CloudCommand

Cyber Security

CloudCommand GmbH chr.schumacher@gmx.tm

CloudCommand GmbH chr.schumacher@gmx.tm

AGENDA

01 DHCP

02 DNS

03 Zusammenspiel von DHCP und DNS

01 DHCP

DHCP – Automatische IP-Adressvergabe

DHCP = Dynamic Host Configuration Protocol

DHCP ist ein Protokoll, das dafür sorgt, dass Geräte in einem Netzwerk automatisch eine IP-Adresse und weitere Netzwerkinformationen (wie Subnetzmaske, Standard-Gateway, DNS-Server) zugewiesen bekommen. Dies reduziert den manuellen Aufwand und vermeidet Konflikte durch doppelte IP-Adressen.

Wie funktioniert DHCP?

Der DHCP-Prozess läuft in vier Phasen ab (DORA):

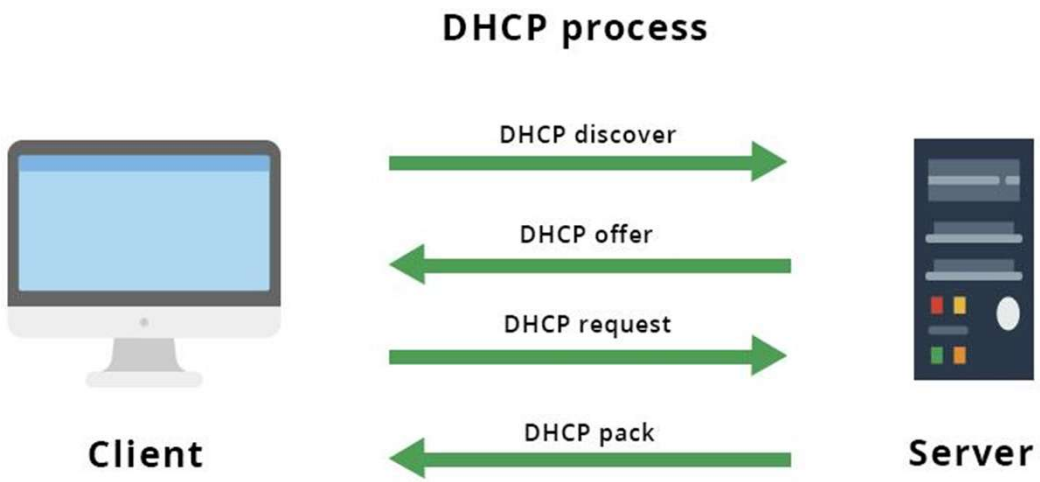
Discover: Ein Gerät (Client) sendet eine Broadcast-Nachricht, um einen DHCP-Server zu finden.

Offer: Der DHCP-Server antwortet mit einem Angebot, das eine verfügbare IP-Adresse und andere Konfigurationsdaten enthält.

Request: Der Client akzeptiert das Angebot und fordert die IP-Adresse vom Server an.

Acknowledge: Der DHCP-Server bestätigt die Zuweisung und der Client verwendet die Adresse.

Wie funktioniert DHCP?



Hauptfunktionen von DHCP:

Automatische IP-Zuweisung:
Geräte erhalten automatisch eine gültige IP-Adresse aus einem definierten Adresspool.

Netzwerkkonfiguration:
Neben der IP-Adresse werden auch andere Einstellungen wie Subnetzmaske, Gateway und DNS-Server verteilt.

Leasing:
Die IP-Adressen werden temporär (oder unbefristet) zugewiesen, sodass Adressen effizient genutzt werden können.

Vorteile von DHCP:

Zentralisierte Verwaltung: Alle IP-Adressen und Netzwerkkonfigurationen werden an einem zentralen Ort verwaltet.

Fehlerreduktion: Minimiert manuelle Konfigurationsfehler.

Flexibilität: Neue Geräte können einfach ins Netzwerk eingebunden werden.

DHCP-Failover:

In unternehmenskritischen Netzwerken wird oft ein zweiter DHCP-Server konfiguriert, um Ausfallzeiten zu vermeiden.

Beide Server können als **aktiv-aktiv** (Load Balancing) oder **aktiv-passiv** (Hot Standby) betrieben werden.

Konfiguration von DHCP (z. B. in deinem Firmennetzwerk):

Scope: Der Adresspool, aus dem IP-Adressen vergeben werden.

- Beispiel: Im VLAN 200 (Personal) liegt der DHCP-Bereich zwischen 192.168.3.33 und 192.168.3.62.

Lease-Time: Gibt an, wie lange eine IP-Adresse an ein Gerät vergeben wird (z. B. 24 Stunden).

Options: DHCP kann zusätzliche Informationen bereitstellen, z. B.:

- Subnetzmaske (255.255.255.224)
- Standard-Gateway (z. B. 192.168.3.33)
- DNS-Server (z. B. 192.168.3.224)

Was kann DHCP alles übertragen?

Grundlegende Netzwerkparameter

Diese Parameter sind für die grundlegende Netzwerkfunktionalität notwendig:

- **IP-Adresse:** Die eindeutige Adresse, die dem Client zugewiesen wird.
- **Subnetzmaske:** Gibt an, welcher Teil der IP-Adresse das Netzwerk und welcher Teil den Host beschreibt.
- **Standard-Gateway:** Die IP-Adresse des Routers, der als Ausgangspunkt für Verbindungen in andere Netzwerke dient.

Was kann DHCP alles übertragen?

DNS-Konfiguration

DHCP kann alle für die Namensauflösung notwendigen Parameter bereitstellen:

- **Primärer DNS-Server:** IP-Adresse des Haupt-DNS-Servers.
- **Sekundärer DNS-Server:** Alternative DNS-Server-IP-Adresse, falls der primäre ausfällt.
- **DNS-Domänenname:** Der Domänenname, in dem sich der Client befindet (z. B. **ccbb.local**).

Was kann DHCP alles übertragen?

Zeit- und Serverinformationen

- **NTP-Server (Network Time Protocol):** Synchronisiert die Uhrzeit des Clients mit einer zentralen Quelle.
- **WINS-Server:** Unterstützt die Namensauflösung in älteren Windows-Netzwerken.
- **Zeitserver:** Alternativer Server für Zeitsynchronisation.

Was kann DHCP alles übertragen?

Netzwerkdienste

- **TFTP-Server:** Ermöglicht das Laden von Bootloadern oder Konfigurationsdateien (häufig für Thin Clients oder IP-Telefone verwendet).
- **PXE-Boot-Server:** Überträgt die Startdatei für netzwerkbasiertes Booten (z. B. für die Installation von Betriebssystemen).
- **Boot-Image:** Verweist auf die Datei, die für das Netzwerkboot verwendet werden soll.

Was kann DHCP alles übertragen?

Sicherheits- und Routing Informationen

- **Router-Optionen:** Zusätzliche Router, die als Alternativen genutzt werden können.
- **Hostnamen:** Ein Name, der dem Client zugewiesen wird.
- **Domain-Name-Suffix:** Der Suffix, der standardmäßig bei DNS-Anfragen angehängt wird.

Was kann DHCP alles übertragen?

QoS und Netzwerkkonfiguration

- **MTU-Größe (Maximum Transmission Unit):** Maximale Paketgröße, die übertragen werden darf.
- **Broadcast-Adresse:** Adresse, an die Broadcast-Pakete gesendet werden.
- **Classless Static Routes:** Ermöglicht die Konfiguration von spezifischen Routen (z. B. für Subnetze oder externe Netzwerke).

02 DNS

DNS – Namensauflösung im Netzwerk

DNS ist ein System, das Domänennamen wie **www.beispiel.de** in IP-Adressen wie **192.0.2.1** übersetzt. Ohne DNS müssten Benutzer IP-Adressen statt leicht merkbarer Namen verwenden..

Hauptfunktionen von DNS:

Namensauflösung:
Übersetzt Domänennamen in IP-Adressen und umgekehrt.

Hierarchische Struktur:
DNS nutzt eine baumartige Struktur mit verschiedenen Domänen (z. B. .com, .de).

Caching:
Häufig abgefragte Namen werden lokal gespeichert, um die Geschwindigkeit zu erhöhen.

DNS-Hierarchie:

Die DNS-Hierarchie besteht aus mehreren Ebenen, die wie ein umgedrehter Baum organisiert sind:

Root-Server (.)

- Die oberste Ebene im DNS-System, oft als "Wurzel" bezeichnet.
- Sie enthält keine Namen wie **.com** oder **.de**, sondern verweist auf die Nameserver der Top-Level-Domains.
- Es gibt weltweit 13 Hauptinstanzen von Root-Servern, die über viele Standorte verteilt sind.
- Beispiel: Eine Anfrage nach **verkauf.ccbb.local** beginnt bei einem Root-Server, der auf **.local** verweist (falls unterstützt).

DNS-Hierarchie:

Top-Level-Domain (TLD)

- Die nächste Ebene unter den Root-Servern.
- Es gibt zwei Hauptarten von TLDs:
  - **Generische TLDs (gTLDs):** z. B. .com, .org, .net.
  - **Länderspezifische TLDs (ccTLDs):** z. B. .de (Deutschland), .fr (Frankreich), .uk (Vereinigtes Königreich).
- Die TLD-Server verweisen auf die Nameserver der Second-Level-Domains.

DNS-Hierarchie:

Second-Level-Domain

- Diese Ebene repräsentiert den spezifischen Namen einer Organisation, eines Unternehmens oder einer Person.
- Beispiel: **ccbb** in **ccbb.de.**
- Der TLD-Server leitet Anfragen für **ccbb.de** an den zuständigen Nameserver weiter.

DNS-Hierarchie:

Subdomain

- Diese Ebene unterteilt eine Domain weiter in logische oder organisatorische Gruppen.
- Beispiel: **verkauf.ccbb.local**:
  - **verkauf** ist eine Subdomain von **ccbb.local**.
  - Subdomains werden oft verwendet, um Abteilungen, Dienste oder Standorte zu repräsentieren (z. B. **mail**, **ftp**, **www**).

Fully Qualified Domain Name (FQDN)

Ist der vollständige Name eines Hosts im Domain Name System (DNS), der eindeutig seine Position innerhalb der hierarchischen Struktur angibt. Ein FQDN enthält alle Teile eines Domain-Namens, beginnend mit dem Hostnamen und endend mit der Top-Level-Domain (TLD).

Aufbau eines FQDN

Ein typischer FQDN hat die folgende Struktur:

[Hostname].[Subdomain].[Domain].[Top-Level-Domain]

Fully Qualified Domain Name (FQDN)

Beispiel

Für den Host **www** innerhalb der Subdomain **example** unter der Domain com lautet der FQDN:

www.example.com

Das abschließende Punktzeichen (nach .**com**.) bezeichnet die Root-Zone des DNS.

Es wird in der Praxis oft weggelassen, ist aber technisch Teil des FQDN.

Fully Qualified Domain Name (FQDN)

Merkmale eines FQDN

Eindeutigkeit: Jeder FQDN ist einzigartig und verweist auf einen spezifischen Host.

Hierarchisch: Die Struktur des FQDN spiegelt die hierarchische Organisation des DNS wider, von spezifisch (Hostname) zu allgemein (Root-Domain).

DNS-Abhängigkeit: Ein FQDN wird verwendet, um IP-Adressen über DNS zuzuordnen.

Fully Qualified Domain Name (FQDN)

Verwendung von FQDNs

- **Zugriff auf Ressourcen:** FQDNs werden genutzt, um Hosts im Netzwerk zu identifizieren, z. B. bei der Konfiguration von E-Mails, Servern oder Netzwerkdiensten.
- **SSL-Zertifikate:** Zertifikate binden sich oft an FQDNs, um sichere Verbindungen zu gewährleisten.
- **Interne Netzwerke:** In Unternehmensnetzwerken werden FQDNs oft für die Organisation von Ressourcen verwendet, z. B. **dc1.company.local**.

Fully Qualified Domain Name (FQDN)

Unterschied zwischen Hostname und FQDN

- Hostname: Der Name eines einzelnen Geräts in einem Netzwerk, z. B. **server1**.
- FQDN: Der vollständige Name inklusive Domain und Subdomain, z. B. **server1.company.com.**

DNS-Abfrageprozess (Name Resolution):

Der Prozess, wie ein Name in eine IP-Adresse aufgelöst wird, erfolgt in mehreren Schritten:

Client-Anfrage:

- Ein Client (z. B. Browser) möchte die IP-Adresse für **verkauf.ccbb.local** wissen.
- Die Anfrage wird an den lokalen DNS-Resolver (oft Teil des Betriebssystems) gesendet.

Root-Server-Abfrage:

- Der Resolver fragt einen Root-Server: "Wo finde ich die Nameserver für **.local?**"
- Der Root-Server verweist auf die zuständigen Nameserver für **.local**.

DNS-Abfrageprozess (Name Resolution):

TLD-Server-Abfrage:

- Der Resolver fragt den TLD-Server für **.local**: "Wo finde ich die Nameserver für **ccbb.local**?"
- Der TLD-Server liefert die Adresse des zuständigen Second-Level-Domain-Servers.

Second-Level-Domain-Abfrage:

- Der Resolver fragt den Second-Level-Domain-Server: "Wo finde ich die IP-Adresse für **verkauf.ccbb.local**?"
- Der Server liefert die gewünschte IP-Adresse zurück (z. B. **192.168.3.100**).

Antwort an den Client:

- Der Resolver speichert die Antwort (Caching) und sendet sie an den Client zurück.

DNS-Caching:

Um die Geschwindigkeit zu erhöhen, speichert der DNS-Resolver bereits abgefragte Namen für eine gewisse Zeit (TTL – Time to Live).

Dadurch muss nicht jede Anfrage erneut den gesamten hierarchischen Prozess durchlaufen.

Arten von DNS-Eintragen:

A (Address Record): Verknüpft einen Namen mit einer IPv4-Adresse.

AAAA (Quad A Record): Verknüpft einen Namen mit einer IPv6-Adresse.

PTR (Pointer Record): Ermöglicht die Rückwärtssuche (IP-Adresse → Name).

MX (Mail Exchange): Gibt den Mailserver einer Domain an.

CNAME (Canonical Name): Alias für einen anderen Namen (z. B. *www* auf *server01*).

SRV (Service Record): Gibt Dienste und Ports an (z. B. für Active Directory).

DNS-Zonen:

Forward-Lookup-Zone: Übersetzt Namen in IP-Adressen.

Reverse-Lookup-Zone: Übersetzt IP-Adressen in Namen.

Primäre Zone: Enthält die Originalkopie der DNS-Datenbank.

Sekundäre Zone: Eine schreibgeschützte Kopie, die für Lastverteilung oder Redundanz verwendet wird.

DNS-Failover und Redundanz:

Sekundäre DNS-Server: Halten Kopien der DNS-Datenbank bereit, falls der primäre Server ausfällt.

Round-Robin-DNS: Verteilt Anfragen auf mehrere Server, um Last zu verteilen.

DNS-Caching: Lokale DNS-Caches reduzieren die Abhängigkeit von externen Servern.

DNS in deinem Netzwerk:

Die Domain Controller (z. B. **DC01** und **DC02**) dienen oft gleichzeitig als DNS-Server.

Lokale Geräte wie Clients und Server verwenden die internen DNS-Server, um interne Namen und IP-Adressen aufzulösen.

Für externe Anfragen wird der DNS-Server des Internet Service Providers genutzt.

03
Zusammenspiel von DHCP und DNS

Zusammenspiel von DHCP und DNS:

In einem gut konfigurierten Netzwerk arbeiten DHCP und DNS Hand in Hand:

Dynamische DNS-Updates: Der DHCP-Server kann bei der Vergabe einer IP-Adresse die Informationen direkt an den DNS-Server übermitteln.
Beispiel: Wenn ein Gerät die IP-Adresse **192.168.3.100** erhält, wird gleichzeitig der Name **client01.verkauf.ccbb.local** im DNS registriert.

Hostnamen-Management: Geräte können über Namen anstatt über IP-Adressen adressiert werden (z. B. **client01** statt **192.168.3.100**).

Unterstützung für Active Directory: In Active-Directory-Netzwerken sind DNS und DHCP essenziell, um die Domänenstruktur, Authentifizierungsdienste und Service-Lokalisierung zu ermöglichen.

Häufig gestellte Fragen

Was ist der Unterschied zwischen DNS und DHCP?

DNS (Domain Name System) ist ein Benennungssystem, das Domänennamen in IP-Adressen übersetzt, während DHCP (Dynamic Host Configuration Protocol) ein Netzwerkverwaltungsprotokoll ist, das den Prozess der Zuweisung von IP-Adressen zu Geräten in einem Netzwerk automatisiert.

Wie arbeiten DNS und DHCP zusammen?

DNS und DHCP arbeiten zusammen, wenn ein Client-Gerät eine IP-Adresse vom DHCP-Server anfordert und der DHCP-Server dem Client-Gerät auch die IP-Adresse des DNS-Servers bereitstellt. Dadurch kann der Client DNS verwenden, um Domänennamen in IP-Adressen aufzulösen.

Welche Rolle spielt DNS in einem Netzwerk?

DNS ist für die Übersetzung von Domänennamen wie www.example.com in IP-Adressen verantwortlich, die von Netzwerkgeräten verstanden werden können, um die entsprechenden Server im Internet zu finden.

Was ist der Zweck von DHCP in einem Netzwerk?

DHCP vereinfacht den Prozess der Netzwerkkonfiguration durch die dynamische Zuweisung von IP-Adressen, Subnetzmasken, Standard-Gateways und anderen Netzwerkkonfigurationsparametern zu Geräten in einem Netzwerk und reduziert so den Verwaltungsaufwand.

Wie funktioniert DNS?

DNS funktioniert, indem es für Menschen lesbare Domänennamen in IP-Adressen übersetzt. Wenn ein Benutzer einen Domänennamen in einen Webbrowser eingibt, ist der DNS-Server dafür verantwortlich, diesen Domänennamen in die entsprechende IP-Adresse aufzulösen.

Wie funktioniert DHCP?

DHCP funktioniert durch die Vermietung von IP-Adressen an Client-Geräte in einem Netzwerk. Wenn ein Gerät dem Internet beitritt, kann es eine IP-Adresse vom DHCP-Server anfordern, der dann dynamisch eine verfügbare IP-Adresse aus einem vordefinierten Bereich zuweist.

Wie konfiguriere ich DHCP in einem Netzwerk?

Um DHCP in einem Netzwerk zu konfigurieren, müssen Sie einen DHCP-Server einrichten und den Bereich von IP-Adressen definieren, die er Client-Geräten zuweisen kann. Sie können auch andere Netzwerkkonfigurationsparameter angeben, z. B. die IP-Adresse des DNS-Servers und das Standard-Gateway.

Was sind die Hauptunterschiede zwischen DNS und DHCP?

Ein wesentlicher Unterschied besteht darin, dass DNS hauptsächlich für die Namensauflösung verwendet wird, während DHCP für die dynamische Zuweisung von IP-Adressen verwendet wird. DNS löst Domänennamen in IP-Adressen auf, während DHCP Geräten IP-Adressen, Subnetzmasken und andere Netzwerkparameter zuweist.

Welche Rolle spielt DNS in einer Active Directory-Domäne?

In einer Active Directory-Domäne ist DNS von entscheidender Bedeutung, da es als Namensauflösungsmechanismus für in die Domäne eingebundene Computer und Dienste dient. DNS wird zum Auffinden von Domänencontrollern, LDAP-Servern und anderen Ressourcen innerhalb der Active Directory-Domäne verwendet.

Welche Beziehung besteht zwischen DHCP- und DNS-Diensten?

Die Beziehung zwischen DHCP- und DNS-Diensten besteht darin, dass DHCP häufig die IP-Adressen von DNS-Servern an Clientgeräte verteilt. Dadurch können die Client-Geräte DNS zur Domänennamenauflösung verwenden und so einen nahtlosen Zugriff auf Ressourcen im Netzwerk gewährleisten.

CloudCommand

CloudCommand GmbH chr.schumacher@gmx.tm