ComConsult Research

Der Netzwerk Insider

April 2010

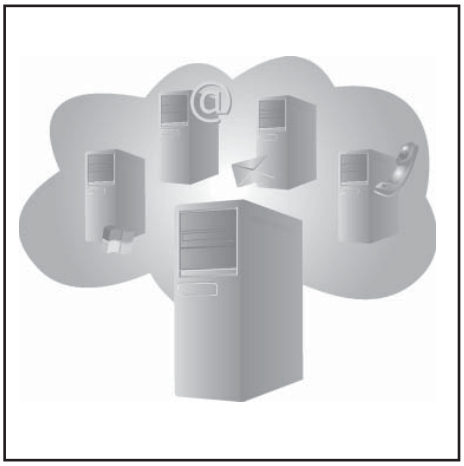
Systematische Weiterbildung für Netzwerk- und IT-Professionals

Schwerpunktthema

Virtualisierung: Virtual Desktop Infrastructure - steht das Rechenzentrum vor dem Kollaps?

von Dipl.-Inform. Matthias Egerland, Jonas Goede

Nach der erfolgreichen Virtualisierung des Serverumfelds und den damit verbundenen Konsolidierungsvorteilen steht nun in vielen Unternehmen die Virtualisierung der Client-Seite an. Auch hier locken eine flexiblere, einfachere Administration, mehr Energieeffizienz und ein höherer Sicherheitsgrad über die zentralisierten Daten. Doch welche Anforderungen stehen dem im Rechenzentrum gegenüber? Müssen die Rechenzentren von morgen einem völlig anderen Design unterliegen, um die Ansprüche einer Virtual Desktop Infrastructure (VDI) bedienen zu können?



Dieser Artikel analysiert den Übertragungsweg der virtualisierten Desktops in Richtung Clients und beleuchtet den architektonischen Unterschied der marktgängigen Desktop-Übertragungsprotokolle RDP, ICA und PCoIP. Daraus werden die Anforderungen an die Rechenzentrumsinfrastruktur abgeleitet.

weiter auf Seite 20

Zweitthema

IP Version 6 - das Internet der nächsten Generation (Teil 2)

von Dipl.-Inform. Petra Borowka-Gatzweiler

3. Autokonfiguration, DNS und DHCP

3.1 Autokonfiguration

Aktuell fließt immer noch ein erheblicher Aufwand in die statische oder automatische Konfiguration von IP-Endgeräten / IP Hosts (IP-Adresse, Maske, Default Gateway und weitere Optionen). Um diesen Betriebsaufwand für IPv6 zu reduzieren, wurden Mechanismen festgelegt, die eine Autokonfiguration der Endgeräte erlauben. Die explizite Konfiguration von IP-Adressen und Router-Einträgen in End-geräten sollen künftig entfallen - diesen Job regelt das IPv6-Protokoll dynamisch und selbstlernend: Bei der Autokonfiguration wird nach dem Booten von IP dynamisch eine Link-lokale Adresse festgelegt, die netzweit eindeutig, aber nicht fix im Endgerät konfiguriert ist. Darüber hinaus werden weitere für die Kommunikationsfähigkeit erforderliche Parameter wie „nächster Router“, MTU, Hop Limit etc. in Erfahrung gebracht. Die IPv6 Standardisierung bezeichnet Endgeräte / IP Hosts als „Station“. Dieser Artikel übernimmt im nachfolgenden Text diese Diktion.

weiter auf Seite 12

Aktueller Kongress

ComConsult IT-Sicherheits-Forum 2010

ab Seite 6

Geleit

Der Wechsel auf IPv6 muss jetzt starten!

ab Seite 2

Kennenlern-Aktion

ComConsult-Study.tv bis zum 15.04.2010

auf Seite 19

Zum Geleit

Der Wechsel auf IPv6 muss jetzt starten!

Die Diskussion über IPv6 ist jetzt fast 10 Jahre alt. Genauso alt sind die Prognosen, wann der IPv4-Adressraum so langsam ausgehen wird. Tatsache ist, dass einige der Megatrends der letzten Jahre erheblichen Einfluss auf diese Entwicklung haben:

- Die Anzahl mobiler Endgeräte, die eine fast permanente Adresse benötigen, explodiert. Die aktuelle Diskussion über das Apple iPad kontra HP Slade und den Bedarf für einen neuen Typ von Endgerät ist das perfekte Beispiel dafür

- Die Zahl der Anbieter für Cloud Computing und Software as a Service nimmt immer schneller zu. Neue Service-Infrastrukturen im Web entstehen und müssen ggf. stärker als bisher eingebunden werden

- Die Anzahl der Geräte in den Unternehmen, die in permanenten Verbindungen mit der Außenwelt stehen, nimmt genauso explosiv zu wie die der mobilen Endgeräte im Konsumermarkt, Unified Communications und Collaborations lassen grüßen

- Wussten Sie, dass der PKW der Zukunft mindestens 20 IP-Adressen benötigt?

Darüber hinaus gibt es auch eine Reihe von direkten Argumenten auf der Unternehmensseite, um nicht länger mit dem Einstieg in IPv6 zu warten:

- Auf die meisten Unternehmen kommt im Rahmen dieser Entwicklung eine schnell steigende Zahl von mobilen Endgeräten zu. Je später der Wechsel auf IPv6 erfolgt, desto aufwendiger wird der Umstieg

- Neue Installationen größerer Gerätemengen sollten am besten jetzt in IPv6 erfolgen

- Ab 2011 werden die ersten Service-Anbieter im Web nur noch über IPv6 erreichbar sein, ein Dual-Stack wird dann nicht mehr möglich sein. Betrachtet man die rapide Ausbreitung einiger neuer Web 2.0 Dienste, dann muss man in Betracht ziehen, dass ihr Unternehmen ggf mit diesen Diensten arbeiten will. Damit entsteht bereits der erste Parallelbetrieb mindestens im Router / in der Firewall für ihr Unternehmen

- Für viele Unternehmen steht der Wechsel auf Windows 7 auf der Projektliste. Eigentlich der perfekte Zeitpunkt, um wirtschaftlich und mit optimalem Aufwand zu wechseln. Ansonsten packen sie genau diese Geräte in ein bis zwei Jahren schon wieder an, also besser jetzt sofort

- Der Umstieg wird mindestens für die größeren Unternehmen Jahre erfordern. Zum einen ist eine nicht zu unterschätzende Lernphase für die Betreiber erforderlich, IPv6 ist deutlich mehr als nur ein Adresswechsel. Zum anderen gibt es eine Reihe von Geräten in den Unternehmen, die sich vermutlich nicht oder nur schwer migrieren lassen. Dafür müssen Konzepte ausgearbeitet werden, ein Test ist unvermeidbar

- IPv6 kann das gesamte Sicherheits-Szenario verändern. Zum einen sind Firewalls und Router direkt betroffen, zum anderen erhält mit IPv6 der Aspekt der sicheren Peer-to-Peer-Verbindung eine gewisse Bedeutung. Viele der bestehenden Konzepte, Angriffsmuster und Abwehrverfahren müssen komplett neu durchdacht werden.

Fasst man die Situation der Unternehmen nach diesen Ausführungen zusammen, dann gilt:

1. Der Wechsel nach IPv6 ist unvermeidbar

2. Er ist komplex und wird in der Regel unterschätzt

3. Er wird in den meisten Fällen zwischen 1 und 3 Jahren dauern

Betrachtet man angesichts dieser Aussagen die Entwicklung im Internet und die zunehmende Knappheit der IPv4-Adressen, das massive Umstellen in China, Japan und auch in den USA addiert den Druck der EU auf dieses Thema, dann wird klar, dass der Zeitpunkt zum Start dieses Projekts für die meisten Unternehmen jetzt gekommen ist. Wer jetzt noch wartet, handelt mehr als fahrlässig.

So schön, so gut. Aber IPv6 ist weit mehr als der simple Austausch einer IPv4-Adresse durch eine neue IPv6-Adresse. Hinter IPv6 steckte in völlig neues Konzept von Netzwerk. Dies betrifft viele wichtige Bereiche unserer Netzwerke, darunter vor allem auch DNS und DHCP.

Wer also jetzt mit der Planung beginnt, der läuft auf eine Reihe von Kernfragen. Wir diskutieren diese auf unserem Netzwerk-Redesign Forum 2010, sowohl in einem Vortrag von Frau Borowka als auch in einem ganztägigen Workshop von Herrn Flüs. Eine einmale Chance, schnell und kompakt auf den aktuellen Stand der Diskussion zu kommen. Als Vorgeschmack auf das Forum sollen die folgenden Fragen dienen:

- Ist IPv6 wirklich ausgereift?
- Stateless kontra Stateful, was ist der bessere Weg?
- Ist Autokonfiguration sinnvoll, kann auf DHCP ganz verzichtet werden?
- Wie wird DNS integriert?
- Wie erfolgen Adresswechsel?
- Was bedeutet IPv6 für Firewalls und Application Level Gateways?
- Was passiert mit NAT?
- Wie sehen Migrations-Konzepte aus?
- Wo sollen wir beginnen?

K.O.-Kriterium wird für die meisten Unternehmen die Frage sein, ob IPv6 ausgereift genug ist. Die Antwort ist schwierig. Für die Massenprodukte ist sie mit einem klaren ja sehr positiv. Windows 7 ist ein typisches Beispiel. Aber dem stehen jede Menge von Sonderprodukten gegenüber, zum Beispiel Fertigungs-Steuerungen, Zugangskontrollen, Videoüberwachungen, Spezial-Produkte der Automatisierungstechnik, alte Geräte im allgemeinen. Aus der Liste ist sofort zu entnehmen, dass kein Unternehmen an einem Test vorbei kommen wird. Der wird in der Regel schon deshalb erforderlich, weil Implementierungs-Varianten verglichen werden müssen und das Betriebspersonal sich einarbeiten muss. IPv6 ist sehr umfangreich und beinhaltet viele Optionen und auch noch offene Bereiche wie den von Mobile IPv6. Die Einarbeitung wird Zeit kosten.

Zweitthema

IP Version 6 - das Internet der nächsten Generation (Teil 2)

Fortsetzung von Seite 1

Dipl.-Inform. Petra Borowka-Gatzweiler leitet das Planungsbüro UBN und gehört zu den führenden deutschen Beratern für Kommunikationstechnik. Sie verfügt über langjährige erfolgreiche Praxiserfahrung bei der Planung und Realisierung von Netzwerk-Lösungen und ist seit vielen Jahren Referentin der ComConsult Akademie. Ihre Kenntnisse, internationale Veröffentlichungen, Arbeiten und Praxisorientierung sowie herstellerunabhängige Position sind international anerkannt.

Autokonfiguration wird über die so genannte „Nachbarerkennung“ implementiert. Dies hat folgende Vorteile:

- **Leichte Änderbarkeit,** indem die Station bei einer Adressänderung (z.B. neue Adapterkarte) ein so genanntes Nachbar Update als Multicast an alle Hosts / Knoten und Router sendet.
- **Höhere Effektivität:** Den intervallmäßig gesendeten Router Updates (Advertisements) kann eine Station alle erforderlichen Konfigurationis-Parameter entnehmen (Netzteil der Adresse, Präfixe, MTU).
- **Sicherheit:** Der Router wird automatisch gefunden, der ARP Request an den Router entfällt. Fehlen ein oder mehrere Präfixe im Router Advertisement, so kann die Station nicht direkt kommunizieren und muss den Router für die Kommunikation benutzen (indirect Routing).
- **Fehlertoleranz:** Endgeräte können den für sie zuständigen Router auf Erreichbarkeit prüfen und im Fehlerfall einen Backup Router finden.

Die **Nachbarerkennung** beinhaltet neun Funktionen / Dienste, die nachfolgend kurz erläutert werden.

1. **Router Discovery (NDP):** Die Station wartet auf eines der periodisch gesendeten Router Advertisements oder macht sich mit dem Neighbor Discovery Protokoll auf die Suche d.h. sendet eine **Router Solicitation Nachricht**. So „findet“ sie alle Router, die am lokalen Link angebunden sind und baut eine Liste von Default Routern auf. Das NDP basiert auf ICMPv6. Eine Blockierung aller ICMPv6 Pakete (analog zur heutigen Praxis, alle ICMPv4 Pakete auszufiltern) wird daher im Normalfall nicht praktikabel sein.
2. **Präfix Discovery:** Die Station lernt die Adress-Präfixe, die festlegen, welche Adressen Link-lokal (im selben Subnetz) oder über einen Router anzusprechen sind. Hierzu wertet sie ein Router Advertisement aus oder fordert per Router Solicitation eines an.
3. **Parameter Discovery:** Über Warten / Anfordern werden die notwendigen IP-Parameter wie MTU oder Hop Limit gelernt.
4. **Adress-Autokonfiguration:** Wird nicht automatisch die MAC-Adresse als Hostadresse (Interface-Adresse) verwendet, so kann eine Adresse angefordert werden. Hierfür spricht die Station z.B. einen DHCP Server an, der nach dem bekannten Request/Response Protokoll dem Endgerät seine Adresse sendet.
5. **Next Hop Bestimmung:** Anhand der gelernten Präfixe erkennt die Station, für welche Zieladressen sie einen Router ansprechen muss. Diesen wählt sie aus der Default Router Liste aus. Die entsprechende Router-IP-Adresse speichert sie in einem Cache.
6. **Adress-Resolution:** Ein IP Host kann die Link-Adresse (im LAN: MAC-Adresse) einer Peer Station im selben Subnetz mit der sogenannten Neighbor Solicitation anfordern und somit lernen (Auswerten des Neighbor Advertisement, das als Antwort gesendet wird). Die Adress-Resolution wird durch das NDP geleistet, welches das ARP Protokoll der IPv4-Welt ablöst.
7. **Entdecken der Nichterreichbarkeit:** Durch Senden einer Neighbor Solicitation Anfrage kann eine Station überprüfen, ob die Zielstation (im selben Subnetz) oder der Zielrouter noch erreichbar sind.
8. **Entdecken einer Adress-Duplizierung (DAD):** Über eine Neighbor Solicitation Nachricht kann abgefragt werden, ob die eigene autokonfigurierte Adresse schon vorhanden ist.
9. **Redirect:** Ein Router kann einer Station mit einer Redirect Nachricht die Adresse eines anderen Routers mitteilen, der für eine bestimmte Zielstation (=Zieladresse) besser geeignet ist. Ein Redirect kann der angesprochenen Station auch mitteilen, dass die Adresse des Zielpartners Link-lokal ist und demzufolge gar kein Router zu benutzen ist.

Für die Nachbarerkennung und alle damit zusammenhängenden Funktionen werden verschiedene **Caches** und **Listen** aufgebaut, die für die weitere Kommunikation benutzt und gepflegt werden.

Im **Nachbar-Cache** tragen Stationen die Link-lokalen Adressen ein, mit denen zuletzt kommuniziert wurde. Hierzu gehören Flags für Typ (Station, Router), Erreichbarkeit, Status, Anzahl unbeantworteter Anfragen, Timer für die nächste Überprüfung etc. Dieser Cache ist erkennbar aufwändiger (Speicher, CPU) als der unter IPv4 geführte ARP-Cache.

Im **Empfänger-Cache** tragen Stationen die Link-lokalen und globalen Adressen ein, mit denen zuletzt kommuniziert wurde. Diese Adressen werden, soweit nötig, auf den nächsten Link-lokalen Router gemappt. Ebenso werden Redirect Nachrichten in den Cache eingepflegt. Zwischen Empfänger-Cache und Nachbar-Cache gibt es einen Abgleich.

In die **Präfix-Liste** werden alle gelernten Präfixe ein getragen, anhand derer Adressen als Link-lokal oder global klassifiziert werden.

IP Version 6 - das Internet der nächsten Generation (Teil 2)

In die **Router-Liste** trägt eine Station analog die gelernten Adressen der Link-lokalen Router ein, die die sie zur Kommunikation benutzen kann. Zu diesen Eintragungen werden Erreichbarkeits-Informationen aus dem Nachbar-Cache in der Liste mitgeführt.

Auf der Basis der Nachbarerkennungs-Funktionen / -Dienste erfolgt die Autokonfiguration in insgesamt neun Schritten:

1. **Automatische Konfiguration** der eigenen IP-Adresse, alternativ über zustandsfreie / zustands-abhängige (stateful / stateless) Konfigurations-Anforderung: Die **zustandsfreie** d.h. **Autokonfiguration** erfolgt durch Auswerten oder Anfordern von Router Advertisements, d.h. Empfang/Senden der Multicast-Gruppe FF02::1 (alle Knoten, alle Router) und Kombination mit der eigenen MAC-Adresse. Zur initialen Kommunikation mit dem Router weist sich der IP Host eine Link-lokale Adresse zu, die z.B. aus der Hardware-Adresse (d.h. MAC Adresse) berechnet werden kann, sofern ein Ethernet NIC vorhanden ist. Diese Konfiguration wird als **stateless** bezeichnet, weil praktisch nirgendwo „Buch geführt wird“, welches Endgerät sich welche Adresse gegeben hat. Alternativ zur Autokonfiguration kann die Station als zustandsabhängige Konfiguration eine Host-Adresse über DHCP anfordern (siehe Unterpunkt 3.2)

2. **Überprüfung** der Adresse auf **Eindeutigkeit** durch Abfrage / Senden einer Solicitation Nachricht; jeder IP Host muss die Duplicate Adress Detection (DAD) durchführen, wenn er sich per Autokonfiguration eine IP Adresse ausgewählt hat. Die DAD findet automatisch mittels NDP statt ohne dass der Benutzer hier aktiv werden muss.

3. **Lernen der Link-lokalen Router** bzw. ihrer IP-Adressen über die Router Discovery

4. **Lernen der Präfixe** der Link-lokalen Stationen (des eigenen Subnetzes) über die Präfix Discovery; Router können bei der Präfix-Mitteilung endliche Gültigkeitszeiten mitteilen (valid lifetime, preferred lifetime). Innerhalb der Valid Lifetime darf der IP Host das mitgeteilte Präfix zur Kommunikation verwenden, innerhalb der Preferred Lifetime soll er es einem Präfix vorziehen, dessen Lifetime abgelaufen ist. Die Verlängerung der Gültigkeitszeiten erfolgt automatisch durch die Router Advertisements.

5. **Erfragen der Link-lokalen MTU und des Hop Limit** über die Parameter Discovery

6. **Lernen der Link-Adressen von IPv6-Partnern**, die Link-lokal sind und deren IPv6-Adresse bekannt ist, über die Adress-Resolution

7. **Lernen des nächsten Routers** für nicht Link-lokale Zielpartner über die Präfix Discovery und Next Hop Bestimmung

8. **Überprüfen der Erreichbarkeit** gewünschter Zielpartner über die Neighbor Solicitation

9. **Auswerten von Redirect** Nachrichten und somit Optimierung der Kommunikationswege.

3.2 DHCP und DNS

DHCP

Autokonfiguration macht die IP Adresse typischerweise abhängig von der MAC-Adresse sprich NIC Hardware. Aus Gründen der Flexibilität und Hardware-Unabhängigkeit (weltweit überall dieselbe IPv6 Adresse, auch bei Nutzung unterschiedlicher Zugangstechnologien wie WLAN, WiMax, Ethernet) kann dies unerwünscht sein. Ein weiterer Nachteil der Autokonfiguration ist die Nutzung / Lieferung der Hardware (MAC) Adresse anstelle von sprechenden Namen für PTR bei reverse DNS. Eine flexible Alternative für beide Probleme bietet hier der Einsatz von DHCPv6.

Anstelle von Autokonfiguration kann die Station eine Host-Adresse über DHCP anfordern: Diese **zustandsabhängige Konfiguration** findet statt, wenn kein Router vorhanden ist oder das Router Advertisement besagt, dass zustandsfreie Autokonfiguration aus Sicherheitsgründen nicht erwünscht ist. In diesem Fall wird über den Multicast FF02::1:0 der nächste DHCP Server gefunden und eine komplette Adresse von diesem Server angefordert. Diese Konfiguration unterscheidet sich prinzipiell von der stateless Autokonfiguration: Sie wird als **stateful** bezeichnet, weil der DHCP Server darüber „Buch führt“, welchem Endgerät er welche Adresse gegeben hat.

Die Autokonfiguration ist zwar wunderschön, liefert dem Endgerät aber keine Informationen über Hostnamen, Domänennamen, DNS Server, NTP Server, TFTP Server etc. Ein Hauptproblem liegt darin, dass das Endgerät bei der Autokonfiguration keine DNS Server Adresse lernt. Diese Adresse mag zwar einigermaßen stabil sein, aber das Endgerät hat trotzdem ein Problem, den DNS Server respektive seine korrekte IP Adresse zu finden und zu konfigurieren. Zur Abhilfe für dieses Problem wurden einige Lösungen vorgeschlagen, darunter Multicast, Anycast und: der Einsatz eines DHCPv6 Servers.

Daher kann trotz stateless Autokonfiguration zusätzlich ein DHCPv6 Server zum Einsatz kommen. Das NDP (Neighbor Discovery Protokoll) kann sogar explizit auf die Möglichkeit einer weitergehenden Konfiguration durch DHCPv6 verweisen. Der DHCPv6 Server liefert den Endgeräten in diesem Fall die gewünschten Zusatz-Informationen, kümmert sich aber nicht um die Adressvergabe. Die Kombination von Autokonfiguration mit DHCPv6 wird als „**stateless DHCPv6**“ bezeichnet (RFC 3736).

DNS

Fällt es dem Otto-Normal-Verbraucher schon schwer, sich IPv4 Adressen zu merken, die dezimal codiert und nur 4 Byte lang sind, so hat er mit IPv6 bei einer Adresslänge von 16 Byte und Hexcodierung ganz verloren. Für Nutzer und Betreiber wird es daher noch wichtiger, DNS als funktionierendes Namenssystem zur Verfügung zu haben.

Der DNS Dienst

DNS besteht aus einer Reihe von Funktionen und Diensten, die ein zuverlässiges Mapping beziehungsweise eine Übersetzung von Namen (FQDNs) in Adressen (IPv4, IPv6) und vice versa leisten. Zusätzlich bietet DNS Funktionen zur Unterstützung spezieller Anwendungen (MX für das Routen von E-Mail, ISATAP, NAT-PT).

Die Implementierung von DNS läuft auf Namensservern (Master Server, Slave Server, verteilte Namens-Datenbank), die untereinander und mit den anfragenden Clients kommunizieren. Der DNS-Agent im Client heißt Resolver. Seine Anfragen (Query Requests) lauten entweder auf Forward oder Reverse Domänennamen-Suche. Forward Lookup übersetzt den angefragten Namen in eine IP Adresse, Reverse Lookup liefert einen Namen für eine angefragte IP Adresse. Letzteres ist insbesondere für Management-, Sicherheits- und Debugging Tools wichtig.

Zur Nutzung von DNS für IPv6 wurde in RFC 3596 als Ressourcentyp (RR) ein Quad-A Record (AAAA) für DNS-Abfragen definiert. Der AAAA Record löst genau wie der A Record einen Namen in eine IPv6 Adresse auf (Forward Lookup). Die Auflösung einer IPv6 Adresse in einen Namen (reverse Lookup) nutzt nach wie vor den PTR Record Typ, der ebenfalls neu definiert wurde. Allerdings ist die Reverse Domäne

Schwerpunktthema

Virtualisierung: Virtual Desktop Infrastructure - steht das Rechenzentrum vor dem Kollaps?

Dipl.-Inform. Matthias Egerland hat an der RWTH Aachen Informatik studiert und ist seit 2005 Mitarbeiter der ComConsult Beratung und Planung GmbH. Er ist Leiter des Competence Centers Virtuelle IT und arbeitet als Berater in den Competence Centern IT-Sicherheit und Netze. Neben den Schwerpunkten Desktop-, Server- und Infrastruktur-Virtualisierung beschäftigt sich Herr Egerland insbesondere mit der Sicherheit in virtualisierten Umgebungen.

Jonas Goede ist Berater bei der ComConsult Beratung und Planung GmbH. Dort ist er in den Bereichen Virtuelle IT und Data Center tätig. Neben diesbezüglichen Praxiserfahrungen ist er spezialisiert auf die Planung und Durchführung von Testszenarien im Bereich Virtual Desktop Infrastructure Lösungen.

Fortsetzung von Seite 1

1. Einführung in die Desktopvirtualisierung

Nachdem in den letzten Jahren viele Firmen und Anwender die Servervirtualisierung erfolgreich eingesetzt haben, verstärkt sich zunehmend der Trend, auch andere Bereiche der IT in den Fokus der Virtualisierung zu nehmen. Bei der Desktopvirtualisierung sollen bekannte Konzepte der Virtualisierung von Servern und Speicher, auf Arbeitsplatzrechner (Clients) übertragen werden. Arbeitsplatzrechner werden traditionell mit lokal installiertem Betriebssystem und lokal installierten Anwendungen betrieben. Oftmals haben große Teile der Anwender in einer Firma neben dem identischen Betriebssystem auch noch viele ähnliche Anwendungen im Einsatz. Hierin liegt das Optimierungspotential: Zusammenfassen gleichartiger Bestandteile zu einer gemeinsam genutzten Ressource. Da aber Arbeitsplatzrechner (Desktops) - je nach Arbeitsanforderung - höchst individuell gestaltet sein können, liegt in der Wahrung dieser Einzigartigkeit die zusätzliche Herausforderung der Desktopvirtualisierung.

1.1 Komponenten einer Virtual Desktop Infrastructure

Der Grundaufbau einer Virtual Desktop Infrastructure ist bei allen marktüblichen Lösungen gleich. Auf der einen Seite stehen Server, die für den Betrieb der virtuellen Desktop Hard- und Software sorgen, die so genannte „Hosting-Infrastruktur“. Auf der anderen Seite stellen Server die Inhalte (Betriebssystem und Anwendungs-Software) den virtuellen Desktops dynamisch bereit. Daneben gibt es noch Komponenten, die den Zugriff auf die virtuellen und physischen Maschinen steuern. Auf diesen Servern laufen spezielle Tools, die für vorbereitende Maßnahmen und den laufenden Betrieb notwendig sind. Außerdem ermöglichen Konsolen und Managementwerkzeuge in zentralen Bereichen die Administration der Komponenten.

Für das grundlegende Hosting von virtuellen Desktops kann ein sogenannter Hypervisor eingesetzt werden, wie er auch aus der Servervirtualisierung bekannt ist. Jeder virtuelle Desktop arbeitet damit genau wie jede andere virtuelle Maschine in einer für ihn abgeschlossenen Umgebung, ohne dabei in Konflikt mit den Hardwarezugriffen der anderen virtuellen Maschinen zu geraten.

Um die virtuellen Desktops, die auf dem Hypervisor laufen, dynamisch mit Software zu versorgen, wird ein so genannter Provisionierungsserver eingesetzt. Dieser sorgt für die Bereitstellung des Betriebssystems und der Applikationen, indem er diese aus vorkonfektionierten Images bezieht. Eine Imagedatei dient dann als Softwarebasis für eine Vielzahl von virtuell laufenden Desktops auf dem Hypervisor.

Wenn ein Endgerät Zugriff auf einen solchen virtuellen Desktop benötigt, stellt es eine Anfrage an einen speziellen Server, den so genannten „Connection Broker“. Dieser Server fragt seinerseits beim Hypervisor nach, ob eine passende virtuelle Maschine für diesen Zweck zur Verfügung gestellt werden kann. Ist eine entsprechende VM vorrätig, stellt der Hypervisor eine direkte Verbindung zwischen anfragendem Endgerät und der virtuellen Maschine her, auf die dann der Provisionierungsserver das passende Betriebssystem-Image lädt. Ist eine solche VM nicht verfügbar, veranlasst der Connection Broker den Hypervisor, eine solche zu starten. Die Übertragung zwischen Client und virtuellem Desktop wird anschließend über spezielle Protokolle (RDP, ICA, PCoIP) abgewickelt und läuft ohne die Zwischenschaltung des Connection Brokers. Abbildung 1 zeigt die schematische Darstellung einer Virtual Desktop Infrastructure.

1.2 Hardwareszenarien

Die Anforderungen auf Nutzerseite sowie die Implementierungsvariante haben Auswirkungen auf die Hardware sowohl Server- als auch Endgeräte-seitig.

Bei ThinClient-Lösungen greift eine leistungsreduzierte Hardware auf die Server der Virtual Desktop Infrastruktur zu. Diese

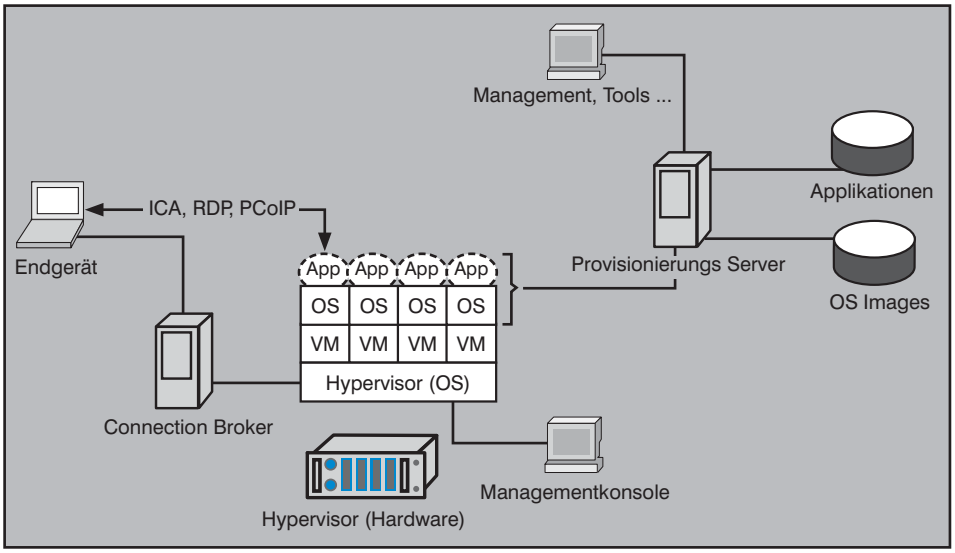


Abbildung 1: Schematische Darstellung einer Virtual Desktop Infrastructure

senden dann meist nur den Bildschirminhalt an eben diesen ThinClient, welcher wiederum die Benutzereingaben zurückgibt. Alternativ können je nach Hardwareausstattung auch Software/Betriebssystem Pakete an diese Geräte gestreamt werden, um sie lokal auf dem Desktop auszuführen und damit die Server im Rechenzentrum zu entlasten und mobiles Arbeiten zu ermöglichen (s. Modelle zur Desktopbereitstellung in Abschnitt 1.3).

Anstelle von ThinClients können BladePCs eingesetzt werden, die über eine Bildschirm- und Eingabe-Verlängerung mit dem Benutzer verbunden sind. Ein BladePC wird im Rechenzentrum auf eigener Hardware betrieben und fungiert dort als eigenständige Maschine. Somit ist diese Lösung physikalisch unabhängig von anderen Systemen und kann gezielt für einen Benutzer seine komplette Rechenleistung zur Verfügung stellen. Diese Art der Desktopbereitstellung wird oft dann gewählt, wenn ein User (oder eine kleine Gruppe von Usern) im Gegensatz zum überwiegenden Anteil der sonstigen Benutzer eine außergewöhnlich hohe Rechenleistung für sich allein beansprucht. Hier wären z.B. CAD Arbeitsplätze zu nennen, die mit hohen Anforderungen an die Grafikleistungen alle „normalen“ Arbeitsplätze übersteigen. Ohne weitere Mechanismen findet eine Virtualisierung im eigentlichen Sinne somit nicht statt. Der Desktop-PC wurde lediglich in Form des Blade-PCs in das Rechenzentrum verlagert.

Im folgenden Abschnitt werden die verschiedenen Möglichkeiten aufgezeigt, diese Virtuellen Umgebungen mit dem Benutzer zu verbinden, sprich die Desktops bereitzustellen.

1.3 Modelle zur Desktopbereitstellung

Generell ist es bei allen Benutzertypen das vorrangige Ziel, den Desktop nicht mehr auf lokalen Maschinen zu betreiben, sondern den Betrieb ins zentrale Rechenzentrum zu verlagern. Welche Konzepte zur Virtualisierung dort eingesetzt werden und wie der Benutzer Zugriff auf seinen Desktop erhält, ist je nach Anforderung unterschiedlich lösbar.

Bei der Applikationsvirtualisierung – auch Anwendungs- oder Softwarevirtualisierung genannt, handelt es sich nicht um eine komplette Virtualisierung des Desktops. Es werden lediglich einzelne Anwendungen virtualisiert. Diese Software läuft dann entweder auf einem entfernten Server und kann dort von mehreren Clients gleichzeitig genutzt werden (Terminal Server). Alternativ erhält jeder Benutzer seine Anwendungen zur lokalen Ausführung per Netzwerkstream auf seinen Client. Hierbei kann entweder die gesamte Anwendung übertragen werden, oder nur der Teil der Software, der gerade genutzt wird. Bei der Komplettübertragung der Software entsteht zunächst zwar eine höhere Netzwerklast als bei einer Teilübertragung, jedoch kann die Applikation danach komplett ohne Netzwerkanbindung betrieben werden (Offline-Fähigkeit).

Ähnlich wird auch die Verbindung zu einem komplett virtualisierten Desktop bereitgestellt. Entweder erhält der Anwender einen Netzwerkstream mit einem (Teil)Paket zur lokalen Ausführung oder ihm wird nur der Bildschirminhalt übertragen und er sendet seinerseits die Benutzereingaben zurück. Je nach Methode muss das Endgerät des Benutzers unterschiedliche Fähigkeiten beherrschen. Reicht bei einer reinen Bildübertragung eine relativ geringe Rechenleistung aus, werden bei der Streaming-Methode dem Client wortwörtlich mehr Aufgaben „übertragen“. Abbildung 2 zeigt das Modell eines gestreamten Desktops.

Um neben der reinen Bildübertragung weitere Interaktionen zwischen Client und Server vornehmen zu können, spielt das Übertragungsprotokoll eine sehr große Rolle. Es muss beispielsweise zusätzlich für die Verbindung von Druckern mit PCs Methoden bereitstellen, damit diese Geräte nicht nur dem lokalen Gerät bekannt sind, sondern auch bis zur virtuellen Maschine „durchgereicht“ werden. Ähnlich verhält es sich z.B. bei USB Geräten. Der folgende Abschnitt gibt einen Einblick in die Leistungsfähigkeit solcher Protokolle.

1.4 Übertragungsprotokolle

1.4.1 Remote Desktop Protocol (RDP)

Das Remote Desktop Protocol (RDP) wurde von Microsoft mit dem Ziel entwickelt, die Grafikausgabe eines entfernten Computers auf dem lokalen Bildschirm darzustellen und so beispielsweise entfernte Server im Rechenzentrum zu administrieren. Mit fast jedem neuen Microsoft Desktop- oder Serverbetriebssystem wurde RDP weiterentwickelt und mit neuen

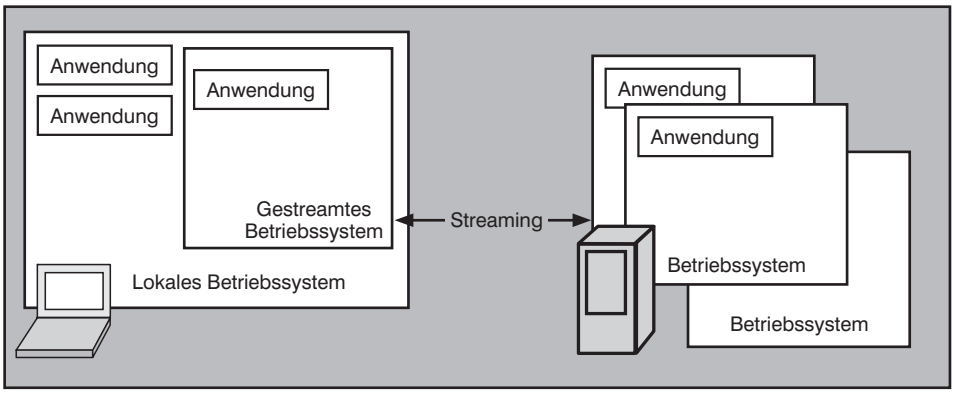


Abbildung 2: Modell Desktopstreaming