Introduction to Data Networks

1. **Course number and name:** 020INRES1 Introduction to Data Networks

2. **Credits and contact hours:** 6 ECTS credits, 3x1:15 contact hours

3. **Instructor's or course coordinator's name:** Marc Ibrahim

4. **Text book:**
   a. **Other supplemental materials:**
      Professor slides, CCNA R&S online material.

5. **Specific course information**
   a. **Catalog description:**
      This course introduces the basic principles and the various techniques governing the operation of data networks and the Internet, with particular focus on the TCP / IP stack protocols. It covers the architecture of data networks and the Internet; Circuit and packet switching; Protocols and standardization bodies; OSI and TCP / IP layers; Access mechanisms and Ethernet/Wifi technologies in local area networks; The switched architecture of local area networks; IP (IPv4 and IPv6); Routing; Designing IP addressing; Transport protocols (TCP and UDP) and their reliability mechanisms, WEB, mail, DNS and DHCP services; Socket programming, the basic concepts of security. On a more practical level, this teaching unit offers a set of practical exercises that introduces the student to the implementation of a network and configuration of the switching equipment; The use of network simulation tools and protocol analysis; Socket programming. This is a blended course offering the Semester 1 of Cisco CCNA Routing & Switching online material.

   b. **Prerequisites:**

   c. **Required:** Required for CCE students

6. **Specific goals for the course**
   a. **Specific outcomes of instruction:**
      – Recognize communication mechanisms and protocols implemented in data networks.
      – Develop and implement an IP addressing plan in an enterprise network.
      – Understand and use basic network services and applications in IP networks (WEB, mail, DNS, DHCP, etc.).
      – Design and implement an enterprise network with basic services.
      – Analyze and diagnose the operation of an IP network.
      – Use sockets to program applications that can communicate over the network.
      – Understand the basic concepts of network security.

b. KPI addressed by the course:

KPI	a2	b3	e1	e3	k2	k3
Covered	x	x	x	x	x	x
Assessed	x	x	x	x	x	x
Give Feedback						

7. Topics and approximate lecture hours:

- Introduction (1 lecture)
  a. Towards a connected world
  b. Network ingredients
  c. Network classification
  d. Current trends and emerging technologies

- Networking fundamentals (3 lectures)
  a. Protocols
  b. OSI and TCP/IP models
  c. Switching principles
  d. Loss and delay

- Network access (2 lectures)
  a. Physical layer overview
  b. Data link layer: LLC and MAC
  c. Access mechanisms
  d. LAN switching

- Networking equipment (routers and switches) configuration (1 lecture)

- Diagnosis and simulation tools: Wireshark and Packet Tracer (2 lectures)

- Ethernet (3 lectures)
  a. Ethernet frame and addressing
  b. Physical layer evolution
  c. ARP protocol
  d. Ethernet switching

- Building my first network (2 lab sessions)

- Network layer (6 lectures)
  a. IPv4 and IPv6 protocols
  b. IP addressing in enterprise network.
  c. Routing principles, routing table configuration and analysis, NAT/PAT.
  d. ICMPv4 and ICMPv6 protocols

- IP addressing and routing case study using simulation (3 lab sessions)

- Transport layer (3 lectures)
    a. Transport services
    b. Introduction to UDP and TCP protocols.
    c. Reliability in TCP: acknowledgments, numbering, flow control, congestion control.

- Application layer (4 lectures)
    a. Application architectures
    b. Understand and use Networking services: HTTP, mail, DNS, DHCP, Telnet, etc.

- Application and transport layer analysis on Wireshark (2 lab sessions)

- Introduction to Socket programming under Python (4 lab sessions)

- Case study: building an enterprise network(2 lab sessions)
    a. Requirements
    b. IPP addresses planning
    c. Equipment and servers configuration
    d. Test and diagnosis.

- Introduction to network security (4 lectures)
    a. Security services
    b. Cryptography principles: symmetric-key and PKI.
    c. Mail security
    d. SSL
    e. PGP