Moritz Hahn
Sarah Altenkrüger

1	2	3	4	Σ

Übungsblatt Nr. 4

(Abgabetermin 20.05.2024)

Aufgabe 4.1

1.

DHCP, das Dynamic Host Configuration Protocol, wird verwendet, um Netzwerkgeräten automatisch IP-Adressen zuzuweisen. Es ermöglicht die dynamische Zuweisung von IP-Adressen, Subnetzmasken, Standardgateways und anderen Netzwerkkonfigurationen an Geräte in einem Netzwerk, ohne dass diese manuell konfiguriert werden müssen.

Im Gegensatz dazu steht RARP, das Reverse Address Resolution Protocol. RARP wird verwendet, um die MAC-Adresse eines Geräts in eine IP-Adresse umzuwandeln. Es war in früheren Netzwerken vor DHCP weit verbreitet, aber es hat einige Einschränkungen im Vergleich zu DHCP.

Der Hauptunterschied zwischen DHCP und RARP liegt in ihrer Funktionsweise und ihrem Anwendungsbereich:

1. DHCP ist dynamisch und bietet eine flexible Konfiguration, da IP-Adressen je nach Bedarf an Geräte vergeben werden können. RARP hingegen ist statisch und erfordert eine manuelle Konfiguration der IP-Adressen und der zugehörigen MAC-Adressen in einer zentralen Datenbank.

2. DHCP bietet eine zentralisierte und automatisierte Verwaltung von IP-Adressen, was die Netzwerkadministration erheblich vereinfacht. RARP erfordert hingegen eine manuelle Konfiguration und Wartung der RARP-Tabellen auf jedem Host im Netzwerk.

3. DHCP unterstützt die Vergabe von weiteren Netzwerkkonfigurationen wie Subnetzmasken, Standardgateways, DNS-Servern usw., während RARP nur die Zuordnung von MAC-Adressen zu IP-Adressen ermöglicht.

2.

Der Vorteil von DHCP gegenüber RARP liegt in seiner Dynamik, Automatisierung und der Unterstützung zusätzlicher Netzwerkkonfigurationen. DHCP erleichtert die Verwaltung von IP-Adressen und anderen Netzwerkressourcen in großen Netzwerken erheblich.

3.

Nehmen wir an, ein Clientgerät, sagen wir ein Laptop, wird an ein Netzwerk angeschlossen und benötigt eine IP-Adresse sowie andere Netzwerkkonfigurationen. Der Ablauf von DHCP kann wie folgt beschrieben werden:

1. **DHCP Discover (Entdecken):**

   Der Client sendet ein DHCP-Discover-Paket über das Netzwerk. Dies ist ein Broadcast-Paket, das an alle Geräte im lokalen Netzwerk gesendet wird. Das Paket enthält die

MAC-Adresse des Clients und den DHCP-Client-Identifier. Der Zweck dieses Pakets ist es, einen DHCP-Server im Netzwerk zu finden und um Konfigurationsinformationen zu bitten.

2. **DHCP Offer (Angebot):**

   Ein oder mehrere DHCP-Server im Netzwerk empfangen das DHCP-Discover-Paket und senden als Antwort DHCP-Offer-Pakete. Jedes Angebot enthält eine IP-Adresse, Subnetzmaske, Standardgateway, DNS-Server und möglicherweise andere Konfigurationsinformationen. Jeder Server kann ein Angebot senden, aber der Client wählt normalerweise das erste erhaltene Angebot aus.

3. **DHCP Request (Anfordern):**

   Der Client wählt aus den erhaltenen Angeboten eines aus und sendet ein DHCP-Request-Paket an den ausgewählten Server. Dieses Paket bestätigt die Auswahl der angebotenen Konfiguration. Es enthält normalerweise die IP-Adresse, die der Client möchte.

4. **DHCP Acknowledge (Bestätigen):**

   Der DHCP-Server empfängt den Request des Clients und sendet ein DHCP-Acknowledge-Paket als Bestätigung zurück. Dieses Paket enthält die endgültige Zuweisung der IP-Adresse und anderer Netzwerkkonfigurationen. Sobald der Client dieses Paket empfängt, wendet er die erhaltenen Konfigurationen auf sein Netzwerkinterface an und ist nun vollständig in das Netzwerk integriert.

Dieser Ablauf stellt sicher, dass das Clientgerät dynamisch eine IP-Adresse und andere Netzwerkkonfigurationen erhält, ohne dass eine manuelle Konfiguration erforderlich ist. DHCP ermöglicht eine effiziente Verwaltung von IP-Adressen und anderen Netzwerkkonfigurationen in Netzwerken jeder Größe.

Aufgabe 4.2

1.

Traceroute ist ein Diagnosetool, das verwendet wird, um den Weg zu einem Zielhost im Netzwerk zu verfolgen. Es funktioniert, indem es eine Serie von ICMP Echo Request (Ping) Paketen mit inkrementierenden TTL (Time-to-Live) Werten sendet. Jedes Paket wird an einen Router auf dem Weg zum Ziel gesendet. Wenn ein Router ein Paket mit einem TTL-Wert von 0 empfängt, verwirft er das Paket und sendet eine ICMP Time Exceeded-Fehlermeldung zurück an den Absender. Durch die Analyse dieser Fehlermeldungen kann Traceroute den Weg zum Ziel host verfolgen, da jeder Router auf dem Weg seine eigene ICMP Time Exceeded-Fehlermeldung zurücksendet. Auf diese Weise kann Traceroute den Pfad durch das Netzwerk anzeigen und die Round-Trip-Zeiten (RTTs) zu jedem Hop messen.

2.

Path MTU Discovery ist ein Mechanismus, der verwendet wird, um die maximale Übertragungseinheit (MTU) auf dem Pfad zwischen einem Sender und einem Empfänger zu bestimmen. Dies ist wichtig, um sicherzustellen, dass Pakete nicht fragmentiert werden müssen, was die Effizienz und Leistung des Netzwerks beeinträchtigen kann. Path MTU Discovery funktioniert, indem der Sender Pakete mit der DF (Don't Fragment) Bit gesetzt sendet. Wenn ein

Paket auf seinem Weg durch das Netzwerk auf einen Router mit einer kleineren MTU als der Größe des Pakets trifft, wird der Router das Paket ablehnen und eine ICMP Fragmentation Needed-Fehlermeldung zurücksenden. Diese Fehlermeldung enthält Informationen über die maximale Größe des Pakets, das am Router passieren kann, ohne fragmentiert zu werden. Durch die Analyse dieser Fehlermeldungen kann der Sender seine Paketgröße anpassen, um Fragmentierung zu vermeiden und die Effizienz der Datenübertragung zu maximieren.

3.

Um festzustellen, auf welches Paket sich eine ICMP-Fehlermeldung bezieht, muss der Empfänger der Nachricht das Feld ̈Identifierïm ICMP-Header überprüfen. Dieses Feld wird normalerweise von der Anwendung oder dem Protokoll festgelegt, das das ICMP-Paket ausgelöst hat. Es dient dazu, die ICMP-Nachricht einem bestimmten Paket zuzuordnen. Darüber hinaus kann das Feld SSequence Number"verwendet werden, um die Reihenfolge der Pakete zu verfolgen, insbesondere wenn mehrere Pakete vom gleichen Sender gesendet wurden. Durch die Analyse dieser Felder kann der Empfänger einer ICMP-Nachricht das betroffene Paket identifizieren und geeignete Maßnahmen ergreifen.

Aufgabe 4.3

1.

Eine von einer echten MAC-Adresse abgeleitete link-local IPv6-Adresse beginnt normalerweise mit dem Präfix "fe80::"gefolgt von den Interface-Identifier-Bits. Um festzustellen, ob eine link-local Adresse von einer echten MAC-Adresse abgeleitet wurde, können Sie die Interface-Identifier-Bits überprüfen. Wenn die Interface-Identifier-Bits die MAC-Adresse des Geräts widerspiegeln, dann wurde die link-local Adresse wahrscheinlich von der MAC-Adresse abgeleitet.

2.

Mit SLAAC (Stateless Address Autoconfiguration) wird aus einer link-local IPv6-Adresse eine globale IPv6-Adresse durch die Hinzufügung des globalen Präfixes. Das globale Präfix kann entweder manuell konfiguriert sein oder über Router Advertisement-Nachrichten (RA) empfangen werden. Nachdem das globale Präfix hinzugefügt wurde, kann die global eindeutige IPv6-Adresse gebildet werden.

3.

Die Privacy Extension für SLAAC wurde eingeführt, um die Privatsphäre der Benutzer zu verbessern und die Möglichkeit zu verhindern, dass Netzwerkanalyse-Tools mithilfe von IPv6-Adressen das Verhalten und die Aktivitäten der Benutzer verfolgen können. Mit der Privacy Extension generiert ein Host regelmäßig zufällige Interface-Identifier-Bits für seine IPv6-Adressen anstelle der Verwendung seiner MAC-Adresse. Auf diese Weise werden die Identität und der Standort des Hosts vor zufälliger Identifizierung geschützt.

4.

DAD wird im Kontext von SLAAC verwendet, um sicherzustellen, dass die automatisch konfigurierte IPv6-Adresse eindeutig im Netzwerk ist. Bevor ein Host eine IPv6-Adresse

aktiv verwendet, führt er DAD durch, indem er eine Neighbor Solicitation-Nachricht sendet, um sicherzustellen, dass keine anderen Geräte im Netzwerk dieselbe Adresse verwenden. Wenn eine Antwort empfangen wird, bedeutet dies, dass die Adresse bereits verwendet wird und der Host muss eine andere Adresse generieren. DAD stellt sicher, dass es keine Adresskonflikte im Netzwerk gibt.

Aufgabe 4.4

1.

IP-Multicast ist eine Technik zum Senden von Datenpaketen an eine Gruppe von Empfängern in einem Netzwerk. Es ermöglicht die effiziente Übertragung von Daten an mehrere Ziele, ohne dass jedes Paket einzeln an jedes Ziel gesendet werden muss. Ein Anwendungsgebiet für IP-Multicast ist z.B. das Video-Streaming, bei dem ein Video an mehrere Benutzer gleichzeitig übertragen werden soll.

2.

Endgeräte können Multicast-Gruppen beitreten, indem sie Multicast-Mitgliedschaftsprotokolle wie Internet Group Management Protocol (IGMP) verwenden. Ein Beispiel für den Ablauf einer Multicast-Anwendung ist das Video-Streaming über das Internet. Wenn ein Benutzer eine Videostreaming-Anwendung startet und einem Multicast-Stream beitreten möchte, sendet sein Endgerät eine IGMP-Mitgliedschaftsnachricht an den Router, um dem Multicast-Stream beizutreten. Der Router fügt das Endgerät dann zur Multicast-Gruppe hinzu, sodass es die Multicast-Datenpakete empfangen kann, die vom Streaming-Server gesendet werden.

3.

Der Hauptunterschied zwischen mehrfachem IP-Unicast und echtem IP-Multicast liegt in der Art und Weise, wie Daten an mehrere Empfänger gesendet werden. Beim mehrfachen IP-Unicast sendet der Sender separate Kopien der Daten an jeden einzelnen Empfänger, was zu einer höheren Netzwerklast führt, insbesondere wenn viele Empfänger vorhanden sind. Im Gegensatz dazu verwendet echter IP-Multicast eine einzelne Kopie der Daten, die über das Netzwerk an alle Mitglieder der Multicast-Gruppe verteilt wird, was die Netzwerklast erheblich reduziert.

4.

Ein Host ändert seine IP-Adresse nicht zu der Adresse der Multicast-Gruppe, wenn er dieser beitritt. Stattdessen bleibt seine IP-Adresse unverändert. Der Host muss lediglich dem Multicast-Gruppenadressbereich beitreten, um Multicast-Datenpakete empfangen zu können. Dies geschieht normalerweise über Multicast-Mitgliedschaftsprotokolle wie IGMP.

5.

Source-Based Trees und Group-Shared Trees sind zwei verschiedene Ansätze für das Multicast-Routing. Bei Source-Based Trees wird ein separater Baum für jede Quelle im Netzwerk erstellt, während bei Group-Shared Trees ein einziger Baum für eine Gruppe von Empfängern gemeinsam genutzt wird. Der Hauptunterschied besteht also darin, wie die Routingbäume erstellt und verwaltet werden.

6.

Bei Source-Based Trees benötigen die Router mehr Zustandsinformationen, da sie separate Routingbäume für jede Quelle im Netzwerk verwalten müssen. Im Gegensatz dazu benötigen Router bei Group-Shared Trees weniger Zustandsinformationen, da sie einen einzigen Routingbaum für eine Gruppe von Empfängern gemeinsam nutzen. Das Verhältnis von Zustandsinformationen zwischen Source-Based Trees und Group-Shared Trees hängt von der Anzahl der Quellen und der Anzahl der Empfänger in der Multicast-Gruppe ab. In großen Netzwerken mit vielen Quellen und Empfängern kann das Verhältnis deutlich sein, wobei Source-Based Trees mehr Zustand erfordern.