Bevezetés a hálózatok világába

Alkalmazási réteg

OSI és TCP/IP-modellek felelevenítése

A hálózati szakemberek mind szóban, mind pedig az írott műszaki dokumentációban az OSI és a TCP/IP modelleket egyaránt alkalmazzák (lásd ábra). Ezeket a modelleket használhatják a protokollok és az alkalmazások viselkedésének leírására.

Az OSI-modellben az adat rétegről-rétegre halad, elindulva a forrásállomás alkalmazási rétegéből, haladva lefelé a hierarchiában a fizikai rétegig, át a kommunikációs csatornán egészen a célállomásig, ahol aztán elindul felfelé a hierarchiában egészen az alkalmazási rétegig.

Az alkalmazási réteg mind az OSI mind a TCP/IP-modellnek a legfelső rétege. A TCP/IP-modell alkalmazási rétege számos, a végfelhasználói alkalmazások szolgáltatásaihoz szükséges protokollt tartalmaz. A TCP/IP alkalmazási rétegbeli protokolljainak funkciói nagyjából az OSI-modell felső három rétegének, az alkalmazási-, megjelenítési- és viszonyrétegnek felelnek meg. Az alkalmazásfejlesztők és gyártók az OSI-modell 5., 6. és 7. rétegére hivatkoznak hálózati hozzáférést igénylő termékeik, pl. egy web böngésző kapcsán.

Az alkalmazási réteg

A végfelhasználóhoz az alkalmazási réteg van a legközelebb. Ahogy azt az ábra is mutatja, ez az a réteg, amely az interfészt biztosítja az általunk kommunikációra használt alkalmazások és a mögöttes hálózat között, amelyen üzeneteink továbbítódnak. Az alkalmazási rétegbeli protokollokat a forrás- és célállomásokon futó programok közötti adatcserére használjuk. Számos alkalmazási rétegbeli protokoll létezik, és mindig vannak új, fejlesztés alatt álló protokollok is. A legismertebb alkalmazási rétegbeli protokollok a HTTP (Hypertext Transfer Protocol), az FTP (File Transfer Protocol), a TFTP (Trivial File Transfer Protocol), az IMAP (Internet Message Access Protocol) és a DNS (Domain Name System) protokoll.

A megjelenítési réteg

A megjelenítési rétegnek három fő funkciója van:

- Megjeleníti a forrásállomásról származó adatokat, vagy átalakítja azokat a célállomás által igényelt formára.
- Tömöríti az adatokat egy a célállomás által kitömöríthető formátumban.
- Titkosítja az adatokat az átvitelhez, valamint a célállomáson visszafejti azokat.

Amint az ábrán látható, a megjelenítési réteg az alkalmazási réteg adatait alakítja át, valamint határozza meg az egyes fájlformátumokra vonatkozó szabványokat. Az ismertebb videó szabványok közé tartozik a QuickTime és az MPEG (Motion Picture Experts Group). A QuickTime egy videóra és hangra vonatkozó Apple Computer által jegyzett szabvány, míg az MPEG szintén egy videó- és hangtömörítésre, valamint kódolásra szolgáló formátum.

A hálózatokon használt ismertebb grafikus képformátumok közé tartozik a GIF (Graphics Interchange Format), a JPEG (Joint Photographic Experts Group) és a PNG (Portable Network Graphics). A GIF és a

JPEG rasztergrafikus képek tömörítésére és kódolására szolgáló szabványok. A PNG-t a GIF formátum bizonyos korlátainak kiküszöbölésére, majd végül a formátum lecserélésére tervezték.

A viszonyréteg

Ahogy a neve is utal rá, a viszonyréteg feladatai a forrás- és célalkalmazások közötti párbeszédek (munkamenetek) létrehozása és fenntartása. A viszonyréteg kezeli a párbeszédek kialakításához, fenntartásához, valamint a megszakadó vagy hosszabb ideje tétlen viszonyok újraindításához szükséges információcserét.

TCP/IP alkalmazási rétegbeli protokollok

Míg az OSI-modell megkülönbözteti az alkalmazási-, megjelenítési- és viszony funkciókat, addig a széles körben ismert és használt TCP/IP-alapú alkalmazások egyesítik a három réteg funkcionalitását.

A TCP/IP alkalmazási protokolljai számos népszerű internetes kommunikációs szolgáltatás formátumát és vezérlőinformációit határozzák meg. Ezen TCP/IP-protokollok közé tartoznak az alábbiak:

- Tartománynév-kezelő rendszer (Domain Name System, DNS) - Ez a protokoll az internetes nevek IP-címekhez történő hozzárendelését végzi.
- Telnet - Szerverekhez és hálózati eszközökhöz való távoli hozzáférésre használjuk.
- Egyszerű levéltovábbító protokoll (Simple Mail Transfer Protocol, SMTP) - Ez a protokoll e-mail üzeneteket és csatolmányokat továbbít.
- Dinamikus állomáskonfiguráló protokoll (Dynamic Host Configuration Protocol, DHCP) - A protokollt arra használjuk, hogy egy állomáshoz IP-címet, alhálózati maszkot, alapértelmezett átjárót és DNS szervert rendeljünk.
- Hiperszöveg továbbító protokoll (Hypertext Transfer Protocol, HTTP) - Ez a protokoll a világháló weboldalait felépítő fájlokat továbbítja.
- Fájlátviteli protokoll (File Transfer Protocol, FTP) - A protokollt rendszerek közötti interaktív fájlátvitelre használjuk.
- Fájlátviteli protokoll (File Transfer Protocol, FTP) - Ezt a protokollt kapcsolat nélküli aktív fájlátvitelre használjuk.
- Rendszerbetöltő protokoll (Bootstrap Protocol, BOOTP) - Ez a protokoll a DHCP protokoll előfutára. A BOOTP egy hálózati protokoll, amelyet a rendszerindítás során az IP-címzési információk megszerzésére használunk.
- Postahivatal protokoll (Post Office Protocol, POP) - A protokollt a levelezőkliensek az e-mailek távoli szerverről történő letöltésére használják.
- Internetes levélhozzáférési protokoll (Internet Message Access Protocol, IMAP) - Ez egy másik, szintén a levelek letöltését szolgáló protokoll.

A kommunikációs folyamat során az alkalmazási rétegbeli protokollokat mind a forrás-, mind pedig a célállomás egyaránt használja. Hogy a kommunikáció sikeres legyen, a forrás- és célállomásokon használt alkalmazási rétegbeli protokolloknak egymással kompatibilisnek kell lenniük.

Egyenrangú (Peer-to-peer) hálózatok

Amikor egy hálózati eszközön - legyen az PC, laptop, tablet, okostelefon vagy bármilyen más hálózatra csatlakoztatott eszköz - hozzáférünk valamilyen információhoz, akkor nem biztos, hogy az fizikailag is az adott eszközön van tárolva. Ebben az esetben az információ eléréséhez egy kérést kell küldeni az adatokat tároló eszköznek. Az egyenrangú (P2P, peer-to-peer) hálózati modellben az adatok elérése dedikált szerver használata nélkül, egy társ eszközről (peer) történik.

A P2P hálózati modell két részre bontható: P2P-hálózatokra és P2P-alkalmazásokra. Mindkét résznek hasonlók a tulajdonságaik, de a gyakorlatban egészen másként működnek.

P2P-hálózatok

Egy P2P-hálózatban két vagy több számítógép csatlakozik egymáshoz a hálózaton keresztül úgy, hogy dedikált szerver nélkül oszthatják meg egymás között az erőforrásaikat (pl. nyomtatókat vagy fájlokat). Minden csatlakoztatott végberendezés (más néven peer) működhet szerverként és kliensként is egyben. Egy számítógép az egyik adatátviteli folyamatban betöltheti a szerver szerepkörét, míg egy másikban ezzel egyidejűleg kliens is lehet. A szerver és a kliens szerepköröket az egyes kérések határozzák meg.

Példa lehet erre egy egyszerű otthoni hálózat két számítógéppel, ahogy az az ábrán is látható. A példában Peer2-nek van egy hozzá USB-n közvetlenül csatlakoztatott nyomtatója és be van állítva a hálózati megosztása úgy, hogy azon Peer1 tudjon nyomtatni. Peer1 pedig egy meghajtó vagy egy mappa hálózati megosztására van beállítva. Ez Peer2-nek lehetővé teszi a megosztott mappához való hozzáférést és abba fájlok mentését. Egy ilyen hálózat a fájlok megosztásán kívül a felhasználóknak a hálózati játékok használatát, vagy egy internetkapcsolat megosztását is biztosíthatja.

A P2P-hálózatok decentralizálják a hálózat erőforrásait. Az adatok dedikált szerverek helyett bárhol és bármely csatlakoztatott eszközön megoszthatók. A legtöbb mai operációs rendszer további szerverszoftver igénye nélkül támogatja a fájl- és nyomtatómegosztást. A P2P-hálózatok a jogosultságok kezelésére nem alkalmaznak központosított felhasználói fiókokat vagy hozzáférési szervereket. Ezért a néhány számítógépnél többet tartalmazó hálózatok esetében is már bonyolult lehet a biztonsági és a hozzáférési házirendek érvényre juttatása. A felhasználói fiókokat és a hozzáférési jogosultságokat az egyes eszközön egyedileg kell beállítani.

Peer-to-Peer alkalmazások

Egy peer-to-peer (P2P) alkalmazás lehetővé teszi, hogy egy eszköz ugyanabban a kommunikációban egyszerre kliens és szerver is lehessen (lásd ábra). Ebben a modellben minden kliens szerver is és minden szerver kliens is egyben. Mindkettő kezdeményezhet kommunikációt és a kommunikációs folyamatban egyenrangúnak tekintendők. A P2P-alkalmazások megkövetelik azonban, hogy minden végberendezés biztosítson egy felhasználói felületet és egy háttérszolgáltatást is futtasson. Amikor elindítunk egy adott P2P-alkalmazást, az betölti a szükséges felhasználói felületet és a háttérszolgáltatásokat, majd ezt követően az eszközök már közvetlenül tudnak egymással kommunikálni.

Bizonyos P2P-alkalmazások úgynevezett hibrid rendszert használnak, ahol az erőforrások megosztása ugyan decentralizált, de az erőforrások helyeire mutató indexeket már egy központi címtárban tárolják. A hibrid rendszerekben minden csomópont (peer) hozzáfér egy indexszerverhez, ahonnan lekérdezheti a más csomópontokon tárolt erőforrások helyét. Az indexszerver segíthet a két csomópont összekapcsolásában, de azt követően a csomópontok közötti kommunikáció már a szervertől függetlenül zajlik.

P2P-alkalmazásokat használhatunk P2P-hálózatokban, kliens-szerver hálózatokban és az interneten

keresztül is.

Gyakori P2P-alkalmazások

P2P-alkalmazást használva a hálózat valamennyi számítógépe kliensként és szerverként is szolgálhat a hálózat azon többi számítógépe számára, amelyek ugyanazt az alkalmazást futtatják. Az ismertebb P2P-alkalmazások közé tartoznak a következők:

- eDonkey
- eMule
- Shareaza
- BitTorrent
- Bitcoin
- LionShare

Bizonyos P2P alkalmazások a Gnutella protokollra épülnek. A Gnutella lehetővé teszi felhasználóinak, hogy megosszák egymással a merevlemezeiken lévő fájlokat. Amint az az ábrán is látható, egy Gnutella kompatibilis kliensszoftver lehetővé teszi a felhasználóknak, hogy az interneten Gnutella szolgáltatásokhoz kapcsolódjanak, és más Gnutella csomópontok által megosztott állományokat találjanak meg és érjenek el. A Gnutella hálózat elérésére számos kliensalkalmazás létezik, közöttük a BearShare, a Gnucleus, a LimeWire, a Morpheus, a WinMX és a XoloX.

Míg az alapprotokollt a Gnutella Fejlesztői Fórum (Gnutella Developer Forum) gondozza, addig az alkalmazásforgalmazók gyakran fejlesztenek hozzá kiterjesztéseket, hogy a protokollt az alkalmazásaikba illeszthessék.

Számos P2P alkalmazás nem használ központi adatbázist, valamennyi fájlt a peer-ek tartanak nyilván. Lekérdezésre a hálózat valamennyi eszköze elmondja a többieknek, hogy rajta keresztül mely fájlok érhetők el, majd a fájlmegosztó protokollt és a szolgáltatásokat használják az állományok megkeresésére.

Kliens-szerver modell

A kliens-szerver modellben az információt kérő eszközt kliensnek, a kérésre válaszoló eszközt pedig szervernek vagy kiszolgálónak nevezzük. A kliens- és szerverfolyamatokat az alkalmazási réteghez soroljuk. A párbeszédet a kliens kezdeményezi azzal, hogy adatokat kér a szervertől, amely aztán a kliensnek egy vagy több adatfolyam elküldésével válaszol. A kliensek és szerverek közötti kérések és válaszok formátumát az alkalmazási rétegbeli protokollok határozzák meg. A tényleges adatátvitel mellett ez a párbeszéd a felhasználó hitelesítését, valamint az átvitt adatfájl azonosítását is megkövetelheti.

A kliens-szerver hálózat egy példája, amikor egy ISP e-mail szolgáltatását használjuk levelek küldésére, fogadására és tárolására. Egy otthoni számítógépen lévő levelezőkliens egy kérést intéz az ISP levelezőszerveréhez egy olvasatlan levélért. A szerver ezután a válaszüzenetében elküldi a kért levelet a kliensnek.

Bár az adatok általában a szerverről áramlanak a kliens felé, bizonyos adatok mindig a kliens felől haladnak a szerver irányába. Az adatáramlás lehet mindkét irányban lehet egyenlő mértékű, de lehet akár nagyobb is a klienstől a szerver irányába. A kliens például tárolási célból átmásolhat egy fájlt a

szerverre. Ahogy az ábra is mutatja, a kliensről a szerverre történő adatátvitelt feltöltésnek (upload), míg a szerverről a kliensre történőt letöltésnek (download) nevezzük.

Alkalmazási rétegbeli protokollok feleleventése

Több tucat alkalmazási rétegbeli protokoll létezik, de egy átlagos napon talán csak ha ötöt vagy hatot használunk. Három olyan alkalmazási rétegbeli protokoll van, amelyek a mindennapi munkánkat vagy játékainkat biztosítják:

- Hiperszöveg továbbító protokoll (Hypertext Transfer Protocol, HTTP)
- Egyszerű levéltovábbító protokoll (Simple Mail Transfer Protocol, SMTP)
- Postahivatal protokoll (Post Office Protocol, POP)

Ezek az alkalmazási rétegbeli protokollok teszik lehetővé a világháló böngészését, valamint az e-mailek küldését és fogadását. A HTTP-t internetes weboldalakhoz való kapcsolódásra használjuk. Az SMTP e-mailek küldését teszi lehetővé. A POP pedig az e-mailek fogadására szolgál.

A következő néhány oldal erre a három alkalmazási rétegbeli protokollra fókuszál.

Hiperszöveg átviteli protokoll (HTTP) és hiperszöveg leíró nyelv (HTML)

Amikor egy webcímet vagy URL-t (Uniform Resource Locator) begépelünk egy webböngészőbe, a böngésző a HTTP-protokollt használva építi ki a kapcsolatot a szerveren futó web-szolgáltatással. Az URL-ek azok az egységes erőforrás-azonosító (URI, Uniform Resource Identifier) nevek, amelyeket a legtöbb ember a webcímekkel társít.

A http://www.cisco.com/index.html URL egy olyan példa, amely egy meghatározott erőforrásra, az index.html nevű weboldalra hivatkozik a cisco.comnevű szerveren. Kattintsunk az ábra melletti számokra a HTTP által használt lépések megtekintéséhez!

A webböngésző a kliensalkalmazásoknak egy típusa, amelyet egy számítógép a világhálóra történő csatlakozásra, és egy webszerveren tárolt állományok elérésére használ. Mint a legtöbb szerverfolyamat, a webszerver is háttérszolgáltatásként fut és különböző típusú fájlok elérését teszi lehetővé.

A tartalom elérésére a webes kliensek kapcsolatokat alakítanak ki a szerverrel, majd kérik tőle a kívánt állományokat. A szerver a kért állománnyal válaszol, majd a böngésző értelmezi a kapott adatokat és megjeleníti a felhasználó számára.

A böngészők számos adattípust képesek értelmezni és megjeleníteni (ilyenek például az egyszerű szöveg, vagy a hiperszöveg, a nyelv melyben a weboldalakat írják). Bizonyos adattípusok ugyanakkor egyéb szolgáltatást vagy programot is igényelhetnek, amelyeket általában beépülő modulnak (plug-in) vagy kiegészítőnek (add-on) neveznek. A kapott fájl típusának megállapításában a böngészőt a szerver az állomány adattípusának meghatározásával segíti.

A webböngésző és a webszerver interakciójának jobb megértése érdekében vizsgálhatjuk meg, hogy egy oldal hogyan nyílik meg a böngészőben. A példához használjuk a http://www.cisco.com/index.html URL-t!

Ahogy az 1. ábra mutatja, a böngésző az URL három részét vizsgálja:

1. http (az alkalmazott protokoll vagy séma)

2. www.cisco.com (a szerver neve)

3. index.html (a kért fájl neve)

Ahogy a 2. ábra mutatja, a böngésző ezek után a névszerverhez fordul, hogy a www.cisco.com nevet egy numerikus címmé alakítsa át, amit majd a szerverhez történő csatlakozáshoz használ. A böngésző egy a HTTP szabványának megfelelő GET-üzenet küldésével kéri a kiszolgálótól az index.html fájl elküldését. Majd ahogy a 3. ábra mutatja, a szerver elküldi a böngészőnek az oldal HTML kódját. Végül a böngésző értelmezi a HTML kódot és megjeleníti az oldalt a böngészőablakban (lásd 4. ábra).

HTTP és HTTPS

A HTTP-t a világhálón keresztüli adatátvitelre használjuk és egyike a leggyakrabban használt alkalmazási protokolloknak. Eredetileg egyszerűen HTML oldalak közzétételére és letöltésére találták ki, ám a HTTP-t a sokoldalúsága az elosztott közösségi információs rendszerek egyik alapvető alkalmazásává tette.

A HTTP egy kérés/válasz protokoll. Amikor egy kliens, általában egy webböngésző, kérést küld a webszervernek, a kommunikációhoz HTTP-üzenettípusokat használ. A három leggyakoribb üzenettípus a GET, a POST és a PUT (lásd ábra).

A GET a kliens adatkérése. A kliens (webböngésző) egy GET-üzenetet küld a webszervernek a HTML oldalak lekérésére. Amikor a szerver megkapja a GET-kérést, egy állapotkóddal (mint például a „ HTTP/1.1 200 OK ”), valamint magával az üzenettel válaszol. A kiszolgáló üzenete lehet maga a kért HTML fájl amennyiben az elérhető, vagy tartalmazhat egy hiba-, illetve információs üzenetet, mint például „A kért oldal nem található”.

A POST és PUT-üzeneteket az adatfájlok webkiszolgálóra történő feltöltésére használjuk. Amikor egy felhasználó például kitölt egy weblapba ágyazott űrlapot (mint amikor egy megrendelést töltünk ki), a webszervernek egy POST-üzenet lesz elküldve. A felhasználó űrlapon beküldött adatait a POST-üzenet tartalmazza.

A PUT állományokat vagy egyéb tartalmakat tölt fel a webszerverre. Ha egy felhasználó például megpróbál egy fájlt vagy képet feltölteni a weboldalra, a kliens egy PUT üzenet küld a szervernek a csatolt fájllal vagy képpel.

Bár a HTTP rendkívül rugalmas, de nem egy biztonságos protokoll. A kérésüzenetek az információt kódolatlan szövegként továbbítják a szerverhez, amely így elfogható és mások által is elolvasható. A kiszolgálói válaszok, jellemzően HTML oldalak, ugyancsak titkosítatlanok.

A biztonságos internetes kommunikáció érdekében a webkiszolgáló eléréséhez vagy adatok közzétételéhez a HTTPS (HTTP Secure) protokollt használjuk. Az adatbiztonság megvalósítására a HTTPS a kliens és a szerver közötti adatforgalomra hitelesítést és titkosítást is alkalmazhat. Az adatok alkalmazási- és szállítási rétegek közötti továbbítására a HTTPS további szabályokat határoz meg. A HTTPS ugyanazt a kliens kérés és szerver válasz folyamatot használja mint a HTTP, csak a hálózati átvitelt megelőzően az adatfolyamot SSL-el (Secure Socket Layer) titkosítja. A forgalom titkosítása és visszafejtése miatt a HTTPS használata egy szerveren többletterhelést és feldolgozási időnövekedést okoz.

SMTP, POP és IMAP

Az elektronikus levelezés az ISP-k által nyújtott egyik elsődleges szolgáltatás. Egyszerűsége és

gyorsasága révén az e-mail forradalmasította az emberek kommunikációját. Az e-mail használata egy számítógépen vagy más végberendezésen különböző alkalmazásokat és szolgáltatásokat is igényel.

Az elektronikus levelezés egy tárol és továbbít (store-and-forward) módszer az üzenetek hálózaton keresztüli küldésére, tárolására és letöltésére. Az elektronikus leveleket a levelezőszervereken adatbázisokban tárolják. Az internetszolgáltatók gyakran olyan levelezőszervereket üzemeltetnek, amelyek egyszerre több előfizető fiókjait is kezelik.

A levelezőkliensek a szervereken keresztül küldik és fogadják a leveleket. Az üzeneteket egyik tartományból egy másikba történő továbbítása esetén a levelezőszerverek más levelezőszerverekkel is kapcsolatba kerülnek. Levélküldéskor a kliensek nem közvetlenül egymással kommunikálnak. Ehelyett mindkét kliens a levelezőszervert bízza meg az üzenetek továbbításával. Ez még abban az esetben is így történik, ha mindkét felhasználó ugyanabban a tartományban van.

Az levelezőkliensek az alkalmazás beállításaiban megadott levelezőszervernek küldik el az üzeneteket. Amikor a szerver megkapja az üzenetet, ellenőrzi hogy a címben szereplő tartomány megtalálható-e a helyi adatbázisában. Amennyiben nem, akkor egy DNS-kérést küld a címzett tartományért felelős levelezőszerver IP-címének meghatározására. Az e-mailt ezek után már a megfelelő szerverhez továbbítja.

Az e-mail három különböző protokollt használ a működéséhez: SMTP (Simple Mail Transfer Protocol), POP (Post Office Protocol) és IMAP (Internet Message Access Protocol). A levelet elküldő alkalmazási rétegbeli folyamat az SMTP-t használja. Ez az az eset, amikor egy kliens a szervernek, vagy egy szerver egy másik szervernek küldi az üzenetet.

Ugyanakkor a levelek letöltéséhez a kliens a POP vagy az IMAP alkalmazási rétegbeli protokollok valamelyikét használja.

Az SMTP (Simple Mail Transfer Protocol) megbízhatóan és hatékonyan továbbítja a leveleket. Az SMTP alapú alkalmazások megfelelő működéséhez a levélüzenetnek megfelelő formátumúnak kell lenni, valamint az SMTP-folyamatnak mind a kliensen, mind pedig a szerveren futnia kell.

Az SMTP üzenetformátuma egy üzenetfejlécből és egy üzenettörzsből áll. Míg az üzenet törzse tetszőleges mennyiségű szöveget tartalmazhat, addig a fejlécnek megfelelő formátumban meg kell tartalmaznia a címzett és a feladó e-mail címét. A fejléc minden más része opcionális.

Amikor egy kliens e-mailt küld, akkor az SMTP-folyamata a jól ismert 25-ös porton kapcsolódik a szerver SMTP-folyamatához. A kapcsolat létrejötte után a kliens megpróbálja a levelet elküldeni a szervernek. Amikor a szerver megkapja az üzenetet, helyi címzett esetén azt egy helyi postafiókban helyezi el, vagy további kézbesítésre egy ugyanilyen SMTP-folyamattal átadja azt egy másik szervernek.

Előfordulhat, hogy az üzenetek küldésekor a címzett levelezőszervere nem elérhető. Ilyenkor az SMTP várakoztatja az üzeneteket, hogy azokat egy későbbi időpontban elküldhesse. A szerver rendszeresen ellenőrzi, hogy vannak-e üzenetek a várakozási sorában, és megpróbálja azokat újra elküldeni. Ha az üzenet egy előre meghatározott idő lejárta után sem kézbesíthető, akkor kézbesítetlenül visszakerül a feladóhoz.

A POP (Post Office Protocol) lehetővé teszi, hogy a munkaállomások e-mailek fogadjanak egy levelezőszervertől. POP használatakor a levelek a szerverről letöltődnek a kliensre, majd törlődnek a szerverről.

A szerver a POP-szolgáltatást a kliensek kapcsolódási kéréseire várva a 110-es TCP port passzív

figyelésével indítja. Amikor a kliens a szolgáltatást igénybe kívánja venni, akkor egy kérést küld a szervernek a TCP kapcsolat felépítésére. A kapcsolat létrejötte után a POP-szerver egy üdvözlő üzenetet küld. Majd a kliens és a POP-szerver parancs- és válaszüzeneteket váltanak, amíg a kapcsolat le nem záródik, vagy meg nem szakad.

Mivel a kliensek letöltik az e-mail üzeneteket, majd azok eltávolításra kerülnek a szerverről, ezért a levelek nem egy központi helyen tárolódnak. A POP nem tárolja az üzeneteket, ezért használata nem előnyös olyan kisvállalkozások esetében, amelyeknek központosított biztonsági mentésre van szükségük.

A POP3 ugyanakkor megfelelő választás az ISP-k számára, mivel csökkenti a levelezőszervereiken kialakítandó nagyméretű tárolóterület kezelésének felelősségét.

Az IMAP (Internet Message Access Protocol) egy másik protokoll, amely ugyancsak az e-mail üzenetek letöltésére szolgál. A POP-al ellentétben, amikor a felhasználó egy IMAP-szerverhez csatlakozik, a kliensalkalmazáshoz csak az üzeneteknek egy másolata töltődik le. Az eredeti üzenetek továbbra is a szerveren maradnak, míg azokat külön le nem töröljük. A felhasználók az üzeneteknek csak a másolatát látják a levelezőprogramjukban.

A felhasználók a szerveren a levelek tárolására és rendszerezésére egy fájlhierarchiát hozhatnak létre. A fájlhierarchia másolata a levelezőkliensen is létrejön. Amikor a felhasználó egy üzenet törléséről dönt, a szerver szinkronizálja a műveletet és törli azt a szerverről is.

Kis- és középvállalkozások szempontjából számos előnye van az IMAP használatának. Az IMAP támogatja az e-mailek hosszú távú tárolását és központosított biztonsági mentéstét is. Több helyről, különböző eszközökről és különböző kliensprogramokkal is biztosítja az alkalmazottak hozzáférését e-mailjeikhez. A postafiók mappaszerkezetének megtekintése független annak elérési módjától.

Egy ISP számára az IMAP nem biztos, hogy a legmegfelelőbb választás. Költséges lehet a nagyszámú e-mail tárolásához szükséges lemezterület megvásárlása és karbantartása. Ezenkívül amennyiben az előfizetők elvárják postafiókjainak rendszeres biztonsági mentését, az tovább növelheti az ISP költségeit.

Tartománynév szolgáltatás (Domain Name Service)

Az adathálózatok eszközei a hálózaton keresztüli adatküldéséhez és fogadáshoz numerikus IP-címeket használnak. A legtöbb ember azonban nem képes megjegyezni ezeket a számokat. A numerikus címek egyszerű, megjegyezhető nevekké alakítására tartományneveket hozták létre.

Ezek az internetes tartománynevek, mint például a http://www.cisco.com, sokkal könnyebben megjegyezhetők, mint mondjuk a 198.133.219.25, ami ennek a szervernek a tényleges numerikus címe. Ha a Cisco úgy dönt, hogy megváltoztatja a www.cisco.comnumerikus címét, azt a felhasználók nem is veszik észre, mivel a tartománynév ugyanaz marad. Az új címet egyszerűen a meglévő tartománynévhez kötik és így az elérhetőség továbbra is fennmarad. Amíg kisméretűek voltak a hálózatok, egyszerű feladat volt a címek és a hozzájuk tartozó tartománynevek egymáshoz rendelésének a karbantartása. Ahogy a hálózatok mérete és az eszközök száma növekedett, ez a kézi megoldás kezelhetetlenné vált.

A hálózatok tartományneveinek címekké fordítására a tartománynév-kezelő rendszert (Domain Name System, DNS) hozták létre. A DNS a címekhez tartozó nevek meghatározására egy elosztott szerverhálózatot használ. Kattintsunk az ábrán lévő gombokra a DNS címfeloldás lépéseinek megtekintéséhez!

A DNS-protokoll egy automatikus szolgáltatást definiál, amely erőforrásneveket társít a kért numerikus hálózati címhez. Tartalmazza még a lekérdezések, a válaszok és az adatok formátumát. A DNS-protokollra épülő kommunikációk egyetlen, üzenetnek nevezett formátumot használnak. Ezt az üzenetformátumot használják a klienslekérdezések és a szerverválaszok minden fajtájához, a hibaüzenetekhez, valamint az erőforrásrekordok szerverek közötti továbbításához.

A számok 1-től 5-ig a DNS névfeloldás lépéseit mutatják.

A DNS üzenetformátuma

Egy DNS-szerver a névfeloldást a BIND(Berkeley Internet Name Domain) vagy ahogy gyakran nevezik a névfeloldó démon (name daemon vagy named) segítségével biztosítja. A BIND-ot eredetileg a kaliforniai Berkeley Egyetem négy diákja fejlesztette ki még az 1980-as évek elején. Ahogy az az ábrán is látható, a BIND által használt üzenetformátum a legszélesebb körben alkalmazott DNS-formátum az interneten.

A DNS-szerver a nevek feloldásához különböző típusú erőforrásrekordokat tárol. Ezek a bejegyzések a rekord nevét, címét és típusát tartalmazzák.

Néhány rekordtípus a következő:

- A – Egy állomás címe.
- NS - Egy mérvadó névkiszolgáló.
- CNAME - A kanonikus név (vagy teljes tartománynév, FQDN) egy álnév (alias). Akkor alkalmazzuk, amikor egyetlen hálózati címen több szolgáltatás fut, de ugyanakkor minden szolgáltatásnak saját DNS-bejegyzése van.
- MX – Levelezőszerver rekord (Mail Exchange). Az adott tartományhoz tartozó levelezőszerverekhez rendel egy nevet.

A kliens lekérdezésére a szerver BIND-folyamata a névfeloldáshoz először saját rekordjait vizsgálja meg. Ha a tárolt rekordjai alapján nem tudja a nevet feloldani, más szerverekkel lép kapcsolatba annak meghatározásához.

A kérés számos szerveren haladhat át, ami külön időt vesz igénybe és sávszélességet emészt fel. Miután keresés eredményre vezetett, és a válasz is visszajutott az eredeti kérelmező szerverhez, az a névhez tartozó címet átmenetileg egy cache memóriában tárolja.

Ha ismét ugyanazt a nevet kérik, az első szerver már a cache memóriájában tárolt értéket használva is képes a címet visszaadni. A gyorsítótárazás csökkenti mind a DNS-lekérdezések okozta adathálózati forgalmat, valamint a hierarchiában feljebb lévő szerverek terhelését. A Windows-os PC-k DNS-kliense a névfeloldás teljesítményét úgy optimalizálja, hogy a korábban feloldott neveket a saját memóriájába is eltárolja. A ipconfig /displaydns utasítás egy Windows-os számítógép gyorsítótárának DNS-bejegyzéseit mutatja meg.

DNS-hierarchia

A DNS-protokoll a névfeloldásra egy hierarchikusan felépített adatbázist használ. A hierarchia úgy néz ki, mint egy fordított fa, tetején a gyökérrel és alatta ágakkal (lásd ábra). A hierarchiát a DNS által használt tartománynevek alkotják.

Az elnevezési struktúra kisebb, könnyen kezelhető zónákra lett osztva. Minden DNS-szerver egy

meghatározott adatbázisfájlt tart karban, és a teljes DNS-struktúra csak egy kis részének név-IP-cím hozzárendeléséért felelős. Amikor egy DNS-szerver egy olyan névfeloldási kérést kap, amely nincs benne a zónájában, akkor azt a szerver egy másik, a megfelelő zónához tartozó DNS-szerverhez továbbítja.

Megjegyzés: A DNS jól méretezhető, mivel az állomásnevek feloldása számos szerver között oszlik meg.

A legfelső szintű tartományok a szervezet típusát vagy a származási országot jelölik. Példák a legmagasabb szintű tartományokra:

- .hu - Magyarország
- .co - Kolumbia
- .com - kereskedelem vagy ipar
- .jp - Japán
- .org - egy non-profit szervezet

A legfelső szintű tartományok után a második szintű tartománynevek következnek, azok alatt pedig az egyéb alacsonyabb szintű tartományok vannak. Minden tartománynév egy a gyökértől kiinduló lefelé vezető út ebben a fordított fában. Ahogy az ábra példája mutatja, a gyökér (root) DNS-szerver nem feltétlenül tudja, hogy a mail.cisco.com levelezőszerver rekordja hol van tárolva, de fenntart egy rekordot a .com legfelső szintű tartományhoz. Hasonlóképpen a .com tartományba tartozó szerverek nem biztos hogy rendelkeznek a mail.cisco.com rekorddal, de van egy bejegyzésük a cisco.com tartományhoz. A cisco.com tartományba tartozó szervereknek pedig már van egy rekordjuk (egész pontosan egy MX rekordjuk) a mail.cisco.com-ra.

A DNS az erőforrásrekordok decentralizált szerverek hierarchiáján történő tárolására és karbantartására épül. Az erőforrásrekordok a szerver által feloldani képes tartományneveket és a kérések feldolgozásának további szervereit tartalmazzák. Ha egy szervernek a tartományhierarchia szintjének megfelelő erőforrásrekordjai vannak, akkor ezekre a bejegyzésekre vonatkozóan őt mérvadónak mondjuk. Például a cisco.netacad.net tartományban egy névszerver nem lehet mérvadó a mail.cisco.com rekordra, mert ezt a rekordot egy magasabb tartományi szintű szerver tartja nyilván, konkrétan a cisco.com tartomány névszervere.

nslookup

A DNS egy kliens-szerver szolgáltatás, ámbár különbözik egyéb kliens-szerver szolgáltatásoktól. Míg más szolgáltatások egy kliensalkalmazást (például böngészőt, levelezőprogramot) használnak, addig a DNS-kliens egyidejűleg maga is szolgáltatásként fut. A DNS-klienst gyakran DNS-feloldónak (resolver) nevezik. Névfeloldást biztosít az azt igénylő alkalmazások és szolgáltatások számra.

Egy hálózati eszköz konfigurálásakor általában egy vagy több DNS-szerver címét is megadjuk, melyeket a DNS-kliens a névfeloldáskor használ. A DNS-szerverek címeit rendszerint az internetszolgáltató (ISP) biztosítja. Amikor a felhasználó alkalmazása név alapján szeretne egy távoli eszközhöz csatlakozni, a kérelmező DNS-kliens ezen névszerverek egyikét kérdezi le, hogy a nevet numerikus címmé alakítsa.

A számítógépes operációs rendszereknek van egy nslookup nevű segédprogramja is, amely lehetővé teszi egy adott állomásnév feloldásához a névszerverek manuális lekérdezését. Ezt a segédprogramot

névfeloldási problémák hibakereséséhez és a névszerverek pillanatnyi állapotának ellenőrzésére is használhatjuk.

Amikor kiadjuk az nslookup parancsot, az állomásunkon alapértelmezettként beállított névszerver jelenik meg (lásd ábra). Ebben a példában a DNS-szerver a dns-sj.cisco.com, aminek a címe 171.70.168.183.

Az nslookup parancssorába egy állomás vagy tartomány nevét írhatjuk be. Az ábrán az első lekérdezés a www.cisco.com lekérdezése. A válaszoló névszerver a 198.133.219.25 címet adja rá vissza.

Az ábrán látható lekérdezések csak egyszerű próbák. Az nslookup számos lehetőséget biztosít a DNS-folyamat átfogó tesztelésre és ellenőrzésére. Befejezéskor az exit parancs begépelésével léphetünk ki az nslookup segédprogramból.

Dinamikus állomáskonfiguráló protokoll

A dinamikus állomáskonfiguráló protokoll (Dynamic Host Configuration Protocol, DHCP) szolgáltatás a hálózaton lévő eszközök számára biztosítja, hogy egy DHCP-szervertől IP-címeket és egyéb információkat kaphassanak. A szolgáltatás automatizálja az IP-címek, alhálózati maszkok, átjárók és egyéb IP-hálózati paraméterek kiosztását. Ezt dinamikus címzésnek nevezzük. A dinamikus címzés alternatívája a statikus címzés. Statikus címzés alkalmazásakor a rendszergazda manuálisan állítja be az IP-címzési információkat a hálózat állomásain.

A DHCP lehetővé teszi, hogy egy állomás a hálózatra csatlakozásakor dinamikusan kaphasson IP-címet. Kapcsolatba lép egy DHCP-szerverrel és kér tőle egy IP-címet. A DHCP-szerver választ egy címet a hatókörnek (pool) nevezett, előre konfigurált címtartományból és egy meghatározott időtartamra kiutalja (bérbe adja) azt az állomásnak.

Nagyobb helyi hálózatokban, vagy ahol a felhasználók gyakran változnak, a DHCP a javasolt címkiosztási módszer. Új felhasználók jöhetnek, akiknek csatlakozásra van szükségük a laptopjaik számára, mások új munkaállomásokat kaphatnak, amiket ugyancsak csatlakoztatni kell. Ahelyett, hogy minden munkaállomáshoz a hálózati rendszergazdának kellene IP-címeket rendelnie, sokkal hatékonyabb, ha azok kiosztása dinamikusan, a DHCP használatával történik.

A DHCP által kiosztott címek nem végérvényesen vannak az állomásokhoz rendelve, csak egy adott időtartamra adják bérbe azokat. Ha az állomást kikapcsolják vagy eltávolítják a hálózatról, a cím újrafelhasználásra visszakerül a készletbe. Ez különösen a mobil felhasználók esetében hasznos, akik csak úgy jönnek-mennek a hálózaton. A felhasználók szabadon mozoghatnak egyik helyről a másikra és hozhatnak létre újra hálózati kapcsolatokat. Az állomás a hardveres kapcsolat létrejötte után kap IP-címet, akár vezetékes- akár vezeték nélküli LAN-on keresztül csatlakozik.

A DHCP lehetővé teszi, hogy repülőtereken vagy kávézókban vezeték nélküli hotspot-okon keresztül csatlakozzunk az internetre. Amikor egy vezeték nélküli eszköz csatlakozik a hotspot-hoz, a DHCP-kliense a vezeték nélküli kapcsolaton keresztül kapcsolatba lép a helyi DHCP-szerverrel, ami kioszt egy IP-címet az eszköznek.

Ahogy az ábra mutatja, különböző típusú eszközök lehetnek DHCP-szerverek, amennyiben DHCP-szerverszoftvert futtatnak. A legtöbb közepes- és nagyméretű hálózatban a DHCP-szerver általában dedikáltan egy helyi PC-alapú szerver. Otthoni hálózatokban a DHCP-szerver általában azon a helyi forgalomirányítón található, amely az otthoni hálózatot az ISP-hez csatlakoztatja. A helyi állomások közvetlenül ettől a helyi forgalomirányítótól kapják az IP-címzési információkat. A helyi forgalomirányító pedig az ISP DHCP-szerverétől kap egy saját IP-címet.

A DHCP biztonsági kockázatot is jelenthet, mivel bármely a hálózatra csatlakozó eszköz kaphat egy címet. Ez a kockázat meghatározó tényezővé teszi a fizikai biztonságot, akár dinamikus, akár manuális címzést használunk. Mind a dinamikus-, mind a statikus címzésnek helye van a hálózatterezésben. Sok hálózat használ egyszerre DHCP-t és statikus címzést is. DHCP-t használunk általában az általános célú állomásokon, mint a végfelhasználói berendezéseken, és statikus címzést használunk a hálózati eszközökön, mint az átjárókon, kapcsolókon, szervereken és nyomtatókon.

A DHCP működése

DHCP nélkül a felhasználóknak hálózatra csatlakozáskor manuálisan kellene megadniuk az IP-címet, az alhálózati maszkot és egyéb hálózati beállításokat. A DHCP-szerver egy IP-címkészletet kezel, és ad bérbe belőle egy címet bekapcsoláskor bármely DHCP-képes kliensnek. Mivel az IP-címek dinamikusak (béreltek), ellentétben a statikus címzéssel (állandó hozzárendelés), a már nem használt címek újbóli kiosztásra automatikusan visszakerülnek a készletbe. Amint az ábra mutatja, amikor egy DHCP-re konfigurált eszköz elindul vagy csatlakozik a hálózatra, a kliens egy szórásos DHCP-felfedező (DHCPDISCOVER) üzenetet küld szét, hogy egy a hálózaton elérhető DHCP-szervert találjon. A DHCP-szerver egy DHCP-ajánlás (DHCPOFFER) üzenettel válaszol, amely a kliensnek felajánl egy címbérletet. Az ajánlat tartalmazza a kiosztott IP-címet és alhálózati maszkot, a DNS-szerver IP-címét, valamint az alapértelmezett átjáró IP-címét. Az ajánlott címbérlet tartalmazza még bérlet időtartamát is.

A kliens több DHCPOFFER üzenetet is kaphat, amennyiben egynél több DHCP-szerver is van a helyi hálózaton. Ezért választania kell közülük, majd a kliens egy DHCP-igénylés (DHCPREQUEST) üzenetet küld az elfogadott bérleti ajánlatra az azt kibocsátó szervernek. Egy kliens dönthet úgy is, hogy egy olyan címet kér, amelyet a szerver egyszer korábban már kiosztott neki.

Abban az esetben, ha a kliens által megigényelt vagy a szerver által kiajánlott IP-cím továbbra is rendelkezésre áll, a szerver egy DHCP-nyugta (DHCPACK) üzenettel válaszol, amely visszaigazolja a kliensnek a bérlet véglegesítését. Ha az ajánlat már nem érvényes egy esetleges időtúllépés miatt, vagy mert egy másik kliens már megkapta a címbérletet, akkor a kiválasztott szerver egy negatív DHCP-nyugta (DHCPNAK) üzenettel válaszol. Amennyiben egy DHCPNAK-üzenet érkezik vissza, akkor a kérelmezési folyamatot újra kell kezdeni egy DHCPDISCOVER üzenet kiküldésével. Miután a kliens megszerezte a címbérletet, a bérleti idő lejártakor azt egy újabb DHCPREQUEST üzenettel meg kell újítania.

Az IP-címek egyediségét a DHCP-szerver biztosítja (ugyanazt az IP-címet nem lehet párhozamosan két hálózati eszközhöz hozzárendelni). A DHCP használata lehetővé teszi, hogy a hálózati rendszergazdák a kliensek IP-címeit könnyen, a kliensek manuális módosítása nélkül újrakonfigurálhassák. A legtöbb internetszolgáltató DHCP-t használ a statikus címet nem igénylő előfizetőik címkiosztásához.

Fájlátviteli protokoll

Egy másik általánosan használt alkalmazási rétegbeli protokoll a fájlátviteli protokoll (File Transfer Protocol, FTP). Az FTP-t egy kliens és egy szerver közötti adatátvitelre fejlesztették ki. Az FTP-kliens egy FTP-démont (FTPd) futtató szerverről való adatletöltésre vagy arra történő adatfeltöltésre szolgáló alkalmazás.

Amint azt az ábra is mutatja, a kliens és a szerver közötti sikeres adatátvitelhez az FTP két kapcsolatot igényel. Egyet a parancsoknak és a válaszoknak, a másikat pedig a tényleges fájlátvitelhez.

- Az első kapcsolatot a szerverrel a kliens kezdeményezi a kliens parancsaiból és a szerver

válaszaiból álló vezérlési forgalomnak.

- Szintén a kliens kezdeményezi a tényleges adatátvitelre szolgáló második kapcsolatot is a szerverrel. Ez a kapcsolat minden egyes adatátvitel alkalmával létrejön.

Az adatátvitel mindkét irányba megtörténhet. A kliens tölthet le adatokat a szerverről és oda tölthet is fel adatokat.

Server Message Block

Az SMB (Server Message Block) egy az IBM által az 1980-as évek végén kifejlesztett kliens-szerver fájlmegosztó protokoll, amely olyan osztott hálózati erőforrások szerkezetét írja le, mint például könyvtárak, fájlok, nyomtatók és soros portok. Ez egy kérés-válasz protokoll.

Az SMB-protokoll leírja a fájlrendszer elérését, valamint azt, hogy a kliensek hogyan kérhetik le a fájlokat. Leírja továbbá az SMB-protokoll folyamatok közötti belső kommunikációját is. Minden SMB-üzenetnek közös a formátuma. Ez a formátum egy állandó hosszúságú fejlécet és egy azt követő változó méretű paraméter- és adatkomponenst használ.

Az SMB-üzenetek az alábbiakra alkalmasak:

- Párbeszédek indítása, hitelesítése és lezárása.
- Fájl- és nyomtatóelérés vezérlése.
- Egy alkalmazás és egy másik eszköz üzenetváltásainak biztosítása.

Az SMB alapú fájlmegosztás és nyomtatás a Microsoft legfőbb hálózati szolgáltatásaivá vált. A Windows 2000 szoftversorozat megjelenésével a Microsoft megváltoztatta az SMB által használt mögöttes struktúrát. A Microsoft termékek korábbi verzióiban az SMB-szolgáltatások névfeloldásra még nem TCP/IP-re épülő protokollt használtak. A Windows 2000-től minden Microsoft termék már DNS neveket használ, ami közvetlenül támogatja az SMB-erőforrások TCP/IP protokoll alapú megosztását (lásd 1. ábra). A 2. ábra két Windows PC közti SMB-alapú fájlcserefolyamatot szemlélteti.

A fájlátviteli protokollal (FTP) ellentétben a fájlmegosztásra a kliensek tartós kapcsolatokat építenek ki a szerverekkel. A kapcsolat létrejötte után a kliens felhasználója a szerveren lévő erőforrásokat helyi erőforrásként tudja elérni.

A Linux és Unix operációs rendszerek egy SAMBA nevű SMB-verzió alkalmazásával biztosítanak módszert a Microsoft hálózatokkal történő erőforrás-megosztásához. Az Apple Macintosh operációs rendszerek ugyancsak támogatják az SMB-protokoll alapú erőforrás-megosztást.