IIC2523
Sistemas Distribuidos

Hernán F. Valdivieso López
(2025 - 2 / Clase 24)

Casos Aplicados
VPN vs TOR, Eduroam y BitTorrent

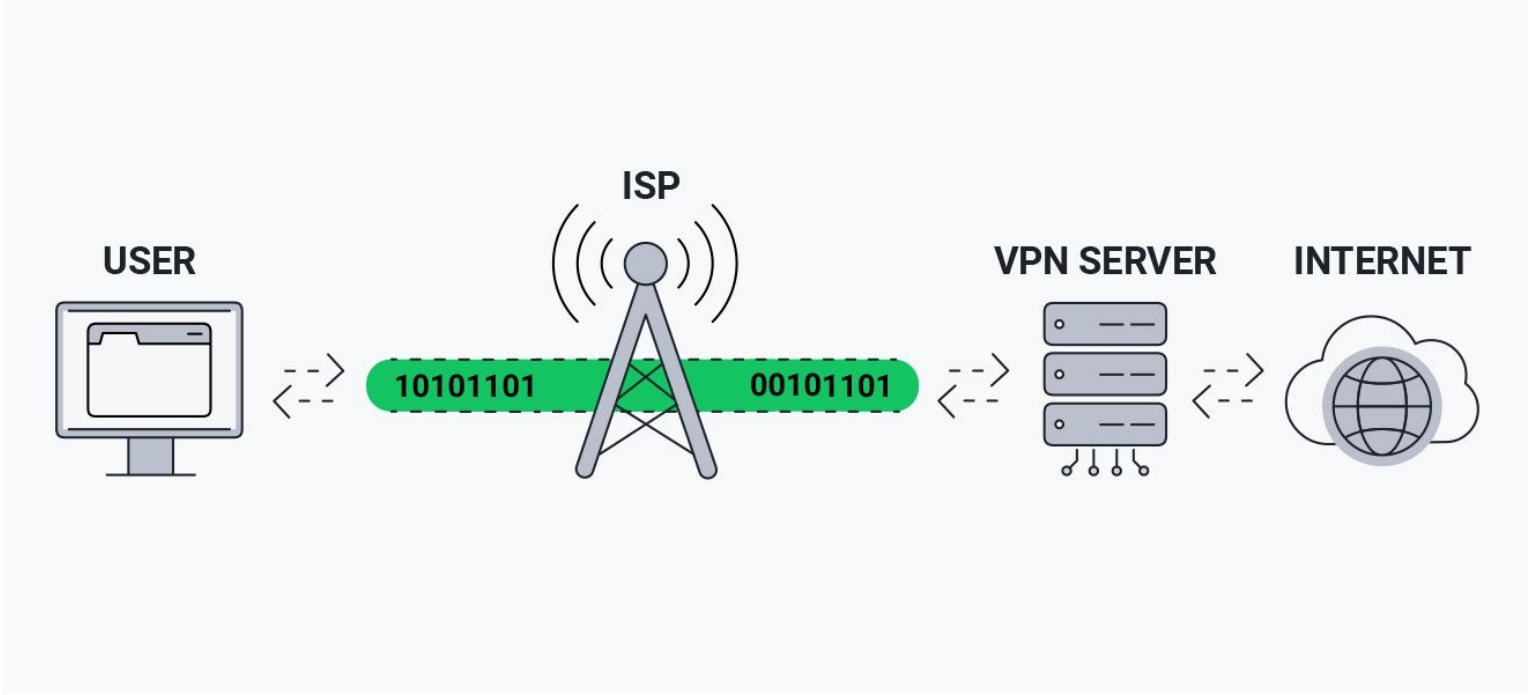
Temas de la clase

1. VPN vs Tor
2. Eduroam
3. Bittorrent

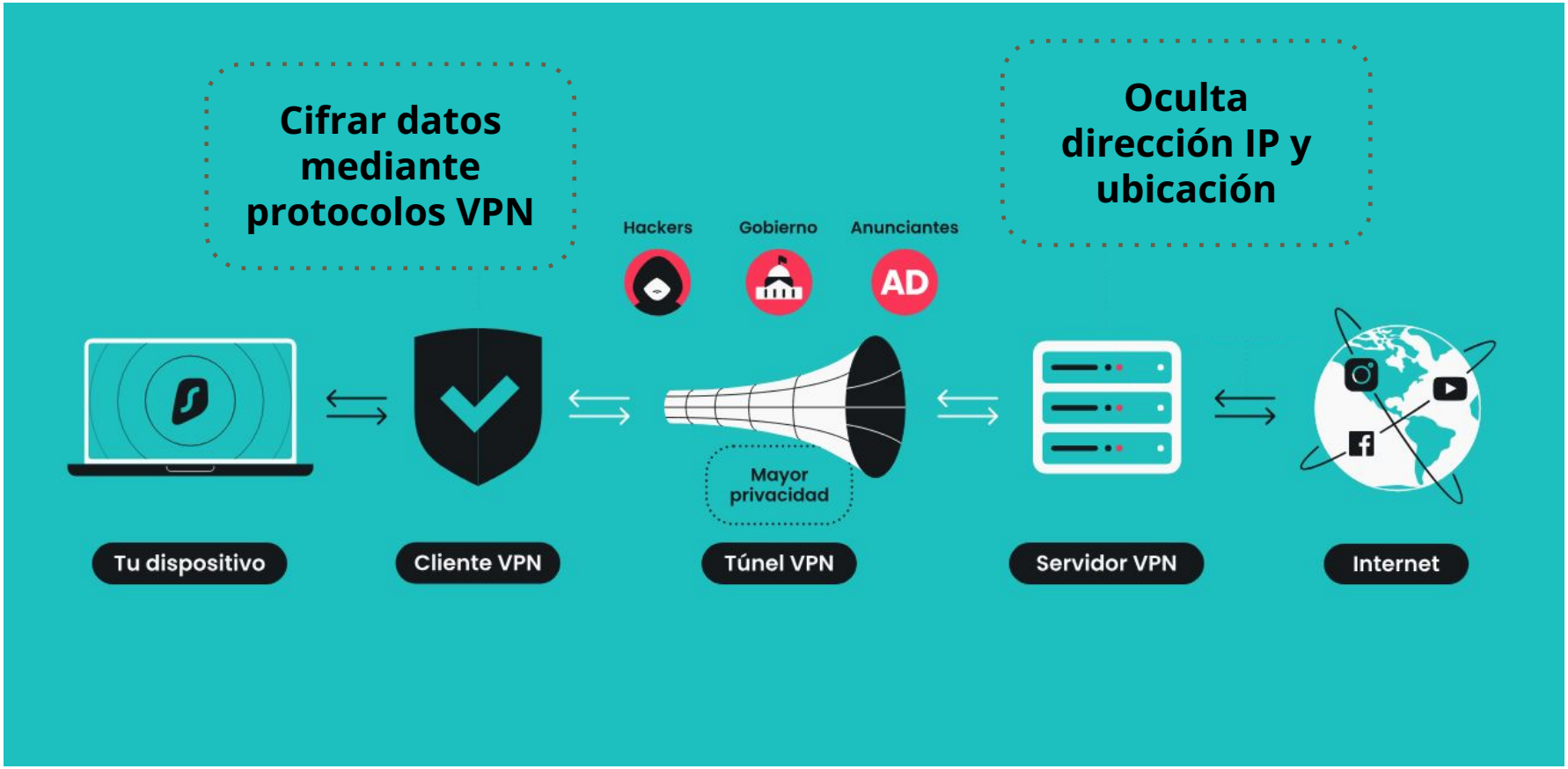
Red privada Virtual (VPN)

Red privada Virtual (VPN)

- Túnel seguro y privado a través de Internet entre el usuario y una página.
- Ayudan a eludir la censura, bloqueos de contenido y restricciones de sitios web.

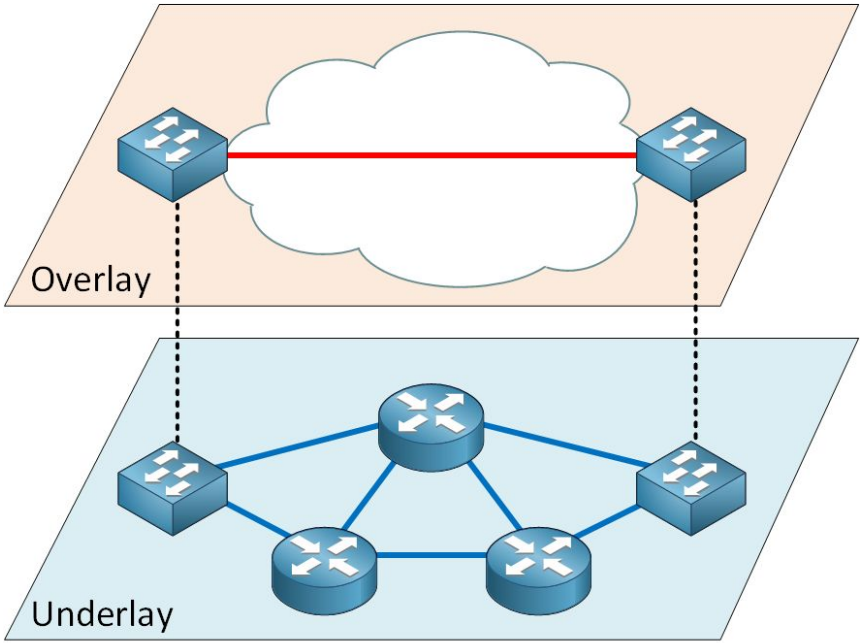


Red privada Virtual (VPN) - Seguridad



Red privada Virtual (VPN) - *Overlay Networks*

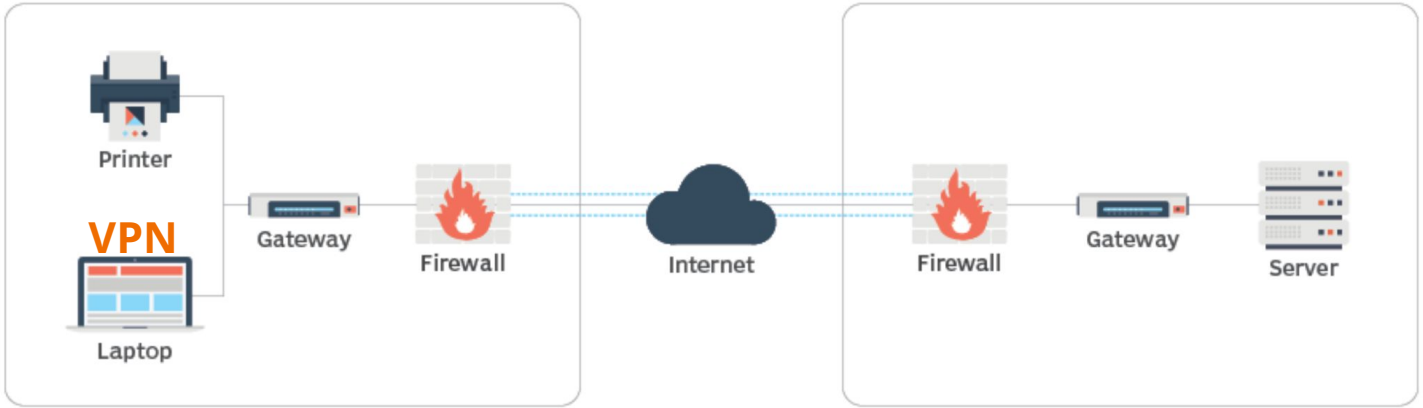
- Las VPN se clasifican como una *Security Overlay networks*.
- Construyen una red virtual sobre una red subyacente
  - Protocolos de cifrado específicos (como IPsec o WireGuard).
  - Funcionalidades adicionales que no están presentes en la red base.



Red privada Virtual (VPN) - Tipos

***Remote Access* VPN**

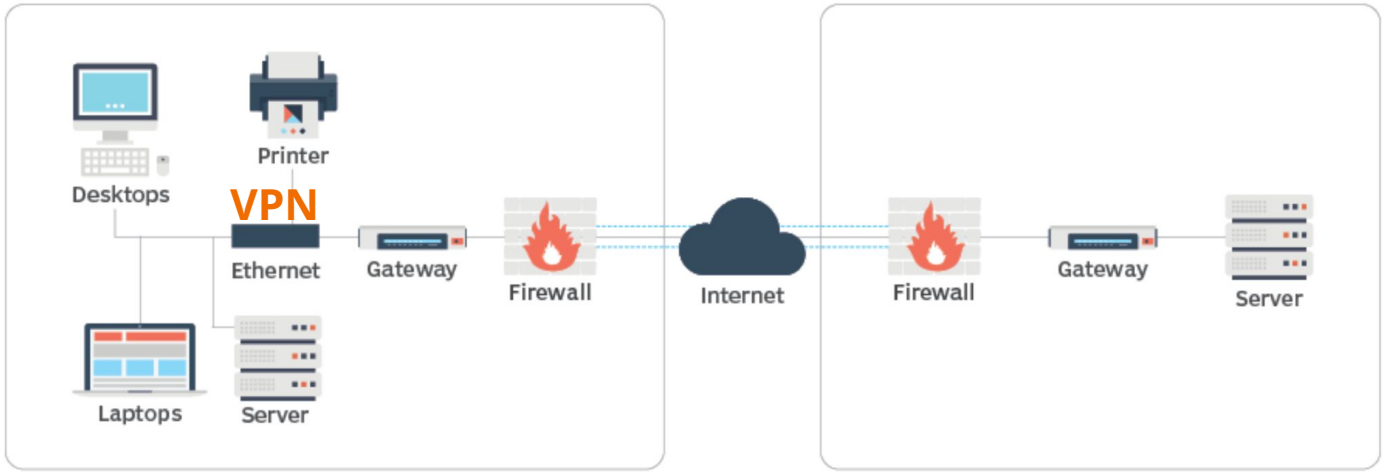
- Permite que usuarios individuales se conecten desde cualquier lugar a una red.
- El cliente dispone de un *software* VPN para comunicarse la otra red.
- Usado para acceso seguro a recursos internos desde ubicaciones remotas o públicas



Red privada Virtual (VPN) - Tipos

***Site-to-Site* VPN**

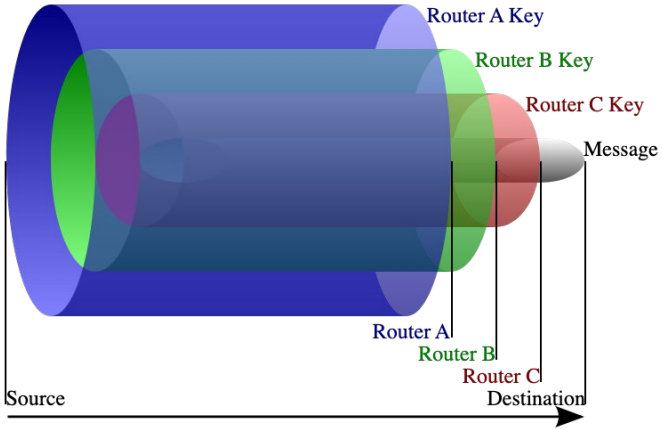
- Conecta dos o más redes completas entre sí, por ejemplo, dos sucursales.
- Permite que todo el tráfico entre las redes viaje seguro a través de Internet.
- Usado para integrar redes geográficamente separadas como si fueran una sola red privada.

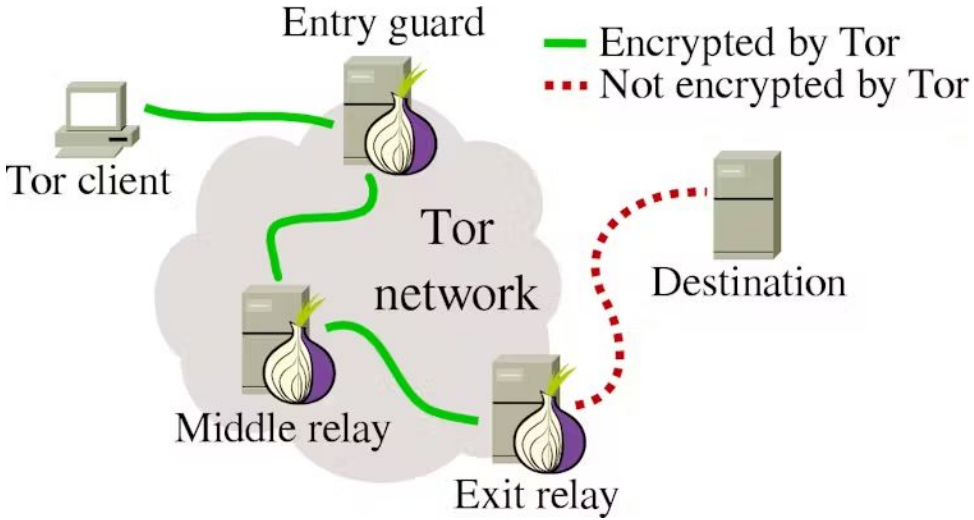


The Onion Router (Tor)

The Onion Router (Tor)

- Red P2P de anonimato compuesta por nodos voluntarios.
- Uso de *onion routing* para cifrado multicapa.
- Circuito de 3 nodos: entrada → medio → salida.





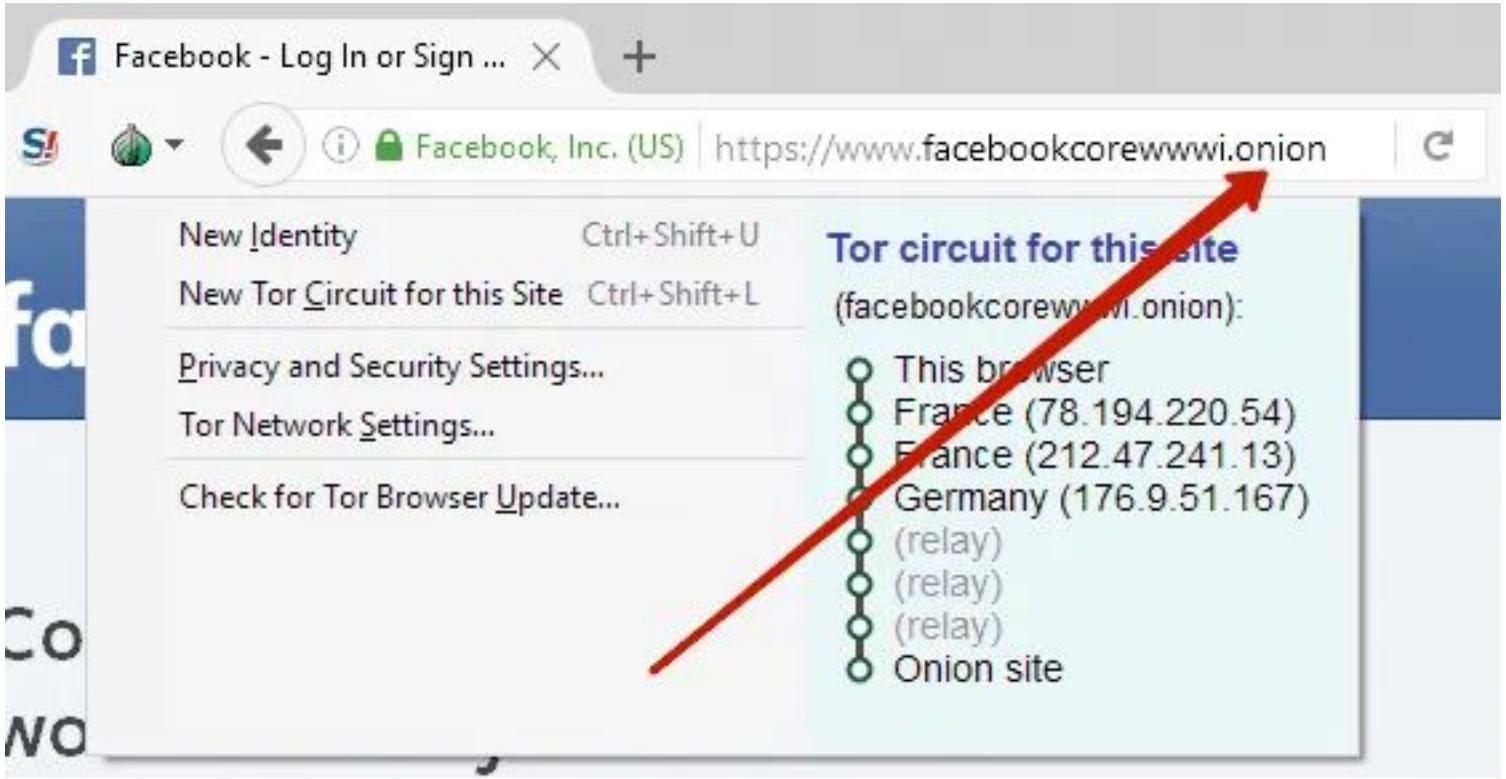
The Onion Router (Tor) - Tipos de accesos

2 tipos de accesos

- **Acceso a sitios normales (.cl, .com, etc.)**
  El usuario mantiene anonimato, pero el servidor es conocido.
- **Acceso a sitios .onion**:
  Anonimato mutuo dentro de la red Tor.

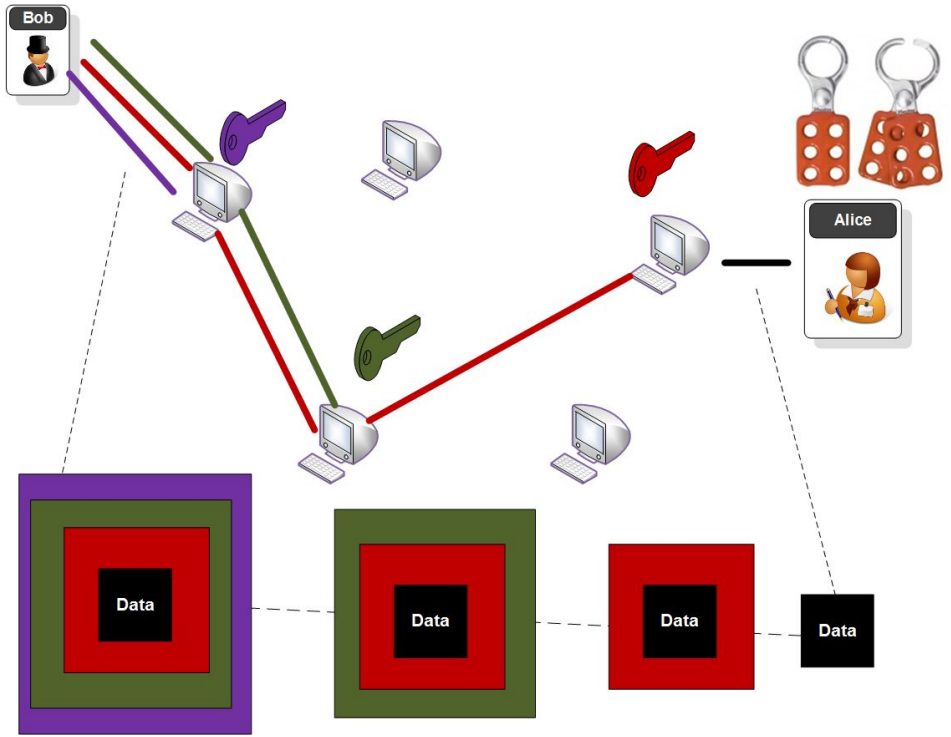
The Onion Router (Tor) - Tipos de accesos

Ejemplo - [Facebook onion address - Wikipedia]



The Onion Router (Tor) - Seguridad

- Al igual que VPN, es una *Security Overlay networks*.
- Uso de varias capas de cifrado para proteger el mensaje (*Onion Routing*)
  - Ningún nodo tenga toda la información sobre el origen, destino y contenido, preservando anonimato.



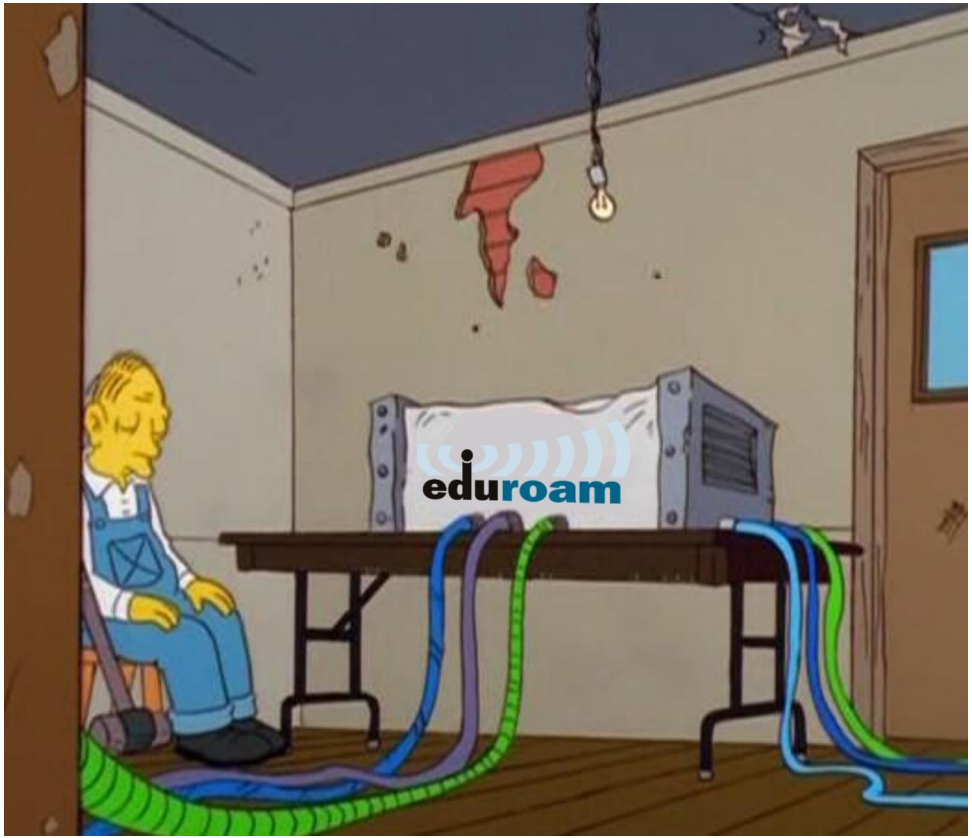
The Onion Router (Tor) - Ventajas y Desventajas

- Alta seguridad de cifrado.
- Alto anonimato, los nodos no saben quién eres ni adónde vas al final.
- Problemas:
  - Nodo de salida puede ver tráfico si no está cifrado (HTTP).
  - Más lento por la cantidad de saltos.
  - Objetivo de vigilancia en algunos contextos.

The Onion Router (Tor) - vs VPN

Aspecto	VPN	Tor
Punto de falla	Único (el servidor VPN)	Múltiples nodos independientes.
Conexión	Directo entre cliente y servidor	Circuito con 3 nodos
Riesgos	Confianza en proveedor	Nodo de salida malicioso
Anonimato	El proveedor te ve, pero servidor final no.	Alto, IP y enrutamiento anónimo.
Velocidad	Alta (en general)	Baja (múltiples saltos cifrados)
Escalabilidad	Limitada por el proveedor VPN	Alta, P2P.
Uso	Navegación segura, acceso contenido bloqueado.	Anonimato, acceso a la Dark Web

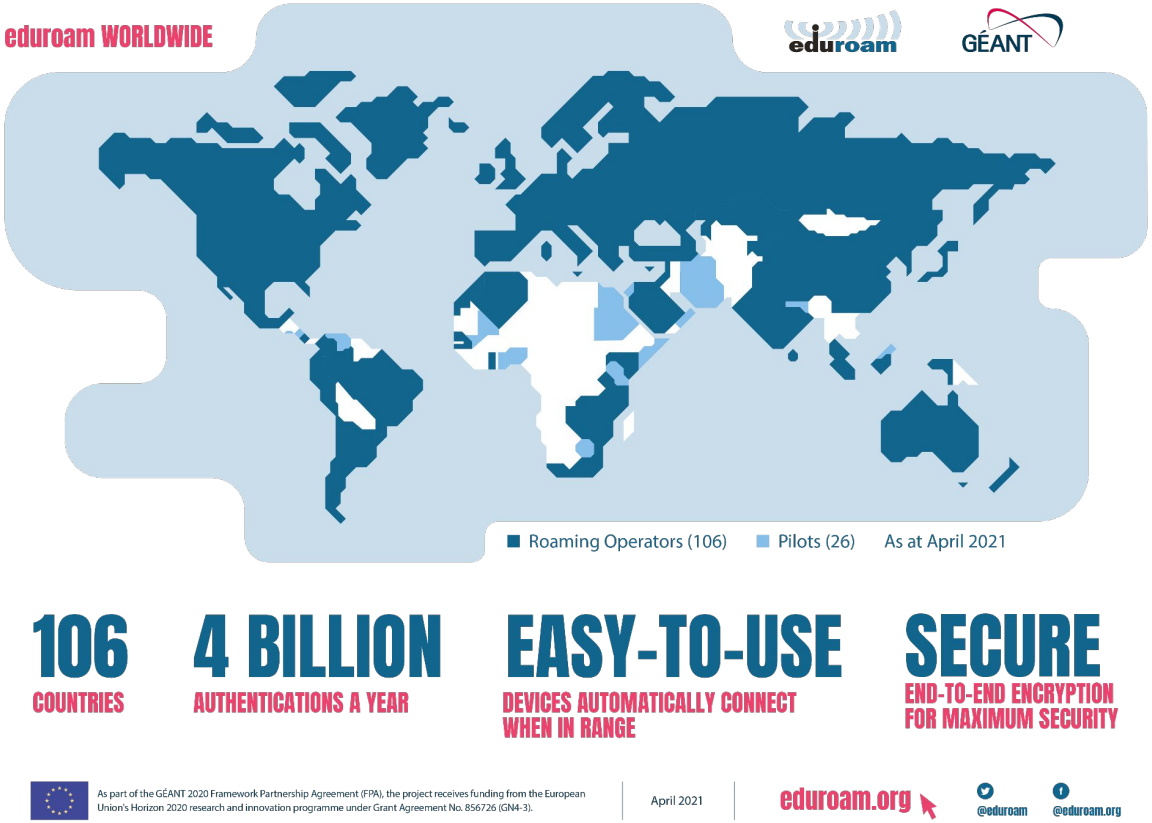
Eduroam



Eduroam

- Una red Wi-Fi internacional diseñada específicamente para instituciones educativas y de investigación.
- Federación de sistemas locales que colaboran para ofrecer un servicio global.
  - Cada institución actúa como un componente independiente en la red distribuida.

Eduroam - Alcance



Fuente: [eduroam media and resources]

Eduroam - Sistema Distribuido

- Rol de autenticación y de prestador de servicio está separado.

SP - Service Provider

- La institución visitada donde el usuario se conecta a la red Wi-Fi.
- Proporcionar el "acceso físico a la red" una vez que la autenticación es exitosa

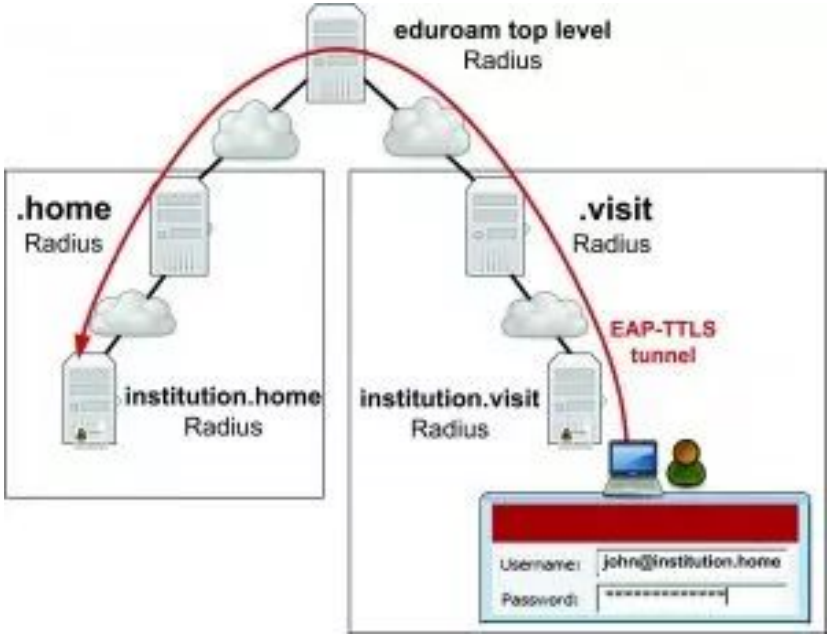
IdP - Identity Provider

- La institución de origen del usuario.
- Es responsable de autenticar a sus propios usuarios. Piensen en él como el "servidor de autenticación" centralizado para sus propios usuarios, pero distribuido a nivel global.

- Uso de protocolo Radius para comunicar ambas entidades distribuidas por el mundo.

Eduroam - Protocolo RADIUS

- El enrutamiento de solicitudes RADIUS se basa en el nombre de usuario (usuario@dominio), donde el dominio (ej., institución.tld) se usa para dirigir la solicitud a la *IdP* correcta,
- Análogo a lo que realiza DNS.



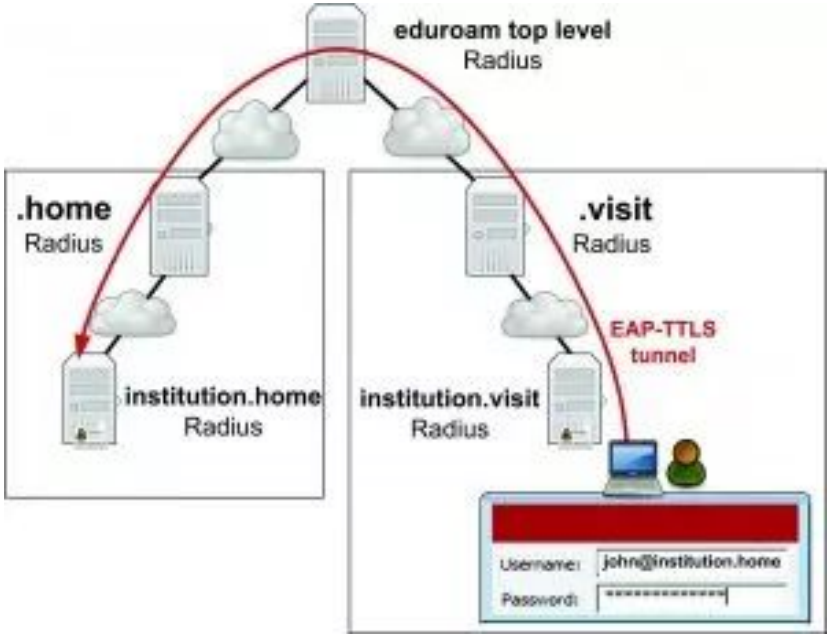
Eduroam - Protocolo RADIUS

Servidor RADIUS Organizacional

Representa a cada institución participante (por ejemplo, uc.cl, uchile.cl, usach.cl).

Cuando un usuario se conecta (local o visitante), la solicitud de autenticación es recibida por este servidor.

- Si el usuario pertenece a la misma institución, este servidor lo autentica directamente.
- Si el usuario pertenece a otra organización, reenvía la solicitud al siguiente nivel (federación nacional).



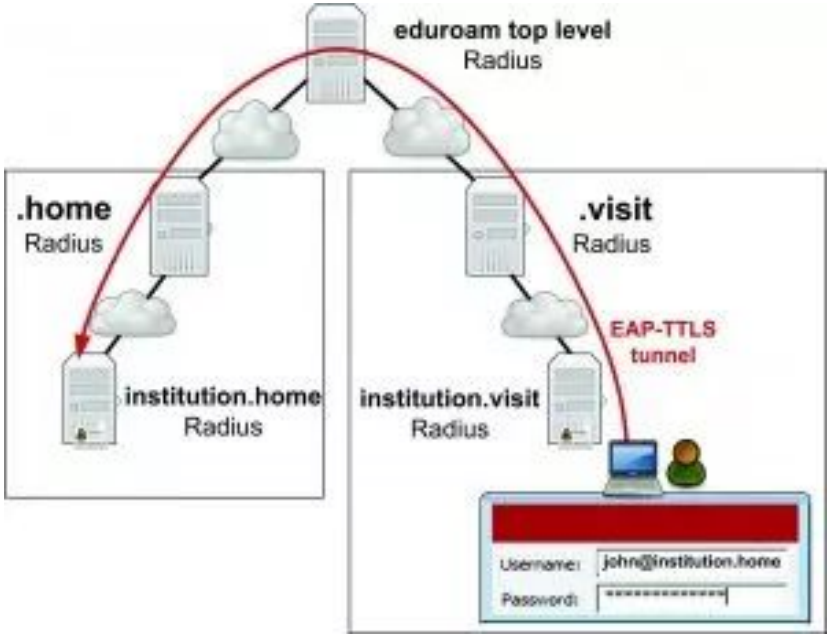
Eduroam - Protocolo RADIUS

Servidor RADIUS de Federación Nacional

Opera a nivel país (por ejemplo, eduroam.cl en Chile).

Su función es enrutar solicitudes entre instituciones nacionales.

- Si reconoce el dominio del usuario (por ejemplo, @uchile.cl), reenvía la solicitud al servidor correspondiente.
- Si no reconoce el dominio, reenvía la solicitud al servidor de confederación global.



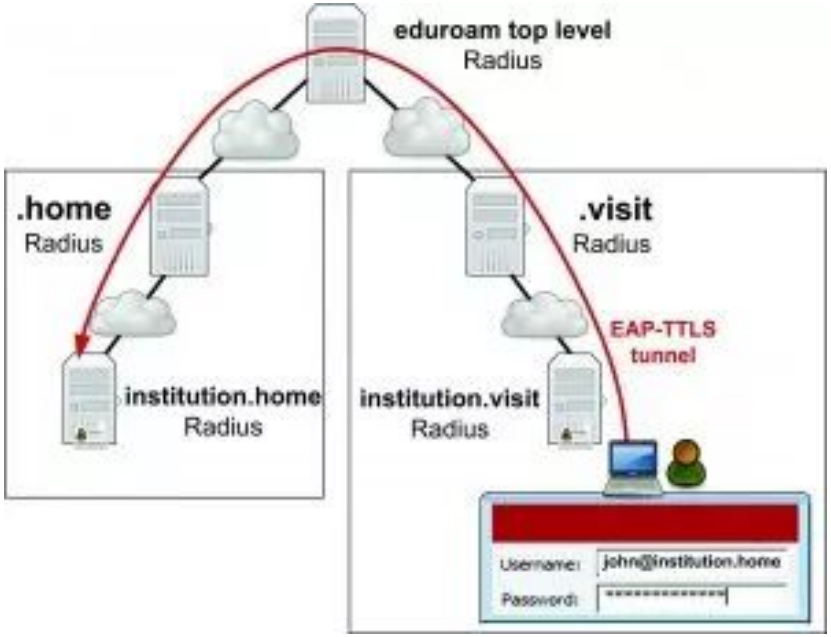
Eduroam - Protocolo RADIUS

Servidor RADIUS de Confederación Global

Es el nivel más alto de la jerarquía RADIUS de eduroam.

Se encarga de enrutar solicitudes entre federaciones nacionales.

- Basado en el dominio organizacional (por ejemplo, @ox.ac.uk), determina a qué federación nacional pertenece el usuario.
- Reenvía la solicitud a esa federación para su resolución final.



Eduroam - Seguridad

Autenticación Federada y Confianza:

- La clave es que la autenticación se realiza en el IdP del usuario, no en el SP. Esto permite que una única credencial funcione globalmente.
- El SP confía en el IdP para autenticar al usuario.

Autorización y Control de Acceso:

- Una vez autenticado por el IdP, el SP otorga acceso a la red.
- EL SP controla lo que puede ver el usuario.

Eduroam - Seguridad

Confidencialidad e Integridad de Credenciales

- Las credenciales del usuario se encapsulan y cifran dentro de un túnel TLS.
- Se asegura la privacidad y la integridad del intercambio de credenciales, haciéndolas invisibles para el SP y los servidores Radius excepto del IPs.

Monitoreo

- Los RADIUS intermedios (federal o global) pueden registrar *logs* de autenticación.
- Los SP pueden registrar tráfico, aunque sin ver credenciales.

BitTorrent

"How do you have a bigger movie selection than Netflix does?"

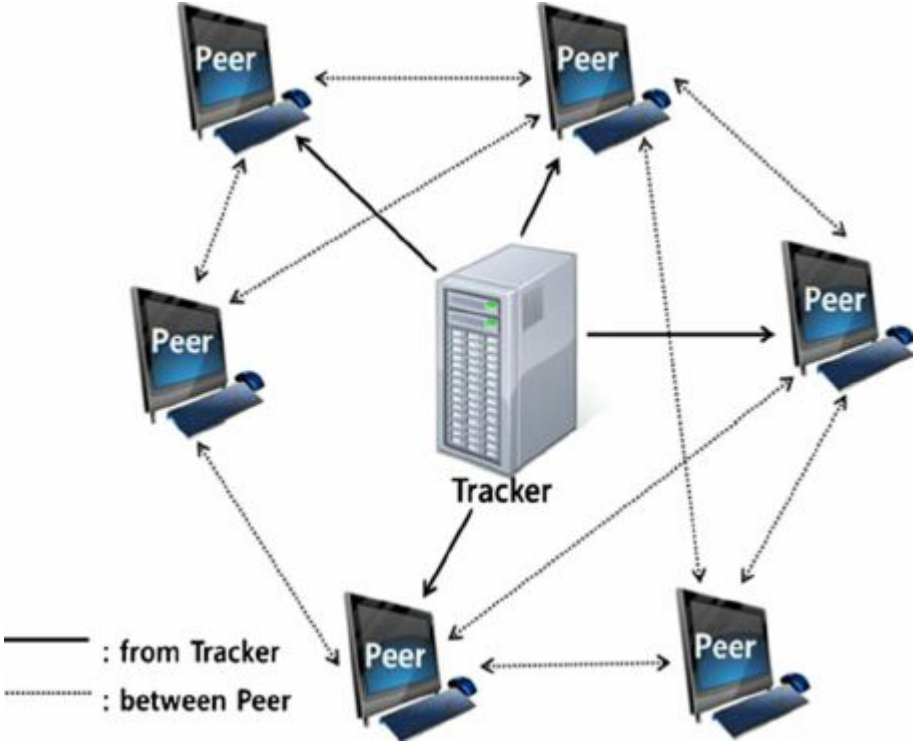
Me:

BitTorrent

- BitTorrent es un **red P2P** diseñado para la distribución eficiente de archivos grandes, dividiéndolos en **piezas pequeñas** y permitiendo a los *peers* compartir directamente entre sí.

BitTorrent - En sus inicios como P2P Centralizado

- Red P2P **no estructurada**
  - La topología entre nodos se forma dinámicamente.
  - No existe un control global sobre dónde se almacenan los fragmentos del archivo.
- Utilizaba un ***tracker*** **centralizado**
  - Uno o más servidor que mantienen una cuenta precisa de los nodos activos que tienen fragmentos del archivo solicitado.



BitTorrent - Actualidad como Modelo Híbrido

- Se incorporan DHT para que los nodos colaboran en la función de búsqueda de *peers* sin depender del *tracker*.
  - Los *trackers* siguen existiendo, pero su rol se reduce a la entrega inicial de algunos *peers*.
  - Con DHT, solo se exige encontrar al menos 1 *peer* activo.
- Se añade *Peer Exchange* para que clientes intercambiar listas de *peers* entre sí.
- Se combinan ambos enfoques: coordinación inicial centralizada y descubrimiento dinámico distribuido.

BitTorrent - Archivo .torrent

Contiene meta-información:

- Nombre y estructura del archivo(s) a descargar.
- Tamaño y *hash* de cada fragmento.
- URL del *tracker* (en caso de utilizarlo).
- Opcionalmente, otros campos como comentarios, creador, etc.

BitTorrent - Sistema distribuido

- ***Tracker*: servidor que coordina la red.**
  - No transfiere archivos.
  - Informa a cada *peer* sobre otros *peers* disponibles que están compartiendo el mismo *torrent*.
- ***Peers*: nodos participantes en la red:**
  - *Leechers*: están descargando el archivo y pueden estar subiendo al mismo tiempo fragmento del archivo.
  - *Seeders*: tienen el archivo completo y solo lo comparten.
- ***Swarm*: *leechers + seeders***
  - Conjunto de todos los peers que están compartiendo un archivo identificado por un mismo *hash*.

BitTorrent - Sistema distribuido

- ***Tracker*: servidor que coordina la red.**
  - No transfiere archivos.
  - Informa a cada *peer* sobre otros *peers* disponibles que están compartiendo el mismo *torrent*.
- ***Peers*: nodos participantes en la red:**
  - *Leechers*: están descargando el archivo y pueden estar subiendo al mismo tiempo fragmento del archivo.
  - ***Seeders*: tienen el archivo completo y solo lo comparten.**
- ***Swarm*: *leechers + seeders***
  - Conjunto de todos los peers que están compartiendo un archivo identificado por un mismo *hash*.

BitTorrent - Sistema distribuido

- ***Seeders*: tienen el archivo completo y solo lo comparten.**

BitTorrent - Riesgos

- Un nodo malicioso puede enviar datos corruptos o distintos con *hashes* válidos, comprometiendo la integridad.
  - Funciona si se ocupa un *hash* fácil de corromper.
  - También se le conoce como *Peer poisoning.*
- Dispersión de archivos maliciosos compartido por múltiples *peers* que "garantizan" que es el archivo esperado.
- La falta de cifrado por defecto permite que intermediarios inspeccionen, limiten o censuren el tráfico BitTorrent.

BitTorrent - Seguridad

- Integridad de datos mediante *hashing*
  - Cada pieza tiene un *hash* que verifica su integridad, protegiendo contra datos corruptos o maliciosos.
- Los fragmentos de archivos se replican en varios nodos para asegurar disponibilidad y reducir la existencia de fragmentos corruptos.
- BitTorrent incorpora otros mecanismos de defensa basados en **incentivos**.

Algoritmo *Choking / Unchoking*

Los *peers* eligen a quién subir datos según reciprocidad, evitando *free-riders*.

Optimistic Unchoking

Periódicamente se conecta a un *peer* aleatorio para descubrir nuevos colaboradores.

BitTorrent - Resumen de propiedades

Propiedad	BitTorrent
Tolerancia a fallos	Alta, los archivos se replican entre muchos nodos,
Transparencia	Media: el usuario ve partes del sistema, como velocidad, *peers*, etc.
Acoplamiento	Temporal y referencial
Escalabilidad	Alta, los nodos pueden entrar y salir sin problema.
Consistencia	Eventual, los bloques de archivos se propagan hasta que todos los nodos lo completan

Poniendo a prueba lo que hemos aprendido 👀

Respecto a lo visto hoy en clases, ¿Cuál o cuáles de las siguientes afirmaciones son **incorrectas**?

a. El propósito principal del *Onion Routing* es proteger la privacidad del usuario ocultando su identidad mediante capas de cifrado y nodos intermedios.

b. Usar una VPN elimina el riesgo de que alguna externa al proveedor pueda monitorear tu tráfico de Internet.

c. En Eduroam, el rol de autenticación y de prestar servicio está centralizado en un servidor central de RADIUS.

d. En BitTorrent, los *seeders* son los *peers* que tienen el archivo completo y ayudan a distribuirlo a otros *peers*.

e. Tor y VPN son herramientas excluyentes, es decir, te conectas a una página web con una de ellas.

Poniendo a prueba lo que hemos aprendido 👀

Respecto a lo visto hoy en clases, ¿Cuál o cuáles de las siguientes afirmaciones son **incorrectas**?

a. El propósito principal del *Onion Routing* es proteger la privacidad del usuario ocultando su identidad mediante capas de cifrado y nodos intermedios.

b. Usar una VPN elimina el riesgo de que alguna externa al proveedor pueda monitorear tu tráfico de Internet.

c. **En Eduroam, el rol de autenticación y de prestar servicio está centralizado en un servidor central de RADIUS.**

d. En BitTorrent, los *seeders* son los *peers* que tienen el archivo completo y ayudan a distribuirlo a otros *peers*.

e. **Tor y VPN son herramientas excluyentes, es decir, te conectas a una página web con una de ellas.**

Resumen Final

Aspecto	VPN	Tor	Eduroam	BitTorrent
Uso	Navegación segura	Navegación anónima	Acceso a internet	Descarga de archivos
Modelo	Cliente-servidor	P2P	Federación distribuida	P2P
Cifrado	Canal cifrado hasta el servidor	Cifrado en capas (*onion routing*)	TLS	Parcial (en propuestas recientes)
Autenticar	Proveedor VPN	No hay identidad visible	Autenticación federada (IdP)	No estándar, depende del cliente
Privacidad	Media, el proveedor ve todo	Alto, no se conoce la IP del origen	Media, SP ve tráfico	Bajo, sin cifrado por defecto
Amenazas Clave	*Logging* y servidor comprometido	Nodo de salida	*Logs* RADIUS	*Peer poisoning*, *Eavesdropping*

Próximos eventos

Próxima clase

- Se me acabó la materia... si tienen ideas de contenidos que hubieran querido aprender, diganmelos para considerarlos el otro semestre 😁
- La última clase del curso está reservada para una convivencia.
- Las demás clases se usarán como sala de ayuda para el control 6 y la investigación.

Evaluación

- Mañana se publica el último control que evalúa hasta esta clase.

IIC2523
Sistemas Distribuidos

Hernán F. Valdivieso López
(2025 - 2 / Clase 24)