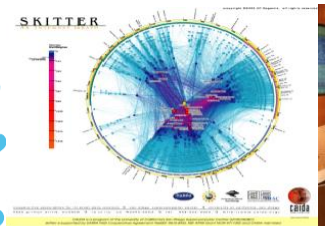
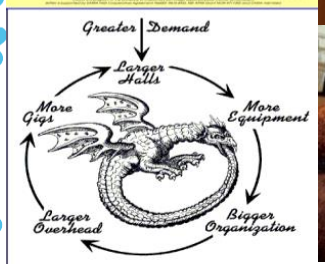
# Cómo responder a un ataque DDOS (edición para proveedores de servicios)



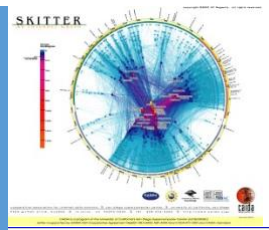

# Esquema

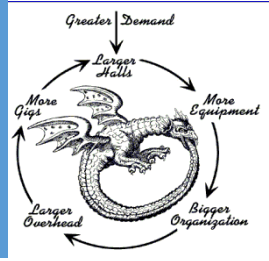
- Principios básicos para combatir un ataque DoS
- Puesta en marcha de las herramientas - Ataque DDOS

# Larga historia - Formación en línea

- NANOG 23 - Seguridad ISP - Técnicas del mundo real II - por Barry Raveendran Greene, Cisco Systems; Chris Morrow, UUNET/Verizon; Brian W. Gemberling, UUNET
- NANOG 25 - Actualización de seguridad de BGP - por Barry Raveendran Greene, Cisco Systems
- NANOG 26 - Seguridad de los ISP - Técnicas del mundo real - por Barry Raveendran Greene, Cisco Systems; Kevin Houle, CERT
- NANOG 28 - Seguridad de los ISP: Despliegue y uso de Sinkholes por Barry Raveendren Greene, Cisco Systems; Danny McPherson, Arbor Networks
- NANOG 36 - ISP Security 101 Primer por Barry Greene, Cisco Systems y Roland Dobbins, Cisco Systems
- NANOG 47 - Las diez principales técnicas de seguridad de NSP-SEC por Barry Greene, Juniper Networks
- NANOG 54 - Kit de herramientas de "seguridad" para proveedores de servicios por Barry Greene, ISC (Parte 1) y (Parte 2)
- **MAAWG 26 - Taller sobre seguridad de las PE**
- Taller CommunicAsia 2015

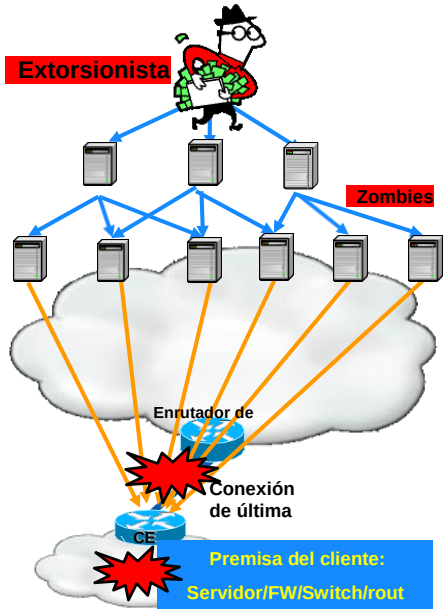
# Principios básicos para combatir un ataque DoS




# ¿Cómo se detiene realmente un ataque DDOS?

- Clean Pipes, Scrubbing Centers y otras herramientas "Anti-DDOS" *no detienen los ataques DDOS*.
- Estas herramientas son fundamentales, pero sólo deben utilizarse para proporcionar:
  - ✓ Restauración completa del servicio para determinados servicios de misión crítica
  - ✓ Hora de remediar el ataque DDOS




- Detener un ataque DDOS requiere la capacidad de hacer:

1. Resistir el ataque y no ceder a la extorsión/amenaza
2. Visibilidad/retorno a las fuentes del ataque
3. Remediar las herramientas utilizadas en el ataque (BOTNETs y Reflectores)
4. Rastreo hasta el C&C utilizado para dirigir el ataque.
5. Triangulación de la persona o personas que lanzan el ataque.

# Essential Principio de resistencia Essential al DoS

***Construir una infraestructura segura para servicios rentables***

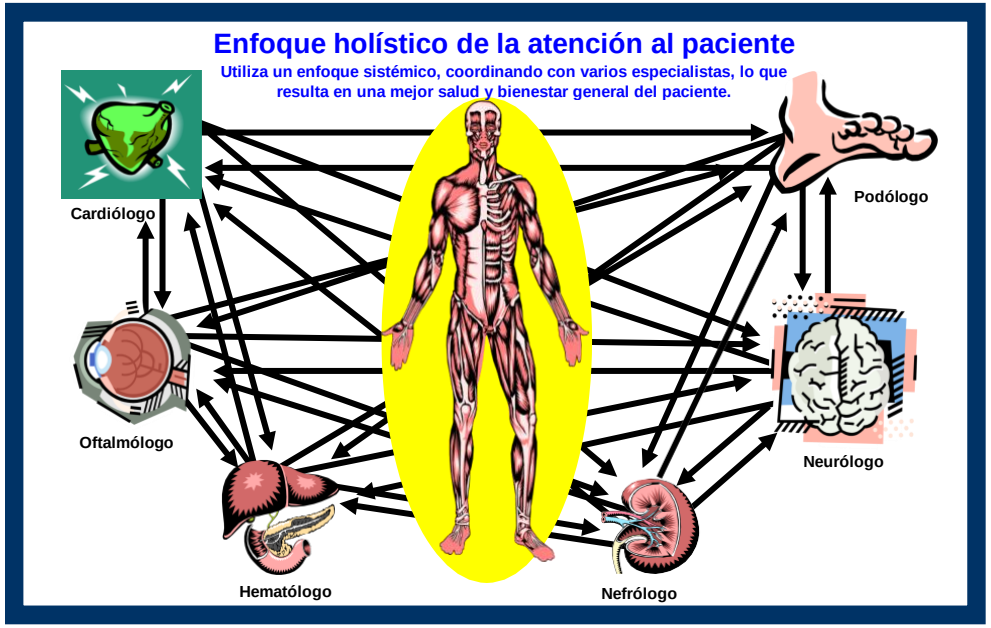
**Control total de todo el tráfico en la red.**

**Máxima disponibilidad de todos los servicios.**

**Visibilidad total en todos los aspectos de la red.**

# ¿Qué significa la visibilidad?

- La visibilidad es un elemento fundamental de la industria de las telecomunicaciones.
- Necesita saber todo lo que hacen sus clientes, qué aplicaciones impulsan su red y comprender la dirección que toma su negocio.
- LA MAYORÍA DE LAS EMPRESAS DE TELECOMUNICACIONES ACTUALES NO HACEN ESTO CON TCP/IP!

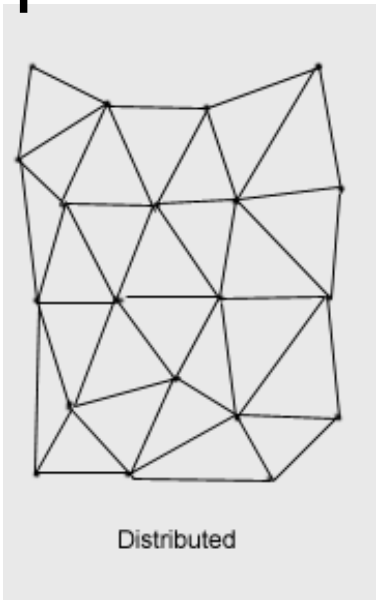


# ¿Qué does Control significa?

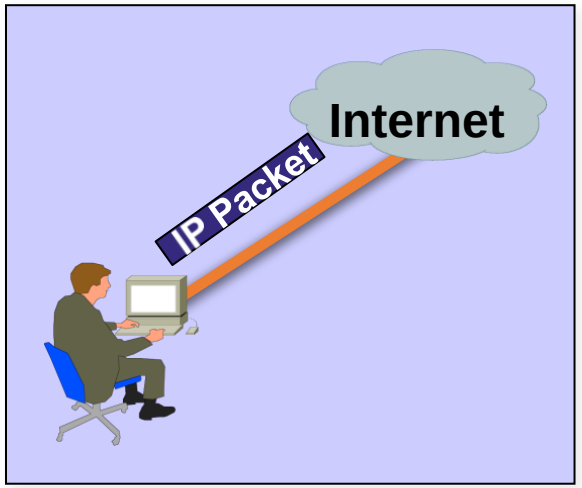
1. **Necesita saber exactamente lo que ocurre con sus clientes y su red.**
2. **Tiene que ser capaz de dar forma, manipular y servir a sus clientes basándose en ese conocimiento.**
3. **Necesitas que tu red se mantenga más allá de *cinco 9s***

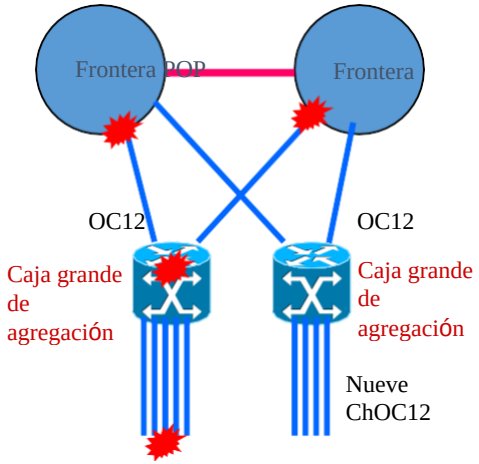
# ¿Qué significa disponibilidad?

- La red debe funcionar al 99,999%.
- Lo hacemos con el modelo de disponibilidad y resistencia de Paul Baran.
- Problema: La mayoría de los ingenieros de IP no conocen los principios del modelo de disponibilidad y resistencia de Paul Baran.



# Se all  trata del paquete  ……..

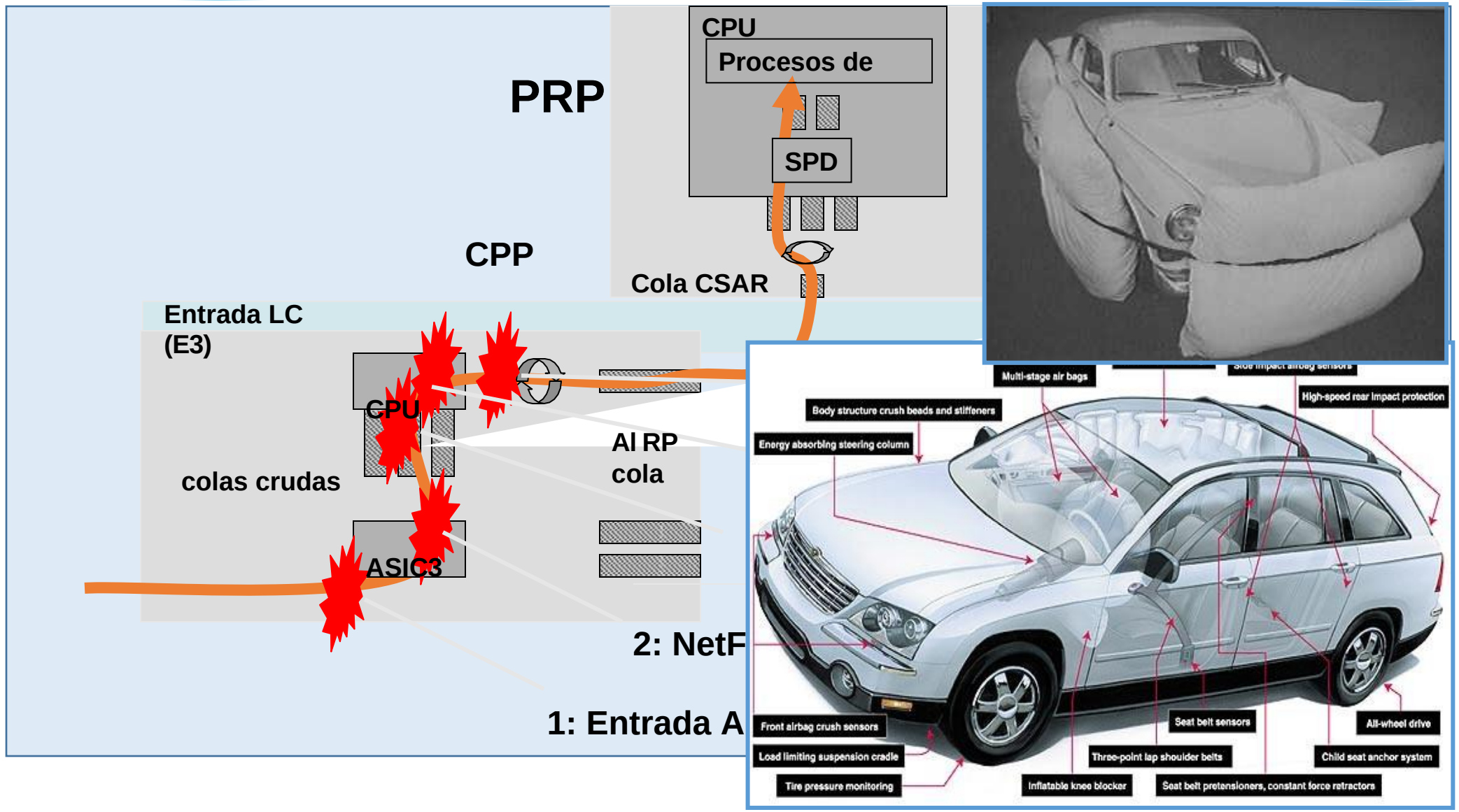


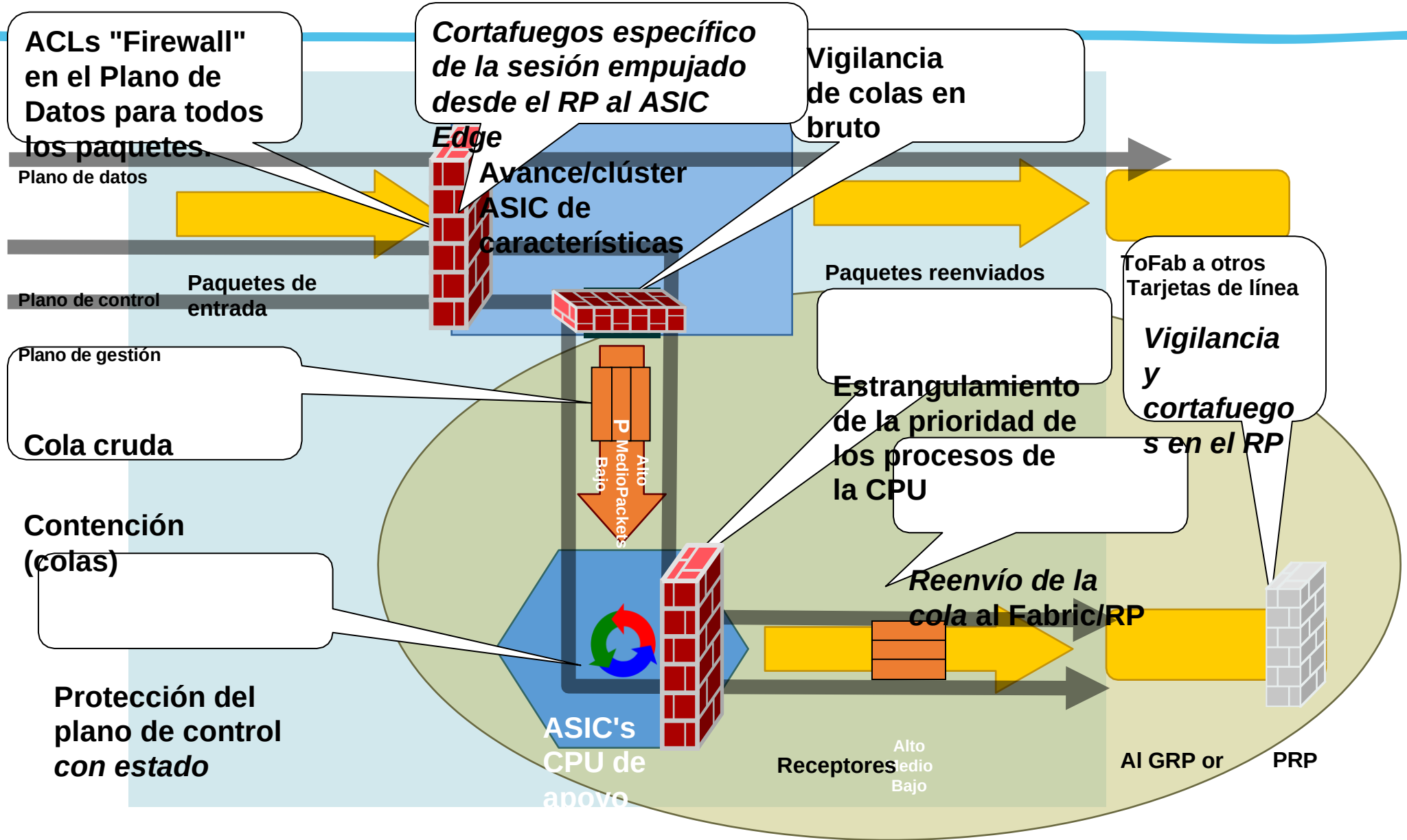

- **Se trata del paquete .....**
- **Una vez que un paquete entra en Internet, alguien, en algún lugar, tiene que hacer una de estas dos cosas:**
  - ***Entregar el paquete***
  - ***Suelte el paquete***
- **En el contexto de los ataques DoS, las preguntas son: *¿quién* y *dónde* se producirá la acción de "soltar el paquete"?**

# El *conjunto de herramientas de* seguridad del operador - *Utilizar todo*

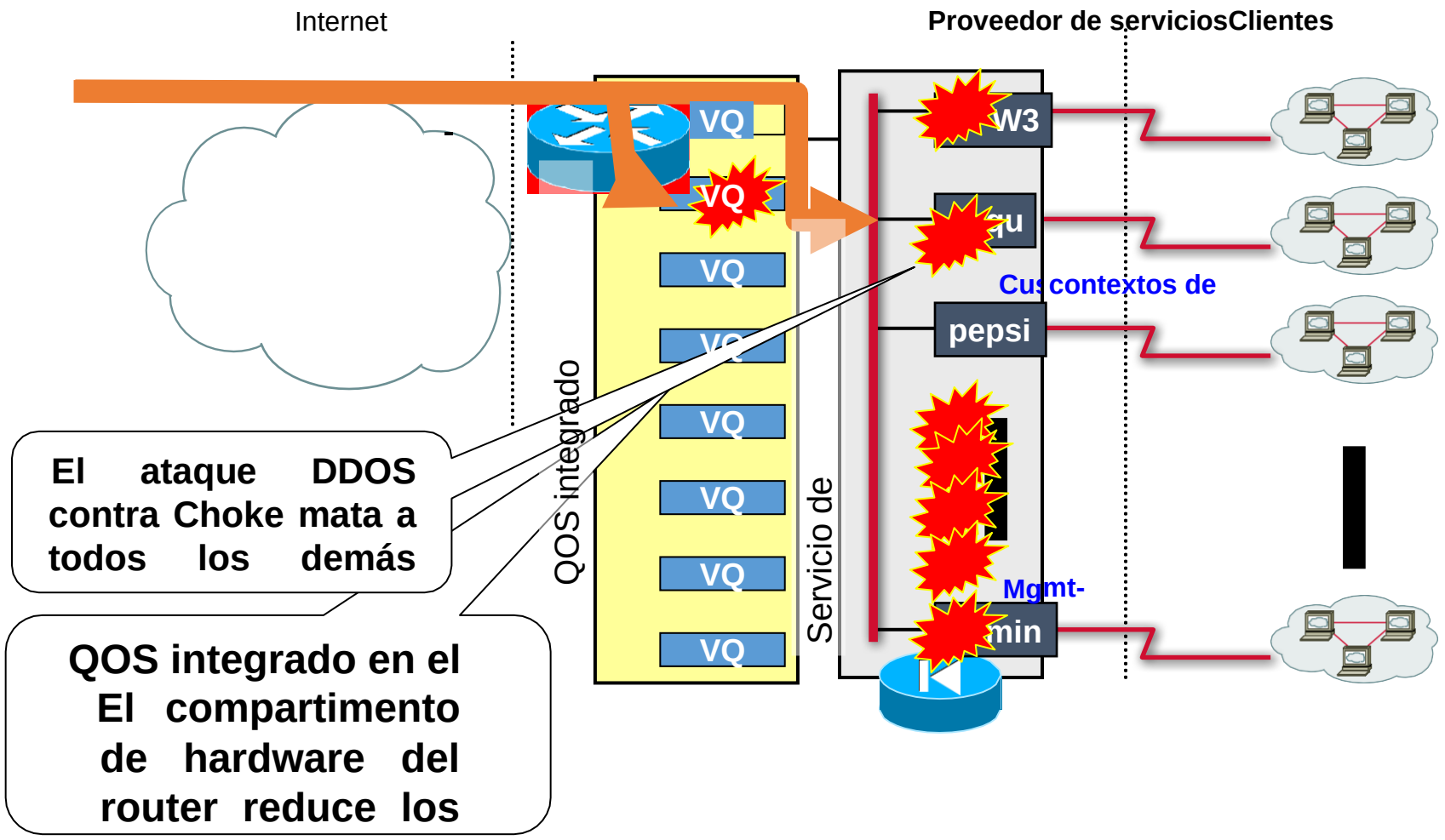
# La seguridad no puede ser algo secundario



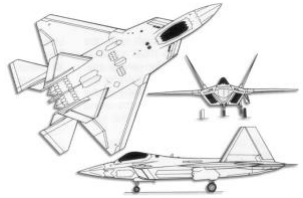
# ¿Qué puede hacer para protegerse dentro de un router?



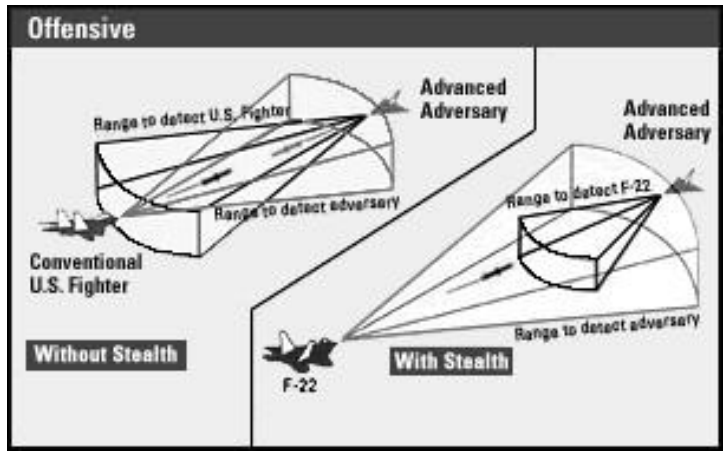
# ¿Arrojando hardware al problema?

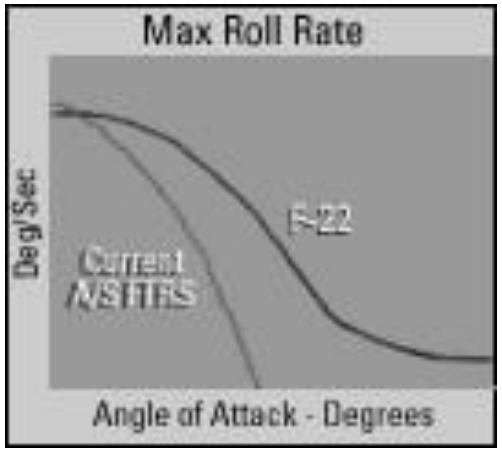


# ¿Explota usted los límites?

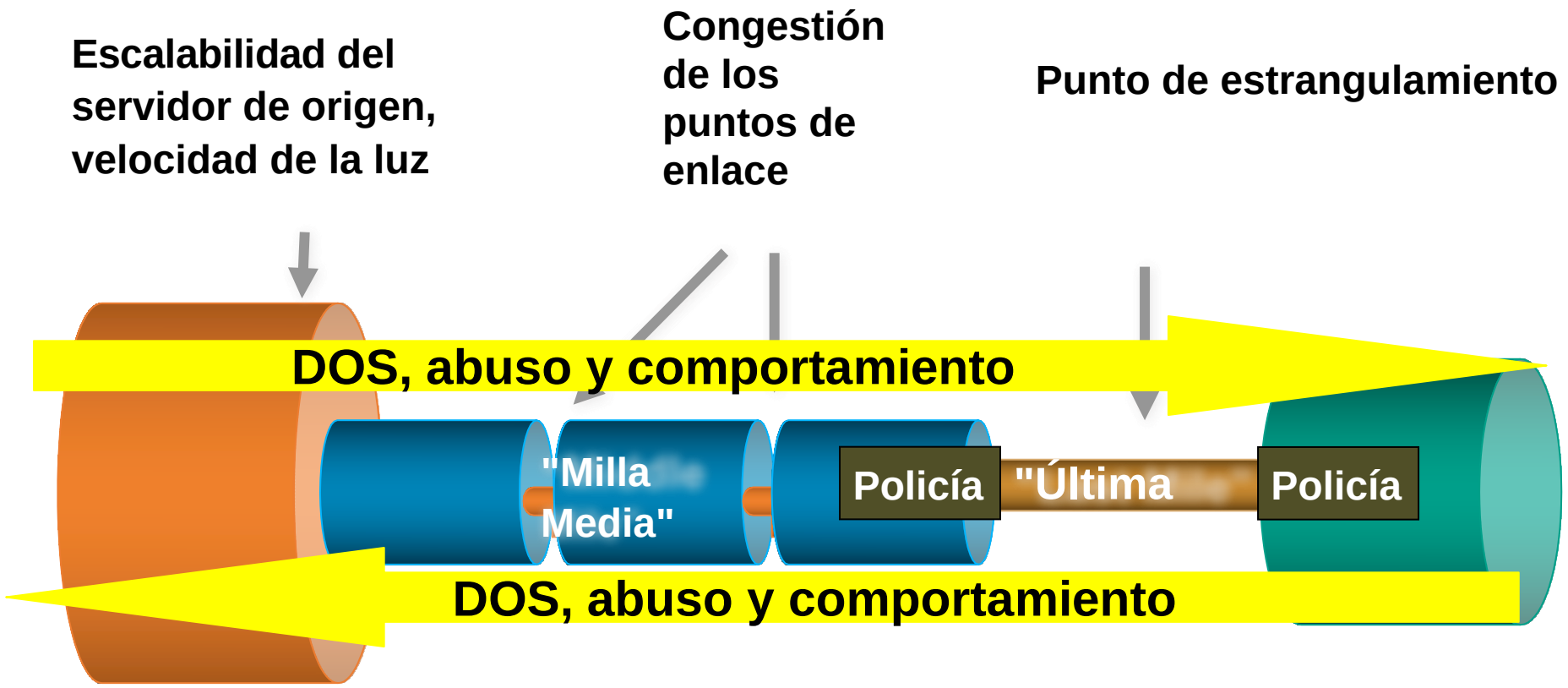


- Conozca su equipo e infraestructura:
  - Conozca el rendimiento de todos sus equipos (routers, switches, estaciones de trabajo, etc.). Tiene que saber lo que su equipo es realmente capaz de hacer. Si no puede hacerlo por sí mismo, es un requisito de compra.
  - Conozca las capacidades de su red. Si es posible, pruébela. Las sorpresas no son agradables durante un incidente de seguridad.

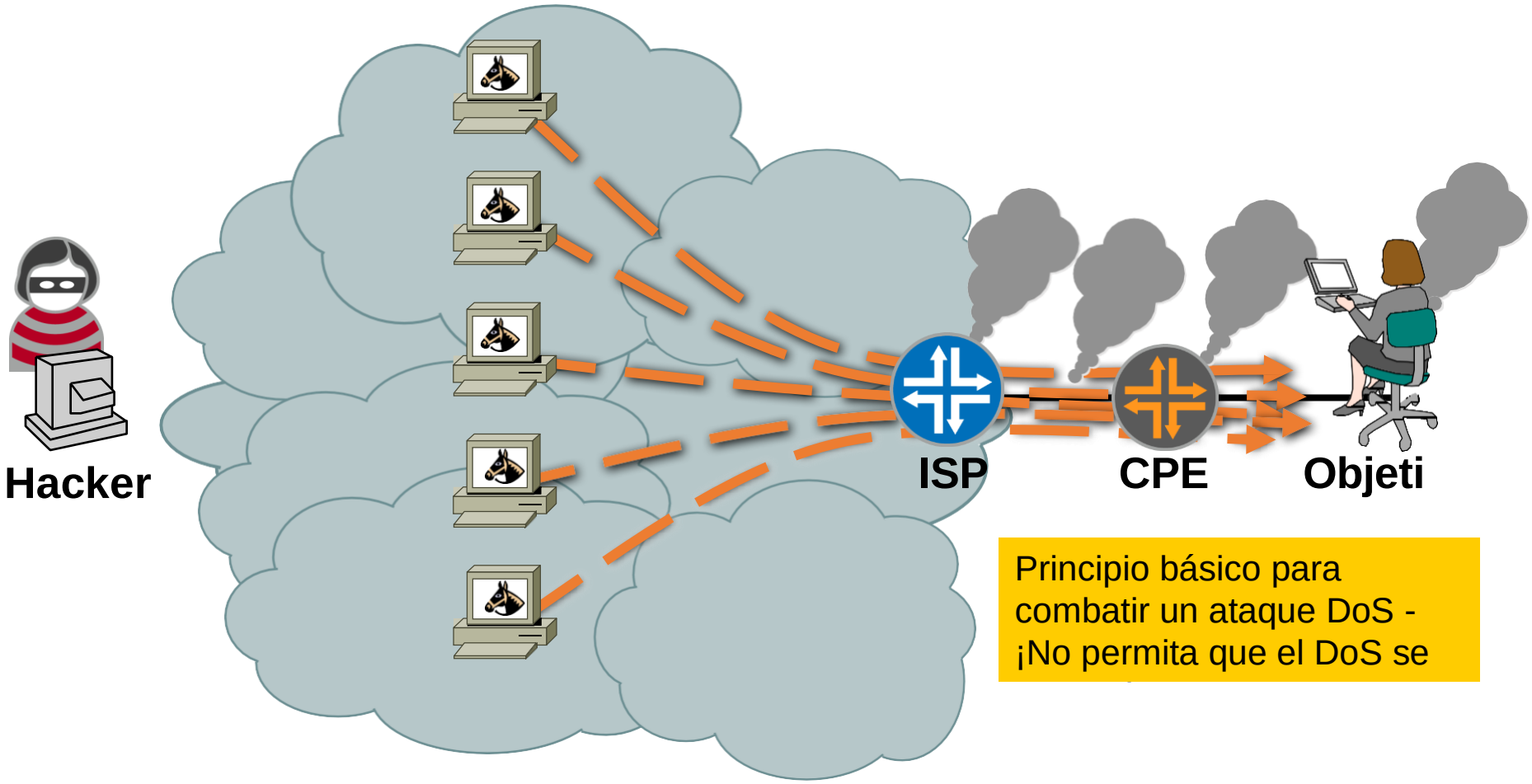



# Puntos de estrangulamiento = Collateral Daño

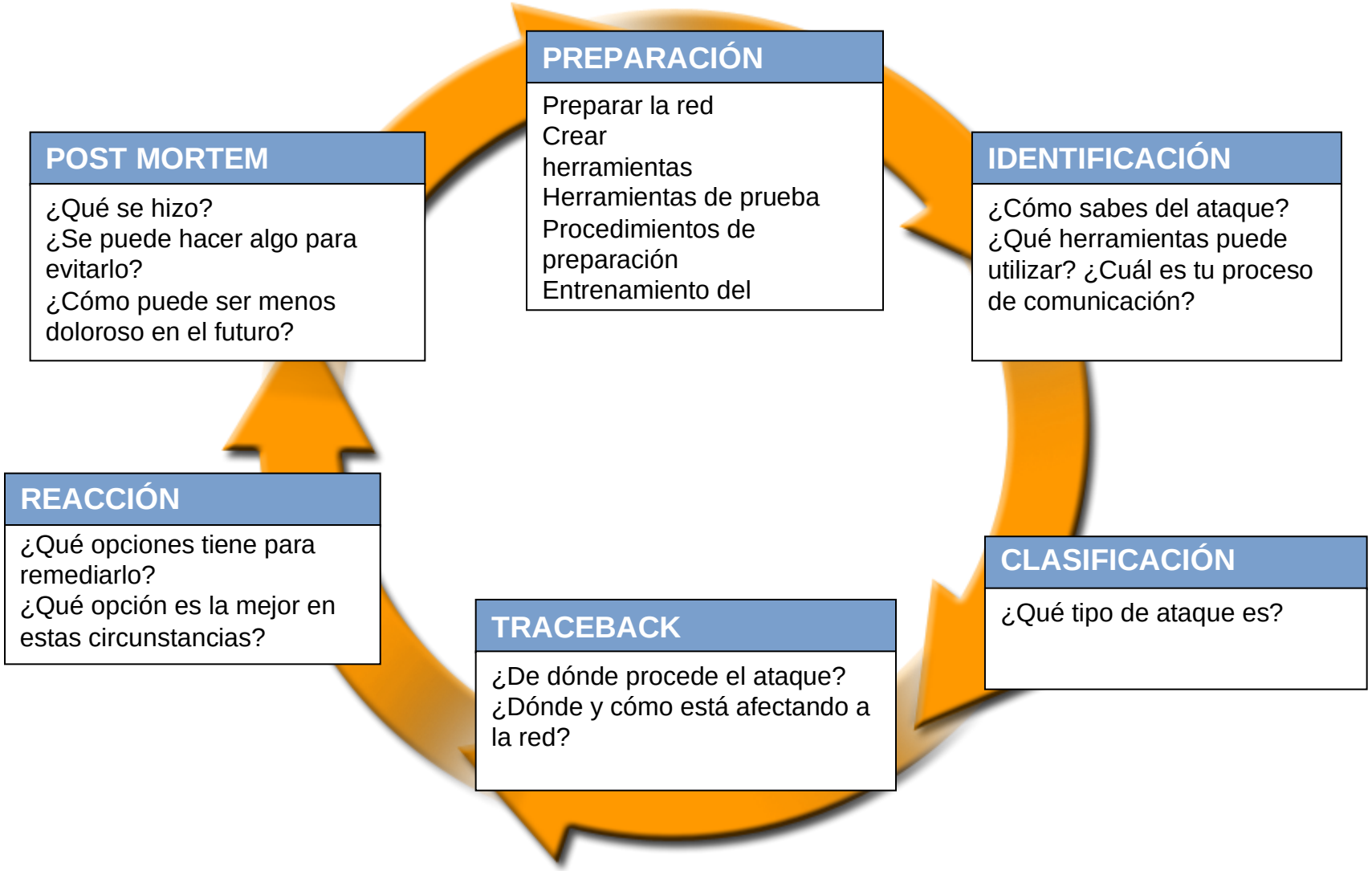


# Punto de agregación DoS

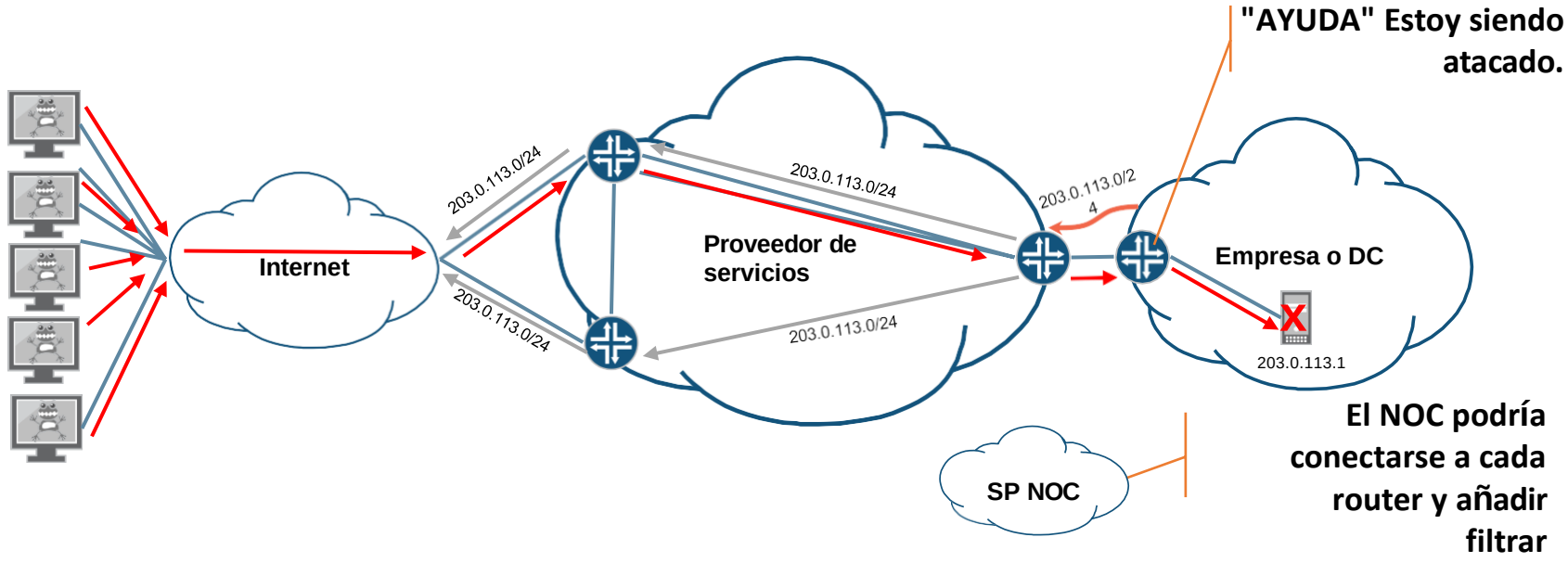



Principio básico para combatir un ataque DoS - ¡No permita que el DoS se

# Seis fases de la respuesta a incidentes

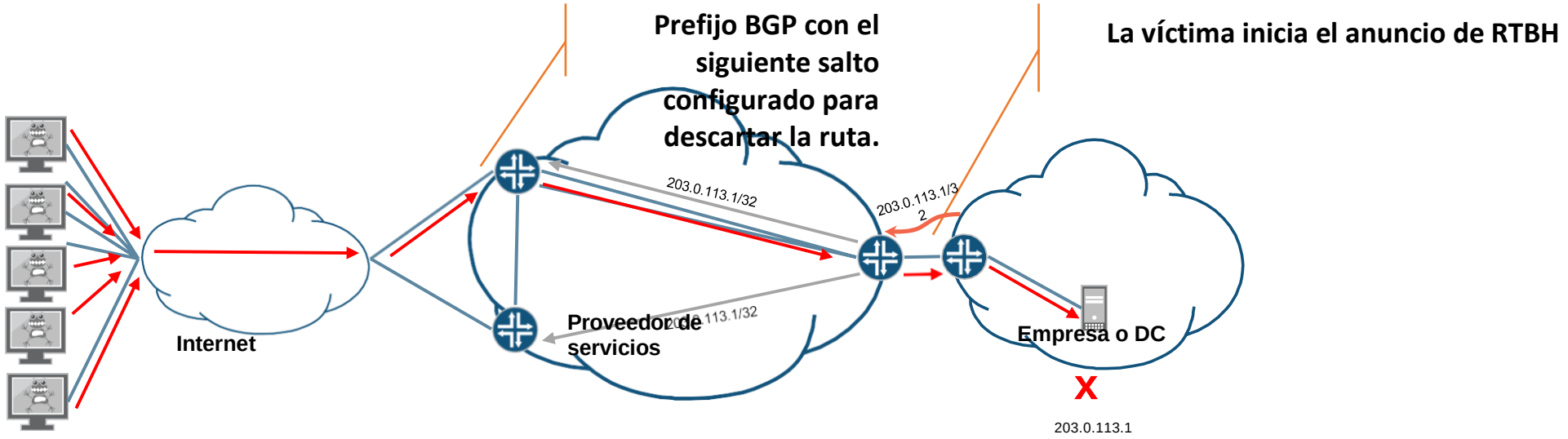


# Bloqueo de DDoS en los "viejos" tiempos



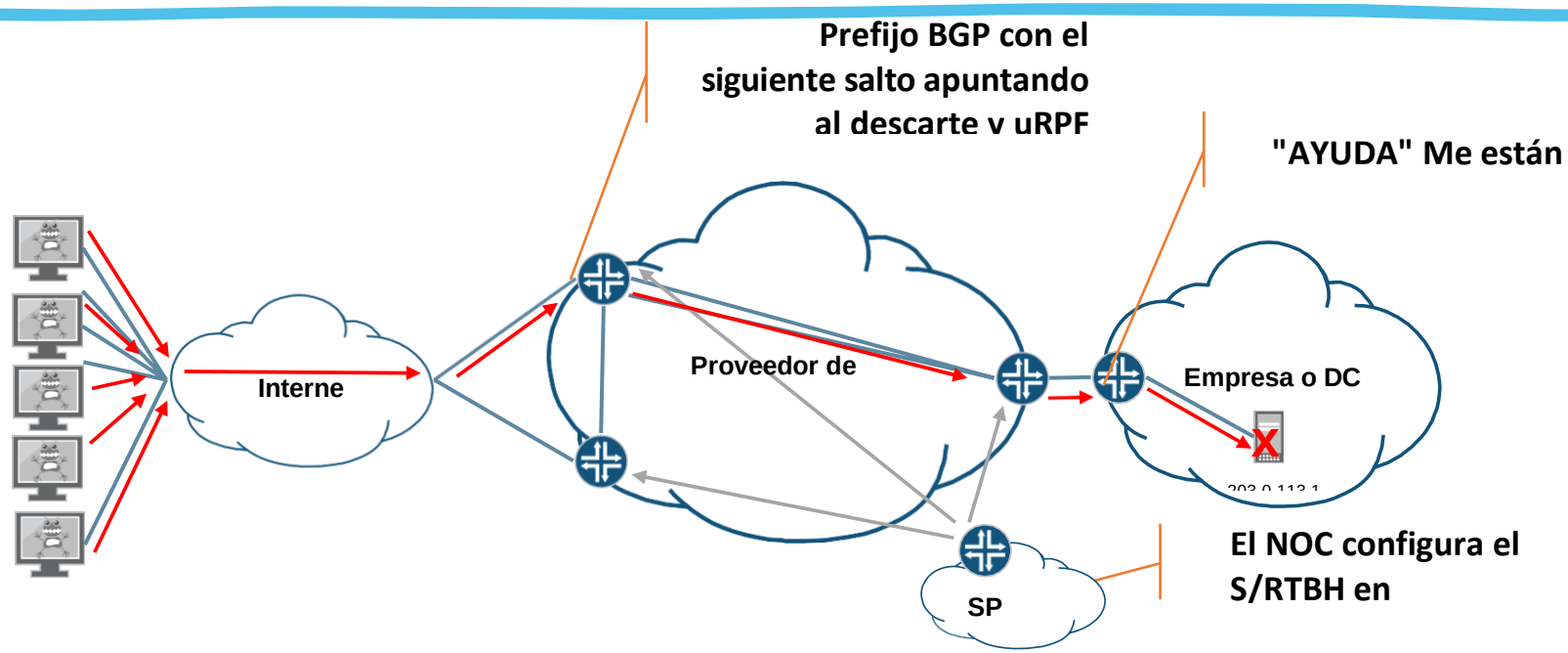

- Facilidad de aplicación y uso de conceptos bien entendidos
- Requiere un alto grado de coordinación entre el cliente y el proveedor
- Es difícil de escalar en un gran perímetro de red
- Posible y costoso error de configuración

# Agujero negro desencadenado a distancia en destino (D/RTBH)



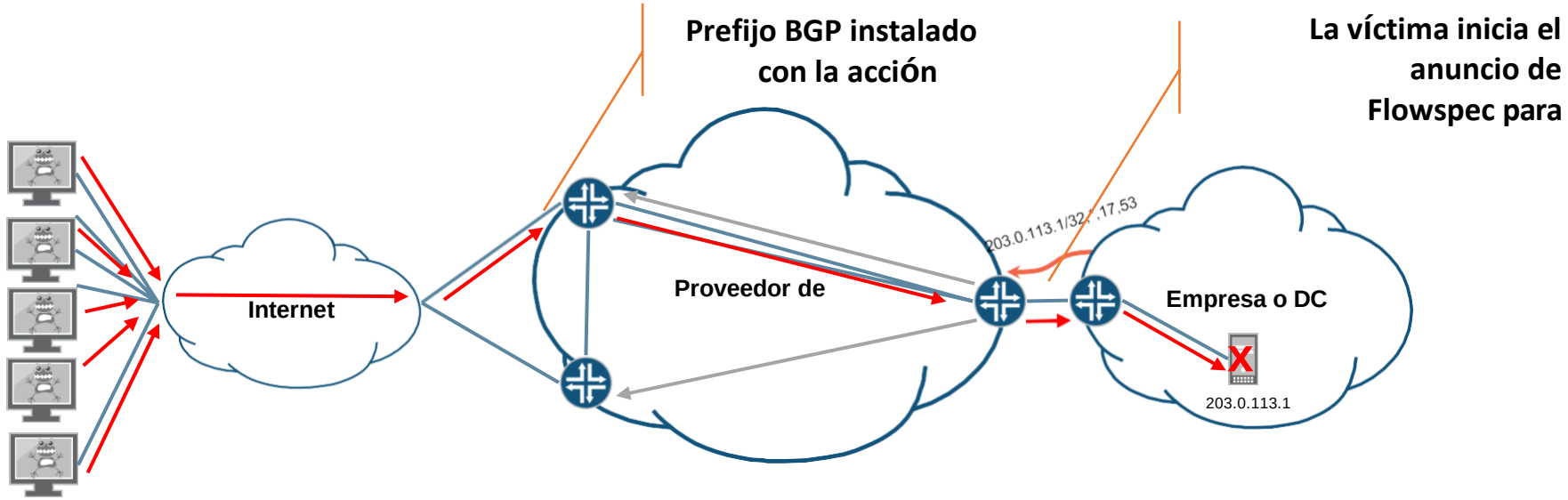

- RFC 3882 alrededor del año 2000
- Requiere la preconfiguración de la ruta de descarte en todos los routers de borde
- La dirección de destino de la víctima es completamente inalcanzable, pero se detiene el ataque (y los daños colaterales).

# Agujero negro desencadenado a distancia (S/RTBH)



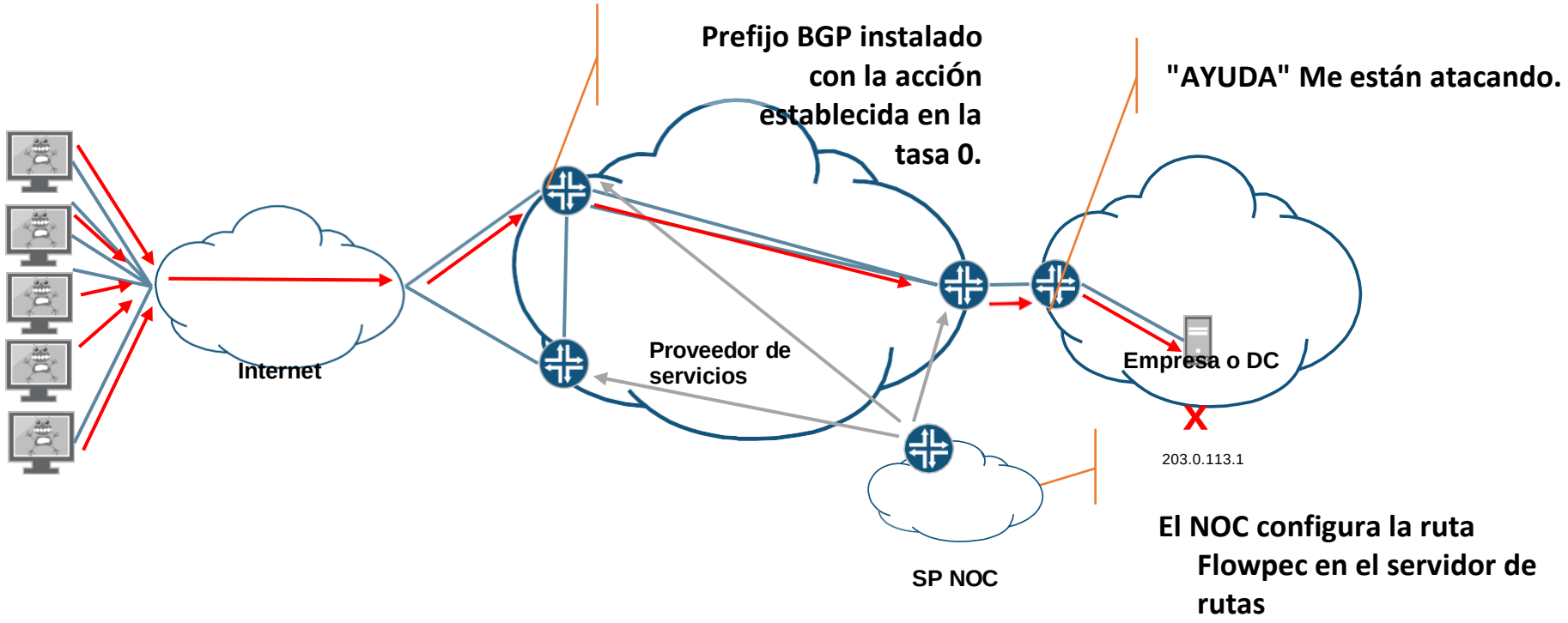

- RFC 5635 alrededor de 2005
- Requiere la preconfiguración de la ruta de descarte y uRPF en todos los routers de borde
- La dirección de destino de la víctima sigue siendo utilizable
- Sólo funciona para una única (o pequeña) fuente.

# Mitigación de DDoS entre dominios mediante Flowspec



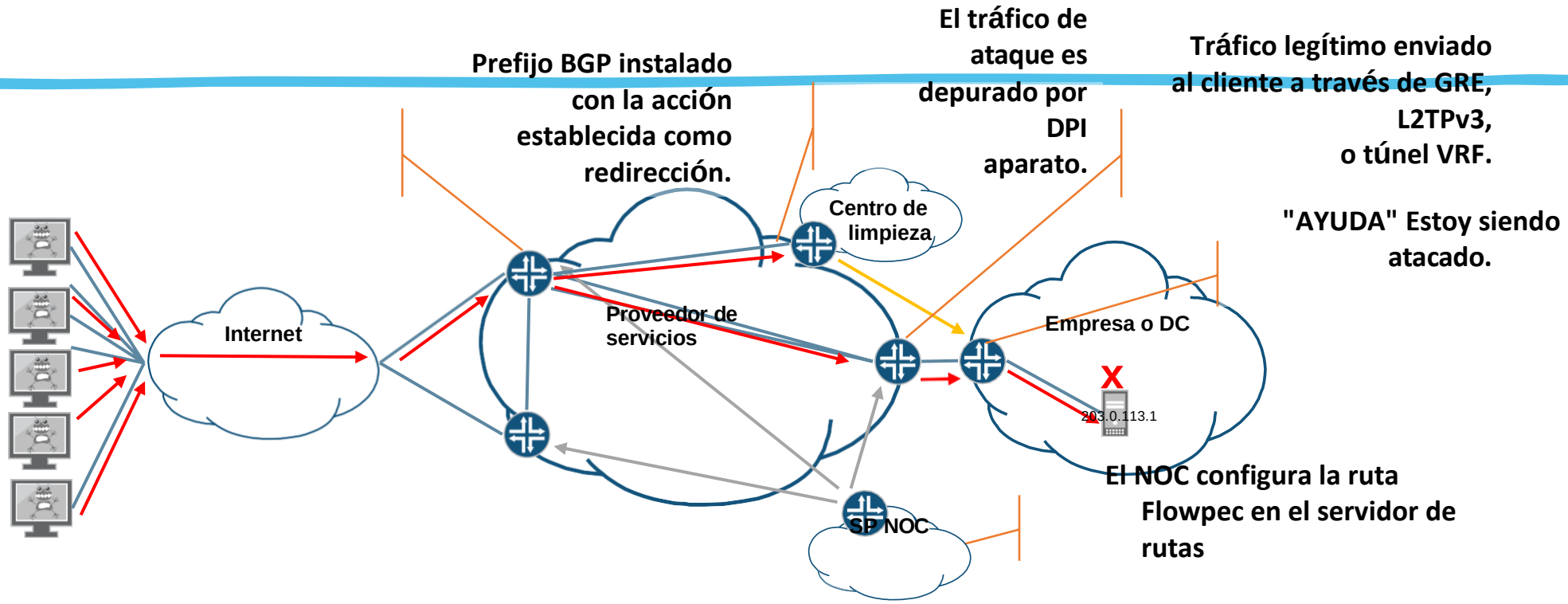

- Permite que el cliente del ISP inicie el filtro.
- Requiere un filtrado sano en el borde del cliente.

# Mitigación de DDoS dentro del dominio utilizando Flowspec



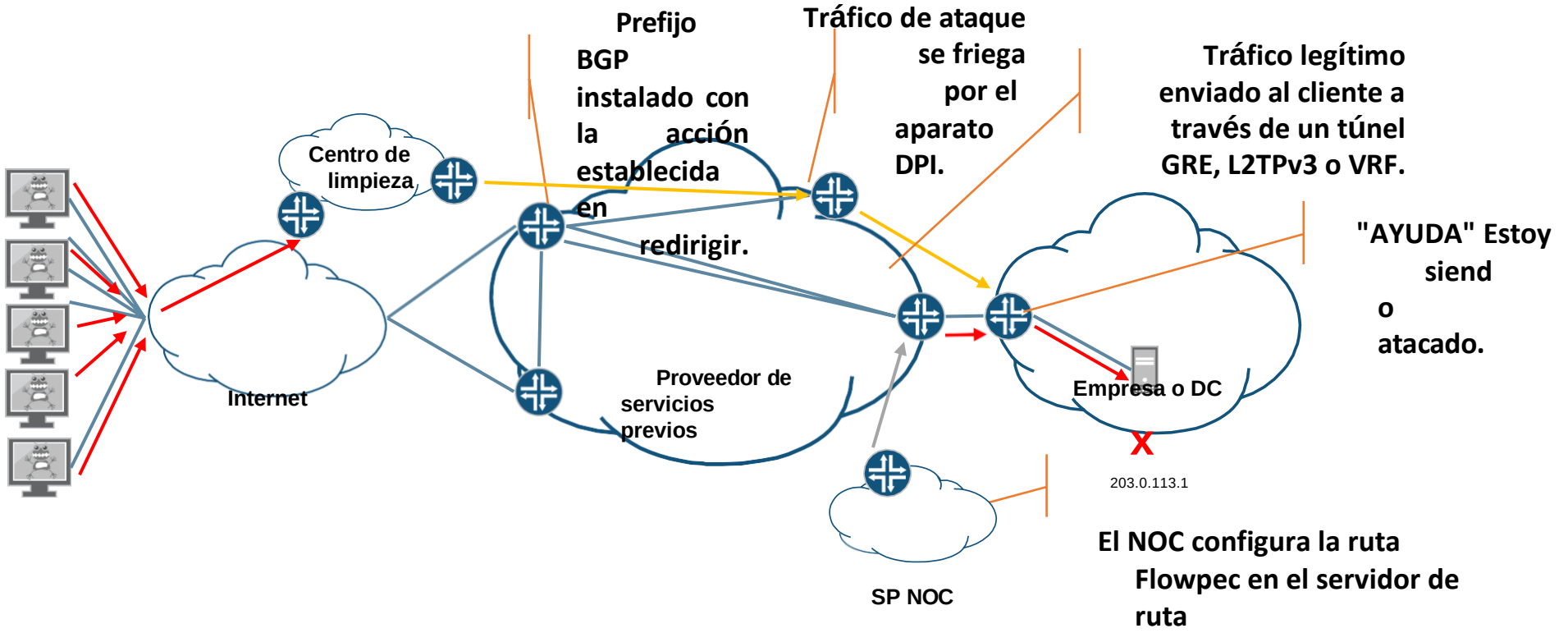

- Puede iniciarse mediante una llamada telefónica, la detección en la red de SP o un portal web para el cliente.
- Requiere la coordinación entre el cliente y el proveedor.

# Mitigación de DDoS mediante Scrubbing Center



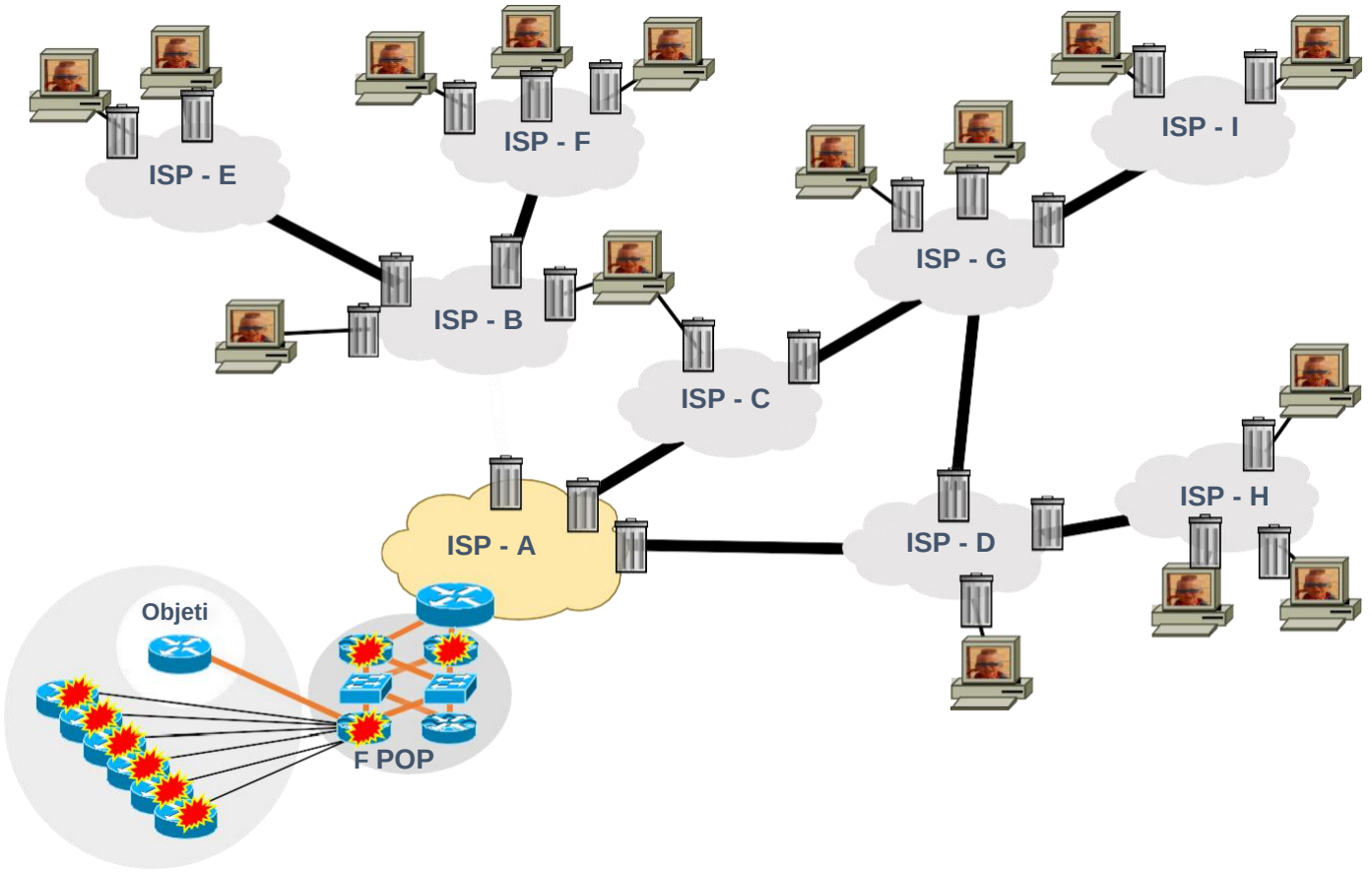

- Puede iniciarse mediante una llamada telefónica, la detección en la red de SP o un portal web para el cliente.
- Permite mitigar los ataques de la capa de aplicación sin completar el ataque.

# Mitigación de DDoS mediante Scrubbing Center

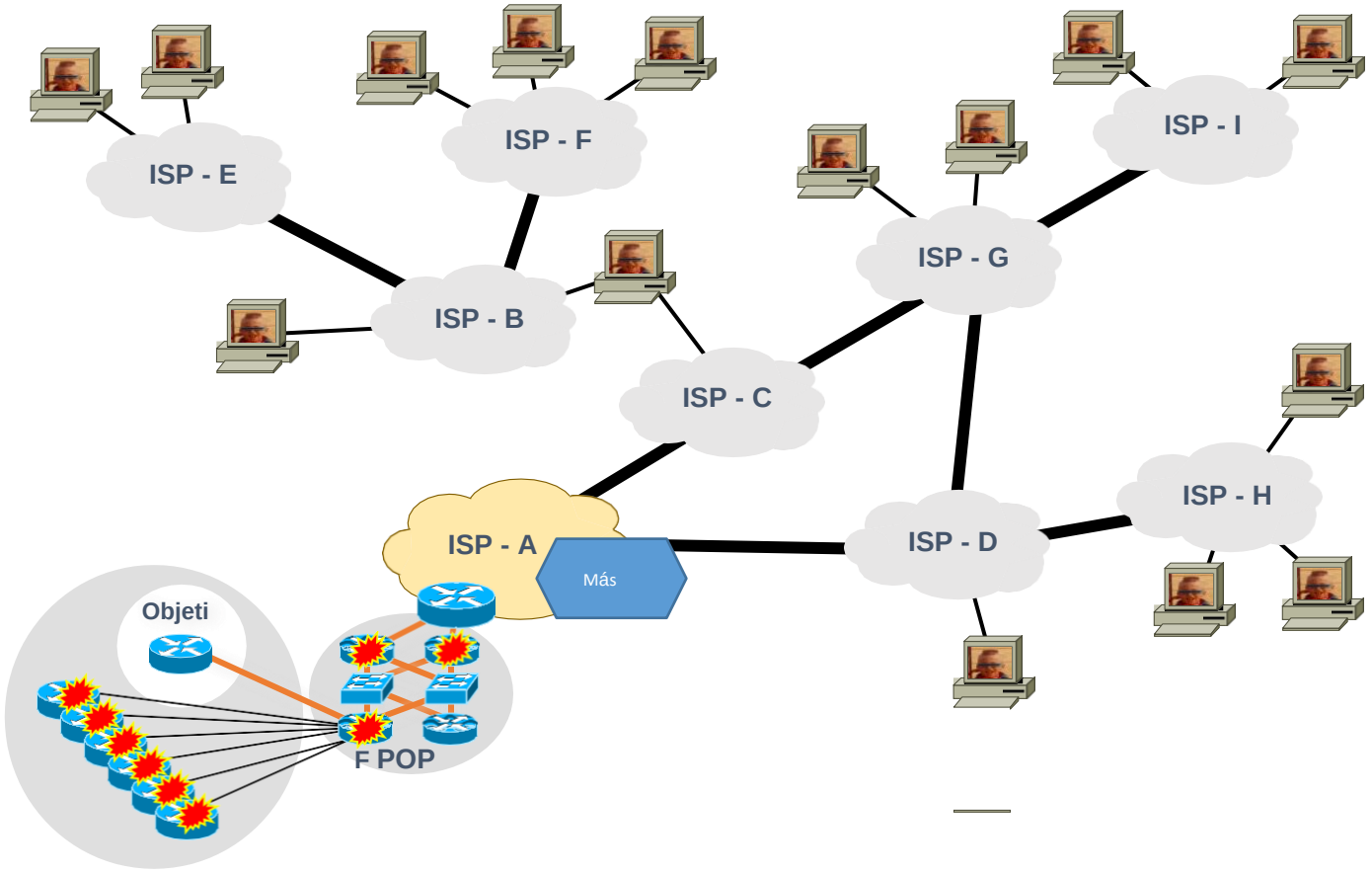



- Puede iniciarse mediante una llamada telefónica, la detección en la red de SP o un portal web para el cliente.
- Permite mitigar los ataques de la capa de aplicación sin completar el ataque.

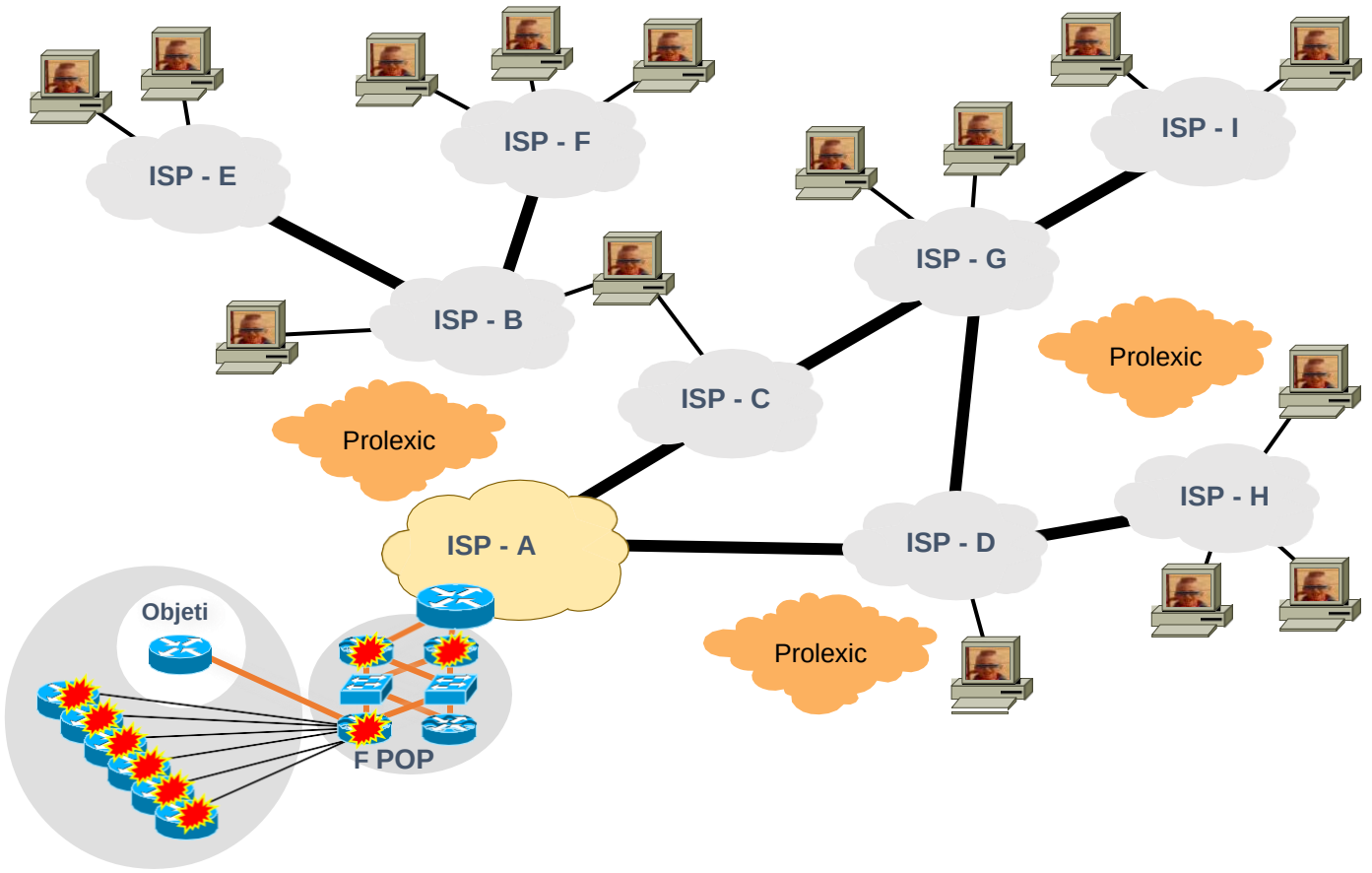
# DDOS Today - Podemos contratacar con RTBH



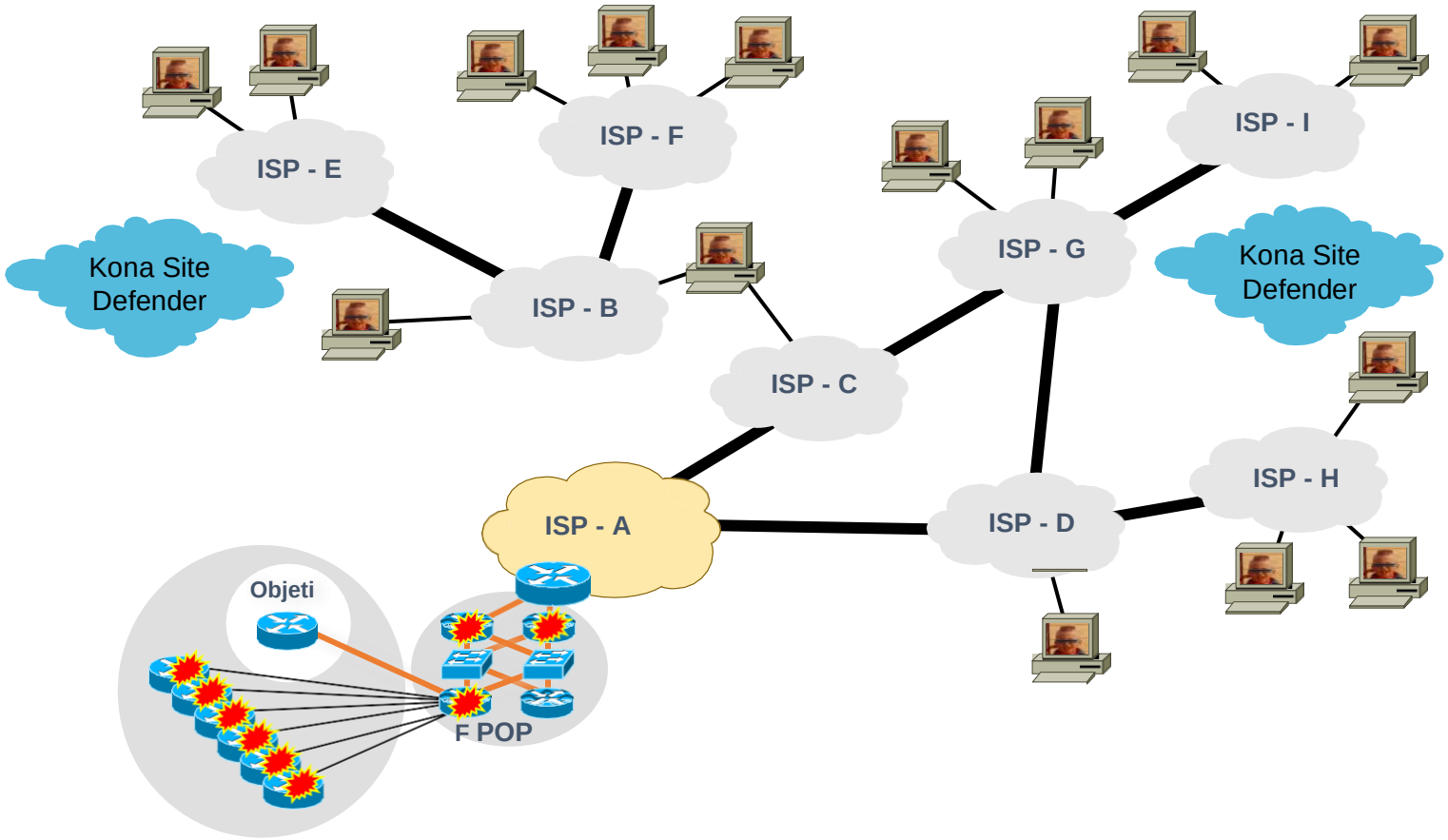
# DDOS Today - Ride out the Attack - Limpieza in situ



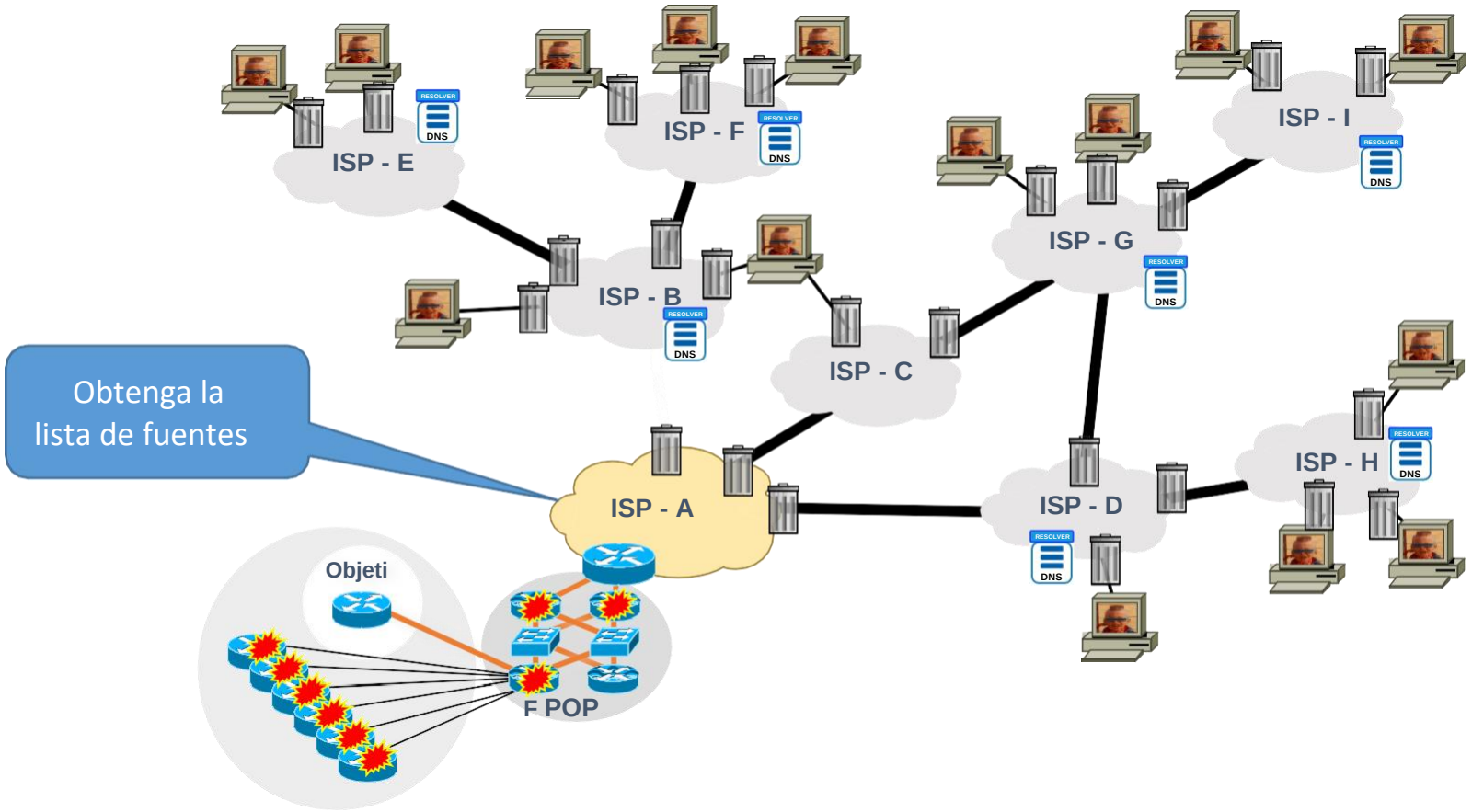
# DDOS Today - Ride out the Attack - Off Premise



# DDOS Today - Construir servicios más resistentes

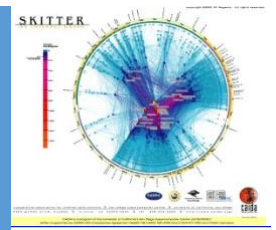


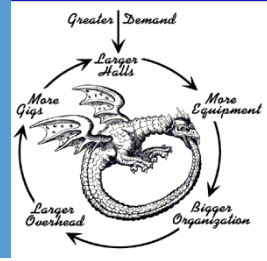
# Now podemos remediar como parte de una Federación



# Pausa para preguntas

# Puesta en marcha de las herramientas
# - Ataque DDOS

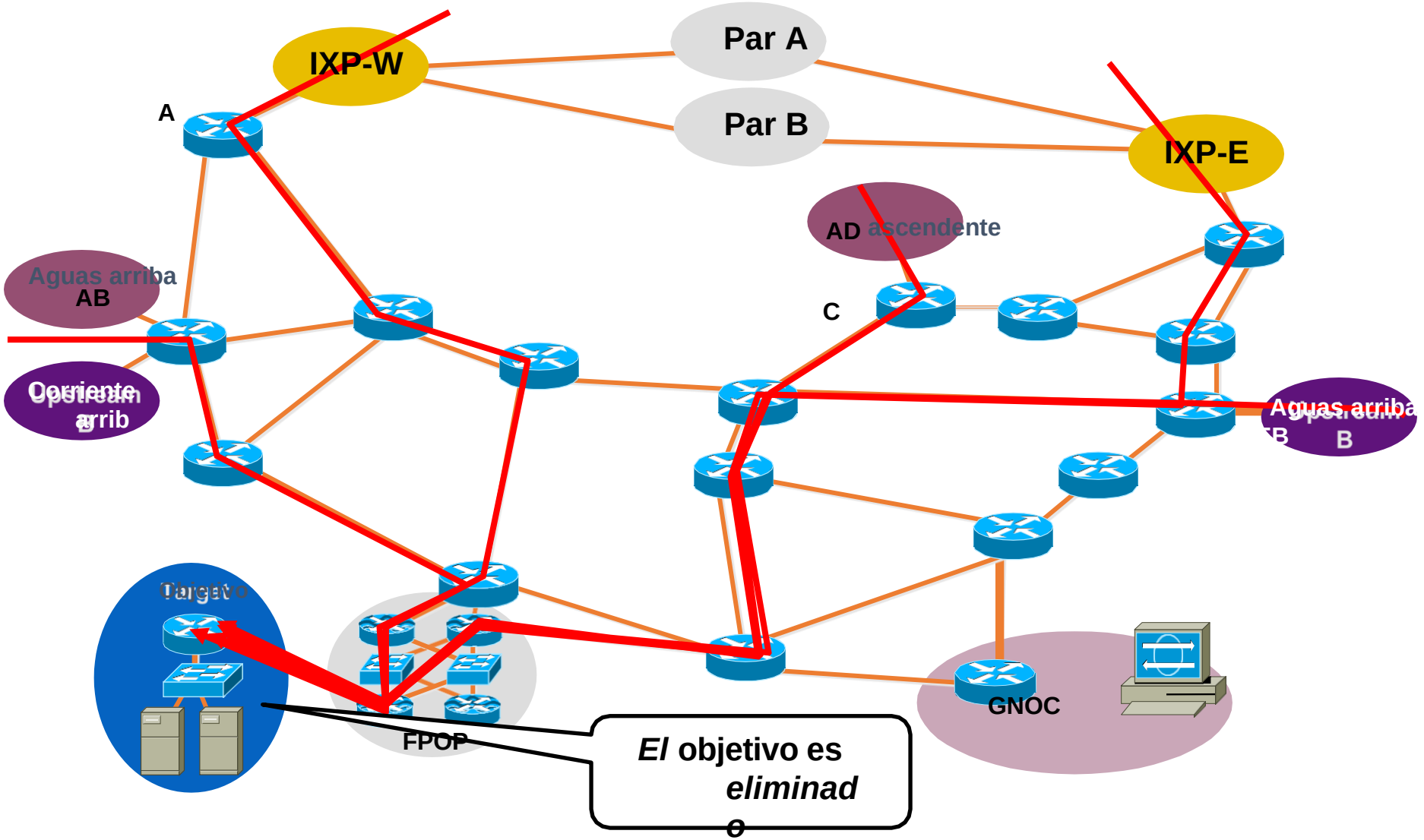


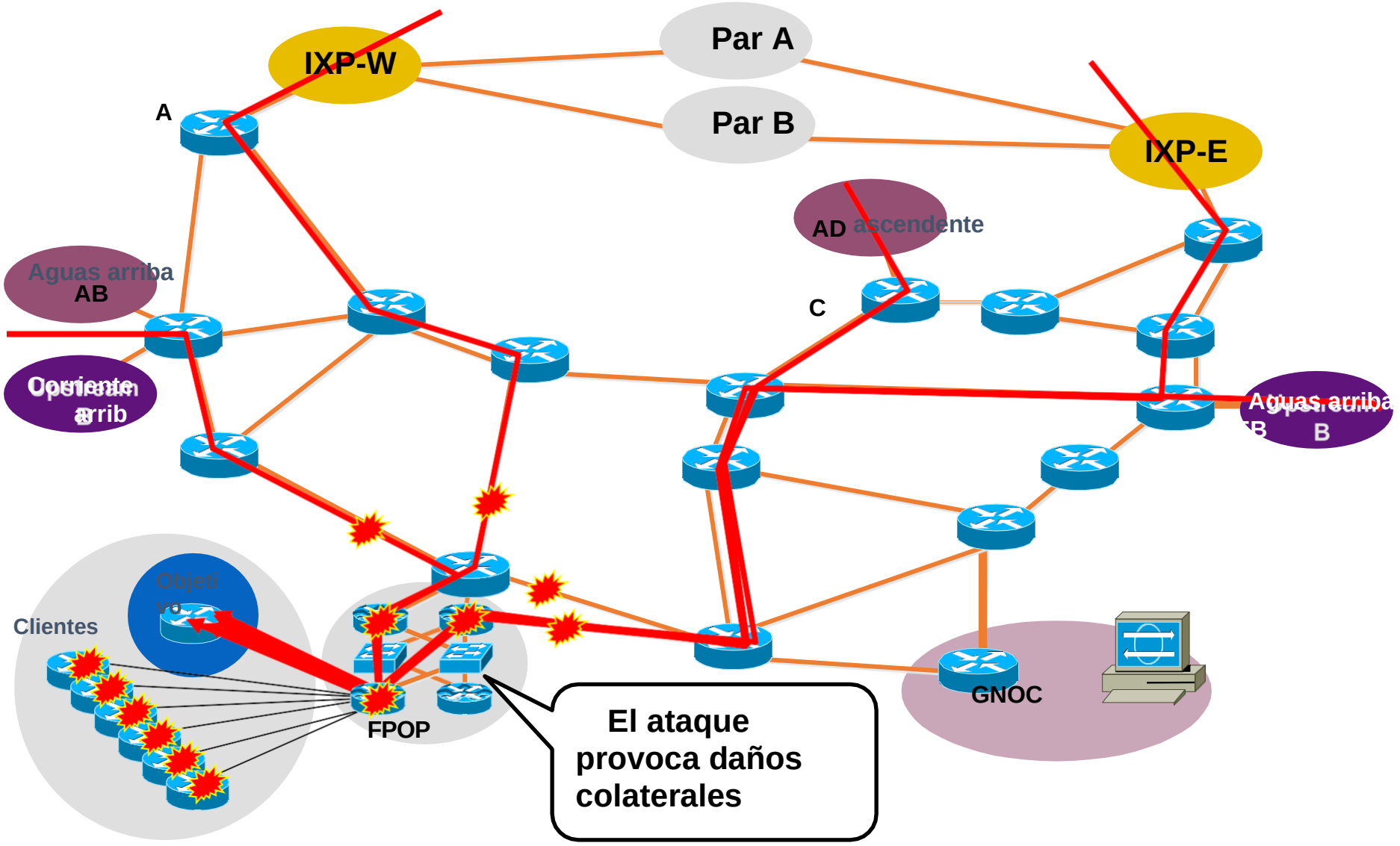

# SITREP

- Todo es normal en la Red.
- Entonces saltan las alarmas: algo está pasando en la red.

# El cliente es DOSed-Before



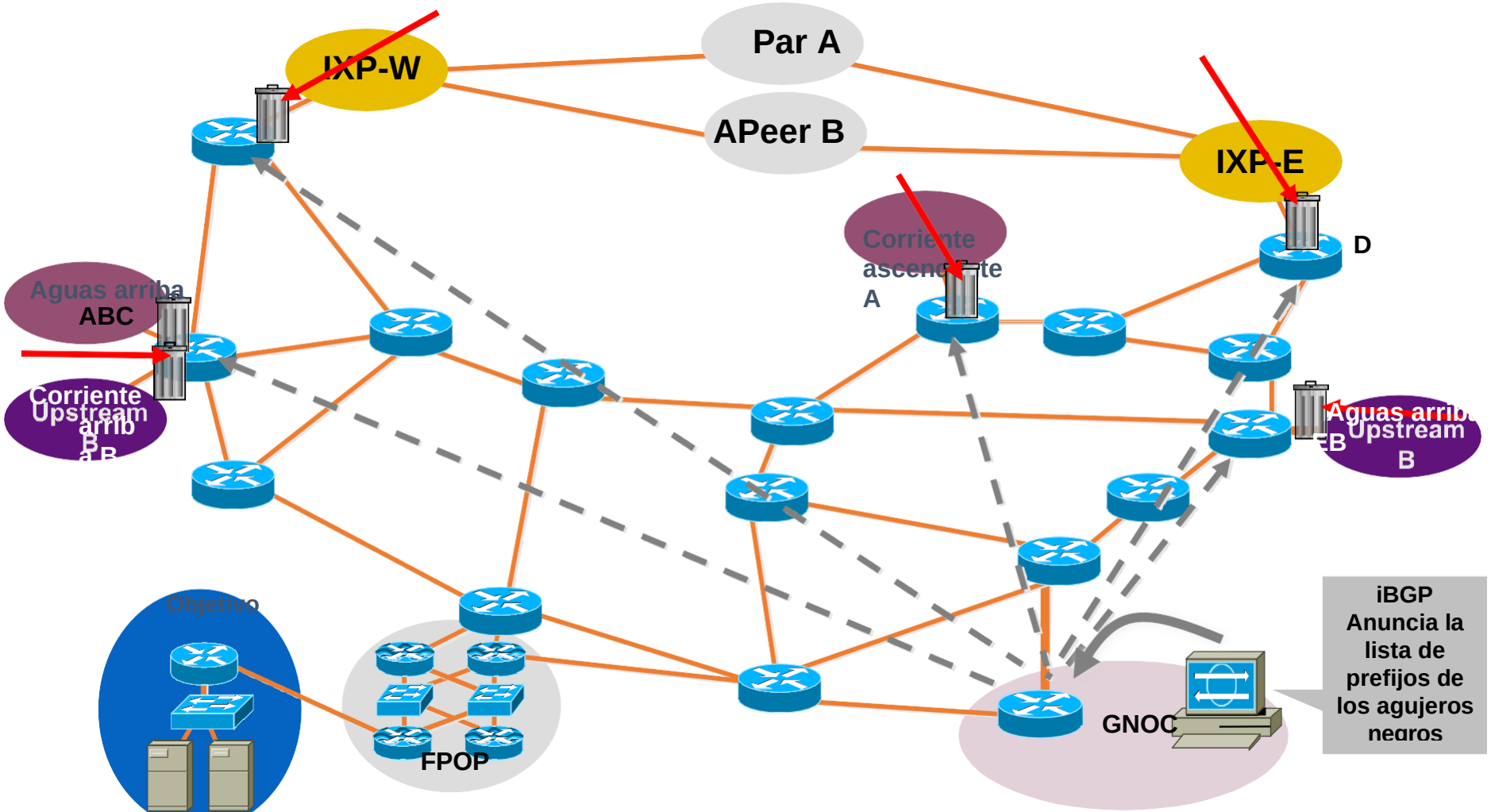
# El cliente es DOS-antes-daño colateral



# SITREP - Ataque en curso

- El ataque a un cliente afecta a varios clientes.
- ¡INCIDENTE DE DAÑO COLATERAL!
- Acción inmediata: Resolver los problemas de daños colaterales.

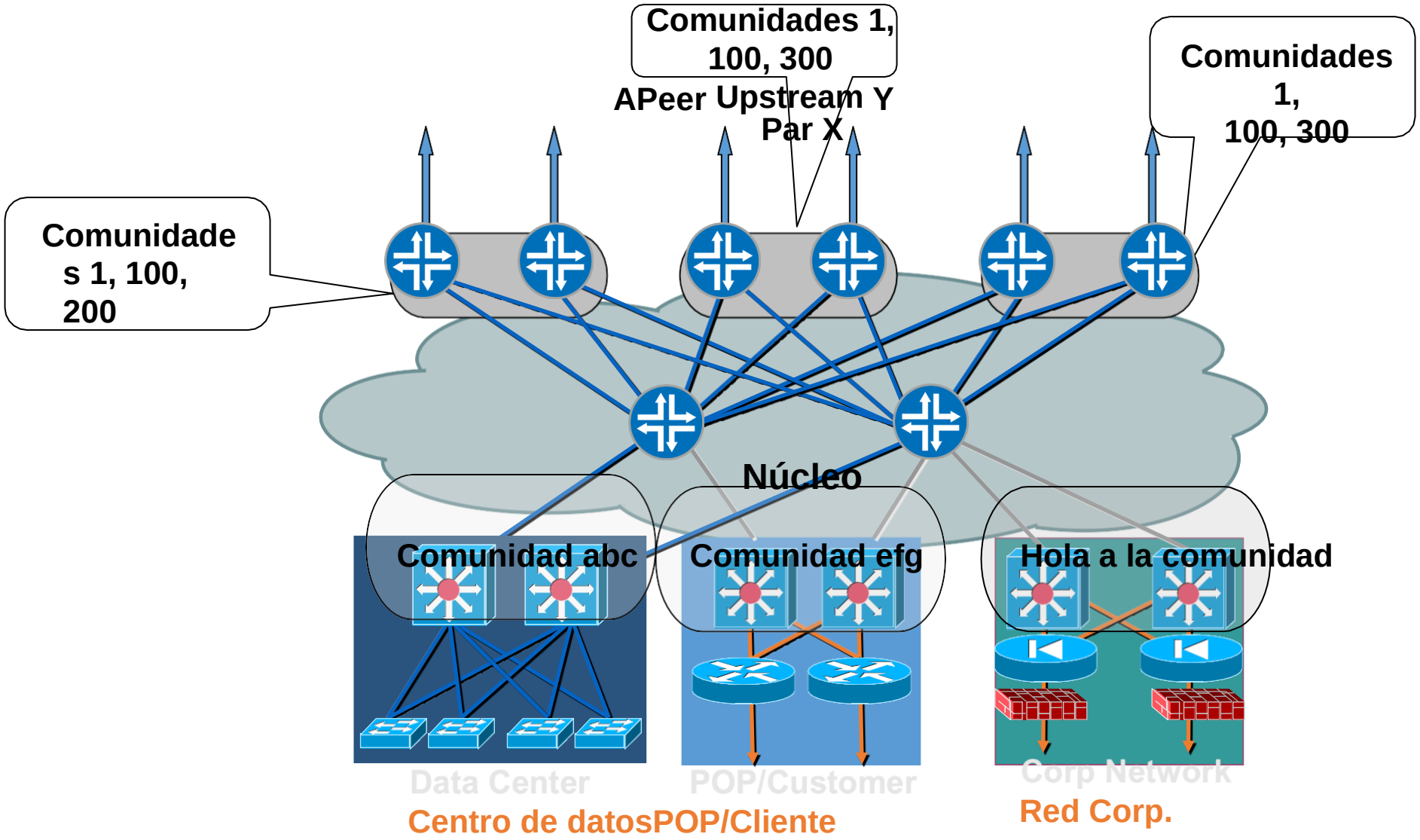
# El cliente es DOSed-Después de que los paquetes caigan en el borde



# SITREP - Ataque en curso

- Daños colaterales mitigados
- El cliente agredido tiene un SERVICIO PARCIAL.
- El ataque DOS sigue activo
- Opciones:
  - Sink Hole una parte del tráfico para analizar.
  - Observe el ataque del DOS y espere la rotación del ataque o el cese.
  - Active "Clean Pipes" para una recuperación completa del servicio.

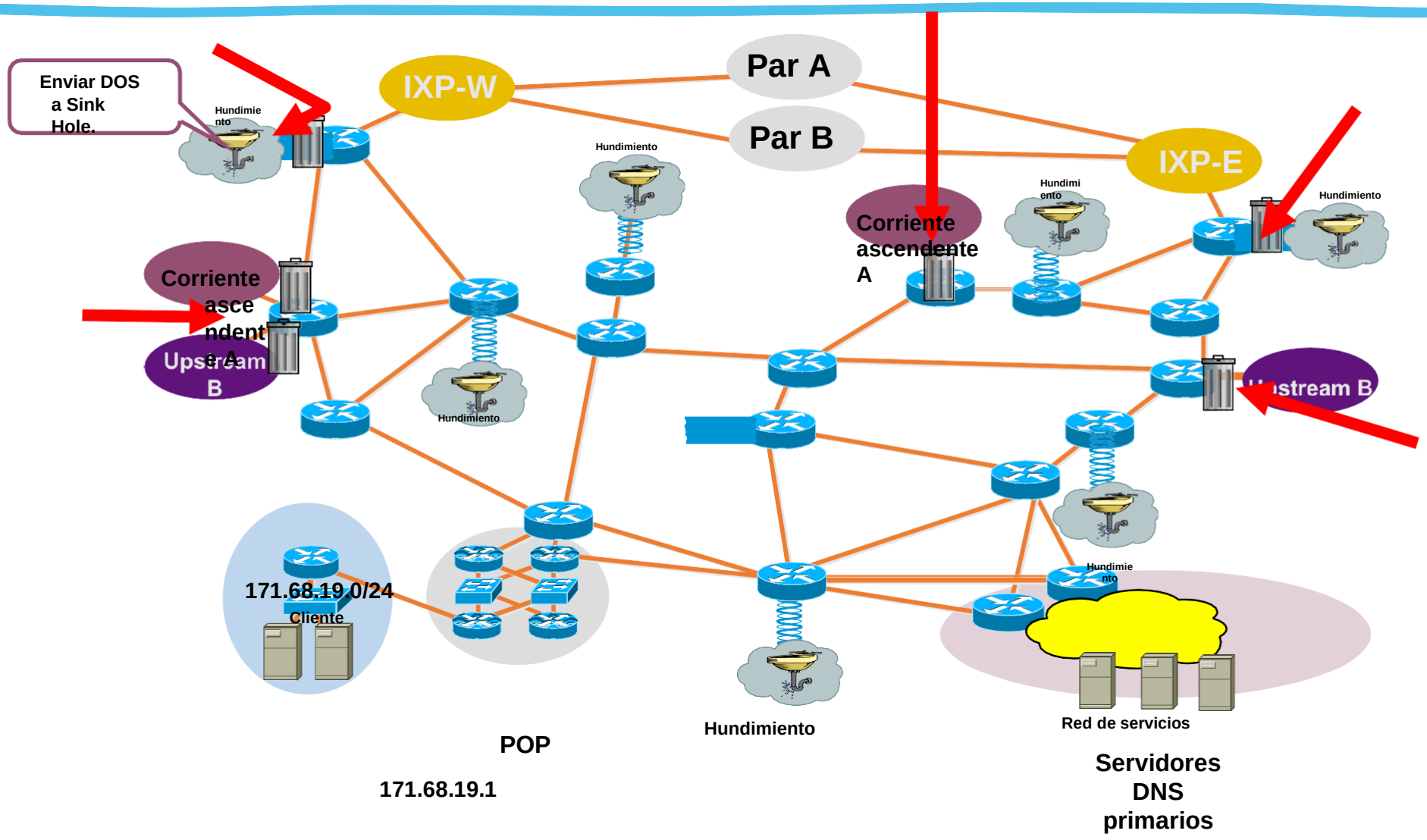
# Desconexiones remotas y comunidades BGP



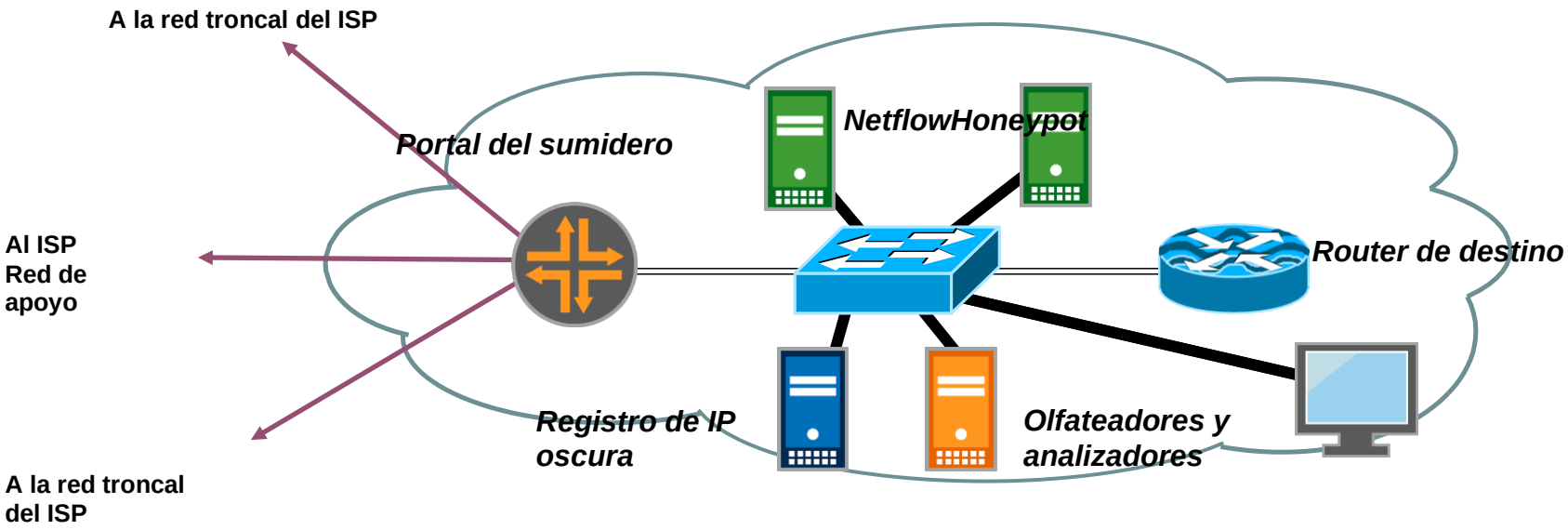
# SITREP - Ataque en curso

- Daños colaterales mitigados
- El cliente agredido tiene un SERVICIO PARCIAL.
- El ataque DOS sigue activo
- Acción: Vigilar el ataque y obtener más detalles sobre el mismo
  - Utilizar la activación basada en la comunidad BGP para enviar un flujo de regiones a un Sink Hole

# Activación de la comunidad BGP a Sinkhole



# Analizar el ataque




- Utilice las herramientas disponibles en Internet y de los proveedores para analizar los detalles del ataque.
- Esto le proporcionará información sobre lo que puede o no puede hacer a continuación.

# SITREP - Ataque en curso

- Daños colaterales mitigados
- El cliente agredido tiene un SERVICIO PARCIAL.
- El ataque DOS sigue activo
- Acción: Proporcionar al cliente damnificado un servicio de recuperación del servicio completo de Clean Pipes (fuera de los detalles específicos del proveedor).

# ¿Qué es la recuperación de Full servicios?

- "Tuberías limpias" es un término utilizado para describir la recuperación completa del *servicio*. Las expectativas para una recuperación del servicio completo son:
  - El ataque DDOS está en plena vigencia y TODOS los servicios a los clientes funcionan con normalidad, cumpliendo el SLA contratado.
  - El dispositivo utilizado para la recuperación del servicio completo no es vulnerable al DDOS y la infraestructura no es vulnerable a los daños colaterales.
- Los productos de servicio completo de recuperación/limpieza de tuberías son muy especializados. Hable con el proveedor correspondiente.

# Full frente a la recuperación del Partial servicio

- La recuperación parcial del servicio es fácil ... hacer retroceder el ataque hasta el borde de la ASN.

- La recuperación del servicio completo requiere una planificación centrada en los servicios clave.

# Pausa para preguntas

# ¿Qué es lo siguiente?

- Descargue los libros blancos, los blogs y los materiales de los talleres de www.senki.org

- Conéctate! Barry se conecta con compañeros, colegas y aspirantes a talento a través de Linkedin (www.linkedin.com/in/barryrgreene/). También puedes seguir a Barry en Twitter (@BarryRGreene) o sus blogs en Senki (www.senki.org).