بسم الله الرحمن الرحیم

عنوان تحقیق

Dynamic Host Configuration Protocol (DHCP)

استاد محترم: جناب آقای مهندس منصوری

نگارنده: یوسف رشیدی

جهت درس: MCSA 2016

مجتمع فنی تهران

هدف کلی تحقیق

DHCP چیست و چطور کار می کند

اهداف جزئی

۱. آشنایی با پروتوکل DHCP

۲. تاریخ معرفی DHCP

۳. آشنایی با مزایای DHCP

۴. آشنایی با روش های تخصیص IP

۵. آشنایی با عملکرد DHCP(DORA)

۶. آشنایی با ساختار پیام‌های DHCP

۷. آشنایی با DHCP Relay Agents

۸.آشنایی با معماری DHCP

۹. چالش های پیش روی پروتکل DHCP

۱۰. DHCP و دیوارهای آتش

هدف کاربردی

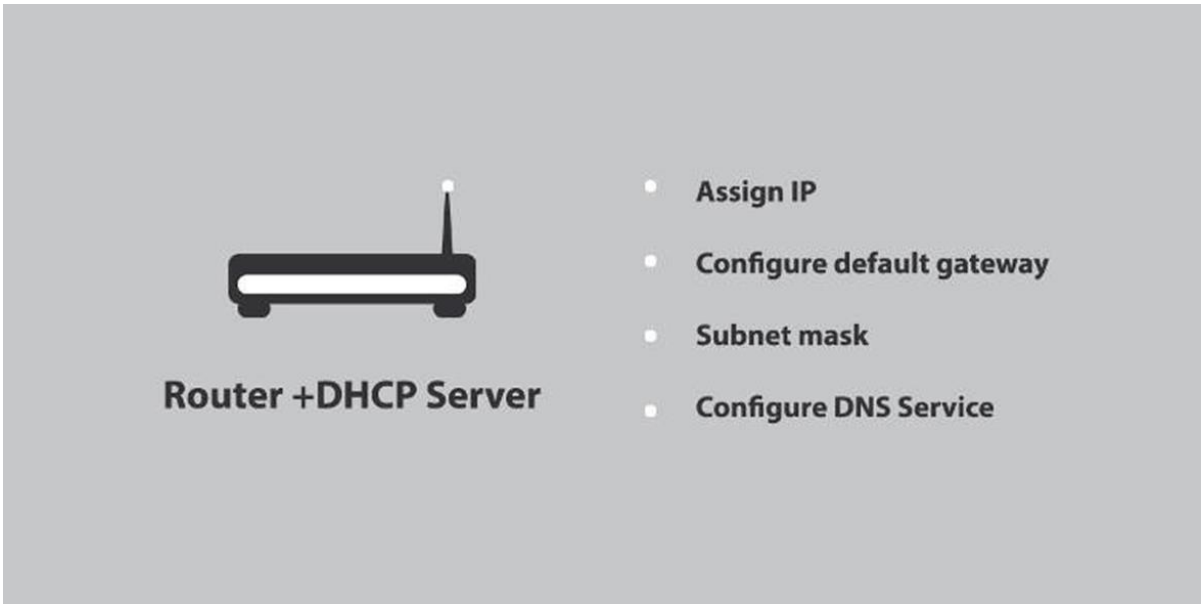
اختصاص اتوماتیک ۱. IP Address ۲. Subnet Mask ۳. Default Gateway ۴. Domain Name System برای کاربران یک شبکه

DHCP چیست و چطور کار می کند

اتصال به شبکه برای هر سیستم درون شبکه، منوط به داشتن یک آدرس IP صحیح است. پروتکل DHCP کار اختصاص IP بصورت خودکار را در یک شبکه انجام می‌دهد.

پروتکل DHCP مخفف Dynamic Host Configuration Protocol ، نوعی از پروتکل برای پیکربندی Host به‌طور پویا است که به هر دستگاه موجود در شبکه، یک آدرس IP اختصاص می‌دهد. هر دستگاه با اتصال به شبکه نیازمند آدرس IP است. این آدرس از طریق یک Router دارای سرویس DHCP اختصاص داده می شود. در شبکه‌های خیلی بزرگ یک Router به‌تنهایی نمی‌تواند تمام دستگاه‌های متصل را مدیریت کند. در این موارد یک Server اختصاصی فقط برای اختصاص آدرس IP به دستگاه‌ها در شبکه قرار می‌گیرد. در این حالت پروتکل DHCP به جای Router ، روی Server اجرا می‌شود.

DHCP نه تنها اختصاص‌دهنده‌ی IP آدرس است، بلکه مدیریت پیکربندی شبکه برای Subnet Mask ، Default Gatewayو سرویس DNS نیز برعهده‌ی این پروتکل است. با بکارگیری این پروتکل، حجم کار مدیریت سیستم به شدت کاهش می‌یابد و دستگاه‌ها می‌توانند با حداقل تنظیمات یا بدون تنظیمات دستی به شبکه افزوده شوند.



DHCP برای اولین بار در اکتبر سال ۱۹۹۳ به عنوان یک پروتکل (در RFC 1531) معرفی شد. در آن زمان DHCP به منزله ی گسترش پروتکل Bootstrap Protocol یا (BOOTP) در نظر گرفته می‌شد. ایده تغییر و گسترش پروتکل BOOTP این بود که این پروتکل نیازمند یک دخالت دستی برای اضافه کردن اطلاعات هر کاربر

بود. همچنین این پروتکل مکانیزمی را برای استفاده دوباره از نشانی‌های IP را که استفاده نمی شوند ارائه نمی‌داد. این به منزله این بود که برای اتصال به اینترنت یک فرایند دستی نیاز بود. پروتکل BOOTP خودش نیز برای اولین بار در RFC951 تعریف گردید و به عنوان جایگزینی برای پروتکل RARP در نظر گفته شد. دلیل عمده جایگزینی BOOTP با RARP این بود که پروتکل RARP در لایه پیوند داده‌ای Data link layer قرار داشت. این امر پیاده‌سازی و اجرا را بر روی پلتفرم‌های سرور مشکل می‌ساخت و نیازمند این بود که آن سرور در هر لایه‌ای از شبکه پاسخگو باشد. BOOTP نوآوری بدیعی را با نام relay agent معرفی کرد. طبق آن ارسال پاکت داده‌ای BOOTP در شبکه با مسیریابی استاندارد IP محیا شده بود و بنابراین سرور BOOTP مرکزی می‌توانست به سرویس گیرنده‌ها (کاربران) با تعداد زیادی IP Subnet سرویس ارائه دهد.

آشنایی با مزایای DHCP

پروتکل DHCP (Dynamic Host Configuration Protocol) روشی برای اداره کردن جایگزینیِ پارامتر شبکه، در یک سرور DHCP مستقل، یا گروهی از چنین سرورهایی است که به شیوه‌ای مقاوم در برابر اشکال چیده می شوند و با DHCP تکمیل شده‌اند؛ حتی در شبکه‌ای با چند ماشین سیستم DHCP مفید می‌باشد، زیرا یک ماشین توسط شبکه‌ای محلی و با کمی تلاش قابل افزودن می‌باشد.

حتی در سرورهایی که نشانی‌ها یشان به ندرت تغییر می‌کند، DHCP برای قرار دادن نشانی‌های آن‌ها توصیه می‌شود بنابراین اگر لازم باشد سرورها دوباره نشانی‌گذاری شوند ، تغییرات باید در کمترین جاهای ممکن صورت گیرند. برای دستگاه‌هایی چون مسیر یاب‌ها و دیوارهای آتش نباید DHCP را بکار بریم، عاقلانه اینست که سرورهای TFTP و SSH را در دستگاهی مشابه که DHCP را اجرا می‌کند قرار دهیم تا مدیریت دوباره متمرکز شود.

این پروتکل برای تخصیص مستقیم نشانی‌ها در سرورها و سیستم‌های رومیزی مفید می‌باشد و نیز بواسطه یک PPP پروکسی برای شماره‌گیری و میزبان‌های پهن باند در صورت درخواست و نیز برای خروجی‌ها (برگردان آدرس شبکه) و مسیریاب‌ها کاربرد دارد. DHCP معمولاً برای زیر ساخت (خدمات بنیادین) مانند مسیریاب‌های غیر حاشیه‌ای و سرورهای DNS مناسب نمی‌باشند.

هدف DHCP پیکره بندی خودکار نشانی IP یک کامپیوتر، بدون مدیر شبکه می‌باشد. IP آدرس‌ها معمولاً از طیف وسیعی از آدرس‌های اختصاص داده شده که در پایگاه داده سرور ذخیره شده‌اند، تشکیل شده‌اند و به کامپیوتری

که درخواست یک IP جدید می‌کند، اختصاص داده می‌شود. یک IP آدرس، برای یک بازه زمانی به یک کامپیوتر اختصاص داده می‌شود، و پس از آن کامپیوتر باید IP آدرس جدیدی را از Server دریافت کند. ممکن است کامپیوتر درخواست تمدید مهلت، یا همان افزایش زمان برای استفاده از IP را به Server بفرستد و Server درخواست افزایش زمان را رد کرده و کامپیوتر را مجبور کند تا IP جدیدی در فاصله‌ای که سپری شده درخواست کند.

DHCP به کامپیوترها (کاربران) اجازه می‌دهد تا تنظیمات را در مدل کاربر – سرور client-server model از سرور دریافت کند. DHCP در شبکه‌های مدرن بسیار رایج است؛ و در شبکه‌های خانگی و شبکه‌های دانشگاهی استفاده می‌شود. در شبکه‌های خانگی، ارائه دهنده خدمات اینترنت ISP ممکن است، یک IP آدرس خارجی منحصربه فردرابه یک مسیر یاب Router یا مودم اختصاص دهد و این IP آدرس برای ارتباطات اینترنتی استفاده شود. همچنین ممکن است روتر خانگی (یا مودم) از DHCP به منظور تأمین یک IP آدرس قابل استفاده برای دستگاه‌های متصل شده به شبکه خانگی استفاده کند تا به این وسایل اجازه ارتباط با اینترنت را بدهد. IP آدرس‌های جهانی منحصر به فردی که توسط ارائه دهنده خدمات اینترنت (ISP) اختصاص داده می شوند با IP آدرس‌هایی که به وسایل جهت اتصال به روتر خانگی داده می‌شود متفاوت‌اند. این مهم به دلیل در نظر گرفتن طرح IPv4 برای حمایت از IPv4 آدرس‌ها است.

روش های تخصیص IP

بسته به نوع تنظیمات، سرور DHCP برای تخصیص IP آدرس ها از یکی از سه روش زیر استفاده می کند:

Dynamic allocation: سرور DHCP به طور پویا (Dynamic) یک IP آدرس را برای مدت زمانی مشخص به دستگاهی که درخواست کننده می باشد، اختصاص می دهد و پس از زمان تعریف شده می تواند مجدد آن IP را برای همان دستگاه تمدید کند.

Automatic allocation: سرور DHCP به طور اتوماتیک یک IP آدرس آزاد را برای مدت زمانی مشخص به دستگاه درخواست کننده اختصاص می دهد. این همانند Dynamic allocation است با این تفاوت که سرور DHCP در حالت Automatic یک جدول از IP های اختصاص داده شده را نگه می دارد، به طوری که می تواند به یک دستگاه IP آدرسی را اختصاص دهد که قبلاً آن را داشته است.

Manual allocation: در این حالت تنها دستگاه هایی که MAC آدرس آنها در جدول سرور DHCP موجود است می توانند از آن سرور درخواست تخصیص IP کنند. این حالت دارای امنیت بیشتری نسب به دو حالت قبلی می باشد.

تخصیص پویا : مدیر شبکه محدوده خاصی از IP آدرس‌ها را به DHCP اختصاص می‌دهد، و هر کامپیوتر کاربر که بر روی شبکه داخلی (LAN) پیکره بندی شده‌است درخواست یک IP آدرس را از DHCP Server در زمان مقدار دهی اولیه ارسال می‌کند. فرایند درخواست و اعطا با استفاده از مفهوم اجاره نامه در یک دوره زمانی خاص قابل کنترل است، که سرور DHCP اجازه تمدید (وپس از آن تخصیص دوباره) IP آدرس‌هایی را که هم‌اکنون تمدید نکرده‌است را می‌دهد.

تخصیص خودکار : سرور DHCP به‌طور دائم یک IP آدرس آزاد که توسط ادمین شبکه تعیین شده‌است را به کاربری که درخوا ست‌کننده می‌با شد، تخ صیص می‌دهد. این همانند تخ صیص پویا ست، اما DHCP Server یک جدول از تخ صیص قبلی IP را نگه می‌دارد به‌طوری‌که می‌تواند به یک کاربر IP آدر سی را اختصاص دهد که قبلاً آن را داشته‌است.

تخصیص ثابت : IP Address DHCP Server هایی مبتنی بر جدول جفت " MAC آدرس / IP آدرس " اختصاص می‌دهد که این تخصیص د ستی ا ست (شاید تو سط مدیر شبکه). فقط به کاربران با MAC آدر سی که در لیست این جدول قرار دارند IP آدرس تخصیص داده خواهد شد. این ویژگی که توسط همه سرورهای DHCP پشتیبانی نمی‌گردد به‌طور وسیعی با نام تخصیص ثابت DHCP خوانده می‌شود.

آشنایی با عملکرد DHCP(DORA)

عملکرد DHCP به چهار قسمت پایه تقسیم می‌گردد

- **DHCP Discovery**
- **DHCP Offer**
- **DHCP Request**
- **DHCP Acknowledgement**

این چهار مرحله به صورت خلا صه با عنوان DORA شناخته می شوند که هر یک از حرف‌ها، سرحرف مراحل بالا می‌باشد.

DHCP Discovery

هر سرویس گیرنده (کاربر) برای شنا سایی سرورهای DHCP موجود اقدام به فر ستادن پیامی در زیر شبکه خود می‌کند. مدیرهای شبکه می‌توانند م سیریاب محلی را به گونه ایی پیکربندی کنند که بتواند بسته داده‌ای DHCP را به یک سرور DHCP دیگر که در زیر شبکه متفاوتی وجود دارد، بفرستد. این مهم باعث ایجاد بسته داده با پروتکل UDP می‌شود که آدرس مقصد ارسالی آن ۲۵۵٫۲۵۵٫۲۵۵٫۲۵۵ یا آدرس مشخص ارسال زیر شبکه می‌باشد. کاربر (سرویس گیرنده) DHCP همچنین می‌تواند آخرین IP آدرس شناخته شده خود را درخواست بدهد. اگر سرویس گیرنده همچنان به شبکه متصل باشد در این صورت IP آدرس معتبر می‌باشد و سرور ممکن است که درخواست را بپذیرد. در غیر اینصورت، این امر بستگی به این دارد که سرور به عنوان یک مرجع معتبر باشد. یک سرور به عنوان یک مرجع معتبر درخواست فوق را نمی‌پذیرد و سرویس گیرنده را مجبور می‌کند تا برای درخواست IP جدید عمل کند. یک سرور به عنوان یک مرجع غیرمعتبر به سادگی درخواست را نمی‌پذیرد و آن را به مثابه یک درخواست پیاده‌سازی از دست رفته تلقی می‌کند؛ و از سرویس گیرنده می‌خواهد درخواست را لغو و یک IP آدرس جدید درخواست کند.

DHCP Offer (پیشنهاد DHCP)

زمانی که یک سرور DHCP یک درخوا ست را از سرویس گیرنده (کاربر) دریافت می‌کند، یک IP آدرس را برای سرویس گیرنده رزرو می‌کند و آن را با نام DHCP Offer برای کاربر می‌فر ستد. این پیام شامل: MAC آدرس (آدرس فیزیکی دستگاه) کاربر؛ IP آدرسی پیشنهادی توسط سرور؛ Subnet Mask ؛ زمان تخصیص IP (lease Duration) و IP آدرس سروری می‌باشد که پیشنهاد را داده‌است.

DHCP Request (درخواست DHCP)

سرویس گیرنده با یک درخوا ست به مرحله پیشین پا سخ می‌گوید. یک کاربر می‌تواند پیشنهادهای‌های مختلفی از سرورهای متفاوت دریافت کند. اما فقط می‌تواند یکی از پیشنهادها را بپذیرد. بر اساس تنظیمات شناسایی سرور در درخواست و فرستادن پیام‌ها (identification option)، سرورها مطلع می‌شوند که پیشنهاد کدام یک پذیرفته

شده‌ا ست. هنگامی که سرورهای DHCP دیگر این پیام را دریافت می‌کنند، آن‌ها پیشنهادهای دیگر را، که ممکن است به کاربر فرستاده باشند، باز پس می‌گیرند و آن‌ها را در مجموعه IP های در دسترس قرار می‌دهند.

DHCP Acknowledgement (تصدیق DHCP)

هنگامی که سرور DHCP، پیام درخواست DHCP را دریافت می‌کند، مراحل پیکربندی به فاز پایانی می‌رسد. مرحله تصدیق شامل فرستادن یک بسته داده‌ای (DHCP Pack) به کاربر می‌باشد. این داده بسته‌ای شامل: زمان تخصیص IP یا هرگونه اطلاعات پیکربندی که ممکن بوده‌است که سرویس گیرنده درخواست کرده باشد، می‌باشد. در این مرحله فرایند پیکربندی IP کامل شده‌است.

ساختار پیام‌های DHCP

پیغام‌های DHCP در دیتا گرام‌های UDP حمل می‌شوند و در سمت سرویس دهنده از شماره پورت ۶۷ و در سمت سرویس گیرنده از پورت ۶۸ استفاده می‌کند. پروتکل‌هایی که در ارتباط با DHCP کار می‌کنند شامل IP, RARP, TCP, UDP , BOOTP می‌باشند. در جدول زیر ساختار پروتکل DHCP را مشاهده می‌نمایید.

OP	HTYPE	HLEN	HOPS
TRANSACTION ID			
SECS		FLAGS	
CIADDR (Client IP address)			
YIADDR (Your IP address)			
SIADDR (Server IP address)			
GIADDR (Gateway IP address)			
CHADDR (Client hardware address (16 OCTETS))			
SERVER HOST NAME (64 OCTETS)			
BOOT FILE NAME (128 OCTETS)			
OPTIONS (VARIABLE)			

۱. **Operation Code : اختصاص یافته به پیام که می‌تواند BOOTREQUEST یا BOOTREPLY باشد به عبارتی دیگر مشخص می‌کند که پیام از سرویس دهنده تولید شده‌است یا سرویس گیرنده و اندازه این پیام همان‌طور که در جدول هم مشاهده می‌شود 8bit که معادل یک بایت است.**

۲. **HTYPE : نوع آدرس سخت‌افزاری موجود در فیلد chaddr را مشخص می‌کند و اندازه آن هم یک بایت است.**

۳. **Hlen : طول آدرس سخت‌افزاری موجود در فیلد Chaddr را بر حسب بایت نشان می‌دهد.**

۴. **Hops : تعداد مسیریابهای موجود بین سرور و سرویس گیرنده را مشخص می‌کند و اندازه آن یک بایت است.**

۵. **Xid یا Transaction ID : حاوی یک شناسه برای نسبت دادن جوابها به درخواستها می‌باشد و به نوعی کد متعلق به فرایند اختصاص یافته بین سرویس دهنده و سرویس گیرنده می‌باشد و چهار بایت است.**

۶. **Secs : مدت گذشته از زمان شروع یک تخصیص آدرس یا فرایند تمدید اجاره را مشخص می‌کند و ۲ بایت حجم آن است.**

۷. **Flags : مشخص می‌کند که سرورهای DHCP و واسط‌های رله‌کننده باید برای ارتباط با یک سرویس گیرنده به جای انتقال تک بخشی از انتقال یا بخش همگانی استفاده کنند یا خیر و ۲ بایت است.**

۸. **CIADDR : آدرس IP سرویس گیرنده به عبارت دیگر آدرس IP کامپیوتر زمانی که در وضعیت باند، تمدید اجاره IP یا ارتباط مجدد می‌باشد را دارا است و اندازه آن چهار بایت است.**

۹. **YIADDR : آدرس IP سرویس گیرنده شما به عبارت دیگر آدرس IP که توسط DHCP به یک کامپیوتر واگزار شده‌است را دربردارد و اندازه آن چهار بایت است.**

۱۰. **SIADDR : آدرس IP سرور بعدی را در یک دنباله Bootstrap مشخص می‌کند از این مقدار فقط زمانی که سرور DHCP یک فایل راه انداز اجرایی به یک سرویس گیرنده بدون دیسک می‌دهد استفاده می‌شود و اندازه آن ۴ بایت است.**

۱۱. **GIADDR : در صورت نیاز، حاوی آدرس IP یک واسط رله‌کننده DHCP مستقر روی شبکه‌ای دیگر می‌باشد و اندازه آن ۴ بایت است.**

۱۲. **CHADDR : آدرس سخت‌افزاری سرویس گیرنده یا به عبارتی دیگر، با استفاده از نوع و اندازه‌ای که در فیلدهای htype و hlen مشخص شده‌است نشان دهنده آدرس سخت‌افزاری سرویس گیرنده می‌باشد؛ و مقدار آن ۱۶ بایت است.**

۱۳. **SERVER HOST NAME** :که یا حاوی نام **DHCP server** اســت یا حاوی داده‌های ســر ریز فیلد **option** می‌باشد؛ و مقدار آن ۶۴ بایت است.

۱۴. **BOOT FILE NAME**: شامل نام فایل **boot**، یک ر شته خاتمه دهنده تهی، نام عمومی یا یک ر شته تهی در **DHCPDISCOVER**، یک **fully qualified directory-path name** در **DHCPOFFER** ا ست و به عبارتی برای **client** های بدون دی سک حاوی نام و آدرس یک فایل راه انداز اجرایی می‌با شد و ۱۲۸ بایت است.

۱۵. **Option**: فیلد پارامتر های اختیاری و به نوعی حاوی مجمو عه‌ای از گزینه های **DHCP** می باشــد که مشخص‌کننده پارامترهای پیکربندی کامپیوتر سرویس گیرنده هستند.

DHCP relaying

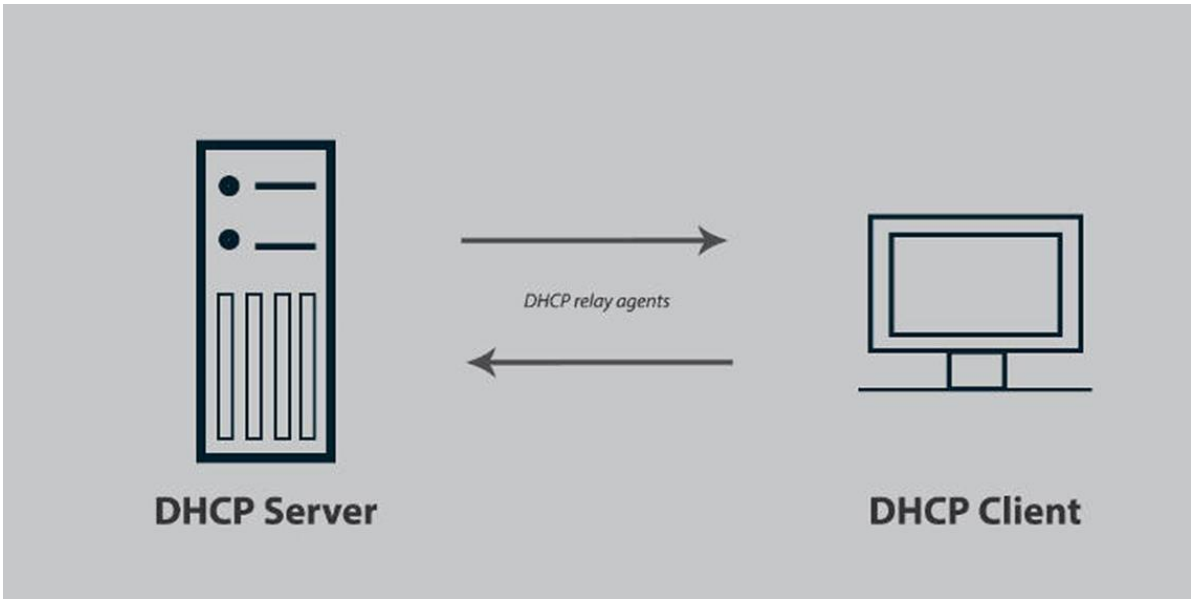
در شـبکه های کوچک معمولا از یک **Subnet** برای تمامی شـبکه اسـتفاده می شـود و یک **DHCP** سـرور به طور مسـتقیم درخواسـت های دسـتگاه های داخل شـبکه را دریافت و آنها را پاسـخ می دهد. اما در شـبکه های بزرگ و گسـترده معمولا از چندین **Subnet** اسـتفاده می شـود که به منظور یکپارچه سـازی و ارتباط بین **Subnet** های مختلف از **Router** ا ستفاده می گردد. در حالت پیش فرض به دلیل **Broadcast** بودن درخوا ست های **DHCP** و عدم وجود **Rout** منا سب، چنین درخوا ست هایی تو سط **Router** عبور داده نمی شود به عبارتی در صورتی که دسـتگاه درخواسـت کننده در یک **Subnet** غیر از **Subnet** سـرور **DHCP** قرار گرفته باشـد، نمی تواند از سرویس **DHCP** آن سرور ا ستفاده کند. برای رفع این مو ضوع از ویژگی **DHCP relaying** ا ستفاده می شود، این ویژگی این امکان را فراهم می سازد تا درخوا ست های **DHCP** به وا سطه **DHCP relay agents** در بین **Subnet** های مختلف عبور کرده و تمامی دستگاه ها موجود در شبکه از سرویس **DHCP** استفاده کنند.

معماری DHCP

در معماری **DHCP** سه بخش حائز اهمیت است: یک مشتری **DHCP**، یک سرور **DHCP** و عامل رله **DHCP**.

مشتری یا کلاینت، هر دستگاهی است که می‌تواند به اینترنت وصل شود و با سرور ارتباط برقرار کند. نه تنها تلفن‌ها و سیستم‌های کامپیوتری مشتری محسوب می شوند، بلکه پرینترها و سرورهای داخل شبکه نیز شامل مشتریان هستند. سرور **DHCP** یک سیستم کامپیوتری است که کار اختصاص **IP** را انجام می‌دهد.

DHCP relay agents یا عوامل رله ارسال سیگنال تقاضا بین کلاینت و سرور را انجام می‌دهند. آنها بخش ضروری یک شبکه نیستند، ولی در شبکه‌های عظیم حضور آنها لازم است.



تداخل IP با DHCP

با اینکه DHCP مسئول اختصاص IP است، گاهی می‌تواند خود عامل تداخل ای پی نیز باشد. وجود خطا در DHCP باعث ایجاد این مشکل می‌شود، اما خود این پروتکل می‌تواند در حین کار مشکل را برطرف کند. اغلب اوقات زمانی‌که خطای تداخل IP را روی سیستم خود می‌بینید، تنها کافیست آن‌را نادیده بگیرید تا مشکل خودبه‌خود برطرف شود. اگر مشکل باقی بماند، باید روتر را ریستارت کنید. باز هم اگر مشکل تداخل برطرف نشود، احتمالا با مساله‌ی بزرگتری در شبکه روبه‌رو هستید که روتر و DHCP با آن دست به‌گریبان هستند.

امنیت

در مورد نحوه کار پروتکل DHCP و مراحل پاسخ دادن به درخواست یک سیستم خاص توضیح داده شد. در این بخش تمرکز این مقاله را بر روی چالش های امنیتی که پیش روی این پروتکل است می گذاریم.

همانطور که گفته شد پیغام DHCP Discovery یک پیغام Broadcast است، از این رو در صورتی که بیش از یک سرور DHCP در شبکه موجود باشند، هرکدام از آن سرورها به صورت مجزا به سیستم درخواست کننده پاسخ می دهند.

در این حالت، سیستمی که پیغام DHCP Discovery را فرستاده است با آن سروری عملیات را ادامه می دهد که پیغام DHCP Offer آن زودتر به دستش رسیده باشد. از این رو در صورتی که یک سرور DHCP تقلبی یا به اصطلاح Rogue DHCP در شبکه وجود داشته باشد درخواست DHCP Discovery به آن می رسد و شروع به ادامه دادن مراحل سرویس DHCP می کند.

در صورتی که DHCP Offer پیشنهاد شده از سمت سرور تقلبی، زودتر از پیغام DHCP Offer پیشنهاد شده از سمت سرور اصلی DHCP برسد، سیستمی که در ابتدا درخواست IP کرده بوده است از یک سرور DHCP مخرب IP را دریافت کرده است.

دریافت IP از سمت سرور تقلبی به خودی خود مشکلی را ایجاد نمی کند، اما حالتی را در نظر بگیریم که حمله کننده تغییراتی را در رنج IP که می خواهد به کاربران پیشنهاد بدهد ایجاد کند. تغییرات می تواند به یکی از حالت های زیر به وجود آید:

۱. پیشنهاد کردن رنج شبکه اشتباه

در این نوع حمله رنج شبکه اشتباهی به کاربر داده می شود. به طور مثال در صورتی که رنج شبکه ما 10.10.10.0/24 است، حمله کننده یک IP از رنج 172.16.31.0/16 به آن می دهد. با به وجود آوردن این تغییر این سیستم خاص امکان برقراری ارتباط با شبکه داخلی خود را ندارد و کار کردن با آن مختل می شود.

۲. تغییر در تنظیمات default gateway

این حمله یکی از انواع حمله های ترکیبی به حساب می آید. نحوه کار شخص حمله کننده در این روش به این گونه است که در IP پیشنهاد شده به کاربر، IP خودش را به عنوان Default Gateway قرار می دهد. در مرحله بعدی حمله کننده با نصب کردن نرم افزارهای جاسوسی شبکه (Wire shark و ...) می تواند تمامی ارتباطات آن سیستم را مانیتور کند و از اطلاعات مورد نظر در راستای اهداف غیر قانونی خود استفاده کند.

۳. تغییر در DNS سرور

این روش حمله کردن را می توان خطرناک ترین نوع حمله در بین این دسته از حملات به شمار آورد. ماهیت حمله به این صورت است که حمله کننده در مرحله اول حمله یک Website تقلبی مالی، اجتماعی، ایمیل و ... همانند وب سایت های دیگر را طراحی کرده است. مرحله بعد راه اندازی یک DNS سرور تقلبی است بدین صورت که به جای

برگرداندن IP واقعی ســایت مورد نظر کاربر(مثل Gmail.com، bank.com و ...) IP وبســایت خود را به کاربر انتقال می دهد. در این صورت تمامی اطلاعات اکانت کاربر به دست حمله کننده می رسد.

۴. روش دیگر مورد استفاده حمله کننده DHCP Flooding است

در روش های حمله ای که در مرحله قبل صحبت شد، فرض بر وجود داشتن همزمان هر دو سرور مخرب و اصلی در شبکه داخلی بود. در این حالت با توجه به زودتر رسیدن یا نرسیدن پیغام DHCP Offer سرور مخرب به کاربران، اطلاعات آن کاربران خاص توسط حمله کننده جاسوسی (Sniff) می-شود.

آیا از دید حمله کننده این روش یک روش بهینه است؟ آیا راه حلی برای sniff تمامی سیستم ها وجود دارد؟ پاسخ این جاست که در صورتی که سرور اصلی DHCP به گونه ای مورد حمله قرار گیرد که قادر به سرویس دهی نباشد، تمامی سیستم های درون شبکه را می توان تحت کنترل خود داشت.

از این رو از روشــی به نام Flooding برای از کار انداختن ســرویس DHCP اســتفاده می شــود. روش کار به این گونه ا ست که حمله کننده با فر ستادن درخوا ست های DHCP Discovery متوالی با MAC Address های تولید شده به صورت تصادفی پایگاه داده IPهای سرور DHCP را خالی می کند. حالا هنگامی که یک کاربر عادی DHCP Discovery را Broadcast می کند، دیگر ســرور DHCP اصــلی به دلیل موجود نداشــتن IP پیغام DHCP Offer را نمی فرستد و تنها جواب از سمت سرویس DHCP راه اندازی شده توسط حمله کننده به دست کاربر می رسد.

DHCP و دیوارهای آتش

دیوارهای آتش معمولاً باید ترافیک DHCP را آشــکارا ممکن ســازند. خصــوصــیات پروتکل ســرور – خدمات گیر DHCP چندین مورد را توضــیح می‌دهد زمانی‌که بســته‌ها باید نشــانی مبدأ ۰۰۰۰۰۰۰۰*۰ یا نشــانی مقصــد FFFFFFFF*۰ را در اختیار داشته باشند. قوانین سیاستی ضد تلاش عمدی و دیوارهای آتش در بر گیرنده و محکم غالباً چنین بسته‌هایی را متوقف می‌سازند.

برای مجاز دانستن DHCP، مدیران شبکه لازم است که چند نوع بسته اطلاعاتی را از طریق دیوار آتش سرور جانبی ممکن سازند.

تمام بسته‌های DHCP به عنوان دیتا گرام‌های UDP منتقل می‌شوند، تمام بسته‌های ارسالی خدمات گیر درگاه منبع ۶۸ و درگاه مقصد ۶۷ دارند، تمام بسته‌های ارسالی خدمات دهنده درگاه منبع ۶۷ و درگاه مقصد ۶۸ دارند.

به عنوان مثال یک دیوار آتش سرور جانبی باید انواع پاکتها که در ذیل آمده را فراهم کند:

- **بسته‌های وارد شده از ۰٫۰٫۰٫۰ یا DHCP-POOL تا DHCP-IP**
- **بسته‌های وارد شده از هر نشانی برای 255.225.255.255**
- **بسته‌های خروجی از DHCP-IP تا DHCP-POOL یا 255.225.255.255**

وقتیکه DHCP-IP هر آدرسی را که روی یک سرور DHCP ترکیب بندی می‌شود را نشان می‌دهد و مجموعه DHCP نشان دهنده مجموعه‌ای است که از آن سرور DHCP نشان‌هایی را به خدمات گیران اختصاص می‌دهد.

نمونه‌ای در دیوار آتش IPFW

برای دادن ایده‌ای از چگونگی ظاهر تولید در پیکر بندی، قوانین زیر برای سرور جانبی دیوار آتش IP امکان تردد DHCP را فراهم می‌آور ند. DHCPd روی میانجی R۱۰ عمل می‌کند و نشانی ها را از 192.168.0.0/24 تخصیص می‌دهد.

باتشکر فراوان از توجه شما استاد عزیز