



Redes VPN, Dark Web y Tor Project

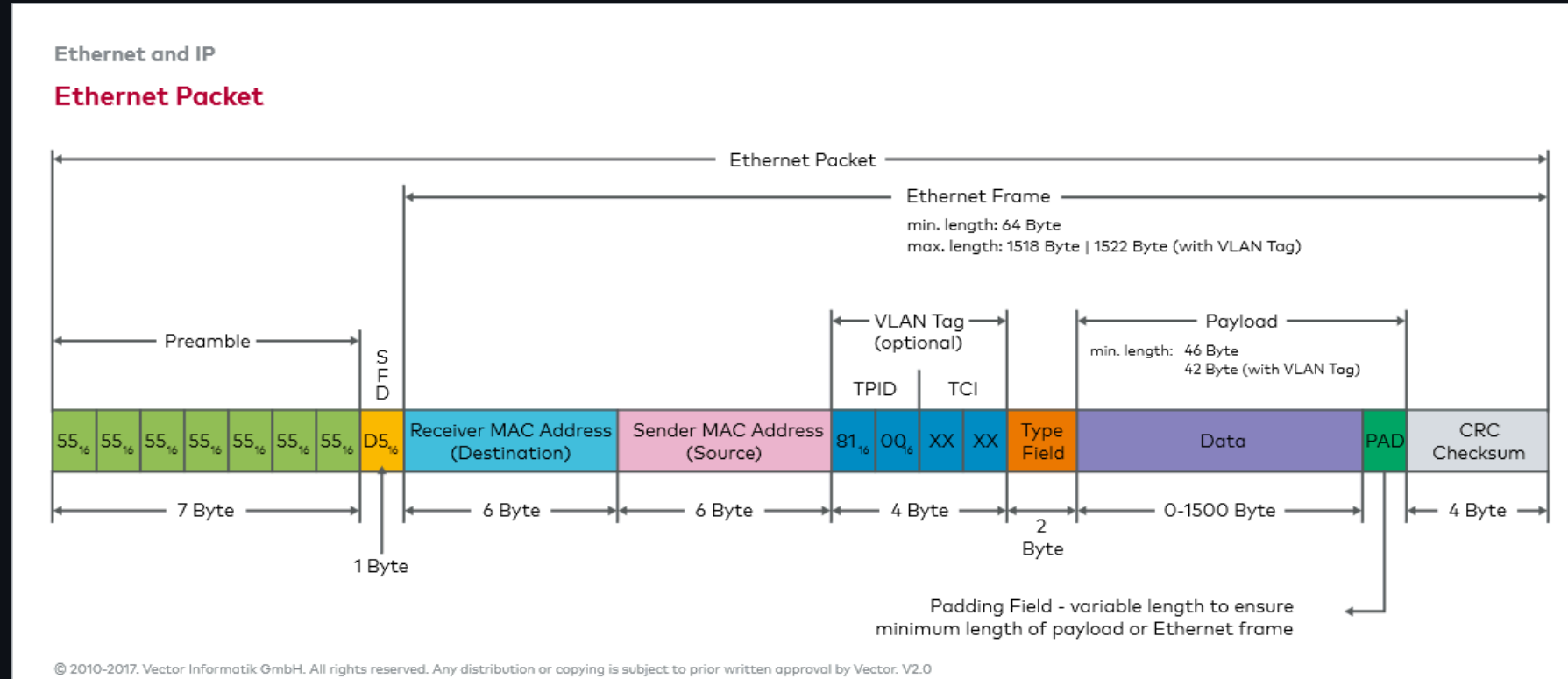
Marc Pomar · CTO @ Kirbic

marc@kirbic.com

Internet

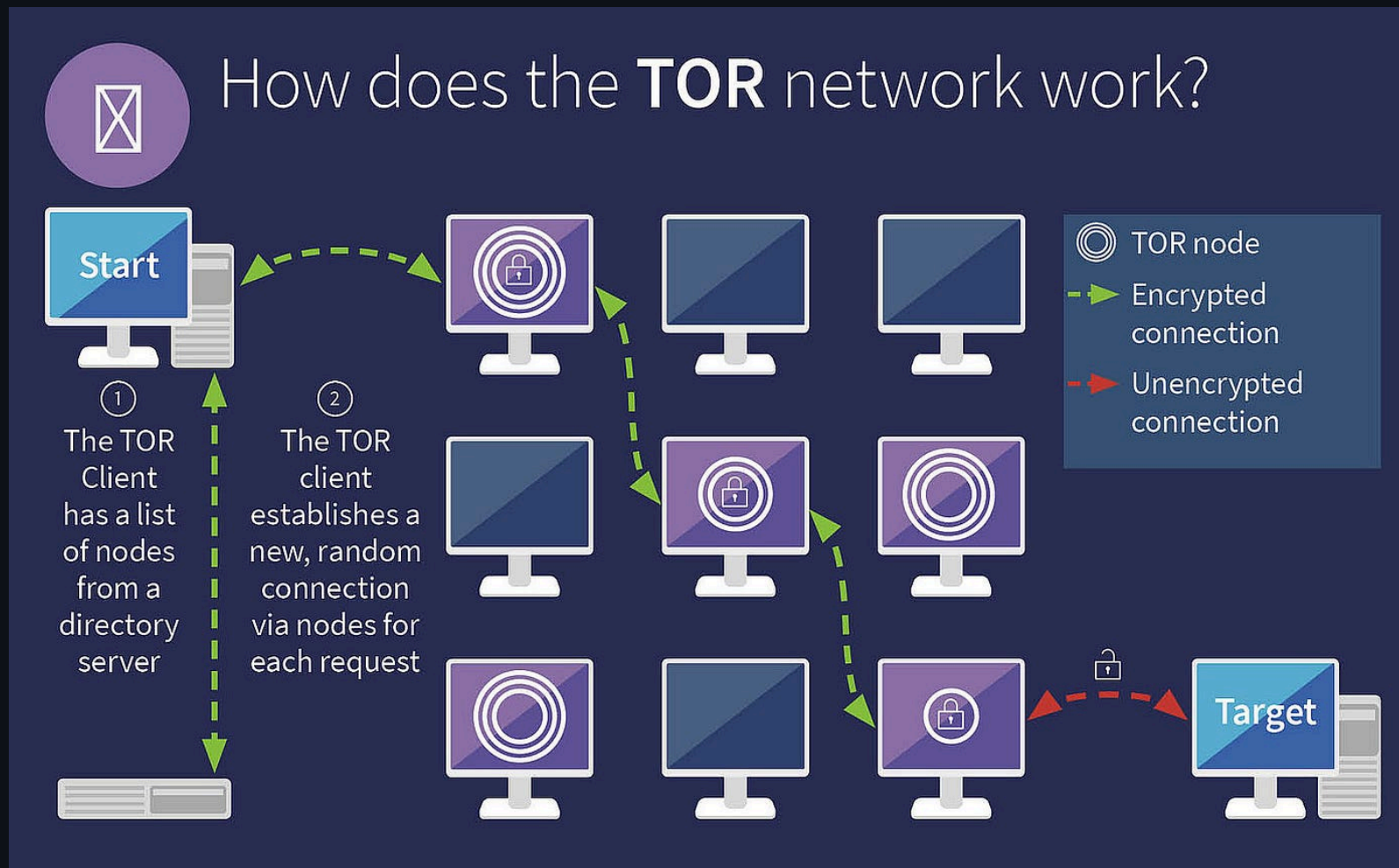
- 🌐 **Surface Web:** Son sitios web conocidos. Ej: Youtube, Bing, etc.
- 🌐 **Deep Web:** Internet no indexado por motores de búsqueda, accesible pero privado. Ej: Dropbox, Google Drive, Dashboards, etc.
- ☠️ **Dark Web:** Sitios web ocultos. Ej: Foros, Ecommerce, Datasets, etc.

Trama Ethernet

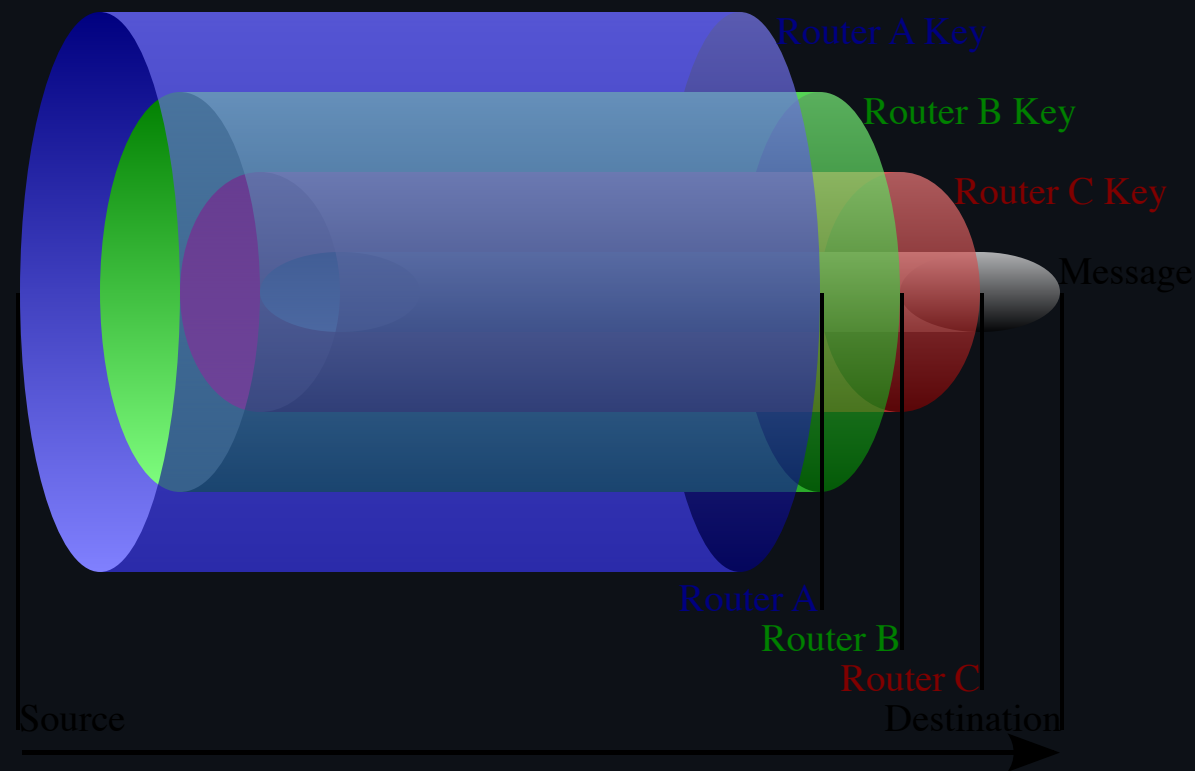


Red Tor

Encripta la conexión del usuario y la redirige a través de una serie de servidores (nodos) antes de llegar al sitio web .onion, lo que dificulta rastrear la actividad del usuario.



Onion Routing:



Tor Project

Navegador Tor

- Es un navegador web basado en Firefox
- Se conecta a la Red Tor (red distribuida)
- Todo el trafico web viaja a través de esta red

Dominios **.onion**

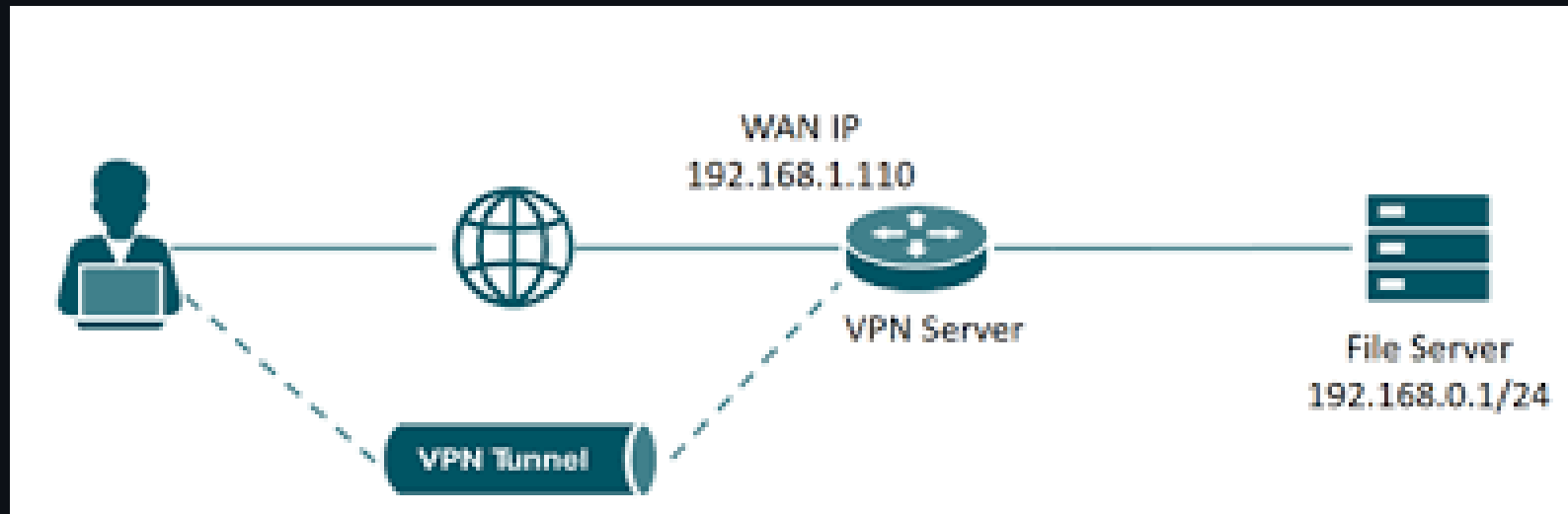
Los dominios .onion son direcciones web utilizadas en la red Tor para acceder a sitios web de forma anónima y segura.

-  [Tutorial](#)

Algunos dominios:

- [Haystack, Darknet Search Engine](#)
- [The Hidden Wiki](#)
- [CNN Secure Drop](#)

¿Que es una VPN?



Una red privada virtual (VPN) te permite atravesar redes no confiables como si estuvieras en una red privada. Te permite tener la libertad de acceder a Internet de manera segura desde un dispositivo cuando está conectado a una red no confiable, como el WiFi de un hotel o una cafetería.

Soluciones VPN:

- Wireguard
- OpenVPN
- [ZeroTier]

VPN: Wireguard

¿Cómo funciona?

1. Crea un túnel VPN:

WireGuard establece una conexión encriptada (túnel) entre dos dispositivos o entre un dispositivo y un servidor VPN.

2. Utiliza criptografía avanzada:

Emplea algoritmos de cifrado de vanguardia para proteger los datos que pasan a través del túnel.

3. Se basa en UDP:

Utiliza el protocolo UDP para una comunicación más rápida y eficiente.

4. Establece conexiones seguras:

Permite la creación de conexiones VPN seguras, ideal para proteger la privacidad y seguridad en línea.

VPN: ZeroTier

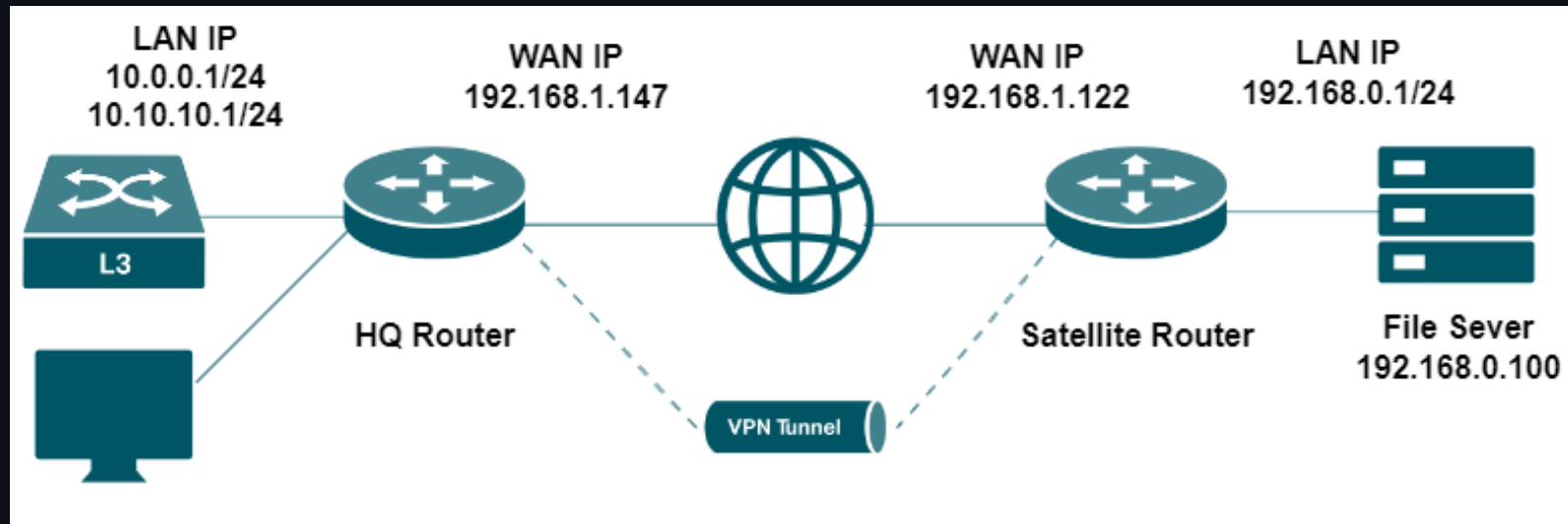
¿Cómo funciona?

- Planet & Moons: Allow nodes to find each other.
- Node: Nodes start with no direct links to one another, only upstream to roots (planet and moons). Every node is uniquely identified on VL1 by a 40-bit (10 hex digit) ZeroTier address.
- Controller: Controllers are what manage access to zerotier networks. It's a completely separate function from a moon. Self hosting a network controller does not require you to set up moons whatsoever, either.

Once a direct Peer to Peer path is established between instances of ZeroTier, all communication between them is done directly. Not through a moon, or root, and definitely not through a network controller.

- Self hosting Zerotier

Ejemplo: VPN Site-to-Site con GNS3



- [Tutorial GNS3](#)

Configuración RouterOS

Asignar IP a interfaz `ether1`

```
ip address add address=10.0.0.101/24 interface=ether1
```

Comprobación

```
ip address print
```