Dynamic Host Configuration Protocol

DHCP

في الشبكات الحديثة، تُعد إدارة عناوين IP من أهم التحديات التي تواجه مسؤولي الشبكات، خصوصا مع تزايد عدد الأجهزة.

من هنا ظهر بروتوكول **DHCP** كحل أساسي يهدف إلى **أتمتة إعدادات الشبكة** وتقليل الأخطاء البشرية.

تعريف بروتوكول DHCP :

هو بروتوكول شبكي يعمل وفق نموذج Client/Server، يُستخدم لتوزيع:

- IP Address
- Subnet Mask
- Default Gateway
- DNS Server

بشكل تلقائي على أجهزة الشبكة، وذلك باستخدام آلية **Lease Time**، مع إمكانية:

- الحجز(Reservation)
- العمل عبر شبكات مختلفة باستخدامDHCP Relay Agent

لماذا نحتاج إلىDHCP ؟

بدون استخدام DHCP :

- يجب إدخال إعدادات الشبكة يدويا لكل جهاز.
- تزداد احتمالية:
  - تكرار عناوينIP
  - إدخال Subnet Mask أو Default Gateway بشكل خاطئ
- يصعب التحكم في الشبكة كلما زاد عدد الأجهزة.

مع استخدام DHCP :

- يتم تقليل الأخطاء ، توفير الوقت والجهد ، سهولة ادارة الشبكة .

مشكلة إعداد IP يدويا

- إذا تم إدخال عنوان IP مكرر:
  - يحدث **IP Conflict**
- إذا كان:
  - Subnet Mask خاطئ ☜ فشل الاتصال داخل الشبكة
  - Default Gateway خاطئ ☜ عدم الوصول للإنترنت (لخارج الشبكة).

لذلك يُعد DHCP حلًا عملي لتفادي هذه المشاكل

إعدادات الشبكة على جهاز العميل (Client)

على جهاز العميل يوجد خياران لإعداد الشبكة:

1. الإعداد اليدوي(Manual Configuration)

- إدخال:
  - IP Address
  - Subnet Mask
  - Default Gateway
  - DNS
- يتطلب معرفة دقيقة بالإعدادات.

2. الإعداد التلقائي (Automatic Configuration)

- يتم اختيار:
  - Obtain an IP address automatically
  - Obtain DNS server address automatically
- في هذه الحالة:

يحصل الجهاز على جميع الإعدادات من DHCP Server.

آلية عمل DHCP (كيف يحصل الجهاز علىIP)

عندما يتصل جهاز Client بالشبكة ولا يمتلك عنوانIP ، تتم العملية التالية:

1. DHCP Discover

- يرسل الجهاز رسالة **Broadcast** إلى الشبكة.
- الهدف منها:
  - البحث عن أي DHCP Server متوفر.

2. DHCP Offer

- يرد DHCP Server بعرض يحتوي على:
  - IP Address
  - Subnet Mask
  - Default Gateway
  - DNS Server

3. DHCP Request

- يطلب العميل رسميا استخدام الإعدادات المعروضة.

4. DHCP Acknowledgment (ACK)

- يؤكد الخادم الطلب.
- يتم تثبيت الإعدادات على جهاز العميل.

تُعرف هذه العملية اختصارا باسم: **DORA**

- Discover
- Offer

- Request
- Acknowledge

أولًا: مرحلة(D) DHCP Discover

تعريفها

- Discoverهي أول رسالة يرسلها جهاز الـ Client عند اتصاله بالشبكة.
- الهدف منها :البحث عن DHCP Server داخل الشبكة.

خصائص رسالة Discover

- تُرسل باستخدام .**Broadcast**
- السبب:
  - الجهاز لا يمتلك IP بعد.
  - لا يعرف عنوان.DHCP Server
- يتم إرسال الرسالة إلى جميع الأجهزة في الشبكة.

البروتوكول المستخدم

- UDPوليس TCP
- السبب:
  - TCPيحتاج إلى Connection و.Acknowledgment
  - Clientلا يمتلك IP ، فلا يمكن إنشاء اتصالTCP

العناوين فيDiscover

- **Source IP**:
  `0.0.0.0` (لأن الجهاز لا يملك IP)
- **Destination IP**:
  `255.255.255.255` (Broadcast)
- **Source MAC**:
  MAC Address الخاص بالـ Client
- **Destination MAC**:
  `FF:FF:FF:FF:FF:FF` (Broadcast)

المنافذ (Ports) في Discover

- **Source Port**: أي رقم اكبر من 1024
- **Destination Port**: 67 (DHCP Server)

ثانيا: مرحلة DHCP Offer (O)

تعريفها

- هي **رد** DHCP Server على رسالة Discover.
- تحتوي على عرض إعدادات الشبكة.

محتوى رسالة Offer

- IP Address
- Subnet Mask
- Default Gateway
- DNS Server
- Lease Time

طريقة الإرسال

- غالبًا تكون Unicast من:
  - DHCP Server → Client
- أحيانًا تكون Broadcast (حسب الإعدادات) .

البروتوكول المستخدم

?

العناوين في Offer

- **Source IP**: IP الخاص بـ DHCP Server
- **Destination IP**:0.0.0.0
- **Source Port**: 68
- **Destination Port**: الرقم الاكبر من 1024

ثالثًا: مرحلة DHCP Request (R)

تعريفها

- يرسلها Client ليؤكد:

- قبوله للـ IP المعروض.

طريقة الإرسال

- تُرسل غالبا Unicast

العناوين فيRequest

- **Source IP**:
  `0.0.0.0` (أو IP المقترح)
- **Destination IP**:
  `Server's IP`
- **Source Port**: الرقم الاكبر من 1024
- **Destination Port**: 67

رابعًا: مرحلةDHCP Acknowledgment (ACK)

تعريفها

- آخر مرحلة في.DHCP
- يرسل DHCP Server رسالة ACKلتأكيد التخصيص.

ماذا يحدث بعدACK ؟

- Client يقوم بـ:
  - تثبيتIP Address
  - Subnet Mask
  - Gateway
  - DNS
- يصبح الجهاز جاهزا للعمل على الشبكة.

طريقة الإرسال

- **Unicast** من DHCP Server إلى.Client

مدة الايجار Lease Time :

عنوان IP الذي يمنحه DHCP لا يُعطى بشكل دائم ، وانما يُمنح لفترة زمنية محددة تسمى: Lease Time .

- إذا انتهت مدة الـ Lease :
  - يتم سحب الـIP
  - أو تجديده تلقائيا إذا كان الجهاز ما زال متصلا بالشبكة ويحتاجه .

نستخدم Lease Time من اجل :

- تنظيم استخدام عناوينIP
- منع نفاد العناوين
- إعادة استخدام العناوين غير المستخدمة

مدة الـ Lease وعلاقتها بنوع الاتصال : تختلف مدة الايجار حسب نوع الشبكة:

في شبكة DSL : في شبكات **DSL** تكون مدة الـ Lease Time قصيرة نسبيا (قد تصل إلى **30دقيقة**).

- السبب:
  - عدد المستخدمين كبير.
  - عناوين IP محدودة.
  - يتم إعادة توزيع العناوين باستمرار.
- عند انتهاء المدة: إذا لم يُجدد الـ Client العنوان، يعود الـ IP إلى الـ **Pool** ليُمنح لجهاز آخر.

Address Pool: هو مجموعة عناوين IP, يقوم DHCP بتوزيعها ، يتم تحديده داخل **Scope**.

في الشبكات العادية (LAN) : في الشبكات الداخلية LAN تكون مدة الـ Lease أطول (قد تصل إلى أيام). ويكون عدد الاجهزة محدود

- الهدف:
  - تقليل الضغط على DHCP Server
  - استقرار العناوين داخل الشبكة.

تصنيفات عناوين IP في الشبكة

داخل الشبكة يوجد: عناوين مستخدمة + عناوين غير مستخدمة(Free IP)

- DHCP Serverمسؤول عن:
  - تتبع العناوين المستخدمة
  - توزيع العناوين المتاحة فقط
- إذا انقطع:Client
  - يعود الـ IP إلى قائمة العناوين الحرة بعد انتهاء الـLease.

لماذا يُفضل تثبيت خدمة DHCP على الـDomain Controller ؟

في بيئات Active Directory Domain، تخضع خدمة DHCP لآلية أمان خاصة تُسمى **Authorization**.

ما معنى*Authorization*؟

- أي DHCP Server داخل الدومين لا يمكنه توزيع عناوين IP إلا بعد أن يتم **تفويضه (Authorization)**من خلال Active Directory
- هذا التفويض لا يستطيع تنفيذه إلا:
  - Domain Controller
  - أو جهاز لديه صلاحيات Domain Admin

الهدف الأساسي هو: منع وجود DHCP Server غير مصرح به (Rogue DHCP) داخل الشبكة.

- DHCPغير المصرح به قد:
  - يوزع IP خاطئة
  - يسبب تعارض عناوين
  - يوجه الأجهزة إلى Gateway أو DNS غير صحيحة
  - يشكل خطرا أمنيا على الشبكة

لماذا يُفضَّل تثبيت DHCP على Domain Controller؟

1. سهولة الإدارة
2. تقليل التعقيد
3. زيادة الأمان

باختصار : في بيئة Domain ، لا يمكن لأي جهاز أن يعمل كـ DHCP Server إلا بعد الحصول على Authorization من Active Directory ، ولذلك يُفضَّل تثبيت DHCP على Domain Controllerلضمان الأمان، سهولة الإدارة، ومنع أي DHCP غير مصرح به داخل الشبكة.

مكونات نظامDHCP

DHCP Client

- أي جهاز يطلب عنوان IP تلقائيا.
- يبدأ العملية بإرسال رسالة .Discover
- لا يمتلك IP في البداية (0.0.0.0) .

DHCP Server

- مسؤول عن:
  - توزيع.IP Address
  - تحديد.Subnet Mask
  - تحديد.Default Gateway
  - تحديد.DNS Server
- يمكن أن يكون: مستقلا أو جزءا من Domain Controller

القسم العملي :

تثبيت DHCP Server (Windows Server)

1. فتح Server Manager
2. اختيار Add Roles and Features
3. الضغط على Next
4. اختيار DHCP Server
5. الضغط على Install
6. إنهاء التثبيت

إكمال إعداد DHCP بعد التثبيت

- بعد التثبيت:
  - يجب تنفيذ **Complete DHCP Configuration**
- تسجيل الدخول بحساب:
  - Administrator
- الموافقة على:
  - Authorization
  - إنشاء الإعدادات الافتراضية

إنشاء Scope في DHCP

Scope : هو النطاق الذي يتم منه توزيع عناوين IP.

خطوات إنشاء Scope

❖ فتح **DHCP Tools** ← اختيار **IPv4** ← الضغط على **New Scope** ← إدخال: اسم ال scope ووصفه .

❖ تحديد مدى العناوين (IP Range) التي يسمح لـ DHCP بتوزيعها.

- مثال:
  - Start IP: `192.168.1.1`
  - End IP: `192.168.1.254`

❖ **تحديد Subnet Mask**

- مثال:
  - `255.255.255.0`

- هذه القيمة تحدد : حجم الشبكة ، عدد الاجهزة الممكنة

إضافة الاستثناءات(Exclusion)

بعض عناوين IP لا يُسمح لـ DHCP بتوزيعها

- مثل:
  - Gateway
  - Servers , Routers , Printers (اجهزة لها IP ثابت).
- مثال:
  - Exclude:
    - 192.168.1.1 → 192.168.1.10

وبالتالي DHCP serve لن يوزع عناوين للاجهزة من ضمن المجال المستثنى

إعدادات إضافية داخل Scope

- تحديد:
  - Lease Time
  - Default Gateway
  - DNS Server
- هذه الإعدادات تُرسل للـ Client تلقائيا.

اضاءة : wins server تستخدم مع الانظمة القديمة لتحويل NETBIOS NAME الى IP نتجاوزها في اغلب الاحيان بوجود ال DNS .

تفعيل Scope

- بعد الانتهاء من الإعداد:
  - يجب تفعيل ال scope (**Activate Scope**)
- بدون التفعيل: لن يتم توزيع أي IP.

مثال عملي على Scope

- Start IP: 192.168.1.1
- End IP: 192.168.1.254
- Subnet Mask: 255.255.255.0

📌هذا يعني :الشبكة تحتوي على 254 عنوان IP صالح للتوزيع .

DHCP Reservation

حجز IP ثابت لجهاز معين باستخدام MAC Address وبالتالي الجهاز يحصل دائما على نفسIP يتم توزيعه من قبل DHCP Server .

تُستخدم مع:

- Servers
- Printers
- أجهزة مهمة

خلاصة شاملة

- DHCPيمنح IP لفترة محددة.(Lease)
- يتكامل مع DNS وDomain Controller
- يعتمد على Scope لتحديد نطاق العناوين.
- لا يعمل DHCP داخل Domain بدون.Authorization
- يمكن وجود أكثر من Scope
- كل Scope مرتبط بشبكة محددة.
- DHCPيسهل إدارة الشبكات الكبيرة.
- يمكن تعديل الإعدادات في أي وقت.

بعد الإعداد والتفعيل، يبدأ التوزيع تلقائيا ....

ملاحظة : يمكن تثبيت أكثر من Role على نفس السيرفر:

- DHCP Server
- DNS Server
- File Server
- Domain Controller

لكن: في الشبكات الكبيرة يُفضل الفصل بين الأدوار لتحسين الأداء والأمان.

متى يظهر APIPA

- عند فشل Client في الحصول على IP من DHCP

- أسباب الفشل:
  - DHCP Serverمتوقف
  - Scopeغير مفعل
  - كابل الشبكة مفصول

بعض أوامر الفحص(CMD)

عرض الإعدادات: ipconfig
عرض التفاصيل: ipconfig /all
تحرير العنوان: ipconfig /release (يعيد IP إلى 0.0.0.0)
طلب IP جديد: ipconfig /renew

..... انتهت الجلسة مع تمنياتي لكم بالتوفيق والنجاح .....