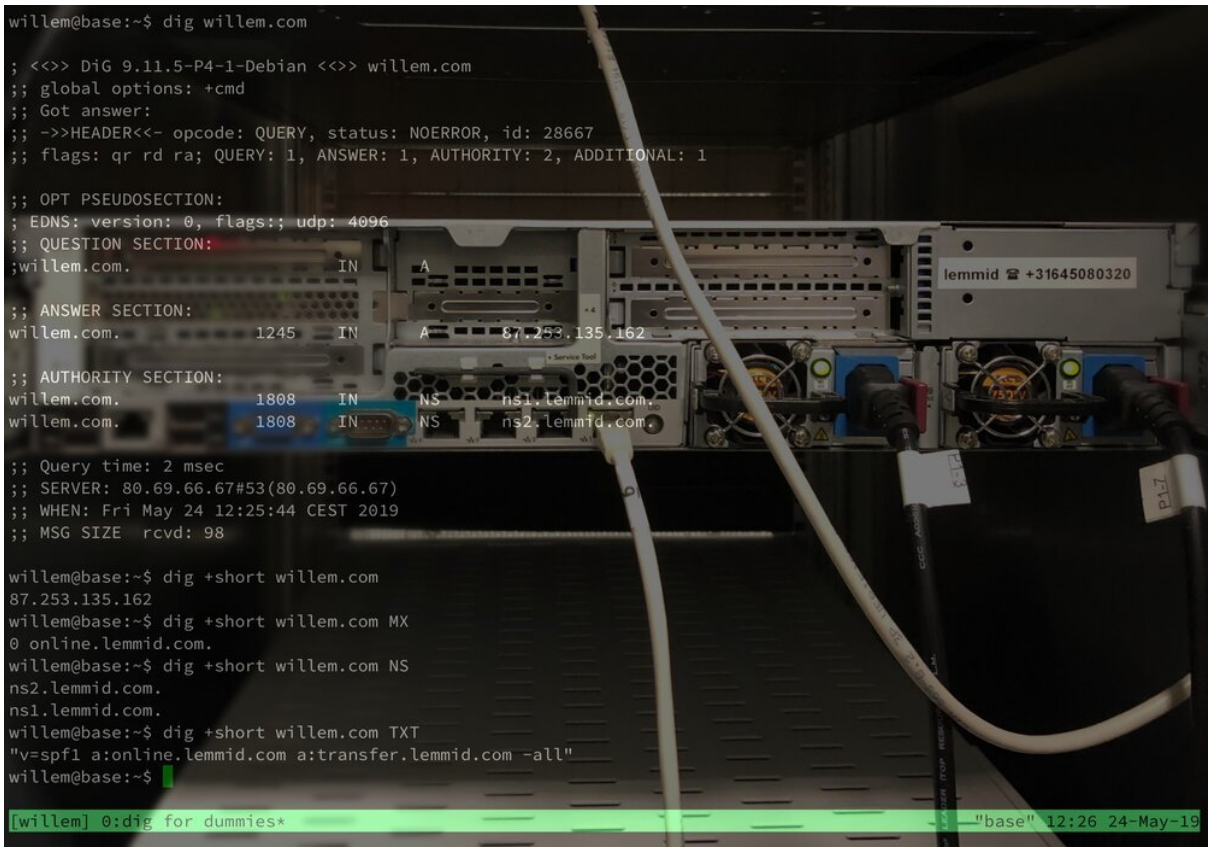
Dig para principiantes

Explicando una herramienta de red muy útil

Willem L. Middelkoop
May 24, 2019



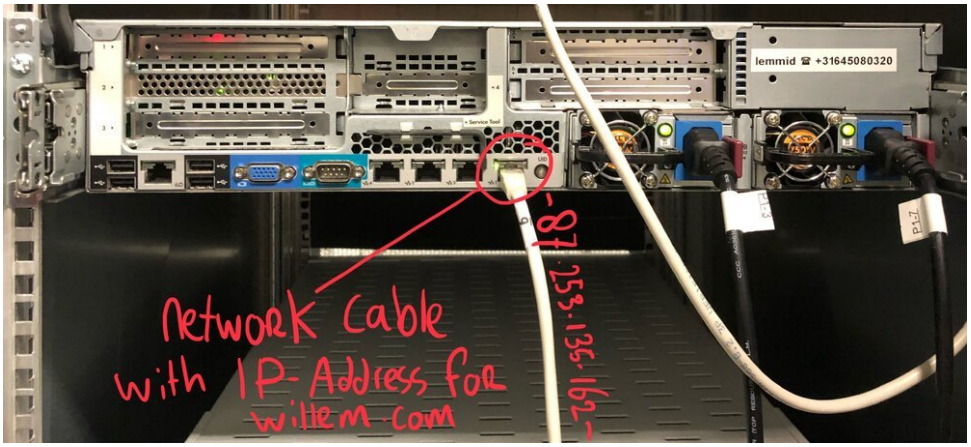
Cuando construyes sitios web, aplicaciones o servicios de correo electrónico, puedes encontrarte con nombres de dominio y sus configuraciones. Cuando todo funciona como debería, la mayor parte de esto es invisible. Pero al solucionar problemas de la configuración de un nombre de dominio, puede ser necesario profundizar un poco más... ¡sigue leyendo para aprender cómo!

Sistema de Nombres de Dominio (DNS)

Internet funciona utilizando direcciones numéricas de protocolo de internet (IP) como medio para localizar e identificar computadoras, servicios (en la nube) y dispositivos en línea. En lugar de memorizar todas estas direcciones IP, el sistema de nombres de dominio se ha convertido en el servicio de directorio mundial esencial, vinculando nombres a números.

Estás leyendo esto en **willem.com**, pero en realidad este nombre de dominio es simplemente un puntero para una máquina física, conectada a internet (¡con cables, de verdad!).

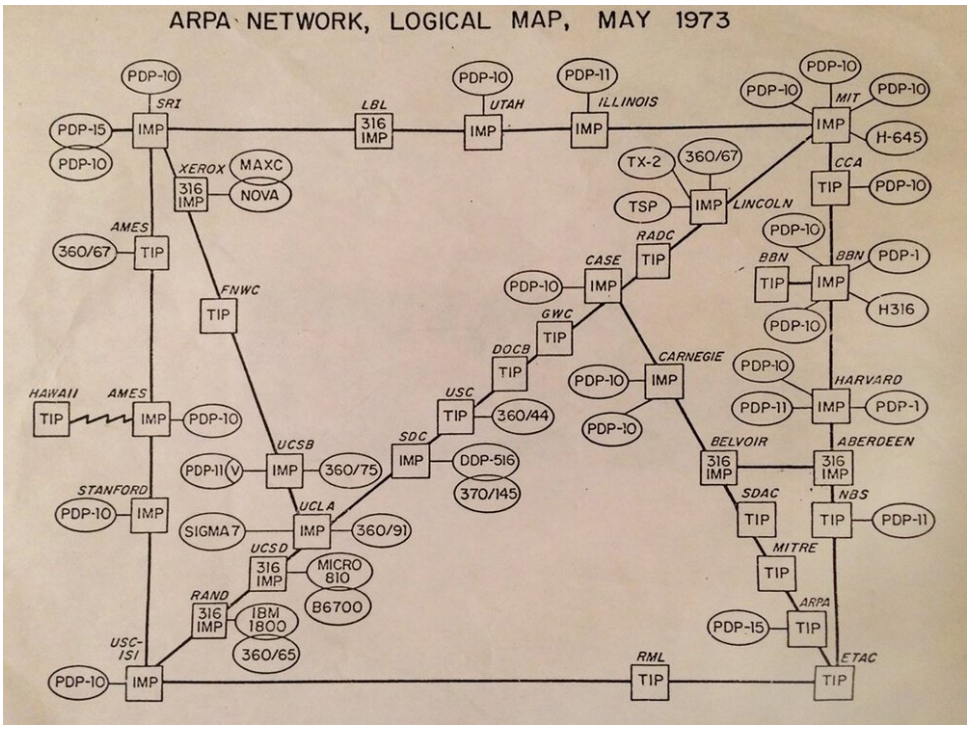
Uno de esos cables está vinculado a la dirección IP **87.253.135.162**. Es responsabilidad del servidor DNS mantener los números correctos (dirección IP) coincidentes con los nombres (de dominio).



El Sistema de Nombres de Dominio (DNS) vincula nombres de dominio a direcciones IP, que a su vez se enrutan a través de cables. ¡Estás leyendo esto, en serio, a través del cable conectado al servidor que se muestra en esta foto!

Distribuido y descentralizado

Cuando los estadounidenses diseñaron su ARPANET a principios de los setenta, uno de sus requisitos de diseño militar era que la red sobreviviera a los ataques (de los enemigos). Lo lograron implementando la conmutación de paquetes, una forma de compartir y reutilizar los cables de red por varias personas de múltiples maneras. Si una parte de la red se daña, los paquetes de información se redirigen a través de otras partes de la red.



[image]

Para lograr la máxima supervivencia, no existe un único servidor DNS raíz. En su lugar, el sistema de nombres de dominio delega la responsabilidad de asignar nombres de dominio y las asignaciones a esos nombres designando un servidor de nombres autorizado para cada nombre de dominio.

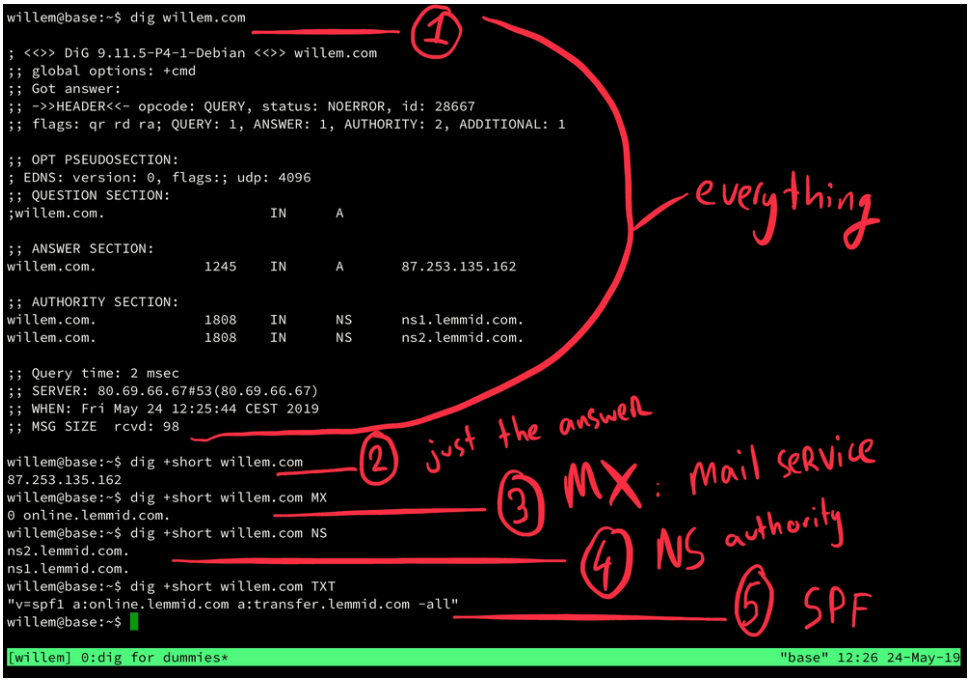
Es por eso que hay muchas configuraciones y servidores DNS diferentes. Con tantas formas y lugares donde las cosas pueden salir mal, necesitas una herramienta para investigar.

dig (buscador de información de dominio)

El comando 'dig' es una herramienta para interrogar a los servidores de nombres DNS para obtener información sobre direcciones IP, nombres de host, servidores de correo y otros tipos de configuraciones de red. El comando dig está disponible en Unix, macOS, GNU/Linux y Windows.

Usando dig para consultar servidores de nombres de dominio

Puedes usar dig para obtener información sobre un nombre de dominio determinado simplemente escribiendo: 'dig willem.com'. Consulta la siguiente captura de pantalla con la explicación:



Un mapa de ARPANET en 1973... ¡imagínense mapear el internet hoy! (Dominio público)

- 1) **dig willem.com** devolverá toda la información sobre la pregunta, la respuesta, la autoridad (la que respondió la pregunta) y las estadísticas de la consulta real (como cuánto tiempo tardó en obtener una respuesta).
- 2) **dig +short willem.com** omite toda la información adicional y solo devuelve la respuesta. Aquí puedes ver que **willem.com** apunta a la dirección IP **87.253.135.162**.

- 3) **dig +short willem.com MX** te mostrará los registros de intercambio de correo (MX). Los registros MX son cruciales para que el correo electrónico llegue al servidor correcto. Básicamente, es la designación de la oficina de correos responsable del correo electrónico vinculado al nombre de dominio. Para **willem.com**, este es un servicio de correo llamado **online.lemmid.com**. Otros servicios de correo populares son Office365 y Google Gmail. Usando dig, puedes averiguar qué servicio de correo electrónico está utilizando alguien.
- 4) **dig +short willem.com NS** te mostrará los servidores de nombres que son responsables de manejar las consultas para este nombre de dominio. Por lo general, estos son los servidores operados por el registro de nombres de dominio, tu proveedor de nombres de dominio. Usando dig puedes encontrar qué tipo de proveedor de nombres de dominio está usando alguien (en el caso de **willem.com**, es **Lemmid**).
- 5) **dig +short willem.com TXT** devolverá el registro de texto vinculado al nombre de dominio, aquí es donde encontrarás el llamado registro SPF. El registro SPF es otra parte crucial del correo electrónico, es útil profundizar un poco más en SPF.

Marco de Políticas de Remitente (SPF)

Para detectar direcciones de remitente falsificadas en correos electrónicos (el llamado spoofing de correo electrónico), el estándar SPF se definió en 2004. Originalmente llamado "Remitente Permitido Desde", SPF es una forma de verificar si alguien está autorizado a enviar correo electrónico en nombre de un nombre de dominio determinado. SPF permite al propietario de un nombre de dominio especificar qué computadoras están autorizadas a enviar correo electrónico con direcciones DE ese dominio.

Si el propietario de un nombre de dominio publica un registro SPF, es menos probable que los spammers y phishers (ab)usen del nombre de dominio para enviar correos electrónicos falsificados, pretendiendo ser de ese dominio. Por lo tanto, es menos probable que un dominio protegido por SPF sea incluido en la lista negra de los filtros de spam, lo que hace que sea más probable que el correo electrónico legítimo del dominio llegue. Sin embargo, un registro SPF mal configurado puede interrumpir la entrega de correo electrónico.

Usando dig para consultar registros SPF

Usando el comando dig, puedes consultar un registro SPF y ver cuál es la política exacta del remitente. Consulta la siguiente captura de pantalla con la explicación:

[image]

- 1) **dig +short TXT google.com** nos mostrará el registro TXT vinculado configurado para google.com, el lugar donde puedes encontrar el registro SPF (entre otras cosas). El registro SPF para **google.com** es **"v=spf1 include:_spf.google.com ~all"**. La parte **include:** significa que para este nombre de dominio también se deben cargar valores SPF externos.
- 2) **dig +short TXT _spf.google.com** muestra cuáles son esos valores SPF externos para **google.com**. En este caso, revela otras tres inclusiones: "_netblocks.google.com", "_netblocks2.google.com" y (qué original...) "_netblocks3.google.com".
- 3) **dig +short TXT _netblocks.google.com** (y las variantes 2 + 3) especifican las direcciones IP reales que pueden enviar correo electrónico en nombre de **google.com**. Como Google es una gran empresa de internet, hay muchas direcciones IP en estas listas. Si miras con atención, notarás que algunas de estas direcciones tienen un sufijo "/", como "/24". Esta es la forma de anotar un bloque completo (por ejemplo, calle) de direcciones IP.

Explicación de los bloques de IP

La forma más fácil de entender la notación de bloques de direcciones IP es mediante los siguientes ejemplos:

- **/8 = 255.0.0.0**
- **/16 = 255.255.0.0**
- **/24 = 255.255.255.0**
- **/32 = 255.255.255.255**

Donde veas '0' en las direcciones anteriores, se incluyen otros valores. Entonces, por ejemplo, 173.194.0.0/16 en realidad significa "todas las direcciones que comienzan con '173.194'". Dadas 255 posiciones posibles en cada octeto, ¡eso es 255x255=65025 direcciones diferentes!

Conclusión

Para resolver problemas, necesitas saber dónde está el problema. Usando el comando dig, puedes aprender sobre una configuración de red y dominio determinada.

Las respuestas de un comando a otro te permiten profundizar en las entrañas de las increíbles interwebs. ¡Buena suerte!