

Optimización de redes de Internet

Recomendaciones y buenas prácticas

Alejandro D'Egidio – adegidio@telecentro.net.ar

Agenda

CGNAT

- Esquema general
- Características principales.
- Esquema de asignación de puertos.
- Logging.
- EIM y EIF.

Tráfico CDN

- Tráfico tradicional con CGNAT.
- Bypass CGNAT.

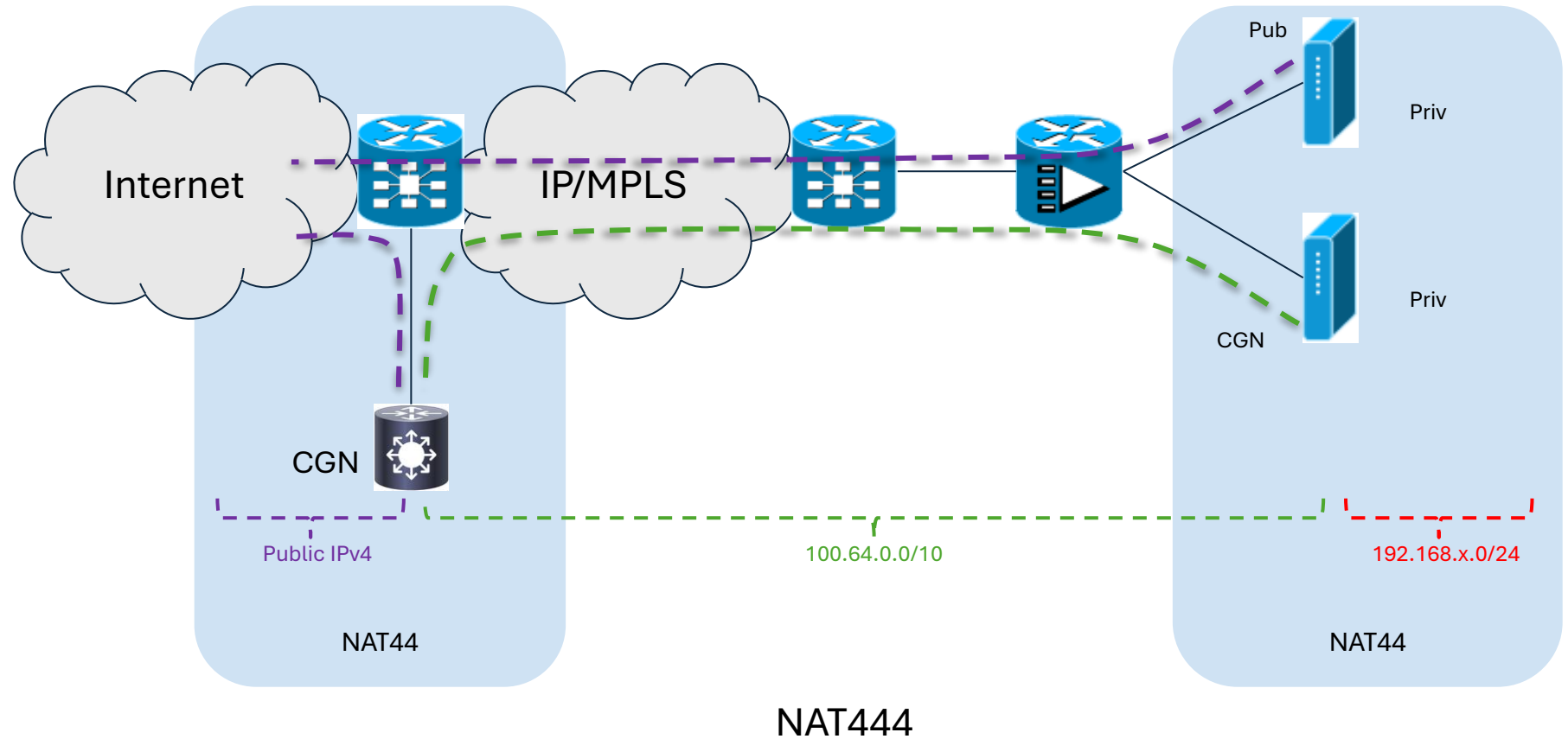
IPv6

- ¿Por qué desplegar IPv6?
- Mecanismos de transición.
- Estrategia general.

CGNAT

CGNAT – Esquema general

- Impulsado por el agotamiento de IPv4 público.
- Doble NAT44 (NAT444).
- Limitación en conectividad externa al hogar.
- Preocupaciones:
 - Rendimiento
 - Juegos
 - Ataques



CGNAT – Características principales

- Definido por:
 - RFC 6888 - Common Requirements for Carrier-Grade NATs (CGNs).
 - Esquema de asignación de puertos.
 - Logging.
 - Endpoint Independent Mapping y Endpoint Independent Filtering.
 - RFC 6598 - IANA-Reserved IPv4 Prefix for Shared Address Space.
 - 100.64.0.0/10 (4.194.304 IPs).
- Características adicionales:
 - Performance
 - Alta disponibilidad
 - Seguridad (DDoS)

CGNAT – Esquema de asignación de puertos

- Tres métodos principales:
 - Large Scale NAT
 - Deterministic NAT
 - Port Block Allocation

Característica	Large Scale NAT	Deterministic NAT	Port Block Allocation
Asignación de puertos	Dinámico	Preasignados	Bloques de puertos
Consistencia de puertos	Variable	Siempre mismos puertos	Consistente dentro de rango
Logging	Alto	Bajo	Moderado
Trazabilidad	Difícil	Fácil	Moderada
Uso de puertos	Eficiente	Poco eficiente	Moderado
Consumo de recursos	Alto	Bajo	Medio

- Consideración:
 - Pooles dinámicos
 - Cuotas

CGNAT - Logging

- Métodos:
 - Syslog
 - Flujos (Ej: Netflow)
- Fuerte impacto dependiendo de:
 - Esquema de asignación de puertos.
 - Limites de puertos/bloques/cuotas.
- Formato syslog:
 - ASCII (mayor espacio, bajo procesamiento).
 - Binario (menor espacio, alto procesamiento).
- Histórico:
 - Es recomendable guardar cierto histórico para casos legales.
 - Gran importancia en Oficios Judiciales de Riesgo de Vida.

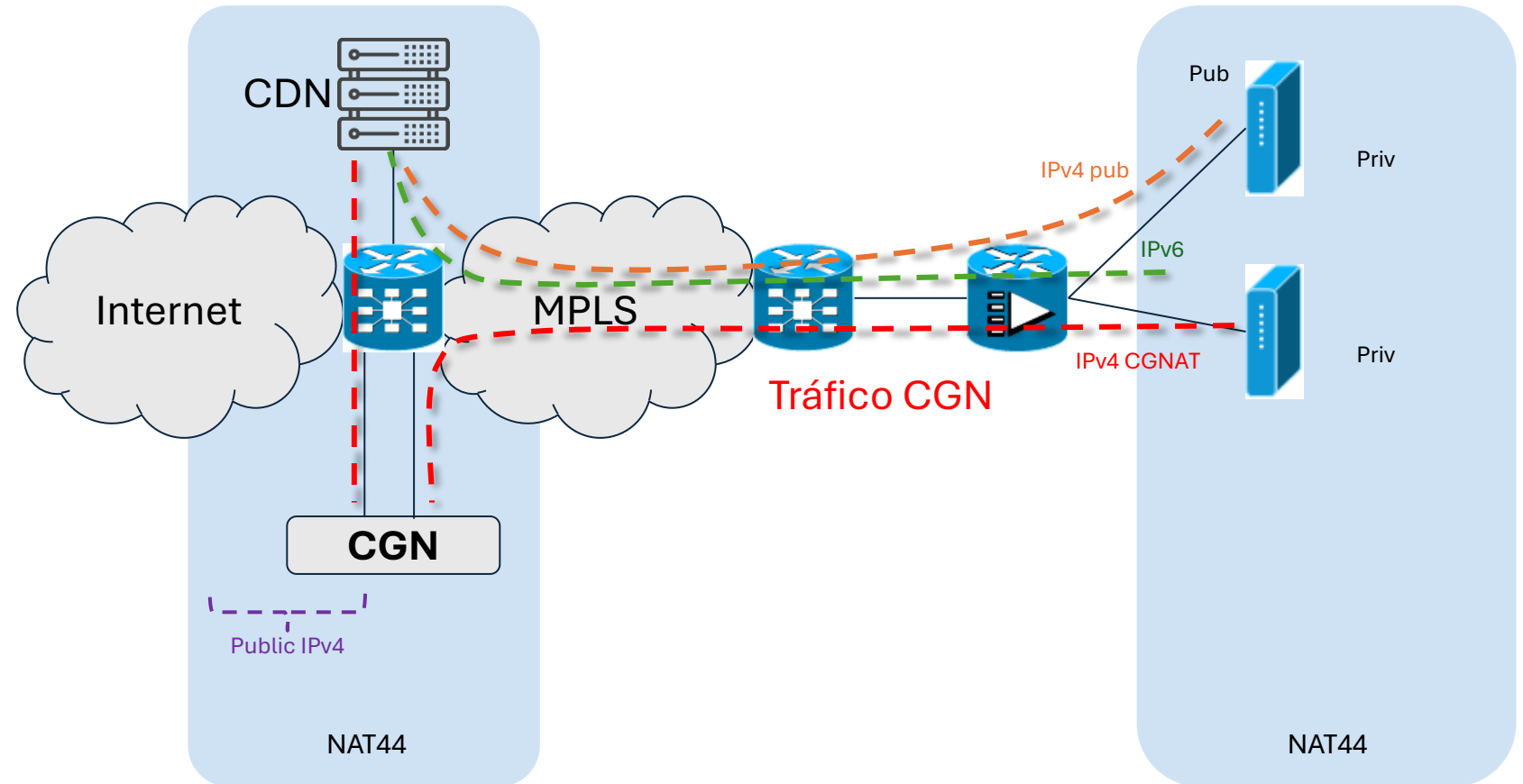
CGNAT – EIM y EIF

- Endpoint Independent Mapping:
 - Reutiliza el mapeo de puertos para próximos paquetes enviados desde la misma IP y puerto interno hacia cualquier IP y puertos externos.
- Endpoint Independent Filtering:
 - Paquetes entrantes desde endpoints externos solo son filtrados solo si su IP y puertos destino no coinciden con ningún mapeo de IP y puertos existentes.
- Un dispositivo que implemente EIM y EIF podrá aceptar tráfico entrante a cualquier IP-puerto mapeados desde cualquier endpoint externo.
- Esto es clave para plataformas de juegos.

Tráfico CDN

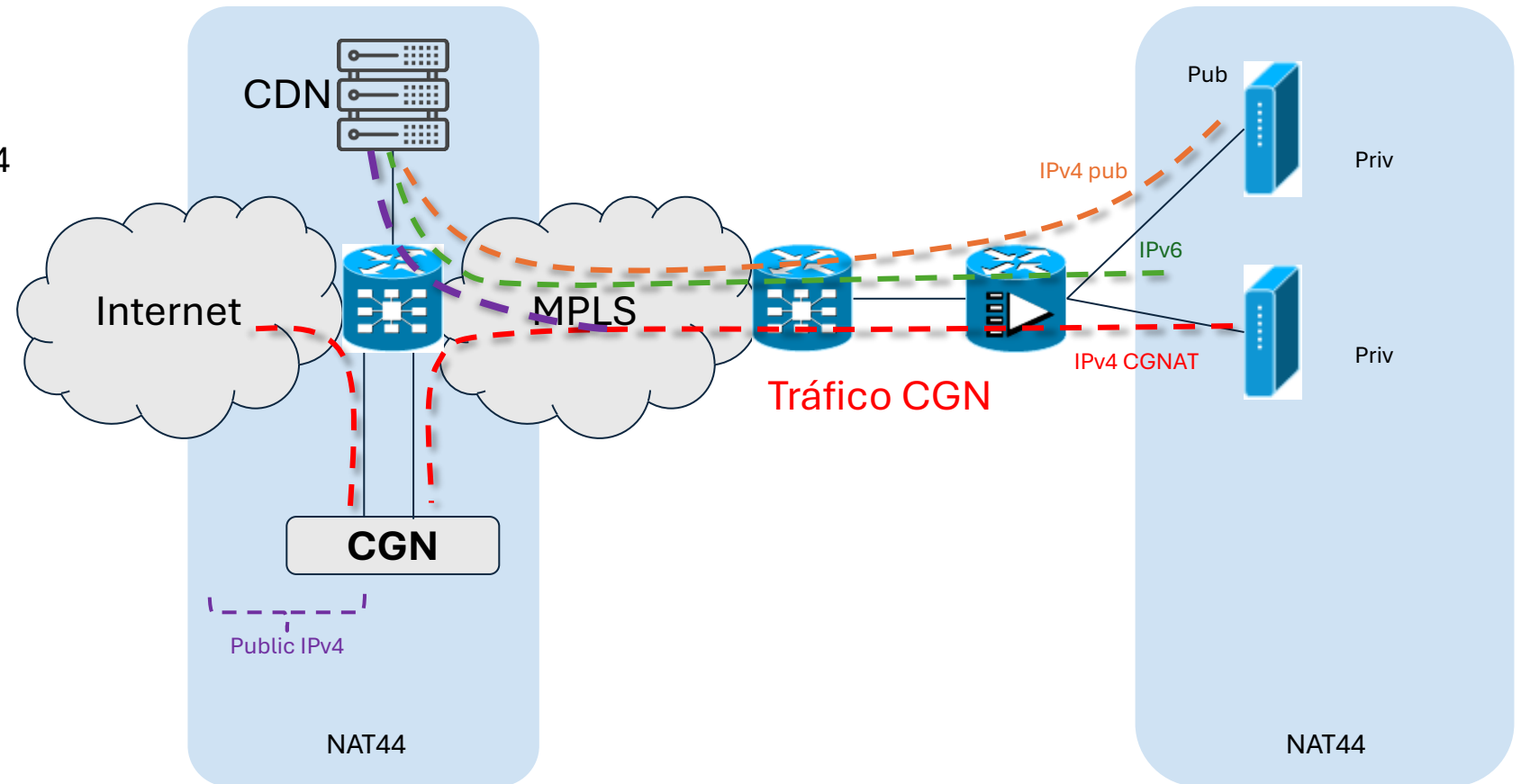
Tráfico CDN - Tráfico tradicional con CGNAT

- Ruteo eficiente con IPs públicas.
- NAT44 adicional con CGNAT.
- Incremento de costos.
- Punto de falla adicional.
- Posible disminución de rendimiento.
- Desafío → entregar contenido público dentro del ISP a Ips privadas de CGNAT.



Tráfico CDN – Bypass CGNAT

- Permite entregar contenido en IPv4 público a destino de IPv4 de CGNAT.
- Libera recursos en CGNAT.
- Mejora rendimiento.
- Reduce costos.
- Solo para servicios dentro del ISP.
- Muchas CDN's soportan esto oficialmente.



IPv6

IPv6 - ¿Por qué desplegar IPv6?

- Eficiencia
 - No hay más NAT en CPE ni en el CORE.
 - CGNAT podría reducir rendimiento.
 - Mejor rendimiento en servicios.
 - Conectividad transparente extremo a extremo.
- Costos
 - Reducción de costos en infraestructura (CGNAT).
 - No se puede eliminar el CGNAT (servicios o tecnologías IPv4).
 - Se puede lograr un 70-80% de Internet en IPv6; los contenidos y servicios de mayor volumen están en Dual Stack.
- B2B
 - Mercado exigente que debe ser atendido correctamente.

IPv6 – Estrategias para comenzar

- Capacitación a los diferentes sectores:
 - Diferentes capacitaciones según necesiten.
 - Muchas capacitaciones disponibles en LACNIC.
- Definir esquema de transición:
 - Esquema simple y con mayor compatibilidad:
 - Dual-Stack Nativo en acceso e Interconexiones.
 - Esquema de Asignación de Direcciones.
- Despliegue en la red:
 - Armar laboratorio (virtual o físico).
 - Backbone (Core, Distribución, ITXs).
 - Equipos de Acceso.
 - Puestos de trabajo.

IPv6 – Estrategias para comenzar

- Servicios de aprovisionamiento:
 - Servidor DHCPv6.
 - DNS.
 - Log de Leases.
- Homologar CPEs.
- Monitoría:
 - Tráfico IPv6 vs IPv4.
 - Servicios IPv6 vs IPv4.

IPv6 – Neighbor Discovery Protocol

- RFC 4861 - Neighbor Discovery for IP version 6 (IPv6)
- Protocolo clave para la seguridad y funcionamiento de dispositivos.
- Define el comportamiento de los dispositivos.
- Permite conocer los nodos vecinos en una LAN.
- Permite conocer los routers en una LAN.
- Está basado en ICMPv6 y direccionamiento Multicast.
- Mensajes:
 - Neighbor Solicitation (NS)
 - Neighbor Advertisement (NA)
 - Router Solicitation (RS)
 - Router Advertisement (RA)
 - Redirect

IPv6 – DHCPv6

- RFC 8415 - Dynamic Host Configuration Protocol for IPv6 (DHCPv6).
- Asigna:
 - IA_NA
 - IA_TA
 - IA_PD
 - Opciones adicionales como DNS, NTP, etc.
- Prefix Delegation (IA_PD):
 - Al no haber NAT los CPEs deben tener prefijos para asignar direccionamiento IPv6 en interfaces LAN.
 - Recomendado asignar al menos un /56 a cada CPE (256 redes /64).
 - Se espera poner una red diferente en cada interfaz LAN y WLAN.
 - Si se pone /64, el CPE debe hacer compartir ese Prefijo entre todas las interfaces LAN y no podrá subdelegar un prefijo si se coloca otro Router detrás del CPE.
 - Para B2B se asigna /48.

Conclusiones

- CGNAT:
 - No es un NAT con mayor capacidad, implica un agregado de características y protocolos adicionales.
 - No necesariamente puede generar problemas de rendimiento, si es que principalmente está correctamente configurado.
- Tráfico CDN:
 - Las CDNs entregan la mayor cantidad de tráfico.
 - Optimizar el tráfico, mejora el rendimiento y reduce costos
- IPv6:
 - No se trata de tener que implementarlo porque es lindo.
 - Implementarlo permite mejorar rendimiento y reducir costos en infraestructura.

¡Muchas gracias!

¿Preguntas?