CloudCommand

Cyber Security

CloudCommand GmbH chr.schumacher@gmx.tm

System- und Netzwerk-administration

CloudCommand GmbH chr.schumacher@gmx.tm

Sendearten

Ethernet

- Der Begriff Ethernet bezieht sich auf die kabelgebundene Datenübertragung innerhalb eines lokalen Netzwerks (Local Area Network / LAN). Innerhalb eines solchen geschlossenen Netzwerks sind Computer, Drucker und Server über spezielle LAN-Kabel miteinander verbunden und können untereinander kommunizieren.
- Ursprünglich diente die Bezeichnung LAN-Kabel als Oberbegriff, während der Begriff Ethernet-Kabel einen bestimmten Typ von Kabel bezeichnete – nämlich ein in sich gedrehtes Kupferkabel, über das Daten in standardisierter Form weitergeleitet werden. Dazu werden die eigentlichen Daten in kleineren Portionen durch sogenannte Ethernet-Frames in etwas größere Ethernet-Pakete verpackt, die neben den eigentlichen Daten auch Informationen wie Prüfsummen und MAC-Adressen enthalten.

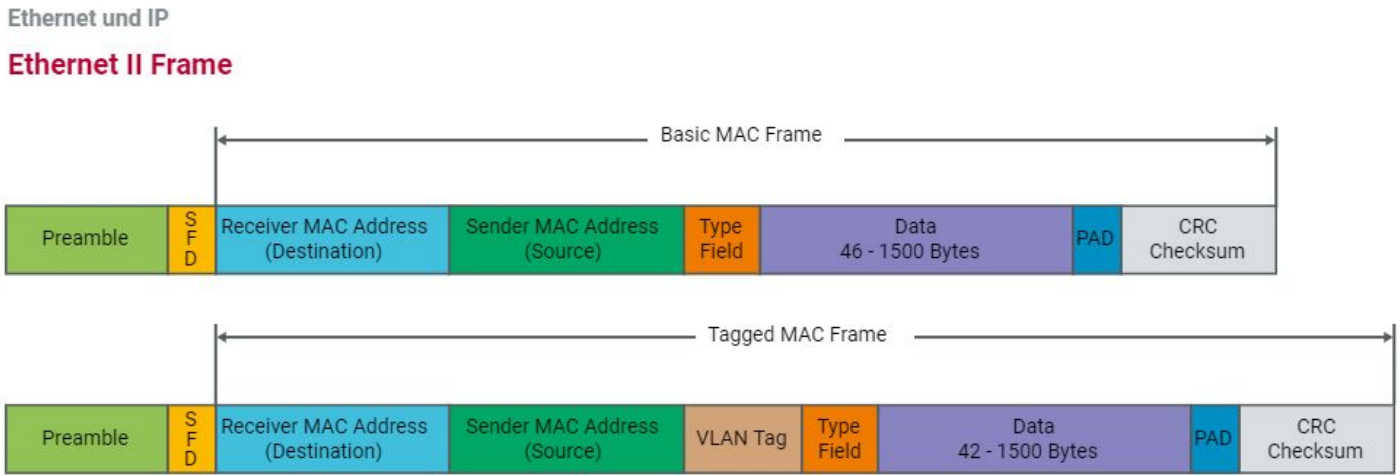
Ethernet Standards

- **IEEE** - Abkürzung für Institute of Electrical and Electronics Engineers) ist ein weltweiter Berufsverband von Ingenieuren, Technikern, (Natur-)Wissenschaftlern und angrenzender Berufe hauptsächlich aus den Bereichen Elektrotechnik und Informationstechnik.
- **ISO** - Die Internationale Organisation für Normung ist eine unabhängige Nichtregierungsorganisation, deren Mitglieder aus verschiedenen nationalen Normungsgremien bestehen.
- **EIA/TIA** - Die Electronic Industries Alliance (EIA; bis 1997 Electronic Industries Association) war eine amerikanische Normungs- und Handelsorganisation , die sich als Zusammenschluss von Handelsverbänden für Elektronikhersteller in den Vereinigten Staaten zusammensetzte.

Ethernet Standard IEEE 802.3

- Ethernet ist ein Satz von Regeln, welche die Übertragung von Daten zwischen dem Netzwerkadapter und den verschiedenen zentralen Koppelelementen steuern.
- Alle Netzwerkadapter und Koppelelemente müssen mit Ethernet kompatibel sein um miteinander zu kommunizieren.
- Computer in Ethernet-Netzwerken kommunizieren per Ethernet-Frames.
- Ein Frame ist eine Gruppe von Bytes bei der Netzwerkübertragung
- Frames befinden sich auf der Schicht 2 des OSI-Modells.
- Standardmäßig verwenden alle Computer in einem Ethernet-Netzwerk einen einzigen Kanal. Aus diesem Grund kann nur von einem Computer zum selben Zeitpunkt übertragen werden.

Ethernet Frame



Ethernet Frame

IEEE-Standard	Bezeichnung	Datenrate	Kabel
802.3	10Base-5	10 Mbps	Dickes Koax (Kupfer)
802.3a	10Base-2	10 Mbps	Dünnes Koax (Kupfer)
802.3i	10Base-T	10 Mbps	TP - Kupfer
802.3j	10Base-FL	10 Mbps	LWL
802.3u	100Base- TX und FX	100 Mbps	TP - Kupfer, LWL
802.3z	1000Base-X	1000 Mbps	LWL
802.3ab	1000Base-T	1000 Mbps	TP - Kupfer
802.3ae	10GBase-ER/EW 10GBase-LR/LW 10GBase-SR/SW 10GBase-LX4	10 Gbps	LWL
802.3ak	10GBase-CX4	10 Gbps	Infiniband-Kupfer
802.3an	10GBase-T	10 Gbps	TP - Kupfer
802.3aq	10GBase-LRM	10 Gbps	LWL
802.3ba	40GBASE-CR4 100GBASE-CR10 40GBASE-SR4 100GBASE-SR10	40 Gbps 100 Gbps 40 Gbps 100 Gbps	TP - Kupfer TP - Kupfer LWL LWL

Power over Ethernet (PoE)

- IEEE 802.3af
- 44 - 57 Volt (meistens mit 48 V und bis zu 15,4 Watt)

Spare-Pair-Use:

- Verwendet die ungenutzten Adern der Leitung

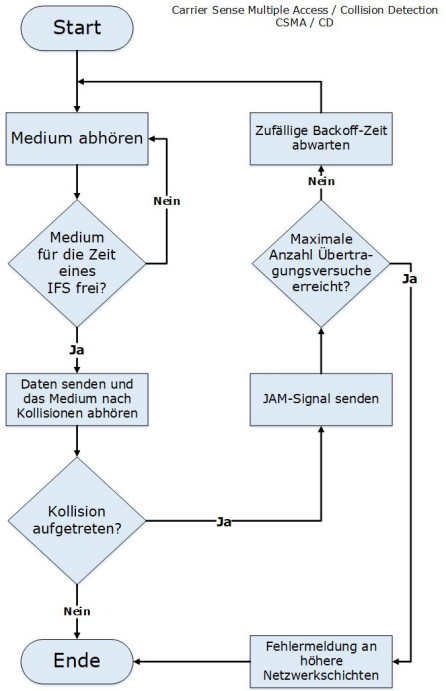
Phantom-Use:

- Zusätzlich zum Datensignal ein Gleichstromanteil über die vier verwendeten Adern übertragen

Steuerung des Leitungszugriffs

- IEEE 802.3 definiert **Carrier Sense multiple Access/Collision Detection oder CSMA/CD**.
- Da Computer in einem Standard-Ethernet-LAN alle den gleichen Kanal verwenden, steuert CSMA/CD die Möglichkeit, wie Computer mit einer begrenzten Anzahl von Kollisionen koexistieren können.
- Wenn eine Organisation drahtloses Ethernet einsetzt, findet **Carrier Sense multiple Access/Collision Avoidance (CSMA/CA)** Verwendung.

CSMA/CD

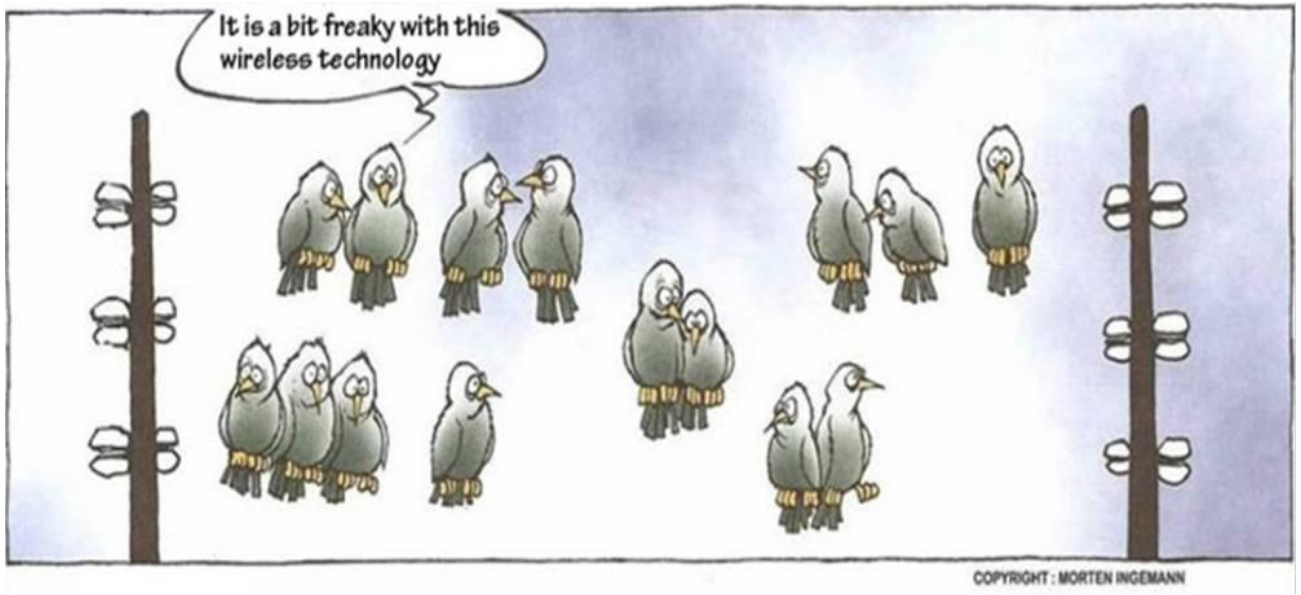

Carrier Sense Multiple Access / Collision Detection
CSMA / CD
Start
Medium abhören
Nein
Medium für die Zeit eines IFS frei?
Ja
Daten senden und das Medium nach Kollisionen abhören
Kollision aufgetreten?
Ja
Nein
Ende
Zufällige Backoff-Zeit abwarten
Nein
Maximale Anzahl Übertra-gungsversuche erreicht?
Ja
JAM-Signal senden
Fehlermeldung an höhere Netzwerkschichten

CSMA/CD

- Das ist ein Zugriffsverfahren für Netzwerke in der Bus-Topologie.
- Der sendebereite Rechner überprüft vor dem Senden, ob die Leitung frei ist
- Dann sendet er zuerst einen Rundspruch an alle im Netzwerksegment befindlichen Rechner, um das Senden anzukündigen.
- Danach erst werden die Daten versandt.

- Dadurch werden Kollisionen mit Sendungen anderer Rechner vermieden. Die Netto-Bandbreite ist aber erheblich geringer als die theoretisch mögliche.
- Anwendung findet es u. a. in LocalTalk, der Netzwerk-Technologie für Macintosh-Rechner der Firma Apple, und in WLAN nach 802.11.

WLAN


It is a bit freaky with this wireless technology
COPYRIGHT : MORTEN INGEMANN

WLAN

IEEE 802.11

- Seit seiner Einführung 1997 hat sich IEEE 802.11sehr schnell verbreitet und wird von allen Wireless-Technologien am häufigsten eingesetzt.
- 802.11 besteht aus mehreren Unterstandards, die sich in den Punkten Frequenzspektrum, Übertragungsrate und Funktechnologie unterscheiden. Sie alle werden jedoch über Funk betrieben.
- Beim WLAN unterscheidet man auch zwischen direkten oder ad-hoc Verbindung und der Infrastruktur-Verbindung mittels zentralem Zugriffspunkt

Wireless Access Point & Ad-hoc

- Am meisten wird WLAN mit einem Wireless Access Point (WAP oder AP) eingesetzt.
- Dieser befindet sich entweder im „Internetrouter“ oder als separates Gerät.
- Dies wird auch als Infrastruktur-Modus bezeichnet

- Im Ad-hoc Modus stellen die W-Lan Geräte eine direkte Verbindung untereinander her

WLAN-Standards

	Frequenzbereich	Übertragungsrate
802.11	2,4 GHz	1 oder 2 MBit/s
802.11a	5 GHz	bis zu 54 MBit/s
802.11b	2,4 GHz	5,5/11/22 MBit/s
802.11g	2,4 GHz	bis zu 54 MBit/s
802.11n	2,4 und 5 GHz	bis zu 600 MBit/s
802.11ac	5 GHz	bis zu 6,9 GBit/s
802.11ax	2,4, 5 und 6 GHz	bis zu 9,6 GBit/s

WLAN-Standards

- Die Reichweite bei WLAN beträgt maximal 100 Meter im Freien ohne Störung.
- Je nach verwendeten Antennen verändert sich der sog. Abdeckungs-bereich.
- Kommen Störfaktoren, wie Wände oder elektronische Geräte dazu, sinkt die Reichweite.

Logos statt kryptischer Kürzel

Sicherheit im WLAN

SSID

- Bei der Verwendung von Infrastruktur-Modus, wird die Basiseinheit (normalerweise ein WAP) mit einem Service Set Identifier (SSID) konfiguriert.
- Dies wird dann der Name des drahtlosen Netzwerks
- Wenn Clients eine Verbindung zum WAP aufbauen wollen, können sie ihn durch die SSID identifizieren.

Sicherheit im WLAN

Authentifizierung

- Im privaten Umfeld, sowie in kleinen Betrieben, erfolgt die Authentifizierung bei einem WLAN mithilfe eines vorab geteilten Schlüssels (Pre-Shared-Key, kurz PSK)
- Größere Unternehmen nutzen bevorzugt eine Zertifikatsbasierte Authentifizierung auf Basis des IEEE 802.1x

Sicherheit im WLAN

Verschlüsselung

- Standardmäßig wird der gesamte Datenverkehr im WLAN zwischen dem AP oder Client und Client verschlüsselt
- Es gibt verschiedene Standards für die Verschlüsselung im WLAN
  - WEP (Wired Equivalent Privacy)
  - WPA (Wi-Fi Protection Access) *
  - WPA2 (Wi-Fi Protection Access)*
  - WPA3 (Wi-Fi Protection Access)

* beide verwenden entweder TKIP (Temporal Key Integrity Protocol) oder AES (Advanced Encryption Standard) als Verschlüsselungsmethode

Mögliche Maßnahmen für mehr Sicherheit

- Eigenes Admin-Passwort für den Access Point vergeben
- WPA2/3-Verschlüsselung einschalten
- Starkes WLAN-Passwort (PSK) verwenden
- Undefinierbare SSID vergeben
- MAC-Adressfilter einsetzen
- SSID Broadcast abstellen
- Funkleistung einschränken
- Zeitplanung einrichten

Mögliche Maßnahmen für mehr Sicherheit

- WLANs von anderen Netzwerk-Segmenten logisch trennen
- VPN einsetzen
- Firewall zwischen WLAN und LAN installieren
- IDS im WLAN aufstellen
- regelmäßige Audits mit aktuellen Hacker-Tools
- Separates Gäste-WLAN-Netzwerk

Der Mensch und die Zahlen

- Computer identifizieren sich mittels IP Adressen in binärer Form
- Das menschliche Gehirn kann mit Zahlen nicht gut umgehen
- „Unser Gehirn denkt ausschließlich in Bildern. Das ist auch der Grund, warum der Mensch ein Meister des Geschichtenerzählens ist. Zahlen dagegen sind abstrakt. Die Höhe eines Gebäudes beispielsweise lässt sich für unser Gehirn nicht logisch ableiten. Im Vergleich zu physischen Gegenständen sind Zahlen nicht greifbar.“

Daher verknüpfen wir IP-Adressen mit Namen

Computernamen

Hostname:

- Bis zu 255 Zeichen lang
- Bestehend aus
  - Buchstaben
  - Zahlen
  - Bindestrichen
  - Punkten
- Teil des „vollqualifizierten Domänennamens“ (FQDN: fully qualified domain name)

FQDN: Computer1.Firma-X.DE.

Computernamen

NetBIOS-Name:

- Bis zu 15 Zeichen lang
- Das 16. Zeichen bestimmt die Funktion
- Keine (hierarchische) Struktur

Computer1[00]

Namensauflösung

Lokal

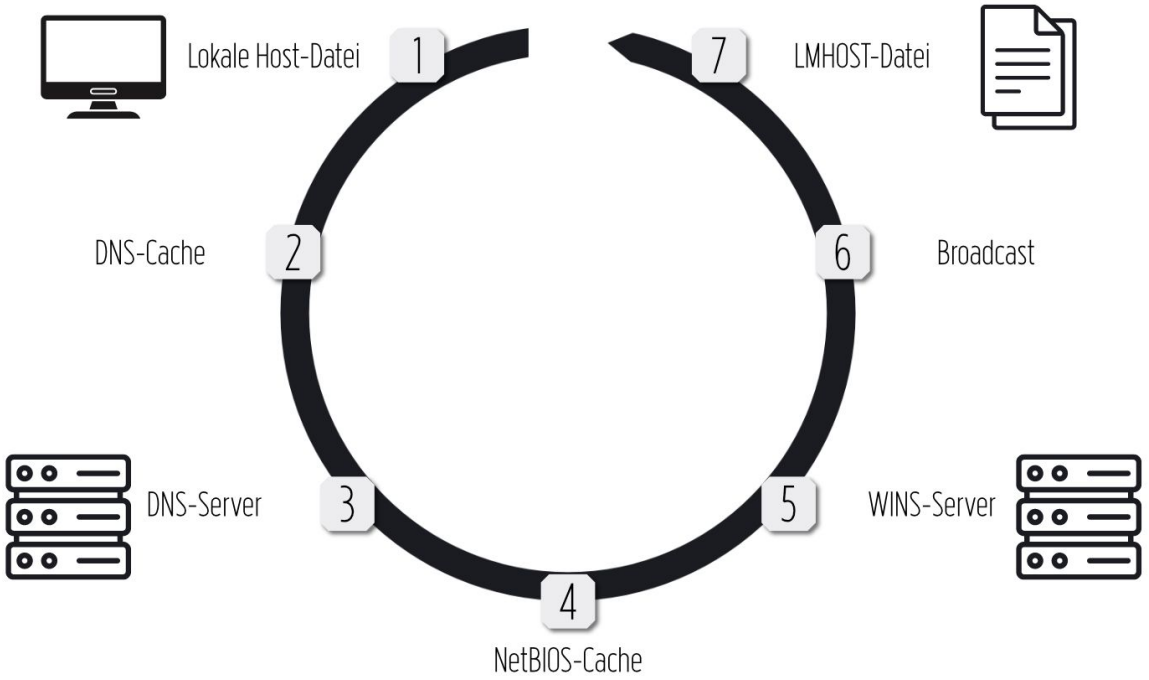
- Lokale Dateien sind die einfachste Art der Namensauflösung
- In einer Textdatei wird der Name einer IP Adresse zugeordnet.
- Die Datei für Hostnamen wird im Ordner „%systemroot%\system32\drivers\etc\hosts“ gespeichert
- Die Datei für NetBIOS Namen wird im Ordner „%systemroot%\system32\drivers\etc\lmhosts“ gespeichert.

Namensauflösung

Remote

- Domain Name System (DNS)
  - Kann Hostnamen zu IP Adressen auflösen.
  - Verwendet FQDN
  - Ist die im Internet verwendete Namensauflösung
- Windows Internet Naming Service (WINS)
  - Löst NetBIOS-Namen auf.
  - Die Daten werden von Client-Rechnern an den WINS-Server gemeldet.
  - Manuelle Konfiguration ist nicht notwendig.

Namensauflösung



Windows Internet Naming Service (WINS)

Wann ist WINS erforderlich?

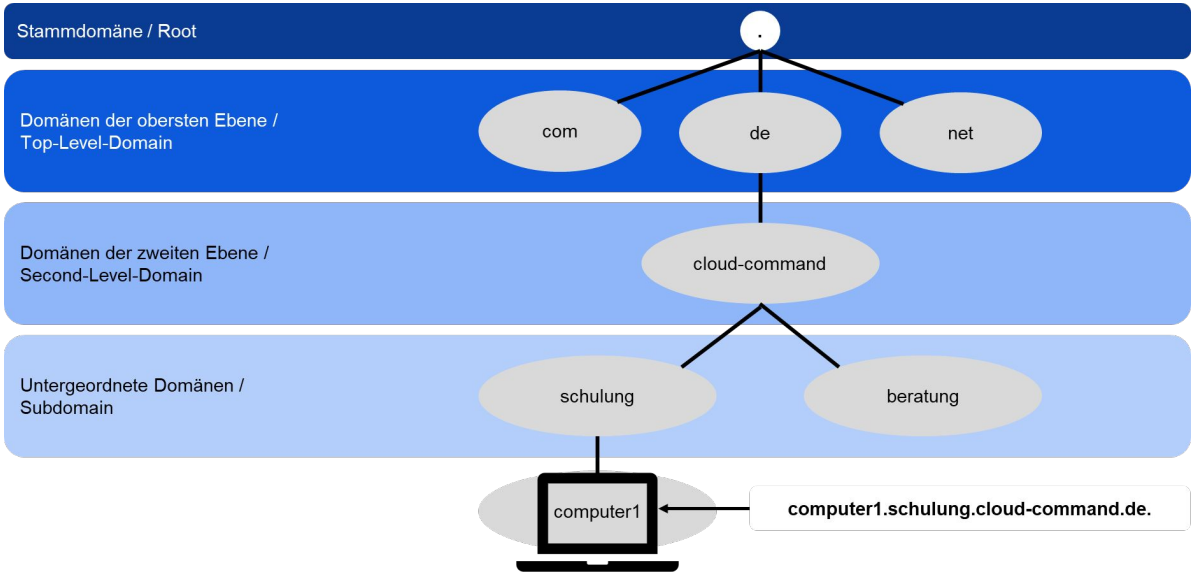
- ältere Versionen von Microsoft-Betriebssystemen (vor Windows 2000) verwendet werden.
- Bestimmte, i. d. R. ältere Anwendungen verwendet NetBIOS-Namen.
- Wenn Benutzer Netzwerkbrowser Features in der Netzwerkumgebung verwenden möchten.

WINS kann vom DNS mit übernommen werden, daher ist kein separater Dienst mehr notwendig.
Es bedarf allerdings am DNS-Server entsprechende Anpassung.

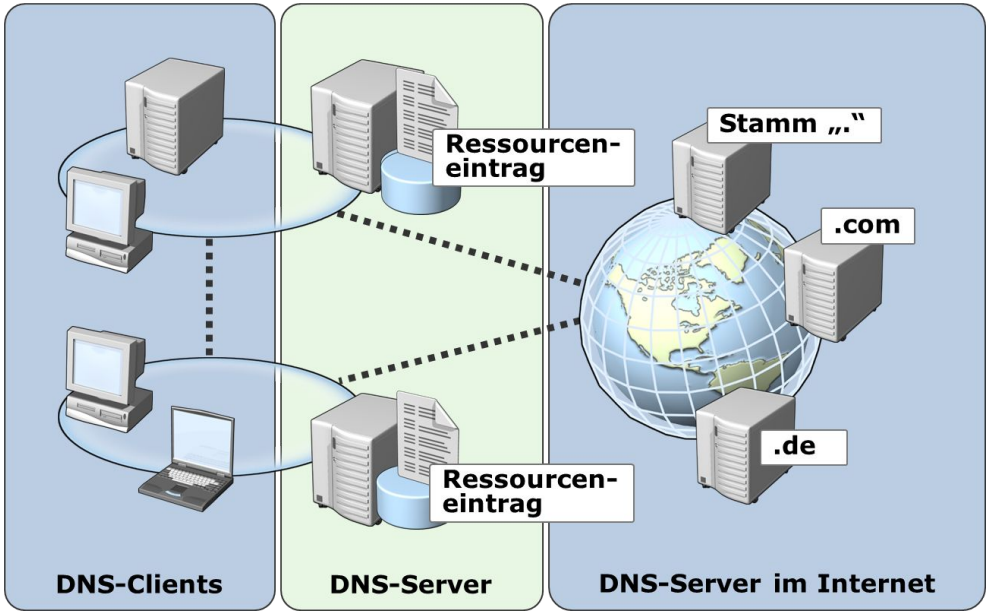
Domain Name System (DNS)

- Domain Name System ist eine hierarchische, verteilte Datenbank.
- DNS bildet die Grundlage des Internet-Benennungsschemas.
- DNS unterstützt den Zugriff auf Ressourcen über alphanumerische Namen.
- InterNIC ist für die Verwaltung der Domainnamen verantwortlich.
- DNS wurde entwickelt, um die wachsende Anzahl von Hosts im Internet zu unterstützen.
- Mit der Einführung von IPv6 ist DNS noch wichtiger geworden.

DNS Aufbau & Fully-Qualified-Domain-Name



DNS Komponenten



DNS Zonen Einträge

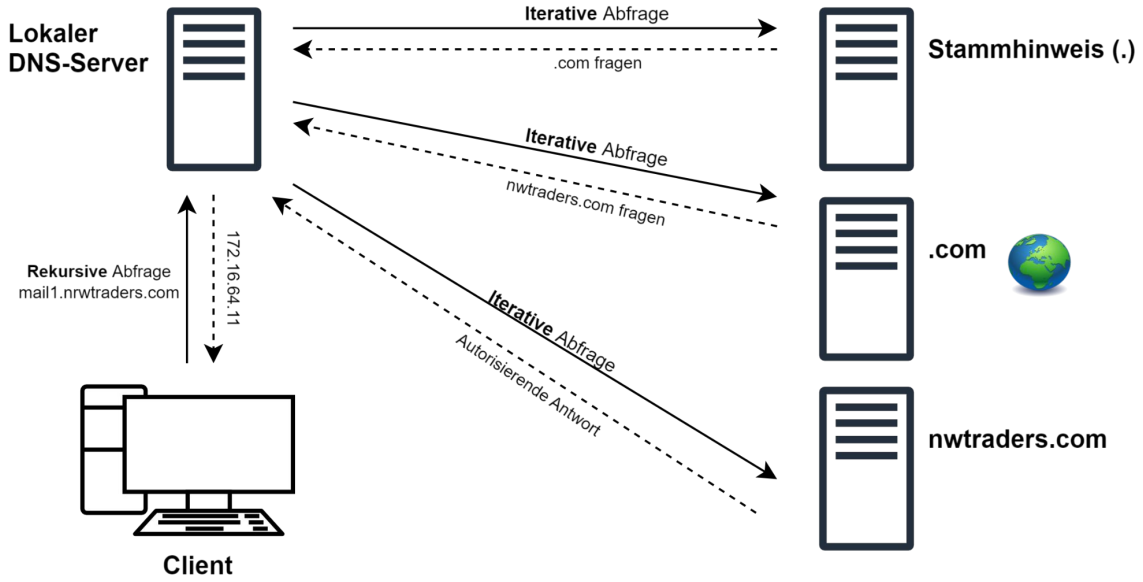
Folgende DNS-Ressourceneinträge sind verfügbar:

- **SOA:** Autoritätsursprung
- **A:** IPv4-Host Eintrag
- **AAAA:** IPv6-Host Eintrag
- **CNAME:** Alias Eintrag
- **MX:** Mail-Exchange-Eintrag
- **SRV:** Dienst Ressourcen
- **NS:** Name Server der Zone
- **TXT:** “Freie” Texteinträge

DNS Zonen Einträge

```
cloud-command.de. 600 IN A 217.160.0.97
cloud-command.de. 600 IN AAAA 2001:8d8:100f:f000::29b
cloud-command.de. 3600 IN MX 1 aspmx.l.google.com.
cloud-command.de. 3600 IN MX 10 alt3.aspmx.l.google.com.
cloud-command.de. 3600 IN MX 10 alt4.aspmx.l.google.com.
cloud-command.de. 3600 IN MX 5 alt1.aspmx.l.google.com.
cloud-command.de. 3600 IN MX 5 alt2.aspmx.l.google.com.
cloud-command.de. 86400 IN NS ns.udag.de.
cloud-command.de. 86400 IN NS ns.udag.net.
cloud-command.de. 86400 IN NS ns.udag.org.
cloud-command.de. 86400 IN TXT "google-site-
verification=PvhAzi00PBZThQwKwMqUm2L_D8abTxh9wkntjZ3Clq4"
cloud-command.de. 86400 IN SOA ns.udag.de. hostmaster.united-domains.de.
```

DNS Abfragen



Was sollte ich auf jeden Fall behalten

- Auf OSI-Layer-2-Ebene gibt es sehr verbreitete Protokolle wie Ethernet und WLAN.
- Auf dieser Ebene gibt es verschiedene Algorithmen zur Sicherstellung, dass die “Leitung” frei ist (CSMA/CD, CSMA/CA).
- Vor allem beim Übertragungsmedium “Luft” (WLAN) sollten viele Erwägungen bzgl. der Sicherheit getroffen werden.

Was sollte ich auf jeden Fall behalten

- Um Menschen das Ansprechen von Endpunkten zu erleichtern gibt es Protokolle, die ihnen “Namen” statt Zahlen zuordnen.
- Das wichtigste und verbreitetste ist das mehrstufige DNS.

  subdomain3.subdomain2.subdomain1.second-level-domain.top-level-domain
- Öffentliche (Root-Server) und lokale DNS-Server sind diesbezüglich wichtige Knotenpunkte.

CloudCommand

CloudCommand GmbH chr.schumacher@gmx.tm