ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

Maestría En Seguridad Informática Aplicada

"IMPLEMENTACIÓN DE UNA NUBE DE SERVIDORES DE DNS AUTORITATIVOS CON DIRECCIONAMIENTO ANYCAST DE UN PROVEEDOR DE SERVICIO DE INTERNET QUE MANTENDRÁ LA INTEGRIDAD Y LA DISPONIBILIDAD DEL SERVICIO DE RESOLUCIÓN DE NOMBRES DE DOMINIOS ANTES LOS ATAQUES DE DENEGACIÓN DE SERVICIOS O FALLOS DE HARDWARE"

EXAMEN DE GRADO (COMPLEXIVO)

Previo a la obtención del grado de:

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

JUAN JOSE COLLANTES DE LUCCA

GUAYAQUIL-ECUADOR

AÑO: 2015

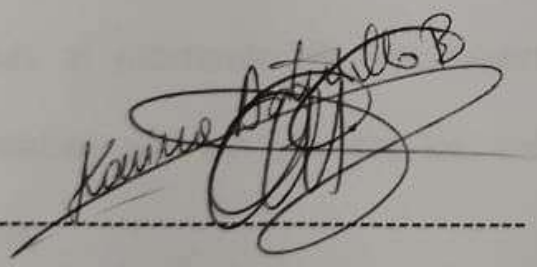
AGRADECIMIENTO

A Dios sobre toda las cosas, a mi familia por estar siempre en las buenas y en las malas brindándome su apoyo y muy en especial a la ESPOL por abrirme las puertas de su gran institución.

DEDICATORIA

A mi familia por brindarme su apoyo incondicional en el logro de mis metas profesionales, a mi hijo Juan Jose y en especial al CSE.

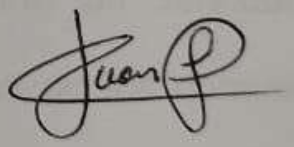
TRIBUNAL DE SUSTENTACIÓN



MGS KARINA ASTUDILLO

PROFESOR DELEGADO

POR LA SUBDECANA DE LA FIEC



ING. JUAN CARLOS GARCÍA

PROFESOR DELEGADO

POR LA SUBDECANA DE LA FIEC

RESUMEN

El presente proyecto tiene como objetivo la implementación de una solución que ayude a mantener la alta disponibilidad en el servicio de DNS Autoritativo de un ISP ante los distintos ataques de denegación de servicios (Denial of services) o fallos de Hardware.

En el capítulo 1 se describirá el problema y el principal riesgo que actualmente enfrentan los administradores de red de los proveedores de internet al momento de implementar y configurar un servidor de DNS Autoritativo que almacenara los archivos de zona de los dominios de sus clientes.

En el capítulo 2 se hace referencia a los conceptos básicos de nombres dominios, tipos de servidores de DNS, Ataques de denegación de Servicios DDOS, tipos de direccionamiento IP y el protocolo de enrutamiento BGP, luego analizaremos la topología actual del servidor de DNS autoritativo y del resto de servidores de servicios configurado en el centro de datos del proveedor de internet y finalmente se revisara el método y el procedimiento

utilizado para la configuración del Nodo DNS Anycast que servirá para mantener la alta disponibilidad del servicio de DNS.

En el capítulo 3 se revisaran y se explicarán los resultados obtenidos. Se detallará el tipo de pruebas realizadas y se presentaran las conclusiones y recomendaciones de la solución propuesta.

ÍNDICE GENERAL

ABREVIATURAS Y SIMBOLOGÍAS

BGP	Border Gateway Protocol
CCTLD	Country Code Top Level Domain
DNS	Domain Name System
DDOS	Distributed Denegation of Services
GTLD	Global Top Level Domain
HTTP	Hypertext Transfer Protocol
ISP	Internet Service Provider
SMTP	Simple Mail Transfer Protocol
TCP	Protocolo de Control de Transmisión
UDP	Protocolo de Datagrama de Usuario
VOIP	Voice over IP

ÍNDICE DE FIGURAS

INTRODUCCIÓN

El servicio de DNS es considerado como de infraestructura critica ya que la resolución de un nombre de dominio o de host es el primer paso para la conexión entre 2 dispositivos conectados en internet. Con los aumentos de ancho de banda y la facilidad de crear códigos maliciosos, los servidores de DNS, por su simplicidad de funcionamiento, son blanco fácil para los ataques de denegación de servicios.

Esta tesis pretende revisar los principales conceptos del servicio de DNS, tipos de ataques a los que está expuesto, también se revisaran conceptos de enrutamiento en internet. Se conocerá el esquema actual del servicio de DNS autoritativo que brinda el ISP para la administración de sus propios nombres de dominio y el de los clientes.

Se realizara las instalaciones del software y las configuraciones necesarias para la implementación del nodo Anycast para el servicio de DNS autoritativo del ISP. Tener un plan de pruebas que detalle paso a paso las pruebas que se deban de realizar para verificar el perfecto funcionamiento de la solución.

Se realizara pruebas en producción con dominios reales, simulando el fallo en uno de los nodos Anycast de DNS, donde se demostrara la restauración del servicio de DNS de forma inmediata.

CAPÍTULO 1

GENERALIDADES

1.1 DESCRIPCIÓN DEL PROBLEMA

El servicio de DNS Autoritativo en un ISP es considerado como de infraestructura critica ya que la resolución de los nombres de dominio del ISP y el de sus clientes, es el primer paso para la conexión de una máquina o de un usuario conectado al internet hacia otro punto o hacia un servicio brindado por los clientes del ISP.

Actualmente los servidores de DNS Autoritativos del ISP están configurados con direcciones IP públicas que son anunciadas desde un solo nodo o punto en internet, al tener esta limitante los servidores de DNS han sido los blancos preferidos por los hackers informáticos, que aprovechando la debilidad del

protocolo UDP, pueden ejecutar con facilidad un ataque de Denegación de Servicios Distribuidos DDOS y al no contar con réplicas de los servidores de DNS en otras ubicaciones (otros proveedores de internet o Puntos de Intercambio de tráfico, etc.), han traído como consecuencia, la interrupción del acceso de los usuarios a los diferentes servicios que brindan los clientes del ISP tales como http, smtp, srteaming, VoIp, aplicaciones y conexiones entre sucursales corporativas.

Otros de los principales problemas que pueden causar una interrupción en el servicio de DNS Autoritativo son los fallos del equipo causado por el desperfecto en unos de sus dispositivos de almacenamiento, tarjetas principales y fuentes de energías.

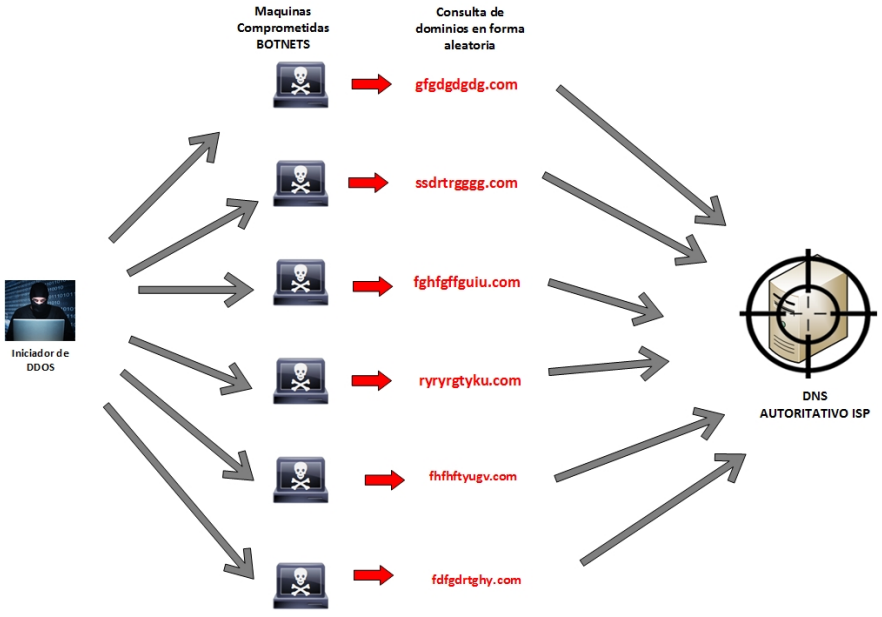


Figura 1.1 Ataque de DDOS por medio de una BOTNET

Síntomas de un ataque de DDOS:

- Incremento en el número de consulta de nombres de dominios.
- Los nombres de dominios consultados son aleatorios Ej.: sdfsfsf.com, xcfhjky.com.
- Incremento en el número de respuesta con el mensaje NXDOMAIN o REFUSED
- Aumento en el consumo de memoria del servidor.
- Desbordamientos en las tablas de conexiones del Firewall
- Incrementos de tamaño en archivos de log disminuyendo la capacidad de almacenamiento en disco.

1.2 SOLUCIÓN PROPUESTA

Como solución a este problema, se usara el esquema de direccionamiento IP Anycast con el protocolo de enrutamiento BGP para crear réplicas de los DNS Autoritativos del ISP.

Al usar este esquema de direccionamiento IP lograremos que un servidor de DNS Autoritativo con una misma dirección IP pública esté configurado e instalado en distintos lugares geográficos en el Internet.

Al tener varios servidores de DNS Autoritativo configurados con la misma dirección IP pública y colocados en distintos puntos en internet se lograra

que cada uno de estos nodos sea accesado por los usuarios más cercanos a este punto.

Con este esquema se obtiene como resultado una distribución de carga, mejorando en el consumo de ancho de banda y optimizando el consumo de recursos de hardware.

En el caso de un ataque de denegación de servicio, este sólo estará direccionado y concentrado en un solo servidor sin afectar al resto de servidores o replicas colocados en los distintos puntos en el internet o en caso de caída de uno de los servidores producto del ataque automáticamente otro servidor dentro de la nube de DNS Anycast estará disponible para brindar el servicio y así de esta manera garantizar un alto nivel de disponibilidad de los servicios del ISP y el de los clientes.

CAPÍTULO 2

METODOLOGÍA DE DESARROLLO DE LA SOLUCIÓN

2.1 MARCO TEÓRICO

2.1.1 ¿QUE ES UN DOMINIO?

Un dominio o nombre de dominio es el nombre que identifica un dispositivo conectado en internet. [1]

Cada dominio tiene que ser único en el Internet por ejemplo el dominio hp.com, www.hp.com (nombre del servidor web de hp).

Un dominio se compone de dos partes: el nombre de la organización (HP) y el tipo de dominio gTLDs (global code Top Level Domain) o ccTLDs (country code top Level Domain).

Los tipos de gTLDs más comunes son .COM para dominios comerciales, .NET para proveedores de internet, .MIL para instituciones militares, y .ORG para organizaciones sin fines de lucro. [2]

El Internet se basa en direcciones IP, y no en nombres de dominio, cada dispositivo conectado en internet requiere de un servidor de nombres de dominio (DNS) para registrar su dirección IP.

Cada dominio tiene un servidor de nombres DNS Autoritativo primario y otro secundario.

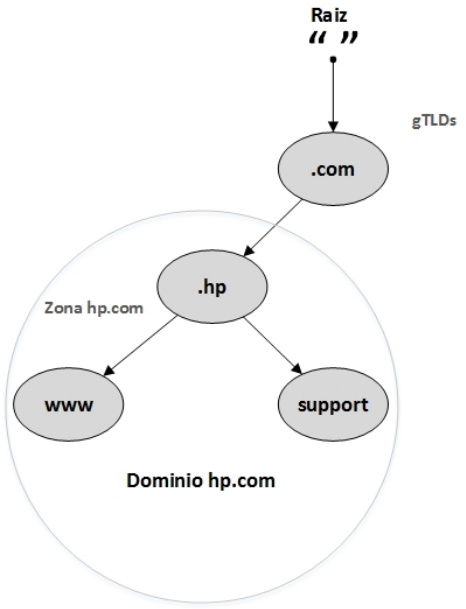


Figura 2.1 Estructura del de Dominio hp.com

2.1.2 ¿QUE ES UN DNS AUTORITATIVO?

Es el servidor de DNS que administra y que almacena el archivo de zona que contiene la información sobre todo el espacio de nombres dentro de un dominio. [3]

La información que contiene un archivo de zona puede ser:

- Registros MX
- Registros de IP
- Registros TXT
- Delegación de Subdominios.

Los servidores de nombres pueden ser autoritativos para múltiples zonas.

```
[root@master ~]# dig hp.com ns

; <<>> DiG 9.10.2 <<>> hp.com ns
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3627
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 7

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;hp.com.                                IN      NS

;; ANSWER SECTION:
hp.com.                 3561    IN      NS      ns3.hp.com.
hp.com.                 3561    IN      NS      ns5.hp.com.
hp.com.                 3561    IN      NS      ns6.hp.com.
hp.com.                 3561    IN      NS      ns2.hp.com.
hp.com.                 3561    IN      NS      ns1.hp.com.
hp.com.                 3561    IN      NS      ns4.hp.com.

;; ADDITIONAL SECTION:
ns1.hp.com.             163139  IN      A       15.219.145.12
ns2.hp.com.             163139  IN      A       15.219.160.12
ns3.hp.com.             163139  IN      A       15.211.192.12
ns4.hp.com.             163139  IN      A       15.203.224.14
ns5.hp.com.             163139  IN      A       15.195.192.37
ns6.hp.com.             163139  IN      A       15.195.208.12

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Tue Jul 21 13:41:43 ECT 2015
;; MSG SIZE  rcvd: 239
```

Figura 2.2 Consulta de los servidores de DNS autoritativos del dominio hp.com

2.1.3 ¿QUE ES LA DELEGACIÓN DE DOMINIOS?

La Delegación de dominios, consiste en asignar la responsabilidad de una parte de su dominio a otra organización o la asignación de autoridad para sus subdominios a diferentes servidores de DNS Autoritativos.

El servidor de nombres en lugar de contener formación sobre el dominio o subdominio que ha sido delegado, incluye referencias hacia los servidores de nombres autoritativos para ese subdominio. [4]

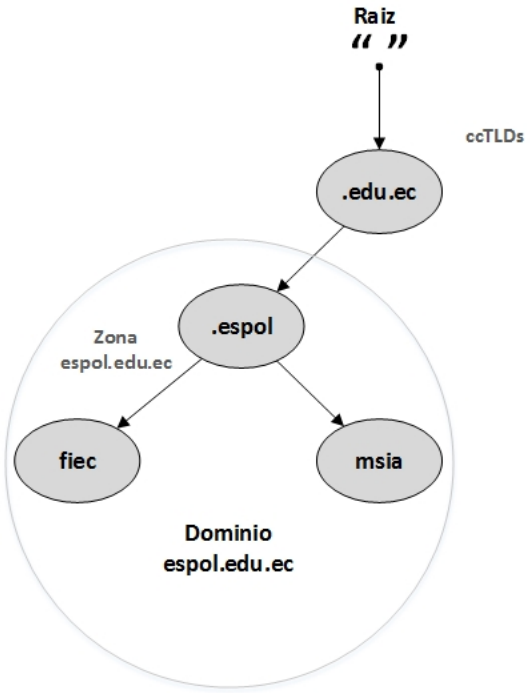
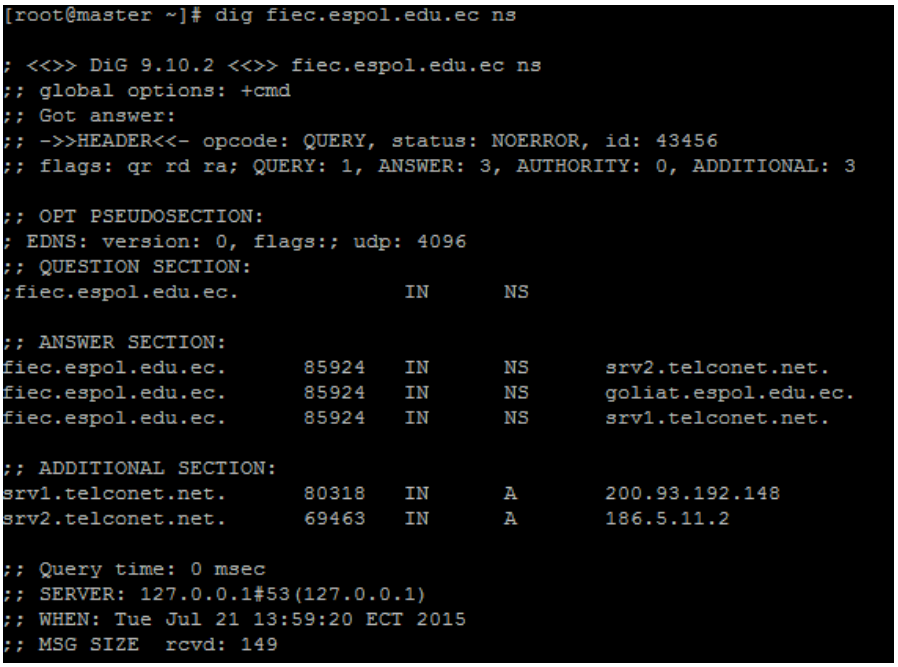


Figura 2.3 Dominio espol.edu.ec

Por ejemplo el subdominio fiec.espol.edu.ec es delegado hacia los siguientes servidores:



```
[root@master ~]# dig fiec.espol.edu.ec ns

; <<>> DiG 9.10.2 <<>> fiec.espol.edu.ec ns
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43456
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;fiec.espol.edu.ec.             IN      NS

;; ANSWER SECTION:
fiec.espol.edu.ec.      85924   IN      NS      srv2.telconet.net.
fiec.espol.edu.ec.      85924   IN      NS      goliat.espol.edu.ec.
fiec.espol.edu.ec.      85924   IN      NS      srv1.telconet.net.

;; ADDITIONAL SECTION:
srv1.telconet.net.      80318   IN      A       200.93.192.148
srv2.telconet.net.      69463   IN      A       186.5.11.2

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Tue Jul 21 13:59:20 ECT 2015
;; MSG SIZE  rcvd: 149
```

Figura 2.4 Delegación del subdominio fiec.espol.edu.ec

2.1.4 TIPO DE SERVIDORES DE DNS

Las especificaciones del servicio de DNS definen dos tipos de servidores de nombres:

Primario y secundario o Maestro y esclavo.

Un servidor primario para una zona lee los datos desde un archivo dentro del servidor y un servidor secundario los obtiene los datos de la zona desde un servidor maestro a través de la transferencia de zona vía AXFR.

Muy a menudo, un servidor puede ser maestro de una zona, pero secundario de otra zona.

Las principales funciones de un servidor de DNS secundario son:

- Proporciona redundancia

- Balanceo de carga.
- Respaldo de los datos de zona transferida desde un servidor maestro. [5]

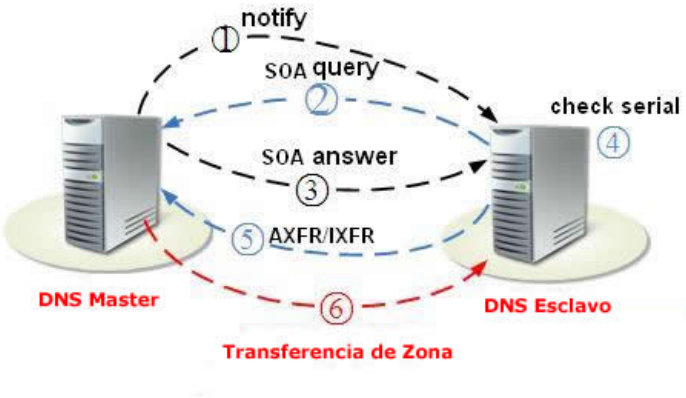


Figura 2.5 Transferencia de archivo de zona

2.1.5 ¿QUE ES EL ENRUTAMIENTO?

Básicamente el enrutamiento consiste en controlar, transportar y decidir por donde deben de transitar los datos en el internet.

Cada flujo de datos desde un dispositivo en la red puede ser este una PC o un dispositivo móvil a otro en Internet.

Consiste en un conjunto de paquetes que incluyen la información de dirección de un origen y de un destino, cada paquete de datos inicia un recorrido pasando por múltiples ruteadores que analizara la dirección IP destino, la

comparara con las direcciones incluidas en su tabla de enrutamiento y escogerá la ruta más óptima para reenviar el paquete hacia su destino final.

Para determinar la distancia entre una red y un dispositivo en particular, es necesario compartir las rutas con los demás ruteadores, así se podrá identificar de entre los ruteadores vecinos, cuál de estos está más cercano a una red de destino en particular. El enrutamiento más desplegado en internet es el enrutamiento IP.

En el enrutamiento IP, cada ruteador almacena todas las redes posibles que tiene a su alcance y vincula a cada una de ellas con las distintas interfaces de salida. El criterio que se usa para establecer la distancia con una red de destino, es la métrica la interfaz de salida escogida es la que tiene la ruta con menor costo.

Las métricas usadas para establecer la ruta con menor costo pueden ser el número de saltos, el Ancho de banda, carga, retardo y confiabilidad. [6]

2.1.6 ¿COMO FUNCIONA EL ENRUTAMIENTO EN INTERNET?

Existen dos niveles de enrutamiento en Internet, enrutamiento en un mismo sistema autónomo y enrutamiento entre sistemas autónomos diferentes.

En el enrutamiento dentro de un Sistema Autónomo podemos encontrar a los protocolos de Borde Interior IGP (Internal Gateway Protocol) como RIP, OSPF, EIGRP, IS-IS, que deciden la selección de rutas en función a los cálculos de las métricas que cada protocolo realiza.

2.1.7 PROTOCOLOS DE BORDE EXTERIOR

El enrutamiento entre distintos sistemas autónomos, debe de tener la capacidad de poder alcanzar todos los sistemas Autónomos en el Internet, por este motivo no es conveniente usar métricas para determinar las rutas más óptimas.

El enrutamiento entre sistemas autónomos se realiza exclusivamente con BGP.[7]

Figura 2.6 iBGP y eBGP Fuente: (Cisco - CCNP)

2.1.8 ¿QUE ES UN SISTEMA AUTÓNOMO (AUTONOMOUS SYSTEM: AS)?

Cuando tenemos una red de computadoras, tenemos tantas direcciones IP diferentes como computadores haya en la red, si los enrutadores tuvieran que recordar todas las direcciones posibles y buscar una dirección de destino en una tabla, la tarea sería simplemente imposible. Para evitar eso se agrupan las direcciones de una misma red en una sola dirección de red.

En una organización, todos los enrutadores administran su tabla de enrutamiento con base en el intercambio de información de redes destino y

costos que se pueden calcular automáticamente o se pueden establecer manualmente, pero siempre con base en direcciones IP de red.

Si la administración de la red de una organización es unificada y la topología es más o menos uniforme o bajo el control de la misma administración, no hay problema en confiar en los cálculos automáticos que hacen los protocolos de enrutamiento dinámico para encontrar las mejores rutas a todas las redes destino, si la administración no es unificada, una parte de la organización puede decidir hacer su enrutamiento dinámico con un protocolo y otra parte de la organización con otro protocolo diferente y éstos no ser compatibles entre sí, en éste último caso, la decisión de cómo hacer el enrutamiento no se basa en los cálculos automáticos sino en las preferencias administrativas de cada parte de la organización. A esto se lo conoce como enrutamiento basado en políticas, es decir, no se basa en métricas sino en conveniencias administrativas.

Un sistema autónomo es una organización con políticas de administración de enrutamiento unificadas, es decir, la forma en que administra sus direcciones IP y su enrutamiento depende de sus políticas administrativas.

Estas políticas administrativas son elegir protocolos de enrutamiento y usar en sus cálculos automáticos.

Un Sistema Autónomo (AS) posee un grupo de direcciones IP públicas, enrutables en Internet y reservadas en una organización regional como LACNIC, RIPE, ARIN.

A cada AS se le asocia un número que lo identifica del 0 a 65535 y a éste se le asocian todas las redes que posee, por lo tanto, los enrutadores de mayor jerarquía establecen rutas en Internet que consisten en secuencias de números de Sistemas Autónomos por los que debe pasar un paquete para llegar a una red destino.

Para que exista enrutamiento completo en Internet no es necesario que todos los enrutadores tengan todas las direcciones IP posibles en Internet, sólo necesitan tener un camino hacia algunos enrutadores muy potentes que tienen resúmenes de rutas apropiadas. [8]

2.1.9 ¿QUE ES EL PROTOCOLO BGP?

BGP o Border Gateway Protocol es un protocolo exterior (EGP por sus siglas en inglés) basado en políticas que enrutan tráfico de redes entre sistemas autónomos.

Es un protocolo de vector de ruta (path vector) que se configura en ruteadores de borde y obtiene tablas de enrutamiento según los ruteadores vecinos.

Las rutas que se propagan por BGP entre sistemas autónomos usualmente son una porción de todas las rutas posibles de Internet, del orden de 100.000 o 120.000 redes destino.

BGP es un protocolo altamente configurable, a cada ruta se le asocian un conjunto de atributos, la selección de la mejor ruta se basa en una serie de reglas y atributos.

BGP se considera un protocolo basado en políticas debido a que los atributos son modificables por el administrador y porque si una organización tiene varios accesos a Internet, es la administración quien decide por cuál de ellos es más conveniente salir.

El principio de la configuración de BGP es establecer adyacencias con vecinos inmediatos en sistemas autónomos diferentes y aplicar políticas de enrutamiento a las actualizaciones de rutas que se envíen o reciban por esa adyacencia.

BGP establece sesiones TCP con el enrutador que envía la solicitud, esa adyacencia se puede autenticar y se implementa en la configuración del proceso BGP. [10]

El intercambio de datos entre ruteadores se realiza por medio de una conexión establecida entre los ruteadores de borde de los sistemas autónomos.

Para lograr una entrega confiable de los datos entre los ruteadores de borde, se hace uso de una conexión TCP en el puerto 179. Esta conexión se debe de mantener activa debido a que ambos ruteadores constantemente se intercambian datos.

Al inicio de la conexión, cada ruteador envía al vecino toda su tabla de enrutamiento y después únicamente se enviarán actualizaciones que incluyen nuevas rutas o las rutas que deben de ser eliminadas.

Periódicamente se envían mensajes para monitorear la conectividad. Cuando una conexión TCP se pierde por algún motivo, cada ruteador que participa de

la conexión debe de dejar de utilizar las rutas que aprendido del otro ruteador. [11]

En la figura 2.7 podemos observar a varios sistemas autónomos conectados mediante enlaces virtuales.

Los enlaces entre sistemas autónomos de mantienen en una conexión TCP. Cada sistema autónomo contiene una o más redes en su interior.

A continuación observamos que existe más de una ruta entre dos sistemas autónomos.

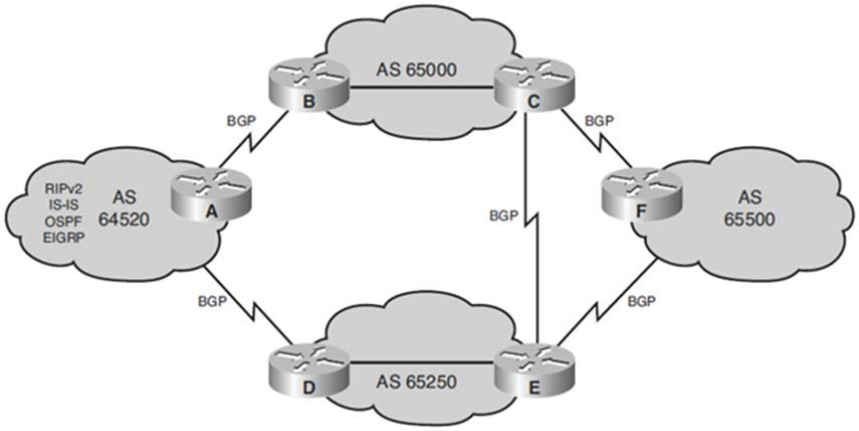


Figura 2.7 Varios AS Conectados Fuente: (Cisco - CCNP)

Como el protocolo BGP está basado en vector distancia, para el intercambio de información de rutas en el internet, una ruta se transmite con el número del Sistema Autónomo (AS) por donde pasado. De este modo se podrá saber cómo alcanzar a cualquier dirección del prefijo anunciado. [12]

core1.fmt2.he.net> show ip bgp routes detail 192.188.59.0

Matching Routes	3
Status Codes	**A** - Aggregate **B** - Best **b** - Not Install Best **C** - Confederation eBGP **D** - Damped **E** - eBGP **H** - History **I** - iBGP **L** - Local **M** - Multipath **m** - Not Installed Multipath **S** - Suppressed **F** - Filtered **s** - Stale

Status	Network	Next Hop	Metric	LocPrf	Weight	Path	Origin
BI	192.188.59.0/24	213.248.67.105	65	70	0	1299, 19169, 27947, 28027	IGP
I	192.188.59.0/24	80.239.167.173	67	70	0	1299, 19169, 27947, 28027	IGP
I	192.188.59.0/24	80.239.167.233	335	70	0	1299, 19169, 27947, 28027	IGP
Last Update	15d14h21m49s ago (1 path installed)						

Figura 2.8 AS PATH del Prefijo 192.188.59.0 perteneciente a la ESPOL Fuente: (http://lg.he.net/ Looking Glass)

BGP Opera en dos modos: EBGP e IBGP. EBGP (BGP EXTERIOR) se utiliza entre distintos sistemas autónomos, e IBGP (BGP Interior) se utiliza entre ruteadores dentro del mismo sistema autónomo.

Figura 2.9 IBGP y EBGP Fuente: (Cisco - CCNP)

2.1.10 ATRIBUTO AS-PATH

Es un atributo que almacena la secuencia de números de sistemas autónomos por donde ha pasado la publicación de un prefijo. Cuando un ruteador de borde anuncia una ruta hacia otro ruteador, incluye a este atributo su número de sistema autónomo.

La secuencia de AS no se modifica si se usa IBGP o si la ruta solo es anunciada dentro del mismo sistema autónomo. Al momento de utilizar el AS-PATH como parámetro de selección de rutas, se seleccionara la que tenga la lista AS-PATH más corta.[13]

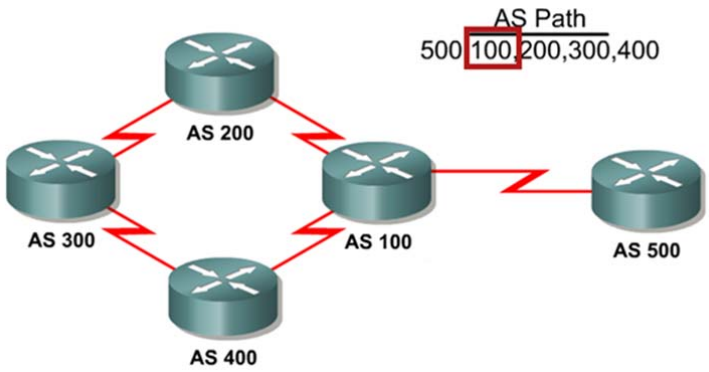


Grafico 2.10 Atributo AS-PATH Fuente: (Cisco - CCNP)

2.1.11 ATRIBUTO NEXT-HOP

Identifica la dirección IP del ruteador del siguiente salto para llegar a un destino.

La dirección IP es la entrada del siguiente sistema autónomo a lo largo de la ruta para alcanzar la red de destino por lo tanto para EBGP el atributo NEXT-HOP es la dirección IP del vecino que envió la actualización.

Al momento de seleccionar una ruta por este atributo se elegirá la de menor costo hacia el siguiente NEXT-HOP, o la de menor número de saltos hacia el siguiente NEXT-HOP. [14]

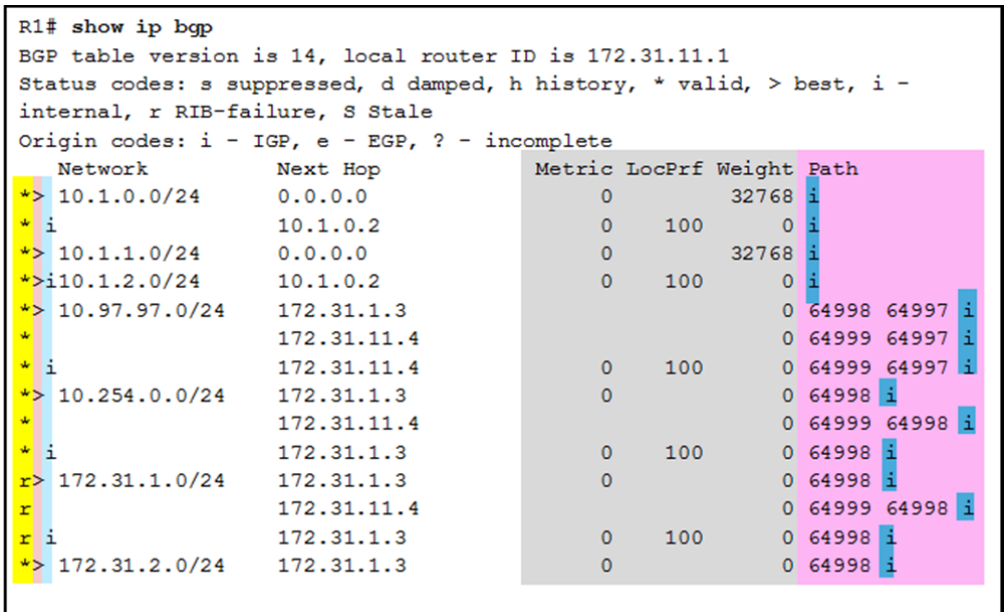
2.1.12 TABLA DE BGP

La tabla de BGP almacena información recibida desde y enviada hacia otros vecinos BGP, también es conocida como tabla de topología BGP o tabla de enrutamiento BGP.

El ruteador ofrece las mejores rutas incluidas en la tabla de BGP a la tabla de enrutamiento.

La tabla de BGP incluye:

- Lista de los vecinos BGP
- Lista de todas las redes aprendidas desde cada vecino
- Lista de los atributos para cada ruta aprendida



```
R1# show ip bgp
BGP table version is 14, local router ID is 172.31.11.1
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 10.1.0.0/24      0.0.0.0                  0         32768 i
* i                 10.1.0.2                 0    100      0 i
*> 10.1.1.0/24      0.0.0.0                  0         32768 i
*>i10.1.2.0/24      10.1.0.2                 0    100      0 i
*> 10.97.97.0/24    172.31.1.3                             0 64998 64997 i
*                   172.31.11.4                            0 64999 64997 i
* i                 172.31.11.4              0    100      0 64999 64997 i
*> 10.254.0.0/24    172.31.1.3               0             0 64998 i
*                   172.31.11.4                            0 64999 64998 i
* i                 172.31.1.3               0    100      0 64998 i
r> 172.31.1.0/24    172.31.1.3               0             0 64998 i
r                   172.31.11.4                            0 64999 64998 i
r i                 172.31.1.3               0    100      0 64998 i
*> 172.31.2.0/24    172.31.1.3               0             0 64998 i
```

Figura 2.11 Tabla de BGP Fuente: (Cisco - CCNP)

Actualmente la tabla de BGP de los Ruteadores de Backbone de internet almacena unas 500.000 entradas. [15]

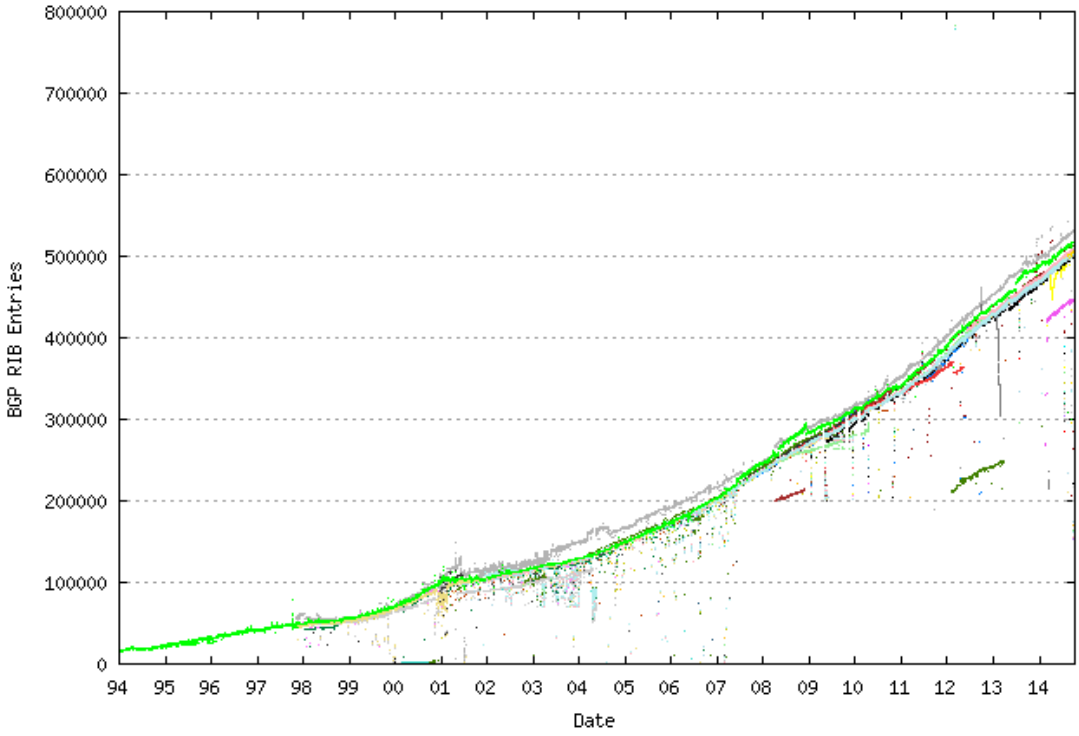


Figura 2.12 Tabla de crecimiento de entradas BGP de Internet Fuente: (http://bgp.potaroo.net/as2.0/bgp-active.html)

2.1.13 DIRECCIONAMIENTO IP UNICAST

La dirección Unicast es el tipo más común en una red IP y es el que está actualmente en uso en Internet.

Un paquete con una dirección de destino unicast está dirigido a un único host receptor específico disponible en internet.

Un ejemplo es un host con la dirección IP 192.168.1.85 (origen) que solicita una página Web a un servidor con la dirección IP 192.168.1.200 (destino).

Para que un paquete unicast sea enviado y recibido, la dirección IP de destino debe estar incluida en el encabezado del paquete IP. [16]

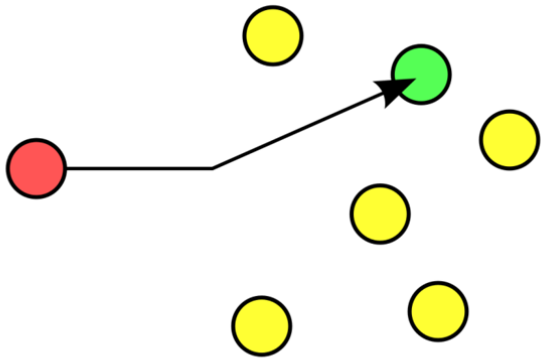


Figura 2.13 Direccionamiento Unicast Fuente:
(http://es.wikipedia.org/wiki/Unicast)

2.1.14 DIRECCIONAMIENTO IP ANYCAST

Anycast es una forma de direccionamiento donde los datos son enrutados hacia el destino con el menor número de saltos y con menor tiempo de latencia.

En el internet, una dirección IP se puede anunciar desde distintos proveedores de internet y los ruteadores intermedios enrutaran los datos hasta el destino más cercano.

Por ejemplo la dirección 192.5.5.241 es la dirección IP Anycast del Root F f.root-servers.net que actualmente cuenta con aproximadamente 50 réplicas instaladas en distintas partes del mundo.

El direccionamiento Anycast se suele usar en servicios con protocolos no orientados a la conexión (como UDP) para obtener alta disponibilidad y balanceo de carga. [17]

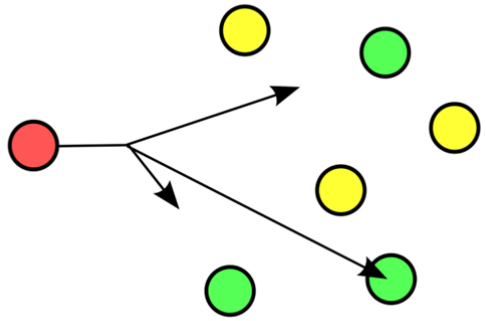


Figura 2.14 Direccionamiento Anycast Fuente:
(http://es.wikipedia.org/wiki/Anycast)

2.1.15 NODOS LOCALES

Ofrece uno o varios servicios a una parte del sistema de Ruteo. Normalmente Los Nodos Locales están conectados a IXP Regionales o locales (Puntos de Intercambio de trafico) y Universidades.

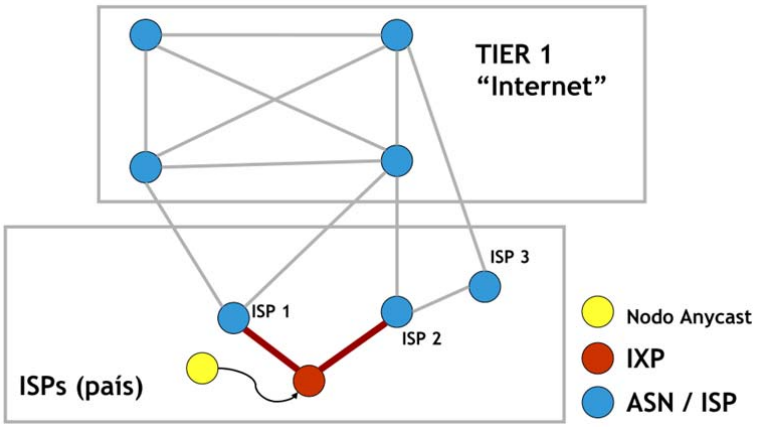


Figura 2.15 Nodos Locales
Fuente: (NIC.MX)

2.1.16 NODOS GLOBALES

Ofrece uno o varios servicios a toda la red de internet. Normalmente un Nodo Global está conectado directamente a un ISP que participa del enrutamiento de internet.

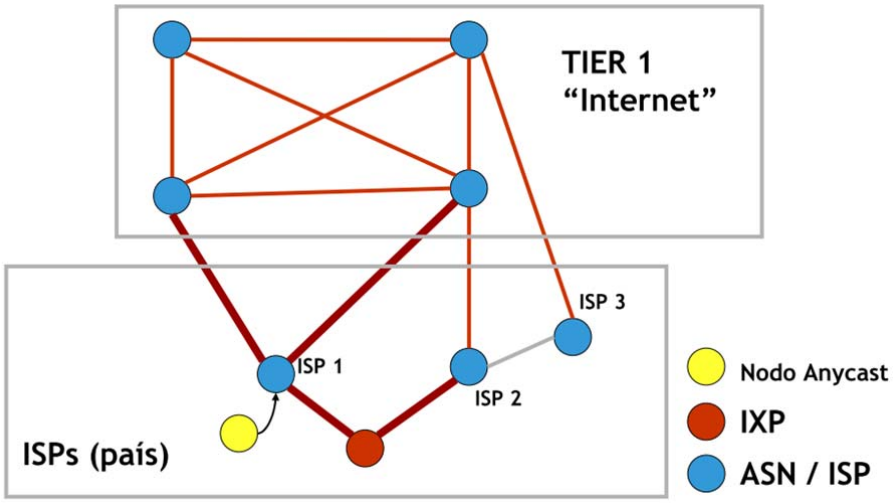


Figura 2.16 Nodos Globales
Fuente: (NIC.MX)

2.1.17 DDOS, BOTNETS Y CONSECUENCIAS

Un ataque de denegación de servicio distribuido es aquel en el que una red de computadoras que previamente han sido comprometidos y controlados por una sola persona, se unen para atacar a un objetivo en común, provocándole la denegación de servicio.

El alto flujo de datos de entrada y de requerimientos que procesa el equipo atacado le provocara el agotamiento de sus recursos y será incapaz de ofrecer sus servicios a usuarios legítimos.

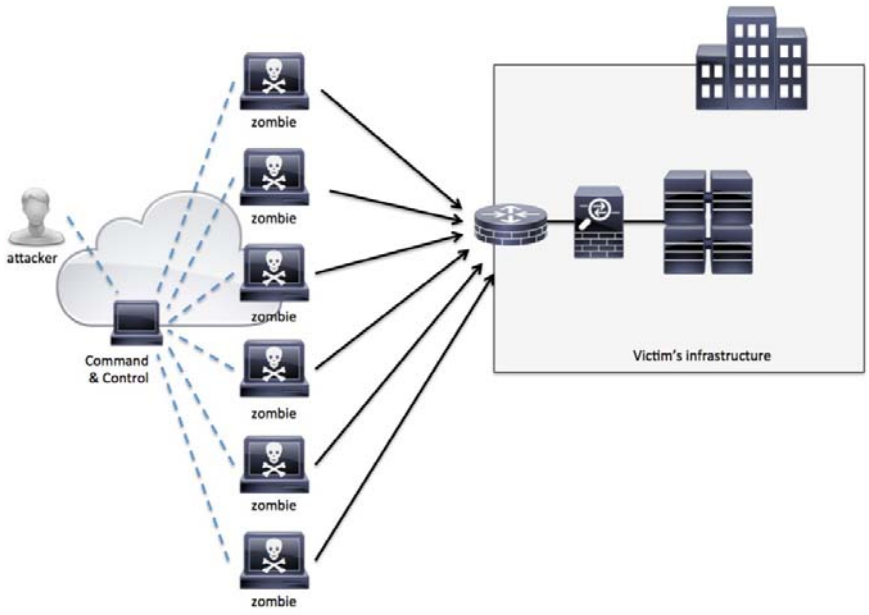


Figura 2.17 DDOS Attacks Fuente: (CISCO Guide to Defending Against Distributed Denial of Service Attacks)

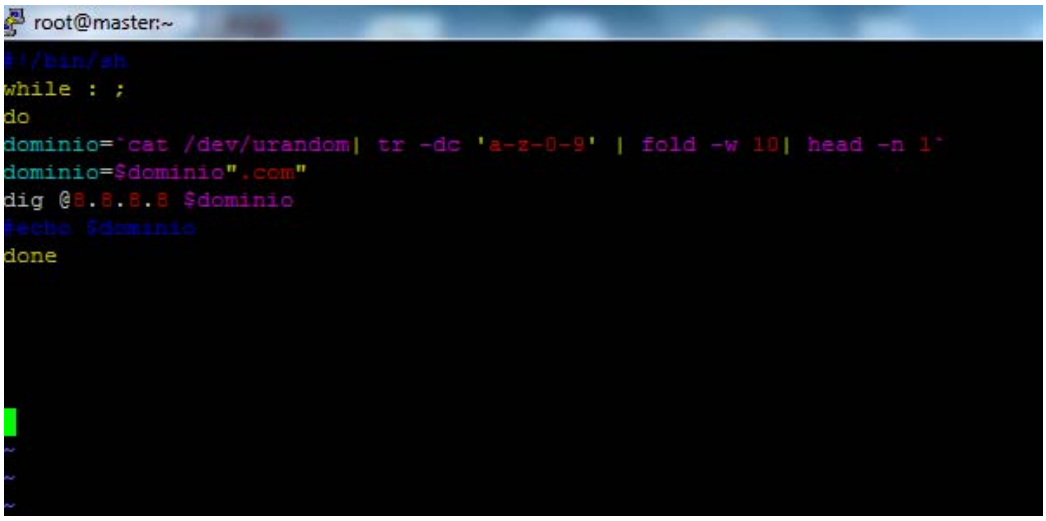


Figura 2.18 DDOS Script

A nivel global, los ataques a los servidores de servicio de DNS han ido creciendo, en parte por la mayor facilidad para crear ataques de DDOS, el fácil acceso a herramientas para realizar actividades maliciosas y también por la mayor cantidad de equipos disponibles mal configurados o con fallos de seguridad que son explotados para generar este tipo ataques y uno de los protocolos más afectados por su fácil explotación es el UDP y por consecuencia todos los servicios que usan este protocolo se ven afectados.

Como es de conocimiento general el servicio de DNS es la columna vertebral del internet y su importancia es de igual de relevante como la del enrutamiento IP.

Todos los servicios corporativos tales como Servidores de Correo, Servidores Web, servidores de archivos no podrían ser accesados sin la ayuda del servicio de DNS.

Una interrupción del Servicio de DNS provocara que los servicios corporativos no puedan ser accesados provocando la pérdida de información, pérdidas económicas y además de comprometer la imagen corporativa de la empresa.

Es de vital importancia que los administradores de red monten sus servidores de DNS sobre infraestructuras de Red robustas, instalando y configurando servidores de DNS en distintas ubicaciones geográficas tomando en consideración las mejores prácticas de configuración y los recursos con que contamos hoy en día, así de esta manera mantener la alta disponibilidad del servicio.

2.2 TOPOLOGÍA ACTUAL DE SERVIDORES DE DNS AUTORITATIVOS DEL ISP

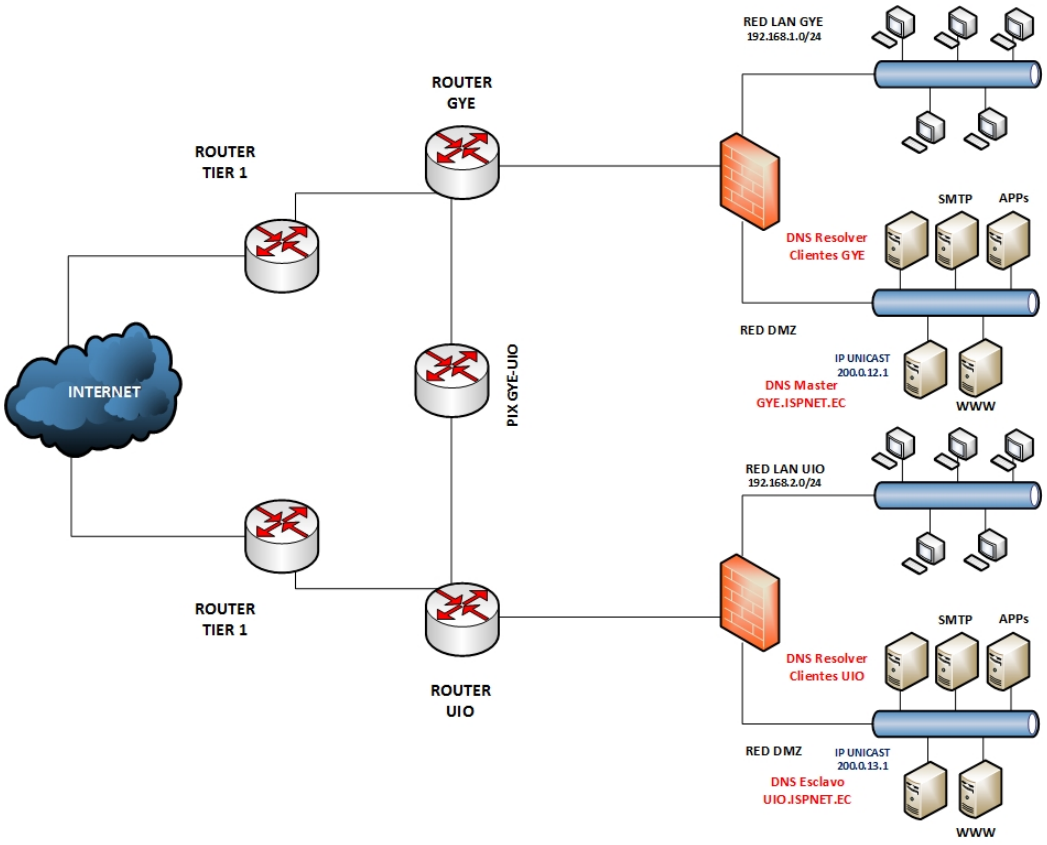


Figura 2.19 Topología de Servidores de DNS del ISP

En la topología actual del proveedor de Internet podemos observar que se está utilizando el bloque de direccionamiento público asignado por el Proveedor de direcciones IP de la región. Los prefijos 200.0.12/24 y 200.0.13/24 son anunciados desde un solo sistema autónomo por lo tanto los servidores de DNS son desplegados con direcciones IP Unicast.

2.3 CONFIGURACIÓN DEL NODO DNS ANYCAST

2.3.1 DISEÑO DE TOPOLOGÍA MÍNIMA REQUERIDA

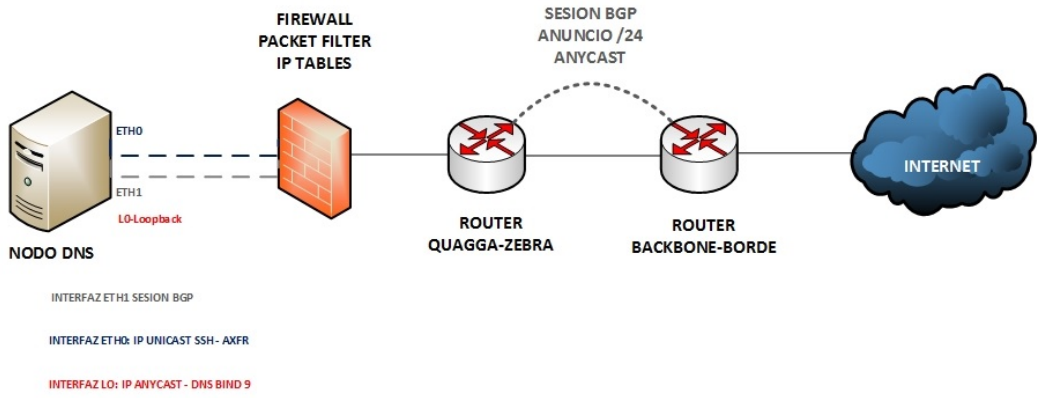


Figura 2.20 Topología necesaria para despliegue de NODO ANYCAST para DNS

Los componentes o requisitos necesarios para el despliegue de un nodo de ANYCAST para DNS son los siguientes:

- Acceso al ruteador de borde del ISP
- Software de ruteo instalado en el servidor que brinda el servicio de DNS puede ser Quagga de libre distribución o cualquier otro.
- Packet Filter o IP Tables instalado en el servidor que brinda el servicio de DNS
- BIND 9 instalado en el servidor que brinda el servicio de DNS
- Bloque de IP publicas /24 asignado por el RIR de la región, en este caso LACNIC
- Sistema Autónomo AS asignado por el RIR de la región
- Bloque de IP publicas /29 asignado por el proveedor de internet

2.3.2 CRITERIOS PARA LA SELECCIÓN DE LA UBICACIÓN DEL NODO O LOS NODOS ANYCAST

Dependiendo a quienes se va a ofrecer el servicio:

- Si el servicio se ofrece a todo el internet el nodo Anycast tiene que ser instalado en un ISP que participe en el ruteo de internet. Este tipo de nodos se los conoce como Globales.
- Si el servicio solo se va a ofrecer solo a una parte del sistema de ruteo de internet el nodo Anycast tiene que ser instalado en un Punto de intercambio PIX. Este tipo de nodos se los conoce como Locales.

En el internet existen proveedores de servicio de redes Anycast para DNS con soporte para un número ilimitado de Zonas y con nodos instalados en varias partes del mundo.

Entre los principales proveedores de servicio Anycast para DNS tenemos a los siguientes:

- Internet Systems Consortium: https://www.isc.org/network/sns/
- Packet Clearing House http://www.pch.net

2.3.3 SOFTWARE UTILIZADOS

- Sistema Operativo Centos 6 Minimal 64-bits

  Sitio de descarga: http://mirror.cedia.org.ec/centos/6.6/isos/x86_64/

- Packet Filters IPtables: http://www.netfilter.org/
- Quagga Routing Suite: http://www.nongnu.org/quagga/
- BIND 9.10.2-P2: http://ftp.isc.org/isc/bind9/9.10.2-P2/bind-9.10.2-P2.tar.gz

2.3.4 INSTALACIÓN BÁSICA DE CENTOS 6:

Figura 2.21 Instalación mínima de Centos 6

En el proceso de instalación del sistema operativo se escoge la opción:

Install o upgrade an existing system

Figura 2.22 Instalación mínima de Centos 6

A continuación se da clic en el botón Skip para continuar con el proceso de instalación.

Figura 2.23 Instalación mínima de Centos 6

A continuación se da clic en el botón para continuar con el proceso de instalación.

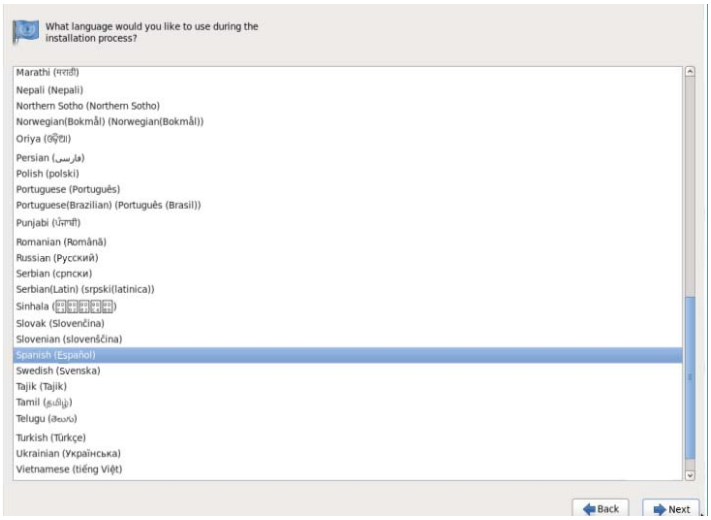


Figura 2.24 Instalación mínima de Centos 6

Se selecciona el idioma que se usara en el proceso de instalación.

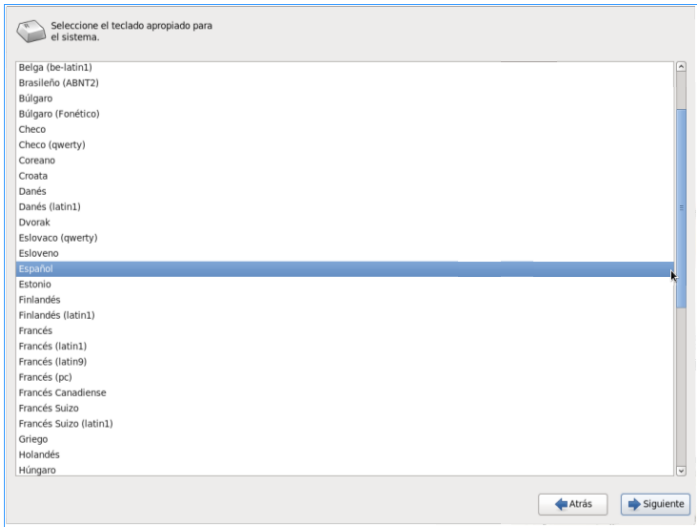


Figura 2.24 Instalación mínima de Centos 6

Se selecciona el idioma apropiado para el teclado del sistema.

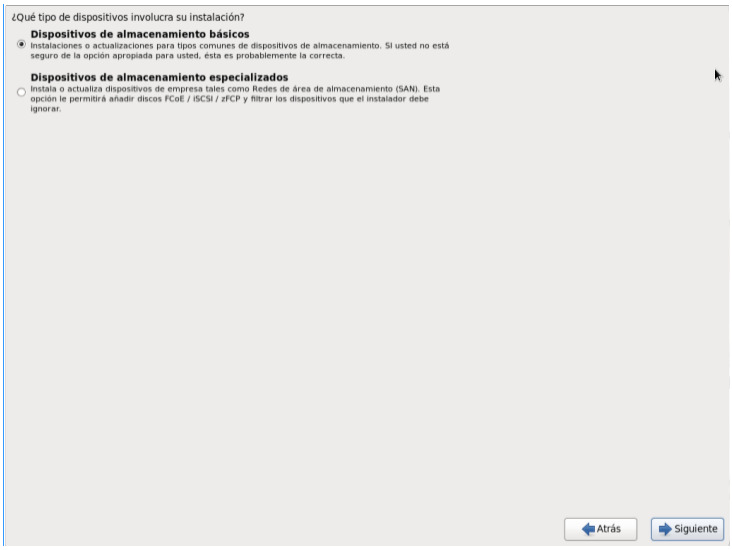


Figura 2.25 Instalación mínima de Centos 6

Se selecciona la opción del tipo de dispositivo de almacenamiento en este caso se continua con la opción seleccionada por defecto.

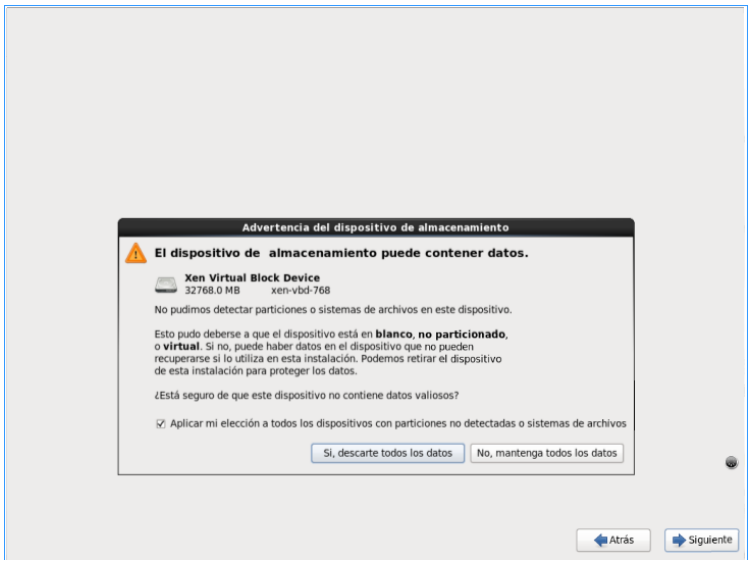


Figura 2.26 Instalación mínima de Centos 6

A continuación se da clic en la opción Si, descarte todos los datos para seguir con el proceso de instalación.

Figura 2.27 Instalación mínima de Centos 6

Se ingresa el nombre host del servidor en este caso ns.ispnet.ec

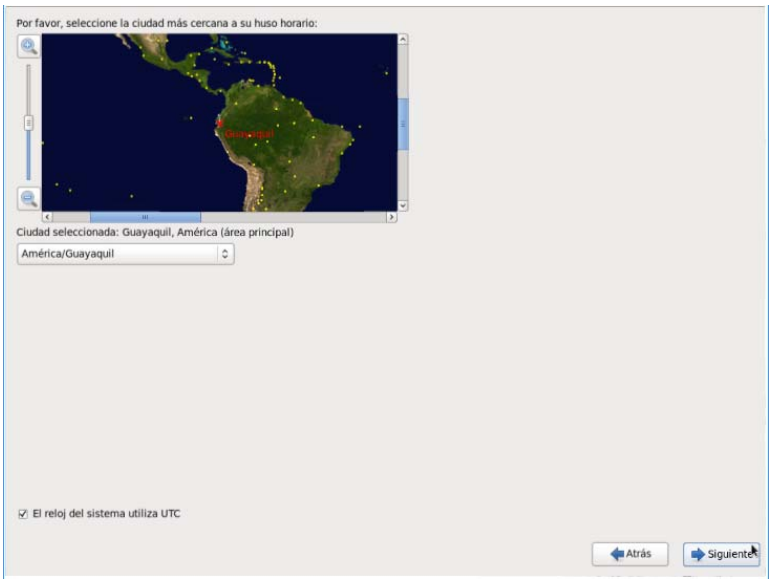


Figura 2.28 Instalación mínima de Centos 6

Se selecciona la ciudad más cercana al uso horario y se selecciona la opción **El reloj del utiliza UTC.**

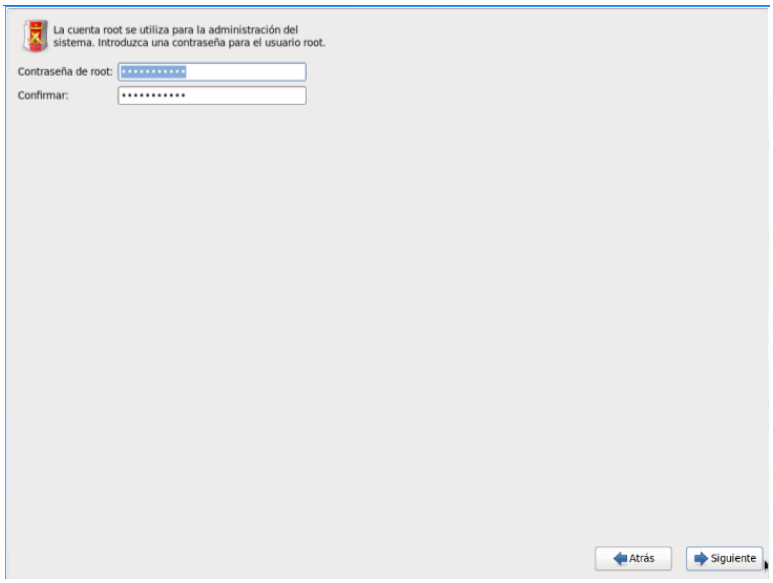


Figura 2.29 Instalación mínima de Centos 6

Se ingresa la contraseña para el usuario Root.

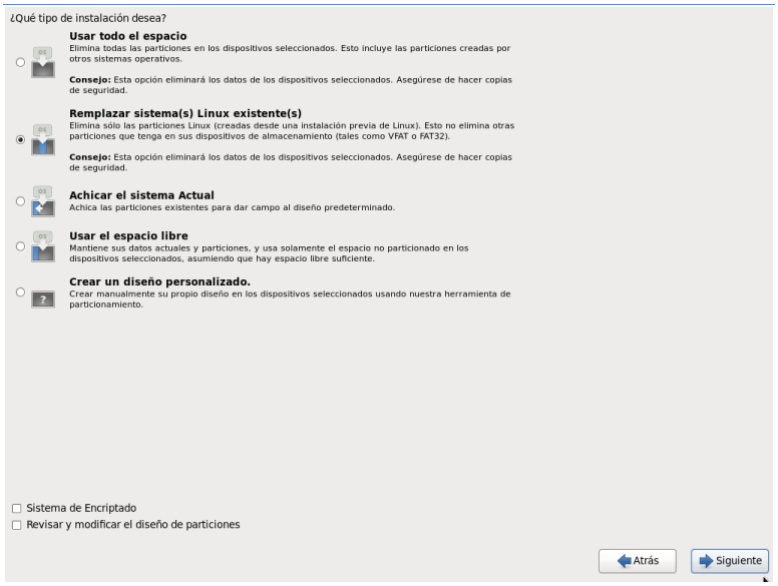


Figura 2.30 Instalación mínima de Centos 6

Se selecciona la opción del tipo de instalación que se desea realizar en este caso se continua con la opción seleccionada por defecto.

El proceso de instalación escribirá en el disco los paquetes necesarios para el funcionamiento básico del sistema operativo.

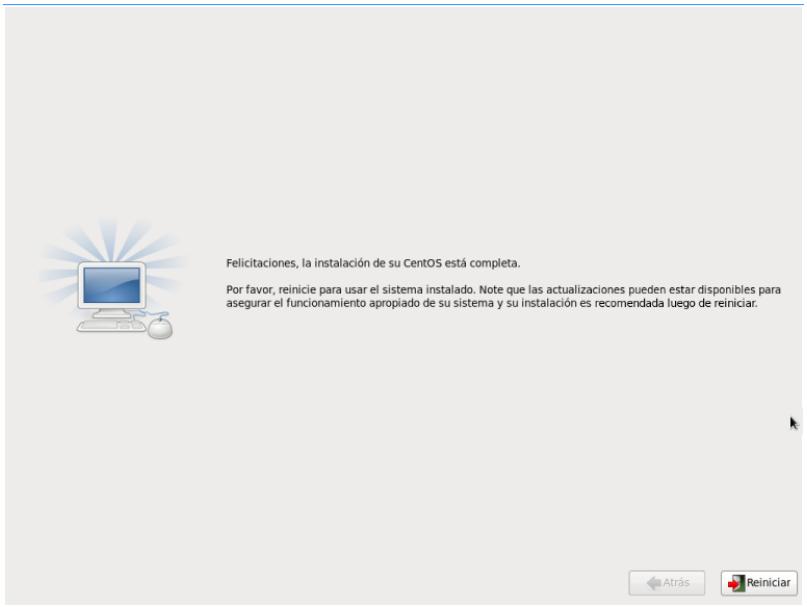


Figura 2.31 Instalación mínima de Centos 6

El proceso de instalación del sistema operativo Centos 6 ha terminado.

2.3.5 CONFIGURACIÓN DE INTERFAZ ETH0 CON IP UNICAST

Editar el archivo ifcfg-eth0 en:

/etc/sysconfig/network-scripts/ifcfg-eth0

DEVICE=eth0

TYPE=Ethernet

ONBOOT=yes

BOOTPROTO=none

IPADDR=**IP Asignada por el ISP**

PREFIX=29

GATEWAY=**IP de la puerta de enlace**

DNS1=**IP del servidor de DNS del proveedor**

DEFROUTE=yes

NAME="System eth0"

HWADDR=EA:42:BA:95:F2:9E

2.3.6 CONFIGURACIÓN DE INTERFAZ LOOPBACK CON IP ANYCAST

Editar el archivo ifcfg-lo:1 en:

/etc/sysconfig/network-scripts/ifcfg-lo:1

DEVICE=lo:1

IPADDR= **IP Asignada por el RIR de la Región LACNIC**

PREFIX=24

ONBOOT=yes

NAME=="loopback Anycast"

2.3.7 INSTALACIÓN DE SOFTWARE BIND9 PARA EL SERVICIO DE DNS AUTORITATIVO

- Descargar archivo desde el sitio de descargas de ISC:

  wget http://ftp.isc.org/isc/bind9/9.10.2-P2/bind-9.10.2-P2.tar.gz

- Descomprimir archivo:

  tar –xzvf bind-9.10.2-P2.tar.gz

- Compilar el código Fuente y crear un ejecutable

  cd bind-9.10.2/

  ./configure --with-libtool --enable-ipv6

  make

  make install

2.3.8 ARCHIVOS DE CONFIGURACIÓN NAMED.CONF PARA SERVIDOR MASTER

- Crear los directorios:

  /var/log/named/

  /etc/named/namedb/zones

- Crear archivo /etc/named.conf:

  //

  // named.conf for Red Hat caching-nameserver

  //

  logging {

  channel warning

  {

  file "/var/log/named/warning.log" versions 5 size 1024k;

  severity warning;

  print-category yes;

```
print-severity yes;
print-time yes;
};

channel general_dns
{
file "/var/log/named/queries.log" versions 5 size 1024k;
severity info;
print-category yes;
print-severity yes;
print-time yes;
};
channel transferencia
{
file "/var/log/named/transfer.log" versions 5 size 1024k;
severity info;
print-category yes;
print-severity yes;
print-time yes;
};

channel todos
{
file "/var/log/named/general.log" versions 5 size 1024k;
```

```
severity info;
print-category yes;
print-severity yes;
print-time yes;
};

channel clientes
{
file "/var/log/named/respuesta.log" versions 5 size 1024k;
severity info;
print-category yes;
print-severity yes;
print-time yes;
};

category default { warning; } ;
category queries { general_dns; } ;
category xfer-in { transferencia; } ;
category xfer-out { transferencia; } ;
category general { todos; } ;
category client { clientes; } ;
};

acl "Secundarios" {ip-servidores-secundarios;};
```

```
options {
directory "/etc/named/namedb";
listen-on {any;};
listen-on-v6 {none;};
recursion no;
check-sibling no;
provide-ixfr yes;
notify explicit;
also-notify {ip-servidores-secundarios;};
};

key "rndc-key" {
algorithm hmac-md5;
secret "yoPufdnW74/7GxquVpX8FQ==";
};
controls {
inet 127.0.0.1 port 953 allow { 127.0.0.1; } keys { "rndc-key"; };
};
zone "." IN {
type hint;
file "zones/named.ca";
};
zone "0.0.127.in-addr.arpa" IN {
type master;
```

```
file "zones/named.local";
allow-update { none; };
};
zone "ispnet.ec" {
type master;
file "zones/ispnet.ec.zone";
allow-transfer { "Secundarios";};
};
zone "cliente1.com.ec" {
type master;
file "zones/cliente1.com.zone";
allow-transfer { "Secundarios";};
};
```

2.3.9 ARCHIVOS DE CONFIGURACIÓN NAMED.CONF PARA EL SERVIDOR SECUNDARIO

- Crear los directorios:

  /var/log/named/

  /etc/named/namedb/zones

- Crear archivo /etc/named.conf:

```
//
// named.conf for Red Hat caching-nameserver
//
```

```
logging {
        channel warning
        {
        file "/var/log/named/warning.log" versions 5 size 1024k;
        severity warning;
        print-category yes;
        print-severity yes;
        print-time yes;
        };

        channel general_dns
        {
        file "/var/log/named/queries.log" versions 5 size 1024k;
        severity info;
        print-category yes;
        print-severity yes;
        print-time yes;
        };

        channel transferencia
        {
        file "/var/log/named/transfer.log" versions 5 size 1024k;
        severity info;
```

```
print-category yes;
print-severity yes;
print-time yes;
};

channel todos
{
file "/var/log/named/general.log" versions 5 size 1024k;
severity info;
print-category yes;
print-severity yes;
print-time yes;
};
 channel clientes
{
file "/var/log/named/respuesta.log" versions 5 size 1024k;
severity info;
print-category yes;
print-severity yes;
print-time yes;
};
category default { warning; } ;
category queries { general_dns; } ;
category xfer-in { transferencia; } ;
```

```
        category xfer-out { transferencia; } ;
        category general { todos; } ;
        category client { clientes; } ;
};
options {
        directory "/etc/named/namedb";
        dump-file "/var/log/named/cache_dump.db";
        statistics-file "/var/log/named/named_stats.txt";
        allow-notify {IP DNS MASTER;};
        request-ixfr yes;
        allow-transfer {"none";};

        recursion no;
};

key "rndc-key" {
        algorithm hmac-md5;
        secret "RZxV+x09vYz7x+PIunHKhA==";
};
controls {
      inet 127.0.0.1 port 953 allow { 127.0.0.1; } keys { "rndc-key"; };
 };

zone "." IN {
```

```
        type hint;
        file "named.ca";
};

zone "0.0.127.in-addr.arpa" IN {
        type master;
        file "named.local";
        allow-update { none; };
};

zone "ispnet.ec" {
 type slave;
 file "slave/ispnet.ec.d";
 masters { IP DNS MASTER; };
};

zone "cliente1.com.ec" {
 type slave;
 file "slave/cliente1.com.ec.d";
masters { IP DNS MASTER; };
};
```

2.3.10 ARCHIVOS DE ZONA

- Editar el archivo de zona para el dominio ispnet.ec

  /etc/named/namedb/zones/ispnet.ec.zone

$TTL 1h

@ IN SOA master.ispnet.ec. dnsadmin.ispnet.ec.)

2015070602; version

6h ; refresh

1h ; retry

30d ; expire

1h) ; minimum

IN NS ns1.ispnet.ec.

IN NS ns2.ispnet.ec.

ns1.ispnet.ec. 3600 IN A ###.###.###.###

ns2.ispnet.ec. 3600 IN A ###.###.###.###

- Editar Archivo de zona para el dominio cliente1.com.ec

/etc/named/namedb/zones/cliente1.com.ec.zone

$TTL 1h

@ IN SOA master.ispnet.ec. dnsadmin.ispnet.ec.)

2015070602; version

6h ; refresh

1h ; retry

30d ; expire

1h) ; minimum

IN NS ns1.ispnet.ec.

IN NS ns2.ispnet.ec.

www.cliente1.com. 3600 IN A ###.###.###.###

cliente1.com. 3600 IN MX 10 smtp.cliente1.com.

smtp.cliente1.com. 3600 IN A ###.###.###.###

2.3.11 INSTALACIÓN DE SOFTWARE DE RUTEO QUAGGA

- Descargar archivo desde el sitio de descargas de Quagga Routing Suite:

  wget http://download.savannah.gnu.org/releases/quagga/quagga-0.99.22.4.tar.gz

- Descomprimir archivo:

  tar –xzvf quagga-0.99.22.4.tar.gz

- Compilar el código Fuente y crear un ejecutable

  cd quagga-0.99.22.4/

  ./configure -prefix=/usr/local/ -sysconfdir=/usr/local/quagga/etc/conf/ -localstatedir=/usr/local/quagga/var/run/

  make

  make install

2.3.12 CONFIGURACIÓN DEL SERVICIO DE RUTEO Y SESIÓN BGP

- Editar el archivo de configuración para el servicio de ruteo:

  /usr/local/quagga/etc/conf/zebra.conf:

! Zebra configuration saved from vty

! 2012/07/06 16:28:22

!

hostname NodoAnycast

password 8 OuQ32cXxsW/IQ

enable password 8 6kKkW8LHfFyRQ

log file /usr/local/quagga/etc/conf/zebra.log

log stdout

service password-encryption

!

interface eth0

ipv6 nd suppress-ra

!

interface eth1

ipv6 nd suppress-ra

!

interface lo

!

interface sit0

ipv6 nd suppress-ra

!

line vty

!

- Editar el archivo de configuración para la sesión BGP:

  /usr/local/quagga/etc/conf/bgpd.conf:

  !

  ! Zebra configuration saved from vty

  ! 2012/07/06 16:19:55

  !

  hostname bgpNodoAnycast

  password 8 fvhv.RZr6O3.6

enable password 8 QRHFc5fmDte4w

log file /usr/local/quagga/etc/conf/bgpd.log

service password-encryption

!

router bgp #NUMERO-SISTEMA-AUTONOMO

bgp router-id #IP-DEL-SERVIDOR

bgp log-neighbor-changes

network PREFIJO/24

neighbor IP-ROUTER-VECINO remote-as 22724

neighbor IP-ROUTER-VECINO soft-reconfiguration inbound

neighbor IP-ROUTER-VECINO prefix-list default in

neighbor IP-ROUTER-VECINO prefix-list nodoAnycast out

ip prefix-list default seq 5 permit 0.0.0.0/0

ip prefix-list nodoAnycast seq 5 permit PREFIJO/24

!

line vty

!

2.3.13 FIREWALL Y HARDENING DE SERVICIOS DEL SERVIDOR

Para proteger el servidor se deben de aplicar las siguientes reglas de filtrado de paquetes que autorizaran todo el tráfico éntrate con destino al puerto 53 usado por el servicio de DNS, también se restringirá el acceso para fines de administración y monitoreo solo para direcciones IP autorizadas al puerto 22 usado por el servicio de SSH y se denegara todo el tráfico que sea invalido.

cd /root/

vi reglasFirewall.sh:

```
#!/bin/sh
#Se detiene  el servicio de IPtable.
service iptables stop
echo -n Aplicando Reglas de Firewall...
# Reseteo de reglas
accion=”DROP”
iptables -F
iptables -X
iptables -Z
iptables -t nat -F

# Estas Son politicas por Default DROP
iptables -P INPUT $accion
iptables -P OUTPUT $accion
iptables -P FORWARD $accion
# Esta es una cadena definida por el Usuario que sirve para manejar
# conexiones entrantes invalidas
iptables -N paquetes_tcp_invalidos
# Estas son cadenas definidas por el Usuario
iptables -N allowed
iptables -N paquetes_tcp
iptables -N paquetes_udp
iptables -N paquetes_icmp
```

```
# Esta cadena rechaza conexiones con status NEW que tienen activadas las banderas SYN,ACK lo cual no es válido por
# que la máquina de conexiones tiene marcada la bandera NEW, enviando un mensaje al host que envió el paquete
iptables -A paquetes_tcp_invalidos -p tcp --tcp-flags SYN,ACK SYN,ACK -m state --state NEW -j REJECT --reject-with tcp-reset

#Luego le aplico la politca de DROP
iptables -A paquetes_tcp_invalidos -p tcp ! --syn -m state --state NEW -j DROP
# allowed chain
iptables -A allowed -p TCP --syn -j ACCEPT
iptables -A allowed -p TCP -j DROP
# reglas TCP
iptables -A paquetes_tcp -p TCP -s IP-AUTORIZADAS --dport 22 -j allowed
iptables -A paquetes_tcp -p TCP -s IP-ROUTER-VECINO --dport 179 -j allowed
iptables -A paquetes_tcp -p TCP -s 0/0 --dport 53 -j ACCEPT

# reglas UDP
iptables -A paquetes_udp -p UDP -s 0/0 --dport 53 -j ACCEPT
iptables -A paquetes_udp -p UDP -s IP-ROUTER-VECINO --dport 179 -j ACCEPT
# reglas ICMP
#Permito paquetes ICMP del tipo Echo request
```

```
iptables -A paquetes_icmp -p ICMP -s IP-AUTORIZADAS --icmp-type 8 -j ACCEPT
# cadena INPUT
# Bad TCP packets we don't want.
# Primero se envia todos los paquetes TCP a la cadena paquetes_tcp_invalidos para ver si son paquetes validos
iptables -A INPUT -p tcp -j paquetes_tcp_invalidos

# Acepta todo trafico para interface loop (lo) con direccion fuente ip 127.0.0.1
iptables -A INPUT -p ALL -i lo -j ACCEPT

# Reglas para paquetes entrantes provenientes de Internet
iptables -A INPUT -p ALL -i eth0 -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A INPUT -p UDP -i eth0 -j paquetes_udp
iptables -A INPUT -p TCP -i eth0 -j paquetes_tcp
iptables -A INPUT -p ICMP -i eth0 -j paquetes_icmp

# cadena OUTPUT
# registro de paquetes invalidos
iptables -A OUTPUT -p ALL -o lo -j ACCEPT
iptables -A OUTPUT -p ALL -o eth0 -j ACCEPT
```

Al instalar la versión mínima de Centos 6 este solo instala los servicios necesarios para su funcionamiento disminuyendo el número de puertos abiertos innecesarios.

De manera predeterminada el proceso de instalación del sistema operativo habilita el servicio de correo **sendmail** y el servicio de servidor web **httpd**

Para deshabilitar estos servicios se debe de ejecutar el siguiente comando:

chkconfig –del httpd

chkconfig –del sendmail

2.3.14 SCRIPTS PARA INICIO DE LOS SERVICIOS DE FIREWALL, NAMED Y QUAGGA

Al momento del arranque del servidor, los comandos especificados en el archivo /etc/rc.local iniciaran los servicios necesarios para levantar el Nodo Anycast de DNS

```
#!/bin/sh
#
# This script will be executed *after* all the other init scripts.
# You can put your own initialization stuff in here if you don't
# want to do the full Sys V style init stuff.
touch /var/lock/subsys/local
/root/reglasFirewall.sh
/usr/local/sbin/named -u named -c /etc/named.conf
/usr/local/sbin/zebra -d
/usr/local/sbin/bgpd –d
```

CAPITULO 3

ANÁLISIS DE RESULTADOS

3.1 SIMULACIÓN DE ATAQUE DE DOS O FALLOS DE HARDWARE

Cuando un atacante tiene en la mira un servidor de DNS autoritativo, este tiene toda su red de computadores BOTNET configurados y listos para ejecutar el ataque de denegación de servicios Distribuidos DDOS.

El atacante tiene el control de cada uno de los computadores miembros de la BOTNET desde un computador central y envía la orden de ataque desde este.

Cada computador que forma parte de la BOTNET envía constantes consultas de nombres de dominios de forma aleatoria hasta el punto de saturar los recursos del servidor causando una sobrecarga de la memoria RAM, incremento en tamaño de archivos de Logs ocupando espacio en disco y consumo excesivo del ancho de banda lo que ocasionara la interrupción de la

sesión BGP entre el servidor de servicio de DNS con el Ruteador de Borde del Proveedor de servicio de Internet.

Al caerse la sesión BGP entre el ruteador de Borde y el Servidor de DNS, este ya no estará disponible para recibir consultas de nombres de dominios.

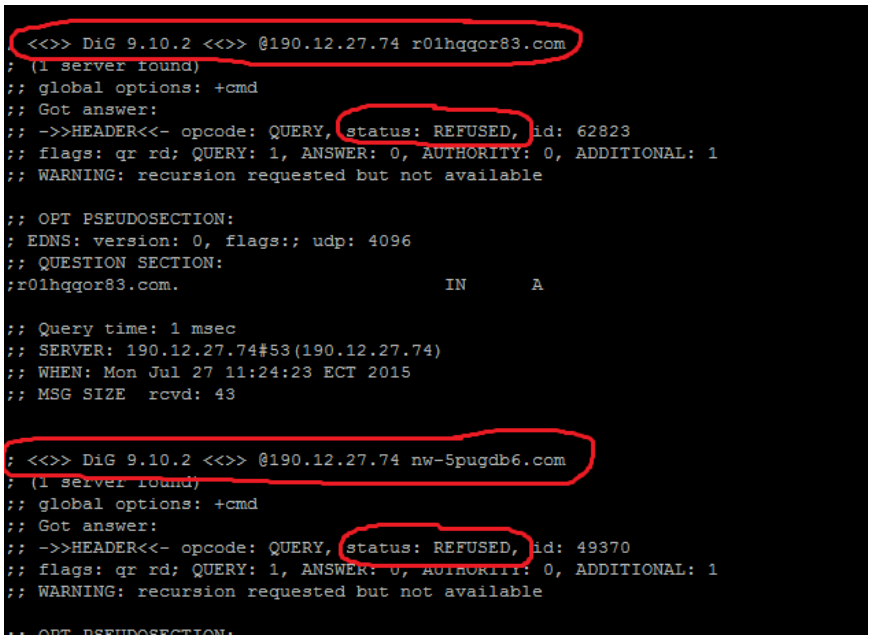


Figura 3.1 Consulta de dominios con nombres aleatorios

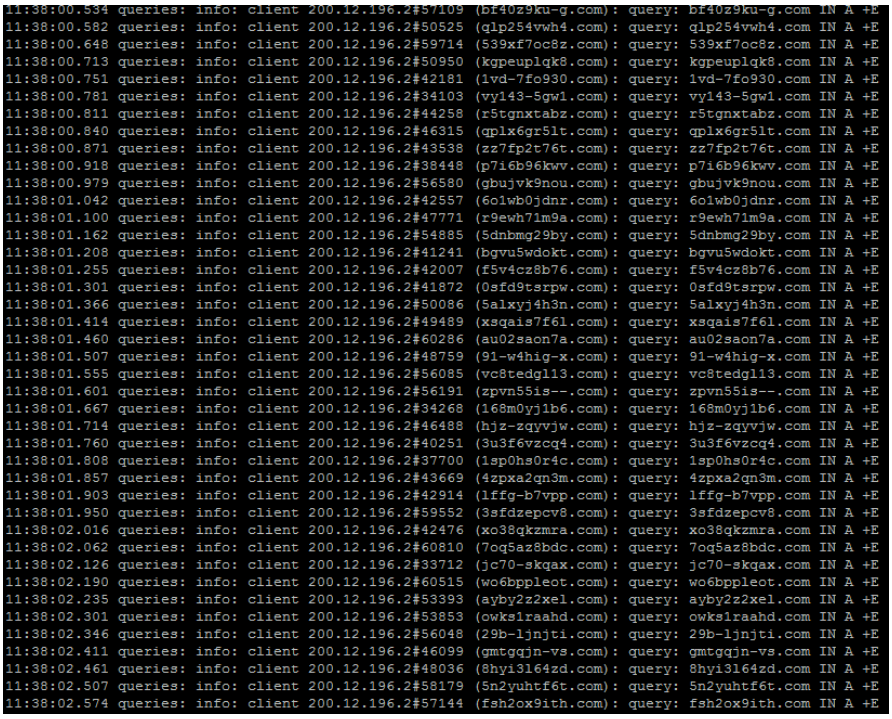


Figura 3.2 Consultas recibidas en el DNS Autoritativo

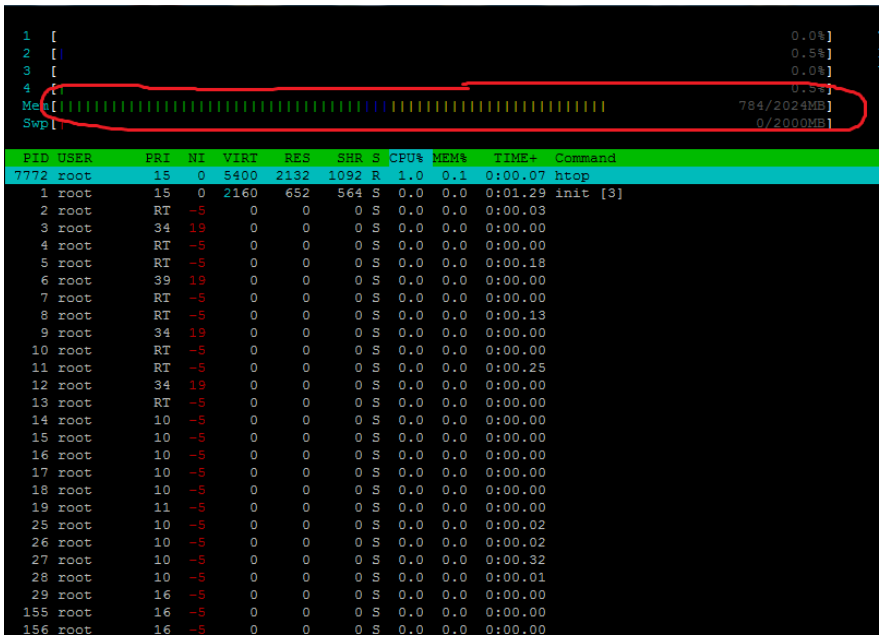
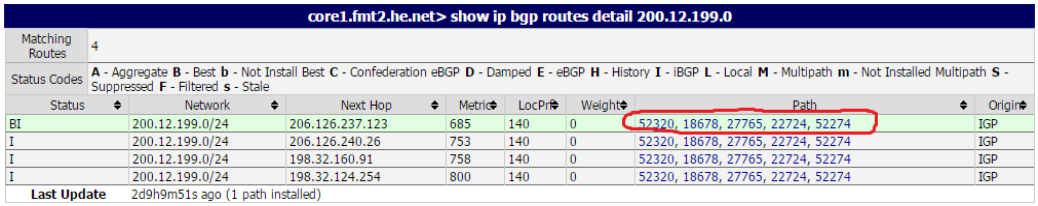


Figura 3.3 Incremento en el consumo de memoria

3.2 PRUEBAS DE LOOKING GLASS Y VERIFICACIÓN DE AS-PATH

En el grafico podemos observar que el nodo de DNS que tiene preferencia en la tabla de BGP de internet y que es el seleccionado para la consulta de los nombres de dominios, es el que se encuentra atrás del AS 22724.



core1.fmt2.he.net> show ip bgp routes detail 200.12.199.0

Matching Routes: 4

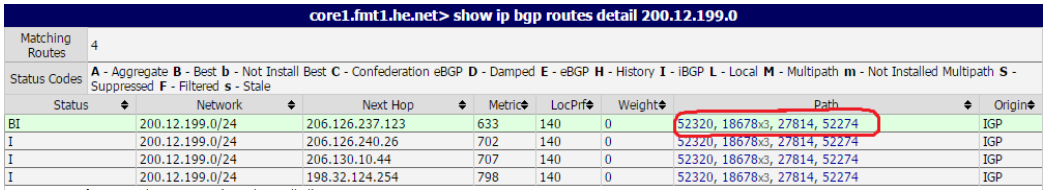
Status Codes: **A** - Aggregate **B** - Best **b** - Not Install Best **C** - Confederation eBGP **D** - Damped **E** - eBGP **H** - History **I** - iBGP **L** - Local **M** - Multipath **m** - Not Installed Multipath **S** - Suppressed **F** - Filtered **s** - Stale

Status	Network	Next Hop	Metric	LocPrf	Weight	Path	Origin
BI	200.12.199.0/24	206.126.237.123	685	140	0	52320, 18678, 27765, 22724, 52274	IGP
I	200.12.199.0/24	206.126.240.26	753	140	0	52320, 18678, 27765, 22724, 52274	IGP
I	200.12.199.0/24	198.32.160.91	758	140	0	52320, 18678, 27765, 22724, 52274	IGP
I	200.12.199.0/24	198.32.124.254	800	140	0	52320, 18678, 27765, 22724, 52274	IGP

Last Update 2d9h9m51s ago (1 path installed)

Figura 3.4 Nodo DNS con preferencia en Internet

Cuando un nodo de DNS deje de funcionar ya sea por una interrupción causada por un ataque de denegación de Servicio o por un fallo de algún componente de hardware, automáticamente otro nodo de DNS miembro de la nube Anycast aparecerá en la tabla de BGP de internet, posicionándose como el servidor preferente y será usado para la consultas de nombres de dominios.



core1.fmt1.he.net> show ip bgp routes detail 200.12.199.0

Matching Routes: 4

Status Codes: **A** - Aggregate **B** - Best **b** - Not Install Best **C** - Confederation eBGP **D** - Damped **E** - eBGP **H** - History **I** - iBGP **L** - Local **M** - Multipath **m** - Not Installed Multipath **S** - Suppressed **F** - Filtered **s** - Stale

Status	Network	Next Hop	Metric	LocPrf	Weight	Path	Origin
BI	200.12.199.0/24	206.126.237.123	633	140	0	52320, 18678x3, 27814, 52274	IGP
I	200.12.199.0/24	206.126.240.26	702	140	0	52320, 18678x3, 27814, 52274	IGP
I	200.12.199.0/24	206.130.10.44	707	140	0	52320, 18678x3, 27814, 52274	IGP
I	200.12.199.0/24	198.32.124.254	798	140	0	52320, 18678x3, 27814, 52274	IGP

Figura 3.5 Nuevo Nodo de DNS Anycast Disponible

El tiempo de transición del posicionamiento y publicación de un nuevo Nodo de DNS en caso de la ausencia de otro en la modalidad Anycast es de menos de un minuto imperceptible para los usuarios.

3.3 PRUEBAS DE TRAZAS DE PAQUETES

Otra prueba recomendable para verificar la conectividad de los Nodos de DNS es la prueba de traza de paquetes o **traceroute.**

A continuación podemos observar que la traza de paquetes pasa por el ruteador con la dirección IP 200.24.159.70 en el salto 9 perteneciente al ruteador del proveedor de internet que tiene la preferencia en la tabla de BGP.

core1.fmt1.he.net> traceroute 200.12.199.1

Target	200.12.199.1
Hop Start	1
Hop End	30

Hop	Packet 1	Packet 2	Packet 3	Hostname
1	10.588 ms	10.661 ms	10.684 ms	**ge5-1.core1.fmt1.he.net** (64.62.134.129)
2	0.731 ms	0.763 ms	0.704 ms	**10ge1-1.core1.pao1.he.net** (184.105.213.66)
3	72.408 ms	68.496 ms	68.583 ms	**10ge1-3.core1.ash1.he.net** (184.105.213.178)
4	70.855 ms	70.843 ms	70.828 ms	**eqix-dc2.cabos-submarinos.com** (206.126.237.123)
5	82.182 ms	82.169 ms	81.845 ms	200.16.69.0
6	121.210 ms	*	121.624 ms	200.16.69.61
7	*	*	*	-
8	*	*	*	-
9	146.409 ms	146.790 ms	146.654 ms	200.24.159.70
10	147.241 ms	147.408 ms	147.103 ms	200.12.199.1

Figura 3.6 Traceroute hacia Nodo DNS con preferencia en Internet

Al no estar disponible el nodo que se encontraba como preferente en la tabla de BGP, automáticamente el segundo nodo se encuentra disponible en internet y puede ser alcanzado por una traza.

core1.fmt1.he.net> traceroute 200.12.199.1

Target	200.12.199.1
Hop Start	1
Hop End	30

Hop	Packet 1	Packet 2	Packet 3	Hostname
1	0.184 ms	0.261 ms	0.279 ms	**ge5-1.core1.fmt1.he.net** (64.62.134.129)
2	0.757 ms	1.078 ms	1.114 ms	**10ge1-1.core1.pao1.he.net** (184.105.213.66)
3	70.419 ms	70.351 ms	70.416 ms	**10ge1-3.core1.ash1.he.net** (184.105.213.178)
4	70.844 ms	70.867 ms	70.852 ms	**eqix-dc2.cabos-submarinos.com** (206.126.237.123)
5	108.290 ms	108.251 ms	81.823 ms	200.16.69.0
6	*	*	123.864 ms	- 200.16.69.61
7	135.264 ms	131.931 ms	134.733 ms	200.16.70.174
8	145.927 ms	146.687 ms	*	179.1.100.5
9	148.430 ms	152.784 ms	149.230 ms	179.1.100.6
10	152.156 ms	147.416 ms	147.462 ms	200.12.199.1

Figura 3.7 Traceroute hacia nuevo Nodo de DNS Anycast Disponible

3.4 PRUEBAS Y REVISIÓN DE CONTINUIDAD DEL SERVICIO DE DNS

Para verificar la disponibilidad del servicio de DNS solamente es necesario realizar una consulta de dominio al servidor de DNS Autoritativo.

Estas consultas se las pueden realizar en varias herramientas como **nslookup** en ambientes Windows, **dig** en ambientes Linux o con cualquier herramienta disponible en internet.

Para el laboratorio se verificara la información de los dominios ispnet.ec y cliente1.com.ec.

A continuación consultaremos la información de los servidores autoritativos para el dominio ispnet.ec

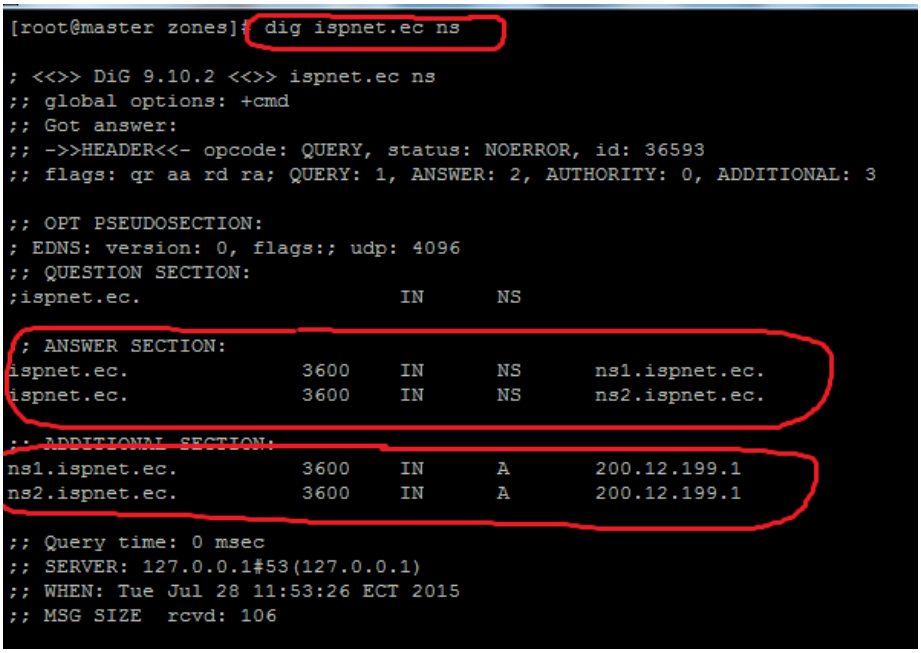


Figura 3.8 Consulta de los servidores autoritativos del dominio ispnet.ec

En la consulta anterior podemos observar que los servidores de DNS Autoritativos para el dominio ispnet.ec son ns1.ispnet.ec y ns2.ispnet.ec ambos

servidores fueron declarados y configurados con la dirección IP 200.12.199.1 anunciado por el proveedor de internet por medio de BGP.

A continuación consultaremos la información de los servidores autoritativos para el dominio cliente1.com.ec

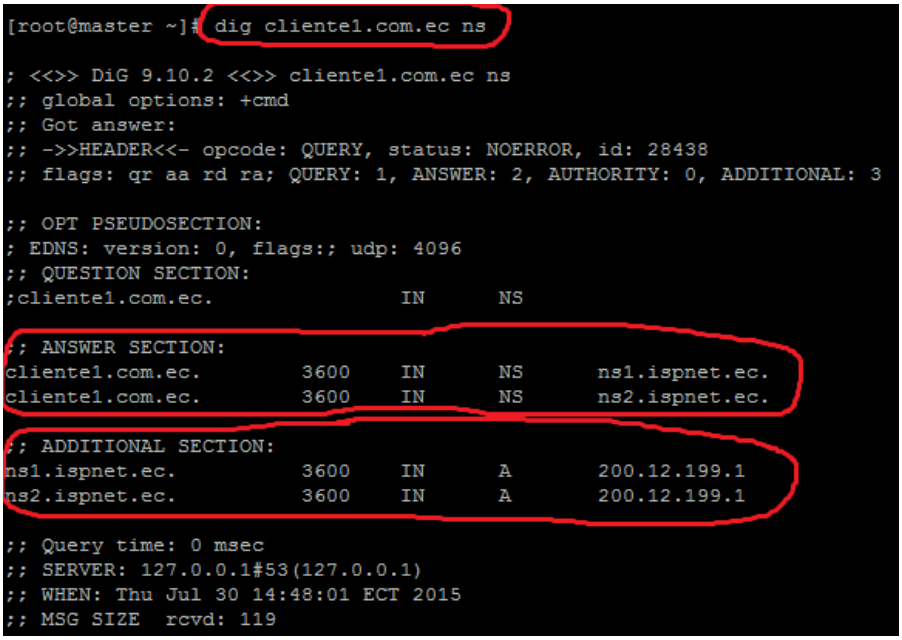


Figura 3.8 Consulta de los servidores autoritativos del dominio cliente1.com.ec

En la consulta anterior podemos observar que los servidores de DNS Autoritativos para el dominio cliente1.com.ec son ns1.ispnet.ec y ns2.ispnet.ec.

El direccionamiento IP Anycast hará que el servidor de DNS autoritativo ns1.ispnet.ec y ns2.ispnet.ec con la dirección IP 200.12.199.1 este siempre disponible en internet.

CONCLUSIONES

1. Hoy en día es muy fácil ejecutar un ataque de denegación de servicio y los servidores de DNS son blanco fácil para estos ataques
2. Configurar los servidores de DNS con direcciones IP Unicast representan un punto crítico con una alta probabilidad de riesgo e indisponibilidad de servicio
3. Mientras más Nodos de DNS Anycast se configuren, se disminuye el riesgo de una indisponibilidad del servicio y los ataques de denegación de servicio pasaran a ser imperceptibles a los usuarios.
4. El tiempo de restauración de un nodo de DNS Anycast en ausencia de otro es de menos de un minuto.

RECOMENDACIONES

1. Adicional a la configuración de los nodos de DNS Anycast dentro de la propia infraestructura del ISP se recomienda contratar este servicio con otros proveedores ya que estos brindaran un mayor número de réplicas ubicadas en distintos lugares geográficos.
2. Siempre que se instale un sistema operativo para el despliegue de un servidor de servicio de DNS se recomienda ejecutar el proceso de instalación mínimo necesario. Este tipo de instalación disminuirá el espectro de vulnerabilidades que un atacante puede explotar
3. Es altamente recomendable configurar servidor de DNS MASTER de manera oculta y no disponible en internet para que su función sea única y exclusiva para la transferencia de Zonas hacia los servidores Secundarios o Esclavos.
4. Se recomienda definir una lista de acceso en el archivo named.conf del servidor de DNS Master que incluya las direcciones IP Unicast de los

servidores secundarios para que estos sean los únicos autorizados en poder realizar la transferencia de zonas.

5. Se recomienda usar firmas TSIG en la trasferencia de zonas entre los servidores secundarios y Maestros.
6. Se recomienda tener más de un servidor Maestro en caso de contingencia
7. Se puede usar direccionamiento Anycast en otras implementaciones como servidores de correo y web.

BIBLIOGRAFÍA

[1] Wikipedia, Dominio de Internet, http://es.wikipedia.org/wiki/Dominio_de_Internet, fecha de consulta Julio 2015.

[2] Liu Cricket, DNS and BIND, O'reilly, fecha de consulta Julio 2015.

[3] Liu Cricket, DNS and BIND, O'reilly, fecha de consulta Julio 2015.

[4] Liu Cricket, DNS and BIND, O'reilly, fecha de consulta Julio 2015.

[5] Liu Cricket, DNS and BIND, O'reilly, fecha de consulta Julio 2015.

[6] Cabrera César, Comprendiendo el enrutamiento en Internet, http://cesarcabrera.info/blog/comprendiendo-el-enrutamiento-en-un-sistema-autonomo/, fecha de consulta Julio 2015.

[7] Cisco Systems, CCNP ROUTE: Implementing BGP, Cisco Networking Academy, fecha de consulta Julio 2015.

[8] Cabrera César, Comprendiendo el enrutamiento en Internet, http://cesarcabrera.info/blog/comprendiendo-el-enrutamiento-en-un-sistema-autonomo/, fecha de consulta Julio 2015.

[9] Wikipedia, Border Gateway Protocol, http://es.wikipedia.org/wiki/Border_Gateway_Protocol, fecha de consulta Julio 2015.

[10] Cabrera César, Comprendiendo el enrutamiento en Internet, http://cesarcabrera.info/blog/comprendiendo-el-enrutamiento-en-un-sistema-autonomo/, fecha de consulta Julio 2015.

[11] Wikipedia, Border Gateway Protocol, http://es.wikipedia.org/wiki/Border_Gateway_Protocol, fecha de consulta

[12] Wikipedia, Border Gateway Protocol, http://es.wikipedia.org/wiki/Border_Gateway_Protocol, fecha de consulta Julio 2015.

[13] Wikipedia, Border Gateway Protocol, http://es.wikipedia.org/wiki/Border_Gateway_Protocol, fecha de consulta Julio 2015.

[14] Wikipedia, Border Gateway Protocol, http://es.wikipedia.org/wiki/Border_Gateway_Protocol, fecha de consulta Julio 2015.

[15] Cisco Systems, CCNP ROUTE: Implementing BGP, Cisco Networking Academy, fecha de consulta Julio 2015.

[16] Wikipedia, Unicast, https://es.wikipedia.org/wiki/Unicast, fecha de consulta Julio 2015.

[17] Wikipedia, Anycast, https://es.wikipedia.org/wiki/Anycast, fecha de consulta Julio 2015.