

Fernwartung über das Internet

Dipl. Ing. Xiaojun Tang

LyconSys GmbH&Co.KG Frankfurt am Main
11. Juni 2009

Zusammenfassung

Dieser Artikel beschreibt die Anbindung von Geräten über das Internet für Fernwartungs-, Fernüberwachungs- und M2M-Applikationen. In der Praxis treten durch dynamische IP Adressen und NAT einige Probleme auf, zu denen in diesem Artikel allgemein angewandte Lösungen beschrieben werden.

Abstract

This article explains the connection of devices over the Internet for remote control and M2M applications. In practice some pitfalls due to dynamic IP addresses and NAT are encountered and common solutions to them will be explained in the sequel.

1 Einleitung

Der Fernwartungs- und M2M-Markt wächst rasant. Maschinen bestimmen und melden autonom Wartungsintervalle, Mitarbeiter steuern Geräte und überwachen Prozesse über das Internet. Stationäre Test- und Prüfstände werden weltweit geteilt und damit optimal ausgelastet. Solche Fernwartungs-Lösungen sind heute nicht mehr teuer und rechnen sich durch entfallende Reisekosten, eingespartes Material und zentralisierte Wartung in vielen Fällen schnell. Aber bei der Internetanbindung treten dann oft Überraschungen auf: zwar sind alle Geräte im Internet miteinander vernetzt, aber bevor diese miteinander Verbindungen eingehen können, sind ein paar Hürden zu nehmen.

2 Dynamic IP und DynDNS

Die grundlegenden Probleme liegen im Internetprotokoll (IP) der Version 4, das nur einen Adressraum von 32 Bit vorsieht¹. Um dennoch mehr Teilnehmer ansprechen zu können, werden IP Adressen vom Internetprovider bei Bedarf verliehen (dynamic IP)². Wählt sich der Teilnehmer beim Provider ein, so bekommt er die IP Adresse zugewiesen.

¹Etwas 4 Milliarden. Dem stehen 7 Milliarden Menschen gegenüber und die Möglichkeit, dass jedes Gerät eine Verbindung zum Internet hat

²Der Spareffekt tritt heutzutage in den Hintergrund. Im Gegensatz zu Dialup-Verbindungen sind DSL Router und Internet Handys in der Regel immer online

Findet für eine gewisse Zeit (lease time) kein Traffic statt, so wird die IP Adresse wieder eingezogen und der Provider kann sie einem anderen Teilnehmer verleihen³.

Wie kann ein Teilnehmer gerufen werden, wenn dessen Adresse dynamisch zugeteilt wird und dem Anrufer unbekannt ist?

Eine Lösung dazu ist DynDNS. Dieser Dienst löst einen Namen in eine IP Adresse auf (wie ein Telefonbuch Namen in Nummern). Jedes Gerät kann sich dort mit seinem (eindeutigen) Namen registrieren. Bekommt der Teilnehmer eine IP Adresse vom Provider, meldet er sich bei DynDNS und teilt Namen und aktuelle Adresse mit.

Möchte ein Teilnehmer mit einem bestimmten Teilnehmer Kontakt aufnehmen, fragt er einfach DynDNS mit dem Namen des gewünschten Teilnehmers an und bekommt als Ergebnis dessen IP Adresse. Mit dieser Zieladresse kann dann der Teilnehmer direkt kontaktiert werden.

Weil der DynDNS-Server selbst eine statische IP Adresse hat, kann er jederzeit angerufen und befragt werden.

Ein DynDNS Client auf dem Gerät des Teilnehmers sorgt dafür, dass oben genannte Prozeduren automatisch im Hintergrund ablaufen und der DynDNS Dienst so unkompliziert zu nutzen ist wie statisches DNS.

3 NAT

In der Regel befinden sich die Teilnehmer in einem eigenen Firmen- oder Privatnetz hinter einer NAT (Network Address Translation). NAT wird benötigt, damit mehrere Teilnehmer "hinter der NAT" das Internet nutzen können, nach außen aber nur eine IP Adresse benötigen. Hinter der NAT erhalten die Teilnehmer private IP Adressen und die NAT bildet diese entsprechend auf die eine öffentliche IP Adresse ab. Ein weiterer Vorteil durch das "NATing" besteht darin, dass die privaten IP Adressen aus einem eigens dafür reservierten Bereich entstammen, die nicht durch das Internet geroutet werden. Aus diesem Grund kann man über das Internet nicht direkt zu einem Teilnehmer eine Verbindung aufbauen, weshalb manche Provider eine NAT vor den Teilnehmeranschluss setzen, um eingehenden (Spam-) Traffic zu vermeiden⁴. Für die Fernwartung oder M2M ist das aber ein großes Problem, denn genau dieses Punkt-zu-Punkt Szenario ist ja das benötigte! Möchte man also eine Verbindung zu einem Teilnehmer hinter einer NAT aufbauen, erreicht man in der Regel nur das Gerät welches das "NATing" durchführt. Für dieses Problem gibt es folgende Lösungen:

1. Der Teilnehmer hinter der NAT muss die Verbindung aufbauen. Dann sieht der angerufene Teilnehmer den NAT-Router mit der öffentlichen IP Adresse und für ihn sieht es so aus, als würde der rufende Teilnehmer der NAT-Router sein.
2. Auf dem NAT-Router wird ein Port-Fowarding eingerichtet. Dieses Forwarding koppelt einen bestimmten Port der öffentlichen IP Adresse beispielsweise an den HTTP Port eines Weberservers im lokalen Netz. Damit ist der HTTP Port auf diesem Rechner im Internet verfügbar.

³Die Strategie der Vergabe ist abhängig vom Provider

⁴Mobilfunkprovider machen teilweise davon Gebrauch, um die teure Luftschnittstelle zu entlasten

Wenn man keine Administratorrechte auf dem NAT-Router hat, etwa weil der Mobilfunkprovider das "NATing"durchführt, dann bleibt nur die erste Möglichkeit. Wegen der praktischen Relevanz betrachten wir im Folgenden nur diesen.

3.1 VPN Server

Eine Möglichkeit Geräte hinter einer NAT zu verbinden bietet der Aufbau eines VPN (Virtual Private Network), wofür ein VPN-Server benötigt wird. Dieser Server hat zweckmässigerweise eine fest IP Adresse, kann aber auch eine dynamische IP Adresse haben. Die Teilnehmer benötigen eine VPN Client Software, die zusammen mit der Serversoftware ein komplettes Subnetz tunnelt. Wählen sich die Teilnehmer bei dem VPN-Server ein und authentifizieren sich entsprechend, dann treten sie dem virtuellen Netz bei. Diese Lösung kommt beispielsweise in Firmen zum Einsatz, die Mitarbeiter im Aussendienst haben welche Zugriff auf das interne Firmennetz benötigen.

Die Vor- und Nachteile dieser Lösung sind:

- + VPN Services mit fester IP gibt es als fertige Dienstleistung
- + Es können viele Teilnehmer im gleichen Netz arbeiten, wie in einem Office-LAN
- Der gesamte Traffic geht über den VPN-Server, der daher hoch-verfügbar sein muss
- Es entstehen Kosten für die Bereitstellung des VPN-Server und in der Regel für das Datenvolumen
- Der Traffic immer über den VPN-Server, auch wenn sich die Verbindungspartner in unmittelbarer Nähe befinden. Steht der Server im Ausland, kann die Kommunikation sehr langsam werden.

3.2 Port Forwarding

In vielen Anwendungsfällen ist der gerufene Teilnehmer einer oder mehrere Rechner im Unternehmen (Zielrechner) mit dem die mobilen oder stationären Teilnehmer in Verbindung treten wollen, etwa um Messdaten oder Ereignisse zu melden. Darüber hinaus sind viele Dienste wie Email, Datei- oder Druckerdienste Client-/Server-basiert. Ein VPN wäre in diesem Fall überdimensioniert. Daher ist es ausreichend, dass der gerufene Rechner die Ports für die entsprechenden Dienste freischaltet. Auf dem NAT werden dann Routen zu den Dienst-Servern eingerichtet (Port Forwarding).

Die Vor- und Nachteile dieser Lösung sind:

- + Kein zusätzlicher Server/Dienst notwendig und damit verbundene Kosten
- + Die Verbindung zwischen den Teilnehmern ist direkt und ohne Umwege
- Es kann kein ganzes Netz getunnelt werden sondern nur einzelne Ports ⁵

⁵Maximal 65535-TCP/IP-Ports

- Der Zugriffsschutz (Access and Authentication) muss auf dem Endgerät gewährleistet werden

3.3 Port Forwarding mit Rendezvous-Server

Im vorangegangenen Abschnitt wird angenommen, dass die NAT vor dem Zielrechner konfigurierbar ist, damit die Route eingetragen werden kann. Wenn das nicht der Fall ist, dann wird ein Rendezvous-Server benötigt bei dem sich beide Teilnehmer einwählen. Dieser Rendezvous-Server muss natürlich von aussen über das Internet erreichbar sein. Der Rendezvous-Server übernimmt dann das Port-Forwarding in beide Richtungen. Diese Lösung kombiniert im wesentlichen die Nachteile der beiden vorangegangenen Ansätze, kann aber günstiger sein, wenn kein ganzes Netz getunnelt werden muss und der Rendezvous-Server selbst verwaltet werden soll. Bei geringer Teilnehmerzahl kann die Aufgabe von einem Embedded-Endgerät erledigt werden und es ist dann kein spezieller Server notwendig.

4 Authentifizierung

Jeder Server, der einen Dienst zur Verfügung stellt, muss mindestens einen Port für diesen Dienst öffnen. In Fernwartungs- bzw. M2M-Applikationen ist es natürlich nicht erwünscht, dass jeder Teilnehmer im Internet Zugriff auf diesen Port hat, sondern nur berechtigte Teilnehmer. Daher muss eine Authentifizierung⁶ und ggf. Datenverschlüsselung vorgesehen werden. Aktuelle VPN- oder Port-Forwarding Dienste bieten immer eine Form der Authentifizierung. In der Praxis verwendet man häufig eine asymmetrische Verschlüsselung (Zertifikat). Hierzu wird ein Privater und Öffentlicher Schlüssel erzeugt. Der Öffentliche Schlüssel wird dann im Server hinterlegt und mit dem Port, der den benötigten Dienst zu Verfügung stellt, verknüpft. Damit hat man erreicht, dass nur derjenige Teilnehmer mit dem passenden Privaten Schlüssel auf den Port zugreifen kann. Das Sperren eines Teilnehmers (z.B. weil ein Gerät durch Diebstahl entwendet wurde) erfolgt dann durch einfaches entfernen des Öffentlichen Schlüssels auf dem Server.

5 Fertige Lösungen

In der Praxis wird man sich auf fertige Lösungen stützen. Dabei lohnt sich ein Blick auf die Flexibilität der zur Auswahl stehenden Komponenten, denn oftmals wachsen Systeme mit den Ansprüchen der Kunden erst im Feld. Einige der Punkte, die bei der Auswahl des System entscheiden sein können, werden an dieser Stelle aufgeführt. Sie sind keinesfalls vollständig, können aber bei der ersten Orientierung helfen.

- Bei kleinen Systemen sollte ein Gerät wahlweise als Client, Server und Rendezvous-Server arbeiten können. Das erspart Einarbeitungs- und Wartungsaufwand, weil die gleiche Hardware alle Aufgaben übernehmen kann und kompatibilitätsprobleme vermieden werden

⁶Im einfachsten Fall Username und Passwort

- Der Lösungsanbieter sollte fertige, PC-basierte Server anbieten, falls die Anzahl der Klienten zu einem späteren Zeitpunkt wächst und ein dedizierter Server als Leitstelle, VPN- oder Rendezvous-Server benötigt wird
- Es sollten Strategien implementiert sein, um bei Strom- und Verbindungsunterbrechungen den betriebsfähigen Zustand automatisch wieder herzustellen
- Für den Einsatz in mobilen, batteriebetriebenen Umgebungen kann eine Überwachung der Umgebungsbedingungen wie Spannung und Temperatur sinnvoll sein
- Eine Zeitsteuerung (Alarm) kann die Leistungsaufnahme sinnvoll reduzieren. Es lohnt sich bei größeren Investitionen ein Blick auf folgende EU Verordnung zur Standby Leistungsaufnahme⁷
- Beim Einsatz von Highspeed Modems (UMTS/HSDPA/HSUPA oder EDGE) ist darauf zu achten, dass diese über USB oder Ethernet verbunden sind. Das gilt auch für integrierte Modems. Serielle Schnittstellen sind mit der Datenrate überfordert
- Die Gerätesoftware sollte modular erweiterbar sein. Im Idealfall existiert eine Programmierschnittstelle für das Fine-Tuning des Systems

6 Zusammenfassung

In diesem Artikel wurden die grundlegenden Probleme in der Fernwartungs- und M2M-Kommunikation aufgezeigt, wobei Eingangs IPv4 als Hauptursache für die dargestellte Komplexität angeführt wird. IPv6 wird in Zukunft die Probleme etwas variieren aber leider nicht vollständig lösen, weil aus Kompatibilitätsgründen eine Tendenz besteht, bei IPv4 bewährte Verfahren auch bei IPv6 anzuwenden. NAT ist ein Beispiel dafür. Glücklicherweise werden diese Probleme für Endkunden und Applikateure nicht sichtbar, wenn sich diese auf fertige, zugeschnittene Lösungen stützen. Das sollte Motivation und Anspruch der Hersteller sein, damit sich Fernwartungs- und M2M-Applikation aus der Nische für Experten heraus und in einen breiten Massenmarkt entwickeln können.

⁷VERORDNUNG (EG) Nr. 1275/2008 DER KOMMISSION vom 17. Dezember 2008