Vereinfachung der Administration von IP-Netzwerken mit dynamischer Hostkonfiguration

Dirk Henrici, Patric de Waha

AG Integrierte Kommunikationssysteme
Technische Universität Kaiserlautern
67663 Kaiserslautern
henrici@informatik.uni-kl.de
patric@p-dw.com

Abstract: Mit DHCP (Dynamic Host Configuration Protocol) ist es möglich, Netzwerkgeräten beim Anschluss an das Netzwerk dynamisch eine IP-Adresse zuzuweisen. Aus der Sicht des Netzwerkmanagements ist jedoch eine statische Konfiguration vorzuziehen, weil damit bei Netzmissbrauch leichter auf den Verursacher geschlossen werden kann. In diesem Beitrag wird gezeigt, wie sich die Vorzüge beider Verfahren vereinen lassen. Der DHCP-Dienst wird so beeinflusst, dass IP-Adressen abhängig von dem Ort der physikalischen Anbindung des Nutzers (Port/Netzwerkdose) zugewiesen werden. Dies erhöht die Transparenz für Administratoren, da aus einer IP-Adresse gleich auf die geographische Position des Nutzers geschlossen werden kann.

1 Motivation und Lösungsidee

Ein Teil der Arbeit eines Netzwerkadministrators besteht darin, den Nutzern einen Zugang zum Netzwerk anzubieten. Welche Art des Zugangs die richtige ist, ist situationsabhängig. So mag es erwünscht sein, dass Nutzer sich bei der Anmeldung an das Netzwerk zuerst authentifizieren müssen oder dass das Netzwerk den Nutzern frei zugänglich ist. Aber auch im letztgenannten Fall eines offenen Netzes ist für Administratoren genaue Kenntnis des Netzwerkgeschehens wichtig. Gesucht ist hier eine Form der Netzwerkzugangs, die für den Nutzer transparent abläuft und gleichzeitig dem Administrator die Vorzüge von statisch konfigurierten Endgeräten bietet. Eine solche Lösung ist Thema dieses Beitrags. Bevor die Lösung dargestellt wird, wird im Folgenden ein Überblick über verbreitete Techniken geboten.

Gang und Gäbe ist ein freier Netzwerkzugang, wobei dem Endgerät aber erst dynamisch durch eine Anfrage an einen DHCP-Server die Konfiguration mitgeteilt wird. Erst nachdem die Konfiguration durch einen DHCP-Server übermittelt wurde, ist der Nutzer in der Lage, das Netzwerk zu nutzen. Der Vorteil dieses Vorgehens liegt darin, dass der möglicherweise unerfahrene Nutzer sich einfach physikalisch mit dem Netzwerk verbinden muss und nicht weiter in den Konfigurationsprozess involviert ist. Diese Einfachheit der Konfiguration ist es unter anderem, für die DHCP entwickelt worden ist.

Allerdings gibt es durchaus Fälle, in denen es sinnvoll ist, einem Endgerät eine bestimmte IP-Adresse wiederholt zuzuordnen. Sei es, um das Transfervolumen zu messen oder um Zugang zu Servern zu regeln. Hier bietet sich eine statische Konfiguration von Endgeräten an. Dies muss dann im Regelfall durch Administratoren vorgenommen und verwaltet werden. Zwar können prinzipiell auch Nutzer die Konfiguration nach Maßgabe der Netzwerkabteilung vornehmen, doch kann nicht jedem Nutzer Wissen über IP-Netzwerke unterstellt werden, was sich durch Fehlkonfigurationen und Supportanfragen äußert. Eine mehr automatisierte Konfiguration, bei der Nutzer nicht direkt involviert sind, wäre daher vorzuziehen.

Eine Möglichkeit, die diesem Wunsch Rechnung trägt, ist das Konfigurieren der Endgeräte mittels DHCP unter Berücksichtigung der MAC-Adresse der Endgeräte. Der DHCP-Server ist in der Lage, jedem Endgerät anhand seiner MAC-Adresse eine bestimmte IP-Adresse fest zuzuteilen. Dies setzt jedoch voraus, dass dem DHCP-Server eine Liste der MAC-Adressen erlaubter Endgeräte zur Verfügung gestellt wurde. Da der Aufwand zur Erfassung von MAC-Adressen erheblich ist, stellt auch dies keine optimale Lösung dar. So wäre es notwendig, dass der Netzwerkadministrator die MAC-Adressen von allen Endgeräten der Nutzer registriert und diese in die Konfigurationsdatei des DHCP-Servers einträgt. Nicht registrierte Geräte dürfen nicht zugelassen werden, wenn eine feste Adresszuordnung gewünscht ist, was die Anwendbarkeit einschränkt. Darüber hinaus muss auch für gerade nicht im Netz befindliche Endgeräte eine IP-Adresse reserviert werden, sodass Adressen schnell ein knappes Gut werden können.

Neben der Identifikation des Endgerätes durch dessen MAC-Adresse bleibt noch die Möglichkeit, den Nutzer aktiv in die Anmeldung an das Netzwerk einzubinden. Zwar ist auch dann eine Registrierung notwendig, doch müssen nur noch Nutzer registriert werden und nicht einzelne Endgeräte. Eine Möglichkeit ist, den Nutzer zu einer Anmeldung an einem VPN-Server zu zwingen, bevor der Nutzer über diesen vollen Zugang ins Netzwerk erhält. Technisch gesehen erhält das Endgerät zwar direkt von einem DHCP-Server eine Netzwerkadresse. Diese dient jedoch nur dazu, die Kommunikation mit dem VPN-Server zu ermöglichen. Die weitere Kommunikation läuft dann nach Anmeldung des Nutzers über einen Tunnel zwischen VPN-Client und VPN-Server. Durch den Anmeldezwang ist eine Zuordnung von Aktivitäten zum jeweiligen Nutzer möglich. Nachteilig ist jedoch, dass die eigentliche Kommunikation über den VPN-Server läuft, was die Performanz beeinträchtigt. Darüber hinaus müssen Nutzer registriert werden und diese auf ihren Endgeräten eine VPN-Client-Software installieren.

Eine Anmeldung wie in VPN ist auch unter Nutzung des IEEE-802.1x-Standards [IEEE04] möglich. Ähnlich wie bei VPN muss eine Authentifizierung erfolgen, bevor der Zugang zum Netzwerk in vollem bzw. höheren Umfang freigegeben wird. Die Anmeldedaten können in die weitere Konfiguration des Endgeräts einbezogen werden. Allerdings sind auch hier eine Registrierung von Nutzern (oder alternativ Endgeräten) und eine passende Konfiguration der Endgeräte erforderlich. Es ist aber auch möglich, ohne Anmeldung einen eingeschränkten Zugang zum Netzwerk zu ermöglichen. So könnte die Einschränkung dann z.B. so aussehen, dass ohne Anmeldung nur bestimmte

Dienste im Netzwerk nutzbar sind. Allerdings ist für diese Nutzung dann wieder nur eingeschränkte Kontrollmöglichkeit gegeben.

Neben den beiden entgegengesetzten Ansätzen der völligen Kontrolle des Netzzugangs z.B. mittels IEEE 802.1x oder im Gegensatz dazu des freien Netzwerkzugangs durch DHCP ist oft ein Mittelweg zwischen beiden sinnvoll. In jedem Fall ist es wünschenswert, ein festes Mapping bei der Zuweisung von IP-Adressen zu haben, sodass zum Beispiel gleichen Nutzern oder Endgeräten immer die gleiche Adresse zugeteilt wird. Über IP-Adressen ist nämlich eine sehr einfache Filterung von Datenverkehr oder auch das Messen des Transfervolumens sehr einfach möglich. Die Nutzung des DHCPs ist insofern sinnvoll, da nur auf diesem Wege die Notwendigkeit von Konfigurationsarbeiten am Endgerät vermeidbar ist. Darüber hinaus muss beachtet werden, dass es manchmal erwünscht ist, auch unbekannten Nutzern, z.B. Gästen bei Vorträgen, Zugang zum Netzwerk zu ermöglichen.

Im Folgenden wird eine Lösung dargestellt, die einen freien Zugang zum Netzwerk ermöglicht und dennoch Vorteile statischer Konfiguration bietet. Grundidee ist es, einer Netzwerkdose, z.B. in einem Hörsaal, eine IP-Adresse (mehrere Adressen sind ebenfalls möglich) fest zuzuordnen. Diese Adresse wird über DHCP dem Endgerät zugewiesen, sodass ein Nutzer keine Konfigurationsarbeiten an seinem Endgerät vornehmen muss. Über die zugewiesene IP-Adresse kann auf die Netzwerkdose und damit die geographische Position des Verursachers von Störungen zurückgeschlossen werden.

Zur Realisierung dieser Methode ist folgender Ansatz möglich: Es ist für DHCP eine Option-82 definiert, mit der Netzwerkgeräte Informationen über die Anbindung des jeweiligen Clients in DHCP-Pakete einfügen können. Damit können Edge-Switches eintragen, über welchen Switchport die Anfrage in das lokale Netzwerk eingespeist wurde. Diese Information kann vom DHCP-Server genutzt werden, um seine Adressvergabe unter Berücksichtigung der Herkunft der DHCP-Pakete zu gestalten. Da die Ports der Edge-Switche direkt mit den Netzwerkdosen verbunden sind, ist es so möglich, Endgeräten an der gleichen Dose immer die gleiche IP-Adresse zuzuweisen.

Im folgenden Kapitel werden zum Verständnis des Konzeptes erforderliche Grundlagen erläutert. Dazu wird erst eine kurze Einführung in DHCP und DHCP-Relay-Agents gegeben, bevor dann die Erweiterungsmöglichkeiten über Optionen und insbesondere die Option-82 präsentiert werden. Im Kapitel drei wird dann die Umsetzung des vorgestellten Ansatzes, nämlich der Erstellung eines Mappings zwischen Netzwerkdose und IP-Adresse, angegangen. Nach der Vorstellung der Voraussetzungen wird am Beispiel eines verbreiteten DHCP-Servers erst das Logging der Option-82-Informationen und danach die Adresszuweisung anhand dieser Informationen gezeigt. Im Anschluss werden die Ergebnisse einer Projektarbeit skizziert, mit der das Konzept auch ohne passende Hardware genutzt werden kann. Abschließend werden einige Anwendungsmöglichkeiten des Konzepts an Hochschulen dargestellt.

2 Grundlagen

Im Folgenden werden die Grundlagen für das Verständnis des Konzepts erläutert. Hierfür ist es nötig, das Protokoll DHCP etwas näher zu betrachten. Zuerst wird auf das DHCP-Protokoll im Ganzen, danach auf DHCP-Relay-Agents und schlussendlich auf die DHCP-Option-82 eingegangen.

2.1 DHCP

Die Abkürzung DHCP steht für "Dynamic Host Configuration Protocol" [RFC1]. Wie bereits im Namen ersichtlich, handelt es sich hierbei um ein Protokoll, das das Konfigurieren von Endgeräten dynamisch vornimmt. Das Konzept von DHCP besteht darin, dass man Endgeräte in ein bestehendes Netzwerk einfügen kann, ohne am Endgerät selbst eine Konfiguration vornehmen zu müssen, vorausgesetzt das Endgerät unterstützt das DHCP. Über das DHCP gelangt das Endgerät unter anderem an wichtige Netzwerkdaten wie z.B. IP-Adresse, Netzmaske, DNS-Server und Default-Gateway.

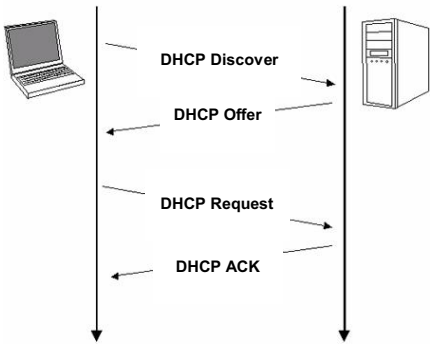

Abbildung 1: DHCP-Konfigurationsprozess

In Abbildung 1 ist ein solcher DHCP-Konfigurationsprozess illustriert. Das unkonfigurierte Endgerät des Nutzers versucht durch das Senden eines DHCP-Discover-Broadcasts einen verantwortlichen DHCP-Server zu erreichen. Der DHCP-Server bietet dem Endgerät in einem Offer-Paket eine Konfiguration an. Ist dem Endgerät des Nutzers diese Konfiguration recht, muss dieser die Konfiguration explizit beim DHCP-Server beantragen. Dieser wird die Anfrage dann mit einem DHCP-Ack bestätigen oder mit einem DHCP-Nak verweigern. Dieser Prozess kann so oft wiederholt werden, bis das Endgerät eine passende Konfiguration erhalten hat.

Ein wichtiges Einsatzszenario für DHCP sind Netzwerke, deren Topologie oft zu Änderungen neigt. Ohne die Vorteile des DHCP müssten die Netzwerkadministratoren dann Änderungen vor Ort an jedem Endgerät durchführen, was einen hohen Aufwand bedeutet. Dieser Aufwand ist mit DHCP vermeidbar. Die Konfiguration wird in einer zentralen Datei auf dem DHCP-Server zusammengefasst und wird von dort aus für die Adressvergabe innerhalb des Netzwerks genutzt.

2.2 DHCP Relay Agents

Ein Endgerät, das noch keine Konfigurationsinformation besitzt, verfügt über keinerlei Informationen bezüglich seines verantwortlichen DHCP-Servers. Um dennoch den DHCP-Server kontaktieren zu können, wird die DHCP-Anfrage vom Endgerät in Form eines Broadcasts auf das Netzwerk gegeben. Ein DHCP-Server, der diesen Broadcast empfängt, kann dem Endgerät nun antworten.

In gerouteten Netzen kann es vorkommen, dass der DHCP-Server außerhalb der Broadcast-Domain platziert ist. In diesem Fall würde der DHCP-Server keine Broadcast-Nachrichten vom Endgerät empfangen. Um dieses Problem zu lösen, wurden DHCP-Relay-Agents (oft auch DHCP-Relays genannt) eingeführt [RFC1].

Ein Router, der DHCP-Relaying unterstützt und aktiviert hat, fängt DHCP-Broadcasts auf und leitet sie als Unicast an den DHCP-Server weiter. Entsprechend werden die Antworten des DHCP-Servers an den Relay-Agent übermittelt, der diese dann in das Subnetz des Clients weitergibt. Somit sind die Grenzen einer Broadcast-Domain überwunden.

2.3 DHCP-Optionen

Das Optionsfeld ist ein wesentliches Kennzeichen von DHCP und seiner Flexibilität. Es befindet sich am Ende eines DHCP-Pakets und enthält eine variable Anzahl an Optionen. Es dient dem DHCP-Server oder DHCP-Client dazu, dem Kommunikationspartner zusätzliche Daten mitzuteilen. So kann z.B. der DHCP-Server in dieses Feld Daten wie Broadcast-Adresse, NIS-Adresse, DNS-Server, Gateway-Adresse und einige andere einkodieren. Die meisten Optionen sind im DHCP-Optionen-RFC [RFC2] spezifiziert. Einige Optionen sind komplizierter oder nachträglich hinzugefügt worden und befinden sich deshalb in einem eigenen RFC wie z.B. die "Relay Agent Information Option" oder die "Rapid Commit Option".

2.4 Vorstellung der DHCP-Option-82

Die nachträglich definierte Option-82 [RFC3] wird auch „Relay Agent Information“ genannt. Diese Option enthält Informationen über die Herkunft einer DHCP-Anfrage und gibt somit dem DHCP-Server mehr Möglichkeiten, um eine Entscheidung über die IP-Vergabe zu treffen.

Ursprünglich war die Option-82 dazu gedacht, Relay-Agents die Möglichkeit zu bieten, Informationen über die Herkunft einer DHCP-Anfrage in die DHCP-Anfrage selbst einzucodieren. Die DHCP-Anfragen werden dabei vom Relay-Agent empfangen und anschließend mit der Option-82 versehen, bevor die Anfrage zum DHCP-Server weitergeleitet wird. Der DHCP-Server hat somit Informationen über die Herkunft der DHCP-Anfrage und kann seine IP-Adressvergabe dementsprechend gestalten. So kann der DHCP-Server z.B. für eine bestimmte Herkunft der DHCP-Anfrage gesonderte IP-Adressen mit kleineren Lease-Zeiten vergeben.

Inzwischen kann die Option-82 auch von Netzwerkgeräten eingefügt werden, die nicht als Relay-Agent arbeiten. Dies ist zwar vom Standard nicht so gedacht, macht aber insofern Sinn, als dass die Option-82 an allen Edge-Switches eingefügt werden kann, an denen sich Nutzer in ein Netzwerk einklinken können, auch wenn diese Switches keine Relay-Agent-Funktion wahrnehmen.

Die Option-82 kann eine variable Zahl von Unteroptionen enthalten, die jeweils eine variable Länge haben können. Ursprünglich waren nur zwei Unteroptionen definiert, inzwischen gibt es aber auch noch weitere Unteroptionen wie die „Subscriber-ID“ [RFC4].

Die erste definierte Unteroption wird Agent-Circuit-ID genannt. Diese Unteroption enthält Informationen über den Anschluss, über den ein Endgerät mit dem Netzwerkgerät, das die Option-82 einfügt, verbunden ist. Die zweite Unteroption wird Agent-Remote-ID genannt. Diese Unteroption ist dazu gedacht, dass das Netzwerkgerät eine eindeutige Kennung des angeschlossenen Endgeräts bzw. Nutzers einkodiert. Zur Verdeutlichung ein Beispiel: Im Falle eines DialUp-Servers könnte die Agent-Remote-ID die Telefonnummer des Anrufers enthalten und die Agent-Circuit-ID könnte die Information enthalten, an welchem Dial-Up-Port der Anruf einging.

In der Definition zur Option-82 wurde allerdings nur die Bedeutung der jeweiligen Unteroption spezifiziert, nicht jedoch der genaue Inhalt der jeweiligen Unteroption und die Kodierung des Inhalts. Dies hat dazu geführt, dass die Unteroptionen uneinheitlich genutzt werden. Nichtsdestotrotz hat sich für Switches inzwischen soweit die Vlan-mod-port-Kodierung etabliert. Im Folgenden soll kurz auf diese Kodierung eingegangen werden, da diese etwas von der ursprünglichen Spezifikation der Option-82 abweicht.

Die Agent-Circuit-ID besteht aus sechs Byte und enthält Informationen über die Herkunft des DHCP-Pakets relativ zum Gerät, das die Option-82 einfügt. Die Aufteilung dieser 6 Byte sind wie folgt: Byte 1 und 2 enthalten eine Längenangabe der folgenden Daten und sind somit konstant 0 bzw. 4. Byte 3 und 4 enthalten die VLAN-ID des VLANs, in das die DHCP-Anfrage gehört. Byte 5 gibt das Modul an, das den Port enthält, über den das Paket gelesen wurde. Byte 6 enthält den Port, über den das Paket gelesen wurde, innerhalb des Moduls.

Die Agent-Remote-ID besitzt eine Länge von acht Byte, wobei die ersten zwei Byte wieder eine Längenangabe sind und die hinteren sechs Byte die MAC-Adresse des Switches enthalten, der die Option-82 eingefügt hat. Dies ist besonders bemerkenswert, da dieses Vorgehen von der Spezifikation abweicht, denn ursprünglich sollte in der Agent-Remote-ID eine eindeutige Kennung des Nutzers einkodiert werden und nicht die Kennung des Netzwerkgeräts selbst.

2.5 ISC DHCP

ISC DHCP ist eine freie Referenzimplementierung des DHCP-Protokolls vom "Internet Systems Consortium" [ISC07]. Das ISC DHCP-Paket enthält sowohl einen DHCP-Server als auch einen DHCP-Client und einen DHCP-Relay-Daemon.

Durch die weite Verbreitung des ISC DHCP und der hohen Funktionalität bietet der ISC DHCP die nötigen Vorrausetzungen, um eine Vergabe von IP-Adressen anhand der Option-82 zu erfüllen. Besonders nützlich im Kontext der hier behandelten Lösung sind die Klassen- und Pool-Funktionen, die der ISC DHCP anbietet.

Für weitere Informationen bezüglich des ISC DHCP sei hier auf die Internetseite [ISC07] des "Internet Systems Consortium" verwiesen.

3 Praktische Umsetzung

In diesem Kapitel wird auf die Umsetzung des Konzeptes mit den vorgestellten Standards und Werkzeugen eingegangen. Die Option-82 wird dazu verwendet, dem DHCP-Server mitzuteilen, an welchem Netzwerkgerät das Paket eingespeist wurde. Mit entsprechender Konfiguration kann man den DHCP-Server soweit beeinflussen, dass dieser die zu vergebende IP-Adresse in Abhängigkeit der Option-82 wählt.

3.1 Voraussetzungen für Option-82

Die Option-82 enthält Daten, die Rückschlüsse auf die Herkunft des DHCP-Pakets erlauben. Diese Option wird nicht vom Endgerät des Nutzers im Paket platziert, sondern von dem Edge-Gerät, das das Paket vom Client entgegennimmt. In Ethernet-Netzwerken wird dies ein Edge-Switch sein, im RFC [RFC3] ist allgemein von „Circuit Access Units“ die Rede. Der Switch empfängt ein DHCP-Paket eines angeschlossenen Nutzers und fügt das Option-82-Feld ein. Dieses Feld enthält die Identifikation des Switches und einen Wert, der Rückschlüsse auf den verwendeten Port erlaubt. Vorgänge, die DHCP-Pakete manipulieren, fallen unter den Begriff des "DHCP-Snooping".

Allerdings verfügt nicht jeder Switch über eine solche Funktionalität. Die direkte Nutzung der Option-82 setzt jedoch voraus, dass in Bereichen, bei denen die Adressvergabe abhängig von den Ports erfolgen soll, ausschließlich Option-82-fähige Geräte zum Einsatz kommen. Es gilt weiterhin, die herstellerspezifische Konfiguration des Switches zu beachten. So kann es sein, dass DHCP-Snooping womöglich nicht aktiviert ist, siehe z.B. [CS07], [AT06]. Das Aktivieren dieses DHCP-Snooping-Features soll in diesem Rahmen jedoch nicht behandelt werden, und es sei an dieser Stelle auf die Dokumentation der jeweiligen Switches verwiesen.

3.2 Logging der Option-82

Der ISC DHCP-Server verfügt über die Möglichkeit, auf Daten aus Optionsfeldern zuzugreifen. Somit können beispielsweise Daten aus dem Option-82-Feld in Log-Kommandos benutzt werden [Al07]. Ein solcher Eintrag ist in Abbildung 2 angegeben. Dieser führt zu einer Ausgabe wie in Abbildung 3 gezeigt.

Die in Abbildung 2 angegebene Konfiguration dient dazu, Informationen über DHCP-Anfragen zu loggen. In der Log-Ausgabe, Abbildung 3, sind Informationen bezüglich

der Herkunft der DHCP-Anfrage enthalten. Wie aus dieser Abbildung ersichtlich, sind die beiden Felder der Option-82 unter den Strings "agent.circuit-id" und " agent.remote-id" verfügbar.

```
log ( info,
      concat(
            "Lease für ", binary-to-ascii (10, 8, ".", leased-address),
            ": verbunden über ", binary-to-ascii(10, 8, "/", suffix( option agent.circuit-id, 2)),
            ", VLAN ", binary-to-ascii (10, 16, "", substring( option agent.circuit-id, 2, 2)),
            " über Relay ", binary-to-ascii(10, 8, ".", packet(24, 4)),
            "(", binary-to-ascii (16, 8, ":", substring( option agent.remote-id, 2, 6)), ")"
      )
);
log ( info,
      concat(
            "Lease für ", binary-to-ascii (10, 8, ".", leased-address),
            ": raw option-82 CID ", binary-to-ascii (10, 8, ".", option agent.circuit-id),
            "; raw option-82 RID ", binary-to-ascii (16, 8, ".", option agent.remote-id)
      )
);
```

Abbildung 2: Konfigurationsblock zum Loggen von Option-82-Informationen

```
Mai 20 11:01:43 dhcpd: Lease für 192.168.1.2: verbunden über 0/16, VLAN 82 über Relay 192.168.1.254
(0a:1b:2c:3d:4e:5f)
Mai 20 11:01:43 dhcpd: Lease für 192.168.1.2: raw option-82 CID 0.4.0.82.0.16; raw option-82 RID
0.6.0a.1b.2c.3d.4e.5f
```

Abbildung 3: Log-Ausgabe des DHCP-Servers

Diese Felder sind jedoch nur dann definiert, wenn das einkommende DHCP-Paket diese Option auch enthält. Deshalb ist es zweckmäßig, die Konfiguration in einen Bedingungsblock wie folgt einzuschließen:

```
if exists agent.circuit-id
{
      # Konfiguration für Logging
}
```

Abbildung 4: Konfiguration mit Bedingungsblock

3.3 Zuweisung von IP-Adressen anhand der Option-82

Im vorherigen Abschnitt wurde gezeigt, wie man für eingehende DHCP-Anfragen auf das Option-82-Feld zugreifen kann, um die enthaltenen Daten in Log-Nachrichten zu verwenden. In diesem Abschnitt wird nun gezeigt, wie man den DHCP-Server so konfigurieren kann, dass dieser bestimmten Option-82-Werten eine bestimmte IP-Adresse zuordnet. Leider wird die Relation zwischen IP-Adressen und Option-82-Werten nicht direkt unterstützt. Mit einem kleinen Konfigurationstrick kann das gewünschte Verhalten jedoch erreicht werden.

```
# ISC DHCPd Konfigurationsdatei

subnet 192.168.0.0 netmask 255.255.255.0 {
      pool {
            range 192.168.0.1-192.168.0.10
            allow members of "Nutzergruppe1";
      }
}
```

Abbildung 5: Beispielkonfiguration für den DHCP-Server mit einem speziellen Pool

Der ISC DHCP-Server kann unterschiedliche Pools von IP-Adressen verwalten [DL02]. Dies dient dazu, spezielle IP-Adressen an spezielle Nutzer zu vergeben. Spezielle Nutzer können anhand eines Kriteriums in Nutzergruppen aufgeteilt werden. Es ist dann möglich, Pools von IP-Adressen an derartige Nutzergruppen zu binden.

Bei der Konfiguration aus Abbildung 5 werden die IP-Adressen 192.168.0.1 bis 192.168.0.10 an Nutzer vergeben, die in der „Nutzergruppe1“ sind. Was in diesem Beispiel nun noch fehlt, ist die Definition der „Nutzergruppe1“. So ist es beispielsweise möglich, alle Nutzer, die ein Windows-Betriebssystem besitzen, zu gruppieren, siehe Abbildung 6.

```
class "Nutzergruppe1"   {
      match if substring(dhcp-client-identifier, 0, 7)="windows";
}
```

Abbildung 6: Nutzergruppe zur Identifizierung von Windows-Clients

Man ist also mit dem ISC DHCP-Server in der Lage, bestimmten Gruppen von Nutzern, bestimmte IP-Adressen zuzuweisen. Wie wir im Kapitel für Logging mit Hilfe der Option-82 gesehen haben, kann man in der Konfiguration auf Option-82-Felder zugreifen. Man ist also in der Lage, eine Nutzergruppe zu definieren, die nur Nutzer enthält, die über einen bestimmten Switch und über einen bestimmten Port angeschlossen sind. Ein Beispiel hierzu ist in Abbildung 7 angegeben.

```
# ISC DHCPd Konfigurationsdatei
# Zuordnung einer IP-Adresse an einen Switchport

subnet 192.168.0.0 netmask 255.255.255.0 {
      class "SWITCH-0A0B0C0D0E0F-PORT2"{
            match if (
            binary-to-ascii(16, 8,"", substring(option agent.remote-id, 2,6)="0A0B0C0D0E0F"
            and
            binary-to-ascii (10, 8, "/", suffix(option agent.circuit-id, 2)) = "0/2"
            and
            binary-to-ascii (10, 16, "", substring( option agent.circuit-id, 2, 2)) = "1"
            );
      }
      pool {
            range 192.168.0.1
            allow members of "SWITCH-0A0B0C0D0E0F-PORT2";
      }
}
```

Abbildung 7: Konfiguration basierend auf Vlan-mod-port-Kodierung

Die Konfiguration in Abbildung 7, die die Vlan-mod-port-Kodierung auswertet, würde jeder DHCP-Anfrage, die vom Switch mit der MAC-Adresse "0A0B0C0D0E0F" und dessen Port "3" aus Modul "0" kommt und VLAN "1" nutzt, die IP-Adresse "192.168.0.1" zuweisen. Angenommen, dieser Switch verfüge über acht Ports, von denen DHCP-Anfragen zu erwarten wären, so müsste für jeden dieser acht Ports eine entsprechende Nutzergruppe definiert werden. Weiterhin muss für jede dieser definierten Nutzergruppen eine Pool-Deklaration existieren, die dieser eine IP-Adresse bzw. einen Adresspool zuordnet. Zweckmäßigerweise generiert man diesen Teil der DHCP-Konfiguration mit einem Skript, das aus tabellarischen Daten die Konfiguration in der passenden Syntax erzeugt.

Fungiert der Edge-Switch auch als Relay-Agent, so fügt er gemäß DHCP-Spezifikation [RFC1] seine IP-Adresse in ein dafür vorgesehenes Feld in die DHCP-Pakete ein. In

diesem Fall kann man statt der MAC-Adresse auch die Relay-Agent-IP-Adresse auswerten. Dies ist die standardkonforme Vorgehensweise und vermeidet auch, dass bei einem Austausch des Switches die DHCP-Konfiguration angepasst werden muss. Das Vorgehen ist in Abbildung 8 dargestellt.

```
# ISC DHCPd Konfigurationsdatei
# Zuordnung einer IP-Adresse an einen Switchport

subnet 192.168.0.0 netmask 255.255.255.0 {
      class "SWITCH-0A0B0C0D0E0F-PORT2"{
            match if (
            binary-to-ascii (10, 8, ".", packet(24, 4)) = "192.168.1.254"
            and
            binary-to-ascii (10, 8, "/", suffix(option agent.circuit-id, 2)) = "0/2"
            and
            binary-to-ascii (10, 16, "", substring( option agent.circuit-id, 2, 2)) = "1"
            );
      }
      pool {
            range 192.168.0.1
            allow members of "SWITCH-0A0B0C0D0E0F-PORT2";
      }
}
```

Abbildung 8: Konfiguration basierend auf Vlan-mod-port-Kodierung und Relay-Agent-IP

Im dargestellten Konfigurationsabschnitt wird direkt auf die IP-Adresse des Relay-Agents im Paket zurückgegriffen, um so den Edge-Switch zu identifizieren. Operiert der Switch nicht im Relay-Agent-Modus, so ist diese Vorgehensweise nicht sinnvoll, da die Adresse dann „0.0.0.0“ ist. Dann muss, wie in Abbildung 7 gezeigt, die MAC-Adressinformation aus der Option-82 dazu genutzt werden, um den Edge-Switch zu identifizieren.

3.4 Unterstützung von nicht Option-82-fähiger Hardware

Nicht jeder Switch ist in der Lage, die Option-82-Informationen einzufügen. Somit ist die in den vorangegangenen Abschnitten gezeigte Vorgehensweise in der Praxis nicht überall gangbar.

Wie in einer Projektarbeit [Wa06] an der TU Kaiserslautern gezeigt wurde, ist es dennoch möglich, die Vorzüge, die das Vorhandensein von Option-82-Informationen mit sich bringt, auch beim Fehlen passender Hardware zu nutzen. Die Grundidee ist, die nötigen Daten für die Option-82 mittels SNMP zu ermitteln, um dann, wie in den vorangegangenen Abschnitten gezeigt, vorgehen zu können.

In der Projektarbeit wurde ein DHCP-Relay-Programm namens „DHCP-Snooper“ entwickelt, das unter [Sf06] heruntergeladen werden kann. Dieses Programm nimmt DHCP-Pakete entgegen. Sind keine Option-82-Informationen in den Paketen enthalten, so werden die benötigten Informationen vom Programm über rekursive SNMP-Anfragen ermittelt. Vorraussetzung dafür sind managebare Switches, die SNMP mit der Bridge- und IF-MIB anbieten. Das Programm fügt dann ein Option-82-Feld ein, das die gleichen Informationen enthält, wie in der Vlan-mod-port-Kodierung vorgesehen. Somit ist es für den DHCP-Server gleichgültig und transparent, ob die Option-82 direkt von den Switches oder vom Programm eingefügt wird.

In Testversuchen unter Laborbedingungen hat sich die Vorgehensweise bewährt. Die Verzögerung der DHCP-Anfragen bis zum Vorliegen der Ergebnisse der SNMP-Abfragen verursachte keine Probleme. Das Programm kann somit eingesetzt werden, um das Fehlen von Option-82-fähigen Switches auszugleichen. Für weitere Informationen bezüglich dieses Projekts sei auf die Projektarbeit [Wa06] und die Webseite [Sf06] verwiesen.

3.5 Anwendungsmöglichkeiten

Durch das vorgestellte Konzept lassen sich die Vorzüge des DHCPs und die der statischen Konfiguration gut kombinieren. Im Folgenden werden zwei Beispielszenarien vorgestellt, in denen man die vorgestellte Adressvergabe anhand des Switchports, an dem ein Endgerät angeschlossen ist, besonders gut nutzen kann.

In Wohnheimen, die Internetzugang über das Universitätsnetz besitzen, sind die Kontrolle auf Netzmissbrauch und eine Erfassung der Transfervolumen wichtige Aspekte. Beispielsweise werden an der TU Kaiserslautern die Nutzer dazu aufgefordert, ihre Endgeräte mit vorgegebenen IP-Adressen zu konfigurieren. Das Konfigurieren der IP-Adresse eines Endgerätes ist zwar an sich kein großer Aufwand, aber für unkundige Anwender mag dies durchaus eine Hürde darstellen. Mit der hier dargestellten Lösung ließe sich dieses Problem umgehen: Die IP-Adresse würde mittels DHCP automatisch zugewiesen werden und wäre dennoch fest an die Netzwerkdose in einem Appartement gebunden. Würde diese IP-Adresse in Zusammenhang mit Missbrauch auffallen, so wäre ein direkter Rückschluss auf den Verursacher möglich. Das Transfervolumen eines Nutzers kann leicht über die IP-Adresse erfasst werden.

Ein weiteres Anwendungsfeld wäre die Nutzung des vorgestellten Ansatz in Hörsälen. Hier kommt es oft zu wechselnden und unbekannten Nutzern. Die Vorzüge von DHCP kommen hier besonders zum Tragen. Dadurch, dass entsprechend dem vorgestellten Ansatz die IP-Adressen der Hörsaal-Netzwerkdosen von den Administratoren festgelegt werden, können Netzwerkdienste für diese IP-Adressen und somit für diese Netzwerkdosen gesperrt werden. Somit ist ein Kompromiss gefunden, die dem Nutzer einfache Netzwerkzugänglichkeit bietet und dennoch ein gewisses Maß an Sicherheit zulässt.

4 Zusammenfassung

Einleitend wurden einige gängige Techniken zur Konfiguration von Endgeräten vorgestellt. Aus Sicht des Netzwerkadministrators ist eine feste Relation zwischen IP-Adressen und Nutzern sinnvoll. So lassen sich über die IP-Adressen auf einfache Weise Dienste für gewisse Nutzer sperren, und es lassen sich leicht Rückschlüsse auf das Nutzerverhalten ziehen. Für den Nutzer hingegen ist ein möglichst einfacher Netzwerkzugang sinnvoll.

Als Kompromiss wurde ein Verfahren vorgestellt, mit dem der DHCP-Dienst so beeinflusst werden kann, dass IP-Adressen nicht "zufällig" sondern abhängig von der physikalischen Anbindung des Nutzers zugewiesen werden. Dies erhöht die Transparenz für Administratoren, da aus jeder IP-Adresse gleich auf die geographische Position (Netzwerkdose) des Nutzers geschlossen werden kann. Andererseits müssen Benutzer ihre Endgeräte nicht wie bei einer statischen Adressvergabe manuell konfigurieren. Dies macht die Nutzung von Notebooks etc. im Hörsaal sehr benutzerfreundlich. Auch für Wohnheime ist die Lösung interessant.

Konkret wurde für die Realisierung des Konzepts der ISC DHCP-Server verwendet und die recht schwach dokumentierte DHCP Option-82. Bei Einsatz von Option-82-fähigen Switches ist der DHCP-Server in der Lage, anhand der Option-82 festzustellen, an welcher Netzwerkdose sich ein Nutzer mit dem Netzwerk verbunden hat. Anhand dieser Informationen kann der DHCP-Server nun eine vorgesehene IP-Adresse an den Nutzer vergeben. Für den Fall, dass die Edge-Switches keine Option-82 unterstützen, kann auf den „DHCP-Snooper“ zurückgegriffen werden, der im Rahmen einer Projektarbeit entwickelt wurde. Er arbeitet als DHCP-Relay und fügt Option-82-Informationen, die über SNMP von den Switches abgefragt wurden, in die DHCP-Pakete ein.

Literaturverzeichnis

[Al07] Brady Alleman: "Cisco DHCP Snooping with ISC DHCPd", Treehouse Technologies http://www.thtech.net/article/10, Abruf 2007-05-22

[AT06] "Use DHCP Snooping, Option 82 and Filtering on Rapier Series Switches", Allied Telesyn, 2006; siehe http://www.alliedtelesyn.com/, Abruf 2007-05-22

[CS07] "Configuring the DHCP Option 82 for Subscriber Identification, Catalyst 3550 Multilayer Switch Software Configuration Guide", Cisco Systems Inc.; siehe http://www.cisco.com/, Abruf 2007-05-22

[DL02] Ralph E. Droms, Ted Lemon: "The DHCP Handbook", Sams-Verlag, 2002

[IEEE04] "Port-Based Network Access Control", IEEE-Standard 802.1X, 2004

[ISC07] Internet Systems Consortium; http://www.isc.org

[RFC1] R. Droms: "RFC 2131: Dynamic Host Configuration Protocol", 1997; siehe http://www.ietf.org/rfc/rfc2131.txt

[RFC2] S. Alexander, R. Droms: "RFC 2132: DHCP Options and BOOTP Vendor Extensions", 1997; siehe http://www.ietf.org/rfc/rfc2132.txt

[RFC3] M. Patrick: "RFC 3046: DHCP Relay Agent Information Option", 2001; siehe http://www.ietf.org/rfc/rfc3046.txt

[RFC4] R. Johnson et al.: "RFC 3993: Subscriber-ID Suboption for the Dynamic Host Configuration Protocol (DHCP) Relay Agent Option", 2005; siehe http://www.ietf.org/rfc/rfc3993.txt

[Sf06] "DHCP-Snooper", OpenSource-Projekt, gehostet auf SourceForge, siehe http://sourceforge.net/projects/dhcpsnooper/

[Wa06] Patric de Waha: "Vereinfachung der Administration von IP-Netzwerken mit dynamischer Hostkonfiguration", Projektarbeit, AG ICSY, TU Kaiserslautern, 2006