opennet 1997

DHCP und das Management nomadischer Systeme in Intranets

Stephen Heilbronner

MNM TEAM

Institut für Informatik
Ludwig-Maximilians-Universität München
Oettingenstr. 67, 80538 München

Email: heilbron@informatik.uni-muenchen.de
WWW: http://www.nm.informatik.uni-muenchen.de

Kurzfassung

In den letzten Jahren haben sich TCP/IP-basierte “Intranets” als weitestgehend optimale Infrastruktur für verteiltes *Client-/Server-Computing* herausgestellt. Mittlerweile unterstützen alle gängigen Client-Betriebssysteme und demnächst wohl auch alle tragbaren Geräte (wie z.B. Notebooks und Personal Digital Assistants) die Internet-Protokolle. Es ist daher möglich geworden, eine weitgehend homogene Infrastruktur auf der Basis offener Standards aufzubauen, die auch effizient verwaltet werden könnte, wenn nur allgemein anerkannte Managementstandards zum integrierten Management dieser Infrastruktur definiert und implementiert wären.

In diesem Vortrag sollen insbesondere die Infrastruktur- und die Managementanforderungen betrachtet werden, die beim Einsatz *mobiler* Endgeräte entstehen (*Nomadic Computing*). Besonders berücksichtigt wird die Verteilung der Konfigurationsinformation mittels des *Dynamic Host Configuration Protocols* (DHCP) in Umgebungen mit verschiedenen Sicherheitsanforderungen, sowie das integrierte Management der Netzinfrastruktur. Den Schluß bildet eine kurze Darstellung geeigneter Produkte sowie demnächst zu erwartende Weiterentwicklungen auf diesem Gebiet.

Überblick

- **Nomadische Systeme in Intranets**
  - Charakteristiken, Probleme
  - Infrastruktur
- **Dynamic Host Configuration Protocol (DHCP)**
  - Infrastruktur
  - Ablauf
- **Sicherheitsanforderungen**
- **Beispielszenario**
- **Managementanforderungen**
- **Produkte**
- **Zukunft**

Stephen Heilbronner

2

Der Vortrag gliedert sich in die folgenden Abschnitte:

•Charakteristiken heutiger TCP/IP-basierter Intranets und Probleme beim Einsatz nomadischer Systeme, typische Infrastrukturkomponenten

•Das Dynamic Host Configuration Protocol (DHCP) Version 4: Organisations-, Informations- und Funktionsmodell

•Die “Sicherheitspolitik”, die “Rechte und Pflichten” der beteiligten Systeme anhand einer Bedrohungsanalyse festlegt, als Voraussetzung für den Einsatz nomadischer Systeme

•Beispielszenario für den integrierten Einsatz von Switch- und DHCP-Server-Management zur Implementierung geschlossener IP-LANs

•Aus dem integrierten Einsatz entstehende Managementanforderungen für die Überwachung und Steuerung der Infrastruktur (Switches, DHCP, DNS etc.)

•Kriterien zur Produktauswahl

•Ausblick

Bemerkung: Der Begriff *nomadisch* anstelle von *mobil* wird i.f. verwendet, um die Abgrenzung der Betrachtungen zum Bereich der mobilen Geräte in der Telekommunikation deutlich zu machen. Dies schließt die Verwirklichung der *Nomadizität* durch TK-Netze nicht aus, die dabei entstehenden Fragen müssen jedoch getrennt diskutiert werden.

Nomadische Systeme in Intranets

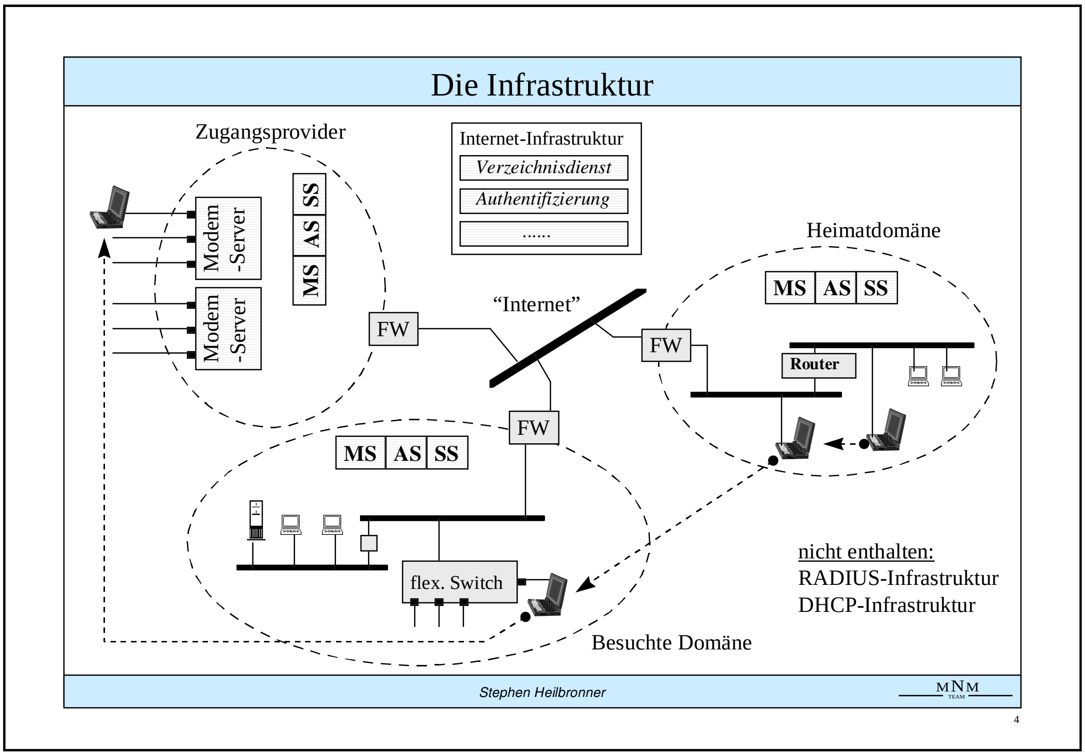
- **Charakteristiken**
  - Netze: TCP-IP-basiert, meist mit *Switches* realisiert, Windows dominiert
  - UNIX/NT/Novell-Server
  - Kaum *integriertes, offenes LAN-Management*
  - Proprietäre Lösungen für externen Zugang
- **Probleme**
  - Manuelle benutzerspezifische und System-Konfiguration
  - Große Heterogenität verwendeter Systeme und Nutzungsanforderungen
  - Nur proprietäre Anwendungskonfiguration
  - Umzug und Migration erfordern großen, manuellen Aufwand
  - Gute Sicherheit nur physisch zu gewährleisten
  - Gewährleistung der Verfügbarkeit durch Replikation kritischer Dienste
- **Nomadische Systeme nur manuell/proprietär anschließbar !!**

Die TCP/IP-basierten Intranets moderner PC-Clients und -Server unterschiedlichster Betriebssysteme sind heute meist nur in den Basisdiensten (und natürlich in den proprietären Anwendungen) interoperabel. Als Problem kommt hinzu, daß die Basisdienste, die für eine Integration nomadischer Systeme (und Benutzer) wichtig sind, kaum in integrierter Weise verwaltet werden können, denn es mangelt an Managementstandards bzw. deren Umsetzung in konkreten Produkten.

Bemerkenswerterweise ergeben sich bei der Suche nach Lösungen für Fragen und Probleme, die sich beim Thema “Unterstützung nomadischer Systeme im Intranet” stellen, oft Teilfragen, deren Lösung auch Probleme anderer Managementaufgaben mit abdeckt, wie zum Beispiel:

- Manuelle benutzerspezifische und System-Konfiguration
- Große Heterogenität verwendeter Systeme und Nutzungsanforderungen
- Proprietäre Anwendungskonfiguration
- Umzug und Migration mit großem manuellem Aufwand
- Gute Sicherheit nur physisch zu gewährleisten
- Gewährleistung der Verfügbarkeit durch Replikation kritischer Server-Dienste

Das Problemfeld wird hier eingeschränkt auf die Teilfrage, wie nomadische Systeme in das Intranet möglichst automatisiert integriert und dabei auftretende Konflikte mit einer zu definierenden Sicherheitspolitik gelöst werden können. Als Basis für die Konfigurierung der Systeme wird der Internet-Standard *Dynamic Host Configuration Protocol (DHCP)* 3 angenommen. Erweiterungen des Protokolls und der aufgestellten Architektur



Ein Intranet in unserem Sinne bietet folgende Zugangsmöglichkeiten für nomadische Systeme:

•Anschluß über einen Ethernet-Hub oder -Switch

•Zugang durch drahtlose Netze (und evtl. einen Router zum drahtlosen Subnetz)

•Zugang vom Internet über eine Firewall

•Modemzugang über einen Modemserver

Die Basiskonfiguration des Systems nach dem Anschluß des nomadischen Systems in den (hier betrachteten) ersten drei Fällen sollte folgenden Anforderungen genügen:

•automatisiert, d.h. kein manueller Eingriff erforderlich

•authentifiziert, d.h. nur zulässige Systeme dürfen Zugriff erhalten (soweit nötig/möglich)

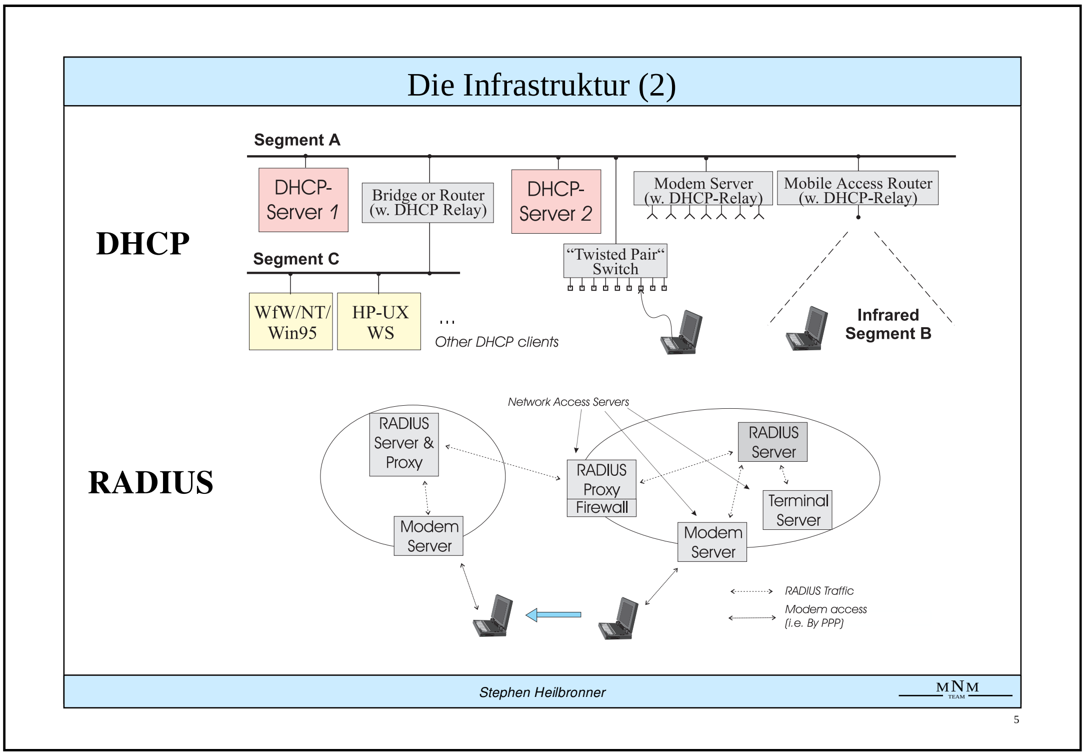
•vollständig (Netz-, System- und Anwendungskonfiguration)

•standardisiert, d.h. für alle Systeme in einheitlicher Form

Diesen Anforderungen genügt das derzeit DHCP am besten, nur die Sicherheitsmechanismen sind derzeit **noch nicht** Teil des Standards, können aber dennoch proprietär implementiert werden.

Bemerkung: Aufgrund einer festgelegten Sicherheitspolitik oder anderen Erwägungen müssen natürlich nicht unbedingt alle o.g. Zugangsmöglichkeiten verwirklicht werden; die Darstellung soll weiteren Managementbedarf motivieren, der bei einer komplexeren Infrastruktur entsteht.

Bemerkung: Zur Unterstützung von Nomadic Computing wird durch die IETF derzeit das Protokoll *Mobile-IP* standardisiert. Da es sich jedoch kaum verbreitet und sein Einsatz aus

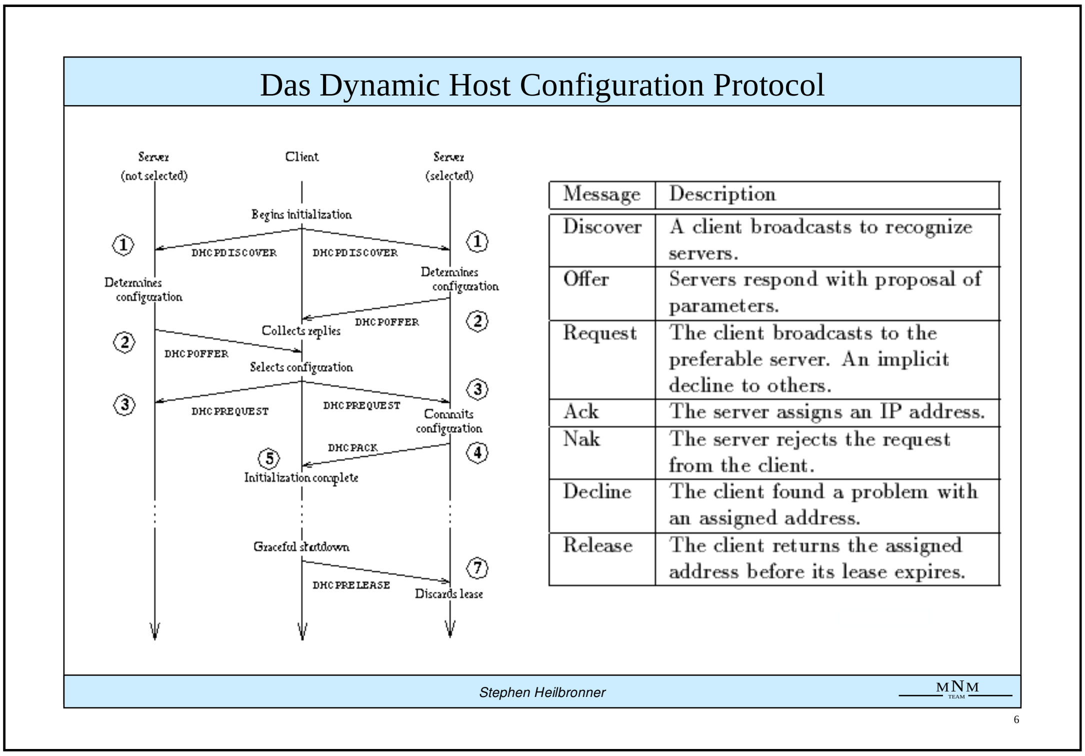


Ein typisches Netz, in dem die Konfiguration der Endsysteme durch DHCP gesteuert wird, besteht aus mehreren Teilnetzen (LAN-Segmente oder Subnetze), die räumlich über das Unternehmen verteilt sind. Zugangspunkte bestehen an den Switches oder durch drahtlose Netze.

Um ein Mindestmaß an Verfügbarkeitsanforderungen zu erfüllen, sollte natürlich mehr als nur ein DHCP-Server vorhanden sein, da ansonsten dessen Ausfall die Funktion sämtlicher Client-Endsysteme beeinträchtigt. Auch in Hinblick auf die Performanz kann es bei zu wenigen Servern zu Problemen kommen ("Montagmorgen-Syndrom").

Für die Standardisierung der Kommunikation der DHCP-Server über die aktuelle Netzkonfiguration sowie der Resynchronisation nach einer Netzpartitionierung existieren derzeit - abgesehen von einigen Vorschlägen auf Mailinglisten - noch kaum Vorschläge. Es scheint, als ob weder die Hersteller noch die entsprechende IETF Working Group (dhc) dies als besondere Notwendigkeit sehen.

Für die standardisierte Authentifizierung am Modem- und am Internetzugang setzt sich zunehmend das RADIUS-Protokoll (Remote Authentication and Dial-In User Service) durch. Seine Client-Proxy-Server-Architektur erlaubt die flexible Positionierung an Netzzugangspunkten und wird von fast allen Herstellern von Modemservern unterstützt. In Kombination mit DHCP und PPP ist die Aufgabe der Konfiguration der anwählenden Endsysteme in automatisierter Weise gelöst.



Eine detaillierte Beschreibung des Dynamic Host Configuration Protocol (DHCP) findet sich in [RFC 1541] oder in [Come 95]. Zum Verständnis der weiteren Ausführungen soll daher hier nur ein kurzer Überblick gegeben werden.

DHCP ist eine Erweiterung des BOOTP-Protokolls und konkurriert in seiner Basisfunktionalität mit RARP. Gegenüber BOOTP zeichnet es sich vor allem durch die Flexibilität bzgl. der abfragbaren Konfigurationsparameter und durch das Konzept der *Lease* aus, d.h. die Möglichkeit eine Information dem Client gegenüber als nur begrenzt gültig zu markieren. Damit wird die Flexibilität bzgl. Veränderungen der Netztopologie und weiterer Konfigurationsparameter gewahrt. Ferner ist die Unterstützung von großen Netzen, in denen nichts stets alle Systeme zugleich aktiv sind, mit limitierten *Pools* von Adressen möglich. Durch die Rückwärtskompatibilität bzgl. des PDU-Formats von BOOTP ist die Verwendung existierender BOOTP *Relay Agents* in Subnetzen ohne DHCP-Server gewahrt.

Beim Start des Systems schickt der Client ein DHCPDISCOVER-Paket in Form eines Broadcasts an 255.255.255.255 (Phase 1). Anhand der Identifikation des Client im Paket können sich einige (oder ein einzelner) DHCP-Server entscheiden, dem Client die gewünschte IP-Adresse sowie andere Konfigurationsinformation in Form eines DHCPOFFER-Pakets zuzuteilen. (Vor der Vergabe können und sollten die Server die Konfliktfreiheit bzgl. der Adresse mittels ICMP-Ping oder ARP prüfen.)

Der Client kann sich in Phase 2 aus den Antworten eine für ihn geeignete aussuchen und bestätigt dies gegenüber dem Server durch ein DHCPREQUEST-Paket (Phase 3). Entscheidungsparameter können z.B. die Leasedauer (t) oder die Menge der angebotenen Konfigurationsinformation

Bei korrekter Information im DHCPREQUEST bestätigt der Server die Lease durch ein DHCPACK-Paket, womit die Konfiguration abgeschlossen ist

Bevor die IP-Adresse verwendet wird, sollte der Client ihre Einzigartigkeit durch ein *Gratuitious ARP* prüfen. Sollte der Client die angebotene Adresse ablehnen wollen, teilt er dies durch DHCPDECLINE-Paket dem Server und beginnt nach einer kurzen Wartefrist erneut mit Phase 1.

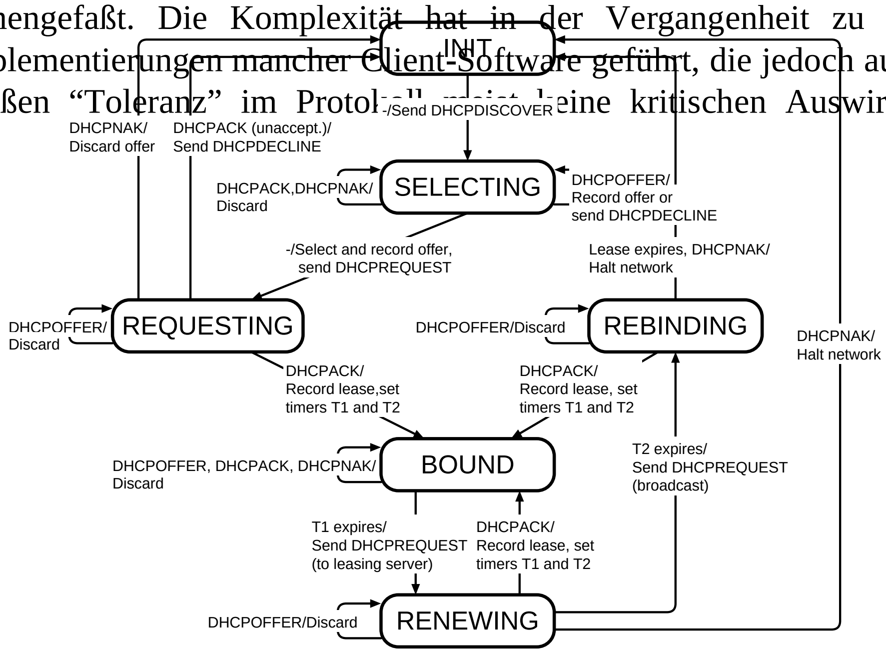
Sobald der Client die Bestätigung durch DHCPACK erhalten hat, ist er für die Überwachung der Lease-Dauer selbst verantwortlich.

Insbesondere kennt das Protokoll in seiner derzeitigen Version auch keine Methode, einem Client die Lease zu entziehen.

Vor Ablauf der Lease-Dauer (meist nach der Hälfte der Zeit = 0,5 * t_l) sollte der Client durch einen erneuten Durchgang durch Phase 3 versuchen, die Lease vom selben DHCP-Server verlängert zu bekommen. Gelingt ihm das nicht, kann er vor endgültigem Ablauf der Lease-Dauer (meist nach ca. 0,8 * t_l) die Phase 1 nochmals durchlaufen, um eine Verlängerung/Neuausstellung der Lease (evtl. von einem anderen Server) zu erhalten.

Die vorzeitige Aufgabe einer Lease sollte der Client dem Server durch ein DHCPRELEASE mitteilen, um den Pool freier Adressen möglichst groß und den Vergabestand im Server möglichst akkurat zu halten.

Alle Zustandsübergange im Client sind in folgender Abbildung zusammengefaßt. Die Komplexität hat in der Vergangenheit zu einigen Fehlimplementierungen mancher Client-Software geführt, die jedoch aufgrund der großen “Toleranz” im Protokoll” meist keine kritischen Auswirkungen hatten.



Sicherheitsanforderungen

- **Verhinderung fehlerhaft konfigurierter Systeme**
  - Netzwerkparameter: IP-Adresse, Broadcast-Masken, Router, DNS
  - Anwendungsserver:
    Zeit (NTP), Email (SMTP), WWW-Proxies (HTTP) u.v.a.m.
- **Ausschluß unerwünschter Systeme**
  - Wiretapping
  - Denial-of-Service Angriffe
  - Inventarisierung
- **Explizite Sicherheitspolitik, -richtlinien**
  - Dokumentation
  - Durchsetzung bzw. Erfassung von Verstößen

Stephen Heilbronner

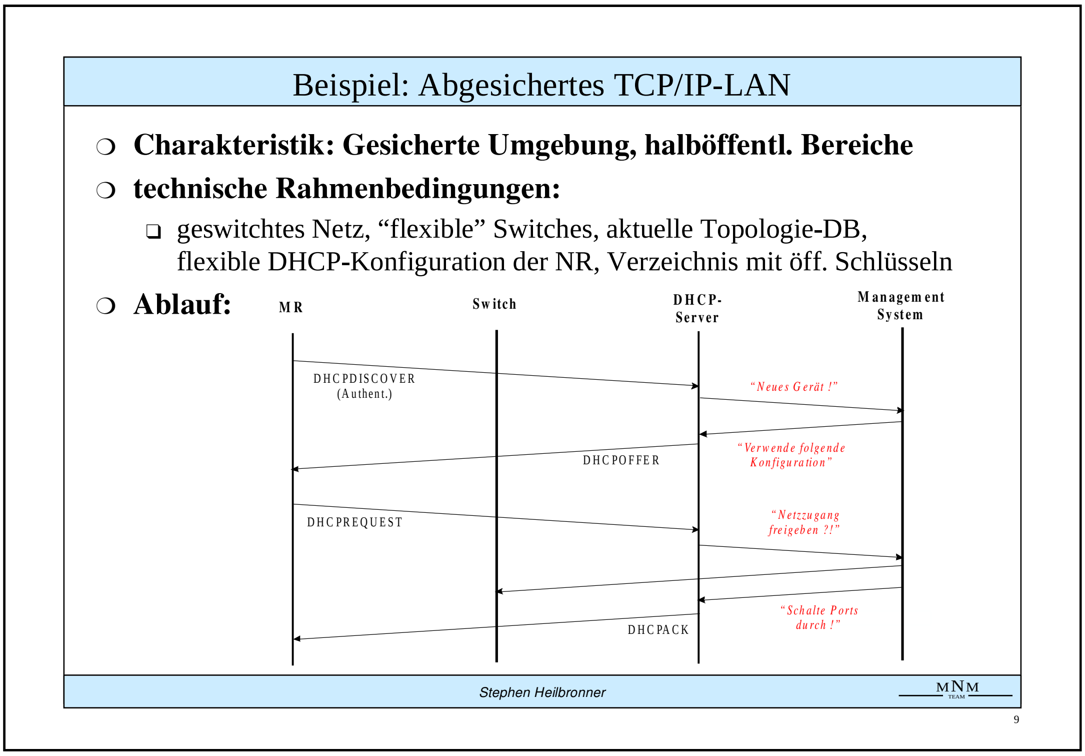
8

Beim Anschluß nomadischer Systeme an das Intranet ist neben der automatisierten Konfiguration der Systeme bzgl. grundsätzlicher Systemeinstellungen die Durchsetzung einer vorher aufzustellenden Sicherheitspolitik eine wichtige Aufgabe. (Diese Politik sollte natürlich nicht nur bzgl. nomadischer Systeme definiert werden, sondern auch Aussagen bezüglich der durch einen unbedarften Anwender leicht umkonfigurierbaren PCs treffen.) In technischer Hinsicht sollten unter anderem Festlegungen bzgl. folgender Bereiche bzw. Konfigurationseinstellungen getroffen werden:

1. Physischer Zugang
2. Weiterleitung von Schicht-2-PDUs (Ethernet/PPP)
3. Authentifizierungsanforderungen an das nomadische System
4. Überwachung Netzverkehr
5. Weiterleitung von Schicht-3-PDUs (IP Routing)
6. Verschlüsselung der Kommunikation (IPsec, Anwendungsebene)

Im folgenden sollen der Kürze halber nur die Durchsetzung der unter 2 bis 4 genannten Festlegungen betrachtet werden; die anderen Parameter erfordern eine hier nicht mögliche, weitergehende Darstellung der Infrastrukturanforderungen.

Die Durchsetzung der Sicherheitspolitik erfordert nun offensichtlich eine Infrastruktur, die integriertes Management aller betroffenen Komponenten erlaubt. Die Anforderungen an diese richten sich natürlich nach den Spezifika der Sicherheitspolitik. Das folgende Beispiel zeigt dies anhand einer geswitchten LANs, das normalerweise weitgehend ungeschützt zugänglich wäre.



In einem der vorher skizzierten Szenarien ist es erwünscht, daß nicht jedes beliebige Endsystem Zugang zum LAN erhält. Das läßt sich erreichen, indem die Ports an Switches nicht a priori freigeschalten sind, sondern die Verbindung erst durch eine spezifische Aktion des Managementsystems hergestellt wird. Voraussetzung für den dargestellten Ablauf ist eine entsprechende Managementfähigkeit der Switches, die leider nur in wenigen Produkten gegeben ist.

Gesichertes Anschließen authentifizierter Endsysteme:

Zu Beginn besteht nur eine Verbindung vom offenen Port zum DHCP-Server, der aufgrund (authentifizierter) DHCP-Anfragen das “Erscheinen” des neuen Endsystems an das Managementsystem meldet.

Dieses entscheidet dann über die “Zulassung” des Endsystems und die von ihm zu verwendende Konfigurationsinformation. Akzeptiert das Endsystem die Information so schaltet das Managementsystem den Switch-Port frei.

Zur Verwirklichung dieser und ähnlicher Szenarien ist es offensichtlich nötig, daß die beteiligten Infrastrukturkompenenten einer genauen Steuerung durch ein Netzmanagementsystem unterworfen werden. Die technische Realisierung dieses Anschlusses sollte natürlich auf der Basis offener Standards geschehen. Hier bietet sich das *Simple Network Management Protocol (SNMP)* an, das in seinen aktuellen Versionen v1/v2 trotz aller Unzulänglichkeiten (Zuverlässigkeit, Sicherheit) der einzig anerkannte Standard für Management in IP-Netzen ist [Rose 94].

Vorteile

- **Kein unbefugter Zugang zum LAN**
- **Verbessertes Abrechnungsmanagement durch**
  - ⇨ Protokollierung der Nutzzugänge
  - ⇨ Integration mit Inventarmanagement
- **Ausfälle der Infrastrukturkompenenten sofort erkennbar**
- **Bei standardisierter Managementinformation Flexibilität bezügliche der Auswahl der Software und Hardware**

Managementanforderungen

- **DHCP-Server**
  - Verwaltung sämtlicher Konfigurationsinformation
  - “Vergebene” Information (*Leases*)
  - Aufgetretene Fehler (fehlerhafte PDUs bzw. Protokollablauf)
- **Switches**
  - Information über angeschlossene Endgeräte
  - Konfiguration virtueller Netze
  - Explizite Vebindungen Port-zu-Port
- **DNS-Server**
  - Überwachung und Kontrolle der dynamischen Aktualisierung
  - Sicherheit, Fehler
- **Modemserver und Firewalls**
- **Internet-Standards (SNMP-MIBs) erst in der Entwicklung**

Stephen Heilbronner MNM TEAM

11

Da der DHCP-Server die Infrastrukturkomponente darstellt, die das gesammelte “Wissen” über die aktuelle Soll- und die (ungefähre) Istkonfiguration der angeschlossenen Clients bereitstellt, ist es wichtig, diese Information dem sonstigen Management möglichst leicht zugänglich zu machen. Managementbereiche, die diese Information benötigen, sind:

•Konfiguration (Inventory)

•Fehlermanagement, Trouble-Ticket-Systeme (TTS)

•Sicherheit (insbesondere bei der Integration mit dem Netzmanagement)

•Abrechnung (Zuordnung der Ressourcennutzung)

SNMP-MIBs, die die hierfür notwendige Managementinformation definieren, wurden bisher kaum entwickelt oder implementiert. Dies gilt insbesondere für das DHCP-Management (mit Ausnahme von Arbeiten am Institut des Autors).

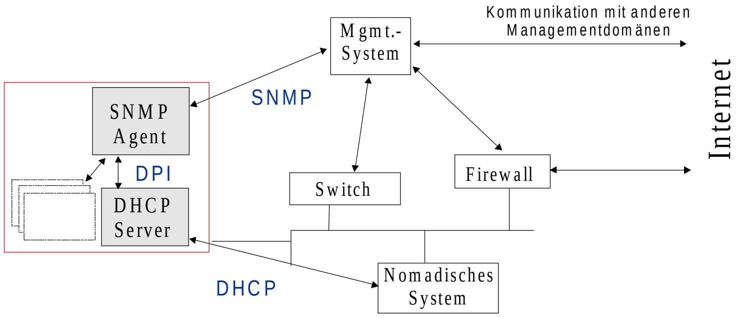
Implementierungen von DHCP-Servern erlauben meist eine gewisse Mindestmenge an automatisiertem Management, die Verwirklichung der vorher genannten Szenarien ist jedoch nicht möglich.

Bemerkung:

Eine Diskussion der Anforderungen an eine DHCP-MIB findet sich z.B. auch in der Archiven der Mailingliste der Working Group *dhc*. Dem Autor sind jedoch keine Implementierungen bekannt.

Modulare SNMP-Agenten

- **Problem: Nur ein SNMP-Agent je Endsystem möglich**
- **Lösungen**
  - Zweiter Agent an nichtstandardisiertem Port, oder
  - Multiplex-Schnittstelle im “Hauptagenten”, Anschluß z.B. durch *Distributed Protocol Interface (DPI)* (RFC 1592)



Produkte

- **Anforderungen**
  - Stabilität, Performanz
  - Unterstützung flex. Konfigurationspolitiken, heterogener Systeme
  - Dynamic-DNS, integriertes Management (SNMP), Interserver-Kommunikation, kommende Standards (z.B. DHCPv6, IPv6)
- **Server**
  - Alle wichtigen BS (z.B. NT-Server, HP-UX 10, AIX, Solaris)
  - Dritthersteller (z.B. JOIN, FTP OnNet, American Internet)
  - ISC, WIDE, CMU
- **Clients**
  - Alle wichtigen Client-BS (z.B. Win 95/NT, OS/2, HP-UX 10, AIX 4, Solaris, Linux)
  - NC-Clients
  - Peripheriegeräte (z.B. Drucker)

Stephen Heilbronner

MNM TEAM

13

Der Markt für DHCP-Server und -Client-Software ist durch eine zunehmende Vielfalt gekennzeichnet. Das Aufkommen nomadischer Endsysteme, Internet-Zugang via Modem und ISP sowie die Unterstützung von Internet-Standards durch alle Betriebssystemhersteller haben den Markt deutlich erweitert. Er ist durch häufige Veränderungen in bezug auf die Möglichkeiten und Flexibilität der Produkte gekennzeichnet, deswegen kann hier auch wegen der gebotenen Kürze auf Merkmale einzelner Produkte nicht eingegangen werden. Bei einer Auswahl sind jedoch insbesondere folgende Merkmale zu beachten, um den langfristigen Auswirkungen der Entscheidung Rechnung zu tragen:

•Performanz, Stabilität und Qualität der Implementierung

•Politik des Herstellers bzgl. der Unterstützung heterogener Endsysteme

•Interoperabilität mit anderen Infrastrukturkomponenten (z.B. Dynamic DNS)

•Standardisierte Managementschnittstellen (SNMP-MIB, GUI, Konfigurations-DB)

•Unterstützung von Ausfallsicherheit durch redundante Server

•Interserver-Kommunikation

•Unterstützung nomadischer Systeme

•Parametrisierbarkeit bzgl.

*Client-Charakteristiken

*Anschlußort

Eine aktuelle Liste von Produkten findet sich [Wob 97].

Ausblick und Referenzen

- **“Dynamische” Netze**
- **Network Computing**
- **Heterogene DV-Landschaft**
- **Drahtlose Netze**
- **NCs**
- **Neue Management-Standards: DHCP/DNS**
- **Migration zu IPv6 (DHCPv6)**
- **Referenzen:**
  - DHCP: **http://www.bucknell.edu/~droms/dhcp**
  - DHCP-FAQ: **http://web.syr.edu/~jmwobus/comfaqs/dhcp.faq.html**
  - Überblick: **http://nws.cc.emory.edu/WebStaff/Alan/Net-Man/Computing/DHCP**

Stephen Heilbronner MNM TEAM

14

Zusammenfassung und Ausblick

Der Einsatz von DHCP in PC-basierten Nutzen ist aus Effizienzgesichtspunkten schon fast ein Muß geworden. Soll jedoch Nomadic Computing in größeren Netzen wirklich automatisiert durchgeführt werden können, und soll die Entwicklung hin zu neuen DV-Versorgungstrukturen wie dem Network Computing unter Administrationsgesichtspunkten tatsächlich gangbar sein, so ist die Einführung integrierten Managements für entscheidende Infrastrukturkompenenten wie DHCP- und DNS-Server sowie Switches, Routern und Firewalls unabdingbar. Bei der Auswahl entsprechender Produkte sind offensichtlich neben den Möglichkeiten zum integrierten Management (aufgrund der fehlenden Standards stets nur schlecht gegeben) insbesondere die Politik des Herstellers in Bezug auf heterogene Client-Systeme und die Unterstützung kommender und offener Standards zu berücksichtigen.

Referenzen:

[Come 95] Douglas Comer, *Internetworking with TCP/IP Vol. I*, 1995, Prentice Hall

[Dobk 97] Alan Dobkin, *Net-Man’s Hotlist of Useful Sites - NC - DHCP Resources*, http://nws.cc.emory.edu/WebStaff/Alan/Net-Man/Computing/DHCP

[Drom 97] Richard Droms, *DHCP - Dynamic Host Configuration Protocol*, http://www.bucknell.edu/~droms/dhcp

[Rose 94] Marshall T. Rose, *The Simple Book*, 1994, Prentice Hall

[Wob 97] John Wobus, *DHCP Frequently Asked Questions*, http://web.syr.edu/~jmwobus/comfaqs/dhcp.faq.html

Danksagung:

Der Autor dankt den Mitgliedern des Münchner Netzmanagement Teams für konstruktive Vorschläge zu früheren Versionen dieses Beitrags. Das MNM Team ist eine Gruppe von