




# Mi Red de Gestión ideal

**ESnog 28**

Carlos Fraga

- 
- Consideraciones iniciales
  - Usos de la red de Gestión
  - Planos de control
  - Tipos de Gestión
    - a. En Banda
    - b. Fuera de banda - Puerto MGMT
    - c. Fuera de banda - Consola
      - i. Hardware que podemos usar
  - Conclusiones finales
  - Preguntas

# Consideraciones Iniciales

- La red de gestión o MGMT es la gran olvidada, y un accidente para algunos.
- Cada uno es soberano de hacer las cosas como quiera en su red o como le dejen.
- La “**capa 0 = Dinero**” del modelo TCP/IP o OSI siempre es importante. En este caso al no tratarse de la red de producción, su justificación puede resultar difícil.





# Usos de la red de Gestión o MGMT

1. Monitorización de los equipos que tenemos en la red (Ping, SNMP, Telemetría)
2. NTP, Syslog, Netflow, ...
3. Provisionar/des-provisionar servicios sobre la red de producción
4. Facturación (antiguas centrales de voz con X25)
5. Actualización firmware: funcionalidades/bugs en los equipos de red.
6. Entorno Centralizado, acotado y controlado para el acceso de determinados usuarios (mediante “Máquinas de salto” deben ser capaces de llegar a cualquier sistema en la red de Gestión)
7. Poder acceder al equipo: Poder ver y arreglar cosas, cuando se estropean 🤖



# “Planos”

- **Management Plane** → Configuración y Comandos que usamos para tener el “control” y la monitorización de los equipos.
- **Control Plane** → Dispone de la información del enrutamiento
- **Forwarding Plane** → Donde el tráfico conmuta
- **Customer Data-Plane** → Esto lo dejamos para otro ESnog



# Tipos de Gestión

1. En banda
2. Fuera banda
  - 2.1 Fuera banda - Puerto MGMT
  - 2.2 Fuera banda - Puerto Consola



# En banda

Cuando Red de Gestión está dentro de la red de Producción

```
interface Loopback101
  description --- interface Lo MGMT ---
  ip address 20.20.20.20/32
!
vlan 101
  name MGMT
!
vrf definition MGMT
  rd 64512:1
!
interface Management1
  shutdown
!
interface Vlan101
  vrf forwarding MGMT
  ip address 10.10.10.10/20
```

Hay casos que es la única solución:

- Nodo aislado
- No se disponen de canales ópticos libres o circuitos adicionales entre datacenters
- Falta de equipamiento dedicado
- Otros ....

# En banda

## Problemas:

- Única vía de acceso al equipamiento de red
- Cuando se “cae el enlace”, perdemos la gestión.
- Consumo elevado de ancho de banda del enlace: saturación (muchos usuarios concurrentes, DDoS,...)

## Recomendaciones:

- VRF separadas
- RFC 4594 - Guidelines for Diffserv Service Class
- Vigilar el “redistribute connected”
- Poner velas a una entidad superior 🕯️ 🕯️

Application Class	Per-Hop Behavior	Queuing & Dropping	Application Examples
VoIP Telephony	EF	Priority Queue (PQ)	Cisco IP Phones (G.711, G.729)
Broadcast Video	CS5	(Optional) PQ	Cisco IP Video Surveillance / Cisco Enterprise TV
Real-Time Interactive	CS4	(Optional) PQ	Cisco TelePresence
Multimedia Conferencing	AF4	BW Queue + DSCP WRED	Cisco Jabber, Cisco WebEx
Multimedia Streaming	AF3	BW Queue + DSCP WRED	Cisco Digital Media System (VoDs)
Network Control	CS6	BW Queue	EIGRP, OSPF, BGP, HSRP, IKE
Signaling	CS3	BW Queue	SCCP, SIP, H.323
Ops / Admin / Mgmt (OAM)	CS2	BW Queue	SNMP, SSH, Syslog
Transactional Data	AF2	BW Queue + DSCP WRED	ERP Apps, CRM Apps, Database Apps
Bulk Data	AF1	BW Queue + DSCP WRED	E-mail, FTP, Backup Apps, Content Distribution





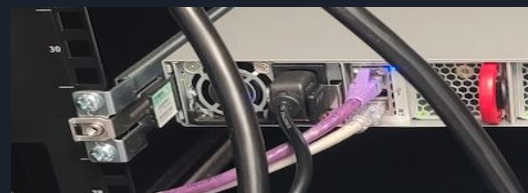
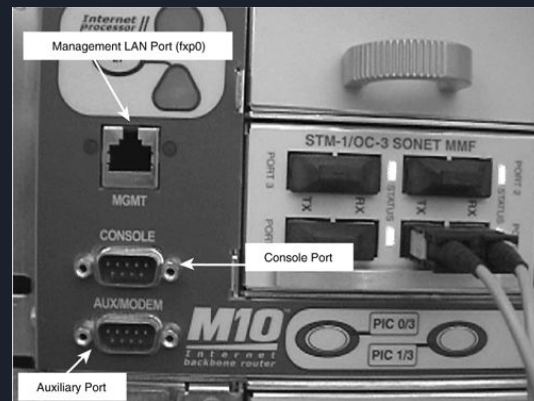
## Fuera de Banda - Puerto MGMT

- Puerto dedicado en los equipos para gestión out-of-band network.
- La gestión del equipo opera en el management plane separado del data plane.
- Es más seguro y resiliente que hacerlo “en banda” (pudiendo funcionar durante congestión del tráfico, device glitch, ..)
- Permite una conexión IP a una red “paralela” a la de producción.

# Puerto MGMT

Características del puerto MGMT:

PARAMETRO	MANAGEMENT PORT
Caso del usos	MGMT In-band y acceso remoto
Direccionamiento IP	Direccion IP configurable
Communication Type	Synchronous
Acceso remoto	SI (Telnet - SSH - HTTP/S)
Separación tráfico	Basado en VRF
Velocidad maxima	1 Gbps
Tipo Connectividad	RJ45
Tipo Management	Our of Band
SNMP, Logging on interface	Configurable
Control de accesos	SI (access-list)



```
interface Management0
vrf MGMT
ip address 10.10.10.10/20
```

# Puerto MGMT: IPv6 everywhere

Antes que alguien lo pregunte:

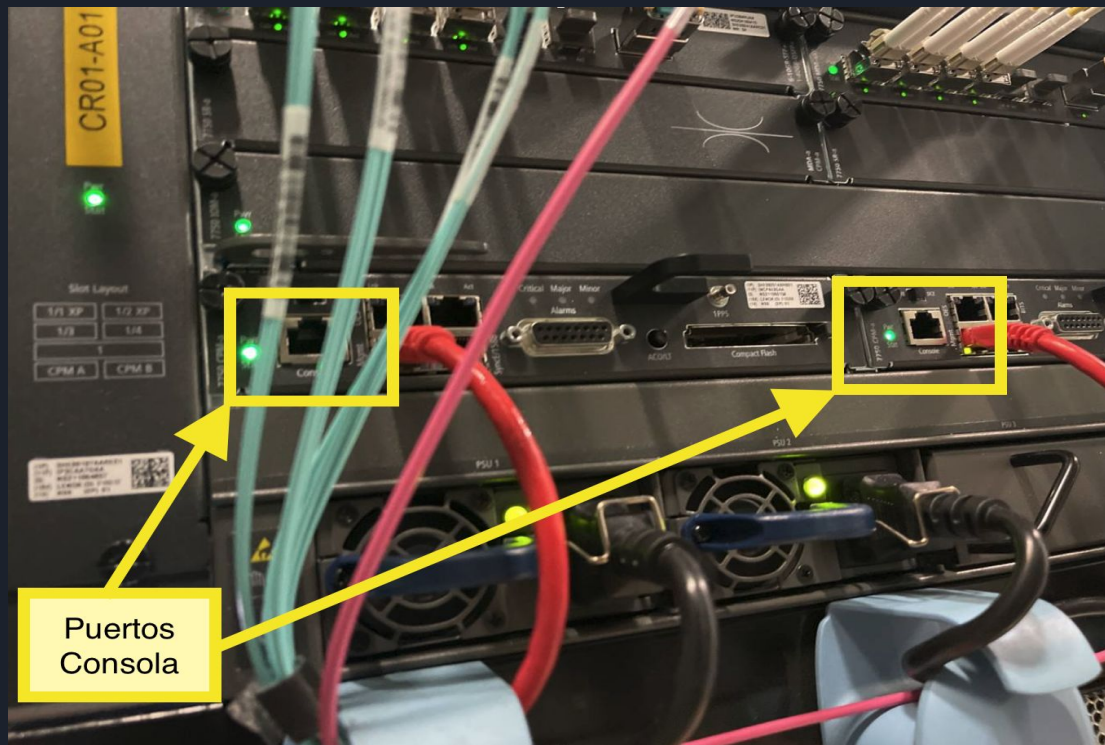
- Los puertos de MGMT admiten IPv6



```
cr01-lab1(s1)(config-if-Ma0)#ipv6 address ?  
A:B:C:D:E:F:G:H   IPv6 address  
A:B:C:D:E:F:G:H/I IPv6 prefix  
auto-config       Use SLAAC to automatically configure the IPv6 address
```

- Nos quedamos sin excusas para no implementar IPv6 😊

# Paseando por los datacenters...





# Acceso por Consola

Características del puerto MGMT:

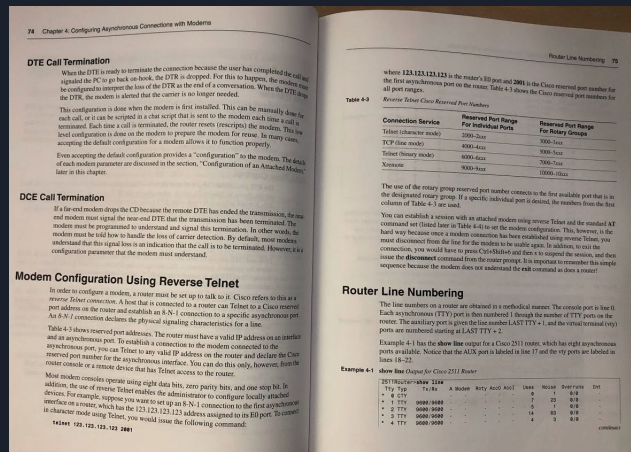
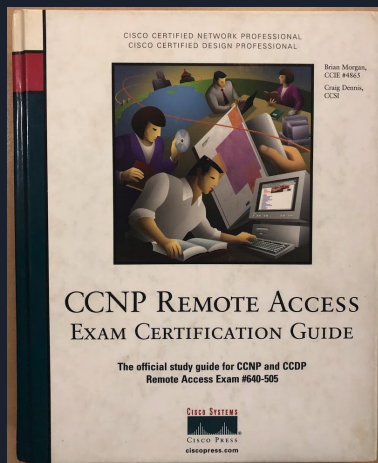
PARAMETRO	PUERTO CONSOLA
Direccionamiento IP	N/A
Tipo Comunicación	Asincrónica
Acceso Remoto (Telnet/SSH)	No
Tipo Acceso	Acceso físico al dispositivo
Separación tráfico	Conexión física totalmente independiente
Velocidad máxima	0.1 Mbps (115200 bps)
Tipo Conectividad	Serial , DB9, DB25 , RJ45
Tipo Gestión	Fuera de Banda
Boot Sequence	Enseña todo el Boot sequence

Ventajas:

- Vemos el proceso completo de reboot, podemos parar en arranque y interactuar. Famoso ROMON de Cisco.....
- Es como estuviésemos delante del equipo configurandolo en el datacenter, pero en nuestra oficina o casa.
- Existen diferentes alternativas hardware para el acceso a la consola remotamente.

# Cisco (2511, NM-16A/32A, HWIC-16A)

Solución basada en los puertos async (TTY) y reverse Telnet de Cisco para la configuración de modem



# Cisco (2511, NM-16A/32A, HWIC-16A)

Parte router



Parte patch panel



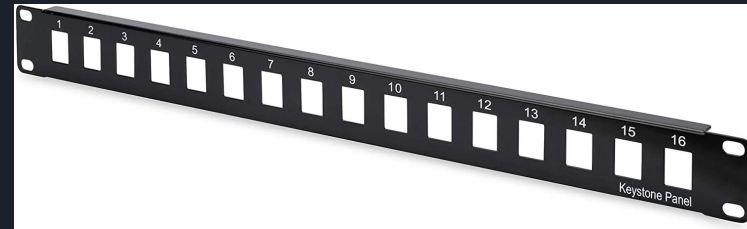
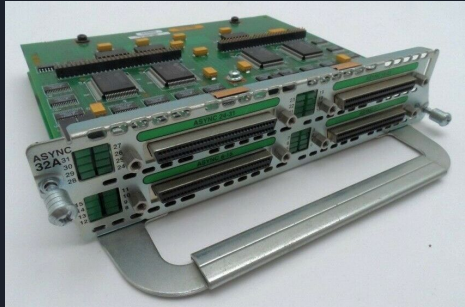
## Materiales:

- Cisco 2511 (ó ISR, SSH mejor)
- NM-16A/32A
- 2xCable Octal Async
- Patch Panel 16 Puertos Keystone
- Adaptadores RJ45 Keystone (utp cat5e)
- UTP cat5e azules == consola



# Cisco (2511, NM-16A/32A, HWIC-16A)

Imágenes de la lista de la compra:





## Configure Terminal Server through Menu Options

Cisco URL: <https://bit.ly/3OtKvtt>

```
interface Loopback0
 ip address 100.100.100.100 255.255.255.255

ip host PUERTO_2066 2066 100.100.100.100
ip host PUERTO_2067 2067 100.100.100.100

menu consolas text 0 salir a RT-00B-ESNOG-28
menu consolas command 0 menu-exit

menu consolas text l<no> Limpia la sesion por numero (p.ejemplo): l5

menu consolas text 1 FREE: PUERTO_2066
menu consolas command 1 resume PUERTO_2066 /connect telnet PUERTO_2066
menu consolas text 2 FREE: PUERTO_2067
menu consolas command 2 resume PUERTO_2067 /connect telnet PUERTO_2067

menu consolas command l1 clear line tty 66
menu consolas command l2 clear line tty 67

menu consolas clear-screen
menu consolas status-line
menu consolas default 20
menu consolas line-mode

line 1/0 1/15
exec-timeout 30 0
logging synchronous
no exec
transport input all
transport output all
stopbits 1

line vty 0 4
autocmd menu consolas
```

```
rt-oob-ESNOG-28#sh line
  Tty Line Typ Tx/Rx A Modem
    0 0 CTY - -
    1 1 AUX 9600/9600 - -
  1/0 66 TTY 115200/115200 - -
  1/1 67 TTY 9600/9600 - -
  1/2 68 TTY 9600/9600 - -
  1/3 69 TTY 9600/9600 - -
  1/4 70 TTY 9600/9600 - -
  1/5 71 TTY 9600/9600 - -
  1/6 72 TTY 9600/9600 - -
  1/7 73 TTY 9600/9600 - -
  1/8 74 TTY 9600/9600 - -
  1/9 75 TTY 9600/9600 - -
 1/10 76 TTY 9600/9600 - -
 1/11 77 TTY 9600/9600 - -
 1/12 78 TTY 9600/9600 - -
 1/13 79 TTY 9600/9600 - -
 1/14 80 TTY 9600/9600 - -
 1/15 81 TTY 9600/9600 - -
```

Server "rt-oob-ESNOG-28" Line 517 Terminal-type xterm-256color C

Bienvenido al servidor de consolas -- ESN0G-28

NODO: ESN0G-28

DATACENTER: UPC

LOCATION: Edificio Vertex (6 Placa d'Eusebi Guell, 08034 Barcelona)

```
0 salir a RT-00B-ESNOG-28
l<no> Limpia la sesion por numero (p.ejemplo): l5
1 FREE: PUERTO_2066
2 FREE: PUERTO_2067
3 FREE: PUERTO_2068
4 FREE: PUERTO_2069
5 FREE: PUERTO_2070
6 FREE: PUERTO_2071
7 FREE: PUERTO_2072
8 FREE: PUERTO_2073
9 FREE: PUERTO_2076
10 FREE: PUERTO_2075
11 FREE: PUERTO_2076
12 FREE: PUERTO_2077
13 FREE: PUERTO_2078
14 FREE: PUERTO_2079
15 FREE: PUERTO_2080
16 FREE: PUERTO_2081
```

CCTeclee un numero para seleccionar una opcion:

# Opengear



- Antigua Cyclades/Digi. Otras marcas pueden ser: Perle, Lantronix...
- Apariencia de switch con múltiples RJ45 pero son puertos RS232 🤪
- Facilidad de instalación en 1U y cableado
- Facilidad gestión remota (https, ssh)
- Linux = Shell script, Ansible playbook, Python, ....



System Name: con01.ord1.us. Model: CM7148-2-DAC Firmware: 4.6.0  
Uptime: 160 days, 15 hours, 32 mins, 36 secs Current User:



Manage: Devices

Managed Devices						Serial
Port #	Label	Connector	Status	Signals	Actions	
1	Port 1	RJ45	No Active Users	Signals: RTS   DTR		
2	vpn01.ord1.us	RJ45	No Active Users	Signals: RTS   CTS   DTR   DCD	Connect: <a href="#">via SSH</a>   <a href="#">via Web Terminal</a>	
3	cr01.ord1.us	RJ45	No Active Users	Signals: RTS   CTS   DTR	Connect: <a href="#">via SSH</a>   <a href="#">via Web Terminal</a>	
4	mgmt-ii94.ord1.us	RJ45	No Active Users	Signals: RTS   CTS   DTR	Connect: <a href="#">via SSH</a>   <a href="#">via Web Terminal</a>	
5	otn01b.ord1.us	RJ45	No Active Users	Signals: RTS   DTR	Connect: <a href="#">via SSH</a>   <a href="#">via Web Terminal</a>	
6	otn03a.ord1.us	RJ45	No Active Users	Signals: RTS   DTR	Connect: <a href="#">via SSH</a>   <a href="#">via Web Terminal</a>	
7	Port 7	RJ45	No Active Users	Signals: RTS   DTR		
8	cr02.ord1.us	RJ45	No Active Users	Signals: RTS   CTS   DTR	Connect: <a href="#">via SSH</a>   <a href="#">via Web Terminal</a>	
9	mgmt-ih94.ord1.us	RJ45	No Active Users	Signals: RTS   CTS   DTR	Connect: <a href="#">via SSH</a>   <a href="#">via Web Terminal</a>	

```
$ uname -a
Linux con01.ord1.us. 3.10.0-uc0 #1 Tue Aug 6 02:58:14 UTC 2019 armv7l unknown
```

```
$ pmshell
```

```
2: vpn01.ord1.us      3: cr01.ord1.us      4: mgmt-ii94.ord1.us  5: otn01b.ord1.us
6: otn03a.ord1.us     8: cr02.ord1.us     9: mgmt-ih94.ord1.us 11: otn03b.ord1.us
13: mr02.ord1         14: otn01c.ord1.us  17: tor-ii94.ord1.us 18: tor-ih94.ord1.us
19: ar01.ord1.us      20: fw01.ord1.us    21: ar02.ord1.us     22: fw02.ord1.us
23: mr01.ord1.us
```

```
Connect to port >
```

# Dispositivos 3G



BLACK BOX®						
System Name: ACSdoc Model: LES1215A Firmware: 2.6.0u2 Uptime: 0 days, 0 hours, 52 mins, 27 secs Current User: root Backup Log Out						
Serial & Network: Serial Port						
Serial & Network						
Serial Port Users & Groups Authentication Network Hosts Trusted Networks Cascaded Ports UPS Connections RPC Connections Environmental						
Ports 1-8 Ports 9-16						
Port #	Label	Mode	Logging Level	Parameters	Flow Control	
1	Port 1	Console (Unconfigured)	0	9600-S-N-1	None	Edit
2	Port 2	Console (Unconfigured)	0	9600-S-N-1	None	Edit
3	Port 3	Console (Unconfigured)	0	9600-S-N-1	None	Edit

- Cisco ISR lite → <https://bit.ly/3P96cU9>
- Conexión 3G
- Solución para entornos remotos
- Dependemos de la cobertura
- Solución “no barata”

# RaspOOB (DIY)

## Premisas:

- Quien no tiene alguna raspberry Pi o derivados Pi en el cajón ?
- Quien no tiene cables de consola en la maleta ? (Azul: cisco - Juniper: Gris)
- Quien no tiene alguna cosa más de utilidad tirada en el cajón ?



# RaspOOB - Conexión consola

```
pi@raspoob-esnog28:~$ dmesg | grep tty | grep USB
[ 322.024109] usb 1-1.5: pl2303 converter now attached to ttyUSB0
```

```
define: &banner \r\nser2net port \p device \d [\B] (SERVIDOR DE CONSOLAS ESN0G-28)\r\n\r\n
connection: &con0096
  acceptor: tcp,2000
  enable: on
  options:
    banner: *banner
    kickolduser: true
    telnet-brk-on-sync: true
  connector: serialdev,
             /dev/ttyUSB0,
             9600n81,local
```

/etc/ser2net.yaml

```
pi@raspoob-esnog28:~$ telnet localhost 2000
Trying ::1...
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.

ser2net port tcp,2000 device serialdev, /dev/ttyUSB0, 9600n81,local [] (SERVIDOR DE CONSOLAS ESN0G-28)

RT-00B-ESN0G-28>
RT-00B-ESN0G-28>|
```

- RaspberryPi
- Bateria externa
- Cable USB-RS232 (DB-9)
- Cable RS232-RJ45 (consola)





### Conexiones puerto Serie:

- ser2net (<https://github.com/cminyard/ser2net>)
- minicom (<https://es.wikipedia.org/wiki/Minicom>)

### Conexión 3G:

- sakis3g.gz
- wvdial

### Securización VPN - lado cliente, que se conecte a un “jump server”

- Wireward
- Openvpn

IP → DNS (en el caso de no disponer IP “pública fija”) [rasspoob28.esnog.land]

- NOIP.com (<https://www.noip.com/>)
- Cloudflare (<https://github.com/K0p1-Git/cloudflare-ddns-updater>)

### Servidor FTP, docker

Mejora → 3G/Wi-Fi Integradas en placa.

Mejora → Pantalla táctil para el ingeniero de campo.



## **Conclusiones (cosas que yo tendría en cuenta)**



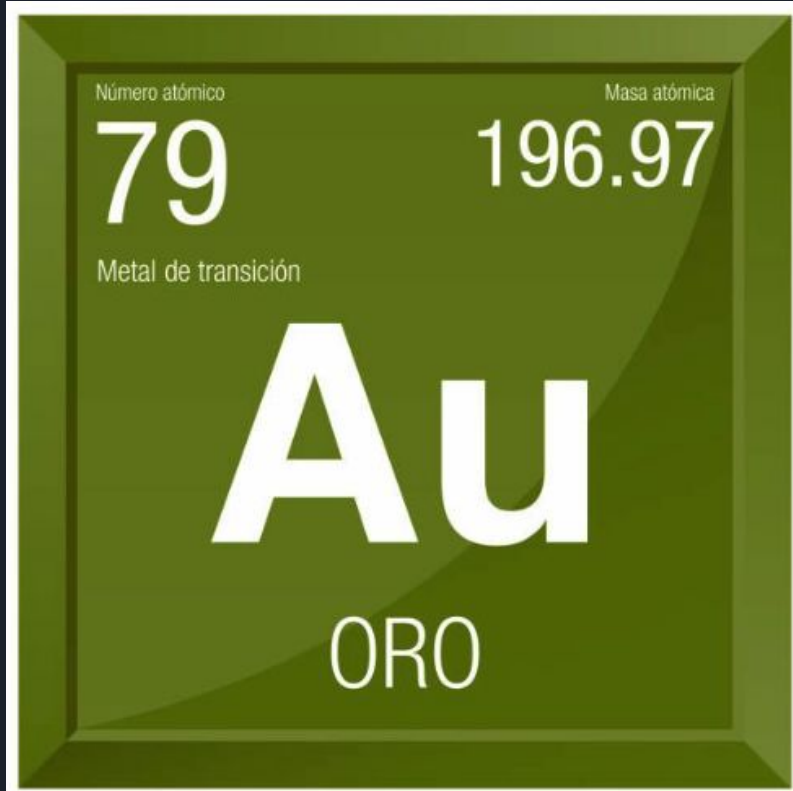
# Acceso Out of Band

## Consideraciones:

- Acceso a independiente a la red.
- Tiene que ser **SEGURO y ROBUSTO !!!!**
- Solución **estándar**
- **No debe ser una solución cara y costosa** de mantener: hay cientos de soluciones (caseras, IoT, vendors dedicados, 2ª mano,....)
- **Descripciones actualizadas** de todos los equipos.
- **FUNCIONAR CORRECTAMENTE** bajo demanda en momentos de crisis (sudor frío del networker) → INTRO ..... (“escogí un mal día para apretar intro”).



El acceso externo a la red en caso de fallo total mediante un proveedor externo es:



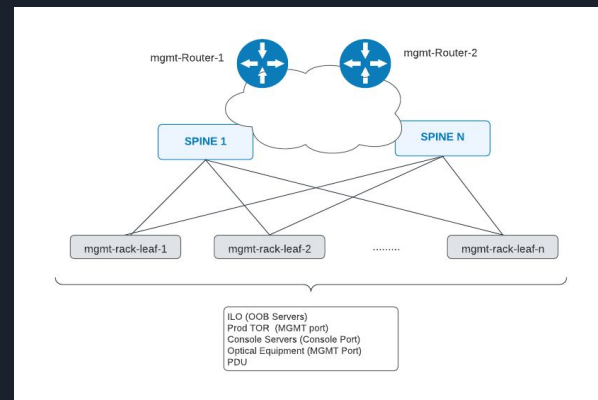


# Acceso a la OOB

- Contratarle a nuestro peor enemigo un acceso (ese que nunca falla según sabiduría popular)
- Algunos TIER-1 con IP Pública directamente. (IPv6 algún día)
- 3G/4G/5G/6G (algún día espero que nos den IPv6 en el móvil)
- Wi-Fi en Datacenter ? 🤔
- Algunos datacenters (Bitnap, ....) pueden ofrecernos enlaces de baja capacidad, con IP Pública dedicada. Puede ser en IPv6 😊
- Como el ESnog es una comunidad genial. Podemos ir reservando un /48 en IPv6 para darnos servicios de acceso OOB los unos a los otros ?
- Es importante incluirlo en los planes de seguridad y en check-list de mantenimiento

# Gestión de datacenters

- CLOS Topology con una red separada:
  - MGMT
  - Producción
- 2 switches por Rack:
  - ToR MGMT
  - ToR Producción
- MGMT switch basado en RJ45, con uplinks de fibra
- MGMT ToR (ILO, iDrac de servidores, MGMT Port ToR producción, Tiras Eléctricas,...)
- Esta red ha de ser paralela a la de producción
- Estarán todos los sistemas de monitorización y serán accesibles, con direccionamiento de la red de MGMT
- Mi premisa → “Keep it simple”, pero cada uno es soberano en su red





# Conexión entre Datacenters

- Solemos tener varios PoPs , Datacenters, nodos, .....
  - Un canal óptico si tenemos fibra oscura y la unión se hace mediante DWDM
  - Una fibra oscura dedicada (SFP+ 10G bidi)
  - VRF
  - IP Pública (1 o varias) con otros proveedores que no sean los mismos de tránsito en ese nodo
- IPsec nos puede ayudar (Full-mesh con Firewalls) , GRE tunnels, .....
- Lo importante es asegurar la conexión permanente en la red de gestión



## Otras consideraciones

- Los servidores de los clouds son tus amigos !!!!!
  - servidores de salto, concentradores de VPN, sistemas de monitorización simples alternativos a tu red interna, .....
- Dominio alternativo al utilizado en la empresa que sea fácil de recordar
  - esnog.**land**

Servidores Auth DNS de MGMT deberán estar fuera de la red de MGMT



**Preguntas ?**