Universidad de Alcalá

Gestión de Redes y Seguridad

Grado en Ingeniería de Computadores

Universidad de Alcalá

Curso Académico 2019/2020

Curso 4º – Cuatrimestre 1º

GUÍA DOCENTE

Nombre de la asignatura:	Gestión de Redes y Seguridad
Código:	591004
Titulación en la que se imparte:	Grado en Ingeniería de Computadores
Departamento y Área de Conocimiento:	Automática
Carácter:	Obligatoria de tecnología específica
Créditos ECTS:	6
Curso y cuatrimestre:	Cuarto curso, primer cuatrimestre
Profesorado:	Elisa Rojas Sánchez (coordinadora). Bernardo Alarcos Alcázar.
Horario de Tutoría:	Se indicará el primer día de clase.
Idioma en el que se imparte:	Español/English Friendly

1.a PRESENTACIÓN

La gestión de redes y servicios y la seguridad de la información son actividades fundamentales que se deben de llevar a cabo en una empresa u organización dependiente de las TIC, para que sus servicios de información funcionen con el nivel de servicio esperado y a un coste razonable. Podemos encontrar la necesidad de la gestión de red en una diversidad de entornos, desde sencillas redes de hogares o pequeñas empresas, a redes de organizaciones o empresas medianas, o grandes empresas del sector de las TICs que dan servicios de acceso a Internet (ISP) o de transporte de datos interconectando ISPs. La fuerte evolución de la actividad económica en el mundo TIC crea una demanda de profesionales con competencias en el diseño, despliegue, securización y gestión de las redes de comunicación, y en este sentido la asignatura de gestión de red colabora en gran medida en la formación de esta especialización.

Es importante resaltar la importancia de la gestión de red y servicios desde el punto de vista empresarial, como uno de los componentes esenciales que maximizan la relación calidad/coste en la gestión de la información a través de los servicios telemáticos. La gestión de red no sólo se centra en los dispositivos de red, sino que abarca cualquier dispositivo o servicio telemático que gestiona la información de la organización. Así, por ejemplo, una impresora en red o servicios como pueden ser el correo electrónico, una aplicación distribuida de contabilidad o una plataforma de comercio electrónico son elementos susceptibles de ser gestionados y asegurados en función del valor que tengan para la organización.

La asignatura pretende aportar al estudiante diferentes conocimientos y capacidades sobre el uso de metodologías, herramientas y mecanismos para gestionar y asegurar los servicios y elementos de red para garantizar un determinado nivel de servicio y seguridad.

En el desarrollo de la asignatura se pretende capacitar al estudiante con propuesta de actividades eminentemente prácticas de forma que vayan aprendiendo las mejores prácticas

en la gestión de red y la teoría asociada, a base de prácticas con las principales herramientas utilizadas en el mercado.

La asignatura se centra en los aspectos siguientes:

- Organización de un Centro de Gestión de Red.
- Conocimiento de la tecnología de Gestión de red Internet y las herramientas involucradas en su aplicación (SNMP, Syslog, Netconf, Netflow…).
- Conocimiento de metodologías utilizadas en la gestión de red aplicadas a diferentes áreas de gestión.
- Conocimiento de las metodologías para evaluar el nivel de seguridad de una infraestructura TIC y seleccionar controles de seguridad a aplicar para mejorarlo.
- Casos de uso: redes de operadores de datos, Infraestructura en la nube, plataformas IoT…

Prerrequisitos y Recomendaciones
Se recomienda tener conocimientos previos de Redes de Computadores.

1.b COURSE SUMMARY

Network management and security is a 6 ECTS course included in the first semester - fourth year of the degree in Computer Engineering.
Network and services management and information security are fundamental activities that must be applied to an enterprise that depend on ICTs, in order to their information services woks inside an expected service level and with a reasonable cost. The need for management can be found in a lot of scenarios (home networks, organizations and enterprises networks, and big ICTs enterprises as Internet services providers or cloud services providers, smart cities infrastructure or IoT... It is important to take into account the business model of the enterprise in order to guarantee a good value for money. The management not only apply to the network infrastructure, it also covers network services (web server, data base, mail server…) and any device connected to the network (print server, automation controller…).
The main objective of this course is to study methodologies, tools and mechanisms to manage the services and elements of a network in order to guarantee a predefined level of service.
The main concepts covered are:

- Organization of a NOC (Network Operation Center).
- Knowledge and practice of management technology and tools: SNMP, Syslog, Netconf, Netflow, RMON…).
- Knowledge and exercise of methodologies applied in different managements areas.
- Use cases: data networks, cloud Infrastructure, IoT platforms…

2. COMPETENCIAS

Competencias generales:

CG3 Capacidad para diseñar, desarrollar, evaluar y asegurar la accesibilidad, ergonomía, usabilidad y seguridad de los sistemas, servicios y aplicaciones informáticas, así como de la información que gestionan.

CG9 Capacidad para resolver problemas con iniciativa, toma de decisiones, autonomía y creatividad. Capacidad para saber comunicar y transmitir los conocimientos, habilidades y destrezas de la profesión de Ingeniero Técnico en Informática.

Competencias Específicas:

CIC6 Capacidad para comprender, aplicar y gestionar la garantía y seguridad de los sistemas informáticos.

CIC8 Capacidad para diseñar, desplegar, administrar y gestionar redes de computadores.

Resultados de Aprendizaje

RA1	Aplicar los objetos de MIBs apropiados para la resolución de un problema de gestión de redes y servicios y diseñar MIBs particulares en casos de que sea necesario.
RA2	Aplicar técnicas gestión de red y servicios basados en monitorización, análisis de flujos y notificación de eventos para resolver problemas de gestión de fallos, prestaciones, contabilidad y seguridad.
RA3	Utilizar herramientas con las que aplicar las diferentes técnicas de gestión de red y servicios y de configuración automática.
RA4	Aplicar las metodologías para determinar el nivel de seguridad de una infraestructura y los controles para llegar al nivel deseado.
RA5	Asociar diferentes tecnologías y metodologías de gestión y seguridad de red y servicios para aplicarlas a un caso concreto de infraestructura y servicios telemáticos, en las diferentes áreas.

3. CONTENIDOS

Bloques de contenido (se pueden especificar los temas si se considera necesario)	Total de clases, créditos u horas

Gestión de red y servicios en Internet. Introducción a la gestión de red. Modelo de datos: Objetivos. Esquema general. Estándares. Modelo de información: SMI. Sintaxis ASN.1. Ejemplos de MIBs existentes. Modelo de comunicaciones. Protocolo SNMP. Seguridad del protocolo. Evolución de SNMP: Arquitectura y aplicaciones. Modelo de Seguridad. Modelo de control de acceso. Configuración de un agente de gestión SNMP. Gestión basada en notificación: Trap, syslog. Uso de herramienta de gestión: descubrimiento de una red, navegación por MIBs, monitorización, alarmas, gestión remota, uso de scripts, herramientas integradas de gestión.	32 horas
Áreas de aplicación de la gestión de red **Introducción a FCAPS.** **Gestión de Detección y corrección de fallos.** Fallos de red. Informes de problemas, síntomas y causas. Solución y diagnosis de problemas. Fuentes de información: monitorización, alarmas, sondeos, logs. Ejemplos de indicadores de fallos. Detección de anomalías y correlación de eventos. Prevención de fallos. **Gestión de Valoración y optimización del Rendimiento.** Indicadores de rendimiento: retardos, utilización, congestión, cuellos de botella… Medidas locales vs end-to-end. Observación pasiva vs sondas activas. Interpretación de medidas (picos de utilización, medias). Planificación de capacidades (router, conmutador, conexión Internet…). **Gestión de Configuración y operación.** Motivación. Parámetros de configuración (relaciones, consistencia…). Configuración integral. Retroceso en los procesos de configuración. Configuración automática: scripting.	12 horas

<u>Gestión de la seguridad de la información</u> **Introducción a la seguridad de la información.** Amenazas y riesgos de seguridad. Medidas de protección. Auditorías de seguridad. **Sistemas de gestión de la seguridad de la información.** Introducción a la gestión de la seguridad. Análisis riesgos en los sistemas de la información. Controles de la seguridad. Políticas de seguridad. Metodologías de gestión de la seguridad de la información.	12 horas
<u>Proyecto de gestión de red y seguridad</u> Analiza diferentes áreas de gestión aplicadas a un caso concreto (red de datos de operador, red de una organización, infraestructura crítica, red de sensores…).	

4. METODOLOGÍAS DE ENSEÑANZA-APRENDIZAJE.-ACTIVIDADES FORMATIVAS

4.1. Distribución de créditos (especificar en horas)

Número de horas presenciales:	56 horas + 4 horas de examen de evaluación
Número de horas del trabajo propio del estudiante:	Preparación de las clases, aprendizaje autónomo, preparación de ejercicios, pruebas y prácticas, preparación de la prueba final: Total: 90 horas
Total horas	150 horas.

4.2. Estrategias metodológicas, materiales y recursos didácticos

Clases Prácticas (en grupos reducidos)	Presentación y/o revisión de conceptos de carácter eminentemente práctico. Visitas a empresas y/o conferencias. Resolución de problemas. Sesiones prácticas de laboratorio: orientadas a consolidar los conceptos presentados previamente, así como a familiarizar al estudiante con las herramientas y metodologías de apoyo al estudio de la materia y futuro desempeño profesional (mejorar la comprensión de los conceptos de gestión de red, mecanismos aplicados a la gestión, análisis de datos de gestión y toma de decisiones sobre estrategias a seguir para conseguir los objetivos). Presentaciones orales y otras actividades.
Tutorías individuales, grupales y vía web (foro, correo, etc.)	Resolución de dudas. Apoyo al aprendizaje autónomo.
Trabajo autónomo	Lecturas. Realización de actividades: ejercicios, búsqueda de información, análisis de datos.

5. EVALUACIÓN: Procedimientos, criterios de evaluación y de calificación

Preferentemente se ofrecerá a los alumnos un sistema de evaluación continua que tenga características de evaluación formativa, de manera que sirva de realimentación en el proceso de enseñanza-aprendizaje por parte del alumno. Para ello se establecen los siguientes

Procedimientos de Evaluación

Convocatoria Ordinaria.

En la convocatoria ordinaria el alumno será evaluado mediante el proceso de Evaluación Continua. En situaciones excepcionales, debidamente justificadas, podrá acogerse a un sistema de evaluación mediante Examen Final. Para ello debe solicitarlo por escrito al Director del centro, en las dos primeras semanas de su incorporación, indicando las razones que le impiden seguir el sistema de Evaluación Continua. En este caso, el Director del centro comunicará la resolución en un máximo de 15 días. Si el alumno no recibe respuesta en ese plazo de tiempo, se considera estimada la solicitud.

Convocatoria Extraordinaria.

La convocatoria extraordinaria consistirá en una prueba similar a la que se plantee en el sistema de evaluación mediante Examen Final.

Criterios de Evaluación.

El alumno será evaluado de acuerdo con los siguientes criterios:

CE1. El alumno muestra que sabe seleccionar los objetos apropiados de las MIBs para resolver un problema de gestión diseñar una MIB particular en caso de no encontrar los objetos apropiados.

CE2. El alumno muestra dominio en el uso de las principales tecnologías para hacer sondeos y notificaciones, aplicados a la resolución de problemas de gestión de red y servicios telemáticos, y el conocimiento de la existencia de otras tecnologías alternativas.

CE3. El alumno es capaz de usar y configurar herramientas de gestión y configuración de red y servicios, incluyendo la recopilación de datos y el análisis resultados con el objetivo de cumplir con los objetivos de la gestión en sus diferentes áreas.

CE4. El alumno muestra criterio para seleccionar y aplicar metodologías que le ayuden a determinar y gestionar el nivel de seguridad de una infraestructura TIC y determinar los controles apropiados a aplicar para alcanzar un determinado nivel de seguridad.

CE5. El alumno muestra capacidad e iniciativa para asociar justificadamente diferentes tecnologías y metodología en la resolución de un problema concreto de gestión de red y seguridad de la información, distinguiendo las principales áreas en las que tiene aplicación la gestión de red.

Instrumentos de calificación.

Esta sección específica los instrumentos de evaluación que serán aplicados a cada uno de los criterios de Evaluación.

1. Pruebas de Evaluación Intermedia (PEI): Consistente en una prueba escrita de resolución de problemas prácticos y cuestiones sobre los temas del modelo de información MIB y SNMP.
2. Trabajos personales con entregables (E): Consistentes en evaluar el dominio del alumno de diferentes técnicas con trabajos personales realizados en casa y/o en clase:
3. Pruebas de seguimiento (PL): el profesor de laboratorio valorará en grupo pequeño si el alumno ha adquirido las habilidades y conocimientos para el uso de diferentes herramientas y técnicas de gestión de red.:
4. Pruebas de Evaluación final (PEF): Consistente en la presentación de un proyecto de tema libre de Gestión en el que el alumno debe integrar diferentes técnicas y metodologías vistas, y un ejercicio escrito en el que se plantea un problema similar al del proyecto, pero con un tiempo limitado, y un tema elegido por el profesor. Se asigna un 50% al trabajo y otro 50% al ejercicio.

En la convocatoria ordinaria y extraordinaria – la evaluación continua la relación entre los criterios, instrumentos y calificación es la siguiente.

Evaluación Continua, Convocatoria ordinaria.

Competencia	Resultado Aprendizaje	Criterio de Evaluación	Instrumento de Evaluación	Peso en la calificación
CG3, CG9, CIC6, CIC8	RA1,RA2, RA4	CE1, CE2, CE4	E	15%
CG3, CG9, CIC6, CIC8	RA1, RA3, RA4	CE1, 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%

Evaluación Continua, Convocatoria Extraordinaria.

En la convocatoria extraordinaria se realizará la prueba PEF y los alumnos que no hayan superado las pruebas prácticas (E o PL) podrán someterse a su evaluación de nuevo.

Competencia	Resultado Aprendizaje	Criterio de Evaluación	Instrumento de Evaluación	Peso en la calificación
CG3, CG9,	RA1, RA2, RA4	CE1, CE2, CE4	E	15%

CIC6, CIC8	RA1, RA3, RA4	CE1, CE3, CE4	PL	15%
	RA1, RA2, RA4, RA5	CE1, CE2, CE4, CE5	PEF	70%

Como criterio general, aquellos alumnos en convocatoria ordinaria que no se presenten a la evaluación de todas las prácticas se considerarán No Presentados.

Evaluación Final, convocatoria Ordinaria y Extraordinaria

Aquellos estudiantes que tengan reconocido el derecho a evaluación final, según fija la normativa de la UAH, deben realizar un examen final que incluye cuestiones teóricas y la realización de uno o más ejercicios, con un peso del 100% de la calificación final. Este procedimiento será el mismo tanto en la convocatoria ordinaria como extraordinaria.

Competencia	Resultado Aprendizaje	Criterio de Evaluación	Instrumento de Evaluación	Peso en la calificación
CG3, CG9, CIC6, CIC8	RA1-RA5	CE1-CE5	PEF	100%

6. BIBLIOGRAFÍA

- Documentación proporcionada: Conceptos teóricos, cuaderno de prácticas, ejercicios.
- Network Managment Fundamentals. Ph. D. Alexadre Clemm. Cisco Press. 2007. https://proquest.safaribooksonline.com/1587201372

Bibliografía Complementaria

- Automated Network Managment 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.

Referencias en Internet

- http://www.simple-times.org

- http://wwwsnmp.cs.utwente.nl
- http://www.asn1.com
- http://net-snmp.sourceforge.net/
- http://www.mrtg.com/

Universidad de Alcalá

Teaching Guide

Network Management and Security

Degree in Computer Engineering

University of Alcalá

Academic Year 2019/2020
4th Year– 1st Term

Universidad de Alcalá

Teaching Guide

Course name:	**Network Management and Security**
Code:	**591004**
Degree:	**Degree in Computer Engineering**
Departament y Knowledge Area:	**Computer Engineering / Telematics Engineering**
Type:	**Obligatory of specific technology**
ECTS credits:	**6**
Year and Term:	**4th year, 1ST Term**
Teaching Staff:	Elisa Rojas Sánchez (coordinator) Bernardo Alarcos Alcázar
Office Hours:	Check it with the teaching staff
Language:	**Spanish/English Friendly**

1. COURSE SUMMARY

Network management and security are two fundamental activities that must be applied to an enterprise that depend 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 enterprises 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 does not only apply to the network infrastructure, but it also covers network services (web server, data base, 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 with the theory lessons, and the student will also practise 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 technology and tools: SNMP, Syslog, Netconf, Netflow, RMON…).
- Knowledge and exercise of methodologies applied in different managements 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

General skills:

CG3 Ability to design, develop, evaluate and ensure the accessibility, ergonomics, usability and safety systems, services and applications, as well as the information they manage.

CG9 Ability to solve problems with initiative, decision making, autonomy and creativity. Ability to communicate and transmit knowledge and skills of the profession of Technical Engineer.

Specific skills:

CIC6 Ability to understand, implement and manage the guarantee and security of computer systems.

CIC8 Capacity for design, deploy, administer and manage computer networks.

Learning Outcomes

Students successfully passing this course 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 an 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

Content blocks	Number of sessions, credits or 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. Network management based on notifications: trap, syslog. Remote monitoring: RMONv1. Other models: Netflow, NETCONF, IPFIX, web network management. Traffic analysis: Netflow. Configuration of an SNMP agent. Network management tools: Network topology discovery, MIB navigation, monitoring, alarms, remote management, scripts, comprehensive management tools (OPManager).	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, etc.). Network capacity planning (router, switch, Internet connection,…). **Configuration and operation management** Motivation. Configuration parameters (relationships, consistency,…). Comprehensive configuration. Configuration processes. Automatic configuration: scripting.	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 METHODOLOGY. FORMATIVE ACTIVITIES

4.1. Credit distribution

Class hours:	56 hours + 4 hours of assessment
Student work hours:	Class preparation, autonomous learning, problem, lab and quiz preparation, final exam preparation: Total: 90 hours
Total hours	150 hours.

4.2. Methodological strategies, materials and resources

Clases Prácticas (en grupos reducidos)	• 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, group and online office hours	• Solving student questions. • Support to autonomous learning.
Autonomous student work	• Reading assignments. • Activities: exercises, information look up, data analysis.

5. EVALUATION: Procedures and criteria for evaluating and grading

Preferably students will be offered a system of continuous evaluation that has characteristics of formative assessment, in order to provide feedback in the process of teaching and learning by students. For this purpose the following evaluation procedures are set :

Evaluation Procedure.

Ordinary Call

In the ordinary call the student will be assessed by Continuous Assessment (EC) process. In duly justified exceptional situations, it may benefit from a system of evaluation by Final Exam. To do this, the student must apply in writing to the center manager in the first two weeks at the beginning of the course, indicating the reasons that prevent him to follow continuous assessment. In this case, the center manager will communicate the decision within a maximum of 15 days. If the student does not receive a response within that period, the request will be considered as accepted.

Extraordinary Call

The extraordinary session will consist of a similar quiz to that arising in the evaluation system by Final Exam.

Evaluation Criteria

Evaluation Criteria must address the extent of acquisition of skills by the student. For this purpose, the following ones 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 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.

Evaluation Instruments.

This section specifies the evaluation tools to be applied to each of the evaluation criteria.

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 class:

   E1. Analysis and interpretation of MIBs.

   E2. Codification of SNMP messages.

E3. Exercises to resolve problems using SNMP and MIBS, applied to the different FCAPS management areas.

E4. Remote monitoring using RMON.

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:

PL1. Configuration of an SNMP agent.

PL2. Configuration of a Syslog distributed system.

PL3. Configuration of notifications system based on SNMP and particular MIBs.

PL4. Configuration of RMON.

PL5. Management tools using graphic interface.

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.

In the ordinary and extraordinary call of the continuous and final evaluation, the relationship between the criteria, instruments and qualification is as follows.

Ordinary Call, Continuous Evaluation.

Competences	Learning Outcomes	Evaluation Criteria	Evaluation Instruments	Score weighting
CG3, CG9, CIC6, CIC8	RA1, RA2, RA4	CE1, CE2, CE4	E	15%
CG3, CG9, CIC6, CIC8	RA1, RA3, RA4	CE1, 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%

Extraordinary Call, Continuous Evaluation.

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

Competences	Learning Outcomes	Evaluation Criteria	Evaluation Instruments	Score weighting
CG3, CG9, CIC6, CIC8	RA1, RA2, RA4	CE1, CE2, CE4	E	15%
	RA1, RA3, RA4	CE1, CE3, CE4	PL	15%

	RA1, RA2, RA4, RA5	CE1, CE2, CE4, CE5	PEF	70%

As a general criterion, those students in ordinary call who do not show up for the evaluation of all practices will be considered as Not Submitted.

Final Evaluation, Ordinary and Extraordinary call

Those students who have recognized the right to final evaluation, according to the regulations of the UAH, must take a final exam that includes theoretical questions and the realization of one or more exercises, with a weight of 100% of the final grade. This procedure will be the same both in the ordinary and extraordinary call.

Competences	Learning Outcomes	Evaluation Criteria	Evaluation Instruments	Score weighting
CG3, CG9, CIC6, CIC8	RA1-RA5	CE1-CE5	PEF	100%

6. BIBLIOGRAPHY

- Provided Documentation: Theoretical concepts, practice books, exercises.
  - Network Management Fundamentals. Ph. D. Alexadre Clemm. Cisco Press. 2007.

    https://proquest.safaribooksonline.com/1587201372

- 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/