Transporte y Ruteo Dinámico

3.1. Protocolos End-to-End

3.2. UDP

3.3. Corrección de Errores

3.4. TCP

3.5. Anycast & Multicast

3.6. Ruteo Interno

3.7. Ruteo Externo

3.8. Seguridad

3.9. DNS

EL5107 Tecnologías de Información y Comunicación

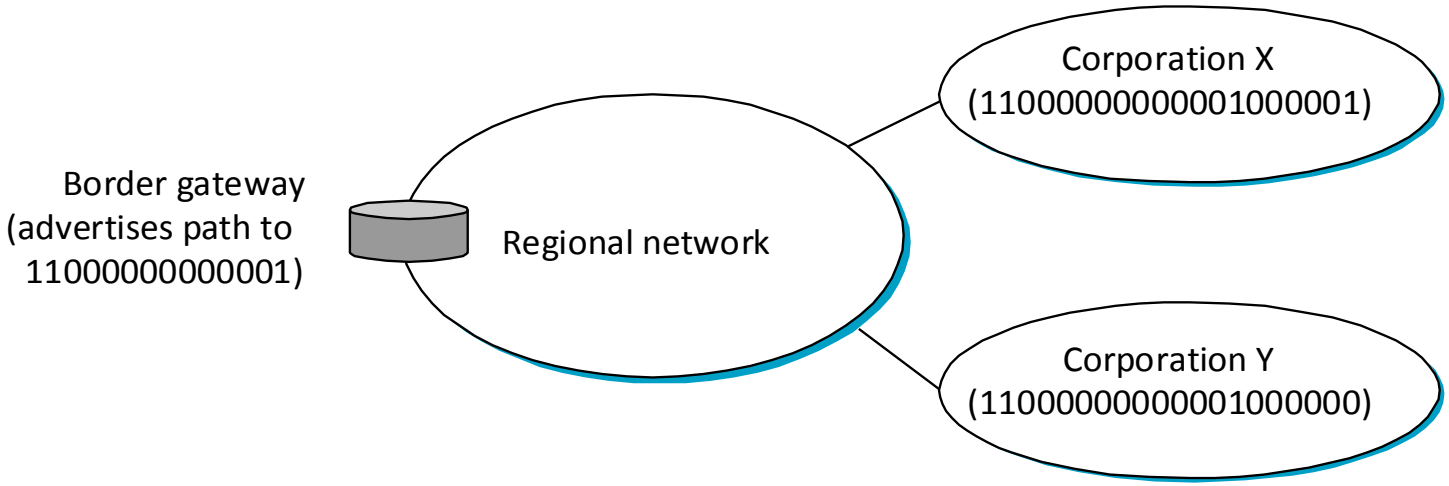
RUTEO EXTERNO

- Ruteo Externo
- Sistemas Autónomos
- BGP

Transporte y Ruteo Dinámico
3.1. Protocolos End-to-End
3.2. UDP
3.3. Corrección de Errores
3.4. TCP
3.5. Anycast & Multicast
3.6. Ruteo Interno
3.7. Ruteo Externo
3.8. Seguridad
3.9. DNS

RUTEO EXTERNO (1)

- Agregación de direcciones
  - Subnetting y supernetting



Transporte y Ruteo Dinámico

3.1. Protocolos End-to-End

3.2. UDP

3.3. Corrección de Errores

3.4. TCP

3.5. Anycast & Multicast

3.6. Ruteo Interno

3.7. Ruteo Externo

3.8. Seguridad

3.9. DNS

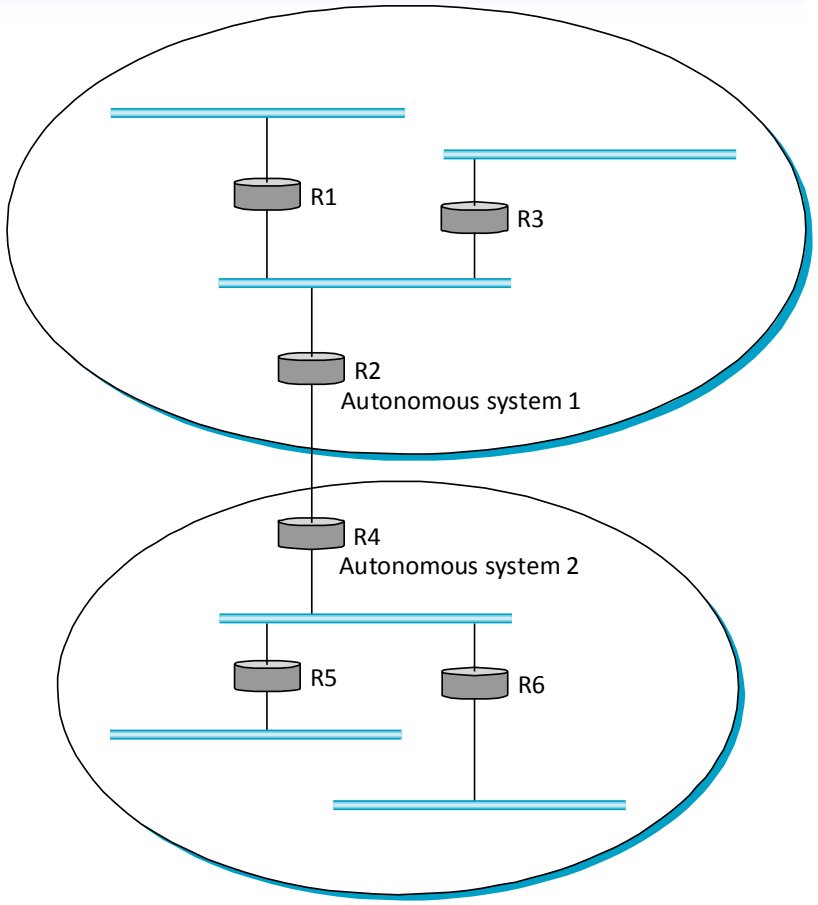
EL5107 Tecnologías de Información y Comunicación

SISTEMAS AUTÓNOMOS (1)

- Unidades bajo la misma administración, permite agregación de direcciones con el objetivo de reducir la cantidad de información global, y con ello permitir una mejor escalabilidad
- Dentro de los AS se pueden usar protocolos internos o externos (pues un AS puede contener otros AS), pero entre AS se usan protocolos externos (o de borde).

SISTEMAS AUTÓNOMOS (2)

- Una red con dos sistemas autónomos
- Protocolos de routing entre AS
  - EGP
    - Forzaba a la red a tener una topología de árbol
  - BGP
    - Actualmente en la versión 4, ampliamente usado en Internet



Transporte y Ruteo Dinámico

3.1. Protocolos End-to-End

3.2. UDP

3.3. Corrección de Errores

3.4. TCP

3.5. Anycast & Multicast

3.6. Ruteo Interno

3.7. Ruteo Externo

3.8. Seguridad

3.9. DNS

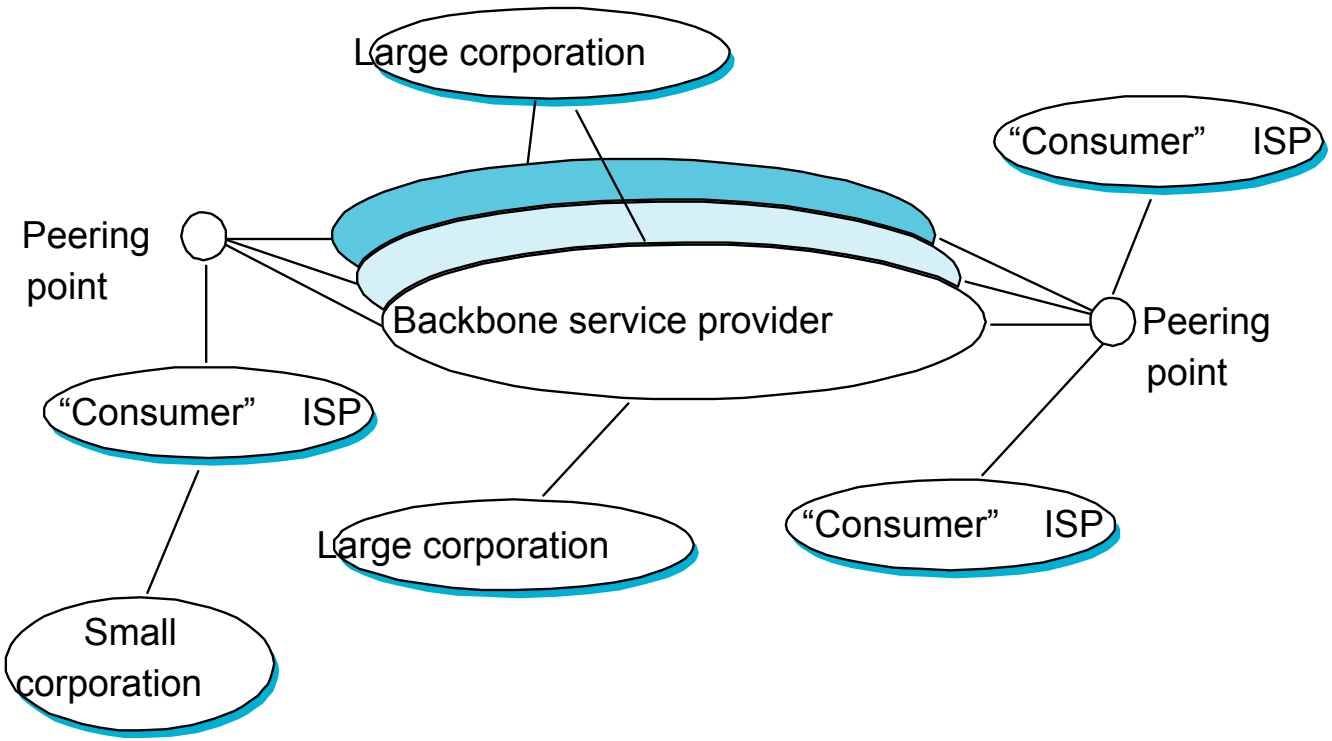
EL5107 Tecnologías de Información y Comunicación

SISTEMAS AUTÓNOMOS (3)

- Tipos de AS
  - Stub AS: Sólo tiene una conexión.
  - Multihomed AS: Tiene conexiones a más de un AS, pero no permite el tránsito de tráfico.
  - Transit AS: Tiene conexiones a más de una AS y permite que circule tráfico local y de tránsito.

SISTEMAS AUTÓNOMOS (4)

- Tipos de AS



Transporte y Ruteo Dinámico

3.1. Protocolos End-to-End

3.2. UDP

3.3. Corrección de Errores

3.4. TCP

3.5. Anycast & Multicast

3.6. Ruteo Interno

3.7. Ruteo Externo

3.8. Seguridad

3.9. DNS

BGP (1)

- Objetivo
  - Permitir encontrar cualquier camino libre de loops al destino. No se puede pretender conseguir el camino óptimo.
- Desafíos
  - Un router de “backbone” debe ser capaz de despachar cualquier paquete destinado a cualquier lugar. Por ello la información bordea las 300.000 entradas.

Transporte y Ruteo Dinámico

3.1. Protocolos End-to-End

3.2. UDP

3.3. Corrección de Errores

3.4. TCP

3.5. Anycast & Multicast

3.6. Ruteo Interno

3.7. Ruteo Externo

3.8. Seguridad

3.9. DNS

EL5107 Tecnologías de Información y Comunicación

BGP (2)

- Desafíos
  - Otros de los desafíos nace de los autonomía de cada sistema para calcular sus rutas internas. Ello no permite calcular el "costo" de un camino, por lo que sólo se anuncia la capacidad de alcanzar una red.
  - El tercer desafío involucra las políticas, pues generalmente se evita convertirse en una red de tránsito o porque se quiere privilegiar ciertos caminos para ciertos destinos.

Transporte y Ruteo Dinámico

3.1. Protocolos End-to-End

3.2. UDP

3.3. Corrección de Errores

3.4. TCP

3.5. Anycast & Multicast

3.6. Ruteo Interno

3.7. Ruteo Externo

3.8. Seguridad

3.9. DNS

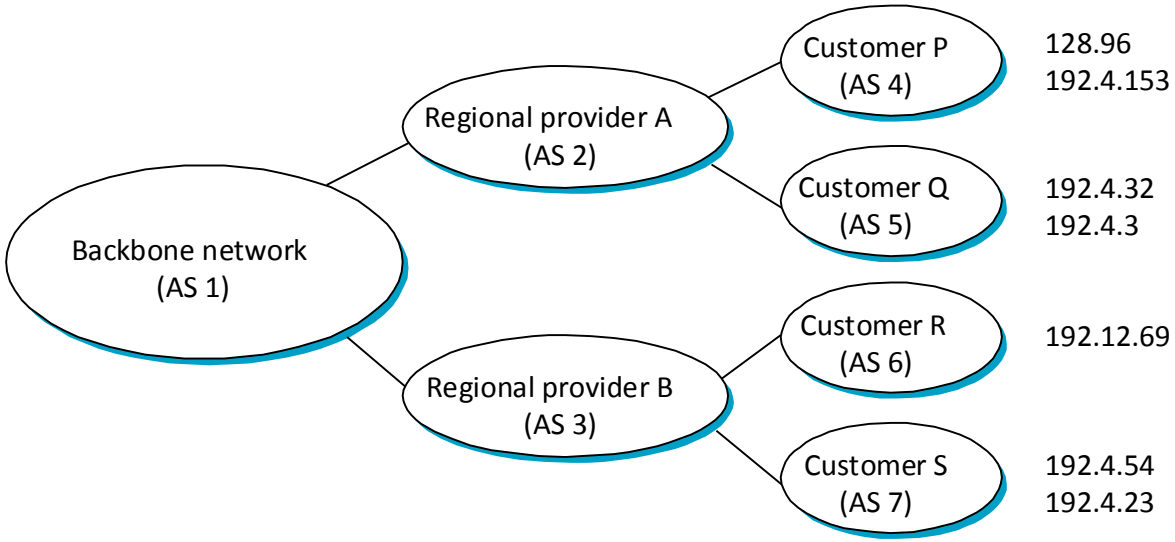
EL5107 Tecnologías de Información y Comunicación

BGP (3)

- A nivel de BGP, se habla de peers o speakers, que son routers que operan BGP y son capaces de recibir y generar anuncios.
- Éstos anuncios consisten en general en redes (número de red y máscara) más la secuencia de AS a recorrer para llegar a esos (llamados AS-Path).

BGP (4)

- Ejemplo de una red con BGP



Transporte y Ruteo Dinámico

3.1. Protocolos End-to-End

3.2. UDP

3.3. Corrección de Errores

3.4. TCP

3.5. Anycast & Multicast

3.6. Ruteo Interno

3.7. Ruteo Externo

3.8. Seguridad

3.9. DNS

BGP (5)

- Ejemplo de Los números que identifican a los AS se llaman ASN (Autonomous System Number), tienen 16 bits (65535 posibilidades).
- Estamos comenzando a usar ASN de 32 bits
- Existen ASN públicos, asignados centralizadamente tal como las direcciones IP.
- Existen ASN privados, que van del rango 64512 al 65535, y son usados por los “Stub AS”.
- BGP funciona sobre TCP.

Transporte y Ruteo Dinámico

3.1. Protocolos End-to-End

3.2. UDP

3.3. Corrección de Errores

3.4. TCP

3.5. Anycast & Multicast

3.6. Ruteo Interno

3.7. Ruteo Externo

3.8. Seguridad

3.9. DNS

BGP (6)

- Entre peers se intercambian mensajes llamados "keepalive", notificando que nada ha cambiado.
- Si un enlace o router falla, no se recibirán sus mensajes y se considerará fuera de servicio, lo que generará el recálculo de la topología.
- Hoy se considera todavía abierto el problema de rutear el Internet completo
- Ver www.caida.org

Transporte y Ruteo Dinámico

3.1. Protocolos End-to-End

3.2. UDP

3.3. Corrección de Errores

3.4. TCP

3.5. Anycast & Multicast

3.6. Ruteo Interno

3.7. Ruteo Externo

3.8. Seguridad

3.9. DNS

BGP (7)

- Dentro de un AS, los routers BGP hablan entre ellos (internal-BGP)
- Entre AS, se habla external-BGP
- Los routers hablan un protocolo de ruteo interno hacia adentro de su AS, pero no anuncian TODO lo que saben
- Cuidado con qué se anuncia y qué no hacia fuera
- Puedo querer ser red de tránsito para ciertos prefijo y para otros no

Transporte y Ruteo Dinámico

3.1. Protocolos End-to-End

3.2. UDP

3.3. Corrección de Errores

3.4. TCP

3.5. Anycast & Multicast

3.6. Ruteo Interno

3.7. Ruteo Externo

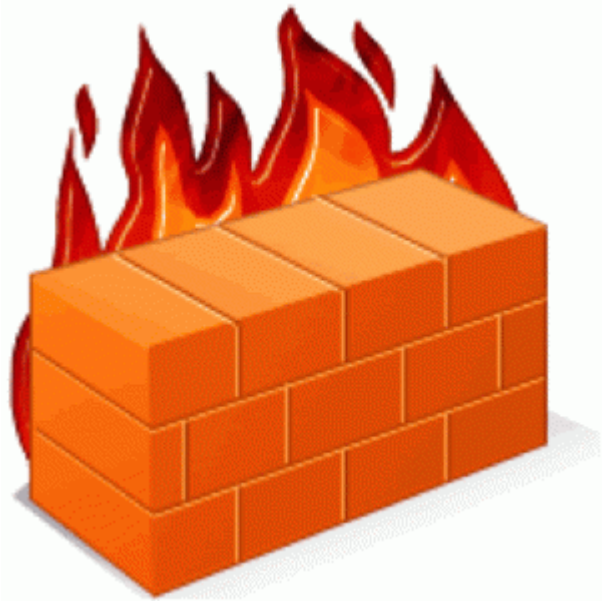
3.8. Seguridad

3.9. DNS

EL5107 Tecnologías de Información y Comunicación

SEGURIDAD

- Firewalls
- Filtro de Paquetes
- Firewalls tipo Proxy



Transporte y Ruteo Dinámico

3.1. Protocolos End-to-End

3.2. UDP

3.3. Corrección de Errores

3.4. TCP

3.5. Anycast & Multicast

3.6. Ruteo Interno

3.7. Ruteo Externo

3.8. Seguridad

3.9. DNS

EL5107 Tecnologías de Información y Comunicación

FIREWALLS (1)

- ¿Qué es un Firewall?
  - Un equipo que se usa para proteger y restringir el acceso desde y hacia computadores en una red.
  - Tiene al menos dos interfaces de red.

Transporte y Ruteo Dinámico

3.1. Protocolos End-to-End

3.2. UDP

3.3. Corrección de Errores

3.4. TCP

3.5. Anycast & Multicast

3.6. Ruteo Interno

3.7. Ruteo Externo

3.8. Seguridad

3.9. DNS

FIREWALLS (2)

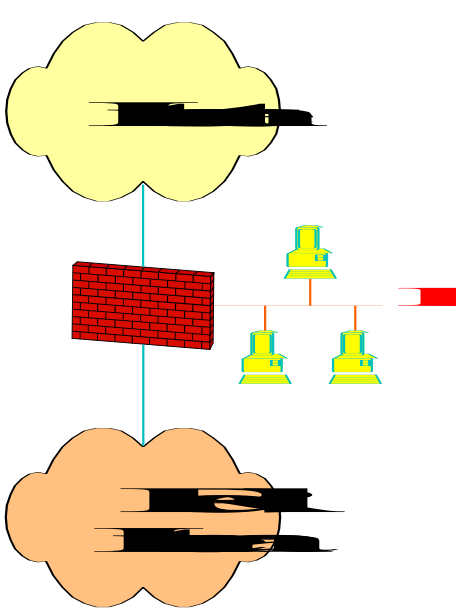
- Se necesitan porque:
  - El nivel de seguridad en los computadores es deficiente. Es imposible mantener todos los computadores con todos los parches de seguridad al día.
  - Podemos restringir tráfico por origen, destino y servicio (aplicación).
  - Sirven para restringir y controlar el tráfico entrante y el saliente.

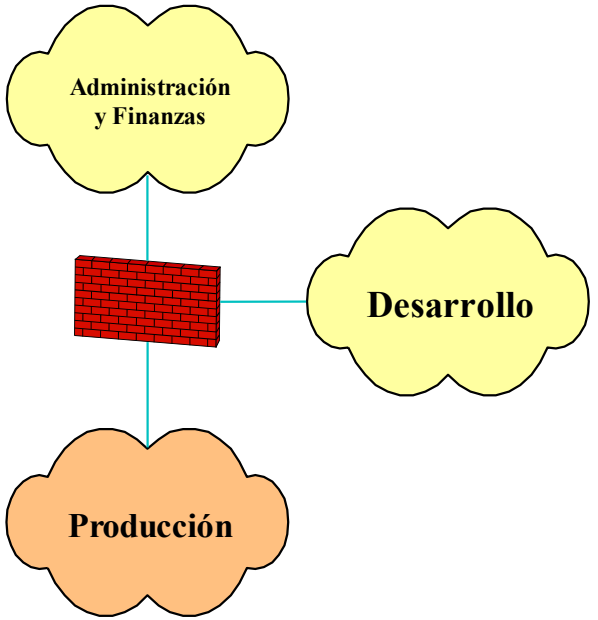
Transporte y Ruteo Dinámico
3.1. Protocolos End-to-End
3.2. UDP
3.3. Corrección de Errores
3.4. TCP
3.5. Anycast & Multicast
3.6. Ruteo Interno
3.7. Ruteo Externo
3.8. Seguridad
3.9. DNS

EL5107 Tecnologías de Información y Comunicación

FIREWALLS (3)

- ¿Dónde se Instala un Firewall?
  - A la entrada de una o más redes que deben protegerse.
  - Puede ser a la salida de Internet o entre subredes. (codelco)





Transporte y Ruteo Dinámico

3.1. Protocolos End-to-End

3.2. UDP

3.3. Corrección de Errores

3.4. TCP

3.5. Anycast & Multicast

3.6. Ruteo Interno

3.7. Ruteo Externo

3.8. Seguridad

3.9. DNS

EL5107 Tecnologías de Información y Comunicación

FIREWALLS (4)

- ¿Qué puede hacer un Firewall?
  - Definir reglas que dependan del día/hora.
    - Permitir que bajen películas después de las 20:00 L-V.
  - Autenticación de usuarios de varias formas:
    - User/password, servidor RADIUS, certificado digital, tarjeta token.
    - Autenticación transparente de usuarios.
    - Disponible para cualquier servicio IP.

Transporte y Ruteo Dinámico

3.1. Protocolos End-to-End

3.2. UDP

3.3. Corrección de Errores

3.4. TCP

3.5. Anycast & Multicast

3.6. Ruteo Interno

3.7. Ruteo Externo

3.8. Seguridad

3.9. DNS

EL5107 Tecnologías de Información y Comunicación

FIREWALLS (5)

- ¿Qué puede hacer un Firewall?
  - Traducción de direcciones IP (NAT)
    - Permite usar direcciones IP inválidas en la red interna y usar direcciones válidas al salir a Internet (RFC 1918).
    - Redes Privadas hoy son enormes
    - Direcciones internas 1-1 o n-1 con direcciones válidas.
      - Cuando la traducción de direcciones incluye traducción de puertos, se conoce como PAT o masquerading.

Transporte y Ruteo Dinámico

3.1. Protocolos End-to-End

3.2. UDP

3.3. Corrección de Errores

3.4. TCP

3.5. Anycast & Multicast

3.6. Ruteo Interno

3.7. Ruteo Externo

3.8. Seguridad

3.9. DNS

EL5107 Tecnologías de Información y Comunicación

Redes Privadas y seguridad

- Han permitido que Internet crezca casi sin usar direcciones públicas
- Pero, ¿aportan en seguridad?
- ¿Son necesarias en IPv6?
- -> Complican las fusiones de empresas con redes privadas
- -> Les encantan a los administradores de redes

Transporte y Ruteo Dinámico

3.1. Protocolos End-to-End

3.2. UDP

3.3. Corrección de Errores

3.4. TCP

3.5. Anycast & Multicast

3.6. Ruteo Interno

3.7. Ruteo Externo

3.8. Seguridad

3.9. DNS

EL5107 Tecnologías de Información y Comunicación

FIREWALLS (5)

- NAT e IPv6
  - NAT is evil
    - En Ipv6 ya no es necesario tener redes privadas
    - ¿Aporta en seguridad?
    - ¿Daña la funcionalidad?

Transporte y Ruteo Dinámico

3.1. Protocolos End-to-End

3.2. UDP

3.3. Corrección de Errores

3.4. TCP

3.5. Anycast & Multicast

3.6. Ruteo Interno

3.7. Ruteo Externo

3.8. Seguridad

3.9. DNS

FIREWALLS (6)

- ¿Qué puede hacer un Firewall?
  - Soporta H.323, FTP y otros protocolos donde la dirección IP del cliente se envía al servidor.
  - Inspección de contenido
    - Antivirus, bloqueo de applets, Java, ActiveX, …
  - Interfaz gráfica o vía browser
    - Administradores read-only vs. read/write.
    - Administración de múltiples firewalls centralizadamente.

Transporte y Ruteo Dinámico

3.1. Protocolos End-to-End

3.2. UDP

3.3. Corrección de Errores

3.4. TCP

3.5. Anycast & Multicast

3.6. Ruteo Interno

3.7. Ruteo Externo

3.8. Seguridad

3.9. DNS

EL5107 Tecnologías de Información y Comunicación

FIREWALLS (7)

- ¿Qué puede hacer un Firewall?
  - Alta disponibilidad
    - Permite configurar dos firewalls en paralelo en modo activo-pasivo que se mantienen sincronizados.
    - En algunos fabricantes en modo activo-activo (balanceo de carga).
  - Genera log para auditoría con software de terceros.
  - Administración de tráfico.
  - Integración de gateway VPN (IPSec)

Transporte y Ruteo Dinámico

3.1. Protocolos End-to-End

3.2. UDP

3.3. Corrección de Errores

3.4. TCP

3.5. Anycast & Multicast

3.6. Ruteo Interno

3.7. Ruteo Externo

3.8. Seguridad

3.9. DNS

FIREWALLS (8)

- Implementación
  - Hardware especializado
    - Sistema operativo propietario
    - Sin disco duro ni memoria virtual
    - No corre otros procesos ni servicios
    - Ejemplos: Checkpoint Firewall-1, Cisco PIX.
  - Software comercial sobre un servidor
    - Sistema operativo comercial (Windows, Unix) o Linux.
    - Ejemplos: ZoneAlarm, Norton Internet Security, Kerio Personal Firewall. Iptables, ipchains o ipforward en Linux. Ipfw en *BSD.

Transporte y Ruteo Dinámico

3.1. Protocolos End-to-End

3.2. UDP

3.3. Corrección de Errores

3.4. TCP

3.5. Anycast & Multicast

3.6. Ruteo Interno

3.7. Ruteo Externo

3.8. Seguridad

3.9. DNS

FIREWALLS (9)

- Implementación
  - Combinación hardware + software
    - Bundle de hardware con sw de firewall cargado en flash.
    - Corre algún sistema operativo jibarizado (Linux, BSD)
    - Switch de alto rendimiento con un firewall externo.

Transporte y Ruteo Dinámico

3.1. Protocolos End-to-End

3.2. UDP

3.3. Corrección de Errores

3.4. TCP

3.5. Anycast & Multicast

3.6. Ruteo Interno

3.7. Ruteo Externo

3.8. Seguridad

3.9. DNS

FILTRO DE PAQUETES(1)

- Permite especificar cuáles paquetes pueden pasar y cuáles no pueden pasar por el filtro. Tienen un conjunto de reglas (conocidas como ACL, Access Control List) que definen:
  - Dirección fuente, dirección destino, servicio, acción.
  - Dirección fuente o destino puede ser una dirección individual, una subred o "todos" (Generalmente se anota en la forma dirección/mascara).
  - El servicio se identifica por el puerto de origen o destino y el protocolo asociado.
  - Acción puede ser "permitir" o "denegar". En algunos casos, la acción de denegación se traduce en un rechazo y en otras en ignorancia.
- Cuando la acción es "permitir", el filtro de paquetes actúa como un router.

Transporte y Ruteo Dinámico

3.1. Protocolos End-to-End

3.2. UDP

3.3. Corrección de Errores

3.4. TCP

3.5. Anycast & Multicast

3.6. Ruteo Interno

3.7. Ruteo Externo

3.8. Seguridad

3.9. DNS

EL5107 Tecnologías de Información y Comunicación

FILTRO DE PAQUETES(2)

- Una regla por defecto al final que deniega todo:

IPorigen	PuertoOrigen	IPDestino	PuertoDestino	Protocolo	Acción	Comentario
*	*	Mail-Server	25	TCP	Permitir	SMTP
*	*	Web-Server	80	TCP	Permitir	HTTP
*	*	Web-Server	443	TCP	Permitir	HTTPS
*	*	DNS-Server	53	TCP, UDP	Permitir	DNS
Red Interna	*	*	80	TCP	Permitir	HTTP
Red Interna	*	*	443	TCP	Permitir	HTTPS
Red Interna	*	*	21	TCP	Permitir	FTP
Mail-Server	*	*	25	TCP	Permitir	SMTP
DNS-Server	*	*	53	TCP, UDP	Permitir	DNS

* * * * * denegar

- En algunos casos, esta regla por defecto permite todo.
- Hay un regla explícita que permite el retorno de los paquetes en respuesta a una conexión permitida. Generalmente es especificada como related o established.

Transporte y Ruteo Dinámico

3.1. Protocolos End-to-End

3.2. UDP

3.3. Corrección de Errores

3.4. TCP

3.5. Anycast & Multicast

3.6. Ruteo Interno

3.7. Ruteo Externo

3.8. Seguridad

3.9. DNS

FILTRO DE PAQUETES(3)

- Paquetes relacionados
  - En el caso de TCP, generalmente se aceptan aquellas conexiones originadas desde el "interior" de la red.
  - Se identifican mediante la detección de un segmento SYN.
  - Se puede permitir conexiones desde el exterior, pero sólo si se hace explícitamente.
  - En el caso de UDP, se relacionan mediante la tupla (D_{origen}, P_{origen}, $D_{destino}$, $P_{destino}$)

Transporte y Ruteo Dinámico

3.1. Protocolos End-to-End

3.2. UDP

3.3. Corrección de Errores

3.4. TCP

3.5. Anycast & Multicast

3.6. Ruteo Interno

3.7. Ruteo Externo

3.8. Seguridad

3.9. DNS

FILTRO DE PAQUETES(4)

- Procesamiento de Paquetes
  - Cuando un paquete llega al filtro:
    - Se revisa la lista de reglas en secuencia hasta encontrar una que haga match con el paquete.
    - Si se encuentra, se toma la acción correspondiente.
    - Si no se encuentra:
      - Si es un paquete de una sesión TCP establecida (respuesta de un servidor a un cliente), dejarlo pasar.
      - Si no, tomar la acción por defecto.

Transporte y Ruteo Dinámico

3.1. Protocolos End-to-End

3.2. UDP

3.3. Corrección de Errores

3.4. TCP

3.5. Anycast & Multicast

3.6. Ruteo Interno

3.7. Ruteo Externo

3.8. Seguridad

3.9. DNS

EL5107 Tecnologías de Información y Comunicación

FILTRO DE PAQUETES(5)

- Procesamiento de Paquetes
  - Como se busca el primer match con una regla, el orden de las reglas importa.
    - Por ello se recomienda colocar las reglas que habilitan servicios primero y luego una que niegue todo lo que no se acepta explícitamente.
  - La conexión TCP es directa entre el cliente y el servidor. El filtro actúa como router.

Transporte y Ruteo Dinámico

3.1. Protocolos End-to-End

3.2. UDP

3.3. Corrección de Errores

3.4. TCP

3.5. Anycast & Multicast

3.6. Ruteo Interno

3.7. Ruteo Externo

3.8. Seguridad

3.9. DNS

FILTRO DE PAQUETES(6)

- Tipos de Filtros de Paquetes
  - Stateless
    - Cada paquete de considera independiente y aislado de cualquier otro.
      - No es capaz de detectar conexiones.
      - Fueron la primera generación de firewalls
  - Stateful
    - Mantienen información de control de los paquetes, asociándolos a un flujo o conexión.
    - Los más avanzados permiten reglas mas complejas, como que un flujo no exceda cierto throughput (traffic shaper) o cierta tasa de conexiones por unidad de tiempo.

Transporte y Ruteo Dinámico

3.1. Protocolos End-to-End

3.2. UDP

3.3. Corrección de Errores

3.4. TCP

3.5. Anycast & Multicast

3.6. Ruteo Interno

3.7. Ruteo Externo

3.8. Seguridad

3.9. DNS

EL5107 Tecnologías de Información y Comunicación

FILTRO DE PAQUETES(7)

- El Problema del FTP

  - Cuando el cliente FTP quiere bajar o subir un archivo, le manda un comando al servidor FTP pidiéndole que le mande el archivo a un puerto de destino especificado en el comando:

  - El cliente FTP espera en un puerto aleatorio y la conexión que vendrá del servidor FTP. El servidor inicia la conexión.

  - ¿Cómo un filtro de paquetes puede permitir esta conexión?

Transporte y Ruteo Dinámico

3.1. Protocolos End-to-End

3.2. UDP

3.3. Corrección de Errores

3.4. TCP

3.5. Anycast & Multicast

3.6. Ruteo Interno

3.7. Ruteo Externo

3.8. Seguridad

3.9. DNS

FILTRO DE PAQUETES(7)

- El Problema del FTP
  - Existe una opción en el FTP llamada “FTP pasivo” que si el cliente y el servidor soportan, hace que el cliente siempre abra la conexión.
  - Otra solución es permitir todas las conexiones desde afuera a clientes internos a puertos > 1024 (no privilegiados).
    - Se corre el peligro de permitir conexiones de afuera que no deberían permitirse.
  - Un problema similar tienen los filtros de paquetes con X Windows (el servidor abre conexiones al cliente).

Transporte y Ruteo Dinámico

3.1. Protocolos End-to-End

3.2. UDP

3.3. Corrección de Errores

3.4. TCP

3.5. Anycast & Multicast

3.6. Ruteo Interno

3.7. Ruteo Externo

3.8. Seguridad

3.9. DNS

FILTRO DE PAQUETES(8)

- Ventajas del filtro de paquetes:
  - Barato (gratis si ya se tiene un router)
  - Soporta cualquier protocolo (servicio TCP)
- Desventajas:
  - No soporta bien FTP, X Windows y otros protocolos donde el servidor abre una conexión al cliente.
  - El filtro de paquetes usa ciclos de la CPU del router. Podría llegar a sobrecargar al router.
  - El rendimiento depende del número de reglas. La mayoría de los paquetes deberían tener un match con las primeras reglas.
  - No puede revisar contenido de los paquetes ni restringir comandos de los protocolos que pasan por él.

Transporte y Ruteo Dinámico

3.1. Protocolos End-to-End

3.2. UDP

3.3. Corrección de Errores

3.4. TCP

3.5. Anycast & Multicast

3.6. Ruteo Interno

3.7. Ruteo Externo

3.8. Seguridad

3.9. DNS

FIREWALL TIPO PROXY (1)

- Es un computador con dos o más interfaces de red que separa físicamente la red interna de la red externa (Internet).
  - No se permiten conexiones directas entre ambas redes.
  - En el firewall existen procesos que actúan como proxy para las conexiones permitidas.
  - Cuando un cliente quiere abrir una sesión TCP contra un servidor, se debe conectar al proceso proxy, quien abre otra conexión al destino final y actúa como intermediario entre las dos puntas. Este tipo de proxy se conoce como SOCKS.
  - Esto permitiría revisar el contenido de los paquetes…
  - Ejemplo: servidor proxy HTTP.

FIREWALL TIPO PROXY (2)

Transporte y Ruteo Dinámico

3.1. Protocolos End-to-End

3.2. UDP

3.3. Corrección de Errores

3.4. TCP

3.5. Anycast & Multicast

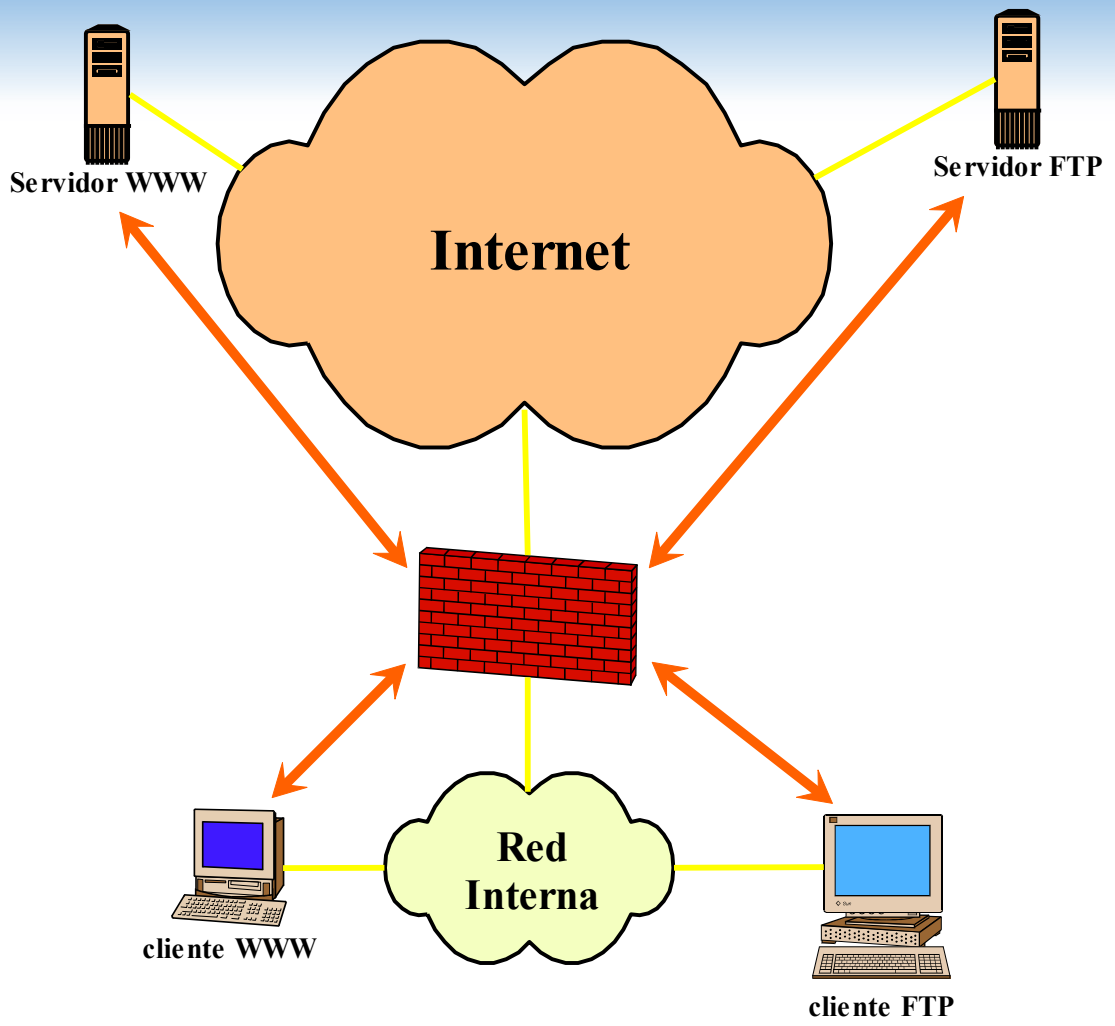
3.6. Ruteo Interno

3.7. Ruteo Externo

3.8. Seguridad

3.9. DNS

EL5107 Tecnologías de Información y Comunicación



Transporte y Ruteo Dinámico

3.1. Protocolos End-to-End

3.2. UDP

3.3. Corrección de Errores

3.4. TCP

3.5. Anycast & Multicast

3.6. Ruteo Interno

3.7. Ruteo Externo

3.8. Seguridad

3.9. DNS

FIREWALL TIPO PROXY (3)

- Ventajas
  - Permite control más fino sobre el contenido de las conexiones.
  - En una conexión FTP o HTTP o SMTP, podría restringir los comandos que se pueden ejecutar o las URLs.
  - El servidor proxy SMTP podría correr un antivirus.
  - Al no existir una conexión directa entre el equipo en la red interna y el equipo en Internet, algunos ataques no se pueden materializar.

Transporte y Ruteo Dinámico

3.1. Protocolos End-to-End

3.2. UDP

3.3. Corrección de Errores

3.4. TCP

3.5. Anycast & Multicast

3.6. Ruteo Interno

3.7. Ruteo Externo

3.8. Seguridad

3.9. DNS

FIREWALL TIPO PROXY (4)

- Ventajas
  - El servidor proxy para FTP puede capturar la dirección IP del cliente y el puerto yy que se envió al servidor FTP para permitir la conexión desde el servidor al cliente durante una cierta ventana de tiempo, lo mismo con otros protocolos que requieren que el servidor se conecte al cliente.
  - Como el cliente se conecta al firewall primero, éste puede pedir una autenticación previa a conectarse a Internet.

Transporte y Ruteo Dinámico

3.1. Protocolos End-to-End

3.2. UDP

3.3. Corrección de Errores

3.4. TCP

3.5. Anycast & Multicast

3.6. Ruteo Interno

3.7. Ruteo Externo

3.8. Seguridad

3.9. DNS

FIREWALL TIPO PROXY (5)

- Desventajas
  - Requiere cambiar las aplicaciones clientes para que soporten el uso de un proxy (no todas lo soportan).
  - Se requiere un proceso proxy por cada conexión TCP establecida, lo que puede congestionar al firewall y requiere más CPU y más memoria que un filtro de paquetes.

Transporte y Ruteo Dinámico

3.1. Protocolos End-to-End

3.2. UDP

3.3. Corrección de Errores

3.4. TCP

3.5. Anycast & Multicast

3.6. Ruteo Interno

3.7. Ruteo Externo

3.8. Seguridad

3.9. DNS

FIREWALL TIPO PROXY (6)

- Desventajas
  - Aumenta la latencia al tener que estar recibiendo paquetes, procesarlos y mandarlos por otra interface de red.
  - Sólo pueden usarse protocolos (aplicaciones) para los cuales existe un servidor proxy en el firewall.
    - Si aparece una aplicación nueva, no será soportada hasta que el proveedor del firewall desarrolle un servidor proxy para ella o provea una API para desarrollar un proxy tipo “puente” rápidamente.

Transporte y Ruteo Dinámico

3.1. Protocolos End-to-End

3.2. UDP

3.3. Corrección de Errores

3.4. TCP

3.5. Anycast & Multicast

3.6. Ruteo Interno

3.7. Ruteo Externo

3.8. Seguridad

3.9. DNS

FIREWALL TIPO PROXY (7)

- Firewalls Mixtos
  - Funcionan como filtro de paquetes para la mayoría de las aplicaciones pero tienen servidores proxy para algunas.
  - Firewall-1 tiene proxy para HTTP, FTP, SMTP, TELNET, rlogin, ping y puede interceptar cualquier servicio para que el usuario se autentique primero.
  - Así, cuando un servicio no requiere un proxy, el firewall actúa como filtro de paquetes. Cuando requiere proxy, levanta un servidor proxy para ese servicio.

Transporte y Ruteo Dinámico

3.1. Protocolos End-to-End

3.2. UDP

3.3. Corrección de Errores

3.4. TCP

3.5. Anycast & Multicast

3.6. Ruteo Interno

3.7. Ruteo Externo

3.8. Seguridad

3.9. DNS

IPTABLES (1)

- Definición
  - Según lo publicado en la página Web http://www.netfilter.org
  - IPTables es una estructura genérica de tabla para la definición de reglas. Cada regla dentro de una tabla IP consiste de un número de clasificadores (matches) y una acción (objetivo)

Transporte y Ruteo Dinámico

3.1. Protocolos End-to-End

3.2. UDP

3.3. Corrección de Errores

3.4. TCP

3.5. Anycast & Multicast

3.6. Ruteo Interno

3.7. Ruteo Externo

3.8. Seguridad

3.9. DNS

IPTABLES (2)

- Características
  - Filtro de paquetes tipo stateless para IPv4 e IPv6
  - Filtro de paquetes tipo stateful para IPv4
  - Todo tipo de NAT y NAPT
  - Infraestructura flexible y extensible
  - Etc.

Transporte y Ruteo Dinámico

3.1. Protocolos End-to-End

3.2. UDP

3.3. Corrección de Errores

3.4. TCP

3.5. Anycast & Multicast

3.6. Ruteo Interno

3.7. Ruteo Externo

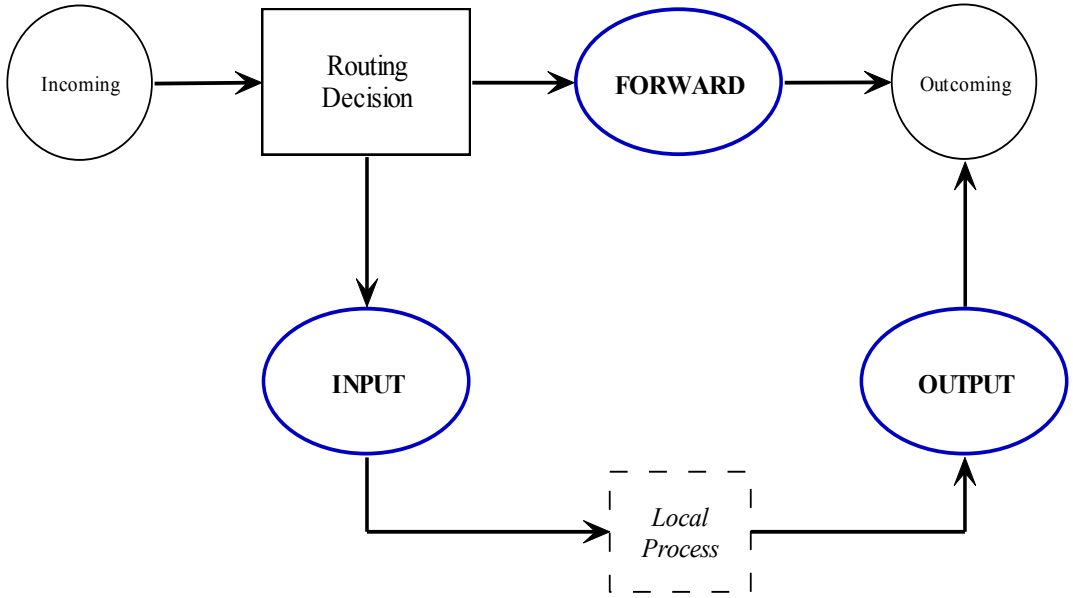
3.8. Seguridad

3.9. DNS

EL5107 Tecnologías de Información y Comunicación

IPTABLES (3)

- Cómo funciona
  - El kernel mantiene una tabla de filtrado.
  - Esta tabla tiene tres listas, llamadas cadenas (chains), que son INPUT, FORWARDING y OUTPUT.
  - Cuando un paquete entra al kernel, se procesa como sigue:



Transporte y Ruteo Dinámico

3.1. Protocolos End-to-End

3.2. UDP

3.3. Corrección de Errores

3.4. TCP

3.5. Anycast & Multicast

3.6. Ruteo Interno

3.7. Ruteo Externo

3.8. Seguridad

3.9. DNS

IPTABLES (4)

- Cada cadena es una lista de reglas.
- Cada regla especifica un “patrón” de calce para un paquete y una acción si calza. La acción puede ser que se “bote” (DROP) o que permita (ACCEPT) el paquete.
- En el caso de ésta herramienta hay que considerar que es parte del kernel y que está ligado con el proceso de forwarding IP, por lo que veamos como opera todo el conjunto.

Transporte y Ruteo Dinámico

3.1. Protocolos End-to-End

3.2. UDP

3.3. Corrección de Errores

3.4. TCP

3.5. Anycast & Multicast

3.6. Ruteo Interno

3.7. Ruteo Externo

3.8. Seguridad

3.9. DNS

EL5107 Tecnologías de Información y Comunicación

IPTABLES (5)

- Procesamiento de paquetes
  - Cuando un paquete llega por una interfaz, el kernel revisa el destino del paquete.
    - Si está destinado a “este” host, continúa su camino hacia la cadena INPUT. Si pasa la cadena INPUT, el proceso que esperaba por el paquete lo recibirá.
    - Si el kernel no tiene habilitado el “forwarding” o bien no sabe como despachar el paquete, entonces se bota. Si el forwarding estaba habilitado y el paquete está destinado a otra interfaz de red, entonces el paquete pasa a la cadena FORWARD. Si es aceptado en esa cadena, se despachará.

Transporte y Ruteo Dinámico

3.1. Protocolos End-to-End

3.2. UDP

3.3. Corrección de Errores

3.4. TCP

3.5. Anycast & Multicast

3.6. Ruteo Interno

3.7. Ruteo Externo

3.8. Seguridad

3.9. DNS

EL5107 Tecnologías de Información y Comunicación

IPTABLES (6)

- Procesamiento de paquetes
  - Finalmente, un programa ejecutando en la máquina puede enviar paquetes. Éstos paquete pasan a través de la cadena OUTPUT inmediatamente. Si es aceptado en la cadena, será despachado por la interfaz que corresponda.

Transporte y Ruteo Dinámico

3.1. Protocolos End-to-End

3.2. UDP

3.3. Corrección de Errores

3.4. TCP

3.5. Anycast & Multicast

3.6. Ruteo Interno

3.7. Ruteo Externo

3.8. Seguridad

3.9. DNS

IPTABLES (7)

- Sintaxis
  - La sintaxis general (muy simplificada para nuestro ejemplo es)
  - `Iptables -t` *`tabla comando cadena`* `definicion_regla -j` *`target`*
  - *Tabla* puede ser **nat**, **filter** o **mangle**; *comando* puede ser –A, -D, -L, -F, -I; *cadena* puede ser INPUT, OUTPUT, FORWARD; *target* puede ser ACCEPT o DROP.

Transporte y Ruteo Dinámico

3.1. Protocolos End-to-End

3.2. UDP

3.3. Corrección de Errores

3.4. TCP

3.5. Anycast & Multicast

3.6. Ruteo Interno

3.7. Ruteo Externo

3.8. Seguridad

3.9. DNS

IPTABLES (8)

- Ejemplos de ACL en un router

```
#
# Reglas que autoriza entrada de cualquier paquete que se origine
# como repuestas a una comunicación interior
#
iptables -A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
#
# Autorizo el ICMP a la red
iptables -A FORWARD -d 200.27.115.0/24 -p icmp -j ACCEPT
# Autorizo accesos a whois.nic.cl TCP (43) UDP (43)
iptables -A FORWARD -d 200.1.123.2 -p tcp -m tcp --dport 43 -j ACCEPT

# Autorizo accesos a www.nic.cl TCP (80,443,5555)
iptables -A FORWARD -d 200.1.123.3 -p tcp -m tcp --dport 80 -j ACCEPT
iptables -A FORWARD -d 200.1.123.3 -p tcp -m tcp --dport 443 -j ACCEPT
iptables -A FORWARD -d 200.1.123.3 -p tcp -m tcp --dport 5555 -j ACCEPT

# Rechazo algunos accesos
iptables -A FORWARD -p tcp -m tcp --dport 1:21 -j DROP
iptables -A FORWARD -p tcp -m tcp --dport 23:24 -j DROP
iptables -A FORWARD -p tcp -m tcp --dport 26:42 -j DROP
```

Transporte y Ruteo Dinámico

3.1. Protocolos End-to-End

3.2. UDP

3.3. Corrección de Errores

3.4. TCP

3.5. Anycast & Multicast

3.6. Ruteo Interno

3.7. Ruteo Externo

3.8. Seguridad

3.9. DNS

EL5107 Tecnologías de Información y Comunicación

IPTABLES (9)

- Ejemplos en un host final

```
# Evitamos que los mails salgan
iptables -A OUTPUT -o eth0 -p tcp --dport 25 -j DROP
# Aceptamos los ICMP
iptables -A INPUT -p icmp --icmp-type any -j ACCEPT
# Aceptamos los accesos al sitio Web
iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT
# Rechazamos todo el resto
iptables -A INPUT -j REJECT --reject-with icmp-host-prohibited
```

Transporte y Ruteo Dinámico

3.1. Protocolos End-to-End

3.2. UDP

3.3. Corrección de Errores

3.4. TCP

3.5. Anycast & Multicast

3.6. Ruteo Interno

3.7. Ruteo Externo

3.8. Seguridad

3.9. DNS

EL5107 Tecnologías de Información y Comunicación

IPTABLES (10)

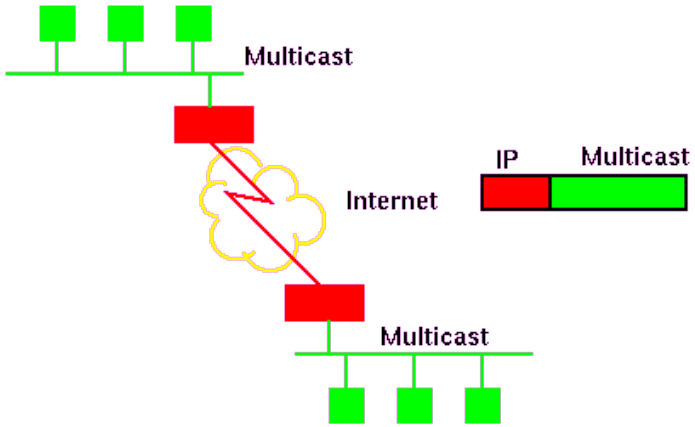
- Ejemplos de NAT

```
#
# Configuracion DNAT
#
iptables -t nat -A PREROUTING -d 200.4.121.6 -p tcp -m tcp --dport 6666 -j DNAT
--to-destination 192.168.10.1
iptables -t nat -A PREROUTING -d 200.4.121.7 -p tcp -m tcp --dport 6667 -j DNAT
--to-destination 192.168.10.11

#
# Configuro SNAT para direcciones locales como 200.1.123.1
#
iptables -t nat -A POSTROUTING -s 172.30.10.0/255.255.255.0 -d 200.27.2.2/255.255.255.255
         -o eth1 -j SNAT --to-source 192.80.24.4
# eth0
iptables -t nat -A POSTROUTING -s 172.30.10.0/255.255.255.0 -d ! 172.30.12.0/255.255.255.0
         -o eth0 -j SNAT --to-source 192.80.23.3
```

VPN (1)

- Túneles IP



Transporte y Ruteo Dinámico

3.1. Protocolos End-to-End

3.2. UDP

3.3. Corrección de Errores

3.4. TCP

3.5. Anycast & Multicast

3.6. Ruteo Interno

3.7. Ruteo Externo

3.8. Seguridad

3.9. DNS

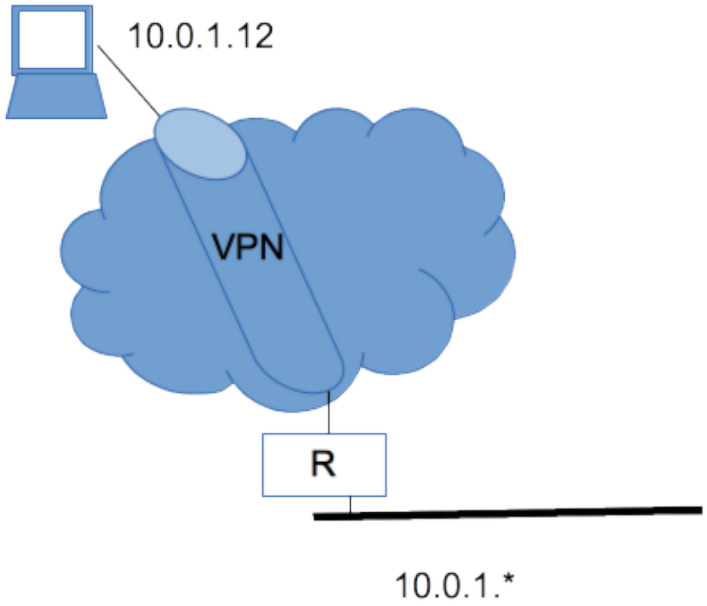
VPN (2)

- Encapsula IP sobre IP
- Funciona como un enlace punto a punto sobre Internet
- La VPN usa un túnel con el router de acceso a la red privada para poder usar una IP de la red interna
- Además, el túnel se encripta y se firma para garantizar privacidad y seguridad
- Para establecer el túnel requiero autenticarme fuertemente

Transporte y Ruteo Dinámico
3.1. Protocolos End-to-End
3.2. UDP
3.3. Corrección de Errores
3.4. TCP
3.5. Anycast & Multicast
3.6. Ruteo Interno
3.7. Ruteo Externo
3.8. Seguridad
3.9. DNS

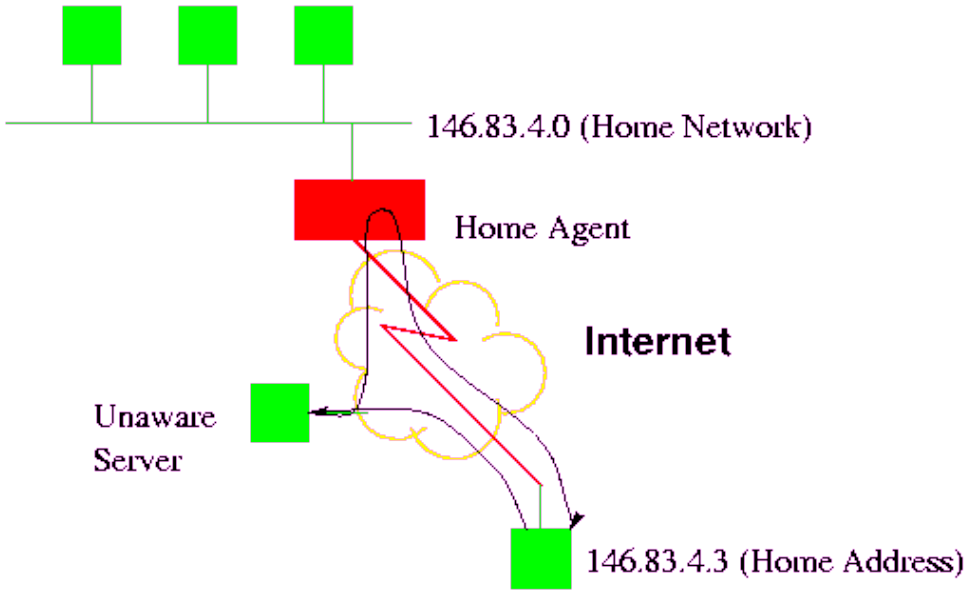
VPN (3)

- VPN



Mobile IP (1)

- Túneles IPv4



Transporte y Ruteo Dinámico

3.1. Protocolos End-to-End

3.2. UDP

3.3. Corrección de Errores

3.4. TCP

3.5. Anycast & Multicast

3.6. Ruteo Interno

3.7. Ruteo Externo

3.8. Seguridad

3.9. DNS

Mobile IP (2)

- Túneles IPv6
  - Conexión usa header de extensión: routing header
  - Permite que las respuestas del servidor viajen directo al host móvil
  - Evita el triángulo de datos con la red hogar

Transporte y Ruteo Dinámico

3.1. Protocolos End-to-End

3.2. UDP

3.3. Corrección de Errores

3.4. TCP

3.5. Anycast & Multicast

3.6. Ruteo Interno

3.7. Ruteo Externo

3.8. Seguridad

3.9. DNS

EL5107 Tecnologías de Información y Comunicación

DNS

- Árbol de Dominios
- Delegación de Autoridad
- Configuración

Transporte y Ruteo Dinámico

3.1. Protocolos End-to-End

3.2. UDP

3.3. Corrección de Errores

3.4. TCP

3.5. Anycast & Multicast

3.6. Ruteo Interno

3.7. Ruteo Externo

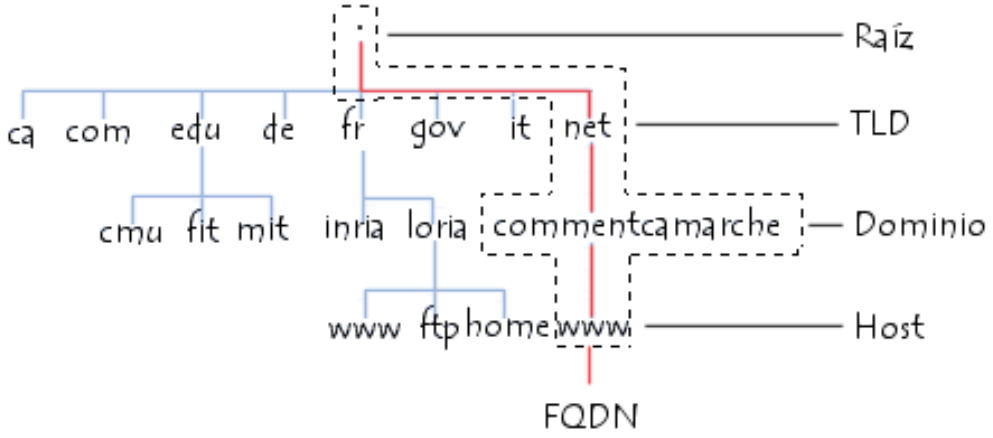
3.8. Seguridad

3.9. DNS

EL5107 Tecnologías de Información y Comunicación

ÁRBOL DE DOMINIOS (1)

- Servicio de nombres distribuido
- Redundante
- Sin administración central
- Traducción IP <-> nombre



Transporte y Ruteo Dinámico

3.1. Protocolos End-to-End

3.2. UDP

3.3. Corrección de Errores

3.4. TCP

3.5. Anycast & Multicast

3.6. Ruteo Interno

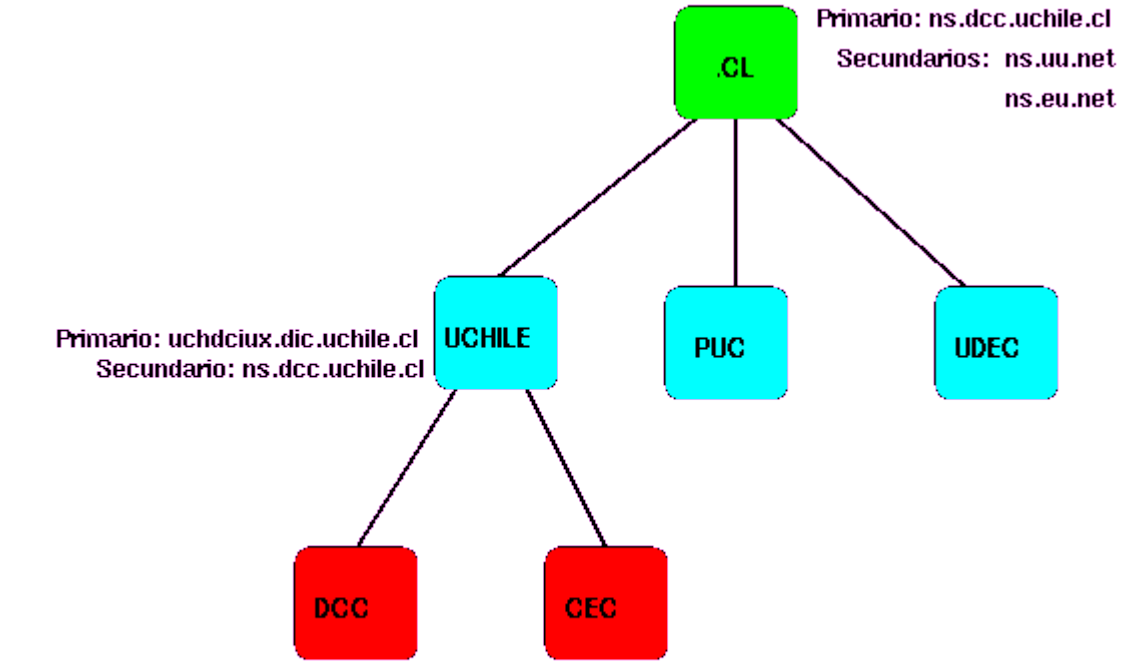
3.7. Ruteo Externo

3.8. Seguridad

3.9. DNS

EL5107 Tecnologías de Información y Comunicación

ÁRBOL DE DOMINIOS (2)



Transporte y Ruteo Dinámico

3.1. Protocolos End-to-End

3.2. UDP

3.3. Corrección de Errores

3.4. TCP

3.5. Anycast & Multicast

3.6. Ruteo Interno

3.7. Ruteo Externo

3.8. Seguridad

3.9. DNS

EL5107 Tecnologías de Información y Comunicación

DELEGACIÓN DE AUTORIDAD (1)

- Delegación de Responsabilidad.
  - Servidor Primario: actualiza .
  - Servidor Secundario: informa.
  - Servidor Cache: informa sin seguridad.
- La raíz tiene primario administrado por ICANN
- Un dominio se delega con un record NS .

Transporte y Ruteo Dinámico

3.1. Protocolos End-to-End

3.2. UDP

3.3. Corrección de Errores

3.4. TCP

3.5. Anycast & Multicast

3.6. Ruteo Interno

3.7. Ruteo Externo

3.8. Seguridad

3.9. DNS

DELEGACIÓN DE AUTORIDAD (2)

- Las preguntas bajo ese dominio son derivadas
  - Por ej: .CL, .com, etc...
- Servidor: Bind, Cliente: Resolver
- Records NS, A y MX: Nombre -> IP
- Dominio Inverso: IP -> Nombre
  - 83.146.in-addr.arpa

Transporte y Ruteo Dinámico

3.1. Protocolos End-to-End

3.2. UDP

3.3. Corrección de Errores

3.4. TCP

3.5. Anycast & Multicast

3.6. Ruteo Interno

3.7. Ruteo Externo

3.8. Seguridad

3.9. DNS

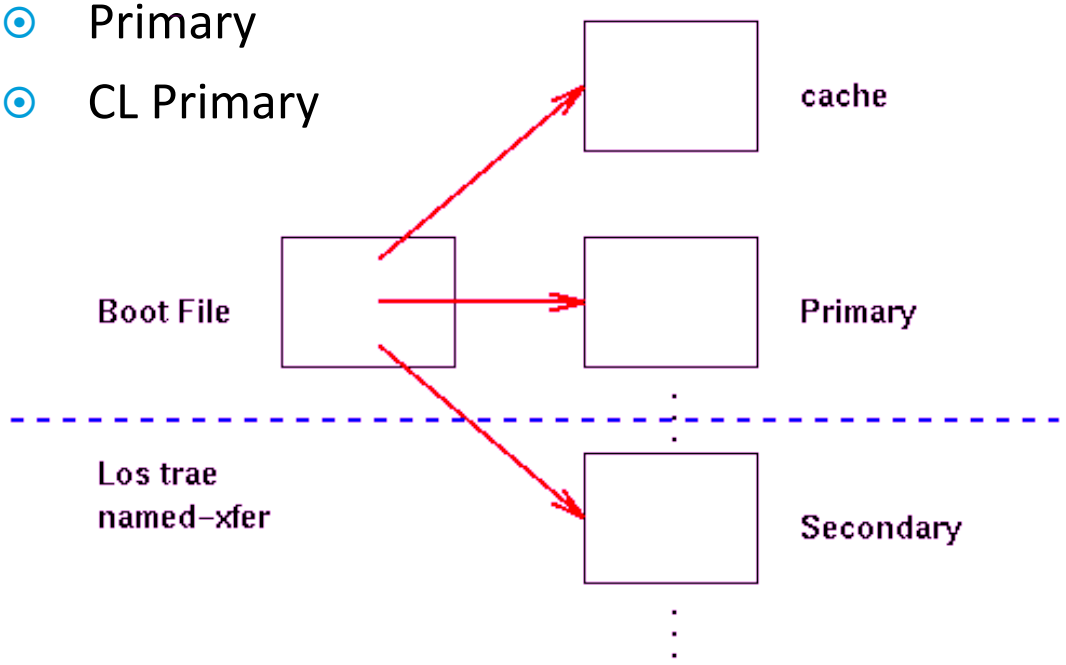
EL5107 Tecnologías de Información y Comunicación

CONFIGURACIÓN (1)

- El cliente requiere un archivo de configuración.
- El servidor requiere de un archivo de partida y un directorio para sus zonas primarias y secundarias.
- Al configurar un primario: conseguir dos secundarios.
- Definir bien los parámetros del record SOA.

CONFIGURACIÓN (2)

- Configuración del Servidor
  - Boot File
  - Cache
  - Primary
  - CL Primary



CONFIGURACIÓN (3)

Transporte y Ruteo Dinámico

3.1. Protocolos End-to-End

3.2. UDP

3.3. Corrección de Errores

3.4. TCP

3.5. Anycast & Multicast

3.6. Ruteo Interno

3.7. Ruteo Externo

3.8. Seguridad

3.9. DNS

- Boot File

```
;
; sunsite.boot : boot file for name server ns.dcc.uchile.cl
;
directory  /usr/etc/named
cache      .                        sunsite.ca
primary    cl                       cl.zone
primary    dcc.uchile.cl            dcc.uchile.cl.zone
primary    srcei.cl                 srcei.cl.zone
primary    4.83.146.in-addr.arpa    4.83.146.revzone
primary    0.0.127.in-addr.arpa     sunsite.local
;
; Secundarios para todos los subdominios de .CL
;
secondary utfsm.cl                  146.83.198.3          back/utfsm.zone
secondary rdc.cl                    146.155.30.25 146.155.1.155 back/rdc.zone
```

Transporte y Ruteo Dinámico

3.1. Protocolos End-to-End

3.2. UDP

3.3. Corrección de Errores

3.4. TCP

3.5. Anycast & Multicast

3.6. Ruteo Interno

3.7. Ruteo Externo

3.8. Seguridad

3.9. DNS

CONFIGURACIÓN (4)

- Cache

```
;
; sunsite.ca : Initial cache data for root domain servers.
;
.                       99999999  IN    NS        A.ROOT-SERVERS.NET.
                        99999999  IN    NS        H.ROOT-SERVERS.NET.
                        99999999  IN    NS        B.ROOT-SERVERS.NET.
                        99999999  IN    NS        C.ROOT-SERVERS.NET.
                        99999999  IN    NS        D.ROOT-SERVERS.NET.
                        99999999  IN    NS        E.ROOT-SERVERS.NET.
                        99999999  IN    NS        I.ROOT-SERVERS.NET.
                        99999999  IN    NS        F.ROOT-SERVERS.NET.
                        99999999  IN    NS        G.ROOT-SERVERS.NET.
;
; Prep the cache (hotwire the addresses).
;
A.ROOT-SERVERS.NET.       99999999  IN    A 198.41.0.4
H.ROOT-SERVERS.NET.       99999999  IN    A 128.63.2.53
B.ROOT-SERVERS.NET.       99999999  IN    A 128.9.0.107
C.ROOT-SERVERS.NET.       99999999  IN    A 192.33.4.12
D.ROOT-SERVERS.NET.       99999999  IN    A 128.8.10.90
E.ROOT-SERVERS.NET.       99999999  IN    A 192.203.230.10
I.ROOT-SERVERS.NET.       99999999  IN    A 192.36.148.17
F.ROOT-SERVERS.NET.       99999999  IN    A 39.13.229.241
G.ROOT-SERVERS.NET.       99999999  IN    A 192.112.36.4
```

CONFIGURACIÓN (5)

Transporte y Ruteo Dinámico

3.1. Protocolos End-to-End

3.2. UDP

3.3. Corrección de Errores

3.4. TCP

3.5. Anycast & Multicast

3.6. Ruteo Interno

3.7. Ruteo Externo

3.8. Seguridad

3.9. DNS

EL5107 Tecnologías de Información y Comunicación

- Primary

```
;
; srcei.zone : Authoritative data for srcei.cl.
;
@          IN    SOA     ns.dcc.uchile.cl. hostmaster.dcc.uchile.cl. (
                 96010214     ;Serial
                 43200        ;Refresh (12 horas)
                 7200         ;Retry   (2 horas)
                 2592000      ;Expire  (30 días)
                 43200)       ;Minimum (12 horas)

; Servidores de Nombres para srcei.cl
           IN    NS      ns.dcc.uchile.cl.
           IN    NS      inti.inf.utfsm.cl.
           IN    NS      huelen.reuna.cl.
;
$ORIGIN cl.
srcei      IN   A      164.96.124.4
$ORIGIN srcei.cl.
netscada   IN A 164.96.64.2
news       IN   CNAME srcei.cl.
*          IN   MX     10              srcei.cl.
```

Transporte y Ruteo Dinámico

3.1. Protocolos End-to-End

3.2. UDP

3.3. Corrección de Errores

3.4. TCP

3.5. Anycast & Multicast

3.6. Ruteo Interno

3.7. Ruteo Externo

3.8. Seguridad

3.9. DNS

CONFIGURACIÓN (6)

- CL Primary

```
;
; cl.zone : Authoritative data for .CL
;
@               IN      SOA     ns.dcc.uchile.CL.  hostmaster.dcc.uchile.CL. (
                                96051856        ; version (yymmddhh)
                                86400           ; refresh (1 día)
                                14400           ; retry   (4 horas)
                                2592000         ; expire  (30 días)
                                172800 )        ; minimum (2 días)
                IN      NS      ns.dcc.uchile.cl.
                IN      NS      sunsite.dcc.uchile.cl.
                IN      NS      pucmon.puc.cl.
                IN      NS      uchile.cl.
                IN      NS      ns.UU.NET.
                IN      NS      sparky.arl.mil.
                IN      NS      ns.EU.net.
                IN      NS      uucp-gw-1.pa.DEC.COM.
                IN      NS      uucp-gw-2.pa.DEC.COM.
                IN      NS      ns.cec.uchile.cl.
                IN      NS      ns.ict.uchile.cl.
; Estos los comentamos para evitar que algunos mails se vayan para USA.
;               IN      MX      100     relay1.UU.NET.
;               IN      MX      100     relay2.UU.NET.
;
; A record de parche porque no recupero la direccion IP de pucmon
pucmon.puc.cl.  IN      A       146.155.1.155
;
```

Transporte y Ruteo Dinámico

3.1. Protocolos End-to-End

3.2. UDP

3.3. Corrección de Errores

3.4. TCP

3.5. Anycast & Multicast

3.6. Ruteo Interno

3.7. Ruteo Externo

3.8. Seguridad

3.9. DNS

CONFIGURACIÓN (7)

- CL Primary (Continuación)

```
;
; Sub dominio Banco de Crédito e inversiones
; encargado: pcousin@bci.cl (Pablo Cousino)
; encargado Tecnico: rleiva@bci.cl (Raul Leiva)
;
BCI             IN      NS      rsnet.bci.cl.
                IN      NS      ns.rdc.cl.
                IN      NS      ns.dcc.uchile.cl.
                IN      MX      10 rsnet.bci.cl.
;
; Sub dominio CONICYT
; encargado wmaldona@uchcecvm.cec.uchile.cl (Waldo Maldonado)
;
CONICYT         IN      NS      daniel.conicyt.cl.
                IN      NS      uchile.cl.
                IN      NS      ns.dcc.uchile.cl.
                IN      MX      10 conicyt.cl.
;
; Sub dominio Orden Ltda.
; encargado: aaraya@tolten.puc.cl (Arnoldo Araya Flores)
;
ORDEN           IN      NS      macha.orden.cl.
                IN      NS      lapa.orden.cl.
                IN      NS      pucmon.puc.cl.
                IN      NS      ns.dcc.uchile.cl.
```

Transporte y Ruteo Dinámico

3.1. Protocolos End-to-End

3.2. UDP

3.3. Corrección de Errores

3.4. TCP

3.5. Anycast & Multicast

3.6. Ruteo Interno

3.7. Ruteo Externo

3.8. Seguridad

3.9. DNS

EL5107 Tecnologías de Información y Comunicación

CONFIGURACIÓN (8)

- Configuración de las zonas
  - SOA

Campo	Dominio (CL)	Sub-dominio (udec.cl)	sub-subdominio (dpi.udec.cl)
refresh	1 dia (86400)	18 horas (64800)	12 horas (43200)
retry	4 horas (14400)	3 horas (10800)	2 horas (7200)
expire	30 dias (259200)	30 dias (259200)	30 dias (259200)
min ttl	2 dias (172800)	1 dia (86400)	12 horas (43200)

- Errores Clásicos
- Lame Delegations
- Punto al final
- SOA mal configurado (expire, ttl)
- Pocos Servidores de nombres

Transporte y Ruteo Dinámico

3.1. Protocolos End-to-End

3.2. UDP

3.3. Corrección de Errores

3.4. TCP

3.5. Anycast & Multicast

3.6. Ruteo Interno

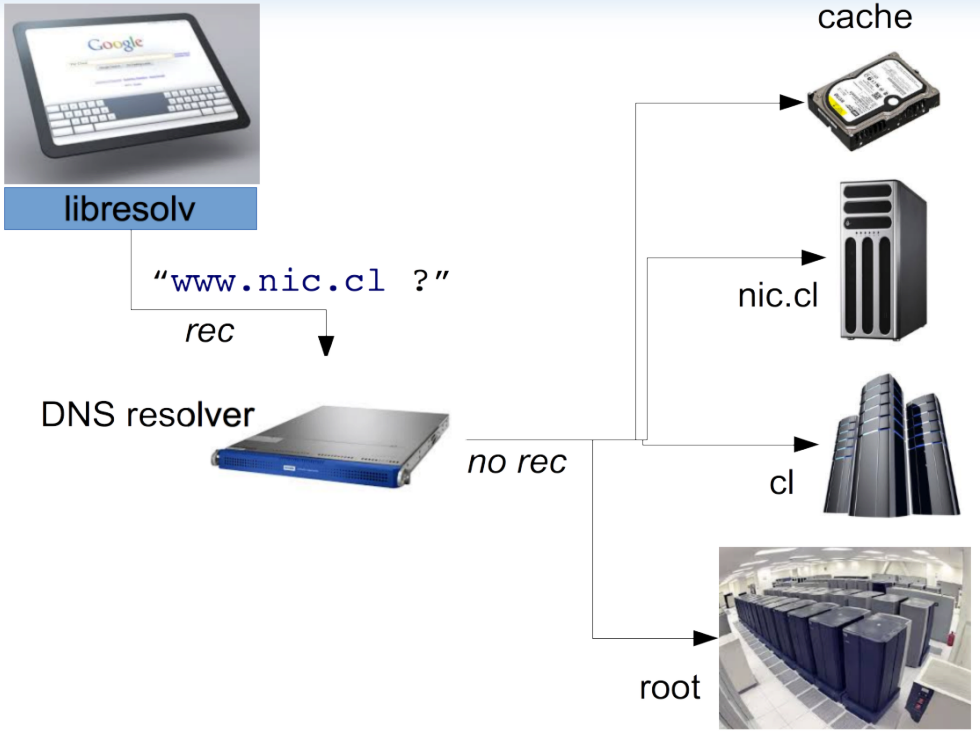
3.7. Ruteo Externo

3.8. Seguridad

3.9. DNS

EL5107 Tecnologías de Información y Comunicación

RESOLUCIÓN (1)



Transporte y Ruteo Dinámico

3.1. Protocolos End-to-End

3.2. UDP

3.3. Corrección de Errores

3.4. TCP

3.5. Anycast & Multicast

3.6. Ruteo Interno

3.7. Ruteo Externo

3.8. Seguridad

3.9. DNS

RESOLUCIÓN (2)

- Cada dominio tiene una lista de servidores (NS)
- ¿A cual le pregunto?
- Round Robin + prioridad por RTT
- Permite elegir al más rápido, distribuyendo la carga
- Los servidores modifican el orden en las listas de sus respuestas, para aleatorizar la primera pregunta

Transporte y Ruteo Dinámico

3.1. Protocolos End-to-End

3.2. UDP

3.3. Corrección de Errores

3.4. TCP

3.5. Anycast & Multicast

3.6. Ruteo Interno

3.7. Ruteo Externo

3.8. Seguridad

3.9. DNS

RESOLUCIÓN (3)

- Hoy hay servidores raíz en muchos países
- ¿De qué sirve?
- Principalmente para los errores
- ¡Que pueden ser millones por segundo!
- Usamos anycast para tener cientos de raíces
- Aunque son solo 13 IPs

RESOLUCIÓN (4)

Transporte y Ruteo Dinámico

3.1. Protocolos End-to-End

3.2. UDP

3.3. Corrección de Errores

3.4. TCP

3.5. Anycast & Multicast

3.6. Ruteo Interno

3.7. Ruteo Externo

3.8. Seguridad

3.9. DNS

.CL (1)

- Necesitamos secundarios en todo el mundo
- Pero la lista de servidores no debe ser muy larga
- Utilizamos anycast: una IP se comparte entre computadores en muchas partes del mundo
- Se usa BGP-4 para difundir todos los caminos que llevan a él
- Se simula que es uno solo, pero en realidad son muchos

.CL (2)

Transporte y Ruteo Dinámico

3.1. Protocolos End-to-End

3.2. UDP

3.3. Corrección de Errores

3.4. TCP

3.5. Anycast & Multi

3.6. Ruteo Interno

3.7. Ruteo Externo

3.8. Seguridad

3.9. DNS

EL5107 Tecnologías de Información y Comunicación

Transporte y Ruteo Dinámico

3.1. Protocolos End-to-End

3.2. UDP

3.3. Corrección de Errores

3.4. TCP

3.5. Anycast & Multicast

3.6. Ruteo Interno

3.7. Ruteo Externo

3.8. Seguridad

3.9. DNS

EL5107 Tecnologías de Información y Comunicación

.CL (3)

- Terremoto
- China / root rogue