

Trabajo Práctico de Integración de Conocimientos

El trabajo final del curso consiste en demostrar habilidades para diseñar, configurar y administrar una solución de conectividad, equipamiento y servicios aplicada a un caso de estudio. Para ello deberá redactar un documento con una estructura específica.

Estructura del documento a redactar

1. Resumen ejecutivo

Se debe describir el problema a solucionar (que forma parte de este enunciado) y la solución que usted propone, detallando cuáles son las principales características de su diseño, ventajas y desventajas. Este apartado debe estar escrito para público de nivel gerencial, no técnico (que no está especializado en redes y telecomunicaciones) y poseer entre media y una carilla de longitud.

2. Características principales del diseño

Se deben presentar las estrategias principales del diseño propuesto y las tecnologías que se utilizarán para resolver el caso de estudio (contratación de enlaces dedicados, uso de VPNs, contratación de enlaces con características de QoS especiales para el problema, etc). Se debe indicar y justificar cualquier otra configuración y/o suposiciones realizadas (o restricciones impuestas).

Tanto este apartado como los siguientes están destinados a lectores técnicos, por lo cual deben estar escritos con lenguaje apropiado y específico.

3. Topología de alto nivel

Se debe especificar en esta sección:

- La arquitectura principal de la red, desde un alto nivel de abstracción, especificando los segmentos de red principales para cada locación o área de interés mediante uno o más gráficos.
- La interconexión entre los lugares y los medios físicos utilizados para lograrlo.
- El direccionamiento de los segmentos de red y de los dispositivos principales.
- Las tablas de ruta de cada uno de los routers principales, indicando: dirección destino/máscara, gateway, interfaz, vlan (si correspondiera) y descripción (mnemónico o comentarios pertinentes).
- Los enlaces necesarios para la conectividad a Internet y otros enlaces punto a punto, para las distintas locaciones, indicando los requerimientos de nivel de servicio (SLAs) de contratación para cada enlace. Se espera que se acompañe a estos datos con las estimaciones y cálculos necesarios para poder llegar a los valores propuestos (esp. para la tasa de transferencia).

4. Topología física

Se debe especificar en esta sección:

- La arquitectura de la red de cada locación, desde un nivel de abstracción menor, especificando los dispositivos activos (switches, routers, access points, servidores, estaciones de trabajo y otros equipos con capa IP) y el direccionamiento de cada dispositivo.
- Si la topología cuenta con VLANs, especificar en qué switches existen y los modos en que están configurados sus puertos.
- Los dispositivos físicos requeridos para la interconectividad solicitada, indicando cantidad, tipo y modelo a partir de los productos disponibles en el mercado.

5. Ingeniería de tráfico

En esta sección se deberán especificar:

- Los flujos de datos principales en la red para la provisión de los servicios **específicos del caso de estudio**, indicando: fuente(s), destino(s) y modelo de cada uno según McCabe, tasa de transferencia requerida y estimada, y prioridad respecto al resto de los flujos.
- En los routers que corresponda, las políticas de acondicionamiento de tráfico a aplicar por servicio y por enlace y los filtros necesario para lograrlo.

6. Administración y gestión de la red

Deben describirse cuáles son los dispositivos que serán monitoreados activamente de forma automatizada, con qué tecnología se realizará, y qué características serán las observadas en cada uno.

7. Seguridad en redes de datos

En esta sección se debe incluir:

- Las herramientas de protección de confidencialidad e integridad del tráfico de red y la gestión de las mismas.
- Cualquier descripción necesaria para comprender la separación de redes en capa 2 (dominios de broadcast) y capa 3 (redes IP).
- La configuración de los firewalls que considere apropiada en formato tabla donde se describa: cadena (según iptables), ip/red origen, ip/red destino, protocolo, puerto, acción y comentario.
- Las tecnologías a utilizar para brindar seguridad en acceso remoto y gestión de certificados (de corresponder).
- Los mecanismos para garantizar la disponibilidad y tolerancia a fallas de los servicios provistos, tales como suministro eléctrico, conectividad y refrigeración. Debe indicarse el esquema de conexión y los dispositivos de red que dispondrán de redundancia.

8. Presentación y evaluación

La propuesta deberá ser entregada en formato digital y papel, con un límite de 30 páginas, excluyendo anexos. La evaluación se basará en la calidad del análisis de requerimientos, la solidez y coherencia del diseño propuesto, y la claridad y detalle de la documentación. Se valorará especialmente la capacidad de justificar las decisiones de diseño y su alineación con los objetivos del proyecto. En este sentido, se busca evaluar tanto sus conocimientos técnicos como su capacidad para abordar un problema de diseño de manera integral y estructurada.

DESAFÍO

Como siempre, este ejercicio no es obligatorio.

Lea los siguientes documentos sobre consideraciones de Redes de Comunicaciones y mencione en pocos párrafos su relación con los temas vistos en la asignatura:

- Callon, R. RFC 1925: The Twelve Networking Truths. 1 de abril de 1996.
<https://tools.ietf.org/html/rfc1925>.
- Erratas del RFC1925. Consultado el 13 de noviembre de 2020.
https://www.rfc-editor.org/errata_search.php?rfc=1925

Caso de estudio 2025: Counter-Trique II Cup Argentina

Como parte de un evento que viene realizándose desde hace años, una productora de eventos nacional tiene planificado realizar una nueva edición del Counter-Trique II Cup, la competencia de eSports tradicional de este particular videojuego.

Teniendo en cuenta que los eventos de eSports ya no son como las pequeñas LAN parties tradicionales sino que involucran gran cantidad de dispositivos, múltiples redes y garantías de seguridad y rendimiento, la empresa le ha acercado a ud. una Solicitud de Propuesta (RFP, en inglés) de una arquitectura de red subyacente que permita una jugabilidad fluida, soporte las transmisiones en directo, permita brindar estadísticas en tiempo real, e incluso la interacción con los aficionados.

Servicios que la arquitectura debe soportar

- **Red de juego**
 - La primera y principal red que conecta las computadoras y/o consolas de los jugadores a los servidores de juego locales. La conectividad debe ser exclusivamente cableada, con alta disponibilidad y muy baja latencia.
 - En las partidas compiten dos equipos de cinco jugadores cada uno. Por las características del torneo, la red debe soportar la ejecución de cuatro partidas en simultáneo. Tanto las partidas como los equipos deben estar aisladas entre sí, pero deben poder llegar a los servidores de juego, que también están en esta red pero como multi-homed hosts.
- **Red de producción/medios**
 - Utilizada por los equipos de streaming, post-procesamiento y transmisión. Transporta múltiples flujos de video (10 a 15 cámaras), que se mezclan en tiempo real y se transmiten a servicios tales como Twitch y YouTube. Los flujos también se almacenan en crudo para la creación de resúmenes y análisis posterior. Como en el caso previo, la conectividad será exclusivamente cableada y preparada para una alta tasa de transferencia.
- **Red de operaciones**
 - Utilizada por el staff técnico y de gestión del evento para tareas internas tales como alta y acreditación de participantes, setup, control y arbitraje de las partidas, y otras. La conectividad será cableada pero debe admitirse también Wi-Fi.
- **Red de sponsors (remotos)**
 - Algunos de los servicios de la red de operaciones también deben estar disponibles en forma remota para ciertas empresas que promocionan el evento, pudiendo ellas dar de alta a sus propios equipos, incorporar nuevos participantes, publicar promociones en el servidor de anuncios en línea, y tener acceso a datos de audiencia. Como tal, esta red requiere consideraciones adicionales en cuanto a seguridad.
- **Red de espectadores**
 - El evento será con público, por lo que se planea brindar conectividad a la audiencia, tanto hacia Internet como también a un servidor de scoreboard y anuncios en línea. Desde luego, la conectividad de usuarios no debe afectar ninguna de las demás redes.
- **Red de voz/comunicaciones**
 - Transporta el chat de voz, los intercomunicadores intra e inter equipos, y la comunicación del staff. Debe soportar tanto VoIP tradicional como protocolos específicos que se ejecutan sobre UDP.
- **Monitoreo continuo y acceso remoto**
 - Se deberá proveer una o más estaciones de monitoreo de red para mantener el monitoreo y control en tiempo real de las métricas de performance y seguridad relevantes, con la posibilidad de envío de alertas automatizadas para tratamiento de incidentes.



Requerimientos de seguridad y performance

La arquitectura debe brindar los tres servicios de seguridad más importantes. El evento depende crucialmente de conectividad continua y puede considerarse *de misión crítica*, por lo cual la red debe soportar la caída de cualesquiera dispositivos y/o enlaces sin afectar la jugabilidad ni la transmisión. Para garantizar la salida a Internet, usted debe contemplar qué SLA se solicitará al/a los ISPs. La redundancia debe extenderse más allá de la conectividad e incluir las capas que están por abajo del modelo OSI.

Adicionalmente, la red debe implementar políticas de control de acceso rigurosas para garantizar que solo el personal autorizado pueda acceder a los sistemas, y que estos no se vean afectados por actores externos ni internos.