**DHCP (Dynamic Host Configuration Protocol)**

Durch DHCP ist die automatische Einbindung eines Computers in ein bestehendes Netzwerk ohne dessen manuelle Konfiguration möglich. An diesem, dem Client, muss im Normalfall lediglich der automatische Bezug der IP-Adresse eingestellt sein. Beim Start des Rechners am Netz kann er die IP-Adresse, die Netzmaske, das Gateway, DNS-Server und gegebenenfalls WINS-Server von einem DHCP-Server beziehen. Ohne DHCP sind dazu – abhängig vom Netzwerk, an das der Rechner angeschlossen werden soll – einige Einstellungen nötig. DHCP ist eine Erweiterung des Bootstrap Protocol (BOOTP), mit dem sich laufwerklose Workstations realisieren lassen, die sich zunächst eine IP-Adresse vom BOOTP-Server holen. Anschließend laden sie ein startbares Betriebssystem aus dem Netz, mit dem sie dann starten. DHCP ist weitgehend kompatibel zu BOOTP und kann mit BOOTP-Clients und -Servern eingeschränkt zusammenarbeiten.

Der DHCP-Server wird – wie alle Netzwerkdienste – als Hintergrundprozess (Daemon oder Dienst) gestartet und wartet auf UDP-Port 67 auf Client-Anfragen. In seiner Konfigurationsdatei befinden sich Informationen über den zu vergebenden Adresspool sowie zusätzliche Angaben über netzwerkrelevante Parameter wie die Subnetzmaske, die lokale DNS-Domain oder das zu verwendende Gateway

**Manuelle Zuordnung**In diesem Modus (*statisches DHCP*) werden am DHCP-Server die IP-Adressen bestimmten MAC-Adressen fest zugeordnet. Die Adressen werden der MAC-Adresse auf unbestimmte Zeit zugeteilt. Der Nachteil kann darin liegen, dass sich keine zusätzlichen Clients in das Netz einbinden können, da die Adressen fest vergeben sind. Das kann unter Sicherheitsaspekten erwünscht sein.  
Manuelle Zuordnungen werden vor allem dann vorgenommen, wenn der DHCP-Client beispielsweise Server-Dienste zur Verfügung stellt und daher unter einer festen IP-Adresse erreichbar sein soll. Auch Port-Weiterleitungen von einem Router an einen Client benötigen in der Regel eine feste IP-Adresse.

**Automatische Zuordnung**Bei der automatischen Zuordnung wird am DHCP-Server ein Bereich von IP-Adressen definiert. Wenn die Adresse aus diesem Bereich einmal einem DHCP-Client zugeordnet wurde, dann gehört sie diesem auf unbestimmte Zeit, denn auch hier wird die zugewiesene IP-Adresse an die MAC-Adresse gebunden. Ist der Adressbereich komplett vergeben, so können sich keine zusätzlichen Clients in das Netz einbinden. Das geht auch dann nicht, wenn die Rechner gar nicht aktiv sind, denn im Cache des DHCP-Servers wird die IP-Adresse gespeichert. Es hilft dann nur ein Löschen des Caches, um die an nicht aktive Rechner vergebenen Adressen verwenden zu können.

**Dynamische Zuordnung**Dieses Verfahren gleicht der automatischen Zuordnung, allerdings hat der DHCP-Server hier in seiner Konfigurationsdatei eine Angabe, wie lange eine bestimmte IP-Adresse an einen Client „vermietet“ werden darf, bevor der Client sich erneut beim Server melden und eine „Verlängerung“ beantragen muss. Meldet er sich nicht, wird die Adresse frei und kann an einen anderen (oder auch den gleichen) Rechner neu vergeben werden. Diese vom Administrator bestimmte Zeit heißt Lease-Time.  
Manche DHCP-Server vergeben auch von der MAC-Adresse abhängige IP-Adressen, d.h. ein Client bekommt hier selbst nach längerer Netzwerkabstinenz und Ablauf der Lease-Zeit die gleiche IP-Adresse wie zuvor (es sei denn natürlich, diese ist inzwischen schon anderweitig vergeben).

Wenn ein Client erstmals eine IP-Adresse benötigt, schickt er eine *DHCPDISCOVER*-Nachricht (mit seiner MAC-Adresse) als Netzwerk-Broadcast an die verfügbaren DHCP-Server. Dieser Broadcast hat als Absender-IP-Adresse 0.0.0.0 und als Zieladresse 255.255.255.255, da der Absender noch keine IP-Adresse besitzt und seine Anfrage „an alle“ richtet. Dabei ist der UDP-Quellport 68 und der UDP-Zielport 67. Die DHCP-Server antworten mit *DHCPOFFER* und machen Vorschläge für eine IP-Adresse. Das geschieht ebenfalls mit einem Broadcast an die Adresse 255.255.255.255 mit UDP-Quellport 67 und UDP-Zielport 68.  
Der Client darf nun unter den eingetroffenen Angeboten (DHCP-Offers) wählen. Wenn er sich für eines entschieden hat (z. B. wegen längster Lease-Zeit oder wegen Ablehnung eines speziellen, evtl. falsch konfigurierten DHCP-Servers, oder einfach für die erste Antwort), kontaktiert er per Broadcast und einem im Paket enthaltenen Serveridentifier den entsprechenden Server mit der Nachricht *DHCPREQUEST*. Alle eventuellen weiteren DHCP-Server werten das als Absage für ihre Angebote. Der vom Client ausgewählte Server bestätigt in einer *DHCPACK*-Nachricht (DHCP-Acknowledged) die IP-Adresse mit den weiteren relevanten Daten, oder er zieht sein Angebot zurück.  
Bevor der Client sein Netzwerkinterface mit der zugewiesenen Adresse konfiguriert, sollte er noch prüfen, ob nicht versehentlich noch ein anderer Rechner die Adresse verwendet. Das geschieht üblicherweise durch einen ARP-Request mit der soeben zugeteilten IP-Adresse. Antwortet ein anderer Host im Netz auf diesen Request, so wird der Client die vorgeschlagene Adresse mit einer *DHCPDECLINE*-Nachricht zurückweisen.

**DNS (Domain Name System)**

Das Domain Name System (DNS) ist einer der wichtigsten Dienste im IT-Netzwerk. Seine Hauptaufgabe ist die Beantwortung von Anfragen zur Namensauflösung.  
Das DNS ist ein weltweit auf tausenden von Servern verteilter hierarchischer Verzeichnisdienst, der den Namensraum des Internets verwaltet. Dieser Namensraum ist in so genannte Zonen unterteilt, für die jeweils unabhängige Administratoren zuständig sind. Für lokale Anforderungen – etwa innerhalb eines Firmennetzes – ist es auch möglich, ein vom Internet unabhängiges DNS zu betreiben.  
Hauptsächlich wird das DNS zur Umsetzung von Domainnamen in IP-Adressen (*„forward lookup“*) benutzt.

DNS-Anfragen werden normalerweise per UDP Port 53 zum Namensserver gesendet. Der DNS-Standard fordert aber auch die Unterstützung von TCP für Fragen, deren Antwort zu groß für UDP-Übertragung sind. Falls kein Extended DNS verwendet wird (EDNS), beträgt die maximal zulässige Länge des DNS-UDP-Pakets 512 Bytes. Überlange Antworten werden daher abgeschnitten übertragen. Durch Setzen des Truncated-Flags wird der anfragende Client über diesen Sachverhalt informiert. Er muss dann entscheiden, ob ihm die Antwort reicht oder nicht. Gegebenenfalls wird er die Anfrage per TCP Port 53 wiederholen.  
Zonentransfers werden stets über Port 53 TCP durchgeführt. Die Auslösung von Zonentransfers erfolgt aber gewöhnlich per UDP.

**DNSSEC (Domain Name System Security Extension)**Die Domain Name System Security Extensions (DNSSEC) ist eine Menge von Erweiterungen des DNS, die Authentizität und Datenintegrität von DNS-Transaktionen gewährleisten. Ein DNS-Teilnehmer kann damit verifizieren, dass die durch den Server, mit dem er kommuniziert, gelieferten Zonendaten auch tatsächlich identisch mit denen sind, die der für die Zone autorisierte und die Zone signierende Server ausliefert. DNSSEC wurde als Mittel gegen Cache-Poisoning entwickelt, Serverauthentifizierung findet nicht statt.

**Funktionsweise**Informationen werden bei DNS in Resource Records (RR) bereitgestellt. DNSSEC sichert die Authentizität dieser Informationen durch eine digitale Signatur ab. Besitzer einer DNS-Information ist derjenige Master-Server, der für die [Zone](http://de.wikipedia.org/wiki/Zone_%28DNS%29), in der die Information liegt, autoritativ ist. Für jede abzusichernde Zone wird ein eigener *Zonenschlüssel* (engl.: *zone signing key*) (ein Paar, bestehend aus öffentlichem und privatem Schlüssel) generiert. Der öffentliche Teil des Zonenschlüssels wird als DNSKEY Resource Record in die Zonendatei aufgenommen. Mit dem privaten Schlüssel wird jeder einzelne RR dieser Zone digital unterschrieben. Dazu wird ein neuer RR-Typ bereitgestellt, der RRSIG Resource Record, der die Signatur zum zugehörenden DNS-Eintrag enthält. Beispiel eines signierten A-Records:

Bei jeder Transaktion wird neben dem eigentlichen [Resource Record](http://de.wikipedia.org/wiki/Resource_Record) auch der zugehörige RRSIG-RR mitgeliefert. Beim Zonentransfer erhalten ihn die Slaves, bei rekursiver Auflösung wird er im Cache gespeichert. Zu guter Letzt landet er beim anfragenden Resolver. Dieser kann dann anhand des öffentlichen Zonen-Schlüssels die Signatur validieren.

Ein Resource Record (genauer: ein Resource Record Set – also ein Satz von RRs gleichen Typs und Namens) kann auch mehrfach (mit verschiedenen Schlüsseln) unterschrieben werden. Das ist dann sinnvoll, wenn die Gültigkeit eines Schlüssels bald ablaufen wird und man frühzeitig einen Nachfolger publizieren möchte. Die Schlüssel werden durch eine eindeutige Nummer, die Key ID (auch "Key Tag" genannt), unterschieden. Eine digitale Unterschrift enthält in DNSSEC außerdem das Datum, ab dem sie gültig ist sowie ein Enddatum, ab dem sie ihre Gültigkeit verliert. Außerdem wird der verwendete Algorithmus spezifiziert.[[3]](http://de.wikipedia.org/wiki/DNSSEC#cite_note-2)

Um das Keymanagement zu erleichtern, wurde zusätzlich zum Zonenschlüssel ein syntaktisch identischer *Schlüsselunterzeichnungs-Schlüssel* (engl.: *key signing key*) definiert, mit dem ausschließlich Zonenschlüssel unterschrieben werden. Ein derartiger Schlüsselunterzeichnungs-Schlüssel wird für die Bildung von Vertrauens-Ketten (engl.: *chains of trust*) verwendet und zusätzlich in der übergeordneten Zone abgelegt. Im Gegensatz zum häufig erneuerten Zonenschlüssel besitzt er eine lange Lebensdauer.

**Auswertung durch Resolver**Herkömmliche DNS-Resolver (in der DNS-Terminologie *Stubresolver* genannt) sind gewöhnlich nicht in der Lage, digital unterschriebene DNS-Records zu validieren. Nach der zurzeit dominierenden DNS-Philosophie sind Resolver sehr einfach aufgebaute Programme, die mit komplexen DNSSEC-Operationen überfordert wären. Stattdessen werden die DNSSEC-Funktionen in einem zentralen – meist lokalen – rekursiven Nameserver gehalten, der über einen leistungsfähigen Resolver verfügt. Ein Client, der einen Namen auflösen möchte, sendet eine entsprechende Anfrage an diesen zentralen Server. Durch setzen des DO-Bits (*DNSSEC OK*) im DNS-Header teilt er mit, dass authentifiziert werden soll. Bei erfolgreicher Authentifizierung setzt der zentrale Server in der Antwort das AD-Bit (*Authenticated Data*). Das Setzen des DO-Bits ist nur im Rahmen der DNS-Erweiterung [EDNS](http://de.wikipedia.org/wiki/EDNS) möglich, welche folglich von Resolvern und rekursiven Nameservern unterstützt werden muss. Ebenso ist EDNS für die erheblich umfangreicheren Paketgrößen erforderlich, die bei der Übertragung von Schlüsseln und Signaturen notwendig werden.

**RARP (Reverse Address Resolution Protocol)**

RARP wird verwendet, wenn jemandem die IP-Adresse eines Computers nicht bekannt ist.

RARP sendet dazu ein *RARP Request*-Broadcast mit der eigenen MAC-Adresse als Inhalt an die am Netzwerk angeschlossenen Rechner. Ein RARP-Server, welcher alle Zuordnungen IP- zu MAC-Adressen kennt, sendet daraufhin eine Antwort mit der IP-Adresse an die anfragende MAC-Adresse (*RARP-Reply*).

Ausgenutzt wird bei RARP, dass den Herstellern weltweit eindeutige Präfixe für MAC-Adressen vergeben werden. Die Hersteller bemühen sich wiederum, weltweit eindeutige MAC-Adressen zu verteilen. In einem Netz der Schicht 2 dürfen keine zwei Geräte dieselbe MAC-Adresse verwenden. Außerhalb eines Schicht-2-Netzes ist dies zwar nicht wünschenswert, jedoch möglich. Die MAC-Adressen können von Benutzern relativ einfach angepasst werden. Daher ist es nicht garantiert, dass eine MAC-Adresse weltweit eindeutig ist.

Die Zuordnungstabelle auf dem RARP-Server, die zu jeder MAC-Adresse die lokal vergebene IP-Adresse enthält, muss vom Systemverwalter manuell gepflegt werden.

**BOOTP (Bootstrap Protocol)**

Verwendet wird BOOTP zum Beispiel zur Einstellung der Netzwerkadresse von Terminals und festplattenlosen Workstations, die ihr Betriebssystem von einem Bootserver beziehen. Die Übertragung des Betriebsprogramms geschieht dann üblicherweise über TFTP. Daneben können einige Peripheriegeräte wie beispielsweise Netzwerkdrucker BOOTP zur Ermittlung ihrer IP-Adresse und Netzwerkkonfiguration (Subnetz/Gateway) verwenden.

Früher wurde RARP zur Ermittlung der IP-Adresse bei festplattenlosen Geräten verwendet. Im Gegensatz zu RARP, das ausschließlich die IP-Adresse liefert, besitzt BOOTP eine Vielzahl von weiteren Parametern, insbesondere können Subnetzmaske, Gateway sowie Bootserver übermittelt werden. Zur Konfiguration von Workstations und PCs reichen diese jedoch nicht aus, da hier zusätzliche Einstellungen wie Drucker, Zeitserver und andere nötig sind. Das Dynamic Host Configuration Protocol (DHCP) stellt eine Erweiterung von BOOTP dar.

### Die BOOTP-Anforderung Beim Einschalten des Gerätes kennt dieses weder seine eigene IP-Adresse noch die des BOOTP-Servers. Es wird ein *boot request* gesendet. Dies ist ein normales UDP-Paket. Als Absender wird, da bisher nichts anderes bekannt ist, die Adresse 0.0.0.0 eingesetzt. Die Empfängeradresse ist die 255.255.255.255, was als Broadcast im eigenen Netz interpretiert wird, da der BOOTP-Client auch nicht die lokale Adresse des Netzwerkstrangs kennt. Ein *boot request* von einem Client wird immer auf den Zielport 67 (*BOOTP Server*) gesendet. Anschließend lauscht der Client auf dem Port 68 (*BOOTP Client*), auf den die Antwort (*boot reply*) gesendet wird.

### Die BOOTP-Antwort Bekommt der BOOTP-Server eine gültige Anfrage auf dem entsprechenden Port, so betrachtet dieser zunächst die MAC-Adresse. Die MAC-Adresse aus der Anfrage wird mit einer Datenbank verglichen, in der den MAC-Adressen IP-Adressen zugeordnet sind. Wird für die Anfrage ein Eintrag gefunden, sendet der Server eine Antwort (*boot reply*). Meist wird die Antwort auch einfach als Broadcast gesendet, es ist jedoch auch möglich, die ARP-Tabelle des Servers manuell zu bearbeiten.

**NAT (Network Address Translation)**

Network Address Translation (NAT) ist in Rechnernetzen der Sammelbegriff für Verfahren, die automatisiert Adressinformationen in Datenpaketen durch andere ersetzen, um verschiedene Netze zu verbinden. Daher kommen sie typischerweise auf Routern zum Einsatz.  
NAT wird in Source-NAT und Destination-NAT unterteilt. Während beim Source-NAT die Adresse des Computers umgeschrieben wird, der die Verbindung aufbaut, wird beim Destination-NAT die Adresse des angesprochenen Computers verändert.

### Verwendung von Source-NAT Große Verbreitung fand Source-NAT durch die Knappheit öffentlicher IPv4-Adressen und die Tendenz, private Subnetze mit dem Internet zu verbinden. Die einfachste Lösung dieses Problems war oft die durch NAT mögliche Verwendung mehrerer privater IP-Adressen mit nur einer öffentlichen IP-Adresse, wobei die Abbildung auf diese aufgrund der 16 Bit breiten Portnummern auf etwa 65.000 Sitzungen (Port-Address-Translation Einträge) beschränkt bleibt. Gerade in privaten oder möglichst preisgünstig ausgeführten Netzinstallationen wird Source-NAT als eine Art Sicherheitsmerkmal und zur Trennung von internem und externem Netz eingesetzt. Während eine NAT-Installation oberflächlich tatsächlich diese gewünschte Wirkung erzielt, kann sie weder Sicherheitsinfrastruktur noch wirksame Maßnahmen zur Trennung von Netzen ersetzen. So wird die Source-NAT-Funktion eines Routers im professionellen Bereich oft durch ein zusätzlich betriebenes *Application Layer Gateway* (ALG) unterstützt.

### Verwendung von Destination-NAT Destination-NAT wird beispielsweise verwendet, um mehrere, unterschiedliche Serverdienste, die auf verschiedenen Computern betrieben werden, unter einer einzigen IP-Adresse anzubieten. Auch wird es manchmal bei Hot Spots benutzt, um Zugriffe auf Webseiten vor der Anmeldung auf den Rechner umzuleiten, der die Anmeldung anbietet.

OSPF (Open Shortest Path First)

Um die Nachteile von RIP (Routing Information Protocol) auszugleichen, wurde ab 1988 das Open-Shortest-Path-First-Verfahren (OSPF) entwickelt. Die Hauptvorteile von OSPF gegenüber RIP bestehen in der schnelleren Konvergenz und der besseren Skalierbarkeit für größere Netzwerke. Wie der Name andeutet, besitzt OSPF zwei Charakteristika, das der Offenheit im Sinne einer öffentlichen Spezifikation als RFC 2328 und das der Verwendung des SPF-Algorithmus. In UNIX-Systemen ist OSPF als gated-Dämon implementiert. OSPF gehört zur Klasse der Link-State-Routing-Protokolle.  
Der Standard definiert nicht, wie die Kosten zu berechnen sind. Die Grundlage des SPF-Algorithmus bilden nicht wie der Name nahelegt die Anzahl der Hops, sondern die Pfadkosten. Entscheidungskriterium für die Vorteilhaftigkeit eines Weges und damit Metrik wird die nominale Bandbreite.

**Merkmale von OSPF**

### OSPF garantiert ein schleifenfreies Routing im Gegensatz zu RIP

* Es nutzt das Hello-Protokoll für die Überwachung der Nachbarn
* Es unterstützt VLSM sowie CIDR
* OSPF ist für große skalierbare Netze gut geeignet
* Das Area-Konzept vereinfacht die Kommunikation und Wartung

**Arbeitsweise**Kernstück von OSPF ist die Nachbarschafts-Datenbank *(Adjazenz-Datenbank)*/*LSD (Link State Database)*, die eine Liste aller benachbarten Router enthält, zu denen eine bidirektionale Verbindung besteht. Sie spiegelt die Topologie des Netzes wider. Damit diese Datenbank aufgebaut oder bei Topologie-Änderungen aktualisiert wird, ist der Austausch von Routing-Informationen notwendig. Diese werden mittels Flooding übermittelt. Um den Umfang der auszutauschenden Informationen gering zu halten, wählen OSPF-Router einen designierten Router *DR* sowie einen Reserve-Router *BDR (Backup Designated Router)*, die als Schnittstellen für den Austausch dienen. Der OSPF-Router, dessen Multi-Access-Schnittstelle die höchste *Router-Priorität* besitzt, wird *DR*. Haben zwei Router die gleiche Priorität, wird der Router mit der höheren *Router-ID* gewählt. Als Router-ID wird die IP-Adresse eines Loopback-Interfaces oder – je nach Hersteller – des Interfaces mit der numerisch höchsten IP-Adresse/des ersten aktiven Interfaces automatisch gewählt.