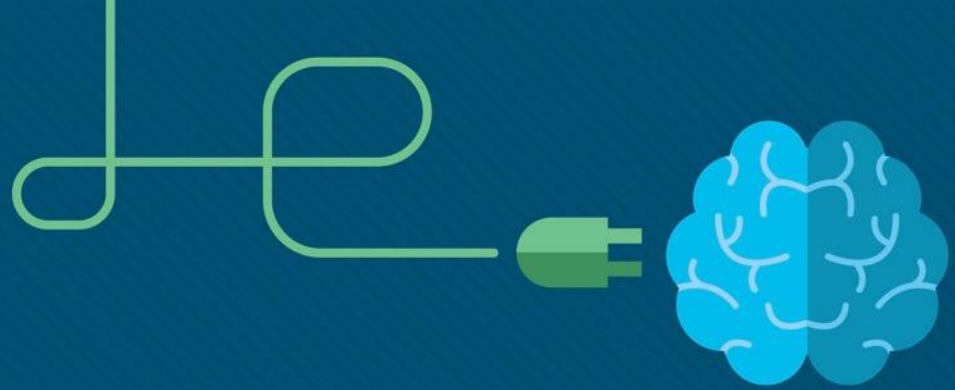


Modul 15: Anwendungsschicht

Unterlagen für Instruktoren

Einführung in Netzwerke v7.0
(ITN)





Modul 15: Anwendungsschicht

Einführung in Netzwerke v7.0
(ITN)



Modulziele

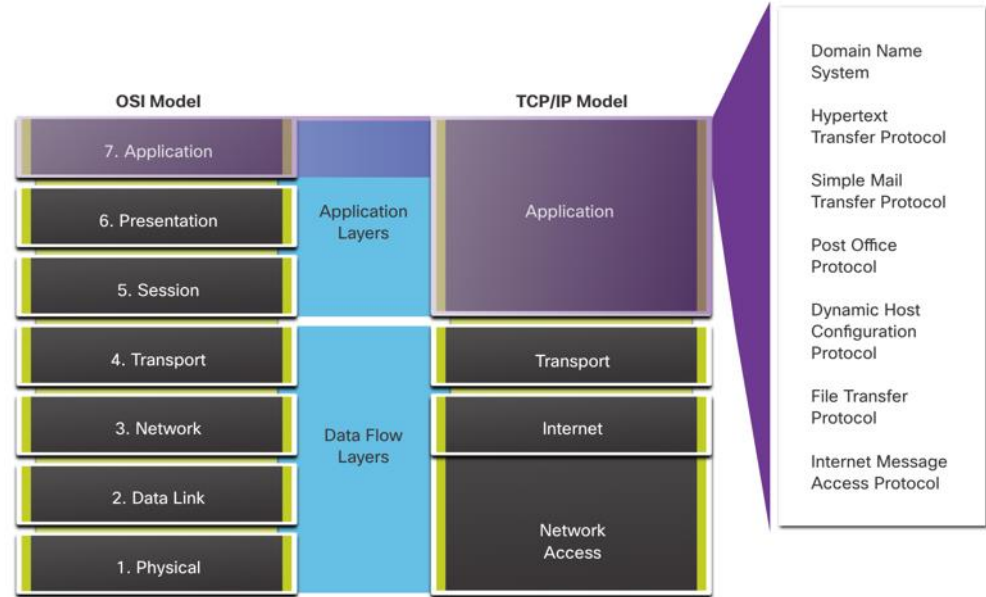
- **Modultitel:** Anwendungsschicht
- **Modulziel:** Erläuterung der Funktionsweise von Protokollen der Anwendungsschicht bei der Unterstützung von Endbenutzer-Applikationen.

Thema	Ziel
Anwendungsschicht, Darstellungsschicht und Sitzungsschicht	Erläuterungen, wie die Funktionen der Anwendungs-, Präsentations- und Sitzungsschicht zusammenwirken, um Netzwerkdienste für Endbenutzeranwendungen bereitzustellen.
Peer to Peer	Erläutern Sie, wie Endbenutzeranwendungen in einem Peer-to-Peer-Netzwerk funktionieren.
Web- und E-Mail-Protokolle	Erläutern Sie, wie Web- und E-Mail-Protokolle funktionieren.
IP-Adressierungsdienste	Erläutern Sie, wie DNS und DHCP funktionieren.
Dateifreigabedienste	Erläutern Sie, wie Dateiübertragungsprotokolle funktionieren.

15.1 Anwendungsschicht, Darstellungsschicht und Sitzungsschicht

Application, Presentation, and Session Application Layer

- Die oberen drei Schichten des OSI-Modells (Anwendungs-, Darstellungsschicht und Sitzungsschicht) definieren Funktionen der TCP/IP-Anwendungsschicht.
- Die Anwendungsschicht bildet die Schnittstelle, zwischen den für die Kommunikation verwendeten Anwendungen und dem darunter liegenden Netzwerk, über das Nachrichten übertragen werden.
- Zu den bekanntesten Protokollen der Anwendungsschicht gehören HTTP, FTP, TFTP, IMAP und DNS.



Anwendung, Präsentation und Sitzung

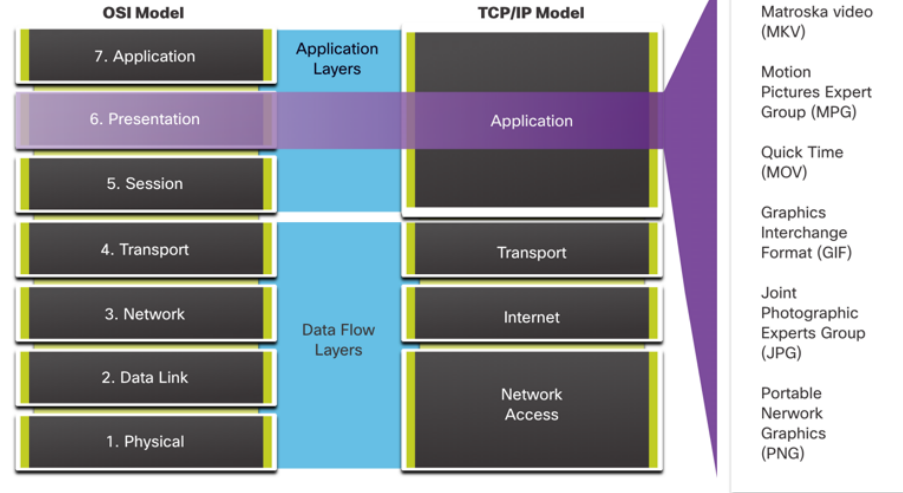
Präsentations- und Sitzungsebene

Die Darstellungsschicht hat drei Hauptfunktionen:

- Formatieren oder Darstellen von Daten auf dem Quellgerät in einer kompatiblen Form für den Empfang durch das Zielgerät
- Komprimieren von Daten, sodass sie vom Zielgerät dekomprimiert werden können
- Verschlüsseln von Daten für die Übertragung und Entschlüsseln der Daten nach dem Empfang

Die Session-Layer-Funktionen:

- Es erstellt und verwaltet Dialoge zwischen Quell- und Zielanwendungen.
- Sie handhabt den Austausch von Informationen, um Konversationen zu initiieren, zu verwalten und Sitzungen, die über einen längeren Zeitraum unterbrochen oder nicht aktiv sind, neu zu starten.



Protokolle für Anwendung, Präsentation und Sitzung TCP/IP- Anwendungsschicht

- Die TCP/IP-Anwendungsprotokolle geben das Format vor und steuern die erforderlichen Informationen für viele gängige Internet-Kommunikationsfunktionen.
- Anwendungsschichtprotokolle werden von den Quell- und Zielgeräten während einer Kommunikationssitzung verwendet.
- Um eine erfolgreiche Kommunikation sicherzustellen, müssen die auf dem Quell- und Ziel-Host implementierten Anwendungsschichtprotokolle kompatibel sein.

Namenssystem

DNS - Domain Name System (oder Service)

- TCP, UDP-Client 53
- Übersetzt Domännennamen wie cisco.com, in IP-Adressen

Host-Konfiguration

DHCP - Dynamic Host Configuration Protocol

- UDP-Client 68, Server 67
- Durch eine dynamische Vergabe der IP-Adressen können diese wiederverwendet werden, wenn sie nicht mehr benötigt werden

Web

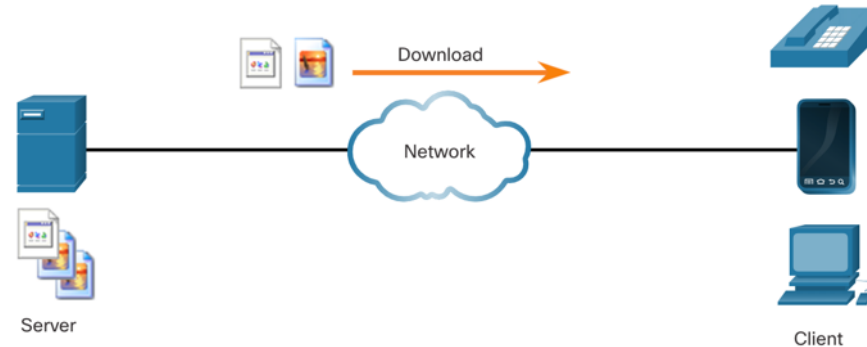
HTTP - Hypertext Transfer Protocol

- TCP 80, 8080
- Eine Reihe von Regeln für den Austausch von Text-, Grafik-, Ton-, Video- und anderen Multimedia-Dateien im World Wide Web.

15.2 Peer-to-Peer

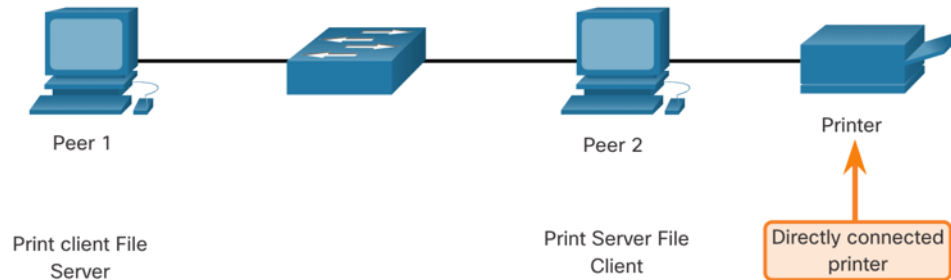
Peer-to-Peer-Client-Server-Modell

- Client- und Server-Prozesse finden in der Anwendungsschicht statt.
- Im Client-Server-Modell wird das Gerät, das Informationen anfordert, als Client, und das Gerät, das auf die Anforderung reagiert, als Server bezeichnet.
- Die Protokolle der Anwendungsschicht beschreiben das Format der Anforderungen und Antworten zwischen Clients und Servern.



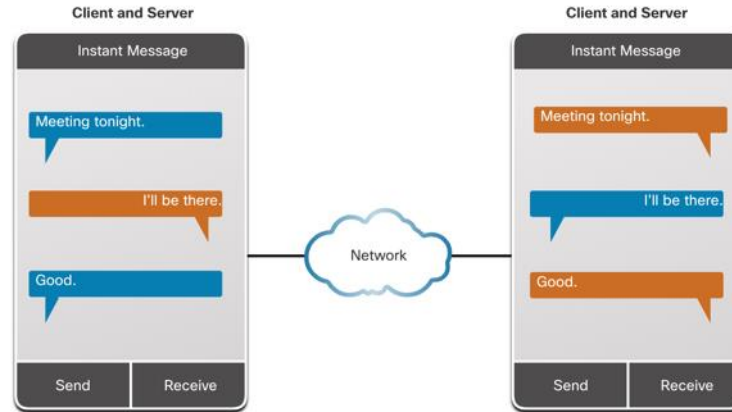
Peer-to-Peer-Netzwerke

- In einem Peer-to-Peer-Netzwerk (P2P) sind zwei oder mehrere Computer über ein Netzwerk verbunden und können Ressourcen gemeinsam nutzen (z.B. Drucker und Dateien), ohne dabei einen dedizierten Server zu verwenden.
- Jedes verbundene Endgerät (der sogenannte Peer) kann sowohl als Server wie auch als Client fungieren.
- Ein Computer könnte die Rolle des Servers für eine Transaktion übernehmen und gleichzeitig die eines Clients für eine weitere Transaktion. Die Rolle als Client oder Server wird bei jeder Anforderung festgelegt.



Peer-to-Peer Anwendungen

- Eine P2P-Anwendung ermöglicht es einem Gerät, in derselben Kommunikationssitzung als Client und als Server zu fungieren
- In einem Hybridsystem greift jeder Peer auf einen Indexserver zu, um den Standort einer auf einem anderen Peer gespeicherten Ressource zu erhalten.

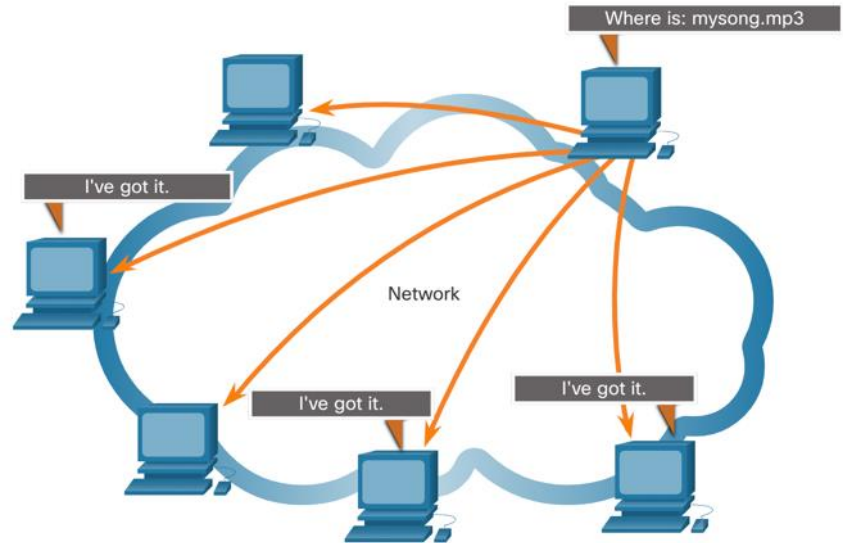


Gängige P2P Anwendungen

Bei P2P-Anwendungen kann jeder Computer im Netzwerk, auf dem die Anwendung ausgeführt wird, als Client oder Server für die anderen Computer im Netzwerk fungieren, die die Anwendung nutzen.

Zu den Beispielen für gängige P2P-Netzwerke gehören:

- BitTorrent
- Direktverbindung
- eDonkey
- Freenet



15.3 Web- und Email-Protokolle

Hypertext Transfer Protokoll und Hypertext Markup Language

Wenn eine Webadresse oder eine URL (Uniform Resource Locator) in einen Webbrowser eingegeben wird, stellt der Browser eine Verbindung zu dem Webdienst her. Der Webdienst wird auf dem Server ausgeführt, der das HTTP-Protokoll verwendet.

Um besser zu verstehen, wie Webbrowser und Webserver interagieren, können wir untersuchen, wie eine Webseite in einem Browser geöffnet wird.

Schritt 1

Der Browser interpretiert die drei Teile der URL:

- http (das Protokoll oder Schema)
- www.cisco.com (der Servername)
- index.html (der spezifische angeforderte Dateiname)

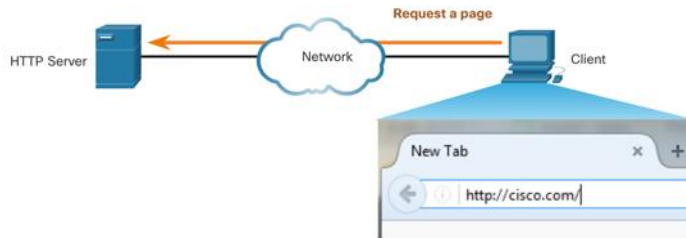


Hypertext Transfer Protokoll und Hypertext Markup Language (Forts.)

Schritt 2

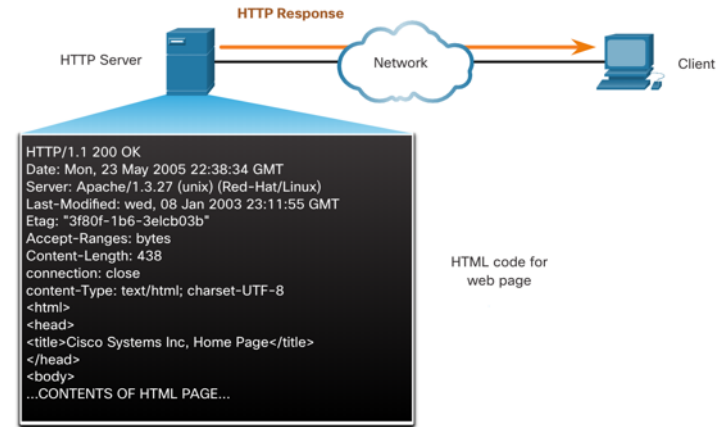
Der Browser überprüft dann mit einem Domain Name System-Server (DNS-Server) die Adresse, konvertiert `www.cisco.com` in eine numerische IP-Adresse und verwendet diese, um die Verbindung zum Server herzustellen.

Der Client initiiert eine HTTP-Anforderung an einen Server, indem er eine GET-Anforderung an den Server sendet und nach der Datei `index.html` fragt.



Schritt 3

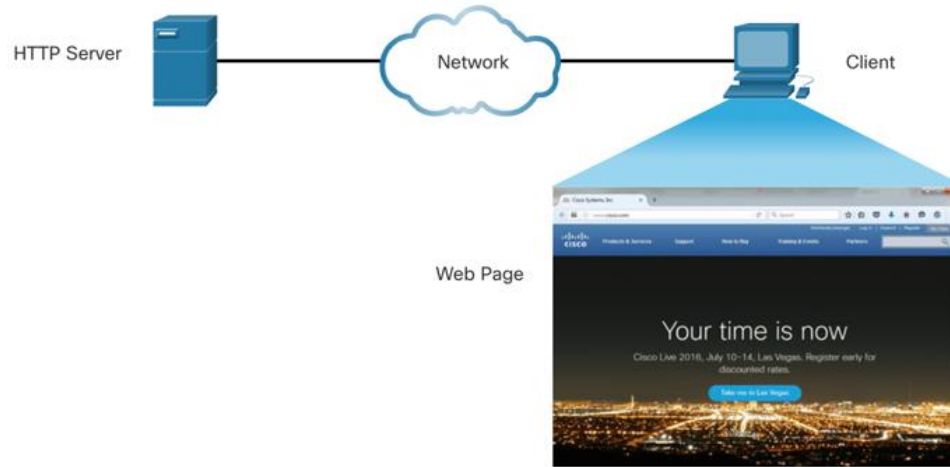
Als Antwort auf die Anfrage sendet der Server den HTML-Code für diese Webseite an den Browser.



Hypertext Transfer Protokoll und Hypertext Markup Language (Forts.)

Schritt 4

Der Browser entschlüsselt den HTML-Code und formatiert die Seite für das Browserfenster.



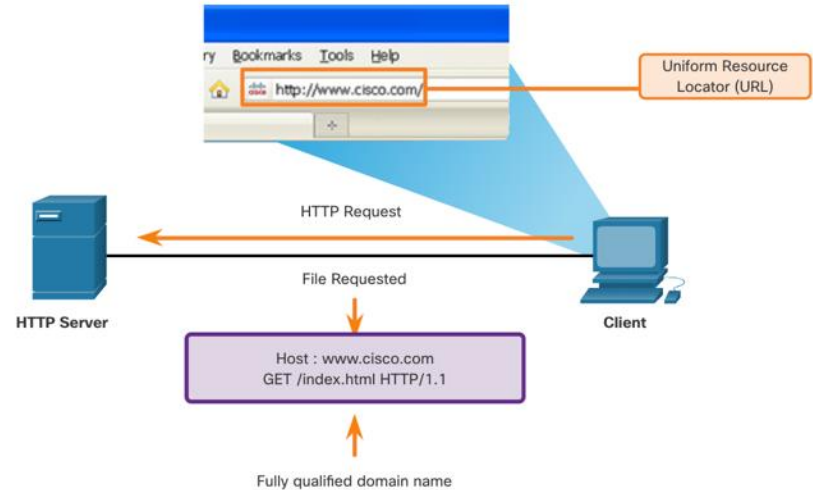
Web- und Email-Protokolle

HTTP und HTTPS

HTTP ist ein Anforderungs-/Antwortprotokoll, das die für diese Kommunikation verwendeten Nachrichtentypen angibt.

Die drei gängigsten Nachrichtentypen sind GET, POST und PUT.

- **GET** – Eine Client-Anforderung nach Daten. Ein Client (Webbrowser) sendet die GET-Nachricht an den Webserver, um HTML-Seiten anzufordern.
- **POST** - – Lädt Datendateien auf den Webserver hoch, z.B. Formulardaten.
- **PUT** - Lädt Ressourcen oder Inhalte auf den Webserver hoch, z.B. ein Bild



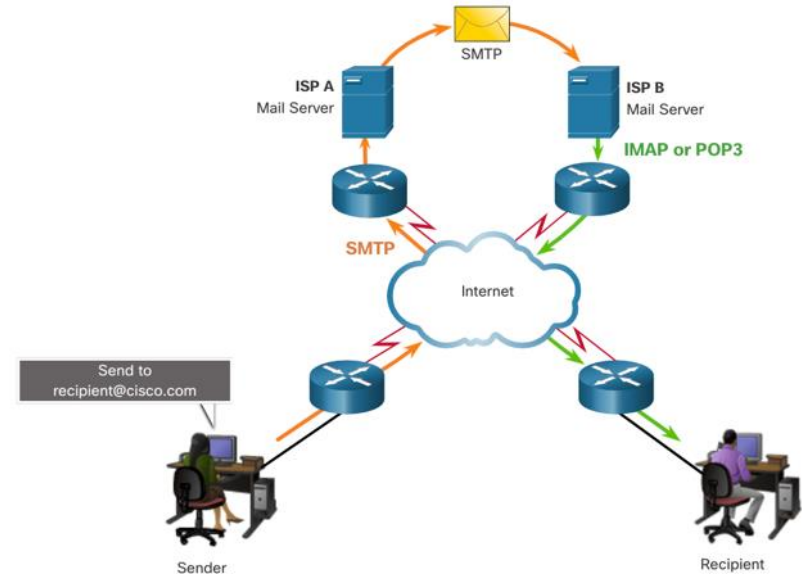
Hinweis: HTTP ist kein sicheres Protokoll. Für sichere Kommunikation, die über das Internet gesendet wird, sollte HTTPS verwendet werden.

E-Mail-Protokolle

Bei E-Mail handelt es sich um ein Store-and-Forward-Verfahren zum Senden, Speichern und Abrufen von elektronischen Nachrichten über ein Netzwerk. E-Mail-Nachrichten werden in Datenbanken auf Mail-Servern gespeichert. E-Mail-Clients kommunizieren mit Mail-Servern, um E-Mails zu senden und zu empfangen.

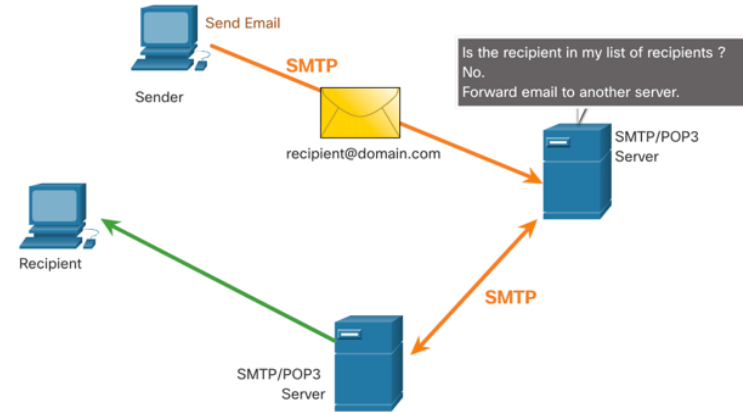
Die für den Betrieb verwendeten E-Mail-Protokolle sind:

- Simple Mail Transfer Protokoll (SMTP) – wird zum Versenden von E-Mails verwendet
- Post Office Protokoll (POP) & IMAP — wird für Clients verwendet, um Emails zu empfangen.



SMTP, POP und IMAP

- Wenn ein Client eine E-Mail sendet, stellt der Client-SMTP-Prozess eine Verbindung mit dem Server-SMTP-Prozess auf dem Well-Known-Port 25 her.
- Nach dem Herstellen der Verbindung versucht der Client, die E-Mail über die Verbindung an den Server zu senden.
- Wenn der Server die Nachricht empfängt, legt er diese entweder in einem lokalen Konto ab, falls der Empfänger ein lokaler Benutzer ist, oder leitet die Nachricht zur Zustellung an einen anderen Mail-Server weiter.
- Beim Senden von Email-Nachrichten ist der Ziel-E-Mail-Server möglicherweise offline oder ausgelastet. Für diesen Fall reiht SMTP die zu versendenden Nachrichten in eine Warteschlange (Spooler) ein, um sie zu einem späteren Zeitpunkt zu senden.

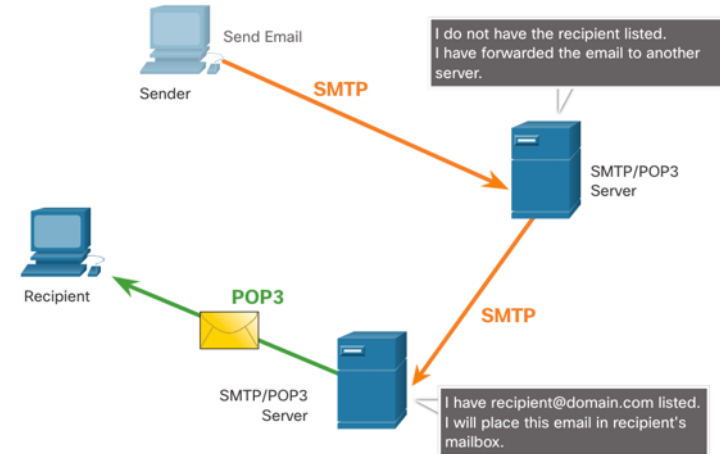


Hinweis: SMTP-Nachrichtenformate erfordern eine Nachrichtenkopfeile (Empfänger-E-Mail-Adresse und Absender-E-Mail-Adresse) und einen Nachrichtentext.

SMTP, POP und IMAP (Fortsetzung)

POP wird von einer Anwendung verwendet, um E-Mails von einem Mail-Server abzurufen. Bei POP wird E-Mail vom Server auf den Client heruntergeladen und dann auf dem Server gelöscht.

- Der Server startet den POP-Dienst, indem er den TCP-Port 110 passiv auf Client-Verbindungsanforderungen abhört.
- Wenn ein Client den Dienst nutzen möchte, sendet er eine Anforderung zum Aufbau einer TCP-Verbindung mit dem Server.
- Wenn die Verbindung hergestellt wurde, sendet der POP-Server eine Begrüßungsnachricht.
- Der Client und der POP-Server tauschen dann Befehle und Antworten aus, bis die Verbindung geschlossen oder abgebrochen

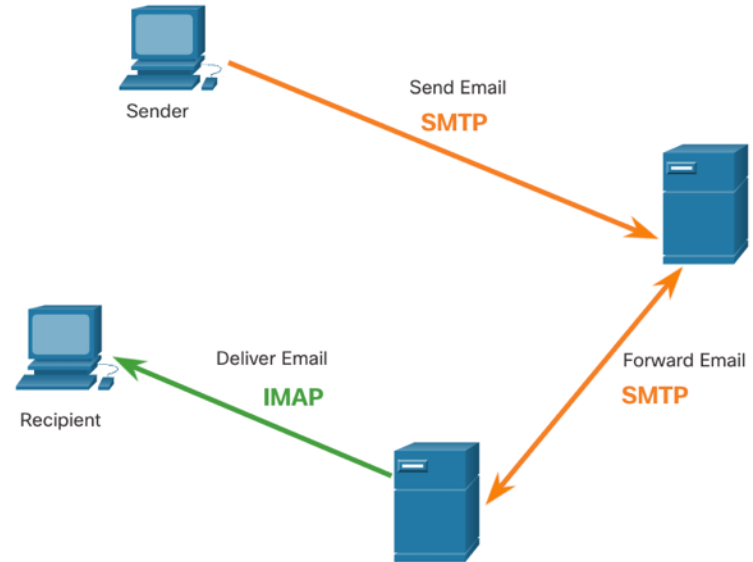


Da POP keine Nachrichten speichert, ist das Protokoll für kleine und mittlere Unternehmen, die eine zentrale Backup-Lösung benötigen, nicht empfohlen.

SMTP, POP und IMAP (Fortsetzung)

IMAP ist ein weiteres Protokoll, das eine Methode zum Abrufen von E-Mail-Nachrichten beschreibt.

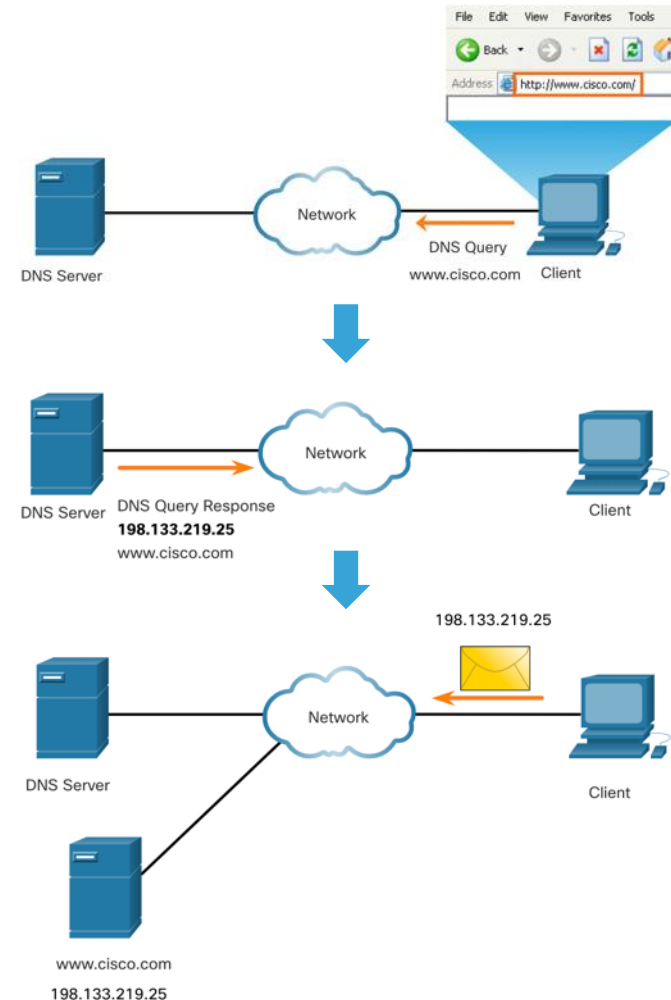
- Im Gegensatz zu POP werden Kopien der Nachrichten in die Client-Anwendung heruntergeladen, wenn der Benutzer eine Verbindung mit einem IMAP-fähigen Server herstellt. Die ursprünglichen Nachrichten werden auf dem Server gespeichert, bis sie manuell gelöscht werden.
- Wenn sich ein Benutzer dazu entschließt, eine Nachricht zu löschen, synchronisiert der Server diese Aktion und die Nachricht wird vom Server gelöscht.



15.4 IP-Adressendienste

Domännennamensdienst

- Domännennamen wurden entwickelt, um die numerische Adresse in einen einfachen wiedererkennbaren Namen zu konvertieren.
- Vollqualifizierte Domännennamen (FQDNs), wie `http://www.cisco.com`, sind für Menschen viel einfacher zu merken als `198.133.219.25`.
- Das DNS-Protokoll definiert einen automatisierten Dienst, der die erforderliche numerische Netzwerkadresse für einen Ressourcennamen ermittelt. Dies schließt das Format für Abfragen, Antworten und Daten mit ein.



DNS-Nachrichtenformat

Der DNS-Server speichert verschiedene Arten von Ressourcendatensätzen, die zur Namensauflösung verwendet werden. Diese Datensätze enthalten den Namen, die Adresse und den Datensatztyp.

Einige dieser Datensatztypen sind wie folgt:

- **A** - Die IPv4-Adresse eines Endgeräts.
- **NS** - Ein autoritativer Namensserver
- **AAAA** - Die IPv6-Adresse eines Endgeräts (ausgesprochen „Quad-A“)
- **MX** - Ein Mail-Exchange-Datensatz

Wenn der Client eine Abfrage durchführt, überprüft der DNS-Prozess des Servers zuerst seine eigenen Datensätze, um den Namen aufzulösen. Wenn er den Namen mithilfe seiner gespeicherten Datensätze nicht auflösen kann, kontaktiert er andere Server für die Namensauflösung.

Wenn eine Übereinstimmung gefunden und an den ursprünglichen abfragenden Server zurückgesendet wurde, speichert der Server die numerische Adresse vorübergehend, für den Fall, dass derselbe Namen erneut angefordert wird.

DNS-Nachrichtenformat (Fortsetzung)

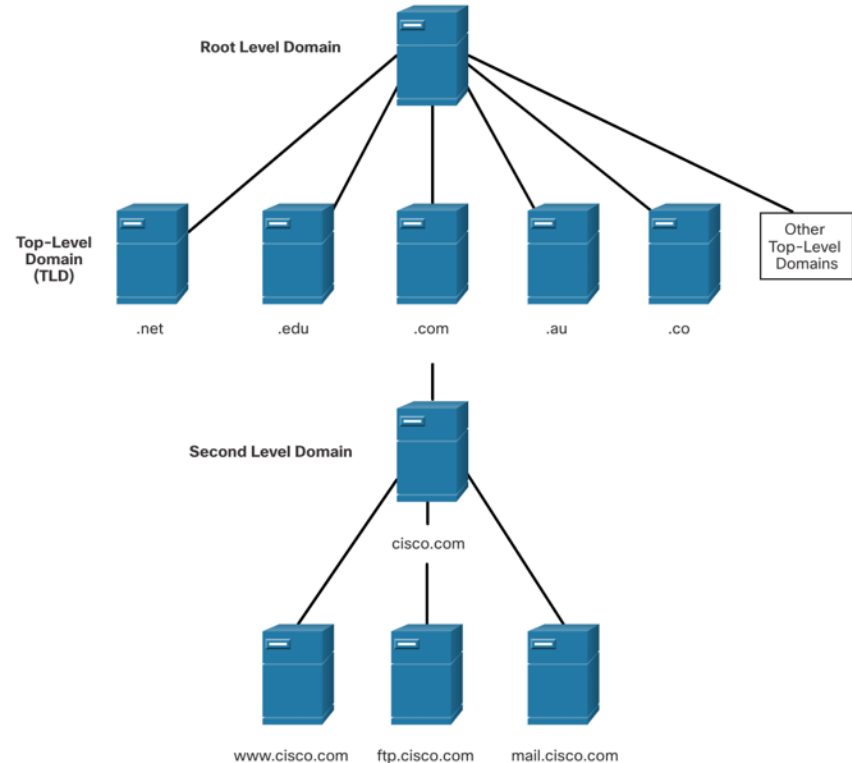
Das DNS-Protokoll verwendet bei der Server-Kommunikation dasselbe Nachrichtenformat, bestehend aus Frage, Antwort, Autorität und zusätzliche Informationen für alle Client-Abfragen und Server-Antworten, Fehlermeldungen und die Übertragung der Ressourcendatensatz-Informationen.

DNS-Nachrichtenabschnitt	Beschreibung
Frage	Die Frage für den Namensserver
Annehmen	Ressourceneinträge zur Beantwortung der Frage
Stelle	Ressourceneinträge, die auf eine Autorität verweisen
zusätzliche	Ressourceneinträge, die weitere Informationen enthalten

IP-Adressierungsdienste

DNS-Hierarchie

- Das DNS-Protokoll verwendet ein hierarchisches System, um eine Datenbank für die Namensauflösung zu erstellen.
- Jeder DNS-Server pflegt eine spezifische Datenbankdatei und ist nur für die Verwaltung der Zuordnung zwischen Namen und IP-Adressen in diesem kleinen Teil der gesamten DNS-Struktur verantwortlich.
- Wenn ein DNS-Server eine Anforderung für eine Namensübersetzung erhält, die nicht seine DNS-Zone betrifft, leitet er die Anforderung zur Übersetzung an einen anderen DNS-Server mit der richtigen Zone weiter.
- Beispiele für Top-Level-Domänen sind wie folgt:
 - **.com**- Ein Unternehmen oder eine Branche
 - **.org** - Eine gemeinnützige Organisation
 - **.au** - Australien



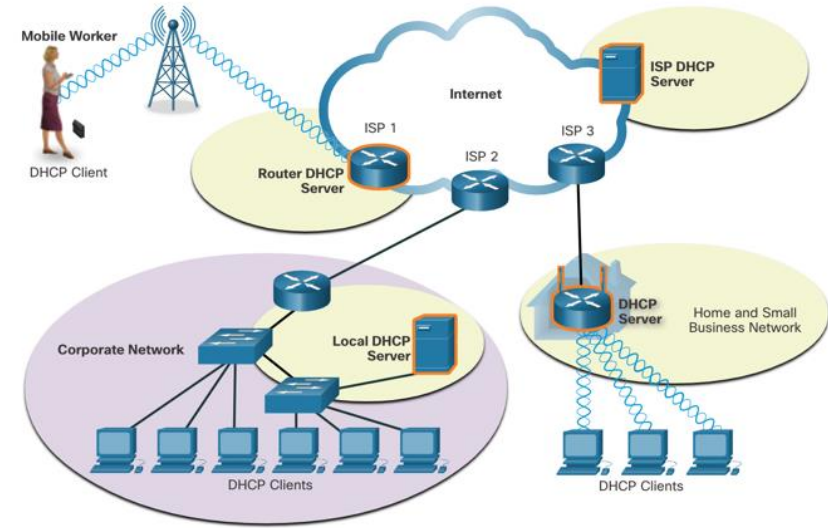
Der Befehl nslookup

- Computer-Betriebssysteme verfügen zudem über ein Dienstprogramm mit der Bezeichnung „nslookup“, mit dem der Benutzer die Namensserver manuell abfragen kann, um einen bestimmten Hostnamen aufzulösen.
- Dieses Dienstprogramm kann auch verwendet werden, um Probleme bei der Namensauflösung zu beheben und den aktuellen Status der Namensserver zu überprüfen.
- Wie in Abbildung1 gezeigt, wird der für Ihren Host konfigurierte Standard-DNS-Server angezeigt, wenn der **nslookup**-Befehl ausgegeben wird.
- Der Name eines Hosts oder einer Domäne kann an der **nslookup**-Eingabeaufforderung eingegeben werden.

```
C:\Users> nslookup
Default Server:  dns-sj.cisco.com
Address:  171.70.168.183
> www.cisco.com
Server:  dns-sj.cisco.com
Address:  171.70.168.183
Name:  origin-www.cisco.com
Addresses:  2001:420:1101:1::a
           173.37.145.84
Aliases:  www.cisco.com
> cisco.netacad.net
Server:  dns-sj.cisco.com
Address:  171.70.168.183
Name:  cisco.netacad.net
Address:  72.163.6.223
>
```

Dynamic Host Configuration Protocol

- Das Dynamic Host Configuration Protocol (DHCP) für den IPv4-Dienst automatisiert die Zuweisung von IPv4-Adressen, Subnetzmasken, Gateways und anderen IPv4-Netzwerkparametern.
- DHCP gilt als dynamische Adressierung im Vergleich zur statischen Adressierung. Bei der statischen Adressierung werden IP-Adressinformationen manuell eingegeben.
- Wenn ein Host eine Verbindung mit dem Netzwerk herstellt, wird der DHCP-Server kontaktiert und eine Adresse wird angefordert. Der DHCP-Server wählt eine Adresse aus einem konfigurierten Adressbereich, dem sogenannten Pool, aus und weist sie dem Host zu (least sie).
- Viele Netzwerke verwenden sowohl DHCP als auch statische Adressierung. DHCP wird für allgemeine Hosts wie Endbenutzergeräte verwendet. Die statische Adressierung wird für Netzwerkgeräte wie Gateway-Router, Switches, Server und Drucker verwendet.



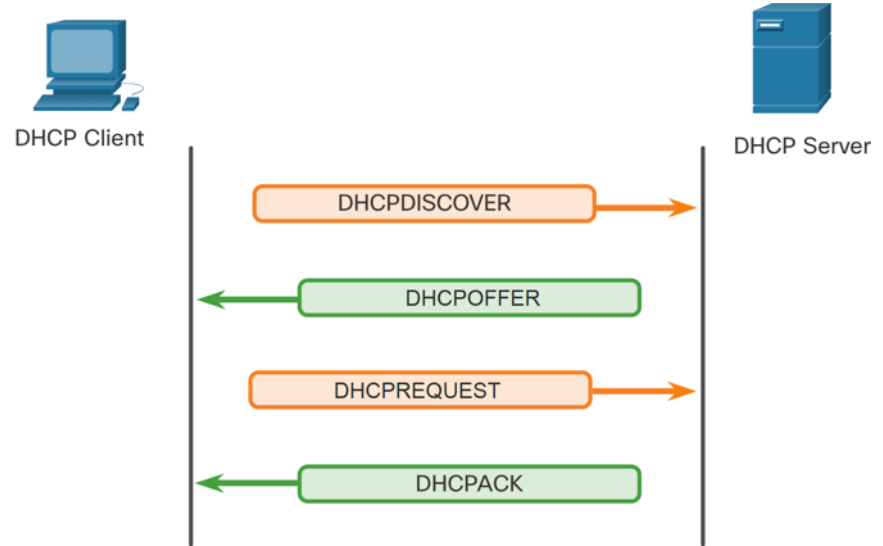
Hinweis: DHCP für IPv6 (DHCPv6) bietet ähnliche Dienste für IPv6-Clients. Jedoch stellt DHCPv6 keine Standard-Gatewayadresse bereit. Diese kann nur dynamisch von der Router Advertisement (RA)-Nachricht des Routers bezogen werden.

IP-Adressierungsdienste

DHCP-Betrieb

Der DHCP-Prozess:

- Wenn ein DHCP-konfiguriertes IPv4-Gerät bootet oder eine Verbindung mit dem Netzwerk herstellt, sendet der Client ein DHCP discover (DHCPDISCOVER), um alle verfügbaren DHCP-Server im Netzwerk zu identifizieren.
- Ein DHCP-Server antwortet mit einer DHCP-Offer-Nachricht (DHCPOFFER), in der dem Client ein Lease angeboten wird. (Wenn ein Client aufgrund mehrerer DHCP-Server im Netzwerk mehrere Angebote erhält, muss er eines auswählen.)
- Der Client sendet eine DHCP-Anforderungsnachricht (DHCPREQUEST), die den genauen Server und das genaue Lease-Angebot identifiziert, der bzw. das vom Client akzeptiert wird.
- Der Server gibt dann eine DHCP-Bestätigungsmeldung (DHCPACK) zurück, die dem Client bestätigt, dass die Lease abgeschlossen wurde.
- Wenn das Angebot nicht mehr gültig ist, antwortet der ausgewählte Server mit einer negativen DHCP-Negativ-Bestätigungsnachricht (DHCPNAK) und der Prozess muss mit einer DHCPDISCOVER Nachricht beginnen.



Hinweis: DHCPv6 verfügt über eine Reihe von Nachrichten, die denen für DHCPv4 ähneln. Die DHCPv6-Nachrichten sind SOLICIT, ADVERTISE, INFORMATION REQUEST und REPLY

Lab — DNS-Auflösung beachten

Mit dieser Übung können Sie die folgenden Lernziele erreichen:

- Anzeigen der DNS-Umwandlung einer URL in eine IP-Adresse
- Anzeigen des DNS-Lookups mithilfe des Befehls **nslookup** auf einer Website
- Anzeigen des DNS-Lookups mithilfe des Befehls **nslookup** auf Mail-Servern

15.5 Dateifreigabedienste

Datenübertragungsprotokoll

FTP wurde entwickelt, um Datenübertragungen zwischen einem Client und einem Server zu ermöglichen. Ein FTP-Client ist eine Anwendung, die auf einem Computer ausgeführt wird, um Daten auf einen FTP-Server hoch- oder von diesem herunterzuladen.



1. Control Connection:

Client opens first connection to the server for control traffic.



2. Data Connection:

Client opens second connection for data traffic.



Schritt 1 - Der Client stellt die erste Verbindung zum Server für Steuerungsverkehr her. Hierfür wird TCP-Port 21 verwendet. Der Datenverkehr besteht aus Clientbefehlen und Serverantworten.

Schritt 2 - Der Client stellt die zweite Verbindung zum Server für die eigentliche Datenübertragung her. Hierfür wird TCP-Port 20 verwendet. Diese Verbindung wird jedes Mal eingerichtet, wenn Daten übertragen werden sollen.

Schritt 3 - Die Datenübertragung kann in beide Richtungen erfolgen. Der Client kann Daten vom Server herunterladen (pull) oder auf den Server hochladen (push).

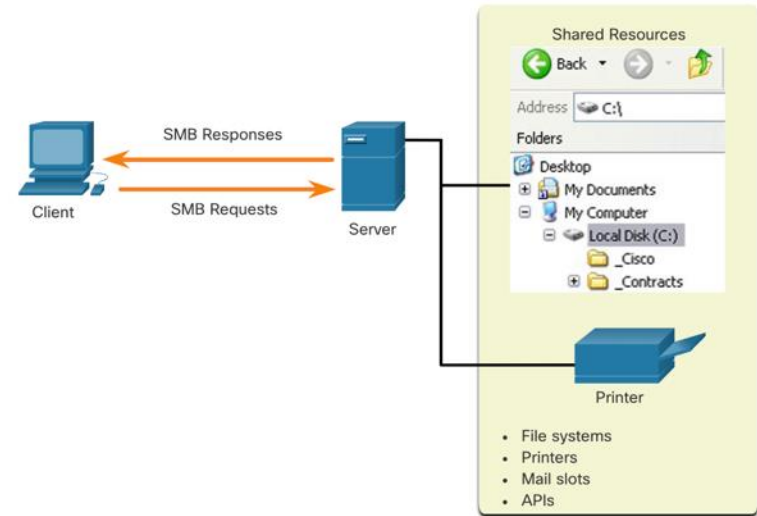
Dateifreigabe-Servernachrichtenblock

Der Server Message Block (SMB) ist ein Client/Server, Request-Response-Dateifreigabeprotokoll. Server können ihre eigenen Ressourcen über das Netzwerk für die Clients verfügbar machen.

Drei Funktionen von SMB-Nachrichten:

- Sitzungen starten, authentifizieren und beenden.
- den Datei- und Druckerzugriff steuern.
- einer Anwendung das Senden oder Empfangen von Nachrichten an oder von einem Gerät ermöglichen.

Anders als bei der von FTP unterstützten Dateifreigabe stellen Clients eine langfristige Server-Verbindung her. Wenn die Verbindung hergestellt wurde, kann der Benutzer des Clients auf die Ressourcen des Servers zugreifen, als ob diese lokal auf dem Client-Host vorhanden wären.



15.6 Modul Praxis und Quiz

Was habe ich in diesem Modul gelernt?

- Die Protokolle der Anwendungsschicht dienen dazu, Daten zwischen Programmen auszutauschen, die auf den Quell- und Ziel-Hosts ausgeführt werden. Die Präsentationsebene verfügt über drei Hauptfunktionen: Formatieren oder Präsentieren von Daten, Komprimieren von Daten und Verschlüsselung von Daten für die Übertragung und Entschlüsselung von Daten nach Erhalt. Die Sitzungsschicht erstellt und verwaltet Dialoge zwischen Quell- und Zielanwendungen.
- Im Client-Server-Modell wird das Gerät, das Informationen anfordert, als Client, und das Gerät, das auf die Anforderung reagiert, als Server bezeichnet.
- In einem P2P-Netzwerk sind zwei oder mehrere Computer über ein Netzwerk verbunden und können Ressourcen gemeinsam nutzen, ohne dabei einen dedizierten Server zu verwenden.
- Die drei gängigsten HTTP Nachrichtentypen sind GET, POST und PUT.
- E-Mail unterstützt drei separate Protokolle für den Betrieb: SMTP, POP und IMAP.
- Das DNS-Protokoll ermittelt die erforderliche numerische Netzwerkadresse für einen Ressourcennamen.
- DHCP für den IPv4-Dienst automatisiert die Zuweisung von IPv4-Adressen, Subnetzmasken, Gateways und anderen IPv4-Netzwerkparametern. Die DHCPv6-Nachrichten sind SOLICIT, ADVERTISE, INFORMATION REQUEST und REPLY
- Ein FTP-Client ist eine Anwendung, die auf einem Computer ausgeführt wird, um Daten auf einen FTP-Server hoch- oder von diesem herunterzuladen.
- Drei Funktionen von SMB-Nachrichten: Starten, Authentifizieren und Beenden von Sitzungen, Steuern des Datei- und Druckerzugriffs und einer Anwendung das Senden oder Empfangen von Nachrichten an oder von einem anderen Gerät erlauben.

