



2023

**GUÍA DE EJERCICIOS DE ESCRITORIO N°2****Unidades Didácticas 6 a 9****6. UNIDAD N° 6: Arquitectura de las redes WAN y protocolos de la subred de acceso****EJERCICIOS RECOMENDADOS PARA TRABAJOS DE LABORATORIOS**

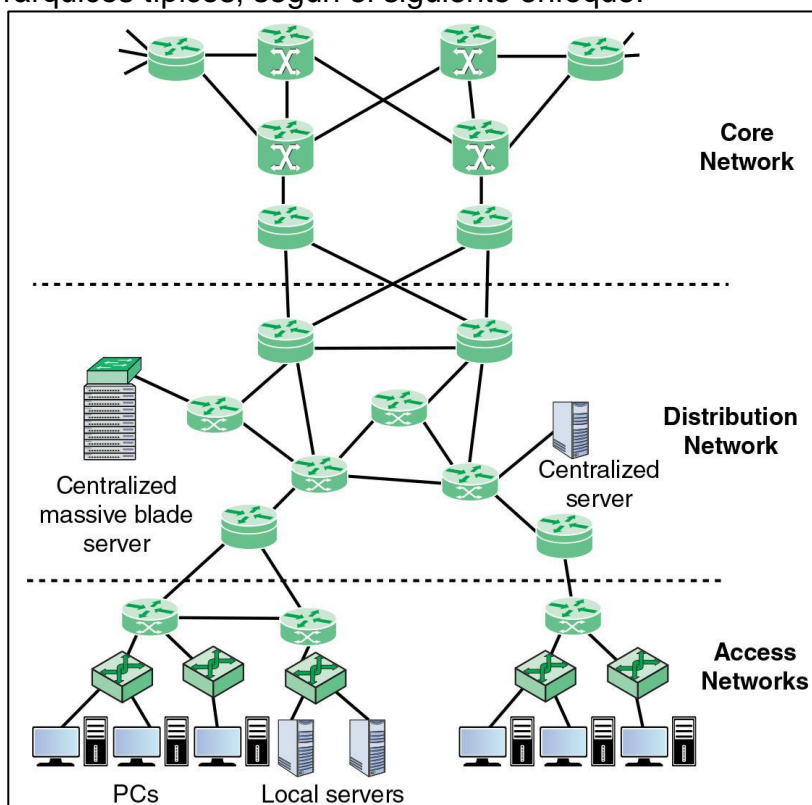
6.1.4.	Análisis
6.2.2. – 6.2.3.	Configuración
6.3.2. a 6.3.4.	Configuración

**6.1. Arquitectura de las redes WAN. La red de transporte, subredes de acceso y backbone. Componentes de una red WAN. Modelo de red empresarial.**

6.1.1. Grafique un esquema de WAN, identificando las redes y subredes.

6.1.2. Realice un cuadro sinóptico de las diferentes arquitecturas de las principales redes WAN, los protocolos de cada capa en las subredes de acceso y backbone. Identifique familias de protocolos y referéncielos con respecto al modelo OSI.

6.1.3. Grafique la estructura de una red empresarial WAN para enlazar la LAN de la casa matriz con las de 5 sucursales, señalando las capas del modelo OSI intervinientes en cada ámbito (LAN o WAN). En cada sucursal, considere los niveles jerárquicos típicos, según el siguiente enfoque:



Fuente: Stallings, William. Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud. Pearson Education. 2016



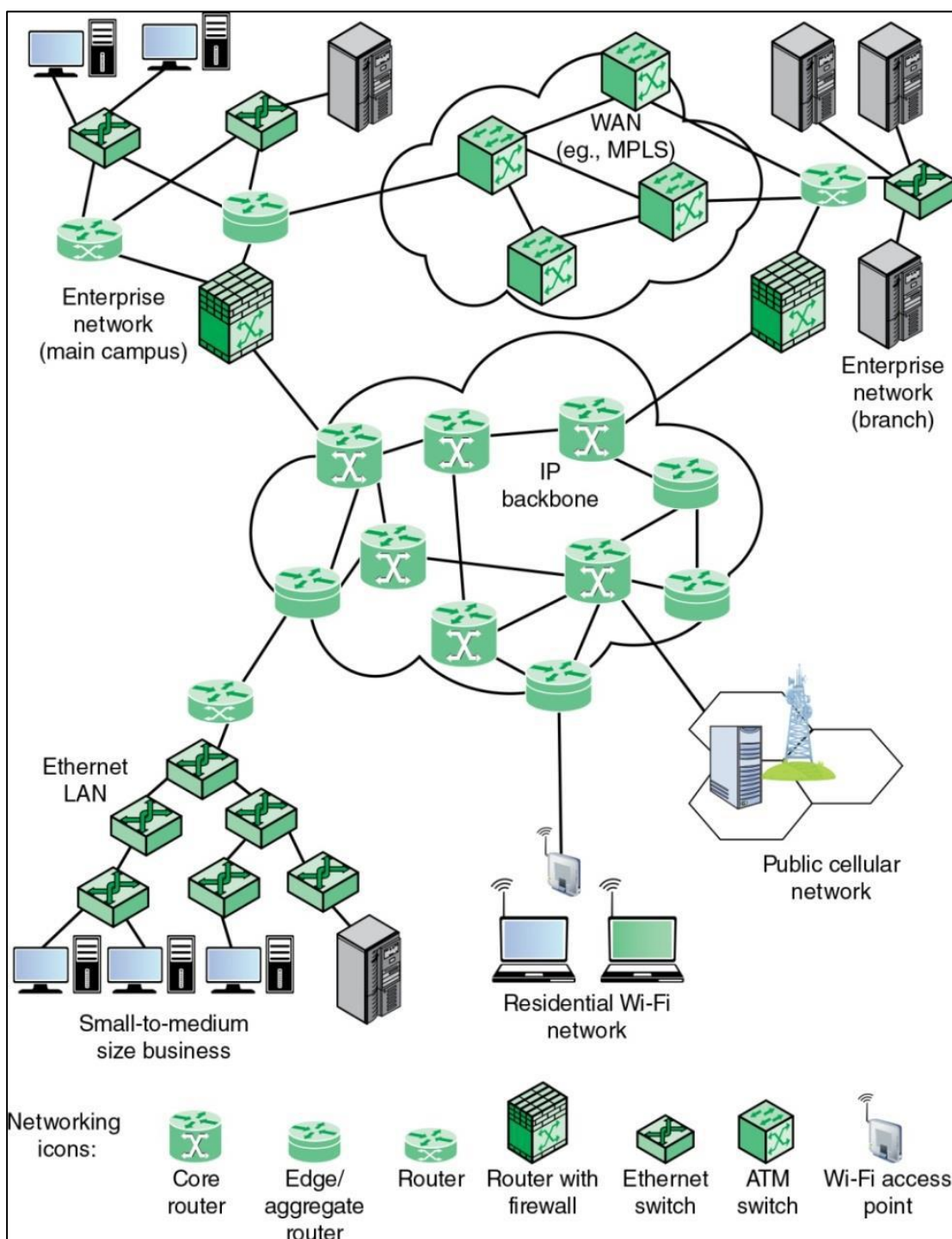
UTN - FRBA

Departamento de Sistemas

**MATERIA:** Redes de Información

**NIVEL:** Cuarto

6.1.4. En base a la topología dada en el Ejercicio Integrador de Autoevaluación u otro TL similar, realice en cada tipo de dispositivo (PC, switch, router, etc.) el desglose de las capas del Modelo OSI y protocolos que funcionarían en cada uno de ellos, para las siguientes redes WAN:



Fuente: Stallings, William. *Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud*. Pearson Education. 2016



## **6.2. Arquitectura de la red Internet. Las redes INTRANET y EXTRANET, características principales. Evolución futura de las redes.**

- 6.2.1. Realice un cuadro comparativo de las características comunes y diferentes entre redes intranet y extranet.
- 6.2.2. ¿Cuáles son las amenazas más comunes a la seguridad y vulnerabilidades en las redes Internet, intranet y extranet? Considerar el proyecto OWASP, <https://www.owasp.org/index.php/Category:Vulnerability>, entre otros.
- 6.2.3. En base a la arquitectura TCP / IP señale los protocolos más seguros que seleccionaría en cada capa, para disminuir los riesgos de las vulnerabilidades señaladas en el apartado anterior.

## **6.3. Protocolos básicos de conectividad punto a punto: PPP, principio de funcionamiento, comparación con el SLIP. Utilización del protocolo PPP, limitaciones.**

- 6.3.1. Señale similitudes y diferencias entre PPP y SLIP.
- 6.3.2. Compare PPP con HDLC.
- 6.3.3. Identifique versiones propietarias de PPP y señale sus particularidades.
- 6.3.4. Compare las opciones de autenticación de enlace PPP con los protocolos PAP y CHAP.

## **7. UNIDAD N° 7: Redes X: 25 y Frame Relay.**

### **EJERCICIOS RECOMENDADOS PARA TRABAJOS DE LABORATORIOS**

**7.2.6. – 7.2.8.**

**Análisis**

## **7.1. Evolución histórica del protocolo X.25. Arquitectura X.25.**

- 7.1.1. Realice un análisis comparativo entre los enlaces punto a punto (dedicados) y los conmutados.
- 7.1.2. Estudie las PDUs de las tramas PPP, HDLC, LAP-F (Frame Relay) y LAP-B (X.25), señalando similitudes y diferencias.
- 7.1.3. Analice los servicios que el protocolo LAP-B proporciona a la capa superior. Para cada servicio, señale el modelo aplicado.

## **7.2. El nivel de enlace, protocolo HDLC. Análisis de la trama HDLC.**

**Funcionamiento e intercambio de tramas del HDLC. Servicios brindados por el HDLC a la capa de red. Comparación del HDLC con el BSC y el SDLC. Subconjuntos del HDLC.**

- 7.2.1. ¿Cuáles son los motivos por los cuales existen tramas HDLC no numeradas?
- 7.2.2. En el protocolo HDLC las tramas llevan paquetes X.25:
  - Provenientes de diferentes Circuitos virtuales.
  - Provenientes del mismo circuito virtual.
  - De datos exclusivamente.
  - ninguna de las anteriores.
- 7.2.3. El protocolo HDLC realiza control de flujo:
  - mediante el mecanismo de la ventana.
  - mediante una línea física de start/stop.
  - mediante tramas específicas para control de flujo.



- operando sobre el nivel 1.
  - no realiza control de flujo.
- 7.2.4. El campo DIRECCION (8 bits) de las tramas de HDLC puede asumir sólo dos valores: "00000001" ó "00000011". ¿Por qué no fue implementado con un solo bit para acortar la longitud de las tramas?
- 7.2.5. Confeccionar un ejemplo de intercambio de tramas de datos entre dos ETD con ventana igual a 4, semiduplex.
- 7.2.6. Detallar los campos de la tramas HDLC y explicar el significado de cada subcampo.
- 7.2.7. Suponiendo que se aplica el protocolo HDLC, distinguir entre los modos de funcionamiento NRM y ABM. Detallar la secuencia de tramas correspondientes a la inicialización del enlace y posterior desconexión del mismo.
- 7.2.8. Realice una comparación de los formatos de tramas correspondientes a los protocolos PPP y HDLC.

### **7.3. Definición de canales lógicos y circuitos virtuales. Establecimiento de los circuitos virtuales en X.25. Facilidades del X.25. Limitaciones y evolución futura del X.25.**

- 7.3.1. Detallar la estructura de los diferentes paquetes utilizados en X.25, indicando las funciones asociadas a cada campo. Detallar la finalidad de cada tipo de paquete.
- 7.3.2. La confirmación de recepción de paquetes X.25 se puede realizar terminal a terminal o local. Indicar los campos del paquete relacionados con este proceso y detallar el mismo cuando se efectúa entre un ETD local, un ECD y un ETD remoto.
- 7.3.3. Detallar el procedimiento de control de flujo a nivel del X.25. Que funciones cumplen los paquetes RR y RNR.
- 7.3.4. Detallar mediante un ejemplo el establecimiento de una llamada virtual, suponiendo que se comunican dos ETD con la red X.25 que dispone de dos nodos ECD. El ETD A se comunica con el ECD 1 y el ETD B con el ECD 2 y los dos ECD entre sí.
- 7.3.5. Indicar por lo menos cinco facilidades X.25. ¿Como se solicitan las mismas en una llamada virtual?
- 7.3.6. Definir canal lógico y circuito virtual e indicar los diferentes tipos existentes. ¿Cuántos canales lógicos pueden existir por acceso físico? ¿Cuál es la velocidad máxima de una conexión X.25 y por qué?
- 7.3.7. Definir las interfaces que se emplean en el nivel físico del X.25 y sus principales características.
- 7.3.8. Confeccionar un diagrama en el cual se detalle la ubicación de un PAD conectado a un terminal que opera en el modo carácter, dos nodos X.25 y un terminal que opera en el modo paquete. Indicar el equipamiento que comprende cada uno de los siguientes protocolos: X.29, X.28, X3 y X.25. Describir las características principales de dichos protocolos.
- 7.3.9. Indicar las diferencias entre el procedimiento "restart" y "reset" en el protocolo X.25, entre un ETD y un ECD. ¿Que cantidad de canales quedan afectados en cada caso?



**7.4. Los canales lógicos en Frame Relay: DLCI. Mapeo de una red Frame Relay. Relación entre las direcciones IP y las DLCI. Detección de la congestión mediante los bits FECN y BECN. Configuración de las placas Frame Relay, parámetros: Access Rate, CIR, TC, Bc y Be. Transmisión de voz en redes Frame Relay. Evolución futura del Frame Relay.**

- 7.4.1. Detallar la estructura de la trama Frame Relay y las funciones de cada campo.
- 7.4.2. Realice un análisis comparativo entre los protocolos LAP-B y LAP-F.
- 7.4.3. Indicar los principales mecanismos utilizados para el control de la congestión en las redes Frame Relay, una vez detectada la misma.
- 7.4.4. Detallar la topología de una red WAN con cuatro routers conectados a una red Frame Relay, cada router tiene una red LAN. Dada la dirección IP 140.10.0.0 asignar las direcciones de subred a las interfaces que corresponda y confeccionar la tabla de enrutamiento (DLCI y Dir IP) de cada router, suponiendo que se requiere vincular al router A con los routers B, C y D. Además, se solicita que D se comunique directamente con B.
- 7.4.5. Supongamos que se contrata con una TELCO un acceso Frame Relay con una línea física E1, es decir 2.048 Kbps. Además se define un PVC con un CIR de 1.024 Kbps. La TELCO configura el enlace con un EIR de 384 Kbps y establece el valor de Tc en 1 segundo (fijando de esta forma los valores de Bc y Be).

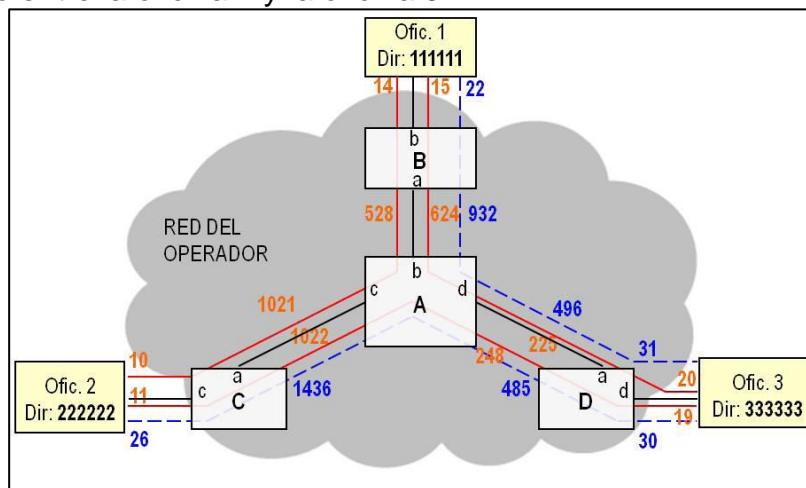
En esta situación se desea enviar un flujo de vídeo en tiempo real a un destino remoto, sin ningún tipo de control de flujo por parte del receptor y sin atender a ninguna notificación de congestión que pueda venir de la red. Supongamos que se dispone de un parámetro en el terminal mediante el cual puede fijar el caudal de tráfico que inyecta en la red. Supongamos también que el envío se hace utilizando siempre tramas de 6.250 bytes (50.000 bits). Se desea saber, si se fija el flujo de datos a transmitir en 2.000 Kbps:

- ¿Cuántas tramas se inyectaran en el conmutador Frame Relay?
  - ¿Cuántas de ellas serán aceptadas sin marcar?
  - ¿Cuántas serán marcadas y cuántas descartadas?
  - ¿Cuál debería ser el caudal inyectado para garantizar el transporte de la TOTALIDAD de las tramas?
- 7.4.6. Diagrame y dimensione los vínculos de una red WAN conectando la casa central de una empresa con 4 sucursales. A través de los vínculos se distribuirá a toda la red el servicio de Internet provisto por un enlace en casa central de 256 Kbps. Deberá considerarse la utilización de 2 canales de voz con cada sucursal. Los canales de voz deben transportarse por un PVC independiente con full-CIR (EIR = 0). Los PVC de datos, deben garantizar un CIR del 25%.
    - ¿Qué access-rate propone para cada acceso?
    - ¿Cuántos circuitos virtuales debe contratar?
    - ¿Con qué CIR cada uno?
  - 7.4.7. Dados los primeros bytes de una trama de Frame Relay, TRAMA: 7E 08 45 3A ..., identifique los siguientes parámetros: DLCI utilizado. ¿Existe





- congestión en la red? ¿En caso de responder afirmativamente, cual es la causa?, ¿Qué garantías brinda la red de que esta trama llegue a destino?
- 7.4.8. Dado un archivo de 1Mbyte, indique cuántas tramas Ethernet DIX v2 serían necesarias para transferir el archivo desde un host a otro dentro del mismo segmento de red. Si la transferencia debiera atravesar un enlace Frame Relay con MTU = 1000 bytes, cuántas tramas serían necesarias?
- 7.4.9. Dado un enlace FR que emplea el 50 % del Access Rate (128 kbps ), y teniendo en cuenta que se transmiten en el tiempo  $T_c = 6.400$  bits, calcular: Bc, Be, EIR y CIR. ¿Habrá tramas rechazadas?
- 7.4.10. Detallar los métodos que se podrían implementar para disminuir la congestión en una red FR.
- 7.4.11. Detallar los principales parámetros que se deben configurar en la interface FR de un router.
- 7.4.12. Un operador de telecomunicaciones dispone de una red de conmutación de paquetes orientada a conexión que consta de 4 conmutadores, siendo uno de ellos (A) el centro de una estrella cuyos extremos son los otros 3 conmutadores (B, C y D). Una empresa que dispone de 3 oficinas en diferentes ciudades. Solicita al operador el servicio de conexión entre sus oficinas mediante circuitos virtuales bidireccionales tanto permanentes (1 entre cada par de oficinas) como conmutados (3 canales lógicos en las oficinas 1 y 3, y 2 en la oficina 2). El operador le ofrece este servicio conectando cada una de las oficinas (1, 2 y 3) de la empresa cliente a los conmutadores (B, C y D) del operador, respectivamente.
- En la figura siguiente se muestra la arquitectura de la red del operador y los equipos del cliente que están conectados a la misma, así como las direcciones de red asignadas por el operador a cada uno de los equipos del cliente (en negrita). En la figura también se muestran gráficamente los circuitos virtuales que están establecidos en un momento determinado, indicándose los LCIs asignados a los mismos en cada enlace:
- En línea **roja continua**, los 3 circuitos virtuales permanentes (CVP).
  - En línea **azul discontinua**, los 2 circuitos virtuales conmutados (CVC) que están establecidos en ese momento, uno entre la oficina 1 y la oficina 3 y el otro entre la oficina 2 y la oficina 3.



Fuente: Redes y Servicios de Telecomunicación. Ejercicios Resueltos, ISBN: 978-84-9860-459-7



Preguntas:

- 7.4.12.1. Indicar cuál es el contenido de las tablas de conexiones de los 4 conmutadores de la red en el momento al que se refiere el enunciado y que se encuentra reflejado en la figura. Identificar cuáles de las entradas de dichas tablas de conexiones se refieren a CVP y cuáles a CVC.
- 7.4.12.2. Teniendo en cuenta que para poder establecer CVCs los conmutadores tienen que decidir hacia dónde encaminar los paquetes de solicitud de establecimiento de CV, y que para ello necesitan tener una tabla de encaminamiento, indicar cuál es el contenido de las tablas de encaminamiento de los 4 conmutadores.
- 7.4.12.3. Suponiendo que la solicitud de establecimiento del CVC existente entre la oficina 1 y la oficina 3 fue iniciada por la oficina 1:
- Indicar cuáles de las entradas de las tablas de encaminamiento de cada conmutador han sido tenidas en cuenta en el establecimiento de dicho CVC.
  - Indicar cuáles de las entradas de las tablas de conexiones de cada conmutador han sido creadas durante el establecimiento de dicho CVC.
- 7.4.12.4. A continuación la oficina 3 solicita el establecimiento de un nuevo CVC hacia la oficina 1:
- Indicar cuáles de las entradas de las tablas de encaminamiento de cada conmutador son utilizadas para establecer dicho CVC.
  - Dibujar el camino que van a seguir los paquetes pertenecientes a ese nuevo CVC, asignando LCIs en cada uno de los tramos del mismo.
  - Indicar el contenido de las tablas de conexiones de los 4 conmutadores después de que dicho CVC haya sido correctamente establecido.
- 7.4.13. Un operador de telecomunicaciones dispone de una red de conmutación de paquetes NO orientada a conexión que consta de 4 equipos, siendo uno de ellos (A) el centro de una estrella cuyas puntas son los otros 3 (B, C y D). Una empresa que dispone de 3 oficinas en diferentes ciudades solicita al operador el servicio de conexión entre sus 3 oficinas. El operador le ofrece este servicio conectando cada una de las oficinas 1, 2 y 3 de la empresa cliente a los equipos B, C y D del operador respectivamente. En la figura adjunta en el ejercicio 1.2.1 se muestra la arquitectura de la red del operador y los equipos del cliente que están conectados a la misma, así como las direcciones de red asignadas por el operador a cada uno de los equipos del cliente (en negrita). La diferencia en este caso, es que se trata de un sistema no orientado a la conexión.

Preguntas:

- 7.4.13.1. Indicar cuál es el contenido de las tablas de conexiones de A, B, C y D.
- 7.4.13.2. Indicar cuál es el contenido de las tablas de encaminamiento de A, B, C y D.
- 7.4.13.3. Suponiendo que la oficina 1 y la oficina 3 mantienen entre sí una comunicación:
- Indicar cuáles de las entradas de las tablas de encaminamiento son utilizadas para hacer posible dicha comunicación.



- Indicar cuáles de las entradas de las tablas de conexiones son utilizadas para conmutar los paquetes de dicha comunicación.

## **8. UNIDAD N° 8: Calidad de servicio, redes IP/MPLS.**

### **8.1. Arquitectura del modelo ATM. El nivel físico ATM. El nivel ATM.**

8.1.1. En una red WAN es necesario colocar varias tramas simultáneamente para aprovechar el canal y maximizar su utilización.

Comparar la utilización en una red ATM, con celdas de 53 bytes, 155 Mbps y 50Km de longitud, para los siguientes casos:

8.1.1.1. Un SOLO paquete simultáneamente en la red.

8.1.1.2. TODOS los paquetes posibles simultáneamente en la red.

8.1.2. Un host utiliza ATM AAL5 para transmitir datos que recibe de una aplicación en forma de mensajes discretos, cada uno de 40 bytes de longitud. El tráfico medio medido en la línea es de 600 Mb/s. Debido a errores de transmisión un 1% de las celdas llega con su contenido totalmente alterado (excepto los 5 bytes de la cabecera ATM).

Calcule el número de celdas erróneas por semana que serán aceptadas como válidas en el host de destino.

### **8.2. El nivel de adaptación al ATM.**

8.2.1. Dos conmutadores Ethernet-ATM están conectados a un conmutador ATM mediante sendos enlaces OC-3c y se interconectan entre sí empleando LAN Emulation. LANE utiliza AAL5 como protocolo de transporte, es decir las tramas Ethernet viajan 'encapsuladas' en celdas ATM de acuerdo con la estructura propia de AAL5.

Calcule el caudal de información que podrá transmitirse a nivel LLC (cabeceras incluidas) cuando las tramas Ethernet tengan 46 bytes de datos y cuando tengan 1500 bytes de datos (longitudes mínima y máxima respectivamente de una trama Ethernet). Suponga que el medio de transmisión está libre de errores y que la eficiencia de los conmutadores es tal que estos nunca representan un factor limitante en la red.

### **8.3. Calidad de servicio en las redes ATM que operan con protocolo IP.**

8.3.1. En una conexión IP sobre ATM utilizando AAL5 se transmiten datagramas de 9000 bytes. Se utiliza multiplexación por VC (*Virtual Circuit*) según el RFC 1483.

Sabiendo que la probabilidad de que se pierda una celda es de  $10^{-3}$  calcule cual es la eficiencia medida por el nivel IP. Suponga que la pérdida de celdas en el flujo transmitido se produce de forma homogénea.

8.3.2. Dos hosts están conectados directamente entre sí mediante una conexión ATM STM-1 (OC-3c) que establece entre ellos un canal virtual; sobre ese canal virtual se establece una conexión TCP (sobre IP), utilizando AAL5 como protocolo de transporte (no se emplea encapsulado 802.2, por lo que en caso de necesitar soporte multiprotocolo se hará utilizando diferentes canales virtuales).





Calcule el caudal efectivo máximo que se podrá obtener a nivel ATM, nivel AAL5, nivel IP, nivel TCP y nivel de aplicación, así como el *overhead* producido en cada caso. Suponga que los datagramas IP generados son todos de 9180 bytes (valor por defecto empleado en 'Classical IP over ATM'), y que no se utilizan campos opcionales de cabecera en los datagramas IP ni en los segmentos TCP.

#### 8.4. El protocolo MPLS. Parámetros de la calidad de servicio en redes IP/MPLS: pérdida de paquetes, demora, *jitter* y disponibilidad de la red. Evolución futura de las redes que operan con IP/MPLS.

### 9. UNIDAD DIDÁCTICA N° 9: Seguridad en redes de datos, redes VPN.

EJERCICIOS RECOMENDADOS PARA TRABAJOS DE LABORATORIOS	
9.1.1. a 9.1.5	Configuración
9.3.1. a 9.3.3	Configuración
9.7.1	Configuración
9.9.2.	Configuración

#### 9.1. Introducción a la seguridad en redes de datos. Estrategias de seguridad. Ataques a la seguridad de una red.

9.1.1. Analice comparativamente el enfoque de seguridad conocido como "Defensa Perimetral" (a veces, llamado del "castillo medieval"):

- <https://www.cisecurity.org/controls/boundary-defense/>
- <https://security.uci.edu/security-plan/plan-control13.html>,
- <https://www.tripwire.com/state-of-security/security-data-protection/20-critical-security-controls-control-13-boundary-defense/>,

y la estrategia de la "Guerra Submarina":

<http://searchsecurity.techtarget.com/feature/Beyond-network-perimeter-defense-A-submarine-warfare-strategy>.

9.1.2. Complemente el análisis anterior con un informe actualizado de amenazas, por ejemplo: <https://www.sans.org/reading-room/whitepapers/awareness/defending-wrong-enemy-2017-insider-threat-survey-37890>.

9.1.3. Estudie el documento "Cisco SAFE: Un modelo de seguridad para las redes de las empresas"

([http://www.cisco.com/c/dam/global/es\\_es/assets/docs/safe\\_wp1.pdf](http://www.cisco.com/c/dam/global/es_es/assets/docs/safe_wp1.pdf)) y analice el "Módulo de Internet de la empresa" identificando los protocolos de red interviniente, los dispositivos y servicios / aplicaciones que se recomiendan para la protección.

9.1.4. Analice desde la perspectiva de "arquitectura de red", el enfoque: [https://www.sans.org/security-resources/IAD\\_top\\_10\\_info\\_assurance\\_mitigations.pdf](https://www.sans.org/security-resources/IAD_top_10_info_assurance_mitigations.pdf)

9.1.5. Analice el enfoque de seguridad **Zero Trust Architecture**, comparándolo con el de "Defensa Perimetral" y "Guerra Submarina", <https://csrc.nist.gov/publications/detail/sp/800-207/final>

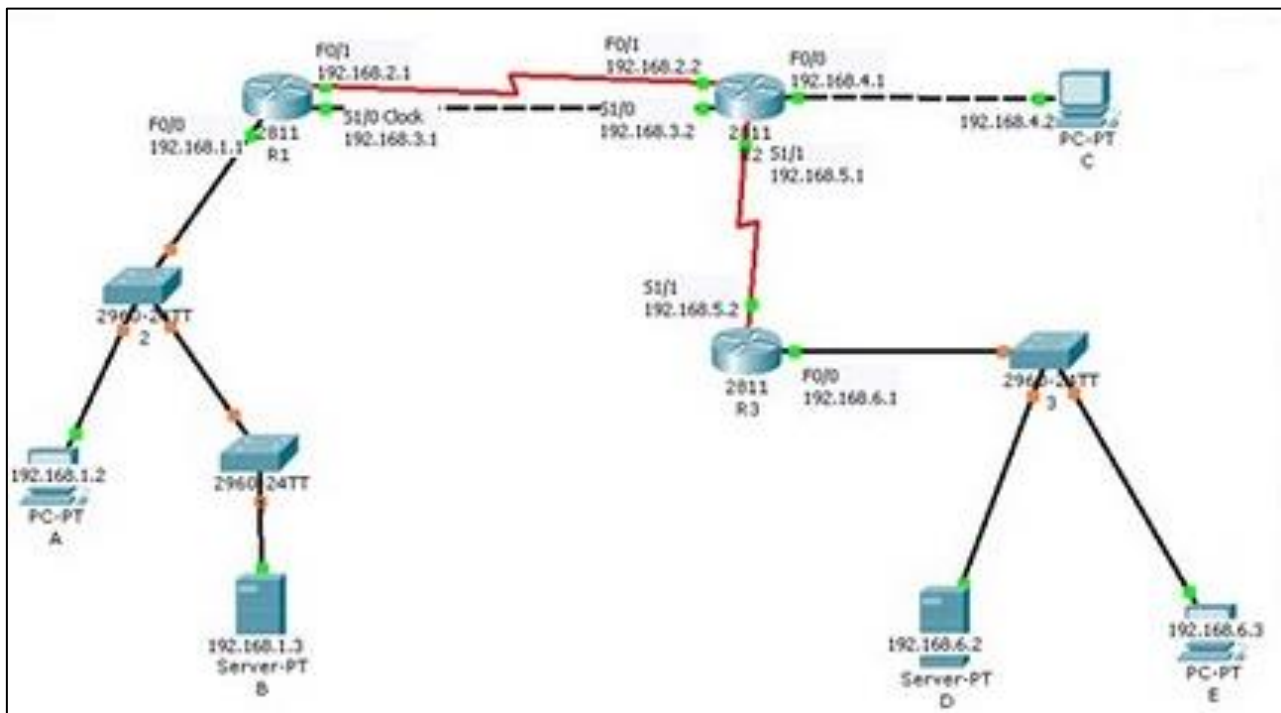
#### 9.2. Arquitecturas de Firewalls.

#### 9.3. Filtrado de paquetes.

9.3.1. Empleando listas de control de acceso, diseñar filtros de paquetes que permitan:



- 9.3.1.1. Evitar que el tráfico del servicio de ECHO (puerto TCP 7) desde un host específico (estación de trabajo con dirección IP 172.20.40.3) conectada a un switch FastEthernet de la interfaz f0/0 del router propio, alcance las redes vecinas, cuyas IP tengan en el 3er octeto los valores 48, 56, 64, 72, 128, 136, 144, 152, 160, 168, pero sí se debe poder ejecutar frente a un servidor situado en cualquier otra red; además, cualquier otro servicio debe de poder funcionar normalmente.
- 9.3.1.2. Evitar que el tráfico del servicio DAYTIME (puerto TCP 13) desde un host específico (estación de trabajo con dirección IP 172.20.56.3) conectada al switch FastEthernet de la interfaz f0/0 del router propio, alcance la red vecina cuyas direcciones se mencionan 9.3.1.1.
- 9.3.2. Diseñar y planificar un plan de seguridad que implemente ACL extendidas. Se debe trabajar con múltiples listas de control de acceso extendidas para simular la regulación del tráfico al que se permite pasar, a través de múltiples routers, a varios servidores e Internet. Puede haber más de una respuesta correcta. A continuación, se suministran los requisitos y algunos supuestos para este ejercicio. En general es mejor intentar usar la menor cantidad posible de listas de acceso y tener en cuenta el potencial de crecimiento de la red. En este ejercicio se usarán ACL extendidas.
- Requisitos:
- 9.3.2.1. Supongamos que sus servidores empresariales se ubican en la red 172.20.56.0 (desde Buenos Aires).
- 9.3.2.1.1. Se debe permitir acceso a través de la Web (protocolo http) a su servidor web 172.20.56.80 para cualquier persona.
- 9.3.2.1.2. Se debe permitir el acceso a través de DNS a su servidor DNS 172.20.56.53.
- 9.3.2.1.3. Se debe permitir que el personal docente tenga pleno acceso desde la red 172.20.72.0 a cualquiera de estos servidores.
- 9.3.2.1.4. No se debe permitir otro acceso a ningún servidor en la red 172.20.56.0
- 9.3.2.2. Suponga que todos los estudiantes se encuentran en la red 172.20.48.0, y se desea controlar el acceso hacia o desde esa red. Supongamos que el router Mendoza pertenece a su ISP y no tiene control sobre él.
- 9.3.2.2.1. No se debe permitir que los estudiantes usen FTP a Internet (¡posibles problemas de virus!).
- 9.3.2.2.2. Se debe permitir que los estudiantes tengan cualquier otro tipo de acceso a Internet.
- 9.3.2.2.3. Se debe permitir que los estudiantes tengan acceso a la red del cuerpo docente 172.20.72.0 para pasar mensajes de correo electrónico (SMTP).
- 9.3.2.2.4. Se debe denegar a los estudiantes cualquier otro tipo de acceso a la red del cuerpo docente 172.20.72.0.
- 9.3.3. Dado el siguiente escenario:



9.3.3.1. Diseñe filtros ACL básicos para descartar por origen el tráfico de las PC con IP par que sea enviado al servidor D (192.168.6.2).

9.3.3.2. Diseñe filtros ACL extendidos para implementar las siguientes políticas:

- D no puede hacer ping A, C
- R3 no puede hacer ping R1.
- E no puede hacer telnet hacia R1.
- B, C no pueden ver el WWW D.
- D, E no pueden ver el WWW de B.
- D no puede hacer telnet hacia R1
- C y A no pueden hacer telnet hacia R3.
- E, B, no pueden hacer ping hacia R2.
- R3 no puede hacer telnet hacia R1.
- A no puede hacer telnet hacia R2.
- R2, D no pueden hacer ping hacia B.

#### 9.4. Sistemas Proxy. Configuración segura de servicios de Internet.

#### 9.5. Políticas de seguridad.

#### 9.6. Autenticación y Firma Digital.

#### 9.7. Diferentes tipos de cifrado: Simétrico, asimétrico y hashing.

9.7.1. Identifique los protocolos criptográficos utilizados en el TL 4 y clasifíquelos según los diferentes tipos de cifrado.

#### 9.8. La firma electrónica.

#### 9.9. Redes VPN, configuración e implementación.

9.9.1. En base a MPLS – VPN (RFC 2547 bis), modelar el diseño de una solución que permita a redes IP de gran escala, ofrecer servicios de VPNs que:

- Escale a un gran número de clientes (100.000 a 1.000.000 VPNs).
- Servicios de valor agregado.



UTN – FRBA

Departamento de Sistemas

**MATERIA:** Redes de Información

**NIVEL:** Cuarto

- Mejor aprovechamiento de la infraestructura existente.
- 9.9.2. Estudie el apunte “**6342ch2 Consideraciones de Diseño de Redes Seguras.pdf**” y realice un análisis comparativo de las arquitecturas, servicios y protocolos de seguridad para cada caso (*Business Partner, Remote office, Remote user*), desde la perspectiva VPN.

**9.10. El monitoreo, gestión y control de las redes teleinformáticas, su relación con la seguridad informática.**

**Nota: en una versión siguiente se incorporarán otras ejercitaciones.**

---

**Bibliografía y otras fuentes**

- Magaña Lizarrondo, E.; Izkue mendi, E; otros. Comunicaciones y Redes de Computadores. Problemas y ejercicios resueltos. PEARSON EDUCACIÓN S.A. 2003.
- Rubén Fusario y docentes de la Cátedra Redes de Información. Apuntes y ejercicios resueltos. FRBA – UTN. 2011.
- Stallings, William. Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud. Pearson Education. 2016.
- <http://mqa.blogspot.com.ar/2011/09/ejercicio-acl-resuelto-reto-n1.html>