UAB
Universitat Autònoma de Barcelona

Network Management and Administration 2026/2027

Code: 102776
Credits: 6

Degree programme	Type	Course
Computer Engineering	OB	3
Computer Engineering	OP	4

Contact lecturer

Name : Remo Suppi Boldrito

Email : remo.suppi@uab.cat

Teaching staff

Joan Josep Piedrafita Farras

Group languages

You can consult this information at the end of the document.

Prerequisites

Recommendations: to have passed the subjects Foundations of Computing, Computer Organisation, Operating Systems and Networks

Objectives

With this subject, the student will obtain the necessary knowledge for the administration and management of computer networks. The student will be able to apply this knowledge in aspects of general configuration and typical services as well as in monitoring, performance analysis, disaster recovery and security.

Learning outcomes

1. Manage time and resources available. Work in an organized manner .
2. Estimate the risks associated to high performance computer systems, in terms of their guarantee and security.
3. Apply knowledge of the security of high performance computer systems.
4. Design components to guarantee the security of high performance computer systems.
5. Apply knowledge of computer networks to design high performance computer networks.
6. Analyse communication requirements in high performance computer systems.
7. Design computer networks for high performance computer systems.
8. Develop a mode of thought and critical reasoning.

Contents

Topic 1: Network management.

- Introduction to Gnu / Linux, Virtualization. Cgroups, Containers (LXC, Docker)
- Administration of networks in Gnu/Linux systems (interconnection of private/public networks, IPv4/6).
- Basic services (DNS/secureDNS, DHCP, LDAP/NIS/AD, SSH).
- Network storage (NFS, DFS, SMB/CIF, CDN).
- Management of integrated networks (WAN, Mobile, Domestic, LAN, IoT).
- Software Defined Networks (SDN)

Topic 2: Network management.

- Standard management models (OSI, Internet).
- Functional areas (configuration, benefits, security, fault, accounting).
- Introduction to SNMP, MIB.
- Monitoring tools (tcpdump, Icinga/Nagios, Netdata, MRTG)

Topic 3: Network security

- PKI Infrastructure and Digital Certificates (Certifying Entity).
- Authentication: Passwords, Hashing (Hash Functions)
- Access Authentication: PAM, LDAP.
- Firewalls and proxies (Iptables, nftables, Apache Proxy, SOCKS, Squid).
- Virtual private network (WireGuard, OpenVPN).
- Security in wireless networks and virtual networks (MITM, DMZ, Brute-Force / SYN Flood Attacks).
- Detection of intrusions and vulnerabilities (Nmap, Snort, OpenVas, Honeypots). Mitigation D/DoS.
- Security in services (WAF).

Learning activities and methodology

Title	Hours	ECTS	Learning outcomes
Conceptual classroms	22.1	0.884	1, 2, 3, 4, 5, 8
Applied concepts	11.5	0.46	2, 3, 4, 5, 8
Labs	11.5	0.46	1, 2, 3, 4, 6, 7, 8
Home work	100	4	

The subject contains three sections where each one will have a methodology appropriate to the type of teaching provided:

- Conceptual classrooms: the theoretical and conceptual aspects of the contents of the subject.
- Applied concepts: collaborative group work in the classroom with tutoring by the teacher in each group and in each session. The group will have to develop certain subjects assigned by the teacher.
- Practical sessions: sessions of groups of 2 students. These students will develop labs about specific items in the laboratory of the subject (the student must have 80% attendance at these sessions).

To promote learning and interaction, it is recommended that each student have a digital device with a browser (preferably laptop) in order to connect to the subject's cloud.

Use of AI: In this course, the use of Artificial Intelligence (AI) technologies is permitted as an integral part of the development of coursework, provided that the final result reflects a significant contribution by the student in terms of analysis and personal reflection. Students must clearly identify which parts have been generated using this technology, specify the tools used, and include a critical reflection on how these tools have influenced both the process and the final outcome of the activity. Failure to disclose the use of AI transparently

will be considered a breach of academic integrity and may result in a grade penalty for the activity or more severe sanctions in serious cases. The teaching staff reserves the right to request an interview with students in order to clarify the concepts and exercises submitted.

Annotation: within the schedule set by the centre or degree programme, 15 minutes of one class will be reserved for students to evaluate their lecturers and their courses or modules through questionnaires.

Assessment

Continuous assessment activities

Title	Weight	Hours	ECTS	Learning outcomes
Labs	45%	2.5	0.1	1, 5, 6, 7
General concepts	30%	1.4	0.056	2, 4, 5, 6, 7, 8
Applied concepts	25%	1	0.04	3, 4, 5, 7, 8

Given its practical nature, this course does not offer a single final assessment option.

a) Assessment Process and Activities

Student evaluation will be based on the following components:

- General Concepts: Automated individual tests (via UAB's Virtual Campus) covering theoretical content. The average score must be 5 or higher.
- Applied Concepts: Automated individual tests (via UAB's Virtual Campus) covering applied content. The average score must be 5 or higher.
- Practical Work: Evaluation of collaborative and personal work in the UAB practice infrastructure and through individually conducted tests. The average score must be 5 or higher.

b) Assessment Schedule

Evaluation is continuous, with submissions made through the Virtual Campus. Dates may change due to unforeseen circumstances, with updates communicated through the Virtual Campus, the official communication platform between instructors and students.

c) Re-assesment Process

Students who fail any component (general/applied concepts or practical work) but maintain an overall weighted score of $\geq$3 may re-assesment the failed component.

- Final grades only include components with $\geq$5. If any component remains below 5 after re-assesment, the course is failed, and the final grade will be the weighted average (if <5) or 4.5 (if weighted average is $\geq$5).
- Re-assesment dates will be published in the School's official exam calendar.

d) Grade Review

- General/Applied Concepts: As grading is automated, students may request a report on failed topics. Answers will not be reviewed unless demonstrable errors exist in the solutions.
- Practical Work: Students who fail may request a review of sections scored below 5 with th professor.

e) Grading

- Honors Distinction (MH): Awarded to students with a final grade $\geq$9.00, following professors deliberation (maximum 5% of enrolled students). This distinction is not automatic and considers both academic

excellence and additional merits.
- No Show: All missing assessments results in a \"Not Evaluated\" mark.

f) Academic Irregularities & Plagiarism

Any irregularity (plagiarism, unauthorized AI use in assessments, prohibited devices, etc.) will result in a 0 for the affected component, with no re-assesment option. If the component is mandatory to pass, the course will be failed immediately.

In future course editions, students committing irregularities will not have any assessment components recognized.

h) Evaluation of Repeating Students

Students who previously passed practical work (grade $\geq$5) may request validation for the current academic year only.

i) For exceptional circumstances, the School's protocol for "rescheduling assessment activities" will be applied.

Bibliography

(BR) Administració/Administració Avançada del Sistema Operatiu GNU/Linux. (OCW-UOC) Edició 2016.	http://hdl.handle.net/10609/60687 http://hdl.handle.net/10609/60685	Remo Suppi i Josep Jorba	Document electrònic

- (BR) Network Security : Private Communications in a Public World. Kaufman, Charlie; Perlman, Radia; Speciner, Mike; Perlner, Ray. 2022/3rd ed.
- (BR) The practice of system and network administration. Limoncelli, Tom; Hogan, Christina J.; Chalup, Strata R. 2017/3rd edition
- Network security essentials : applications and standards. Stallings, William- 2017/ 6th edition
- Network security. Perez, Andre. 2014 1st edition.
- (BR) Network management : principles and practice. Subramanian, Mani. 2011/2nd ed.
- Network management : concepts and practice, a hands-on approach. Burke, J. Richard. 2004
- Fundamentos de seguridad en redes : aplicaciones y estándares. Stallings, William; González Rodríguez, Manuel. 2003/2ª edition.
- Firewalls and Internet security: repelling the Wily Hacker. Cheswick, William R.; Bellovin, Steven M.; Rubin, Aviel D. 2003/2nd edition.
- Network intrusion detection Northcutt, Stephen. 2003/3rd edition

Software

All the software (applications and operating systems) used in the subject is open source software, including VirtualBox, Opennebula and Linux (and all its applications).

Course groups and languages

The information provided is provisional until November 30. After this date, you will be able to consult the language of each group through this link. To access the information, you will need to enter the course CODE

Type of teaching	Group	Language	Semester	Shift
(PAUL) Classroom practices	430	Catalan	first semester	morning-mixed
(PLAB) Practical	431	Catalan/Spanish	first semester	morning-mixed

laboratories				
(PLAB) Practical laboratories	432	Catalan/Spanish	first semester	morning-mixed