NET Aufgabenblatt 2  
  
2.1.1)

**Welche Vorteile und Nachteile ergeben sich in einem Netzwerk durch die Verwendung von DHCP im Vergleich zur statischen Adressvergabe?**  
  
Das Dynamic Host Configuration Protocol, DHCP, ist ein Protokoll, welches IP Adressen und andere netzwerkbasierte Konfigurationen innerhalb eines Netzwerkes verwaltet und somit einem neuen Host, diese Konfiguration sowie auch eine dynamisch alloziierte IP Adresse zuweisen kann. Hierfür sendet der Host eine DHCP Anfrage, an den DHCP Server, welcher via dynamischer Adresszuweisung dem Host eine freie IP sendet. Im Kontrast hierzu steht die statische Adressvergabe, bei welcher die IP des Host direkt vom Netzwerkverwalter (beispielsweise dem ISP) konfiguriert wird.[1]  
  
**Vorteile für die Verwaltung eines Netzwerkes via DHCP:**

* Einem jedem neuen Host innerhalb des Netzwerkes können automatisch, die für das Netzwerk benötigten Einstellungen zugewiesen werden. Dies ermöglicht **eine einfache, unkomplizierte und meistens fehlerfreie Erweiterung des Netzwerkes.**
* **DHCP verringt** folglich **den Verwaltungsaufwand** eines Netzwerkes.
* Gewisse **Internetangebote, die eine Userdifferenzierung anhand der IP-Adresse des Hosts vollziehen können ausgetrickst werden**, indem man sich eine neue IP Adresse für den Host vom DHCP Server zuweisen lässt. Dies trifft beispielsweise auf verschiedene File-Sharing Portale zu.[3]
* Eine regelmäßige Änderung der IP Adresse kann zur Anonymisierung des Nutzers beitragen, indem sie es erschwert den ehemaligen Nutzer hinter einer erneut vergebenen IP Adresse zu bestimmen.

**Nachteile bei einer Verwendung von DHCP:**

* **DHCP Server sind anfällig für Angriffe von innerhalb des Netzwerkes**, da sie jeden neuen Host annehmen und ihn automatisch in ihr Netzwerk eingliedern. Ein Beispiel für einen solchen Angriff von Innen wäre der sogennante **DHCP Starvation Attack**, bei dem ein Angreifer alle möglichen Adressen die der DHCP Server vergeben kann für sich reserviert.  
  Selbst das einfügen eines neuen Gerätes in das Netzwerk wie beispielsweise eines W-Lan Routers, der standardmäßig einen eigenen DHCP Server besitzt, kann ein ganzes Netzwerk lahmlegen.
* Wechselnde IP Adressen der Hosts, machen es schwer Serveranwendungen verlässlich auf einem Host laufen zu lassen. Ein FTP-Server der beispielsweise auf einem Heimrechner läuft, könnte nach einem Stromausfall oder nach dem Ablauf der DHCP-Leasezeit[5], über eine andere IP Adresse erreichbar sein. DHCP verwaltete Geräte ermöglichen keinen ungestörten Serverbetrieb.

**Vorteile der statischen Adressvergabe:**

* Statische Adressen sind verlässlicher, da man davon ausgehen kann, dass sie sich nicht verändern und somit Datenpakete immer an den gewünschten Empfänger weitergeleitete werden. Gewisse Netzwerkkomponenten, können nicht oder nur sehr schwer via DHCP in das Netzwerk integriert werden. Ein Drucker im Netzwerk beispielsweise sollte immer eine statische IP Adresse haben, um zu verhindern, dass für ihn bestimmte Datenpakete aufgrund einer veränderten IP-Adresse woanders ankommen.Aufgrund der statischen IP ist ein Host oder ein Server, eindeutig bestimmbar und ist somit eine gute Umgebung für Serverapplikationen.
* Ein Gerät mit statischer IP kann sehr gut als Server dienen.

**Nachteile der statischen Adressvergabe:**

* Jedes Gerät muss händisch vor der Verwendung im Netzwerk konfiguriert werden.
* Internet Service Provider, vergeben statische IP Adressen zu meist höheren Preisen.[6]
* Nutzer können aufgrund ihrer statischen IP Adresse leicht bestimmt werden.

[1] Seite 308

[2] <http://de.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol#Sicherheit>  
[3] Quelle: Persönliche Erfahrung anhand des Angebots der Website [www.rapidshare.com](http://www.rapidshare.com)  
[5] <http://de.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol#DHCP-Refresh_.28nur_bei_dynamischer_Zuordnung.29>

[6] <http://www.a1.net/business/produkte-loesungen/a1-festnetz-internet-business-tarif>  
[7] Vorlesung Netzwerktechnologien Vorlesungsfolien SS14 Kapitel 3 Draft Folie 13,

[8] Vorlesung Netzwerktechnologien Vorlesungsfolien SS14 Kapitel 3 Draft Folie 19

[9] Buch Seite 261

2.1.2)

Für meine Untersuchungen habe ich Kollegen gebeten mir von verschiedenen Computern und mit verschiedenen Email-Clients, Emails an meine Mailadresse zu senden. Um meine Ergebnisse zu verifizieren bat ich meine Kollegen darum, in den Body der Email Informationen über ihre IP-Adresse, den Email-Client und ihr Betriebsystem zu schreiben. Ich habe diese Emails von meinem Email-Server mit Hilfe des Programmes „Mozilla Thunderbird“ heruntergeladen und den Quelltext analysiert.  
  
Der Eintrag X-Mailer im Header gab mir in manchen Fällen Auskunft über das Programm welches Programm die E-Mail versandt wurde. Zum Beispiel „X-Mailer: Microsoft Outlook 14.0”. Auf das Betriebsystem konnte ich nur in Ausnahmefällen implizit durch die Verwendung bestimmter Programme schließen. Der Eintrag „Mime-Version: 1.0 (Apple Message framework v1085) X-Mailer: Apple Mail (2.1085)” verriet mir beispielsweise, dass es sich um ein Gerät von Apple also folglicherweise einem Computer mit dem Betriebsystem MacOSX handeln musste. Analog hierzu konnte ich durch den Eintrag „User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:24.0) Gecko/20100101 Thunderbird/24.4.0“ einer Email des Herrn Professor Grosser, auf die Verwendung einer Linux Distribution schließen.  
  
In allen Fällen wurde mir auch IP Adressen innerhalb des Headers übermittelt, jedoch bezogen sich diese nicht immer auf den wirklichen Sender der Email, sondern auf die Email-Server über die der Datenverkehr lief.

Insbesondere die Nutzer, welche ihre Emails über Webmail Anwendungen verschickt haben, überlieferten ihre persönliche IP nicht in dem Header sondern stattdessen die IP des Webmail-Servers auf dem die Email über eine Webanwendung erstellt wurde und nicht die IP des Computers von dem aus, sie die Email geschrieben haben.  
  
Im Kontrast hierzu wurden mir die IP Adressen von Anwendern von Email-Anwendungen die auf dem Rechner installiert wurden immer übermittelt.  
  
Zusammenfassen möchte ich sagen, dass sich in den meisten Fällen Informationen über den Sender ermitteln lassen, insbesondere Informationen über die Anwendung und somit inplizit über das Betriebsystem, jedoch die IP Adresse nur manchmal eindeutig bestimmbar ist, wenn die Email nicht über das Webinterface einer Website erstellt wurde.

SOLL ICH NOCH EINEN BSP Header Einfügen? :/

Zitat von http://de.wikipedia.org/wiki/Header\_%28E-Mail%29

*Der Header enthält keine für die technische Zustellung einer E-Mail notwendigen Informationen. Absender und Empfänger werden durch den* [*Envelope Sender*](http://de.wikipedia.org/wiki/Envelope_Sender) *und* [*Envelope To*](http://de.wikipedia.org/wiki/Envelope_To) *angegeben.*

2.1.3)

**Anhand welcher Kriterien entscheiden Sie sich für ein passendes Transportprotokoll zu einer bestimmten Anwendung?**

[7]Um sich über die Kriterien die ein Transportprotokoll erfüllen sollen klar zu werden, muss man sich zunächst überlegen welche Anforderungen die Anwendung an das Netzwerk stellt. Oftmals ist eine sichere **Verbindung ohne Paketverluste und mit Integritätsüberprüfung der Pakete** eine sinnführende Voraussetzung, beispielsweise für Dateitransfere und Vergleichbares. [7] Gleichzeitig jedoch wünscht sich der User, dass jeder Traffic so schnell wie möglich bearbeitet und gesendet werden kann somit muss ein Transportprotokoll auch eine gewisse Bandbreite zusichern können. Eine ständige Überprüfung der Datenpakete auf Vollständigkeit, kann diese Bandbreite vermindern. Um ein neues Beispiel zu nennen, wäre es nicht zwangsmäßig zielführend bei einem Livestream oder einem VoIP-Call, jedes Datenpaket auf Integrität zu überprüfen, da hierdurch nach und nach ein stärkerer zeitlicher Delay entstehen kann.  
  
Ein anderes mögliches Kriterium für eine Anwendung ist die Möglichkeit der Selbstdrosselung der Sendegeschwindigkeit, im Falle dessen, dass Netzwerkknotenpunkte (Router) ausgelastet sind.  
Außerdem könnte eine Anwendung benötigen, dass sich der Server an frühere Anfragen des Clients erinnert.[8]  
  
Ein nicht außer acht zu lassendes Kriterium, ist natürlich auch die Sicherheit die das Protokoll bietet. Eine Anwendung die mit Bankdaten arbeitet, muss nicht nur ohne Paketverluste arbeiten sondern auch eine abhörsicherere verschlüsselte Verbindung bieten können.  
  
Zusammenfassend nochmal die einzelnen Kriterien in Stichworten:

* Paketverluste tolerierbar?
* Paketintegrität muss kontrolliert werden?
* Zusicherung von Bandbreiten?[9]
* Wie hoch darf die Latenz ausfallen? – Soll sie annähernd Echtzeit betragen?
* Senderaten Drosselung erlaubt?
* Zustandslos? Ja/Nein?
* Abhörsicher/Verschlüsselbar?