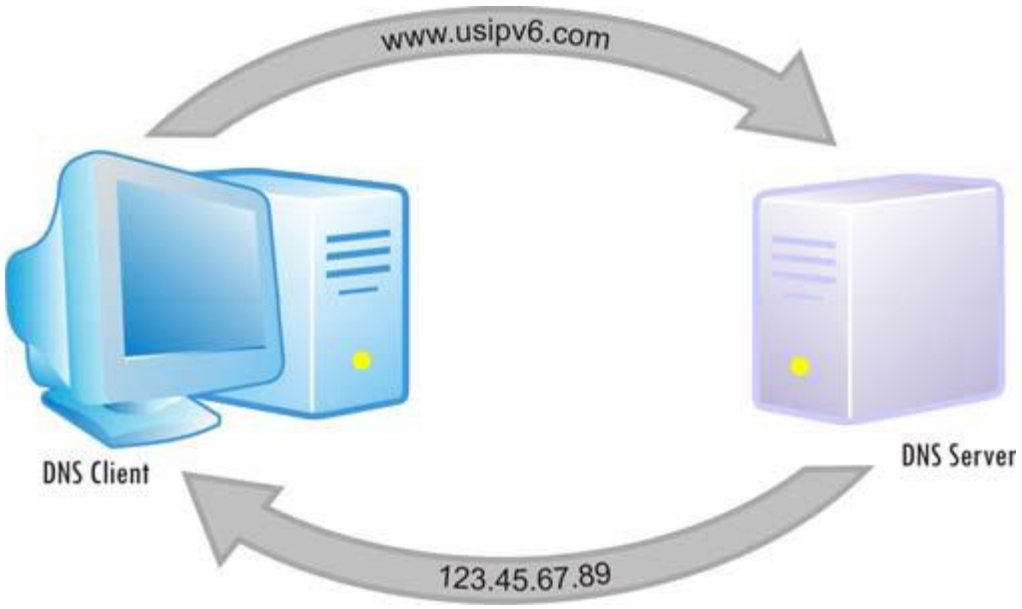
راه اندازی DNS در IPv6

DNS سامانه‌ای است که سالیان متمادی مورد استفاده قرار گرفته است. بدون DNS اینترنت از پایداری و کارایی لازم برخوردار نخواهد بود. وظیفه آن نگاشت نام دامنه سلسله مراتبی به آدرس IP است. به عنوان مثال، DNS آدرس URL، www.usipv6.com را به آدرس IP، 123.45.67.89 نگاشت می‌کند. لازم به توضیح است آدرس IP در سرآیند (Header) بسته‌ها برای هدایت استفاده می‌شود (شکل ۱ را ببینید). DNS را می‌توان مانند یک دفترچه تلفن خودکار تصور کرد.



شکل۱: روش کار سیستم نام دامنه

DNS آدرس IP را هم به نام دامنه نگاشت می‌کند و به شما اجازه می‌دهد که چیزهای به خصوصی را که لازم است دیگران آنها را بدانند منتشر کنید. مانند سرویس‌دهنده پست الکترونیکی که توسط رکورد MX[1] انجام می‌شود. شما می‌توانید سرویس‌دهنده LDPA[2] را برای نام دامنه خودتان اعلام کنید یا حتی از آن برای نگاشت یک شماره تلفن بین المللی یا جهانی به یک یا چند URL که توسط

[1] mail exchange record
[2] Lightweight Directory Access Protocol

ENUM[3] انجام می‌شود استفاده کنید، اما همه این روش‌ها محدود هستند و تنها توسط یک سازنده معمولی پشتیبانی می‌شوند و روشی که برای همه پروتکل‌ها جوابگو باشند نیستند. و از آن برای، IM[4]، VOIP[5] با استفاد از پروتکل SIP[6] استفاده می‌شود. برنامه‌های زیادی برای سرویس‌دهنده DNS وجود دارد که معروف‌ترین آنها برنامه‌ای است که توسط دانشگاه برکلی توسعه داده شده و به BIND[7] معروف است.

مایکروسافت نیز DNS مخصوص خودش را دارد که به همراه سرویس‌دهنده ویندوز ارائه می‌شود. بعضی دیگر از گروه‌ها DNS های رایگان و تجاری تولید کرده‌اند مانند Nominum که توسط آقای Paul Mockapetris (مخترع DNS) رهبری می‌شود.

هر شبکه باید یک سرویس‌دهنده DNS داشته باشد در غیر این صورت، گره‌های آن شبکه تنها با آدرس‌های IP عددی توسط سایرین قابل دسترس خواهد بود. در شبکه‌ای که فقط از محصولات مایکروسافت استفاده می‌کند (یا سیستم های مبتنی بر SMB/CIFS مانند SAMBA) می‌توان به جای DNS از WINS استفاده کرد که برای ثبت و انتشار خودکار نام‌ها استفاده می‌شود NetBIOS[8] یک فضای نام متداول است که می‌تواند آدرس‌های شبکه متنوع مانند شبکه‌های TCP/IP را نگاشت کند. این سیستم خیلی انعطاف‌پذیر نبوده و تنها در محدوده شبکه‌های LAN قابل استفاده است و به وسیله برنامه‌های کاربردی که به صورت گسترده در شبکه اینترنت کاربرد دارند قابل استفاده نمی‌باشد مانند پست الکترونیکی. امروزه حتی مایکروسافت، استفاده از DNS را برای عملیات شبکه مبتی بر SMB به جای گسترش WINS توصیه می‌کند.

IPv4 از آدرس ۳۲ بیتی که با نماد دهدهی نشان داده می‌شوند و با نقطه (.) از هم جدا می‌شوند، استفاده می‌کند (۴ گروه ۸ بیتی که هرکدام از ۰ تا ۲۵۵ متغیر است). امکان اینکه بتوان آدرس‌های IP را به خاطر سپرد سخت است ولی DNS این امر را بی‌نهایت آسان کرده است و باعث می‌شود که کاربران برای استفاده از اینترنت به دانش تخصصی بالایی نیاز نداشته نباشند.

[3] Telephone Number Mapping
[4] Instant Messaging
[5] Voice Over IP
[6] Session Initiation Protocol
[7] Berkeley Internet Naming Daemon
[8] Network Basic Input/output System

دو مفهوم اساسی در شبکه‌ها دیده می‌شود: LAN و اینترنت. برای سرویس‌دهنده‌هایی که تنها نیاز به دسترسی از طریق شبکه LAN دارند مانند Windows Server Domain Controllers یا Print Server/File Server ممکن است کاربران از طریق DNS های داخلی (یا حتی WINS) به این کامپیوتر دسترسی پیدا کنند. برای این منظور از آدرس‌های خصوصی[9] استفاده می‌شود (مطابق RFC 1918، آدرس‌های خصوصی از بازه‌های 10.x.x.x/8، 172.16.x.x/16 و 192.168.x.x/24 تشکیل شده است).

اگر سرویس‌دهنده‌هایی دارید که باید از بیرون شبکه LAN قابل دسترسی باشند (از جمله: E-mail Server یا Web Server) این گره‌ها باید توسط سرویس‌دهنده‌های DNS که از بیرون شبکه LAN قابل دسترسی باشند منتشر شوند (معمولاً این DNS ها توسط ISP یا ثبت کننده[10] راه‌اندازی می‌شود) که از آدرس‌های ثابت خارجی معتبر یا قابل مسیریابی استفاده می‌شود (این آدرس‌ها در شبکه اینترنت واحد هستند).

یک مدیر شبکه با تجربه، نام و آدرس هر گره از شبکه را که نیاز به دسترسی از راه دور باشد در DNS اضافه می‌کند. برخی از مدیران شبکه ممکن است یک سرویس‌دهنده DNS (یا حتی یک جفت برای افزونگی) را برای کاربران خارجی (با آدرس‌های عمومی) در منطقه DMZ و یک سرویس‌دهنده مجزا (یا یک جفت سرویس‌دهنده برای افزونگی) برای کاربران داخلی (با آدرس‌های خصوصی یا عمومی داخل شبکه) در شبکه داخلی پیاده‌سازی کنند. اگر مدیر شبکه خیلی با تجربه باشد می‌تواند آدرس‌های خصوصی را برای استفاده توسط گره‌های داخلی و آدرس‌های عمومی را برای گره‌های خارجی با استفاده از چند BIND در یک سرویس‌دهنده DNS (یا برای داشتن افزونگی در یک جفت DNS) پیاده‌سازی کنند که این DNS هم از طریق داخل شبکه و هم از بیرون شبکه قابل دسترسی خواهد بود.

بسیاری از مدیران شبکه با عمل هدایت[11] در DNS یعنی نگاشت نام به IP آشنا هستند بدین معنا که آنها DNS را طوری تنظیم می‌کنند که با گرفتن نام، IP تحویل دهد (همانند آدرس IP مربوط به www.innofone.com) ولی تعداد کمی با DNS معکوس[12]، یعنی نگاشت آدرس IP به نام هم آشنا هستند (مانند نام گره‌ای که آدرس IP آن 123.45.67.89است)

[9] Private
[10] Registrar
[11] Forward
[12] Reverse

اولین نوع منبع (هدایت در DNS) با تشکیل "حوزه‌های هدایت " که شامل رکوردهای A یا AAAA است، انجام می‌شود. منبع دیگر (DNS معکوس) است که شامل رکوردهای PTR است. در شبکه‌ای که به درستی طراحی شده باشد در همه گره‌ها، باید هم نگاشت هدایت (Forward) و هم نگاشت معکوس (Reverse) در سرویس‌دهنده DNS تعریف شود. چنین شبکه‌ای خیلی بهتر از شبکه‌ای کار خواهد کرد که فقط دارای حوزه‌های هدایت است. درحقیقت، بسیاری از سرویس‌دهنده‌های امروزی سعی می‌کنند که برای سرویس‌دهنده‌های پست الکترونیکی از نگاشت معکوس استفاده کنند و آدرس IP را به ارتباطی که به سمت آنها می‌آید نگاشت کنند و با استفاده از آدرس IP، نام سرویس‌دهنده را پیدا کنند. اگر این سرویس‌دهنده‌ها نتوانند این کار را انجام بدهد یا اگر نام گره با اطلاعات IP مطابقت نکند، سرویس‌دهنده‌های پست الکترونیکی بنا را بر آن خواهند گذاشت که این درخواست از سوی یک سرویس‌دهنده جعلی (Bogus Server) (تولید کننده هرزنامه، هکر و ...) است و ارتباط را قطع خواهند کرد. اگر یک سرویس‌دهنده پست الکترونیکی راه‌اندازی می‌کنید باید مطمئن باشید که هر دو نگاشت هدایت یا معکوس به درستی کار می‌کنند. در غیر این صورت نامه‌های الکترونیکی شما که بیرون می‌رود بازگشت داده شده و پذیرفته نمی‌شود. مطالب بالا هم برای IPv4 و هم برایIPv6 صادق است.

❖ چه چیزهایی در IPv6 متفاوت است؟

در IPv4 بعضی کاربران ممکن است ترجیح دهند به جای نام دامنه آدرس ۳۲ بیتی دهدهی آن را وارد کنند اما این تعداد کاربران در IPv6 به مراتب کمتر خواهد شد. به دلیل اینکه آدرس‌های IPv6 طولانی‌تر و پیچیده‌تر از آدرس‌های IPv4 است. بنابراین در IPv6، نیاز به یک سرویس‌دهنده نام دامنه (DNS)، که به طور دقیق پیکربندی شده باشد و همه گره‌ها را در برگرفته باشد، از اهمیت فوق‌العاده‌ای برخوردار بوده و فراگیرتر است و تمام گره‌هایی که می‌خواهیم به آن دسترسی داشته باشیم بایستی در DNS تعریف شده باشد. اگر بخواهیم یک تلفن VoIP از هر جای دنیا بتواند با تلفن VoIP ما تماس برقرار کند باید آدرس آن را از طریق یک سرویس‌دهنده DNS که از خارج شبکه قابل دسترسی باشد منتشر کنیم (ممکن است شما از ویژگی‌های ENUM در DNS استفاده کنید). در IPv4 یک رکورد هدایت (A) ممکن است به شکل زیر باشد:

```
www    IN      A       123.45.67.89
```

رکورد معکوس متناظر (PTR) آن ممکن است به شکل زیر باشد:

```
89.67.45.123.in-addr.arpa          PTR      www.whazzamattau.edu.
```

ممکن است با استفاده از ویژگی $origin موجود در نرم‌افزار BIND از حالت کوتاه شده دستور فوق هم برای ساده کردن محتوای آن بتوان استفاده کرد (بخصوص اگر تعداد زیادی از رکوردهای معکوس وجود داشته باشند که همه آنها از یک پسوند استفاده می‌کنند. در اینجا origin یا مبدأ نیاز دارد که با یک تعریف نوشته شود).

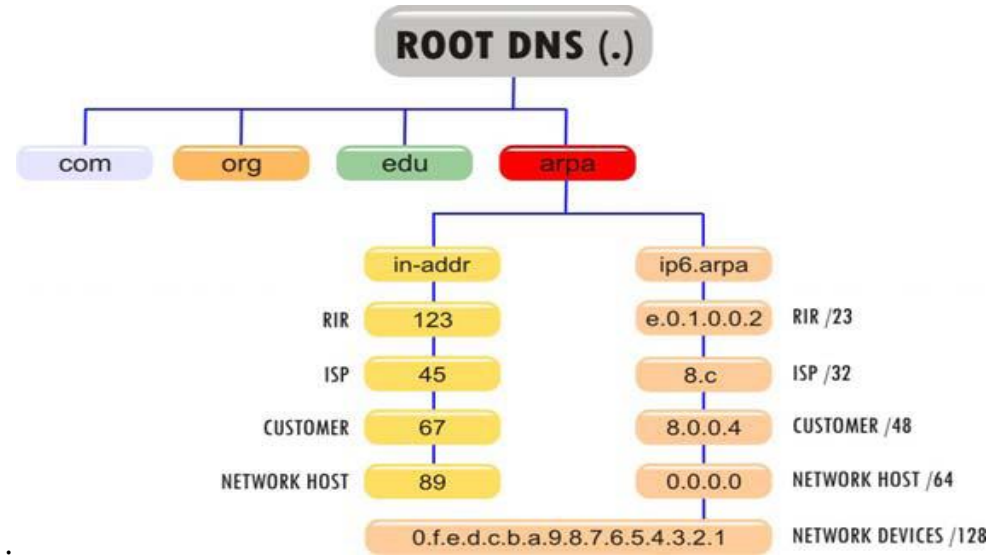
```
$origin 45.123.in-addr.arpa
89.67    PTR      www.whazzamattau.edu.
```

توجه داشته باشید که فیلدهای ۸ بیتی بطور معکوس نوشته شده و عبارت نا آشنای "in-addr.arpa" افزوده شده است. در IPv6 رکورد هدایت (AAAA) ممکن است به شکل زیر باشد:

```
www     IN       AAAA   2001:ec8:4008::1234:5678:9abc:def0
```

رکورد PTR متناظر آن هم با استفاده از قابلیت $origin ممکن است به شکل زیر باشد (شکل ۲ را ببینید).

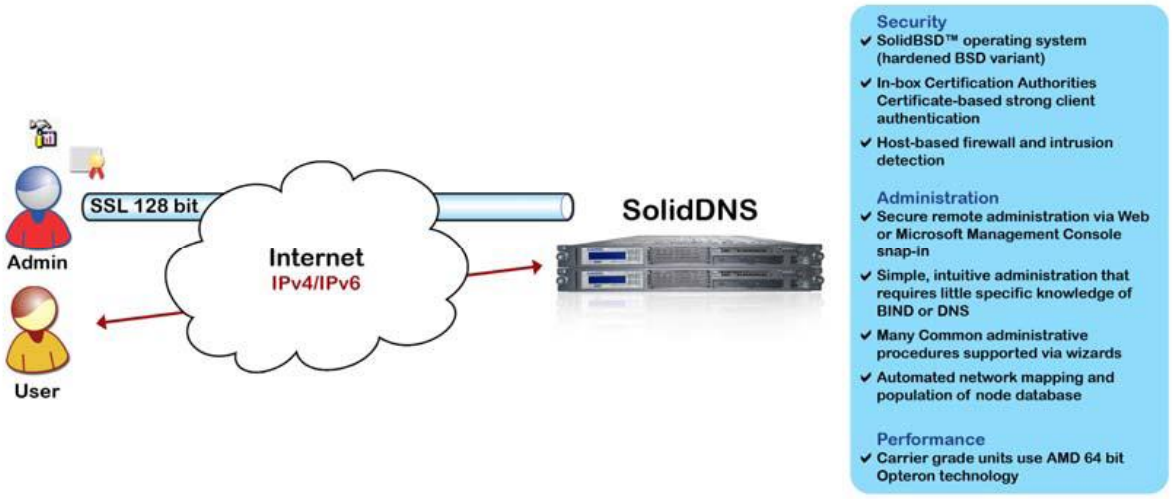
```
$origin 8.40.c8.e.1.20.ipv6.arpa
f0.de.bc.9a.78.56.34.12.0.0       PTR      www.whazzamattau.edu
```



شکل ۲: درخت نگاشت در DNS معکوس

پسوند قبلی که به حالت "ipv6.int." است، جالب نمی‌باشد و نباید استفاده شود. توجه داشته باشید که هر فیلد چهار رقمی هگزادسیمال (۱۶ بیت) به فیلدهای دو رقمی هگزادسیمال (۸بیتی) تبدیل شده و مجدداً به صورت معکوس نوشته شده است. دسترسی به رکوردهای PTR در IPv6 که در سرویس‌دهنده BIND به صورت دستی مدیریت می‌شود، برای بار اول مشکل است. این موضوع که ممکن است به نظر شما پیچیده باشد، (واقعاً هم همین‌طور است) نکاتی را که در ستون‌های شکل بالا آورده شده است، نشان می‌دهد.

در آسیا شرکت InfoWeapons محصولی برای تجاری سازی ساختار IPv6 ساخته است که SolidDNS نامیده می‌شود و این باعث شده است که پیاده‌سازی IPv6 در آسیا از آمریکا هم پیشی بگیرد. در حقیقت SolidDNS یک کپی از BIND است که بر روی یک سخت افزار مبتنی بر AMD Opteron کار می‌کند این موضوع مغایرتی با آنچه که سایر تأمین‌کنندگان DNS را در IPv6 بر روی سیستم‌های خود اجرا می‌کنند، ندارد. در واقع آنها BIND را در یک وسیله با درجه امنیت نظامی جاسازی کرده‌اند (با استفاده از تکنولوژی DARPA و تمام استانداردهای امنیتی DOD).



شکل۳: دستگاه Solid DNS تولید شده توسط Info Weapons

با استفاده از SolidDNS شما می توانید خیلی سریع دامنه‌ها و شبکه های خود را با استفاده از طول پیشوند آدرس‌ها مشخص کنید. سپس نام هر گره و آدرس متناظر آن را در SolidDNS وارد کنید. وقتی دکمه "restart" را کلیک می‌کنید SolidDNS فیلد جدیدی را تشکیل می‌دهد و فایل قلمرو هدایت[۱۳] و قلمرو معکوس[۱۴] را بطور کامل تشکیل می‌دهد. اگر شما فایل‌های مربوط به قلمروBIND را هم از قبل داشته باشید می‌توانید آنها را به پایگاه داده جدید انتقال دهید. اگر از قبل DNS تحت IPv4 داشته باشید، می‌توانید کار ورود آدرس‌های IPv6 را هم با استفاده از ابزارهای InfoWeapons به راحتی انجام داده و مدیریت کنید و برای IPv6 هم مثل IPv4 قلمرو هدایت و قلمرو معکوس کاملی تولید کنید. (برخی از مدیران شبکه بر این باورند که هرگز نباید در BIND یک قلمرو معکوس IPv6 تشکیل داد چون این کار به صورت دستی انجام شدنی نیست و یا انجام آن بسیار سخت است حال آنکه با استفاده از روش بالا تشکیل قلمرو IPv6 در BIND خیلی سریع انجام می‌شود.)

با توجه به اینکه ورود آدرس‌های IPv6 کاری زمانبر، مشکل و خطاپذیر است بنابراین با استفاده از SolidDNS به شما اجازه داده می‌شود که با پیشوندهای[۱۵] داده شده (که معمولاً ۶۴ بیتی است) نام شبکه (Network Name) را تعریف کنید. در زمان وارد کردن آدرس گره‌ها در پایگاه داده DNS شما می‌توانید نام شبکه از قبل تعریف شده را از لیست انتخاب کرده سپس ۶۴ بیت با ارزش پایین

[13] Forward Zone
[14] Reverse Zone
[15] Prefix

آدرس IPv6 را وارد کنید. قسمت واقعاً جالب قضیه این جاست که هر آدرس، نام شبکه‌ای را که برای آن تعریف شده به خاطر می‌سپارد. شما می‌توانید به عقب برگشته و پیشوند آدرس‌های نام شبکه را دوباره تعریف کنید و تمام فایل‌های قلمرو هدایت و قلمرو معکوس را با استفاده از پیشوند جدید تشکیل دهید. با این کار، بدون آنکه DNS را خاموش کنید آن عملی که لازم است تا رکوردهای DNS از IPv6 پشتیبانی نماید انجام می‌شود. فایل‌هایی که با این روش برای قلمروهای مختلف با BIND تشکیل شده است دارای رکوردهای AAAA کامل هستند. با انجام این کار شما می‌توانید شماره‌گذاری مجدد پیشوند را در کسری از ثانیه انجام دهید در صورتی که اگر آن را بطور مستقیم با استفاده از BIND برای یک سایت بزرگ انجام دهید، هفته‌ها به طول می‌انجامد.

DNS پویا (DNSی که رکوردهای آن به صورت خودکار از DHCP گرفته می‌شود) کمی پیچیده‌تر است زیرا، برنامه کاربردی از فایل‌های پیکربندی یک پایگاه داده تولید می‌کند. همچنین به طور عادی، داده‌های جدید در داخل فایل‌های پیکربندی BIND وارد می‌شود. SolidDNS هم از ثبت پویا جلوگیری می‌کند (اجازه ثبت از DHCP یا هر منبع دیگر را نمی‌دهد) بلکه این داده‌های دریافت شده دستی را به داخل پایگاه داده برده و در گام بعدی GUI را به روز می‌کند (ورودی‌ها را در GUI ظاهر می‌کند). این کار با هر دو آدرس IPv4 و IPv6 سازگار است.

شما می‌توانید تمام قابلیت‌های مدیریتی را هم از طریق IPv4 و هم از طریق IPv6 اعمال کنید. برای داشتن ارتباط امن این کار را می‌توان با استفاده از یک کلاینت احراز هویت شده با TSL (گواهی دیجیتال کلاینت می‌تواند از X.509 استفاده کند که بر روی این بسته تولید شده است یا می‌تواند از PKI خارجی استفاده کند) انجام داد. ابزار مدیریتی تحت وب برای ایجاد این برنامه کاربردی وجود دارد که توسط PHP با امنیت بالا ایجاد شده و امنیت آن از ابزارهای مدیریتی که تحت جاوا تولید شده است بیشتر است. اینترفیس ثانویه دیگری ایجاد شده است که به عنوان Snap-in شناخته می‌شود و به طور شگفت انگیزی شبیه ابزارهای مدیریتی است که شامل سرویس‌دهنده DNS مایکروسافت است و مثل آن رفتار می‌کند. عملاً مدیریت BIND با استفاده از سیستم UNIX در IPv6 خیلی سخت است ولی در SolidDNS حتی یک تکنسین مبتدی هم می‌تواند در چندین دقیقه یاد بگیرد که چگونه از آن استفاده کند و ابزارهای مدیریتی ترکیبی بسازد که شامل سایر Snap-in ها در InfoWeapons شود. این ابزار مدیریتی با بهره‌گیری از یک مشتری تصدیق هویت شده بر روی پروتکل TLS کار می‌کند و از نام شبکه و شماره‌گذاری مجدد نیز پشتیبانی می‌کند. تعدادی از کاربران رابط Web/PHP و بعضی دیگر Snap-in را ترجیح می‌دهند.

وقتی حرکت از یک شبکه IPv4 به یک شبکه دوپشته‌ای را شروع می‌کنید به زودی متوجه خواهید شد که بایستی یک سرویس‌دهنده DNS دو پشته‌ای هم داشته باشید و آن را با همه گره‌ها و آدرس‌های آنها مرتبط کنید. تقریبا۳۰٪ تلاش برای مهاجرت به IPv6، شامل این پروسه است. با توجه به این که این قابلیت در داخل ابزارهای SolidDNS آورده شده است این کار می‌تواند تا حد بسیار زیادی در زمان صرفه جویی کند و به شما اطمینان دهد که پیکربندی اعمال شده در هر زمان، خیلی خوب کار خواهد کرد. امروزه بیش از ۷۰٪ سرویس‌دهنده‌های DNS شبکه اینترنت با استفاده پروتکل IPv4، اشتباه پیکربندی شده‌اند. شما فکر می‌کنید چند درصد از DNS های دو پشته‌ای در شبکه‌ای که مستقیماً از BIND استفاده می‌کنند بد پیکریندی شده‌اند؟

برای اطلاعات بیشتر به سایت www.infoweapons.com یا www.infoweapons.net مراجعه کنید. این سایت‌ها هم از طریق IPv4 و هم از طریق IPv6 قابل دسترسی هستند و به شما نشان می‌دهند که با چه آدرس‌هایی وصل شده‌اید. دامنه دومین سایت توسط یک جفت از ابزارهای SolidDNS مدیریت می‌شود. اگر تکمیل چیزی ۱۰ مرحه طول می‌کشد انجام مرحله اول دلیلی برای دسترسی به مرحله دوم است و الی آخر. DNS یکی از مهمترین و اساسی‌ترین مواردی است که واقعاً توسط InfoWeapons چک می‌شود. آیا یک شرکت عملاً IPv6 را پیاده‌سازی کرده است یا این که فقط به این موضوع فکر می‌کند و هیچ فاز عملیاتی انجام نداده است. توصیه می‌شود که تجهیزات سازگار باIPv6 واقعی که بازار را تکان می‌دهند را ببینید. این تجهیزات می‌توانند در سطوح مختلف نسبت به سازمان‌دهی سازگاری با IPv6 کمک کنند و به حرکت واقعی به سمت IPv6 کمک کنند.

ترجمه و تالیف:

بهروز عباس زاده – محبوبه چنگیزی