

IPcopv 1.3 und v1.4

Grundlagen zur Namensauflösung in Netzwerken

<i>Inhaltsverzeichnis</i>	1
<i>Grundsätzliches</i>	1
<i>Vorbereitung</i>	1
<i>Was ist das eigentlich, Namensauflösung und für was ist sie gut?</i>	2
<i>Grundlagen zur Namensauflösung bei NBT</i>	2
<i>Knotentypen</i>	3
<i>Grundlagen zur Namensauflösung bei TCP/IP</i>	3
<i>Namensauflösung unter Windows</i>	4
1. Beispiel, "ping DEINPC01"	4
2. Beispiel, "ping www.heise.de ."	5
3. Beispiel, "ping DEINPC01".....	5
<i>Namensauflösung unter Linux</i>	5
<i>Konsequenzen</i>	6
<i>Netzwerkumgebung</i>	6
<i>Wie verbinde ich ein Netzlaufwerk, wenn die Netzwerkumgebung leer ist?</i>	7
<i>Und jetzt?</i>	7

Grundsätzliches

Da es im Forum www.ipcop-forum.de immer wieder zu Fragen bezüglich der Namensauflösung kam, habe ich mich entschlossen, dieses Thema hiermit möglichst umfassend abzuhandeln. Auf den folgenden Seiten werden daher Grundlagen zum Thema Namensauflösung in Netzwerken vermittelt. Es werden ausserdem die häufigsten Fragen und Probleme betreffend Namensauflösung in gerouteten Netzwerken besprochen.

In aktuellen Netzwerken wird heutzutage fast ausschliesslich TCP/IP gesprochen. IPX/SPX und NetBIOS sind nur noch Randerscheinungen. Meine Ausführungen beschränken sich daher auf TCP/IP und das in Windowsnetzwerken immer noch häufig angetroffene NBT (NetBIOS over TCP/IP).

Vorbereitung

Es wird keine spezielle Konfiguration vorausgesetzt. Probleme bei der Namensauflösung sind nur bei Konfigurationen mit ORAGNGE, BLUE oder VPNs zu erwarten.

Was ist das eigentlich, Namensauflösung und für was ist sie gut?

Wie allgemein bekannt sein dürfte, verwendet TCP/IP zur Adressierung von PCs/Servern und anderem Netzwerkequipment IP-Adressen, die immer aus 4 Oktetten zusammengesetzt sind. Der Mensch ist es aber nicht gewöhnt (und er kann es daher auch nur schlecht), sich lange Zahlenkolonnen, wie z. B. 193.99.144.85 zu merken. Daher haben sich schlaue Köpfe unterschiedliche Systeme ausgedacht, wie aus IP-Adressen leicht merkbare Namen werden können. Die zwei wichtigsten Systeme, DNS für TCP/IP und WINS für NBT möchte ich hier beleuchten. Namensauflösung ist also nichts anderes, als ein Weg, aus IP-Adressen leichter merkbare Namen zu machen. Z. B. ist www.heise.de definitiv leichter zu merken als 193.99.144.85.

Grundlagen zur Namensauflösung bei NBT

NBT ist eigentlich ein Relikt aus vergangenen Zeiten. Als Computernetzwerke noch klein und lokal begrenzt waren, entstand das Netzwerkprotokoll NetBIOS. Dieses beschreibt einen flachen Namensraum, das will heissen, dass es in einem Netzwerk keine zwei Maschinen geben darf, die den gleichen Namen besitzen. Das ist in kleinen Netzwerken kein Problem, bei einem Netzwerk der Grösse des Internet ist dies aber kaum noch realisierbar. Eine weitere Beschränkung stellte die Tatsache dar, dass NetBIOS nicht geroutet werden kann. Diese Schwäche wurde später durch NBT überwunden, da hierbei NetBIOS quasi TCP/IP als Transportmittel verwendete und dadurch dessen Routingfähigkeiten erbt. In dieser Form hat NetBIOS bis heute überlebt, verliert aber mehr und mehr an Verbreitung.

NetBIOS-Namen sind maximal 15 Zeichen lang und jeder der einmal einem Windows-PC einen Namen gegeben hat, hat ihn schon verwendet. Nicht zulässige Zeichen sind: Unicode-Zeichen, Zahlen, Leerzeichen und die Sonderzeichen: / \ [] : | < > + = ; , ? und *

Ursprünglich wurden NetBIOS-Namen nur über Broadcasts aufgelöst. In immer grösser werdenden Netzen führte das aber schnell zu einer starken Netzbelastung, die den Nutzdaten immer weniger Bandbreite übrigliess. Die Lösung von Microsoft, dem Hauptnutzer von NetBIOS, war zuerst die Einführung von "lmhosts"-Dateien (lmhosts steht für LanManager-hosts). In diesen Dateien konnte, analog zu hosts-Dateien aus der TCP/IP-Welt, ein manuelles Mapping zwischen NetBIOS-Name und IP-Adresse festgelegt werden. Stark wachsende Netzwerke machten diese Lösung aber bald zu unflexibel und schwer handhabbar. WINS (Windows Internet Naming Service) sollte diese Probleme lösen, ein Serverdienst, der alle Clientnamen in einem Netzwerk in einer zentralen Datenbank verwaltete und dadurch die Broadcasts (fast) überflüssig machte. Eine weitere Aufgabe von WINS-Servern ist das Füllen der Netzwerkumgebung in gerouteten Netzwerken.

Knotentypen

Die Entscheidung, wie unter Windows NetBIOS-Namen aufgelöst werden, wird durch den Knotentyp bestimmt. Die Einstellungen des Knotentyps erfolgen in der Regel automatisch, kann jedoch in der Registry (unter dem Schlüssel ...NodeType) editiert werden oder dem Client in der DHCP Konfiguration übergeben werden. Es werden 4 verschiedene Knotentypen unterschieden.

B-Knotentyp: Die Namensauflösung erfolgt nur über Broadcasts, dies ist der Defaultwert, wenn kein WINS-Server konfiguriert ist.

P-Knotentyp: Die Namensauflösung erfolgt nur Point to Point mit einem konfigurierten WINS-Server.

M-Knotentyp: Dies ist eine Kombination von B- und P-Knoten. Die Namensauflösung erfolgt zuerst über Broadcasts und dann über einen WINS-Server.

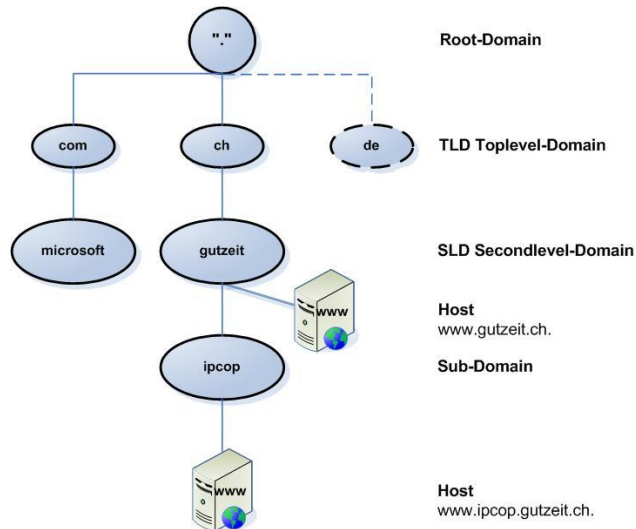
H-Knotentyp: Dies ist ebenfalls eine Kombination von B- und P-Knoten. Die Namensauflösung erfolgt hier aber zuerst über den WINS-Server und dann über Broadcasts. Der H-Knotentyp ist der Default, wenn auf einem Windowsclient ein WINS-Server eingetragen wurde.

Grundlagen zur Namensauflösung bei TCP/IP

TCP/IP verwendete in den Anfängen so genannte hosts-Dateien zur Namensauflösung. Eine statische Textdatei, in der das Mapping zwischen FQDN (Full Qualified Domain Name) und IP-Adresse hinterlegt war. Dieser Ansatz war aber schnell, wie die lmhosts-Datei, zu unflexibel um damals Tausende, heute Millionen von Hosts zu verwalten. Daher wurde das DNS (Domain Name System) entwickelt, welches bis heute seinen Dienst verrichtet.

Der DNS-Namensraum von TCP/IP ist, im Gegensatz zu NetBIOS nicht flach, sondern hat eine baumförmige Struktur. Der Namensraum beginnt mit der Root-Domain. Sie wird durch einen Punkt (.) symbolisiert. Von dieser Root-Domain zweigen dann die bekannten Toplevel-Domains, wie z. B. .com, .org, .ch, usw. ab. Secondlevel-Domains, wie z. B. microsoft, oder gutzeit zweigen wiederum wie Äste von den jeweiligen Toplevel Domains ab. An jeder Secondlevel-Domain können weitere Subdomains angehängt werden, wie z. B. ipcop. Die letzte Stufe bilden dann die eigentlichen Hosts, ein bekanntes Beispiel ist www. Zusammengesetzt ergibt sich dann ein FQDN, welcher eine Maschine im gesamten Namensraum eindeutig beschreibt. www.ipcop.gutzeit.ch ist ein anderer Host, als www.gutzeit.ch. Ein Maschinename (www) darf in diesem Namensraum also mehrfach verwendet werden. Wichtig ist nur, dass er nicht in der gleichen Domäne (gutzeit.ch) mehrfach vorkommt.

In der folgenden Grafik wird die oben beschriebene Struktur noch einmal bildlich dargestellt.



Namensauflösung unter Windows

Die Namensauflösung bei Windows-PCs ist relativ komplex. Abhängig von der Netzwerkkonfiguration und der eigentlichen Anfrage (NetBIOS-Name, oder FQDN) werden unterschiedliche Schritte unternommen, um die IP-Adresse zu dem gesuchten Namen herauszufinden.

Windows unterscheidet zuerst einmal, ob nach einem NetBIOS-Namen oder einem FQDN gesucht wird. Ein Name ohne Punkt wird immer als NetBIOS-Name interpretiert, wenn dagegen ein Punkt im Namen auftaucht, wird er als FQDN behandelt.

1. Beispiel, "ping DEINPC01"

Erste Erkenntnis für Windows, es handelt sich um einen NetBIOS-Namen. Als erstes wird daher der lokale NetBIOS Name-Cache durchsucht. Dann kommt die Netzwerkkonfiguration, bzw. der Knotentyp, s. O., ins Spiel. Wenn ein WINS-Server eingetragen wurde (H-Knotentyp), versucht der Rechner zuerst, den WINS zu kontaktieren um den Namen aufzulösen. Wenn dieser den Namen nicht kennt, oder wenn gar kein WINS-Server auf dem Client konfiguriert ist (B-Knotentyp), wird ein Broadcast ins Netzwerk geschickt, in der Hoffnung, ein PC mit dem gesuchte Namen meldet sich. Zu guter Letzt wird dann noch die lmhosts-Datei durchsucht.

Ein interessantes Feature von lmhosts ist das so genannte Preloading von einzelnen Einträgen. Mit Hilfe des Tags #PRE wird erreicht, dass das Mapping direkt beim Systemstart dauerhaft in den lokalen NetBIOS Name-Cache geladen wird. Da der Cache der erste Ort ist, an dem ein Mapping gesucht wird, ist dies eine gute Möglichkeit, den Namensauflösungsvorgang deutlich zu beschleunigen. Weiter Besonderheiten der lmhosts-Datei sind von Microsoft in der Datei lmhosts.sam, zu finden auf jedem Windowsrechner, dokumentiert.

2. Beispiel, "ping www.heise.de."

Erste Erkenntnis für Windows, es handelt sich um einen FQDN. Der erste Versuch beginnt auch hier mit dem lokalen Cache, hier aber dem DNS-Cache. Danach wird die lokale hosts-Datei ausgewertet und zuletzt wird dann eine Anfrage an den konfigurierten DNS-Server gestartet.

3. Beispiel, "ping DEINPC01"

Das hatten wir doch schon?! Ja, aber jetzt kommt noch eine Spezialität dazu, die Windows erst seit Windows 2000 beherrscht.

Wenn auf der NetBIOS-Schiene kein Ergebnis erreicht wird, kommt bei den aktuellen Windowsversionen ein DNS-Fallback hinzu.

Es ist möglich, einem Windows-PC ein DNS-Suffix anzugeben (Eigenschaften vom "Arbeitsplatz" -> Karteireiter "Computernamen" -> "Ändern" -> "Weitere..."). Wenn dieser DNS-Suffix konfiguriert wurde, verknüpft Windows diesen Suffix mit dem gesuchten NetBIOS-Namen um dadurch einen FQDN zu erhalten, mit dem nun auch die lokale hosts-Datei und der DNS-Server, wie im 2. Beispiel, befragt werden können.

Beim IPCop ist das DNS-Suffix per Default auf "localdomain" eingestellt. Dies kann aber bedenkenlos geändert werden, gute Beispiele für ein Heimnetzwerk sind z. B. "local.lan" oder "home.local". Auf keinen Fall sollten hier allerdings Domainnamen verwendet werden, die schon von dritten Personen im Internet registriert worden sind.

All diese Vorgänge brauchen natürlich Zeit so dass man versuchen sollte, auf möglichst direktem Weg zur Namensauflösung zu kommen. Einen WINS-Server einzutragen, der nicht existiert oder nicht erreichbar ist, verlangsamt die Namensauflösung z. B. enorm.

Namensauflösung unter Linux

Da Linux kein NetBIOS kennt, beschränkt sich die Suche auf den DNS.

Beispiel, "ping www.heise.de."

Der erste Versuch beginnt auch hier mit dem lokalen DNS-Cache. Danach wird die lokale hosts-Datei ausgewertet und zuletzt wird dann eine Anfrage an den konfigurierten DNS-Server gestartet.

Konsequenzen

Bei Linux und Windows-PCs ab Windows 2000 ist die bevorzugte Technik zur Namensauflösung der DNS. Nur bei älteren Windowsversionen muss zwingend auf NetBIOS-Namensauflösung gewechselt werden, da diese Versionen nicht richtig mit DNS umgehen können.

Als DNS-Server kann für PCs an GREEN und BLUE der IPCop verwendet werden. Dazu muss auf dem IPCop unter "Dienste" -> "Hosts bearbeiten" jeder PC/Server mit seiner IP-Adresse und seinem Hostnamen registriert werden. In meinen Installationen wird immer auch der Domainname ausgefüllt. Dieser lautet genau gleich, wie das DNS-Suffix auf allen beteiligten Clients. Das DNS-Suffix darf natürlich nicht auf jedem PC/Server anders lauten, sondern er muss innerhalb des Netzes einheitlich sein. Zuletzt darf natürlich nicht vergessen werden, den IPCop auf dem Client als primären DNS-Server einzutragen.

Netzwerkumgebung

Ein "Problem" sei hier nicht verschwiegen. Sobald unterschiedliche Subnetze im Spiel sind, sei es zwischen GREEN und BLUE oder ORANGE, oder wegen einem VPN, funktioniert die Netzwerkumgebung auf Windows-PCs nicht mehr wie gewohnt. Das heisst, es sind nur die PCs/Server in der Netzwerkumgebung sichtbar, die sich im gleichen Subnetz wie der eigene PC befinden. PCs und Server in Remotesubnetzen erscheinen nicht in der Netzwerkumgebung. Dieses Verhalten ist kein Fehler, sondern per Design so. Die Netzwerkumgebung füllt sich normalerweise mit Hilfe von Broadcasts. Das funktioniert aber nur innerhalb eines Subnetzes, da Broadcasts prinzipiell von allen Routern (nicht nur vom IPCop) geblockt werden. Router begrenzen immer so genannte Broadcastdomains. Ohne dieses Feature würde z. B. das Internet in einem beispiellosen Broadcaststurm in die Knie gehen, für Nutzdaten wäre keine Bandbreite mehr übrig.

Dieses Verhalten stellt an sich kein Problem dar, da durch die DNS-Namensauflösung trotzdem Netzlaufwerke über einen Namen verbunden werden können. Nur der Weg über die Netzwerkumgebung funktioniert halt nicht. Wenn auf die Netzwerkumgebung nicht verzichtet werden kann, muss in einem gerouteten Netzwerk zwingend ein WINS- oder Samba-Server installiert werden. Da dessen IP-Adresse bekannt ist, können sich über diesen Server Clients aus unterschiedlichen Subnetzen ohne Broadcasts registrieren und ebenso natürlich auch gesuchte Namen auflösen.

Wie verbinde ich ein Netzlaufwerk, wenn die Netzwerkumgebung leer ist?

Da gibt es verschiedene Möglichkeiten.

1. Kommandozeile (cmd.exe, command.com) Hiermit kann über eine Befehlszeile wie *net use x: \\SERVERNAME\SHARENAME* die Freigebe *SHARENAME* auf dem Server *SERVERNAME* mit dem Laufwerk *X:* verbunden werden. Diese Zeile lässt sich natürlich auch in einen Batch, oder in ein Loginscript einbauen.

Damit die Verbindung nach dem nächsten Reboot automatisch wieder zur Verfügung steht, kann ihr noch der Schalter */PERSISTENT:YES* angefügt werden. Hilfe zu den weiteren Funktionen findet sich mittels *"net use /?"* auf der Kommandozeile.

2. Explorer (explorer.exe) Hier kann über "Extras" -> "Netzlaufwerk verbinden" ebenfalls festgelegt werden, welche Freigabe mit welchem Laufwerksbuchstaben verbunden werden soll. Ausserdem ist es hier einfach per Mausklick möglich, die Verbindung dauerhaft zu speichern.

Und jetzt?

- Wie wäre es mit einem weiteren Tutorial?
- VPN auf BLUE mit PSK
- VPN auf BLUE mit X.509 Zertifikat
- Web- / Mailserver in der DMZ

Also weiter geht's mit dem nächsten Tutorial.