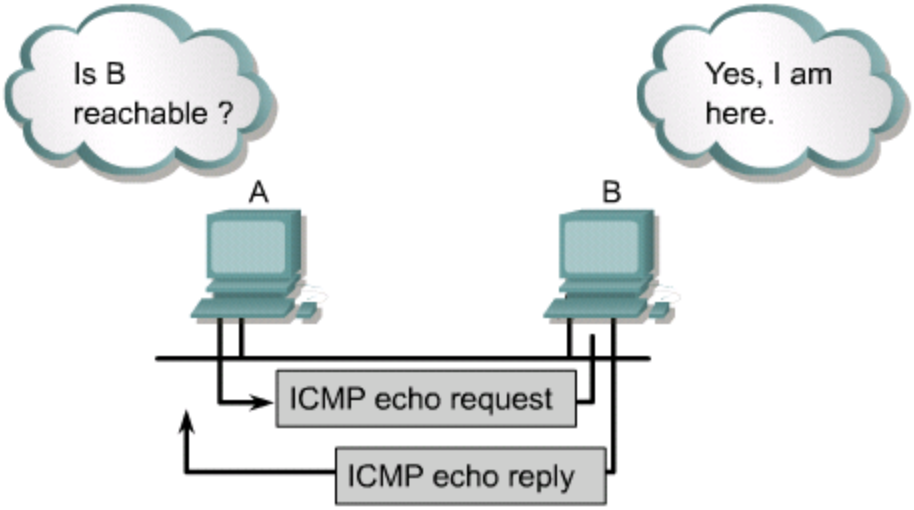
Wireshark

```
Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x5550 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 11 (0x000b)
    Sequence Number (LE): 2816 (0x0b00)
    [Request frame: 21]
    [Response time: 31.140 ms]
  Data (32 bytes)
      Data: 6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869
      [Length: 32]
```

Cisco Packet tracer

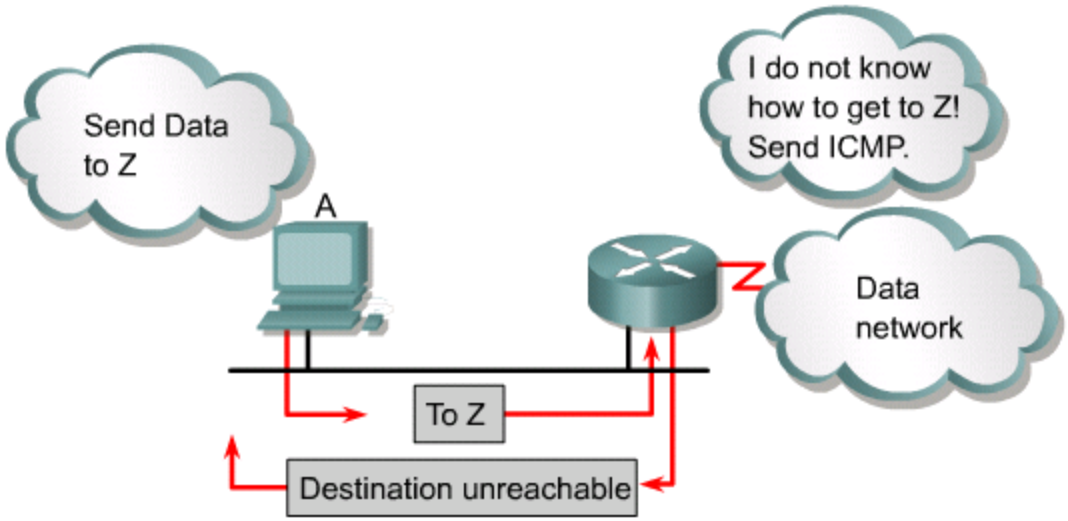


Using ping to test destination reachability (cont.)



Traffic generated by the `ping` command

Destination unreachable



An ICMP destination unreachable meassage is sent if:

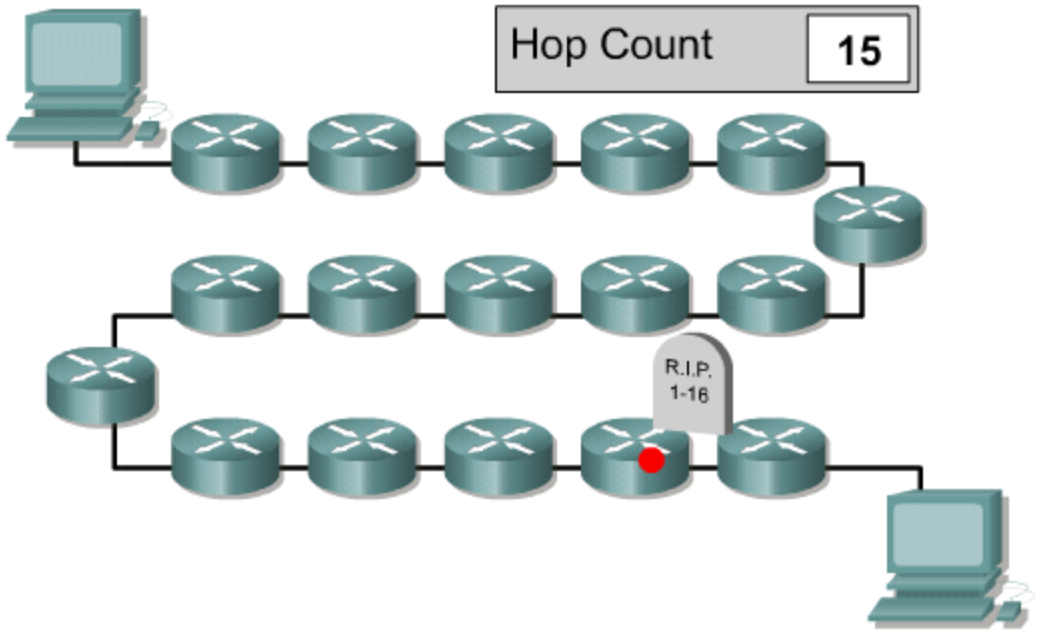
- Host or port unreachable
- Network unreachable

Possible causes

- For instance, the sending device may address the datagram to a non-existent IP address or to a destination device that is disconnected from its network
- Routers can also be points of failure e.g., if a connecting interface is down or if the router does not have the information necessary to find the destination network
  - If a destination network is not accessible, it is said to be an unreachable network

Detecting excessively long routes

ℹ Max Hop count in RIP

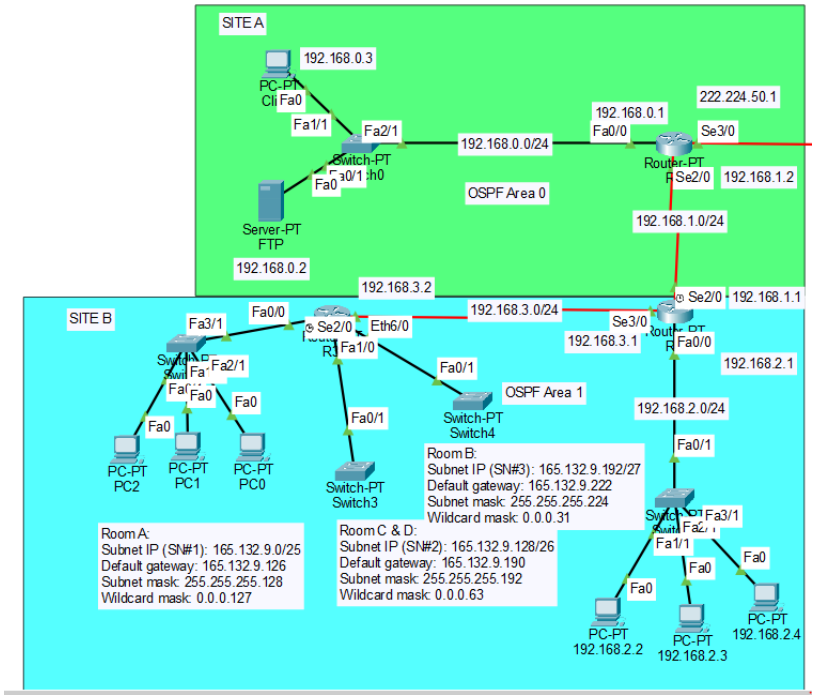


Detecting excessively long routes (cont.)

- Limitations of the routing protocol can result in destinations being unreachable (e.g., Hop 15 count limit in RIP)
- Whether the actual path includes a circular routing path or too many hops, the packet will eventually exceed the maximum hop count
  - This is also known as reaching its time-to-live (TTL), because the TTL value 'typically' matches the maximum hop count defined by the routing protocol
  - As each router processes the packet, it decreases the TTL value by one, and eventually when the value reaches zero, the packet is discarded
- ICMP uses a time exceeded message to notify the source device that the TTL of the packet has been exceeded

Exercise 11: Practical work

- Use your existing cisco packet tracer file (from last class exercise):
  1. Generate ICMP packets:
     1. Generate echo request (and reply)
     2. Generate network unreachable response
  2. View the network packet in simulation mode, take screenshots and place them in a document file including your observations [e.g., What do you see in a specific header field? Does the field value corresponds to a specific octet? If yes, which one is it (e.g., last, first?)]



Alternatively, you can use Wireshark

Use PING and TRACERT/TRACEROUTE commands

Lecture 6 ends here

- Course Slides: Go to MS Teams:
  'Introduction to Computer Networks - Spring 2024 | BSc'
  -> Files section

- Send your questions by email:
  mohammad-salman.nadeem@epita.fr
  OR via direct message using MS Teams

- Thank You!