



Facultad de Ingeniería

Redes II

4 CRÉDITOS



A. Información del profesor

Nombre del profesor

Ing. Dennis Donis

Ing. Carlos Portillo

e-mail

djdonisd@correo.url.edu.gt crportillos@correo.url.edu.gt

Horario:

TEÓRICA:

Viernes de 18:00 a 19:20 horas

PRÁCTICA:

Viernes de 16:30 a 17:50 horas (Sección 01) Sábado de 08:30 a 09:50 horas (Sección 02)



B. Información general

Descripción

El curso de Redes de Computadoras II, amplia los conocimientos obtenidos en el curso de redes de Computadoras I, con un enfoque especializado al área de networking avanzado que le permita al estudiante contar con una base de conocimiento para poder preparar el examen de certificación inicial CCNA. El curso incluye temas adicionales relativos a Redes SDN y NFV, así como a Internet de las Cosas (IoT) y 5G.

Modalidad

Presencial



Facultad de Ingeniería



El egresado landivariano se identifica por:

Pensamiento lógico, reflexivo y analógico	Pensamiento crítico	Resolución de problemas
Habilidades de investigación	Uso de TIC y gestión de la información	Comunicación efectiva, escrita y oral
Comprensión lectora	Compromiso ético y ciudadanía	Liderazgo constructivo
Aprecio	y respeto	

por la diversidad e interculturalidad

Creatividad

COMPETENCIAS ESPECÍFICAS (propias del curso)

Competencia 1:

Identifica y diseña topologías de redes LAN complejas, escalables y redundantes. Explica la forma en que las redes VLAN segmentan dominios de difusión en la red.

Competencia 2:

Conoce los medios a través de los cuales se comunican las redes y los conceptos de seguridad básicos asociados al diseño de ellas.

Competencia 3:

Identifica la función que los protocolos de ruteo dinámico tienen y que hacen posible la comunicación a través de distintas redes de datos que comparten su información de ruteo de manera automática.

Competencia 4:

Entiende la terminología y operaciones generales de NAT y sus distintas implementaciones: estática, dinámica y sobrecargada.

Competencia 5:

Entiende la estructura y asignación de direcciones IPv6 a través de ejercicios prácticos.

Competencia 6:

Identifica la función de la capa de aplicación y la manera en que las aplicaciones, los servicios y los protocolos que están dentro de la capa de aplicación hacen posible la comunicación a través de las redes de datos a través de simulaciones y casos de aplicación.

Competencia 7:

Entiende acerca de las amenazas de seguridad de red más comunes y aplica mecanismos para mitigar su riesgo, por ejemplo, a través del uso de segmentación de la red, listas de acceso, Firewalls, encriptación, entre otros.



Facultad de Ingeniería

Competencia 8:

Conoce y entiende el funcionamiento de herramientas y protocolos para monitoreo de redes e infraestructura, así como herramientas de diagnóstico y automatización de tareas.

Competencia 9:

Conoce, entiende y aplica los conceptos en los que están basadas las redes de nueva generación, mediante su definición en software.



METODOLOGÍA

Este curso se desarrollará a través de los siguientes métodos de aprendizaje-enseñanza:

Aprendizaje invertido

«La exposición de saberes se realiza por medio de documentos, videos y otros materiales por parte del estudiante. El tiempo de sesión síncrona¹ se dedica a la discusión, resolución de problemas y actividades prácticas bajo la supervisión del profesor».

Aprendizaje basado en problemas (ABP)



«Metodología centrada en el aprendizaje, en la investigación y reflexión que siguen los alumnos para llegar a una solución ante un problema planteado. Desarrolla aprendizajes activos a través de la resolución de problemas y casos. Puede desarrollarse de manera sincrónica o asíncrona»



Facultad de Ingeniería

PROGRAMACIÓN

COMPETENCIA 1

Identifica y diseña topologías LAN complejas, escalables y redundantes. Explica la forma en que las redes VLAN segmentan dominio de difusión en la red, describe la operación y ventajas del protocolo STP. Configura los protocolos DTP, VTP, STP y soluciona los problemas asociados. Configura EtherChannel y el protocolo HSRP y soluciona problemas asociados a través de prácticas y casos de aplicación.

Saber conceptual (contenido temático)

- 1. Ethernet y Protocolos de Enlace de Datos
 - 1.1. ETHERNET
 - 1.1.1. Capa física de Ethernet clásica
 - 1.1.2. El protocolo de subcapa MAC de la Ethernet clásica
 - 1.1.3. Funcionamiento de Ethernet, MAC addresses, ARP, switches, VLANs y troncales.
 - 1.2. VLAN
 - 1.2.1. Control de Broadcast
 - 1.2.2. Seguridad
 - 1.2.3. Flexibilidad y escalabilidad
 - 1.2.4. Pertenencia de VLAN
 - 1.2.5. VLANs Estáticas
 - 1.2.6. VLANs Dinámicas
 - 1.2.7. Identificación de VLANs Marcado de Frames
 - 1.2.8. Métodos para identificar VLANs
 - 1.3. Protocolo Troncal de VLAN (VTP)
 - 1.3.1. Modos de operación de VTP
 - 1.3.2. Poda de VTP
 - 1.4. Ruteo entre VLANs
 - 1.4.1. Configuración de VLANs
 - 1.4.2. Asignación de puertos de un Switch a una VLAN
 - 1.4.3. Configuración de puertos Troncales
 - 1.4.4. Configuración de ruteo entre VLANs
 - 1.4.5. Conmutación de capa 3 y SVI
 - 1.5. Etherchannel y HSRP
 - 1.5.1. Conceptos de agregación de enlaces
 - 1.5.2. Protocolos de redundancia de primer salto

Saber procedimental (habilidades y destrezas)

- Analiza y diseña redes locales escalables y redundantes a través de casos de aplicación.
- Entiende y resuelve problemas asociados a la redundancia de la LAN por medio de ejercicios prácticos.
- Entiende y utiliza protocolos para garantizar la redundancia de la puerta de enlace y la agregación de anchos de banda en topologías jerárquicas en casos de aplicación.

Saber actitudinal (conductas observables)

- Escucha con atención las explicaciones del curso.
- Participa activamente en las actividades de clase.
- Trabaja de forma colaborativa con sus compañeros.





Facultad de Ingeniería



Realiza los trabajos asignados en tiempo.

Indicador de logro 1 (resultado):

Implementa redes locales escalables y redundantes por medio de modelos de diseño y protocolos de segmentación, agregación y redundancia.

COMPETENCIA 2

Conoce los medios a través de los cuales se comunican las redes y los conceptos de seguridad básicos asociados al diseño de ellas.

Saber conceptual (contenido temático)

- 2. Tecnologías de redes inalámbricas
 - 2.1. Estándares IEEE 802.11
 - 2.1.1. Comparación de estándares
 - 2.2. Seguridad en redes inalámbricas WEP, WPA, WPA2.

Saber procedimental (habilidades y destrezas)

- Entiende el funcionamiento de los estándares que rigen la comunicación de redes inalámbricas.
- Entiende y utiliza protocolos de conexión seguros en la implementación de redes inalámbricas.

Saber actitudinal (conductas observables)

- Escucha con atención las explicaciones del curso.
- Participa activamente en las actividades de clase.
- Realiza las tareas y laboratorios asignados en tiempo.

Indicador de logro 2 (resultado):

Mediante la aplicación de los conceptos de diseño es capaz de diseñar esquemas de asignación de red funcionales acordes a los problemas que enfrenta.

CEAT
Contro de Ensoñarza, Aprendizaje y Tecnología Educativa

Programa del curso



Facultad de Ingeniería

COMPETENCIA 3

Identifica la función que los protocolos de ruteo dinámico tienen y que hacen posible la comunicación a través de distintas redes de datos que comparten su información de ruteo de manera automática.

Saber conceptual (contenido temático)

- 3. Protocolos de Enrutamiento Dinámico
 - 3.1. Características y operación de protocolo EIGRP
 - 3.1.1. Módulos dependientes del prot ocolo
 - 3.1.2. Descubrimiento de vecinos
 - 3.1.3. Protocolo de Transporte Confiable (RTP)
 - 3.1.4. Algoritmo de Actualización Difusa (DUAL)
 - 3.2. Uso de EIGRP para soportar redes grandes
 - 3.2.1. Descubrimiento y mantenimiento de rutas |
 - 3.3. + Configuración de EIGRP en Ruteadores
 - 3.3.1. Redistribución de rutas
 - 3.3.2. Balanceo de carga mediante EIGRP
 - 3.3.3. Verificación de EIGRP
 - 3.4. +Protocolo OSPF
 - 3.4.1. Habilitar OSPF
 - 3.4.2. Configuración de áreas OSPF
 - 3.4.3. Configuración de red con OSPF
 - 3.5. + Verificación de configuraciones OSPF
 - 3.5.1. Comandos de despliegue de información de OSPF
 - 3.5.2. Depuración de OSPF
 - 3.6. +Elección de OSPF DR y BDR
 - 3.6.1. Vecinos
 - 3.6.2. Adyacencias
 - 3.6.3. Elección de DR y BDR
 - 3.7. OSPF e Interfaces Loopback
 - 3.7.1. Configuración de interfaces Loopback
 - 3.7.2. Prioridad de interfaces OSPF
 - 3.8. Configuración de rutas sumarizadas EIGRP y OSPF
 - 3.9. Protocolo BGP
 - 3.9.1. Características
 - 3.9.2. Sistemas Autónomos
 - 3.9.3. Prevención de Loops
 - 3.9.4. Tipos de Mensajes
 - 3.9.5. Estados de Vecinos
 - 3.9.6. Atributos
 - 3.9.7. Anuncio y Recepción de Rutas
 - 3.9.8. Tabla de Vecinos
 - 3.9.9. Tabla BGP
 - 3.10. Sesiones BGP
 - 3.10.1. Configuración básica
 - 3.10.2. Enlaces redundantes
 - 3.10.3. Seguridad TTL

Saber procedimental (habilidades y destrezas)

- Entiende la forma en que funcionan los protocolos de ruteo dinámico.
- Entiende la forma en que interactúan los dispositivos que hacen uso de protocolos de ruteo dinámico.



Facultad de Ingeniería

• Hace uso de protocolos de ruteo dinámico para comunicar equipos ubicados en diferentes redes.

Saber actitudinal (conductas observables)

- Escucha con atención las explicaciones del curso.
- Participa activamente en las actividades de clase.
- Realiza las tareas y laboratorios asignados en tiempo.

Indicador de logro 3 (resultado):

Comprende la importancia del funcionamiento de los protocolos de ruteo dinámico en redes medianas y grandes ya que facilitan su administración aun cuando no están exentos de presentar retos durante escenarios de falla.

COMPETENCIA 4

Entiende la terminología y operaciones generales de NAT y sus distintas implementaciones: estática, dinámica y sobrecargada. Resuelve problemas relacionados a NAT apoyándose de comandos de depuración.

Saber conceptual (contenido temático)

- 4. NAT y PAT
 - 4.1. Razones para usar NAT
 - 4.2. Tipos de Traducción de Direcciones de Red
 - 4.3. Nombres de NATs
 - 4.4. Funcionamiento de NAT
 - 4.4.1. Configuración estática de NAT
 - 4.4.2. Configuración dinámica de NAT
 - 4.4.3. Configuración de PAT
 - 4.4.4. Verificación de NAT
 - 4.4.5. Prueba y Depuración de NAT

Saber procedimental (habilidades y destrezas)

- Configura NAT estáticas
- Configura NAT dinámicas
- Resuelve problemas asociados al funcionamiento de NAT.

Saber actitudinal (conductas observables)

- Escucha con atención las explicaciones del curso.
- Participa activamente en las actividades de clase.
- Realiza las tareas y laboratorios asignados en tiempo.

Indicador de logro 4 (resultado):

Tiene la capacidad de implementar NAT y sus variantes en una red.



Facultad de Ingeniería

COMPETENCIA 5

Entiende la estructura y asignación de direcciones IPv6 a través de ejercicios prácticos.

Saber conceptual (contenido temático)

- 5. IPV6
 - 5.1. Razones para usar IPv6
 - 5.2. Beneficios y casos de uso de IPv6
 - 5.3. Direccionamiento y Expresiones IPv6
 - 5.3.1. Expresiones abreviadas
 - 5.3.2. Tipos de dirección
 - 5.3.3. Direcciones especiales
 - 5.4. Funcionamiento de IPV6
 - 5.4.1. Autoconfiguración
 - 5.4.2. Configuración de IPv6 en routers
 - 5.4.3. DHCP v6
 - 5.4.4. ICMP v6
 - 5.5. Protocolos de ruteo IPv6
 - 5.5.1. RIPng
 - 5.5.2. EIGRPv6
 - 5.5.3. OSPFv3
 - 5.6. Migración a IPV6
 - 5.6.1. Stack Dual
 - 5.6.2. Tunneling entre IPv4 e IPv6
 - 5.6.3. NAT-PAT
 - 5.7. Configuración de RIPng
 - 5.8. Configuración de OSPFv3

Saber procedimental (habilidades y destrezas)

- Entiende la estructura del encabezado de IPv6 en capa 3 y la estructura de una dirección IPv6 a través de ejercicios básicos.
- Entiende y aplica la asignación de direcciones IPv6 a través de ejercicios prácticos.
- Entiende y configura protocolos que implementan IPv6 a través de ejercicios prácticos y casos de aplicación.

Saber actitudinal (conductas observables)

- Escucha con atención las explicaciones del curso.
- Participa activamente en las actividades de clase.
- Realiza las tareas y laboratorios asignados en tiempo.

Indicador de logro 5 (resultado):

Entiende el funcionamiento básico de IPv6, estructura, direccionamiento y protocolos que lo implementan.



Facultad de Ingeniería

COMPETENCIA 6

Identifica la función de la capa de aplicación y la manera en que las aplicaciones, los servicios y los protocolos que están dentro de la capa de aplicación hacen posible la comunicación a través de las redes de datos a través de simulaciones y casos de aplicación.

Saber conceptual (contenido temático)

- 6. Qué es la capa de aplicación.
 - 6.1. Protocolos y servicios de capa de aplicación reconocidos
 - 6.2. Protocolo de resolución de nombres: DNS
 - 6.3. Protocolos web: HTTP, HTTPs
 - 6.4. Protocolos de correo electrónico: SMTP, POP, IMAP
 - 6.5. Protocolos de asignación de direcciones: DHCP
 - 6.6. Protocolos de transferencia de archivos: FTP
 - 6.7. Aplicaciones P2P
 - 6.8. Redes de distribución de contenido: CDNs, servicios de video streaming

Saber procedimental (habilidades y destrezas)

- Entiende la forma en que funcionan los protocolos web y de correo electrónico
- Entiende la forma en que funcionan e interactúan los protocolos de asignación de IPs y resolución de nombres de dominio.
- Entiende la forma en que funcionan los protocolos de transferencia de archivos.
- Entiende la forma en que funcionan las redes de distribución de contenido estático y de video streaming.

Saber actitudinal (conductas observables)

- Escucha con atención las explicaciones del curso.
- Participa activamente en las actividades de clase.
- Trabaja de forma colaborativa con sus compañeros.
- Realiza los trabajos asignados en tiempo.

Indicadores de logro 6 (resultado): Identifica y comprende el funcionamiento de los protocolos de la capa de aplicación y su interacción con las aplicaciones de usuario final.



Facultad de Ingeniería

COMPETENCIA 7

Entiende acerca de las amenazas de seguridad de red más comunes y aplica mecanismos para mitigar su riesgo, por ejemplo, a través del uso de segmentación de la red, listas de acceso, encriptación, entre otros.

Saber conceptual (contenido temático)

- 7. VPN y Seguridad en Redes
 - 7.1. Creación de redes seguras
 - 7.1.1. Metas al crear redes seguras
 - 7.1.2. Futuro de las redes seguras
 - 7.1.3. Firewall definición y tipos
 - 7.1.4. Zonas de seguridad (inside, outside, DMZ)
 - 7.2. Ataques de Denegación de Servicio DoS
 - 7.2.1. Tipos de ataques DoS
 - 7.2.2. Dificultad para detener ataques DoS
 - 7.2.3. ARP Poisoning
 - 7.3. Configuración de VPN
 - 7.4. Control de acceso a redes
 - 7.5. Seguridad Ethernet
 - 7.5.1. Protocolo de autenticación extendible EAP
 - 7.5.2. EAP sobre Radius
 - 7.6. Certificados digitales
 - 7.7. Entidad certificadora
 - 7.8. Seguridad en Redes Inalámbricas
 - 7.8.1. Acceso a redes inalámbricas
 - 7.8.2. Protección contra gemelo malvado punto de acceso
 - 7.8.3. Protección contra gemelo malvado man in the middle
 - 7.8.4. Ataque de congestión DoS

Saber procedimental (habilidades y destrezas)

- Conoce e implementa principios de seguridad en la creación de redes a través de ejercicios prácticos.
- Pone en práctica mecanismos de seguridad para asegurar la correcta autenticación de usuarios en redes inalámbricas a través de casos de aplicación.
- Entiende y utiliza protocolos de conexión seguros para la administración de dispositivos de red y transporte de datos.

Saber actitudinal (conductas observables)

- Escucha con atención las explicaciones del curso.
- Participa activamente en las actividades de clase.
- Realiza las tareas y laboratorios asignados en tiempo.

Indicador de logro 7 (resultado):

Tiene los conocimientos para diseñar e implementar redes de datos seguras con independencia de la infraestructura con que cuente para enfrentar los desafíos de seguridad.



COMPETENCIA 8

Conoce y entiende el funcionamiento de herramientas y protocolos para monitoreo de redes e infraestructura, así como herramientas de diagnóstico y automatización de tareas.

Saber conceptual (contenido temático)

- 8. QoS y Gestión de Redes
 - 8.1. Que es la calidad de servicio
 - 8.1.1. Funcionamiento de la calidad de servicio
 - 8.1.2. Técnicas para el manejo de calidad de servicio
 - 8.1.3. Mejores practicas
 - 8.1.4. Ventajas del uso de calidad de servicio
 - 8.2. Gestión de Redes
 - 8.2.1. Management Information Base (MIB)
 - 8.2.2. Protocolo de Administración de Red Simple (SNMP)
 - 8.2.3. Herramientas SNMPwalk (CLI) y MIB Browser (GUI)
 - 8.2.4. Sistemas NMS
 - 8.2.5. Comandos SNMP
 - 8.2.6. Seguridad SNMP
 - 8.2.7. Agentes y MIB
 - 8.3. RMONv1 (RFC 2819)
 - 8.4. RMONv2 (RFC 2021) versión mejorada
 - 8.5. Requerimientos de Monitoreo

Saber procedimental (habilidades y destrezas)

- Entiende y utiliza herramientas de monitoreo para administrar la salud de la red.
- Pone en práctica mecanismos de automatización de para el monitoreo de redes para mantener un adecuado funcionamiento de la red.

Saber actitudinal (conductas observables)

- Escucha con atención las explicaciones del curso.
- Participa activamente en las actividades de clase.
- Realiza las tareas y laboratorios asignados en tiempo.

Indicador de logro 8 (resultado):

Tiene la capacidad de utilizar herramientas de software para el monitoreo y automatización de redes, conociendo el estado de la red en todo momento.



COMPETENCIA 9

Conoce y entiende la necesidad de una variada gama de dispositivos los cuales deben establecer comunicación mediante el uso de tecnología de redes de última generación.

Saber conceptual (contenido temático)

- 9. Redes SDN y NFV
 - 9.1. Conceptos de virtualización
 - 9.1.1. Descripción general de la virtualización
 - 9.1.2. Desacoplamiento del hardware de red subyacente
 - 9.1.3. Eficiencia y agilidad de los recursos informáticos y de almacenamiento basados en software
 - 9.1.4. Desacoplamiento de los planos de control y reenvío
 - 9.1.5. Conceptos de hipervisor y máquina virtual
 - 9.1.6. Virtualización de redes y almacenamiento
 - 9.1.7. Orquestación
 - 9.2. + Redes SDN
 - 9.2.1. ¿Qué son las Redes definidas por software?
 - 9.2.2. Características de SDN
 - 9.2.3. Arquitectura de SDN
 - 9.2.4. Implementación de SDN
 - 9.3. NFV
 - 9.3.1. Arquitectura de NFV
 - 9.3.2. Funciones de red virtualizadas
 - 9.3.3. Infraestructura de virtualización de funciones de red
 - 9.4. Diferencias entre NFV y SDN
 - 9.5. Arquitectura de virtualización de funciones de red (NFV)
 - 9.5.1. Virtualización de red (NV) frente a virtualización de funciones de red (NFV)
 - 9.5.2. Requisitos de NFV
 - 9.5.3. Arquitectura y bloques de construcción de NFV
 - 9.6. Virtualización de funciones de red (NFV) aplicada
 - 9.6.1. Virtualización de aplicaciones de red
 - 9.6.2. NFV aplicado a redes móviles
 - 9.6.3. NFV aplicado a redes de entrega de contenido
 - 9.6.4. NFV aplicado a IMS
 - 9.6.5. SDN y OpenFlow
 - 9.6.6. Internet de las Cosas (IoT) y 5G
- 10. Internet de las Cosas (IoT) y 5G
 - 10.1. Introducción a IoT
 - 10.1.1. Definición del Internet de las Cosas
 - 10.1.2. Requerimientos, Funcionalidad y Estructura de IoT
 - 10.1.3. Tecnologías que habilitan a IoT
 - 10.1.4. Arquitecturas de IoT
 - 10.1.5. Protocolos de comunicación y redes de IoT
 - 10.2. Plataformas
 - 10.2.1. Microcontroladores (Arduino uno/mega2560, Raspberry-Pi, ARM)
 - 10.2.2. Almacenamiento en nube/servidor/interno
 - 10.3. Comunicación de Datos
 - 10.3.1.Inalámbrica/Cableada
 - $10.3.2.\mathsf{GSM},\,2\mathsf{g}\,,3\mathsf{g}\,,4\mathsf{g}\,\&\,5\mathsf{g}$
 - 10.3.3. Protocolos de capa de sesión MQTT y CoAP, HTTP-based M2M



Facultad de Ingeniería

10.4. Seguridad en IoT

10.4.1. Difusión de datos y preservación de la privacidad

10.4.2. Modelos de Confianza para IoT

10.4.3. Autenticación en IoT

Saber procedimental (habilidades y destrezas)

- Aplica los conceptos de virtualización tanto a SDN como a NFV a través de máquinas virtuales.
- Al resolver problemas de virtualización comprende la relación que guardan con el hardware subyacente.
- Conoce la dependencia de los protocolos de comunicación que tienen los dispositivos IoT para la transferencia de información medida por ellos.
- Comprende el uso de las distintas tecnologías de red en la comunicación de datos de las redes
 GSM.Error! Bookmark not defined.

Saber actitudinal (conductas observables)

- Escucha con atención las explicaciones del curso.
- Participa activamente en las actividades de clase.
- Realiza las tareas y laboratorios asignados en tiempo.

Indicador de logro 9 (resultado):

Tiene la capacidad de conectar dispositivos que hacen uso de nuevos protocolos de comunicación de manera segura.







a. Estrategias de evaluación sumativa

Estrategias	Puntaje
Tareas e investigaciones	10
Laboratorios semanales (16)	24
Proyecto final (1)	20
Exámenes cortos (3)	6
Exámenes parciales (2)	20
Examen final (1)	20
TOTAL	100

b. Estrategias de evaluación formativa

Técnicas formativas	Procedimiento
Retroalimentación	Se proporciona la resolución de todos los problemas de las hojas de trabajo y exámenes realizados.
Diálogo socrático	Preguntas y respuestas orales a ejemplos y problemas que se realizarán lo largo de la secuencia de aprendizaje.
Padlet colaborativo	Se utiliza en la actividad de contextualización y presentación del curso
Exámenes cortos	Problemas de aplicación del tema seleccionado.
Trabajos en pequeños grupos para resolver dudas	Hojas de trabajo que se resuelven de forma colaborativa entre estudiantes.
Citas individuales	Tutorías de retroalimentación solicitadas por el estudiante, por medios electrónicos





CALENDARIO DE REFERENCIA POR TEMAS

Fecha	Tema	Actividad de evaluación
Semana 1	Ethernet y Protocolos de Enlace de Datos	Laboratorio No. 1
Semana 2	Ethernet y Protocolos de Enlace de Datos	Laboratorio No. 2
Semana 3	Redes Inalámbricas y WiFi	Laboratorio No. 3
Semana 4	Protocolos de Enrutamiento Dinámico	Examen corto 1
(2 agosto)		Laboratorio No. 4
Semana 5	Protocolos de Enrutamiento Dinámico	Laboratorio No. 5
Semana 6	PRIMERA EVALUACIÓN PARCIAL	Primera evaluación parcial
(16 agosto)		Laboratorio No. 6
Semana 7	NAT y PAT	Laboratorio No. 7
Semana 8	IPv6	Laboratorio No. 8
Semana 9	IPv6 y Protocolos capa de aplicación	Examen corto 2
(6 septiembre)		Laboratorio No. 9
Semana 10	Protocolos capa de aplicación	Laboratorio No. 10
Semana 11	SEGUNDA EVALUACIÓN PARCIAL	Segunda evaluación parcial
(20 septiembre)		Laboratorio No. 11
Semana 12	VPN y Seguridad en Redes	Laboratorio No. 12
Semana 13	VPN y Seguridad en Redes	Laboratorio No. 13
Semana 14	QoS y Gestión de Redes	Examen corto 3
	, ·	Laboratorio No. 14
Semana 15	Redes SDN y NFV	Laboratorio No. 15
Semana 16	Redes SDN y NFV	Laboratorio No. 16
Semana 17	Asueto Día de todos los Santos	
(1 y 2 noviembre)	Asueto Día de todos los Muertos	
Semana 18	Repaso y proyecto final	Entrega de proyecto final
(8 y 9 noviembre)		
Semana 19	EXAMEN FINAL	Evaluación final
(15 de noviembre)		



Facultad de Ingeniería

REFERENCIAS BIBLIOGRÁFICAS

- <u>Texto:</u> KUROSE JAMES F., KAITH ROSE (2020), Computer Networking, A Top-Down Approach, 8th Edition. Pearson, United States.
- <u>Texto</u>: CCNA Routing and Switching Complete Study Guide Todd Lammle.
- Texto: Network Warrior Gary A. Donahue.