



TIAGORA.COM

# Virtualización de redes corporativas

**Rogelio Alvez**

ralvez@tiagora.com

**CERTuy**

 **AGESIC**

  
**PRESIDENCIA**  
REPUBLICA ARGENTINA

# Objetivo de la presentación

- **Uso de MPLS/VPN\* como herramienta para proporcionar una mayor privacidad**
- **Detallar la reingeniería de una red que tiende a un modelo virtual**
- **Descripción de una metodología de migración de IP tradicional a MPLS/VPN**



**CERTuy**

 **AGESIC**



# Revisión de enfoques sobre virtualización de red



CCIE, CCSP y CSCI son marcas registradas de Cisco Systems, Inc

# Qué es una VPN (revisión)

- **Un conjunto de sitios (o segmentos de redes) que pueden comunicarse mutuamente**
- **Desde el punto del usuario, TODO aquello a lo que puede acceder**
- **Desde el punto de vista del router que conecta al usuario, su tabla de rutas asociada**

# Redes corporativas: características

- Múltiples grupos comparten una misma red IP
- Heterogeneidad/complejidad de WAN/LAN
- IP unicast
- Posible necesidad de IP Multicast (motivado por aplicaciones multimedia)
- SLA para las aplicaciones
- Recursos comunes: Internet, telefonía, datacenter, email

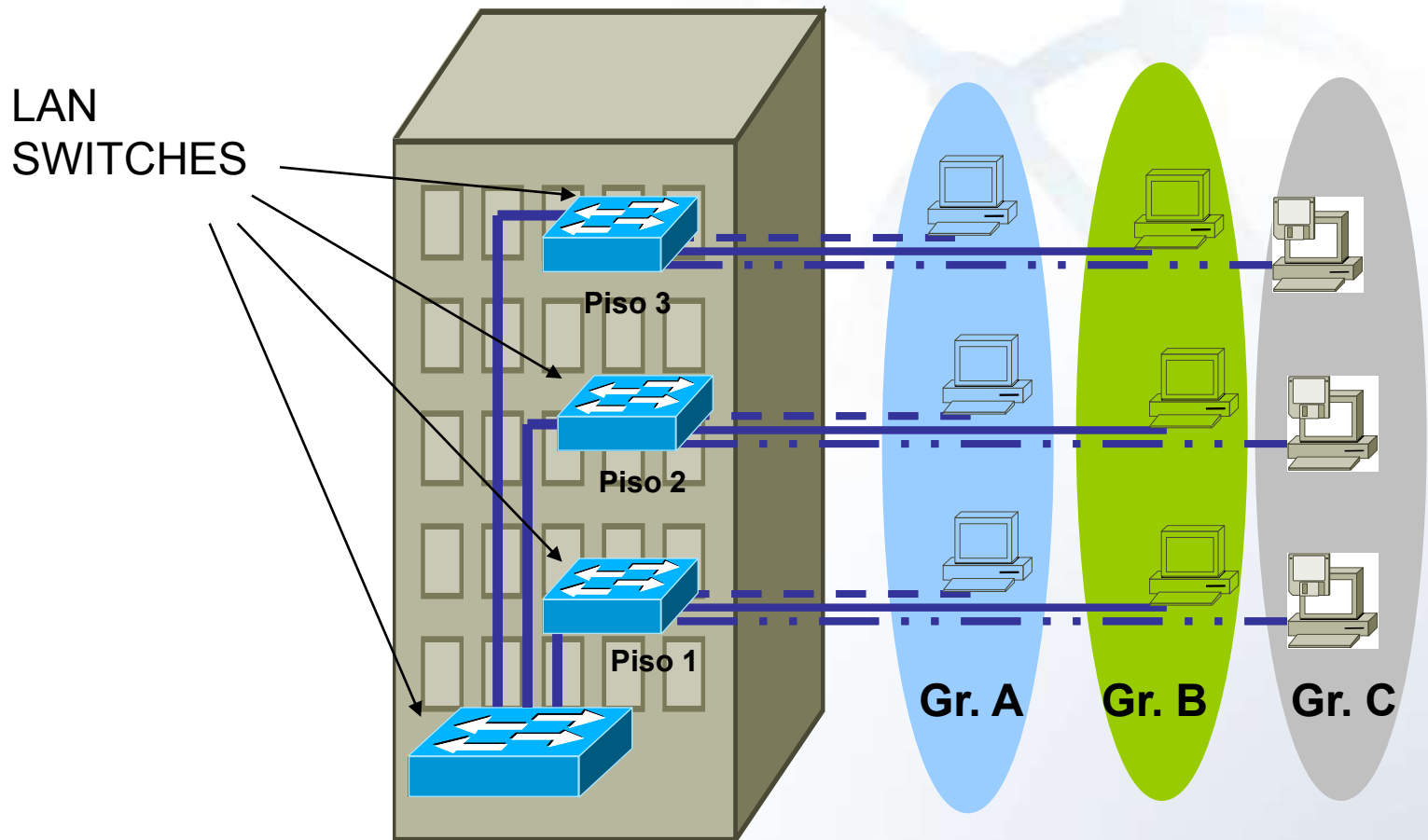
# Perfil de tráfico de una red corporativa

- **Conectividad irrestricta entre casi cualquier par de puntos, pero...**
- **95% del tráfico de usuario se cursa**
  - entre los usuarios y el datacenter
  - o entre los usuarios e Internet
- **Rara vez es necesaria una comunicación “horizontal” (entre usuarios), o bien se resuelve vía “servidores de encuentro”**

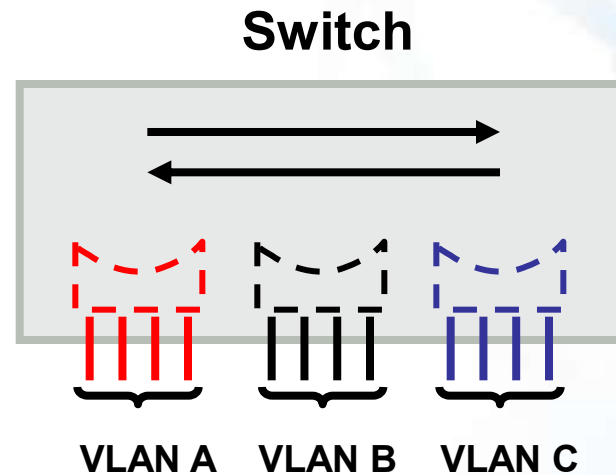
# Riesgos de un modelo “any to any”

- **Puede dejar espacios abiertos a vulnerabilidades**
  - **DoS, intentos de acceso no autorizado, network mapping, etc**
- **Los firewalls suelen no intermediar entre cualquier par de estaciones de trabajo**
- **Los IPS/IDS deben trabajar reactivamente**

# Revisión: Virtual LANs

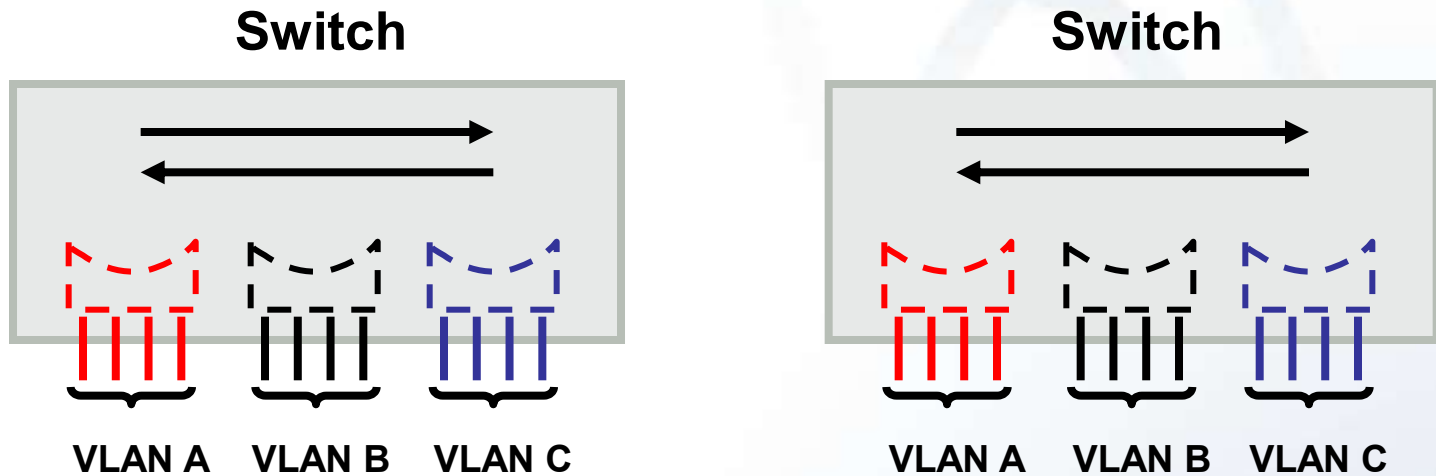


# Cómo operan las VLANs



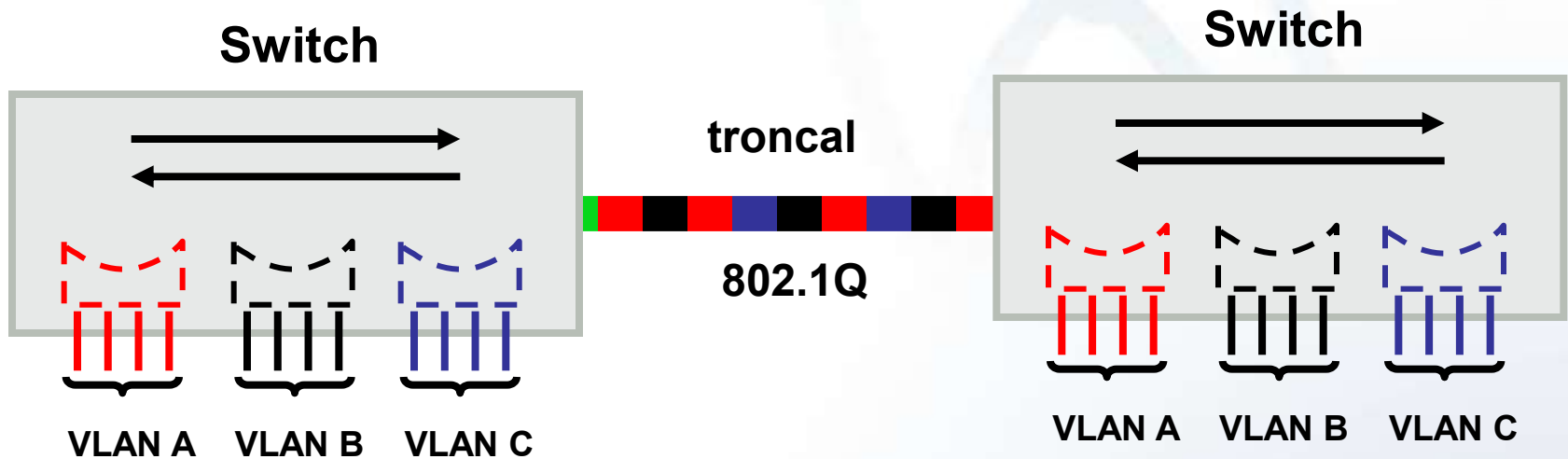
- Cada VLAN es un “switch virtual”
- Si las VLANs necesitan comunicarse, debe haber una función de routing entre ellas

# Cómo operan las VLANs (cont.)



- Una VLAN puede estar presente en más de un switch ***DE UN MISMO CAMPUS***

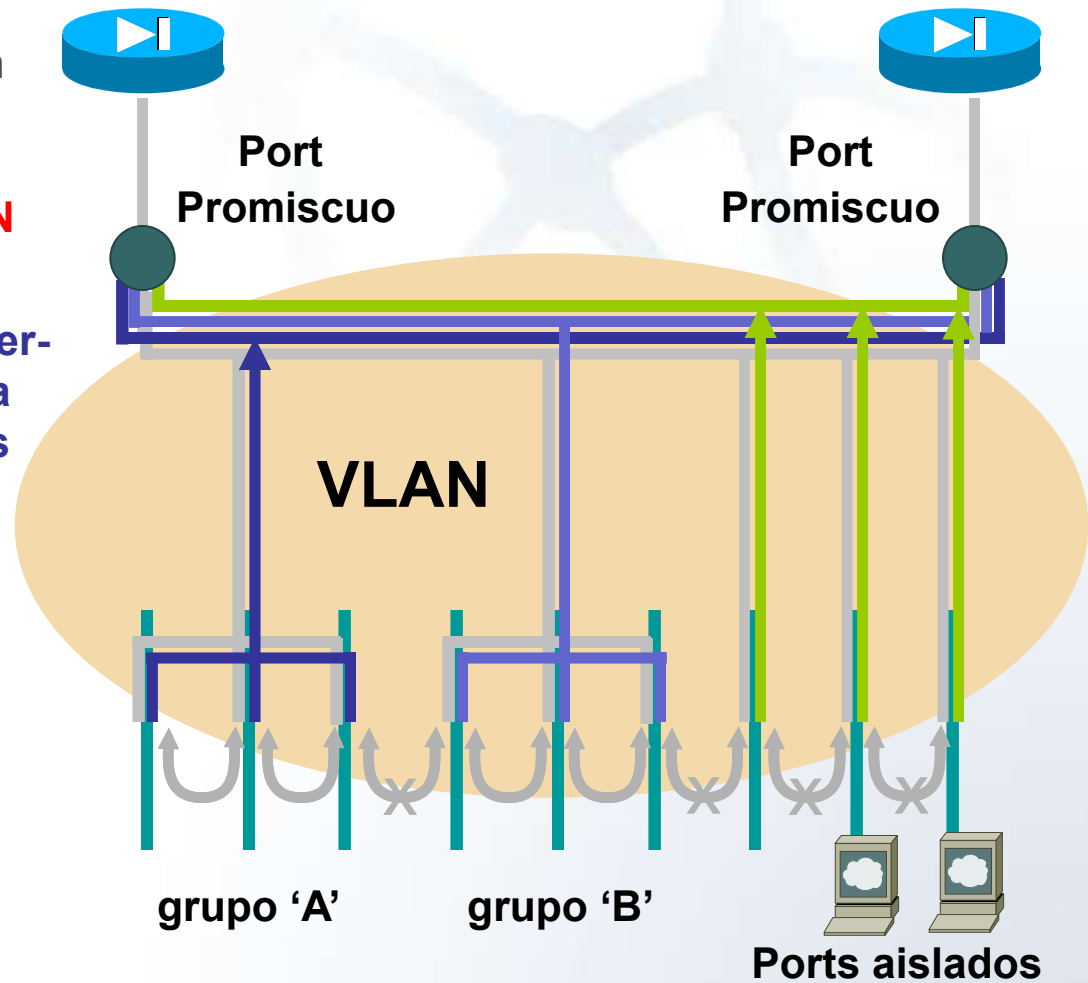
# Cómo operan las VLANs (cont.)



- Un enlace “troncal” con soporte de VLANs, permite la presencia de la misma VLAN en múltiples switches

# Private VLANs

- PVLANS aislarán tráfico en grupos específicos, para crear distintas “redes” dentro de una misma VLAN
- La mayoría de la charla inter-host quedará deshabilitada cuando se habilite PVLANS



# Límite de las VLANs como solución

- **Condición necesaria, pero no suficiente**
  - **Bastará que un router o switch de nivel 3 esté en contacto con dos VLANs, y será posible que se comuniquen**
  - **El alcance de una VLAN es un “campus”**
  - **Una VLAN no es eficiente para limitar el alcance del broadcasting**

# Límite de las “private VLANs”

- **Es complementario al problema mencionado**
  - **Incorporar “private VLANs” ayuda a aislar estaciones de trabajo a nivel 2**
- **Podría impedir comunicaciones necesarias (ej: teléfonos IP entre sí)**

# Contraste entre VLANs y VPNs

- Una VLAN **no necesariamente** es una VPN
  - Una VLAN podría llegar a formar parte de varias VPNs dispersas por toda la red corporativa (ejemplo: el datacenter)
  - Una VPN podría llegar a estar conformada de una o varias VLANs, dispersas por toda la red corporativa (ejemplo: la red de telefonía IP)



**CERTuy**

 **AGESIC**



# Objetivos corporativos de privacidad de red



CCIE, CCSP y CSCI son marcas  
registradas de Cisco Systems, Inc

# Objetivos de privacidad

- **Promover la restricción de comunicación entre grupos a priori disjuntos (habilitar “caso por caso”)**
- **Controlar el flujo de información entre departamentos y dentro del mismo datacenter**
- **Identificar recursos comunes y ponerlos a disposición a través de herramientas de protección adecuadas**

# Solución (I)

- Construir una red física distinta para cada grupo de interés o VPN
  - **No es una postura realista en términos económicos**
  - *Suele hacerse en forma muy puntual en ciertos segmentos de industrias con procesos críticos*

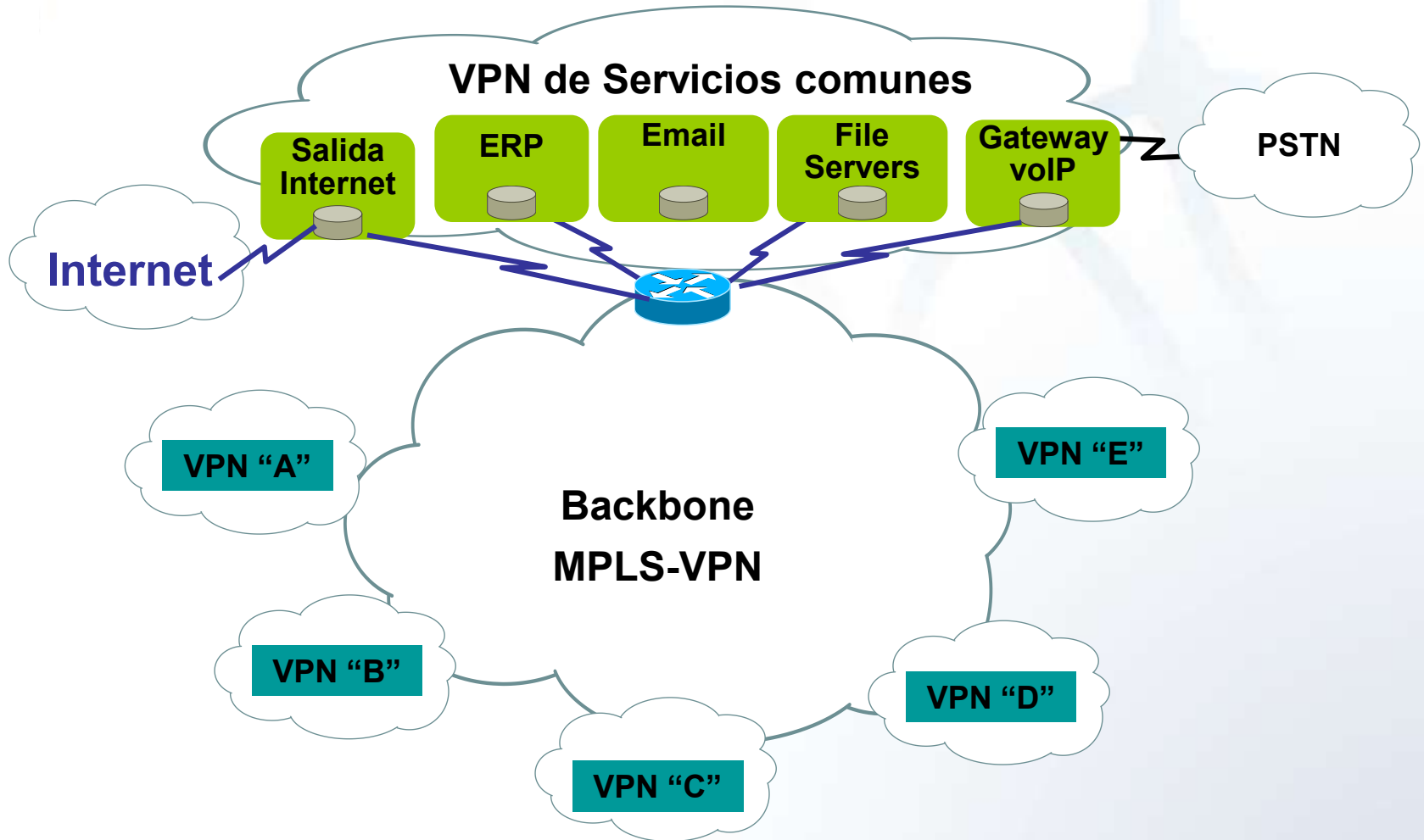
## Solución (II)

- Crear “filtros” o listas de acceso en **cada uno** de los equipos que proporcionen ruteo
  - NO ES UNA TÉCNICA ESCALABLE
  - ES MUY FÁCIL COMETER ERRORES

# Solución (III)

- **Virtualizar la red utilizando MPLS/VPN**
  - **En redes contemporáneas, prácticamente no exige inversión adicional a nivel hardware o software**
  - **Garantiza la separación de los grupos virtuales**
  - **Pueden definirse “puntos de contacto” entre los diferentes grupos, en forma controlada**
  - **Es escalable**
  - **Es una técnica madura**

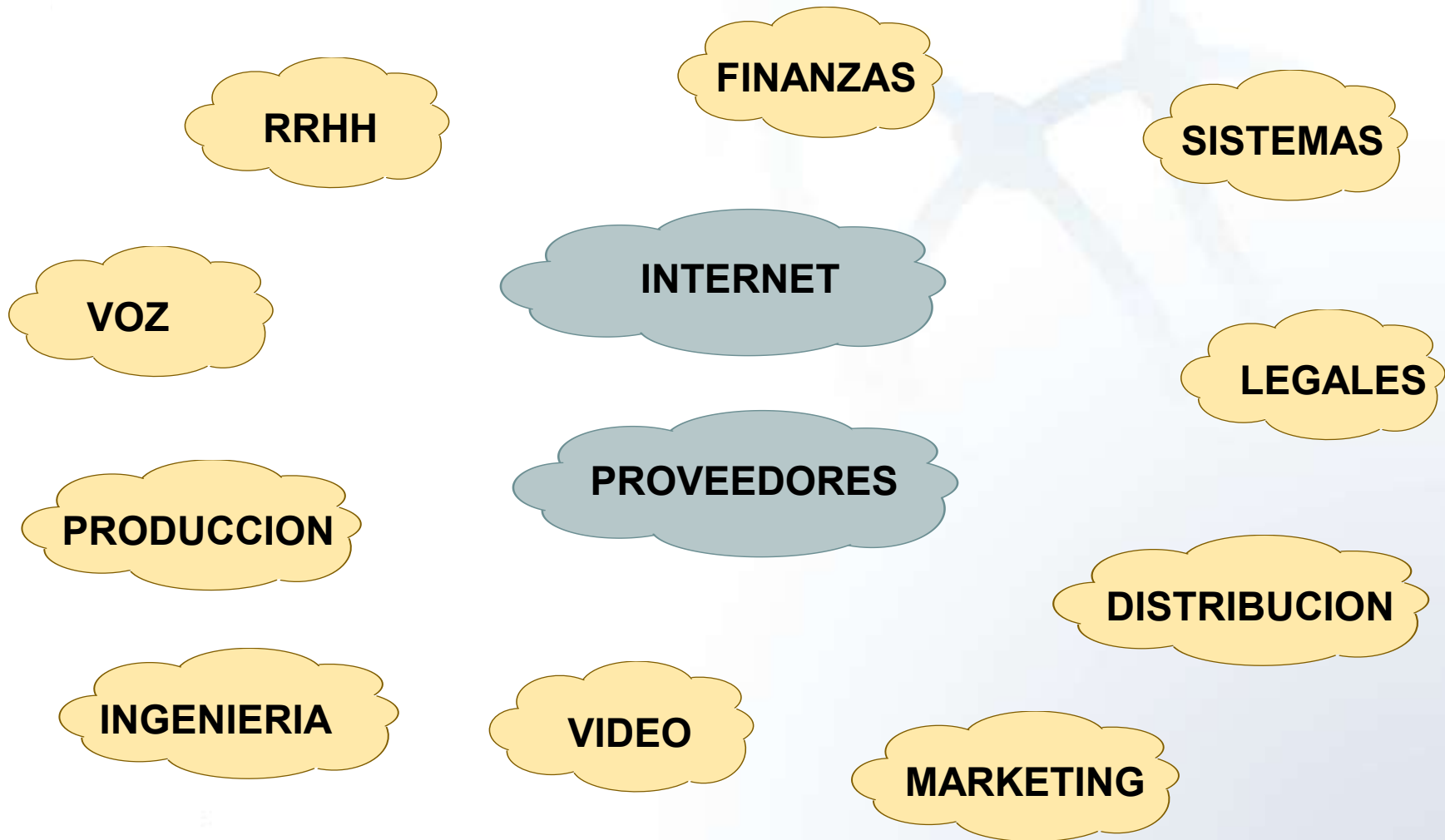
# MPLS/VPN: Objetivo



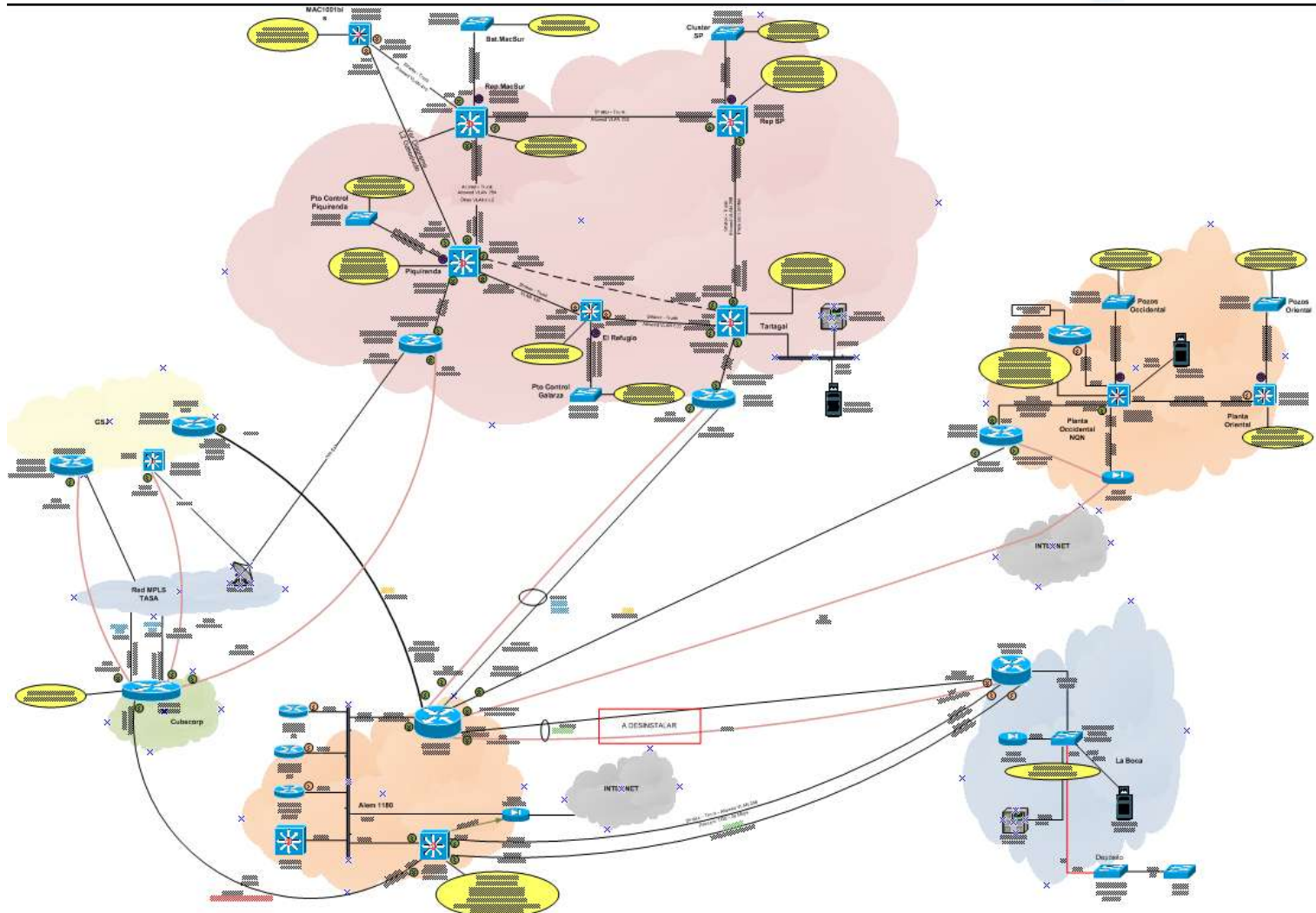
# De quién es el problema de virtualizar?

- El motivador es un requisito de seguridad
- Pero diseñar e implementar la solución es un problema de ingeniería de redes
- Hecha la reingeniería, el área de Seguridad Informática puede montar las políticas de comunicación horizontal
- Si se reutiliza la red existente, la implementación no debería “notarse” (*la red debe seguir operando mientras va siendo migrada*)

# Visión del analista de sistemas

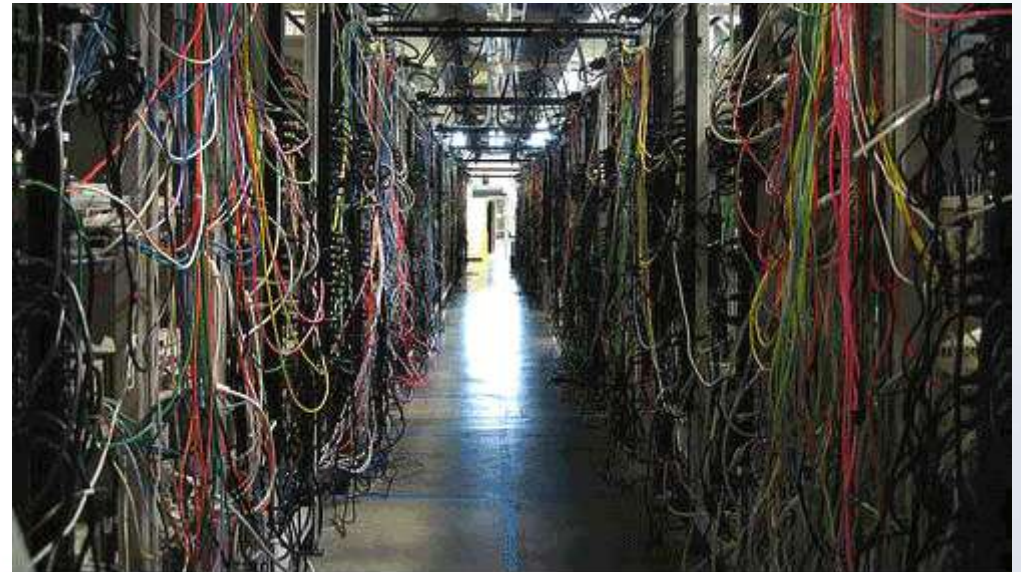


# Visión (general) del administrador de red

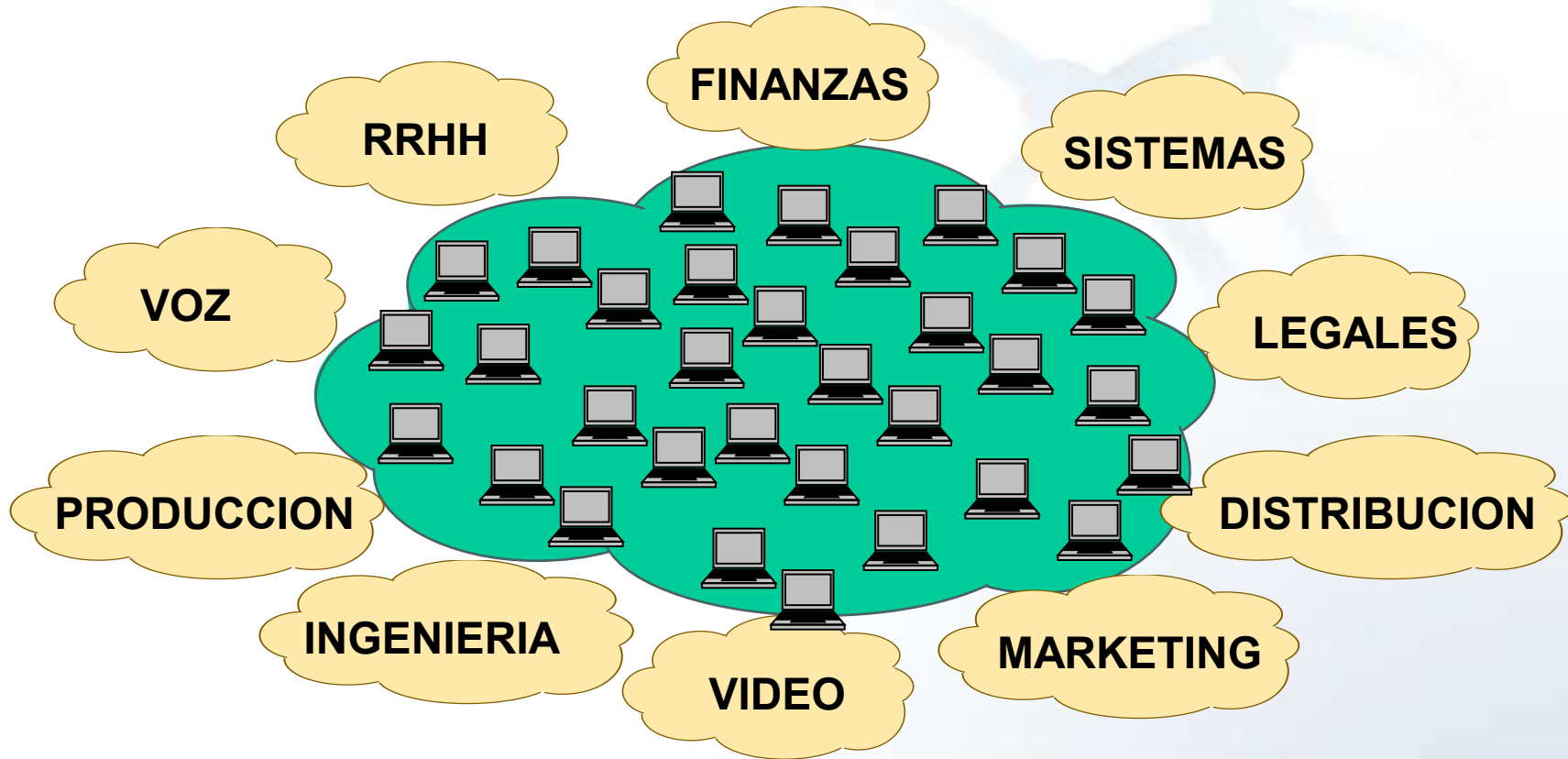




# Visión del administrador (rack)



# La visión “compartimentada”



# Objetivo final de la virtualización





**CERTuy**

 **AGESIC**



# Reingeniería asociada a una virtualización MPLS/VPN

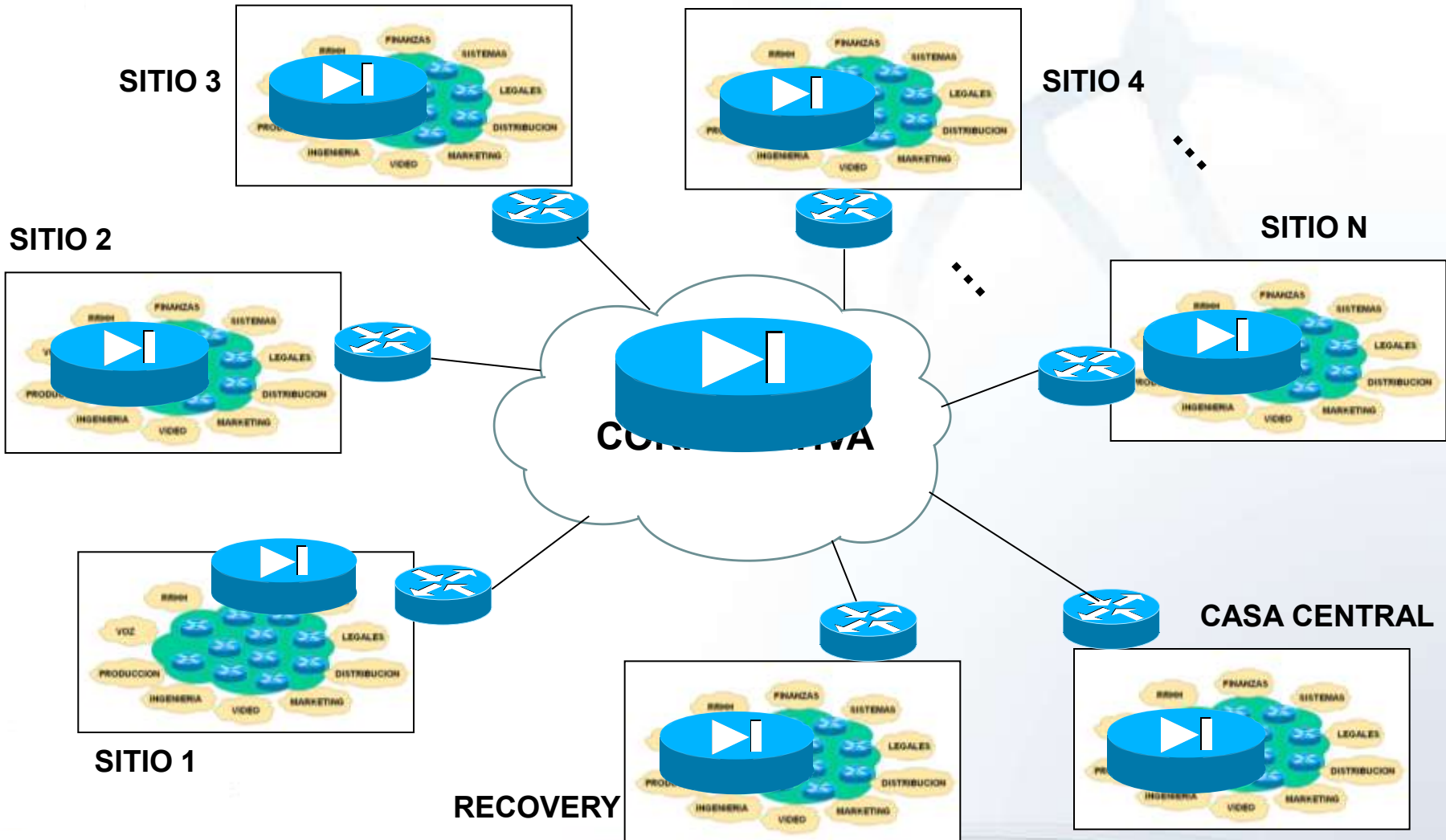


CCIE, CCSP y CSCI son marcas  
registradas de Cisco Systems, Inc

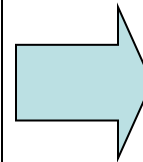
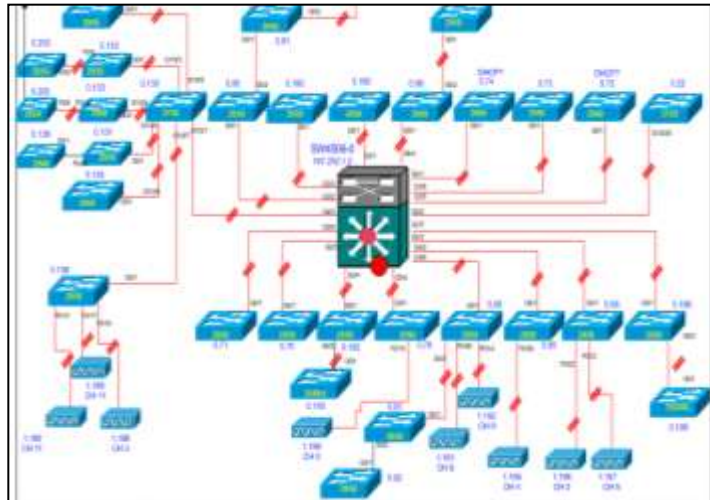
# Estrategia de la solución

- **Pensar a las LANs corporativas como estructuras de una o más VPNs**
- **Definir el backbone MPLS-VPN (usualmente, la vieja WAN)**
- **Montar las VPNs sobre el nuevo backbone**

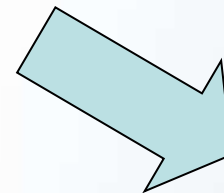
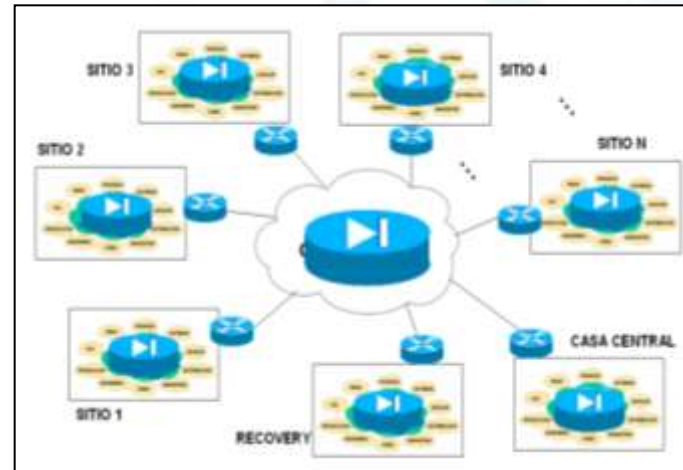
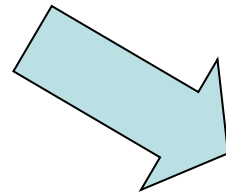
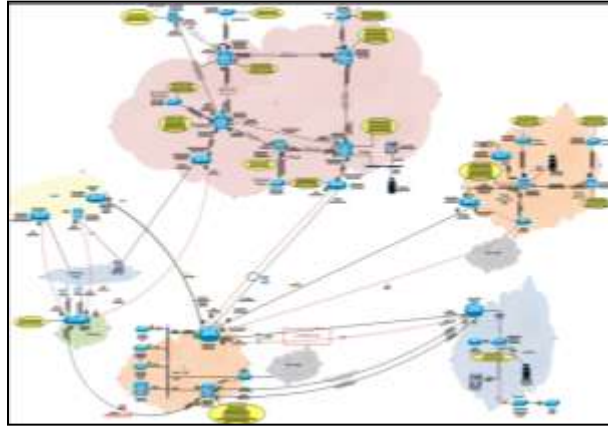
# Objetivo general



# Virtualización de sitio



# Virtualización global



# Proceso incremental de virtualización

- **Es irreal asumir que se podrá modificar la red original solicitando a los usuarios finales que dejen de usar los sistemas hasta que la red “esté lista”**
- **Se deberá ir migrando al esquema final en forma escalonada**
  - **Y tener un plan de contingencia por si algo falla**

# Etapas de la migración

- Red inicial
  - Segmentos sin migrar: 100%
  - Segmentos migrados: 0%
- Red intermedia
  - Segmentos sin migrar:  $X\%$  ( $0 < X < 100$ )
  - Segmentos migrados:  $(100 - X)\%$
- Red final
  - Segmentos migrados: 100%

***ZONA DE “DESAFÍO”***

***SEGURIDAD INFORMÁTICA ESTABLECE POLÍTICAS ENTRE VPNs***

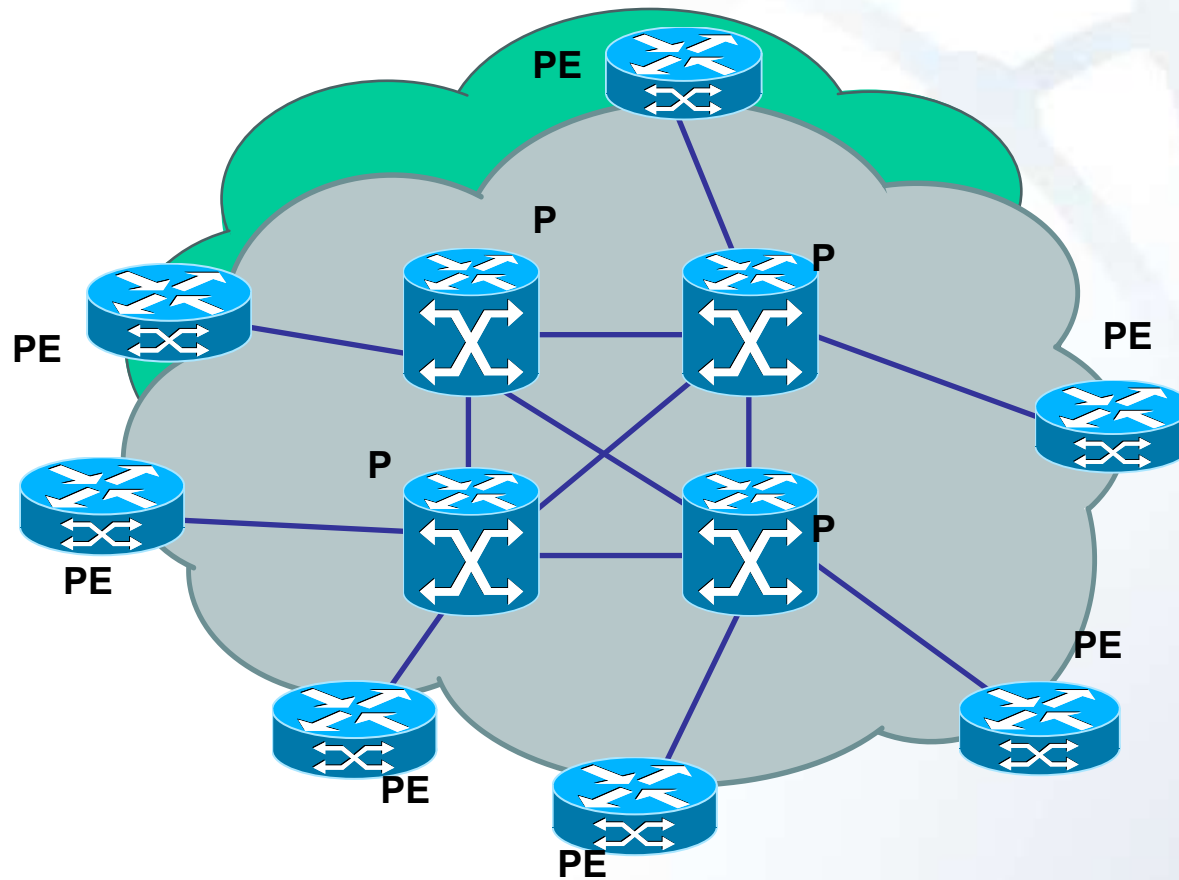
# Interoperabilidad global/virtual

- **Deberá existir un bloque funcional que mantenga “unida” a la red en transición**
  - El mundo de segmentos que aún no han sido migrados
  - Los “mundos” de segmentos, donde cada uno de los cuales ya han sido asignados a su respectivas VPNs
- **Definimos a este bloque funcional como “Estructura Pivotal”**

# Principales bloques de la migración

- Definir VPNs y un mapa de asignación de segmentos de usuarios finales a las estas VPNs
- Estructurar el backbone de equipos P
- Identificar los equipos PE y activar las VRFs asociadas a las VPNs definidas
- Asegurar la interconexión iBGP entre PEs
- Migrar escalonadamente segmentos “globales” a sus respectivas VRFs
- Proporcionar (de ser necesario) conexión de nivel 3 entre las diferentes VPNs

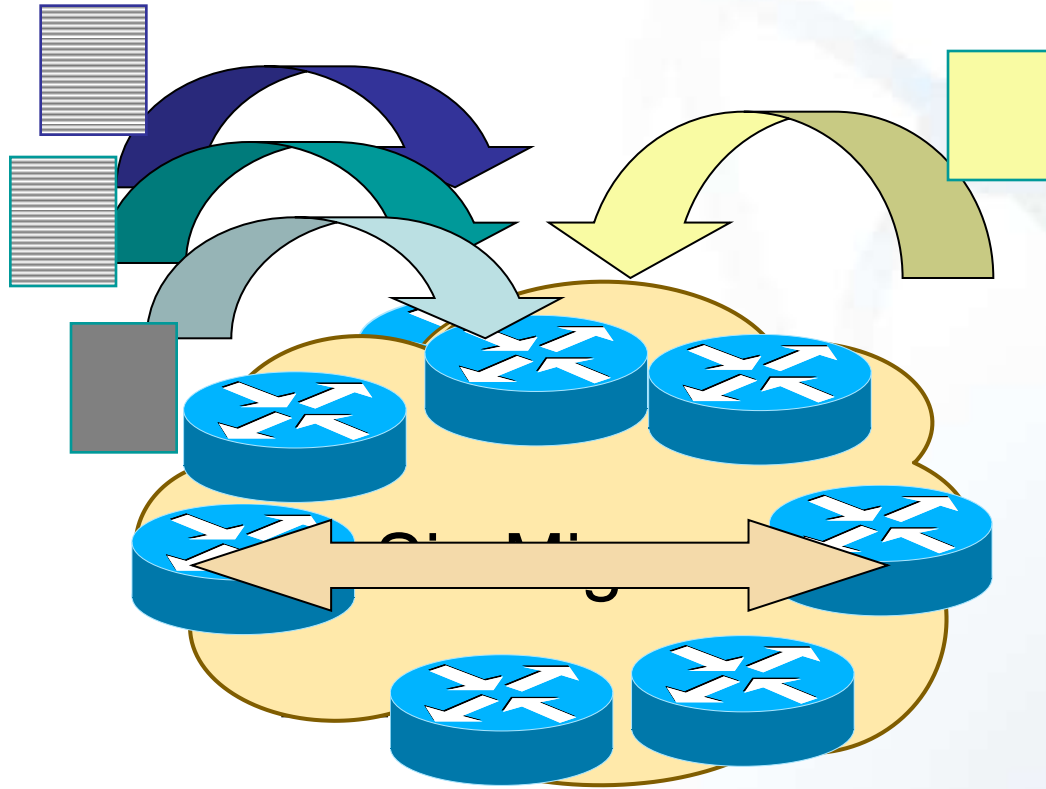
# Estructurar el backbone MPLS/VPN



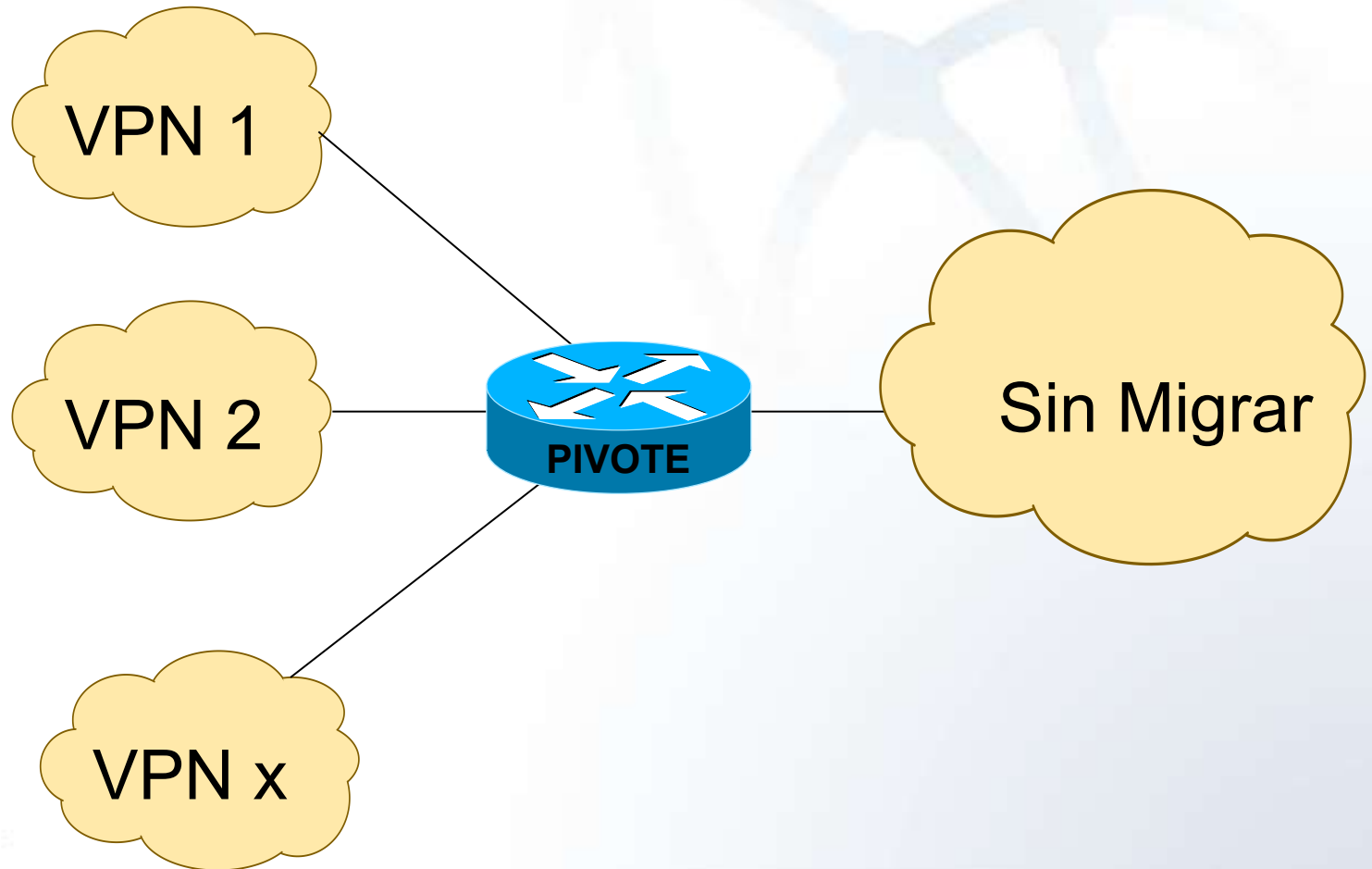
# Candidatos a equipos P y/o a PE

- Equipos “P”: aquellos que no tienen segmentos de usuarios finales directamente conectados
  - Usualmente, los routers de WAN
- Equipos PE: los que están en contacto con segmentos de usuarios finales
  - Routers con múltiples segmentos
  - Algunos fabricantes ofrecen switches de nivel 3 que pueden funcionar “casi como” un PE

# Estructuras Pivotales



# Cruce entre VPNs y redes sin migrar



# Pivote y fin de la virtualización



# El Pivote, cuando el área de Seguridad Informática toma el control



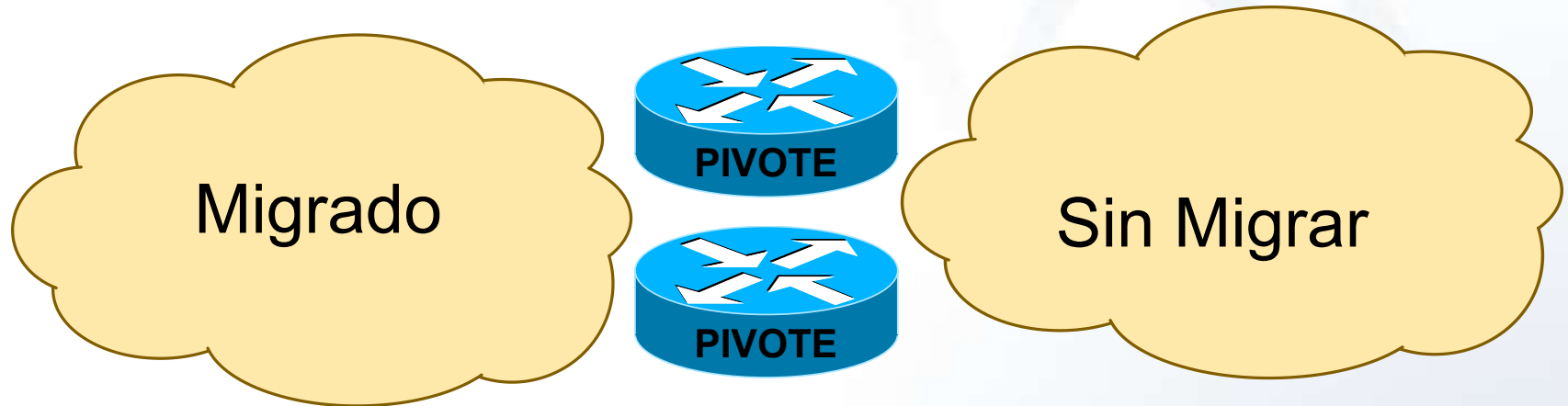
# Estructura del “Pivote”

- **Para la red de VPNs, es un “router de cliente” más**
  - **Si existen dos o más VPNs, el Pivote debe estar conectado a ellas**
  - **Se debe decidir qué VPNs deben mantenerse comunicadas entre sí o con la red “aún sin migrar”**
- **Para la red que no ha migrado, es parte de la estructura tradicional**

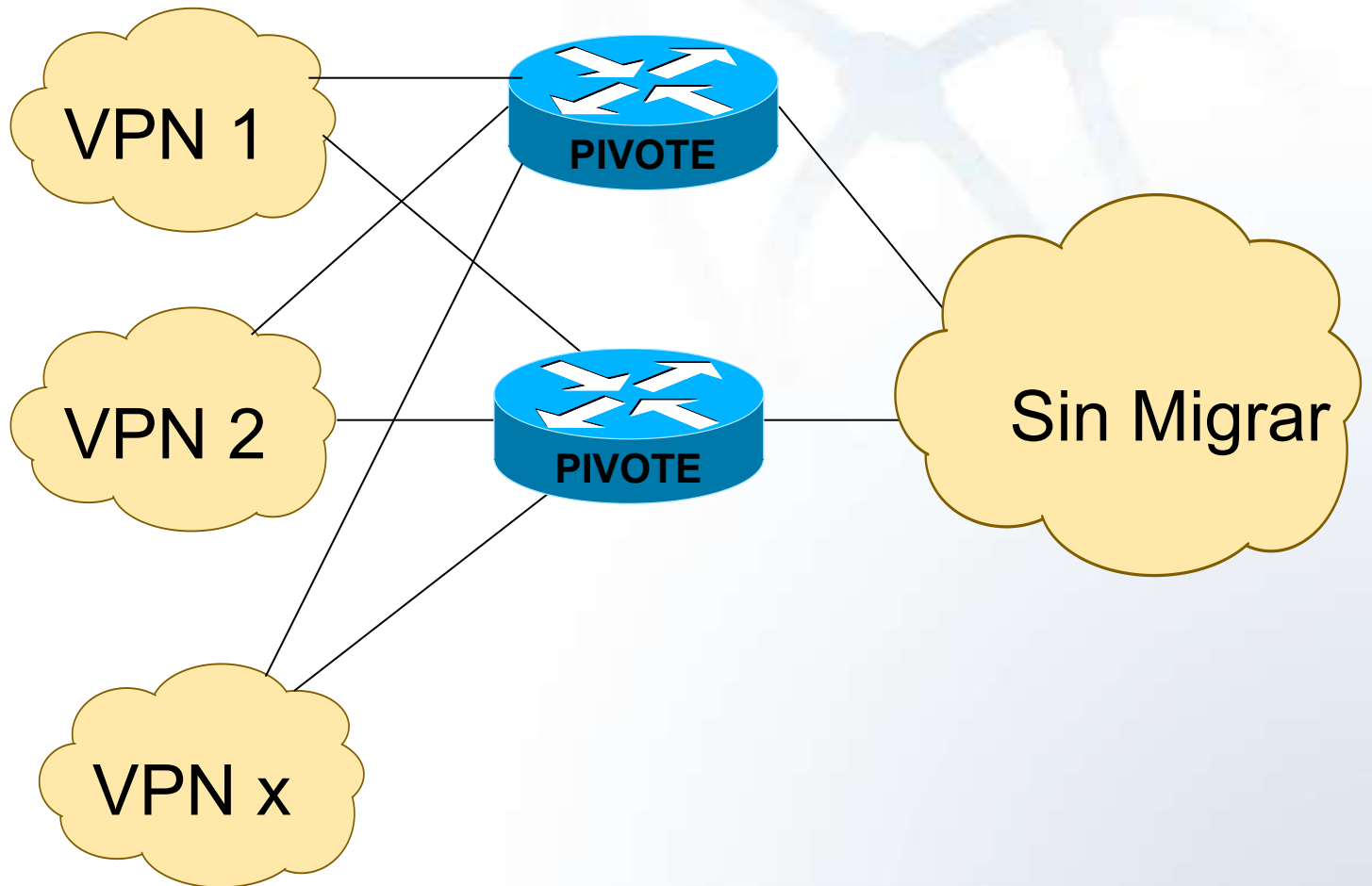
# Lógica de routing del Pivote

- Debe “aprender” las redes que han ido quedando a ambos lados de él
  - Lado “sin migrar”: proceso de routing original
  - Lado VPNs: proceso o procesos del backbone MPLS/VPN que le suministren la información de las redes que ya han migrado

# Redundancia de la función de Pivote



# Cruce de VPNs a redes sin migrar (redundancia)





**CERTuy**

 **AGESIC**



# Aspectos técnicos críticos



CCIE, CCSP y CSCI son marcas registradas de Cisco Systems, Inc

# Estructuras Pivotales: Unicast

- Se debe tener especial cuidado en evitar la generación de routing loops
- Puede ser importante mantener simetría de la comunicación
- Puede ser importante mantener linealidad de la comunicación

# Linealidad de la comunicación

- **Linealidad es garantizar el mismo camino en cada uno de los sentidos de la comunicación**
  - **Importante para aplicaciones sensibles al desorden (como las aplicaciones multimedia)**

# Simetría de la comunicación

- **Simetría es garantizar el mismo camino de ida y de vuelta para los paquetes**
  - **Fundamental si en el camino entre extremos existirán firewalls controlando la comunicación**
- **Se puede permitir cierta asimetría si se desean balancear caminos paralelos**

# Estructuras Pivotales: Multicast

- Se puede llegar a necesitar compartir grupos de IPmc entre una VPN y otra VPN
- Se puede llegar a necesitar compartir grupos de IPmc entre una VPN y una red “sin migrar”
- El Pivote debe dar cobertura a estos casos

# Soporte de Multicast sobre MPLS

- Debe consultarse al fabricante cuáles plataformas soportan este concepto, tanto a nivel backbone, como a nivel de frontera
- Usualmente, obliga a armar un backbone “iBGP” (Salvo excepciones)
- Si es necesario usar iBGP, puede mantenerse escalabilidad utilizando “Route Reflectors”

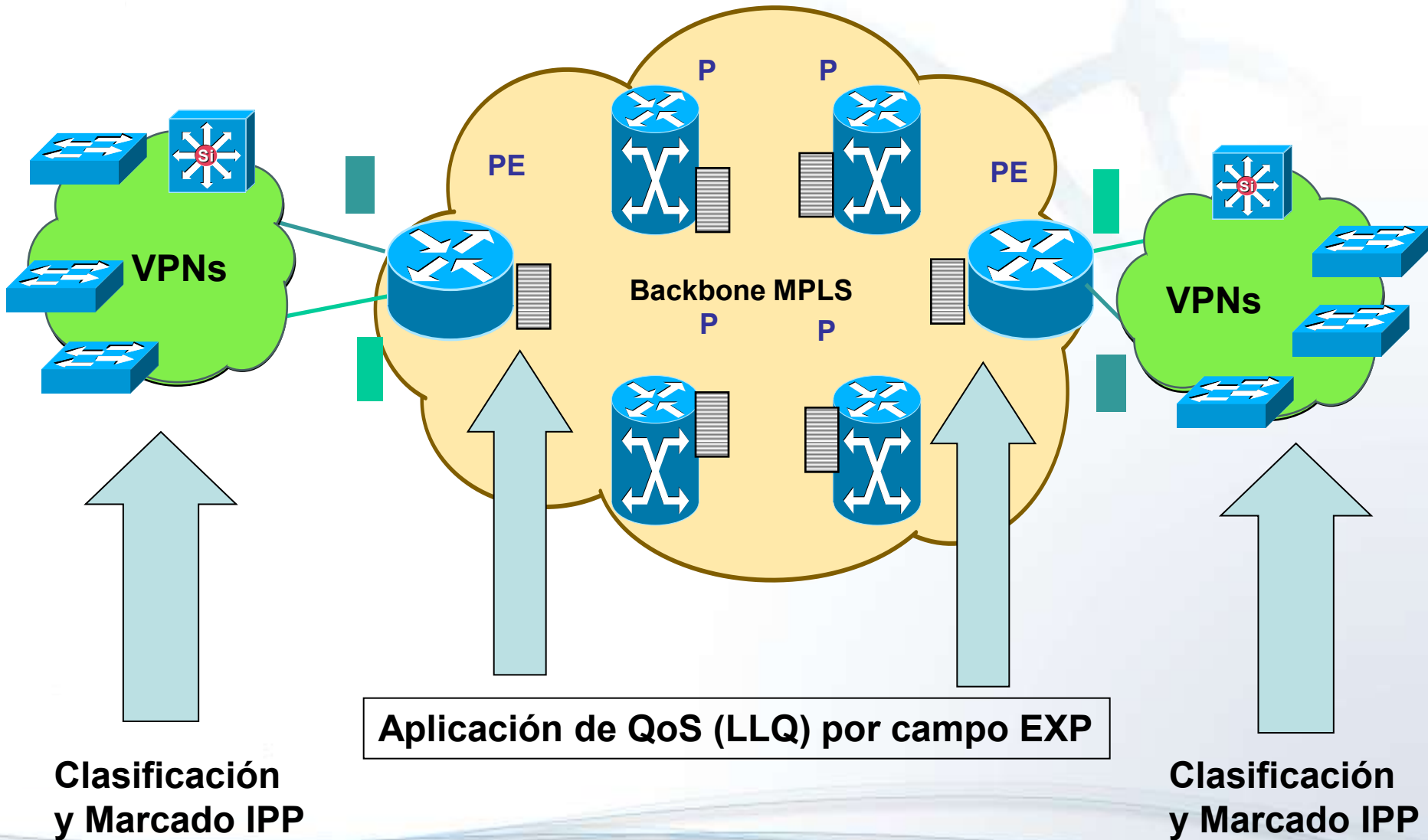
# Soporte de QoS en migración

- Políticas de QoS suelen ser activadas en los enlaces WAN
- Se basan mayoritariamente en información IP de alto nivel (TCP/UDP)
- Dejan de “funcionar” si la WAN muda a modalidad MPLS

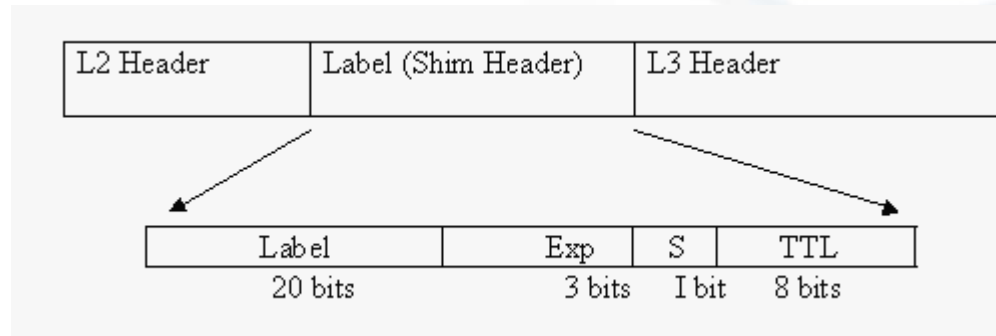
# QoS: soluciones factibles

- **Clasificar los paquetes “antes” de ingresar al backbone MPLS/VPN**
- **Marcar el campo IP Precedence o DSCP como consecuencia de la clasificación**
- **Un router “copia” el valor IPP del paquete IP al campo EXP del paquete MPLS que lo encapsula**
- **Adaptar QoS en la WAN de acuerdo al valor EXP de los paquetes MPLS**

# Políticas de QoS



# Fragmentación de paquetes



**Cada etiqueta “agranda” el paquete IP original, pudiendo llevar a fragmentarlo en ciertos enlaces**

**Este problema es frecuentemente visto en aplicaciones TCP**

**Se puede “pedir” a los routers que alteren la negociación de MSS**

# Estadísticas de una WAN MPLS

- **Netflow suele ser usado en los routers para recolectar estadística de tráfico**
- **El administrador configura Netflow para una red IP, pero el backbone pasa a ser MPLS, perdiendo la información “original”**

# Estadísticas de una WAN MPLS (soluciones en ambientes Cisco\*)

- MPLS Egress NetFlow Accounting
- MPLS-aware NetFlow

*\* No están disponibles en cualquier plataforma*

# Firewalls reemplazando a Pivotes

- Deberán intermediar entre las nuevas VPNs
- Serán puntos “sensibles” de comunicación
  - Deberían contar con redundancia
- El administrador deberá conocer las políticas esperadas entre las VPNs
  - NAT
  - Permisos
  - Restricciones
  - Routing

# Firewalls reemplazando a Pivotes

- Deberá ser “sensible” a aplicaciones que convivan en dos o más VPNs
  - Aplicaciones multimedia
  - Aplicaciones basadas en IP Multicast
- Eventualmente, podría necesitar participar a nivel “routing” con el backbone MPLS/VPN

# Servicios DHCP

**Si el servicio DHCP se brindaba desde un LAN switch que “migra” a una VPN, los pools existentes dejan de ser visibles a nivel VPN**

- **Debe proporcionarse un medio de llegada a ellos, o virtualizarlos**

# Ajustes de los sistemas de management

- Podría tener que ajustarse el sistema de management para incorporar el concepto de “VPNs”
- La red de management de routers y switches podría ser otra VPN (aunque puede permanecer global)

# Firewalls “pivotales”

- **Tantas interfaces (físicas o virtuales) como nuevas redes deban interconectar**
- **Procesos de routing, o rutas estáticas**
- **Verificar escalabilidad a nivel routing**
- **Verificar escalabilidad a nivel CPU**

## **Firewalls “pivotales” (II)**

- **Verificar la escalabilidad de la plataforma a nivel de cantidad de políticas**
- **Verificar la necesidad de IP Multicast entre dos VPNs separadas por uno o más firewalls**



**CERTuy**

 **AGESIC**



# Resumen de la metodología de migración



CCIE, CCSP y CSCI son marcas registradas de Cisco Systems, Inc

# Pasos recomendados (I)

- **Factibilidad**
  - **Análisis técnico**
  - **Maquetas de concepto**
  - **Análisis de inversión complementaria**
  - **Premisas para uso de la tecnología**
  - **Identificación de riesgos**

# Pasos recomendados (II)

## ▪ Diseño

- Definición de VPNs
- Protocolos de routing
- Pivoteo durante la migración
- Recursos corporativos comunes
- Comunicación “horizontal” (entre VPNs)
- Aplicaciones
- Calidad de Servicio
- Sistemas de management
- Integración final de firewalls

# Pasos recomendados (III)

- **Proceso de Migración**
  - **Migraciones preliminares de software en routers y switches**
  - **Protocolo de migración**
  - **Coexistencia con la red actual**
  - **Estrategias de rollback**
  - **Control de cambios**
  - **Control de calidad**
  - **Estructura de las pruebas de consistencia**

# Recursos Técnicos a involucrar

- **Staff de Networking**
  - Diseño general de la arquitectura
  - Project Management
  - Recursos de ingeniería para tareas de soporte y/o “repetitivas”
- **Staff de seguridad**
  - Responsable de firewalls

# Educación\*

- Rudimentos del protocolo BGP
- Introducción al protocolo MPLS
- Introducción al protocolo MPLS/VPN
- Desarrollo de topologías en MPLS/VPN

*\* Se asume que el staff de networking conoce los rudimentos de los protocolos de routing "interiores" y cómo usarlos en su propia red*



**CERTuy**

 **AGESIC**



**Gracias por su tiempo**



**TIÁGORA**  
coherencia en redes