Universidad de Alcalá

TEACHING GUIDE

Network Management and Security

Degree in
Computer Engineering

Universidad de Alcalá

Academic Year 2021/2022

4th Year - 1st Semester

Approved by the School Board on July 6, 2021

TEACHING GUIDE

Course Name:	**Network Management and Security**
Code:	**591004**
Degree in:	**Computer Engineering**
Department and area:	**Automática** **Telematics Engineering**
Type:	**Compulsory**
ECTS Credits:	**6.0**
Year and semester:	**4th Year, 1st Semester**
Teachers:	Por definir
Tutoring schedule:	Consultar al comienzo de la asignatura
Language:	English

1. COURSE SUMMARY

Network management and security are two fundamental activities that must be applied to an enterprise that depends on ICTs so that their information services work inside an expected service level and with a reasonable cost. The need for network management can be found in lots of scenarios (home networks, organizations and enterprise networks, and big ICTs enterprises, such as Internet service providers or cloud service providers, smartgrids, smart cities infrastructure, etc. It is important to take into account the business model of the enterprise in order to guarantee a good value for money. Network management and security do not only apply to the network infrastructure, but it also covers network services (web server, database, mail server…) and any device connected to the network (print server, automation controller…). This has led to a strong demand of engineers with expertise in design, deployment, security, and management of communication networks, and this subject aims to cover that demand.

The main objective of this course is to study methodologies, tools, and mechanisms to manage and secure the services and elements of a network in order to guarantee a predefined level of service and security. During the classes, the student will learn mainly based on practical activities and real-world use cases, directly related to the theory lessons, and the student will also practice their knowledge with the main management and security tools available in the market.
The main concepts covered are:

- Organization of a NOC (Network Operation Center).
- Knowledge and practice of management technologies and tools: SNMP, Syslog, Netconf, Netflow, Vagrant, Ansible…).
- Knowledge and exercise of methodologies applied in different management areas.
- Methodologies to evaluate the security level in an ICT infrastructure and selection of security control mechanisms to improve it.
- Use cases: data networks, cloud infrastructure, IoT platforms, etc.

Prerequisites y Recommendations: Previous knowledge of Computer Networks is recommended.

2. SKILLS

Basic, Generic and Cross Curricular Skills.

This course contributes to acquire the following basic, generic and cross curricular skills:

en_CG3 - Ability to design, develop, evaluate and ensure accessibility, ergonomics, usability and security of computer systems, services and applications, as well as the information they manage.

en_CG9 - Ability to solve problems with initiative, decision making, autonomy and creativity. Ability to know how to communicate and transmit the knowledge, skills and abilities of the profession of Computer Engineering Engineer.

en_CB1 - That students have demonstrated to possess and understand knowledge in an area of study that is based on general secondary education, and is usually found at a level that, although supported by advanced textbooks, also includes some aspects that involve knowledge from the forefront of their field of study.

en_CB2 - That the students know how to apply their knowledge to their work or vocation in a professional manner and possess the competencies that are usually demonstrated through the elaboration and defense of arguments and the resolution of problems within their area of study.

en_CB3 - That students have the ability to gather and interpret relevant data (usually within their

area of study) to make judgments that include a reflection on relevant social, scientific or ethical issues.

en_CB4 - That students can transmit information, ideas, problems and solutions to both a specialized and non-specialized public.

en_CB5 - That the students have developed those learning skills necessary to undertake further studies with a high degree of autonomy.

en_TRU1 - Capacity of analysis and synthesis.

en_TRU2 - Oral and written competencies.

en_TRU3 - Ability to manage information.

en_TRU4 - Autonomous learning skills.

en_TRU5 - Team work.

Specific Skills

This course contributes to acquire the following specific skills:

en_CIC6 - Ability to understand, apply and manage the warranty and security of computer systems.

en_CIC8 - Ability to design, deploy, manage and manage computer networks.

Learning Outcomes

After succeeding in this subject the students will be able to:

RA1. Apply the objects of appropriate MIBs for the resolution of a network management and services problem and design particular MIBs in cases where it is necessary.

RA2. Apply network management techniques and services based on monitoring, flow analysis, and event notification to solve fault management, performance, accounting, and security problems.

RA3. Use tools to implement different network and service management techniques, and automatic configuration.

RA4. Apply different methodologies to determine the security levels of infrastructure, as well as the control mechanisms to reach the desired level.

RA5. Associate different technologies and methodologies of network management and security to apply them to a specific use case of infrastructure and telematic services, in different areas.

3. CONTENTS

Contents Blocks	Total number of hours
Network management and Internet services • **Introduction to network management**. Data models and objectives. General architecture. Standards. Information model: SMI. ASN.1 syntax. Examples of MIBs. • **Communication model**. SNMP protocol. Security of SNMP. BER codification. Codification exercises. • **Evolution of SNMP**: Architecture and applications. Security model. Access control model. • **Configuration of an SNMP agent.** • **Network management based on notifications**: trap, syslog. • **Network management tools**: Network topology discovery, MIB navigation, monitoring, alarms, remote management, scripts, integrated management tools.	32 hours
Application areas in network management • **Introduction to FCAPS** • **Failure detection and correction management:** Network failures. Problem reporting, symptoms and causes. Diagnosis and solution of problems. Information sources: monitoring, alarms, polling, logs. Examples of failure indicators. Anomaly and event correlation detection. Failure prevention. • **Performance management and optimization:** Performance indicators (delays, usage, congestion, bottlenecks,…) Local and end-to-end control. Passive vs. active monitoring. Measure interpretation (peaks, average,...). Network capacity planning (router, switch, Internet connection,…). • **Configuration and operation management:** Motivation. Configuration parameters (relationships, consistency,…). Comprehensive configuration. Configuration processes. Automatic configuration: scripting. Expect. Puppet. Ansible.	12 hours
Information security management • **Introduction to information security:** Security threats and risks. Protection measures. Security audits. Information security management systems. • **Introduction to security management:** Risk analysis. Countermeasures (information protection, firewalls, intrusion detection...) Security policies and methodologies. Other security mechanisms.	12 hours
Network management and security project Analysis of the different network management areas applying them to a specific use case (telco networks, company networks, sensors networks, etc.). It might also consist of a detailed analysis of an advance network management technology already studied in the course or stated as a future trend.	

4. TEACHING - LEARNING METHODOLOGIES. FORMATIVE ACTIVITIES.

4.1. Credits Distribution

Number of on-site hours:	58 hours (56 hours on-site +2 exams hours)
Number of hours of student work:	92
Total hours	150

4.2. Methodological strategies, teaching materials and resources

The teaching strategy of the course is divided into 3 sections: classroom learning and laboratory practice sesiións in small groups, individual and group office hours, and finally individual and group student work.

Classroom learning in combination with laboratory practice sessions in small groups

- Concept presentations and/or reviews, mainly practical scenarios.
- Company visits and/or conferences.
- Problem-solving.
- Hands-on lab sessions: oriented to consolidate concepts, and for students to get used to different tools and to provide methodologies to enhance their study. Also to be applied in their future careers (data analysis, strategies, decision-making, etc.).
- Oral presentations and other activities.

Individual and group office hours (face–to–face or on-line)

- Solving student questions.
- Support to autonomous learning.

Individual or group student work

- Reading assignments.
- Activities: exercises, information lookup, resolution of practical cases.

5. ASSESSMENT: procedures, evaluation and grading criteria

Preferably, students will be offered a continuous assessment model that has characteristics of formative assessment in a way that serves as feedback in the teaching-learning process.

5.1. PROCEDURES

The evaluation must be inspired by the criteria of continuous evaluation (Learning Assesment

Guidelines, LAG, art 3). However, in compliance with the regulations of the University of Alcalá, an alternative process of final evaluation is made available to the student in accordance with the Learning Assesment Guidelines as indicated in Article 10, students will have a period of fifteen days from the start of the course to request in writing to the Director of the Polytechnic School their intention to take the non-continuous evaluation model adducing the reasons that they deem convenient. The evaluation of the learning process of all students who do not apply for it or are denied it will be done, by default, according to the continuous assessment model. The student has two calls to pass the subject, one ordinary and one extraordinary.

Ordinary call

In the ordinary call, the student will be evaluated through the Continuous Evaluation process, except for the exceptions mentioned above.

Extraordinary Call

The extraordinary call will consist of a test similar to the one presented in the evaluation system through the Final Exam.

5.2. EVALUATION

EVALUATION CRITERIA

The assessment criteria measure the level at which the competencies have been acquired by the student. For that purpose, the following are defined::

CE1. The student shows that he knows how to select the appropriate objects of the MIBs to solve a management problem, designing a particular MIB in case of not finding the appropriate objects.

CE2. The student shows mastery in the use of the main technologies to make polling and notifications, applied to the resolution of problems of network management and telematic services, and the knowledge of the existence of other alternative technologies.

CE3. The student is able to use and configure network management and configuration tools, to collect data and analyze results, in order to meet the management objectives in their different areas.

CE4. The student shows criteria to select and apply methodologies to determine and manage the security level of an ICT infrastructure and to determine the appropriate control measures to apply to reach a certain security level.

CE5. The student shows capacity and initiative to justifiably associate different technologies and methodology in the resolution of a concrete problem of network management and information security, distinguishing the main areas in which network management is applicable.

GRADING TOOLS

The work of the student is graded in terms of the assessment criteria above, through the following tools:

1. **Partial Quiz Assessments (PEI)**: Consists of a written test of solving practical problems and questions about the topics of the MIB information model and SNMP protocol.
2. **Personal Work with deliverables (E)**: consists of assessing the student's mastery of different techniques with personal work done at home and/or in the classroom. Final evaluation students will take them at home.
3. **Laboratory Tests (PL)**: the laboratory teacher will evaluate the knowledge application and skills of the students using network management tools in small group sessions

4. **Final Quiz Assessments (PEF)**: It consists of two exercises: 1) the presentation of a project of free theme about network and services management, developing these project the student must integrate different techniques and methodologies seen in the course, and 2) a written exercise resolving a problem like these one in the project, but with a limited time, and a theme chosen by the teacher. 50% is assigned to the project and another 50% to the exercise.

GRADING CRITERIA

In the **ordinary call-continuous assessment** the relationship between the competencies, learning outcomes, criteria, and evaluation instruments is as follows.

Skill	Learning Outcomes	Evaluation criteria	Grading Tool	Contribution to the final mark
CG3, CG9, CIC6, CIC8	RA1, RA2, RA4	CE1, CE2, CE4	E	15%
CG3, CG9, CIC6, CIC8	RA1, RA3, RA4	CE2, CE3, CE4	PL	15%
CG3, CG9, CIC8	RA1, RA2	CE1, CE2	PEI	30%
CG3, CG9, CIC6, CIC8	RA1, RA2, RA4, RA5	CE1, CE2, CE4, CE5	PEF	40%

The grade of "Not presented" will be awarded to the student who, having opted for the continuous evaluation procedure, meets any of the following requirements:

When the student has failed to attend at least 60% of the classes in small groups.
When the student has not delivered, at least 60% of the requested work.
When the student has not delivered, at least 100% of the requested practices. This criterion is equally applicable to final evaluation students.

In the **ordinary call-final evaluation**, the relationship between the competencies, learning outcomes, criteria, and evaluation instruments is as follows.

Skill	Learning Outcomes	Evaluation criteria	Grading Tool	Contribution to the final mark
CG3, CG9, CIC6, CIC8	RA1, RA2, RA4	CE1, CE2, CE4	E	15%
CG3, CG9, CIC6, CIC8	RA1, RA3, RA4	CE2, CE3, CE4	PL	15%
CG3, CG9, CIC6, CIC8	RA1, RA2, RA4, RA5	CE1, CE2, CE4, CE5	PEF	70%

Extraordinary call

In the extraordinary call, the PEF test is carried out, and students who have not passed the E or PL tests, will be able to undergo their evaluation again.

Skill	Learning Outcomes	Evaluation criteria	Grading Tool	Contribution to the final mark
CG3, CG9, CIC6, CIC8	RA1, RA2, RA4	CE1, CE2, CE4	E	15%
CG3, CG9, CIC6, CIC8	RA1, RA3, RA4	CE2, CE3, CE4	PL	15%
CG3, CG9, CIC6, CIC8	RA1, RA2, RA4, RA5	CE1, CE2, CE4, CE5	PEF	70%

6. BIBLIOGRAPHY

6.1. Basic Bibliography

- Provided Documentation: Theoretical concepts, practice books, exercises.
- Network Management Fundamentals. Ph. D. Alexadre Clemm. Cisco Press. 2007. (Available in: https://proquest.safaribooksonline.com/1587201372)

6.2. Additional Bibliography

- **Additional bibliography**
  - Automated Network Management Systems. Dougloas E. Comer. Prentice Hall. 2006.
  - Advances in Network Management. Jianguo Ding. CRC Press. 2009.
  - SNMP, SNMPv2M snmpV3 AND rmon 1 AND 2. (3ª edition). William Stallings. Addison Wesley. 1999.
  - Network Management Standards. 2ª edition. Uyless Black. McGrawHill.
  - Network Management, a practical perspective. Allan Leinwand, Karen Fang. Addison Wesley. 1993.
  - Communication Network Management. Kornel Terplan. Prentice Hall. 1992.

- **Internet References**
  - http://www.simple-times.org
  - http://wwwsnmp.cs.utwente.nl
  - http://www.asn1.com
  - http://net-snmp.sourceforge.net/
  - http://www.mrtg.com/

Disclosure Note

The University of Alcalá guarantees to its students that, if due to health requirements the competent authorities do not allow the total or partial attendance of the teaching activities, the teaching plans will achieve their objectives through a teaching-learning and evaluation methodology in online format, which will return to the face-to-face mode as soon as these impediments cease.