ZH kérdések kidolgozás

07 May 2024 11:16

Mit jelent a 3Play koncepció? Milyen előnyei vannak a hagyományos hálózatokhoz képest?

Hagyományosan 3 kommunikációs hálózat: Telefon, Valós idejű TV, Internet
Gyors IP hálózaton van lehetőség a három szolgáltatást egy hálózaton továbbítani
Szolgáltatónak gazdaságosabb, ügyfélnek egyszerűbb.

Ethernet címzések bemutatása (MAC cím, unicast, multicast, broadcast)

Minden végpontnak (elvileg) globálisan egyedi címe van. 48 bites. Az első 24 bit (23?) a gyártót azonosítja, ilyen gyártói kódot a cégek az ICANN-től vehetnek. Második 24 bit az eszköz azonosítója. Ez az azonosító (elvileg) sosem változik.
A gyakorlatban mára mindig átállítható a MAC cím, sőt gyakori hogy minden pl. WiFi csatlakozáskor új random kódot generál az eszköz a követés megakadályozása érdekében.
Unicast esetén ezzel a célcímmel lehet kommunikálni egy eszközzel. Cím LSB-je (első bitje) 0.
Broadcast: Minden eszköz megkapja, a switchek minden interfészükre továbbítják. Csupa 1-es (ff:ff:…).
Multicast: LSB 1-es (tehát az első küldött bit 1-es). Ebből már tudható, hogy vagy broadcast, vagy multicast lesz az üzenet. Csoportcímek vannak, amikre fel- és le tudnak iratkozni az eszközök IGMP-vel (már az IP stack része).

IPv4 fejléc

Protocol:

A csomagban található adatsor protokolljának kódja. Pl: TCP vagy UDP.

Time to Live:

A csomag élettartamára jellemző. Eredetileg másodpercre vonatkozik, de a gyakorlatban minden hop-nál eggyel dekrementáljuk. Így előzhető meg a csomagok végtelen keringtetése a hálózatban. Ezt használja ki a tracert is (egyre nagyobb TTL-lel ad fel csomagokat)

Source address:

A feladó IP címe

IP QoS IntServ és DiffServ különbsége

IntServ: Integrated Services

Adatfolyamok egyedi azonosításával lefoglalásra kerül minden továbbító ponton a megfelelő kapacitás a QoS biztosítása érdekében (Src IP, port; Dst IP, port; protocol).
A lefoglalás RSVP (Resource Reservation Protocol)-n történik. A küldő a célnak egy ilyen üzenetet küld. A válaszüzenet során lefoglalásra kerül a lehetőségnek megfelelően az erőforrás, és visszajut az adatfolyam azonosításához szükséges adatsor. Többféle foglalási típus is van.

DiffServ: Differentiated Services

IP fejlécben található DSCP (Differentiated Services Code Point) bitek szerint bánik a csomagokkal. Megkülönböztet alacsony, magas, kritikus és hálózatvezérlő csomagokat.
Publikus hálózatokban nem használják, mert bárki küldhetne kritikusnak jelölt csomagokat, mivel "önbevalláson" alapul.

Amikor publikus hálózatról egy szolgáltató belső hálózatába kerül egy adatfolyam, átválthat belső továbbításban az egyszerűbb DiffServ-re.

Ethernet Switch és Router összehasonlítása

Mindkettő közveltlenül kapcsolódik az interfészeire csatlakoztatott eszközökhöz, nem a régi busz topológia elemei.
Switch a 2. (adatkapcsolati, Ethernet) rétegben működik. Router a 3. (szállítási, IP) rétegben

működik.
Switch megfigyeli, mely portján milyen MAC című eszköz van és a megfelelő csomagokat oda továbbítja, betartja a multicast és broadcast üzeneteket.
Router hálózatokat köt össze IP tartományok szerint utat választva. Része lehet a NAT, a tűzfal (protokoll, port szerint akár), stb (ez már 4. réteg).

IGMP protokoll feladata, működése

Internet Group Management Protocol
Ezzel jelzik az eszközök, hogy egy adott IP multicast forrás adatfolyamát szeretnék megkapni.
Belső hálózaton műkdőképes, nyílt interneten, főként szolgáltatók között bonyolult, a megoldások nem terjedtek el.

V1:

Kliensek jelzik a csatlakozást. Router rendszeresen megkérdezi a hálózatot, hogy van-e tag a csoportban. Erre válaszul megerősítik a tagságot a kliensek. Nincs kilépés üzenet, lassan derül ki, ha nincs több aktív tagja a csoportnak.

V2:

Új üzenettípus a Group Leave - ezzel azonnal végrehajtható a csoportról leiratkozás.
Létezik még: IP multicast címek, well-known csoportok (összes router, összes végpont, stb); IGMP snooping (switch).

IP alapú telefon és TV átvitel továbbítási igényei

Telefon

Figyelembe kell venni az Elviselhetőségi Küszöbháromszöget. Ennek részei a késleltetés, érthetőség romlás és a visszhang. Ha egyik rossz, a másik kettőnek jónak kell lennie, stb. Mindegyiknek van felső határa.
IP szempontból a késleltetés (max 150ms ajánlott) és a csomagvesztés miatti torzulás releváns. Meg kell oldani a Best-Effort kialakítású hálózaton a sok kis csomag alacsony jitter-rel (késleltetéskülönbség) és késleltetéssel való továbbítását.
Torzulásra megoldás lehet bizonyos mértékű forward error correction, de ez szükségszerűen növeli a késleltetést: Törekedni kell a csomagvesztés megelőzésére, a priorizálásra.

TV

Nem interaktív a szolgáltatás, így a késleltetés nyugodtan lehet magas. Nagy sávszélesség igény (H.264 720p: 3,5 Mbps).
Csomag újraküldésnek nincs helye, így forward error correction-t kell alkalmazni, ami bizonyos csomagvesztésig helyreállítja a tartalmat. Erre alkalmas a DVB-S-nél is használt TS (transport stream).

Hogyan működik Ethernet hálózatokban a CSMA/CD technológia

Carrier Sense Multiple Access with Collision Detection = Vivőérzékelélses ütközésdetektálásos többszörös hozzáférés
Régi busz topológiás Ethernet hálózatok használták, hozzá hasonló eljárás máig működik a WiFi hálózatokon.
Adás előtt a végpont megfigyeli, hogy szabad-e a csatorna. Ha igen, ad.

Exponential Backoff

Ha ütközés fordul elő, minden végpont észleli, JAM Signal-t küldenek. Várni kezdenek, mindenki sorsol, hogy mennyit. Leteltével újra adnak. Ha megint ütközés fordul elő, mindenki nagyobb határértékből sorsol, így egyre kisebb eséllyel lesz ütközés.

Ez a módszer már 100 Mbps-es hálózatokon nem működik, csak a legrégebbi 10-esen. Mára minden kapcsolat közvetlen.

TCP háromutas kézfogás

Transmission Control Protocol
Forrás SYN, sequence# x
Cél ACK sequence# x+1, SYN sequence# y
Forrás ACK sequence# y+1

Ezek "üres" TCP csomagok, amiknek a vezérlő flagjei jelzik az üzenetek típusait.
A kézfogással létrejön egy csatorna, amit utána a bontásik a felek használhatnak.

TCP és UDP portok funkciója, well-known portcímek

A fő feladat, hogy egy-egy eszközön (legyen az user vagy server) több feladat, folyamat (=entitás) is futhat. Meg kell oldani, hogy egymástól függetlenül kommunikáljanak.
A folyamatok a rendszertől portot kérhetnek. Küldésre egy random port címet kapnak, ahonnan megcélozzák egy szerver fogadó portját. A szerver a válaszában a megfelelő forrás portra továbbít üzenetet, így a kérést indító folyamat kapja meg azt az eszközön.
Fogadásra "listen"-nel kérhet egy folyamat portot, ha erre üzenet érkezik be, azt kezeli és válaszol a kérő fél forrásportjára. Ez szinte mindig szervereken fordul elő, és a kapcsolatokat a kliensek kezdeményezik.

Well-known portok

Bizonyos szolgáltatások "szokásos" portjai. HTTP: 80, FTP: 20-21, HTTPS: 443, stb.
Szerepük kettős. Egyrészt pl. nem kell beírni a böngészőbe a 443-as portot minden cím után, mert tudjuk, hogy a HTTPS lekérésünkre választ a szerver 443-as portján fogunk kapni.
Másrészt fontos a tűzfalak beállításához, megfelelő portokat kiengedve (whitelist) vagy tiltva (blacklist) szabályozhatja egy rendszergazda, hogy milyen forgalom haladhat a hálózatán.

IPv4 multicast (címtartomány, felhasználás)

IP multicastra a "D" osztályú (1110-val kezdődő, 224.0… - 239.255…) címek használhatók.
Akkor használjuk, ha azonos adatfolyamot kell eljuttatni egy hálózatban több végpontra. Ezzel megelőzhető, hogy többszörösen kelljen az adatot továbbítani egy hálózatrészbe, hiszen a multiplikálást a switchek és routerek végzik az olyan interfészeikre, amiken található csoporttag (IGMP snooping). Minden hálózati úton csak egy példányban közlekedik az adatfolyam.
Ha egy végpont szeretné megkapni az adatfolyamot, az adott multicast címre egy IGMP kéréssel csatlakozik, amit routernek küld. Ezt a csomagot a routerig vezető switchek megfigyelhetik snoopinggal, hogy tudják, merre kell majd multipikálni az üzenetet.
Jelenleg IPTV alkalmazásoknál elterjedt, mivel a hálózat szolgáltatója a saját hálózatán belül ezzel spórol, és megfelelő kontrollal rendelkezik.
(egyéb infók a korábbi multicastos kérdésnél)

Milyen szolgáltatásnak miért van szüksége IP QoS biztosítására? (QoS fogalma, összetevői)

Az internet rövid szöveges tartalmakra és aszinkron nagy mennyiségű adat átvitelére lett tervezve, erre alkalmas a Best-Effort felfogás. Mára interneten küldünk olyan adatfolyamokat (VoIP, IPTV), amik jóval érzékenyebbek a késleltetésre és nagyobb, folyamatosan biztosítandó adatmennyiséggel járnak. Itt lép be a QoS (Quality of Service).

Ehhez szükség van a csomagok osztályozására. Ez történhez "önbevallásos" alapon (DiffServ), a csomag DSCP bitjeinek beállításával; ez alkalmas visszaélésekre, hiszen minden csomagot megadhatunk maximális prioritással. A másik módszer az IntServ, ahol a hálózati út résztvevőitől kérünk egy átviteli képességet, és erről visszaigazolást kapunk az adatfolyam megkezdésekor, amit egyedileg azonosítunk. A kérésünk teljesítése korábban tett egyedi megállapodásokon múlik.

A QoS tényleges biztosításához az erőforrásokkal a hálózat eszközeinek kell gazdálkodnia, erre több módszer van.
Leaky Bucket: A változó bejövő adatmennyiség egy folyamatos sebességgel távozó folyammá alakítása. Ha a "vödör" megtelik, a további csomagokat eldobjuk.
Token bucket: Túl lehet lépni a lefoglalt kapacitást ideiglenesen, tokenek ellenében. A tokeneket úgy osztja a rendszer, hogy felhasználásukkal az átlagos átviteli sebesség a lefoglalt kapacitáson belül maradjon.
Ütemezés: A bejövő csomagok sorrendjét változtatjuk továbbküldés előtt, a magasabb prioritásúakat előre sorolva. Primitív módszer esetén sok magas prioritású csomag esetén az alacsonyak felgyűlnek és eldobásra kerülnek, erre megoldás a Fair Queueing (a különböző prioritások listákba rendezése, round-robin elven csomagok továbbítása) - ez viszont nem elég hatékony a QoS biztosításához, nem

biztosítja a késleltetést.
Középút a Weighted Fair Queueing - magasabb prioritásúak több kapacitást kapnak, de az alacsonyak sem éheznek.
Drasztikus eszköz a Traffic Policing - torlódás veszélyekor az alacsony prioritású csomagokat eldobja, hogy a magasak megmaradjanak. Kevésbé draszikus a Random Early Drop.