GESTIÓN DE REDES Y SERVICIOS

CURSO TEÓRICO-PRÁCTICO

DIRIGIDO A: Estudiantes y profesionales en las áreas de computación, informática, telecomunicaciones y sistemas.

MODALIDAD: El curso se realiza a distancia, de forma no-presencial, utilizando un DVD como material de apoyo, complementado con consultas en línea o por correo electrónico. En ese DVD se encuentran las presentaciones de las clases, artículos técnicos y libros electrónicos, guías para las experiencias prácticas, así como los programas y herramientas para efectuar dichas prácticas.

EQUIPAMIENTO: Disponer de PC o laptop de buenas prestaciones y acceso a Internet, preferiblemente sin restricciones impuestas por proxies y firewalls.

REQUISITOS DESEABLES: Conocimientos en el área de telecomunicaciones, redes y protocolos, especialmente TCP/IP. Familiaridad con el uso de computadoras, sistemas operativos (Windows, Linux, Android), redes de área local (LAN), redes inalámbricas Wi-Fi, Internet. Conocimiento instrumental del idioma inglés.

EVALUACIÓN: A lo largo del curso, el participante deberá realizar una serie de actividades. La realización con esmero, dedicación y constancia de las actividades planificadas, determinará el nivel de conocimientos, destrezas y competencias que el participante habrá adquirido al completar el curso. La evaluación del aprendizaje se realiza básicamente mediante cuestionarios y exámenes parciales (tests) sobre la teoría e informes sobre las prácticas.

- Al menos 7 cuestionarios sobre los tópicos de teoría: 25%
- Al menos 7 exámenes parciales (tests) sobre los tópicos de teoría: 25%
- Al menos 6 informes sobre 6 experiencias prácticas: 25%
- Examen final (test general) sobre al menos 7 tópicos de teoría: 25%

DOCENTE: Ing. Vincenzo Mendillo - Profesor Titular (UCV - USB - UNIMET - UCAB)

- Ingeniero Electricista (Especialidad: Telecomunicaciones) - Universidad Central de Venezuela
- Master of Science in Electronics - University of Southampton
- Live Senior Member IEEE - Institute of Electrical and Electronics Engineers
- Miembro de CriptoRed - Red de Criptografía y Seguridad de la Información
- Coordinador del Diplomado STIT en Seguridad en Tecnología Informática y Telecomunicaciones.
- Presidente y miembro fundador de ASOVESINFO (Asociación Venezolana de la Seguridad de la Información)

DESCRIPCIÓN DEL CURSO:
El explosivo desarrollo de las telecomunicaciones y de las tecnologías de la información (TI) ha incrementado enormemente la complejidad de las redes y la gama de servicios disponibles, lo cual resalta la importancia de la gestión de redes como uno de los componentes esenciales para maximizar la relación costos/prestaciones, mediante la utilización de modernas soluciones para configuración, supervisión y mantenimiento. En este curso se presenta una visión integrada sobre los principios, arquitecturas, plataformas, estándares y aplicaciones para la gestión de redes heterogéneas (voz, datos, video). Además se enseña el uso de métodos, técnicas, productos y herramientas que se requieren en las distintas áreas funcionales FCAPS de la gestión (fallas, configuración, contabilidad, desempeño, seguridad). Se procura la familiarización con los principales entornos de gestión de red y que se conozcan los productos existentes, tanto propietarios como de software libre. Se analiza el modelo gestor/agente y se describe el estándar existente para redes TCP/IP basado en SNMP. También se explican los nuevos modelos y paradigmas que han surgido, tales como WEBM, WMI, XML, Java, CORBA, .NET, SOA, ITIL. Otros tópicos que se incluyen son el estándar CMIS/CMIP de ISO y el estándar TMN de la UIT-T para redes de telecomunicaciones, incluyendo sistemas de soporte de operaciones (OSS).

OBJETIVO GENERAL:
Proporcionar las bases conceptuales de la gestión de redes y servicios, y además desarrollar experticia y competencia en métodos, técnicas, productos y herramientas que se requieren en las distintas áreas funcionales FCAPS que abarca la gestión: fallas, configuración, contabilidad, desempeño y seguridad.

OBJETIVOS ESPECÍFICOS:

- Utilizar protocolos de redes (TCP/IP) y sistemas operativos (Windows, Linux).
- Aplicar procedimientos y herramientas para el descubrimiento, supervisión y configuración de los recursos de la red.
- Diagnosticar y resolver problemas mediante herramientas específicas tales como analizadores de redes (sniffers).
- Implantar sistemas de gestión basados en SNMP para el monitoreo y control de redes y servicios.
- Gerenciar redes de telecomunicaciones públicas mediante TMN y sistemas de soporte de operaciones (OSS).
- Comparar los nuevos sistemas de gestión basados en el Web y en ambiente CORBA, XML, Java, .NET, SOA, ITIL.
- Evaluar y comparar las plataformas y productos disponibles para la gestión de redes y servicios.
- Gestionar fallas, eventos, errores, problemas en las redes y sistemas.
- Aplicar los principios de confiabilidad y mantenimiento para el análisis y predicción de fallas.
- Especificar los requisitos de calidad de servicio (QoS) y determinar los acuerdos de nivel de servicio (SLA).
- Utilizar los conceptos básicos de la teoría de colas para analizar la influencia del tráfico y la congestión sobre el desempeño.
- Identificar las amenazas, vulnerabilidades y riesgos existentes en el área de la seguridad y seleccionar las medidas de protección apropiadas.
- Gestionar sistemas de voz sobre IP y telefonía por Internet, identificando los problemas de calidad de servicio y los riesgos de seguridad.
- Operar con software especializado para la simulación, diagramación, visualización y documentación de redes, equipos y sistemas.

CONTENIDO PROGRAMÁTICO

1. INTRODUCCIÓN A LA GESTIÓN DE REDES Y SERVICIOS

Conceptos generales. Gestión, administración y gerencia. Planificación de capacidad. Gestión de redes y administración de sistemas. Gestionabilidad. Estándares OSI y TCP/IP. CMIP (*Common Management Information Protocol*) y SNMP (*Simple Network Management Protocol*). Gestión centralizada, distribuida y jerárquica. Gestión basada en Web y WBEM (*Web-Based Enterprise Management*). Gestión de computadoras de escritorio y DMI (*Desktop Management Interface*). WMI (*Windows Management Instrumentation*). Gestión basada en JAVA y agentes inteligentes. Gestión de dispositivos móviles inteligentes. Gestión distribuida (DCOM, CORBA). SOAP (*Simple Object Access Protocol*). ERP y sistemas de planificación de recursos empresariales. SAP, PeepleSoft. Aplicaciones Web distribuidas. NET y J2EE. Arquitectura orientada a servicios (SOA). ITIL (*Information Technology Infrastructure Library*).

2. MODELOS Y PLATAFORMAS DE GESTIÓN

Las múltiples dimensiones de la gestión. El modelo FCAPS (*fallas, configuración, contabilidad, desempeño, seguridad*) de OSI. El modelo OAM&P (*operación, administración, mantenimiento y aprovisionamiento*). El modelo TMN (*Telecommunications Management Network*) de UIT-T para redes públicas. Sistemas de soporte de operaciones (OSS). El modelo CAF del TeleManagement Forum (*cumplimiento, aseguramiento, facturación*). El mapa para operaciones en telecomunicaciones (TOM, eTOM). Plataformas y productos para la gestión de redes y servicios: Nagios, Zenoss, OpenNMS, JFFNMS, Ntop, Cacti, LoriotPro, Opsview, Hyperic, Big Brother, Webmin, SNMPc, Cisco Works, OpenView, Unicenter, Tivoli, Huawei.

3. SUPERVISIÓN DE REDES Y SERVICIOS

Selección de elementos a supervisar. Estado de los servicios. Monitor del sistema. Visor de sucesos. Órdenes NET de Windows y PowerShell. Órdenes TCP/IP. Supervisión mediante SNMP y RMON. Herramientas de monitoreo populares: Whatsup, Solarwinds, Spiceworks, The Dude, MRTG, PRTG. Supervisión de Windows. Analizadores de protocolo (sniffers) para redes cableadas e inalámbricas. Monitoreo mediante SNMP y RMON. Netflow. Notificación y registro de eventos mediante Syslog. Monitoreo activo mediante ping. Monitoreo de servidores Web. Planificación de capacidad.

4. SISTEMAS DE GESTIÓN MEDIANTE SNMP

Introducción a SNMP (*Simple Network Management Protocol*). Componentes básicos (agente, gestor, MIB). Tipos de mensajes (Get, Set, GetNext, Response, Trap). Formato de los mensajes. Autenticación y nombre de la comunidad. Estructura de la MIB y el OID. Estructura de la información de gestión (SMI) y síntaxis ASN. Grupos de variables MIB públicas y privadas. RMON. Agentes SNMP y MIB para Windows y Linux. Limitaciones de la primera versión de SNMP. Evolución de SNMPv1 hacia SNMPv2. Nuevos tipos de datos y de mensajes en SNMPv2. GetBulkRequest e InformRequest. Seguridad en SNMPv2. Características y arquitectura de SNMPv3. Modelos de seguridad USM y VACM. Coexistencia de SNMP v1, v2 y v3 y uso de proxy.

5. GESTIÓN DE FALLAS

Importancia de la gestión de fallas. Ejemplos de fallas. Costo de las fallas. Causas de fallas. Ley de Murphy y sus corolarios. Gestión de fallas en el modelo FCAPS. Diferencia entre fallas, eventos, errores, problemas. Notificación de eventos. Detección y resolución de problemas. Sistema de boletín de avería (*trouble ticket*). Soporte al usuario y *help desk*. Herramientas para detectar y resolver problemas (*troubleshooting*). Herramientas de diagnóstico para computadores. Causas de fallas en discos duros. Predicción de fallas y SMART (*Self-Monitoring, Analysis and Reporting Technology*). Sistemas tolerantes a fallas. Tecnología RAID (*Redundant Array of Independent Disks*). Failover, clustering y SAN. Prevención de pérdida de datos (DLP). Respaldo y restauración de datos. Recuperación de archivos borrados. Recuperación de datos en discos dañados. Accidentes y desastres (inundación, terremoto, incendio, calor, falla de energía eléctrica, apagón). Plan de contingencia y recuperación ante desastres. Plan de continuidad de negocio (BCP) y análisis de impacto en el negocio (BIA). Alerta temprana y telecomunicaciones de emergencia. Protección de infraestructuras críticas para la seguridad nacional. Fundamentos de confiabilidad y mantenimiento. Tasa de fallas y curva de la bañera. Mantenibilidad y disponibilidad. MTTF, MTBF y MTTR. Confiabilidad de sistemas (serie, paralelo, stand-by, failover). Redundancia 1:1 y 1:N. Confiabilidad de sistemas electrónicos.

6. GESTIÓN DE DESEMPEÑO

Funciones de la gestión de desempeño. Indicadores claves de desempeño (KPI). Calidad de servicio (QoS) y su medición (ancho de banda, caudal, retardo, jitter, tiempo de respuesta, disponibilidad, tasa de errores). Tiempo de respuesta de las aplicaciones. Acuerdo de nivel de servicio (SLA). Calidad de servicio en redes ATM y redes IP. Administración del ancho de banda. Reserva de recursos y RSVP. Ingeniería de tráfico y MPLS (*Multi Protocol Label Switching*). Servicios integrados (*IntServ*). Servicios diferenciados (*DiffServ*). Admisión, clasificación y priorización del tráfico. Mecanismos de calidad de servicio en capa 2 (802.1p/802.1Q). Manejo de colas. Cola lineal (FIFO). Cola justa sopesada (WFQ). Control de congestión. Algoritmos RED y WRED. Conformación del tráfico. Técnica de balde con fuga (*leaky bucket*) y de balde con fichas (*token bucket*).

7. GESTIÓN DE SEGURIDAD

¿Por qué es importante la seguridad? Requisitos básicos para la seguridad de la información: Confidencialidad, integridad, disponibilidad. Otros requisitos: privacidad, secrecía, anonimato, autenticidad, autorización, trazabilidad, no repudiación. Conceptos básicos en seguridad (activo, amenaza, vulnerabilidad, incidente, ataque, exploit, impacto, riesgo, control). Gestión de riesgos. Clasificación de las amenazas y vulnerabilidades. Vulnerabilidades en el software. Bases de datos de vulnerabilidades (CVE, OSVDB, CERIAS, Bugtraq, etc.). Tres principios de la seguridad de la información. Introducción a las medidas de protección. Tipos de controles (disuasivo, preventivo, correctivo, investigativo). Ejemplo de controles. Seguridad física, técnica y administrativa. Seguridad en profundidad. Estrategia de defensa estratificada. Criptografía. Los sistemas de cifrado DES, TripleDES y AES. Integridad y autenticidad de datos. Función hash (MD5, SHA). MAC (*Message Authentication Code*) y HMAC. Firma digital.

8. SEGURIDAD FÍSICA Y AMBIENTAL

Las 3 categorías de la seguridad: administrativa, técnica (lógica) y física. Niveles y anillos de seguridad. Protección física de los equipos. Protección perimetral de un sitio (guardias, casetas, barreras, cercas, iluminación, vigilancia electrónica y CCTV, detección de intrusos). Acceso vehicular y peatonal. Controles de entrada para empleados y visitantes. Acceso a locales y oficinas (llaves y cerraduras, tarjetas de identificación, RFID, NFC, biometría). Selección de un sitio seguro. Ejemplos de Data Center. Sala “cofre”. Seguridad ambiental y protección contra desastres naturales. Protección contra transitorios eléctricos y apagones. Utilización de filtros, UPS y plantas de emergencia. Protección contra incendio. Detección y extinción de incendios. Clases de incendios y agentes extintores. Rociadores. Normas NFPA y COVENIN. Sistemas de ventilación y aire acondicionado (HVAC). Requerimientos para centros de datos. Normas y estándares (NFPA, COVENIN, ANSI/TIA-942, ANSI/NECA/BICSI-002). Seguridad industrial y salud ocupacional. Radiación electromagnética y salud. El ambiente de trabajo (físico, psicológico y social). Estrés laboral. Ergonomía. Ley Orgánica de Prevención, Condiciones y Medio Ambiente de Trabajo (LOPCYMAT). Organización Internacional del Trabajo (OIT).

9. VOZ SOBRE IP Y TELEFONÍA POR INTERNET

Redes telefónicas y redes de datos. Redes de circuitos y redes de paquetes. Congestión y retardo en redes de paquetes. Compresión de la voz y códecs de audio. Introducción a la voz sobre IP (VoIP) y sus características. Integración de voz y datos. Telefonía por Internet. Proveedores de telefonía IP. Número telefónico virtual y DID. Comunicaciones Unificadas (UC). Mensajería Instantánea (IM). Teletrabajo. Central telefónica privada (PBX) e IP-PBX. PBX virtual en la nube (*hosted*). Equipamiento para telefonía IP: PBX, Asterisk y sus derivados, teléfonos IP, softphones. Calidad de servicio (*QoS*) en VoIP. Parámetros de QoS: Retardo (latencia), fluctuación del retardo (jitter), tiempo de respuesta, pérdida de paquetes, disponibilidad, tasa de errores, eco. Algunas opciones para suministrar calidad de servicio (QoS): Differentiated Services (*DiffServ*), IEEE_802.1p/Q y VLAN. Estándares y protocolos para VoIP y aplicaciones multimedia (RTP, RTCP, H.323, SIP, etc.). Dimensionamiento de sistemas de telefonía IP. La inseguridad en VoIP. Ejemplos de amenazas, vulnerabilidades y riesgos en la telefonía IP. Escucha y grabación legal/ilegal de conversaciones.

Interceptación de llamadas telefónicas en telefonía fija y móvil. Captura de tráfico de VoIP mediante sniffers. Interceptación y decodificación de tonos de discado DTMF. Otros tipos de ataques: Enumeración, inundación, negación de servicio, desconexión forzada, spam sobre telefonía IP (SPIT), phishing, fuzzing, etc. Medidas de protección: Segmentación VLAN, autenticación por digest MD5, Secure SIP (SIP over TLS). Encriptación con SRTP y ZRTP. Túneles VPN (*Virtual Private Network*). Sistemas de detección de intrusos (IDS).

10. MODELADO Y SIMULACIÓN DE REDES

Metodología para el modelado y simulación. Aplicaciones (estudio de tráfico, dimensionamiento en fase de diseño, planificación de capacidad, planes de contingencia, incorporación de nuevos usuarios y de nuevas aplicaciones evaluación de alternativas para mejorar el desempeño, gestión de cambios, verificación de acuerdos de niveles de servicio). Software para simulación de redes y sistemas (Arena, Simulink, Packet Tracer, GNS3, NS-2, SimMPLS, NetSim, AdventNet, MIMIC, OPNET, ITGuru). Bases teóricas para la simulación. Fundamentos de probabilidades y estadística. Nociones de teoría de colas. Modelo de cola simple. Factor de utilización. La cola M/M/1. Fórmula de Little. Colas con servidores múltiples.

PRÁCTICAS DE ADIESTRAMIENTO

Las prácticas pueden seleccionarse según los tópicos que más interesan.

1. Configuración y operación de Windows
2. Configuración y operación de Linux
3. Máquinas y redes virtuales
4. Captura y análisis de tráfico en redes
5. Servicios básicos de Internet con Telnet, SSH, SCP, FTP, TFTP
6. Redes inalámbricas de área local (WLAN)
7. Captura y análisis de tráfico en WLAN
8. Configuración de puntos de acceso inalámbricos
9. Redes inalámbricas ad-hoc y AP virtual
10. Control de acceso en WLAN mediante filtros MAC
11. Supervisión de redes y servicios
12. Navegación en Internet con HTTP y autenticación de usuarios
13. Servidores proxy y navegación anónima
14. Gestión de redes con SNMP
15. Gestión de redes con SNMP en Linux
16. Gestión avanzada de redes con Net-SNMP
17. Monitoreo de infraestructuras TI con Nagios
18. Monitoreo de infraestructuras TI con Zenoss
19. Notificación y registro de eventos mediante Syslog
20. Gestión de fallas en redes y sistemas informáticos
21. Documentación y diagramación de redes y sistemas
22. Control de inventario de activos informáticos
23. Acceso remoto a equipos y sistemas
24. Comunicaciones seguras con Red Privada Virtual (VPN)
25. Correo electrónico mediante SMTP, POP3 y MIME
26. Gestión de contraseñas
27. Ataques a las contraseñas de Windows
28. Ataques a las de contraseñas de servicios en línea
29. Respaldo y restauración de datos
30. Recuperación de datos borrados o dañados
31. Protección contra intrusos y software malintencionado
32. Barreras de protección y firewalls
33. Control de acceso mediante RADIUS
34. Control de acceso a WLAN mediante RADIUS
35. Redes P2P y entornos NAT
36. Comunicación en línea, compresión del habla y VoIP
37. Telefonía IP mediante SIP (*Session Initiation Protocol*)
38. Comunicaciones Unificadas y PBX virtual
39. Configuración y operación de una PBX básica (Axon)
40. Configuración y operación de una PBX avanzada (Asterisk)

41. Interceptación de llamadas en telefonía y voz sobre IP
42. Interceptación avanzada de llamadas en voz sobre IP
43. Ataque a la autenticación en telefonía IP
44. Protección de la confidencialidad en voz sobre IP
45. Identificación de hablantes y tonos de marcación en telefonía
46. Bluetooth y redes de área personal (PAN)
47. Comunicaciones avanzadas con Bluetooth
48. Modelado y simulación de redes