Universidad Nacional Autónoma de Nicaragua – León.
Facultad de Ciencias y Tecnología.
Departamento de Computación.
Ingeniería en Telemática. IV Curso. 2021

Proyecto de laboratorio para el II Parcial de la asignatura Redes de Computadoras

Para este segundo parcial, se deberá entregar este proyecto (la miscelánea), el cual está valorado en un 30% de la nota final correspondiente al segundo parcial de la asignatura. El puntaje total para este III Parcial será de **120 puntos**, los cuales se desglosan así:

- **Miscelánea**: **30-40 puntos**. (Miscelánea básica: 30 pts. Miscelánea con cuestiones extras: 40 pts).
- Entrega y defensa de prácticas en NetGUI o en GNS3 + Docker, que incluyen TCP, UDP, Congestión en TCP, Análisis de los protocolos OSPF y BGP, **valoradas en 40 pts (10 pts c/u)**.
- **Quizzes o tests teóricos online** (deberán ser realizados durante la sesión presencial), de los temas UDP, TCP, OSPF y BGP, con un valor de 10 puntos cada uno, para un total de **40 pts**.
- **Opcionales**: **Prácticas de programación de servidores y herramientas de red**, valoradas en 10 puntos cada una. Se propondrán una serie de prácticas y el estudiante deberá escoger como mucho, un máximo de 4 prácticas, para totalizar un total de **40 pts**.
- **Aclaración**: El estudiante deberá elegir o bien, el desarrollo de la miscelánea, o el desarrollo de las prácticas de laboratorio de programación de aplicaciones de red. No se podrán elegir ambas evaluaciones a la vez.

A continuación, se describe el proyecto:

Proyecto: Miscelánea con Packet Tracer

Consiste en realizar una miscelánea completa con Packet Tracer. Se deberá usar la versión más reciente de este simulador, es decir, la versión 7.3, en ambiente Windows o Linux.

Los **aspectos básicos** (entre protocolos, tecnologías y herramientas) que debe llevar la miscelánea en su versión básica, son:

VLAN, VTP, VPN, DHCP, RIP, OSPF, BGP, EIGRP, STP, EtherChannel, VoIP, NAT, VRR o HSRP, Frame Relay, PPP, CHAP, ACLs, Routers Inalámbricos, Access Points Inalámbricos, Autenticación WEP y WPA, RADIUS, ADSL, TV, DNS, HTTP, FTP, TFTP, NTP, SSH, TELNET; NTP, SMTP (email), Syslog, AAA, SNMP, ASA 505, Sniffer, Netflow Collector, IPSEC, telefonía 3G/4G (mirar los elementos Cell Tower y Central Office Server).

Recomendaciones generales:

1. La topología será libre, pero al menos debería incluir 3 o más Empresas (Universidades, Bancos, Instituciones del Gobierno, etc), interconectadas por al menos tres ISPs (simulando con esto un CORE de Internet). En la plataforma les he dejado algunos ejemplos de las topologías más completas, realizadas por estudiantes en años anteriores.
2. Dentro de cada Empresa, podrá haber conexiones de larga distancia, por ejemplo, conexiones entre dos campus universitarios en una ciudad, que pertenecen a la misma Universidad; conexiones de dos sucursales bancarias en una ciudad que pertenecen a un banco, etc. En cada Empresa se deberá desplegar todas las tecnologías posibles de Redes de Area Local así como los protocolos de routing interno, y en el CORE de Internet podrá desplegarse un protocolo de Enrutamiento Externo, como BGP.
3. Hay que prestar una importante atención a la redistribución de rutas entre diferentes protocolos, bien desplegados dentro de las redes de área local, como entre una red de área local y la WAN.
4. En esta versión del simulador Packet Tracer, se encuentra un **ASA 5505** y un **ASA 5506**, ambos con algunas limitaciones en relación con los reales firewalls físicos. Aun así, se valorará el uso de estos dispositivos con las funcionalidades básicas, desplegados en el perímetro de las empresas o de los ISPs.

5. Se valorará también, el despliegue del protocolo IPv6 en las redes de área local y en la red WAN. Por ejemplo, podríamos tener en una de las Empresas, los dos protocolos (IPv4 e IPv6), corriendo simultáneamente, y protocolos de enrutamiento que corran IPv4 e IPv6. Es recomendable que la asignación de direcciones para los hosts finales, tanto en IPv4 como en IPv6, se realice de forma dinámica, ya sea por DHCP o por autoconfiguración.
6. En las listas de acceso y firewall, incluir reglas que hagan uso de las restricciones más comunes: por ejemplo, filtrados de icmp, de dns, de sitios web, de ftp, etc.
7. Las VLANs deberían propagarse dinámicamente mediante VTP.
8. Es recomendable configurar una VPN de acceso remoto entre diferentes sucursales y probar su funcionamiento.
9. Se simulará que cada Institución tiene un dominio y un servidor DNS que administre dicho dominio. Se deberán configurar DNS raíz para ayudar a los servidores DNS locales a resolver direcciones desconocidas. Una vez que cada servidor DNS local aprenda direcciones de los demás dominios, cada servidor DNS de cada empresa, conocerá los nombres de dominio de los servidores de las otras instituciones. Por ejemplo, si hay 3 Universidades cuyos dominios son **unanleon.edu.ni**, **uca.edu.ni**, **unan.edu.ni**, entonces los servidores DNS que administran cada uno de esos dominios de cada una de esas Universidades, deberán conocer todo acerca de las otras Universidades. Así, el servidor DNS de la UCA, (llamado, ns.uca.edu.ni), deberá tener entradas que ha aprendido, para, además de sus propios servidores (www.uca.edu.ni, ftp.uca.edu.ni, mail.uca.edu.ni, ftp.uca.edu.ni,etc), para los otros servidores de las otras Universidades (www.unanleon.edu.ni, ftp.unanleon.edu.ni, mail.unanleon.edu.ni, etc).
10. Un usuario de un servidor de correo de una institución, deberá poder enviarle correo a otro, desde cualquier lugar. Y un usuario, deberá poder descargar su correo desde cualquier sitio en la topología.
11. Las máquinas con acceso Wifi, siempre deberán autenticarse hacia un AP, con WEP o WPA, y este a su vez, deberá autenticarlo hacia un servidor RADIUS.
12. Se valorará la funcionalidad de llamadas VoIP entre teléfonos de la misma sucursal.
13. En el CORE de Internet habrá, como es de esperarse, direccionamiento público de IPv4.
14. Dentro de cada Institución, es recomendable hacer uso de un direccionamiento privado (por ejemplo, partir de la red 10.0.0.0 / 8, y luego hacer subredes para las distintas VLANs) y configurar un NAT sobrecargado. Los servidores podrían tener direcciones privadas (por lo cual, se deberá configurar un NAT apropiado para esto) o tener direcciones públicas del rango asignado por el ISP.
15. Los servidores de la Empresa deberán estar ubicados dentro de la DMZ, y podrán tener, tanto direccionamiento público como direccionamiento privado.

Cuestiones extras que puede llevar la topología:

- Ipv6 totalmente desplegado: Una sucursal de algún banco, una Facultad de alguna Universidad, etc, totalmente implementada con IPv6: deberá incluir OSPFv3, EIGRPv6, RIPNg, IPV6 CEF, Servicios de Red en IPv6, túneles ipv6-ipv4, NAT64, o algún otro mecanismo de transición.

- Uso de: Enrutador 819HGW, Cell Tower, Central Office Server, SmartPhone, Bluetooth, 802.1x, Home Gateway

- Meraki – MX65W Security Appliance.

- Usar los sensores y demás elementos para el Internet de las Cosas (IoT: Internet of Thing). Se valorará la programación que se haga para el correcto funcionamiento de estos dispositivos.

- Llamadas VoIP entre diferentes sucursales.

- Túneles GRE sobre IPSec.

- Uso de la controladora inalámbrica WLC.

- Configuración del protocolo SNMP y uso de MIB Browser.

- Cisco Application Management con Virtual Machines.

Acerca de la entrega:

- La topología deberá rotularse adecuadamente: nombre de interfaces, direcciones, nombres de VLANs, etc.
- El uso de colores para definir áreas está permitido y le dará más realce al proyecto.
- Se deberá crear un enunciado de la topología en un documento aparte y comentar profusamente en la misma topología.
- La topología se deberá entregar y defender ante el profesor durante la clase presencial.
- Es recomendable tener dos topologías a mano: una donde todo esté permitido para comprobar la correcta conectividad a nivel IP, y otra topología igual que la anterior, pero con las restricciones configuradas.
- Se deberán subir y enviar las dos topologías a la plataforma de la asignatura, y como respaldo, también enviarlas al Microsoft Teams.
- El envío se hará al finalizar la defensa de la práctica.

Fecha de defensa de los dos proyectos: El día del examen del segundo parcial de Redes de Computadoras, según el horario que publique el Departamento de Computación.