PÁZMÁNY

Pázmány Péter Katolikus Egyetem
Információs Technológiai és Bionikai Kar

Számítógépes hálózatok

#05 – BOOTP, DHCP, NTP, TFTP

2024. október 11.

Naszlady Márton Bese

naszlady@itk.ppke.hu

#05/1 – Új eszköz konfigurálása a hálózaton

Új belépő eszközök

Mi kell ahhoz, hogy egy frissen csatlakozott hálózati eszköz forgalmazni tudjon az L3 szintű hálózatunkon?

Új belépő eszközök

Mi kell ahhoz, hogy egy frissen csatlakozott hálózati eszköz forgalmazni tudjon az L3 szintű hálózatunkon?

L1 szinten: megfelelő physical interface (pl. alkalmas kábel)
L2 szinten: MAC cím (ha Ethernetet használunk)
L3 szinten: IP(v4) cím, subnet mask, default gateway

Új belépő eszközök

Honnan fogja ezeket az adatokat beszerezni?

L1 szinten: így gyártották

L2 szinten: gyártó beleírta a MAC címet

L3 szinten: ??? → esetleg a gyártó megadta?

→ esetleg kézzel megadjuk?

→ esetleg automatizálható?

Konfigurációs beállításokat adó központi szolgáltatás

Ötlet: legyen egy központi *szerver*, ami a hozzá intézett hálózati konfigurációs kérdésekre válaszol.

Megválaszolható kérdések például:

- mi az egyes L3-as hálózati interfészek IPv4 címe,
- mi a hálózaton belüli címtartomány (CIDR)
- merre találhatók a routerek és/vagy mi a default gateway címe
- honnan kell az operációs rendszert letölteni
- mennyi a pontos idő
- hova kell fordulni a domain nevek hálózati címekké alakításához
- stb.

Az új eszköz és a konfigurációs szerver egymásra találása

Hogyan találja meg az új eszköz,
hogy ki a konfigurációs szerver a hálózaton?

Az új eszköz és a konfigurációs szerver egymásra találása

Hogyan találja meg az új eszköz,
hogy ki a konfigurációs szerver a hálózaton?

Broadcast üzenetet küld; az üzenet típusa „*konfigurációs kérés*”.

Az új eszköz és a konfigurációs szerver egymásra találása

A broadcast üzenet jó, mert…

- az alhálózaton belül mindenkihez eljut → nem kell tudni a címzett címét
- a válasz lehet unicast

A broadcast üzenet nem jó, mert…

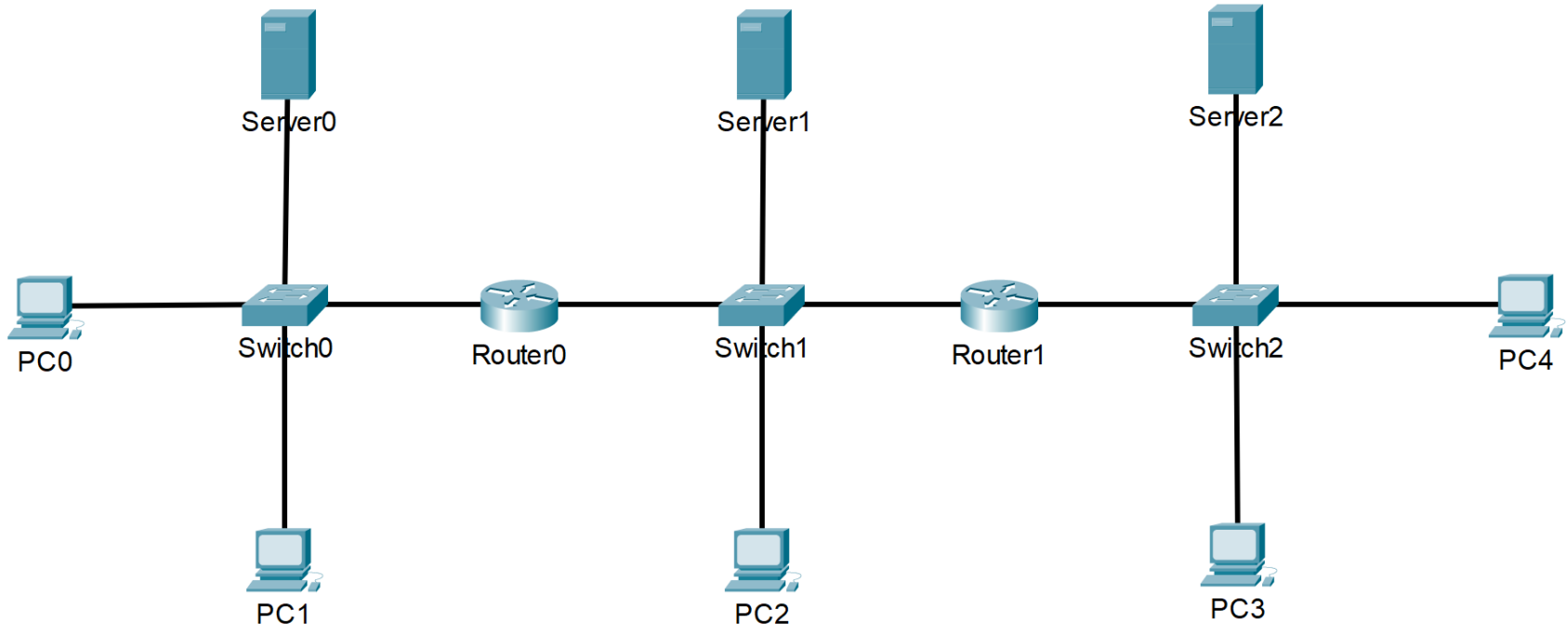
- az alhálózaton belül mindenkihez eljut → terheli a hálózatot
- routeren nem megy át

Konfigurációs szerver elhelyezése

Az új eszköz mindenképpen broadcast üzenettel fogja keresni a szervert.

A router nem engedi át a broadcast üzenetet.

Első megoldás: Minden alhálózatba kell egy külön konfigurációs szerver.

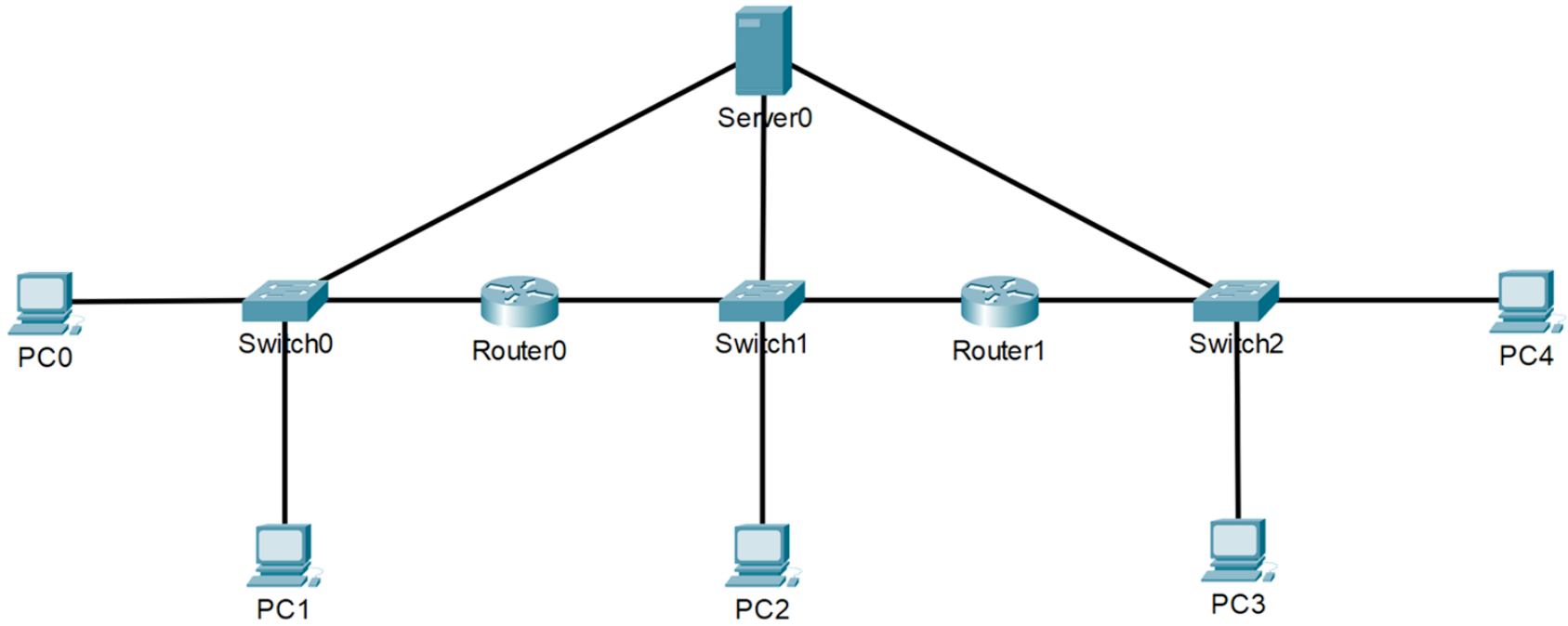


Konfigurációs szerver elhelyezése

Az új eszköz mindenképpen broadcast üzenettel fogja keresni a szervert.

A router nem engedi át a broadcast üzenetet.

Második megoldás: A konfigurációs szerver minden alhálózatban jelen van.

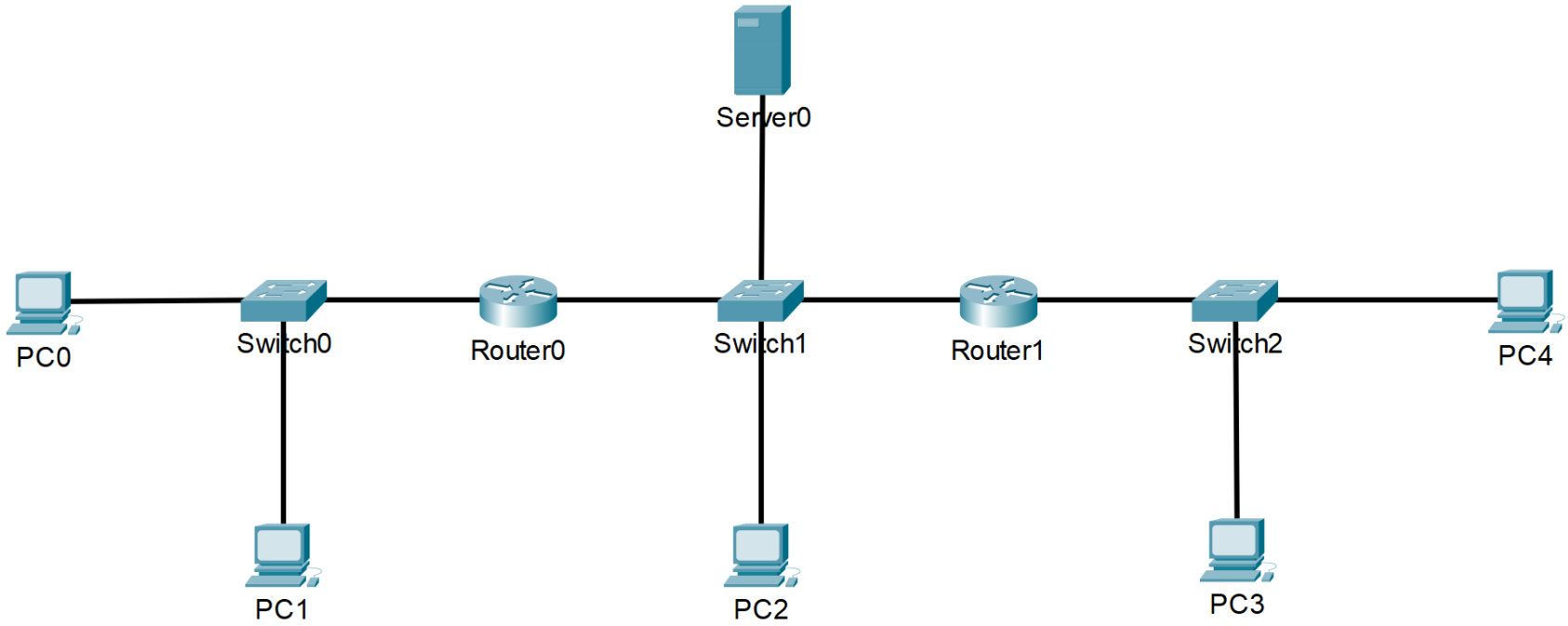


Konfigurációs szerver elhelyezése

Az új eszköz mindenképpen broadcast üzenettel fogja keresni a szervert.

A router nem engedi át a broadcast üzenetet.

Második megoldás: A konfigurációs szerver csak az egyik alhálózatban van jelen, de valamilyen ügyes megoldással mégis eljut hozzá az üzenet.



Relay agent

A ***relay agent*** feladata, hogyha konfigurációs üzenetet hall az alhálózaton belül, de a konfigurációs szerver nem ezen az alhálózaton belül van, akkor a broadcast üzenetben kapott konfigurációs kérést ő a routeren keresztül már közvetlenül a szervernek címezve, unicast üzenetben továbbítsa.

Ehhez a relay agentnek tudnia kell a konfigurációs szerver címét.

#05/1 – Összefoglalás

Elvek	Új eszköz bekapcsolásakor hiányzó információk Szerver, amitől kérdezhetők a beállítások
Eszköz	Relay agent

#05/2 – Bootstrap Protocol

Bootstrap Protocol (BOOTP)

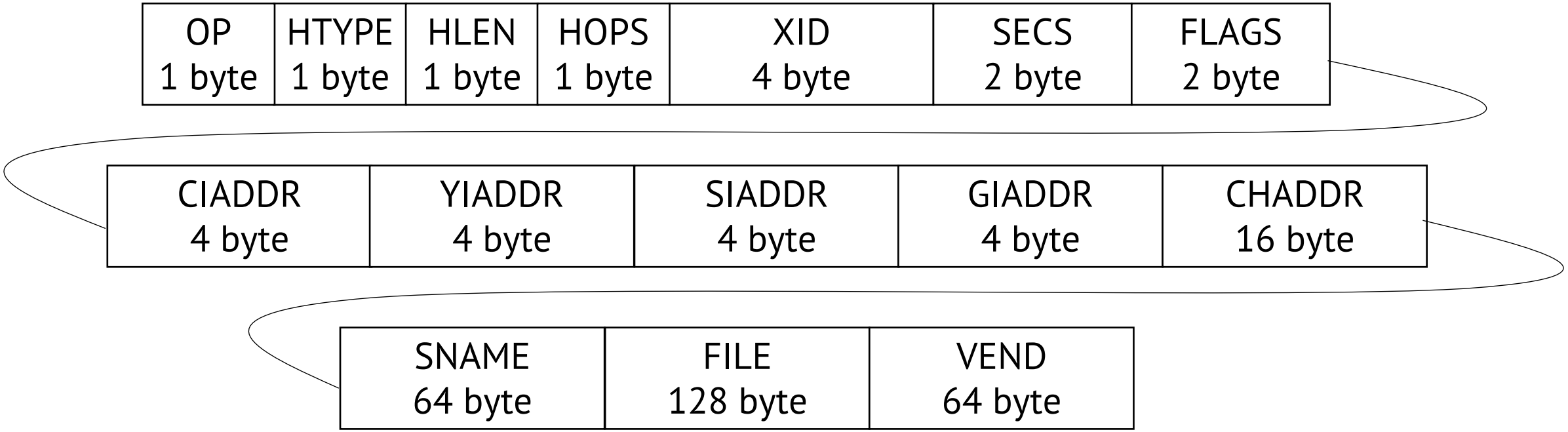
Application layer (L7) szinten működő protokoll a hálózathoz frissen csatlakoztatott eszközök konfigurálására.

A RARP kiváltására jött létre:

- a kérdés route-olható,
- a válasz tartalmazza a felkínált IP címet és a subnet maskot, default gatewayt is,
- a válasz tartalmazhat leírást arra vonatkozóan is, hogy melyik szerverről lehet letölteni az operációs rendszert tartalmazó fájl

BOOTP üzenetformátum

A BOOTP üzenet a következő egységekből áll:



BOOTP üzenetformátum

A BOOTP üzenet a következő egységekből áll:

- OP operation code – a művelet típusa (request, reply)
- HTYPE hardware type – a fizikai hálózat típusa (pl. ethernet)
- HLEN hardware length – a fizikai címek hossza (pl. MAC cím hossza)
- HOPS hop count – az ugrások száma; a BOOTP-t közvetítő routerek növelik.
- XID transaction id – azért, hogy tudjuk, mire mi a válasz
- SECS seconds – az első BOOTP kérés óta eltelt idő
- FLAGS flags – a BOOTP csomag jellemzői. Itt kérhető, hogy a válasz is broadcast üzenet legyen
- CIADDR client IP address – a kérésben a kliens kitöltheti a kért címet
- YIADDR your IP address – ezt a címet kapja a kliens

BOOTP üzenetformátum

A BOOTP üzenet a következő egységekből áll:

- SIADDR server IP address – a szerver IP címe, akivel a boot folytatható
- GIADDR gateway IP address – a BOOTP-t átengedő router címe
- CHADDR client hw address – a kliens fizikai címe (MAC címe)
- SNAME server host name – a szerver neve, ahonnan az oprendszer letölthető
- FILE file name – az operációs rendszert tartalmazó fájl neve
- VEND vendor specific information – ebben található
    - a netmask,
    - a routerek IP címe,
    - a DNS szerverek IP címe

BOOTP folyamat

1. A bekapcsolt számítógép feléleszti a hálózati kártyát, majd a kártya előállít egy BOOTP üzenetet, és elküldi azt broadcast üzenetként.

2. A BOOTP szerver fogadja az üzenetet, válaszol. A válaszban ad egy IPv4 címet a kliensnek, és megadja azt is, hogy lehet-e hálózatról bootolni, és ha igen, akkor mi ennek a boot szervernek az IPv4 címe, neve, és mi a rajta található, operációs rendszert tartalmazó fájl neve.

3. A kliens fogadja a BOOTP üzenetet. Megjegyzi belőle a saját IPv4 címét, és dönt, hogy honnan szeretne bootolni. Ha a hálózati bootot választja, akkor kapcsolatba lép a megadott szerverrel és letölti az oprendszert, bootol. (Vagy dönthet úgy, hogy az IP cím elég, és amúgy a merevlemezről bootol).

Milyet válaszoljon a BOOTP szerver?

A FLAGS mezőben említettük, hogy a kliens kérheti, hogy a szerver boradcast üzenettel válaszoljon. Miért jó ez?

A kliens nem tudja a saját IP címét, épp most kér egyet

- boradcast üzenet kell, különben nem jut el a klienshez
- a kliens az XID mezőből tudja, hogy számára jött-e az adat.

A kliens tudja a saját IP címét

- ebben az esetben nem szükséges a broadcast, mert az unicast is célba talál.

#05/2 – Összefoglalás

Protokoll Bootstrap Protocol rendeltetése

Folyamat BOOTP folyamat

#05/3 – Dynamic Host Configuration Protocol

Dynamic Host Configuration Protocol (DHCP)

Application layer (L7) szinten működő protokoll a hálózathoz frissen csatlakoztatott eszközök konfigurálására.

A BOOTP kiegészítésére jött létre:

- mindent támogat, amit a BOOTP is
- a VEND rész helyett egy bővebb, OPTIONS részt tartalmaz,
- rugalmasan lehet IPv4 címeket kiosztani és elvenni is

DHCP üzenettípusok

Attól függően, hogy hol tartunk a konfigurációban, és hogy mi az elérni kívánt eredmény, a következő DHCP üzenettípusok léteznek:

- DHCPDISCOVER — felderítés (ki a felhatalmazott DHCP szerver)
- DHCPOFFER — a szerver felajánl egy IP címet a kliensnek
- DHCPREQUEST — a kliens megkéri a szervertől a felajánlott címet
- DHCPDECLINE — a kliens mégsem kéri a címet
- DHCPACK — a szerver leokézza a kérést
- DHCPNAK — a szerver nem okézza le a kérést
- DHCPRELEASE — a kliens elengedi az IP címet, nem kell neki többé
- DHCPINFORM — a kliens konfigurációs paramétereket kér

DHCP folyamat

Négylépcsős folyamat (hasonlít a PPPoE esetén látotthoz):

1. A bekapcsolt számítógép feléleszti a hálózati kártyát, majd a kártya előállít egy DHCPDISCOVER üzenetet, és elküldi azt broadcast üzenetként.
2. A DHCP szerver fogadja az üzenetet és egy DHCPOFFER üzenettel válaszol. A válaszban felkínál egy IP címet a kliensnek, illetve az OPTIONS részben megadja a subnet maskot, alapértelmezett átjárót, DNS szerverek címét stb.
3. A kliens fogadja a DHCPOFFER üzenetet. Eldönti, hogy megkéri-e a felkínált címet (és paramétereket). Ha igen, akkor DHCPREQUEST üzenetet küld.
4. A DHCP szerver fogadja a kérést. Ha mindent megfelelőnek talál, akkor egy DHCPACK üzenettel leokézza a történéseket. Ha nem ért egyet, akkor DHCPNAK választ küld.

DHCP leases adatbázis

A DHCP szerver által kiosztott IP címhez lejárati idő is tartozik. (Miért?)

Lease: a kliens + kiosztott IPv4 cím + lejárati idő

A lease-ekről a szerver nyilvántartást vezet.

DHCP leases adatbázis

A DHCP szerver által kiosztható címeknek két fő kategóriája van:

Dinamikus IP cím
Egy beállított intervallumból a DHCP szerver választ egy címet.

Ez a kiadott cím egy idő után lejár (lease time).

Fix (statikus) IP cím
Egy megadott kliens mindig ugyanazt a címet fogja kapni.

#05/3 – Összefoglalás

Protokoll	DHCP rendeltetése
Folyamat	DHCP folyamat
Elvek	Dinamikus és fix IPv4 címek kiosztása

#05/4 – Network Time Protocol

Network Time Protocol (NTP)

Application layer (L7) szinten működő protokoll a hálózathoz kapcsolódó eszközök óráinak szinkronban tartására.

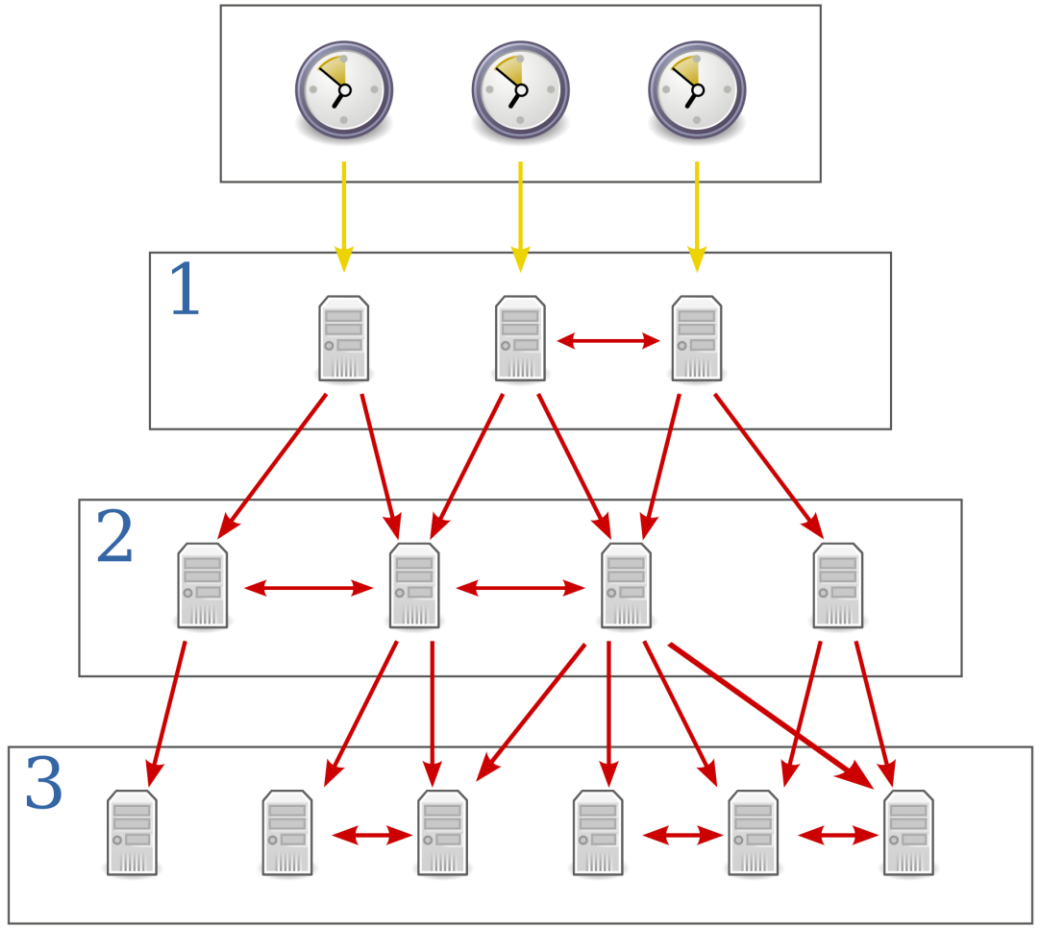
Kizárólag időinformációt szolgáltat:

- az UTC szerinti időt ad vissza,
- ezredmásodperc pontosságra is képes,
- rétegbe szervezett órákat használ a legpontosabbtól lefelé haladva fa struktúrában felépítve

Óra rétegek

Hierarchikus felépítés, a rétegek neve **stratum**. A legfelső réteg (0-s sorszámmal) a legpontosabb időalapokat tartalmazza:

- Stratum 0: atomórák
- Stratum 1: az atomórákhoz kapcsolt szerverek
- Stratum 2: az S1-hez kapcsolt gépek
- és így tovább lefelé



NTP szinkronizációs algoritmus

1. A kliens szeretné tudni a pontos időt. Ehhez legalább három, egymástól eltérő hálózaton lévő szervert kérdez le.
2. A lekérdezések során figyelembe veszi azt, hogy mennyi időbe telik a kérés elküldése és a válasz megérkezése (round trip time – RTT).
3. A kapott csomagokban szereplő időkből és a számolt RTT értékekből statisztikai elemzést készít (hibák kiszűrésére).
4. Több ilyen iteráció után (kiismerve az RTT értéket) a kliens frissíti a saját óráját a szervertől kapott idő és a késleltetés figyelembe vételével.

#05/4 – Összefoglalás

Protokoll NTP rendeltetése

#05/5 – TFTP

Trivial File Transfer Protocol

Motiváció:

Adott egy vékony kliens, amit szeretnénk a hálózatról bootolni.

A kliensen kezdetben jelenlévő kód legyen nagyon egyszerű és „könnyű”.

Az oprendszer, bonyolultabb driverek stb. már jöhessen hálózatról letöltve.

Megoldás:

Trivial File Transfer Protocol (TFTP) – pofonegyszerű („triviális”) implementáció

A boot szerevereknél használatos; a DHCP folyamatban paraméterként kapjuk meg a host címét és a letöltendő fájl nevét.

TFTP csomagformátum

A TFTP csomag mindig egy 16 bites opcode értékkel kezdődik. Az opcode (operation code – művelet kódja) megadja, hogy a küldött csomag az írandó / olvasandó fájl nevét, adatot, nyugtát vagy hibaüzenetet tartalmaz.

Az opcode-ot követő tartalom az üzenet típusától függ:

- írási, olvasási kérésnél (01 és 02 opcode) a fájl neve és az átviteli mód az infó.
- bináris adatátvitelnél (03) az opcode után a blokk sorszáma, majd az adat jön.
- nyugtázásnál (04) a nyugtázott üzenet blokk-sorszáma szerepel benne.
- hibaüzenet esetén (05) pedig a hibára vontakozó információkat tartalmaz.

A csomagban nincs checksum; az adatok sérülhetnek.

TFTP adatátvitel

A TFTP a nagyon könnyű implementálhatóság kedvéért UDP-t használ.

Az UDP miatt...

- a csomagok mérete maximum 512 byte lehet, és
- a nyugtázást az alkalmazás-szinten kell megoldani.

A nyugtázáshoz a stop-and-wait elvet használja:

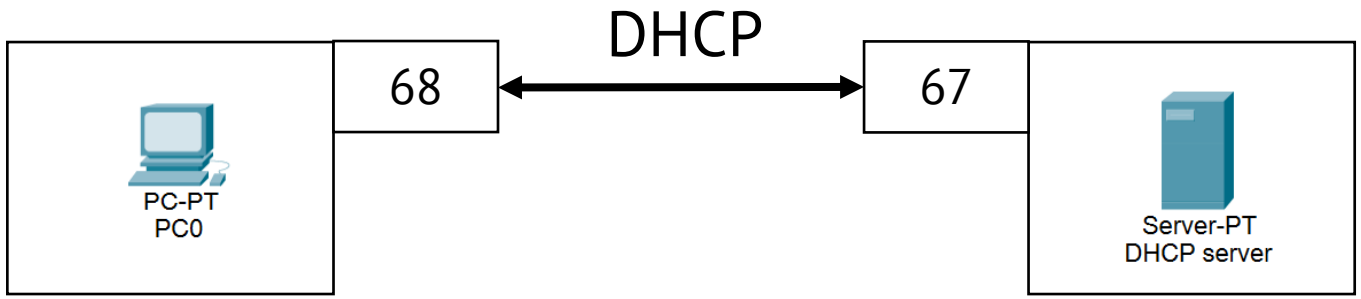
- ha nem jön adat a timeout lejártáig, akkor ismétli az ACK-t.
- ha nem jön ACK a timeout lejártáig, akkor ismétli az adatot.

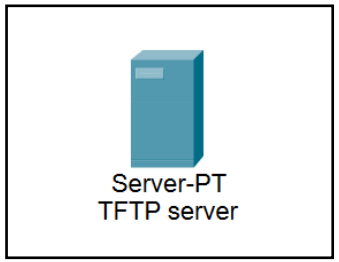
A fájl (ill. az adatátvitel) végét az 512 byte-nál kisebb adatcsomag jelzi.

TFTP adatátvitel

A „kapcsolat” felépítése a következő módon történik:

1. A kliens a DHCP révén kapja meg a TFTP szerver címét.

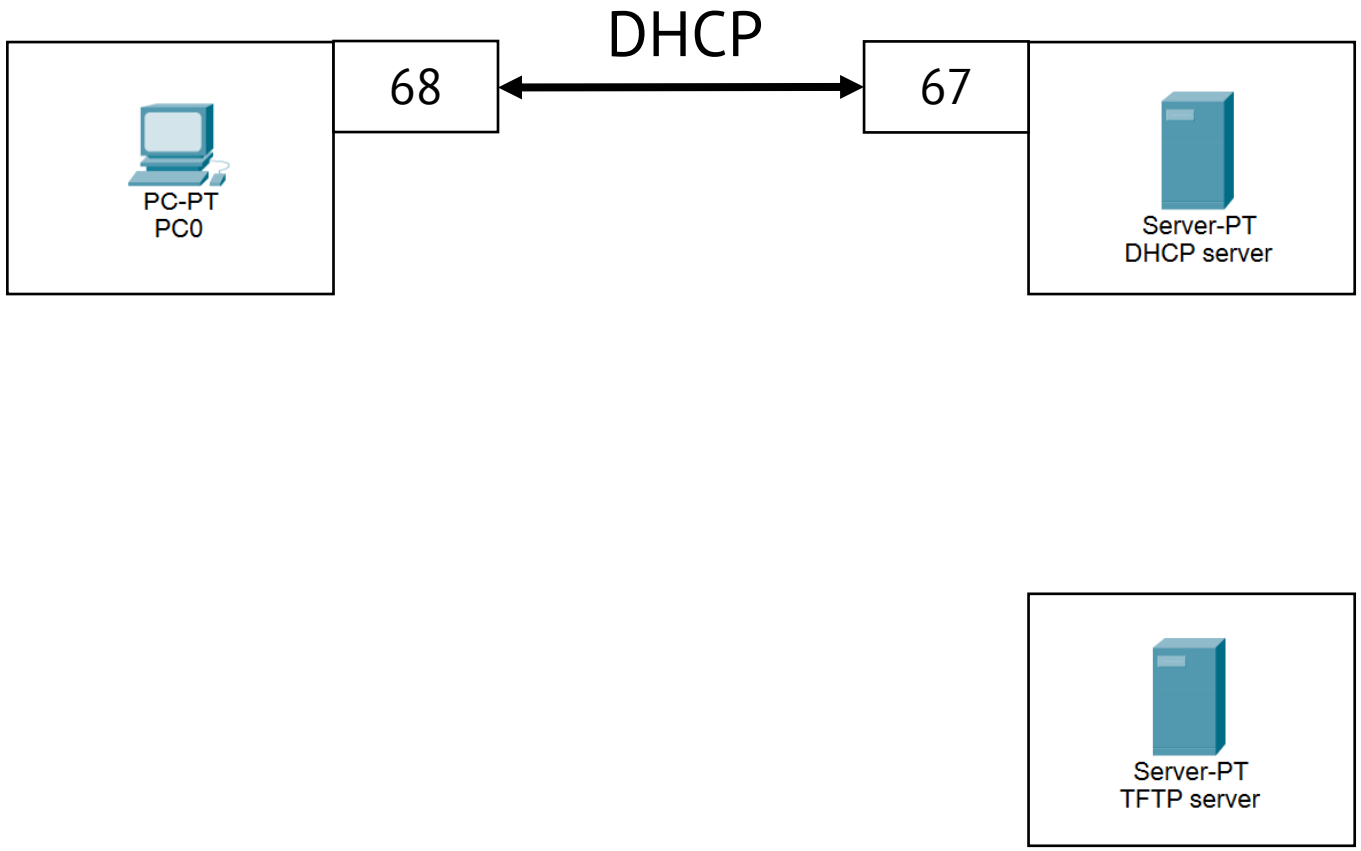




TFTP adatátvitel

A „kapcsolat” felépítése a következő módon történik:

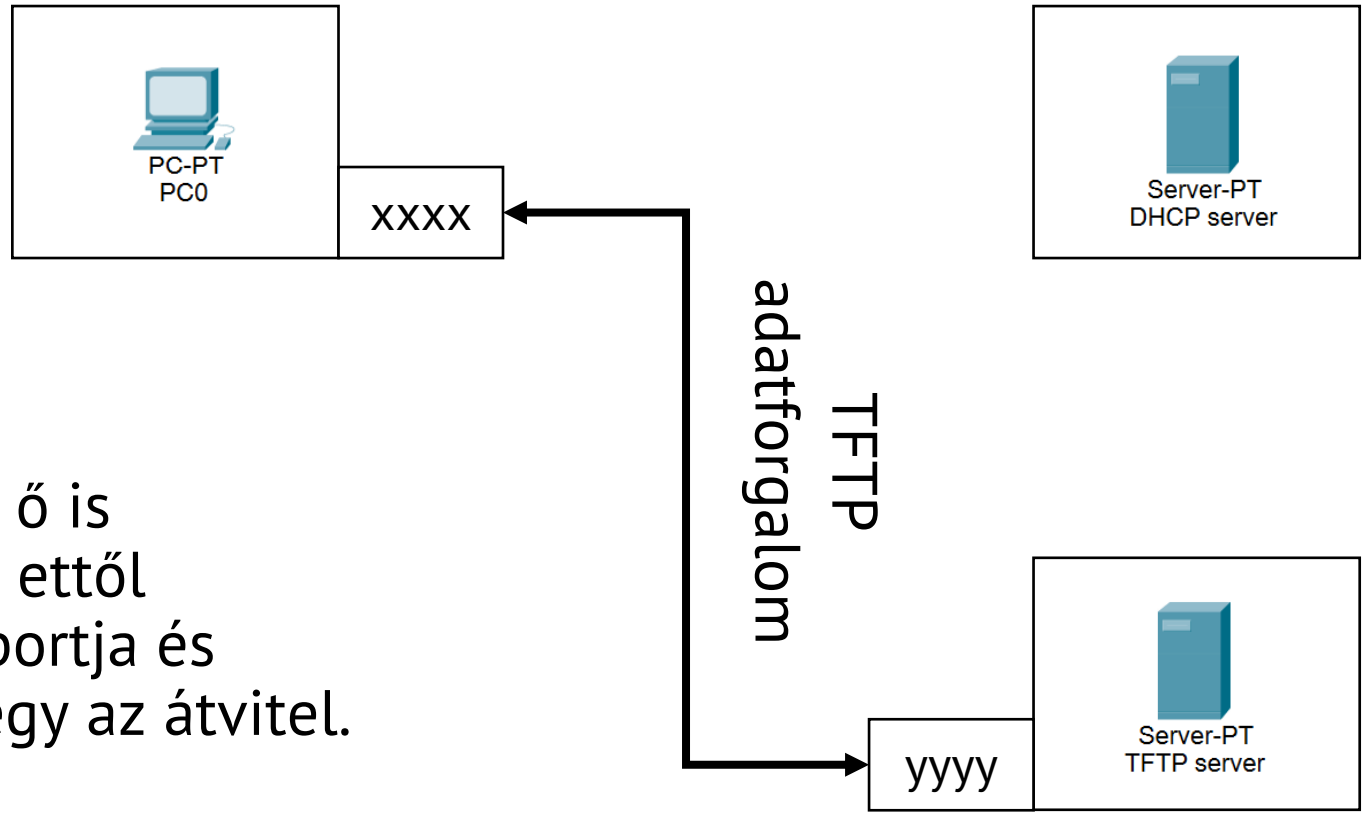
1. A kliens a DHCP révén kapja meg a TFTP szerver címét.
2. A kliens a TFTP szerver 69-es portjára küldi a fájl letöltés kezdeményezését. A kliens ehhez a kéréshez egy random kimenő portot használ (xxxx).



TFTP adatátvitel

A „kapcsolat” felépítése a következő módon történik:

1. A kliens a DHCP révén kapja meg a TFTP szerver címét.
2. A kliens a TFTP szerver 69-es portjára küldi a fájl letöltés kezdeményezését. A kliens ehhez a kéréshez egy random kimenő portot használ (xxxx).
3. A TFTP szerver fogadja a kérést, ő is nyit egy random portot (yyyy) és ettől kezdve a kliens kezdeményező portja és a szerver random portja közt megy az átvitel.



Bűvészinas szindróma

Tegyük fel, hogy a k-adik nyugta késik egy kicsit; pont annyit, hogy azalatt a szerver már újraküldte az adatot.

Egyszercsak megérkezik az elveszettnek hitt k-adik nyugta. Ekkor a szerver el fogja küldeni a k+1-edik adatot.

Ezt követően az a nyugta is megjön, ami szintén a k-ról szól, és az újraküldött adatot nyugtázná le.

A küldő erre is elküldi a k+1-edik adatot.

Végeredményben innentől kezdve minden csomagot kétszer fogunk küldeni.

Biztonsági kérdések

A TFTP protokollban nincs semmilyen azonosító/jelszó.

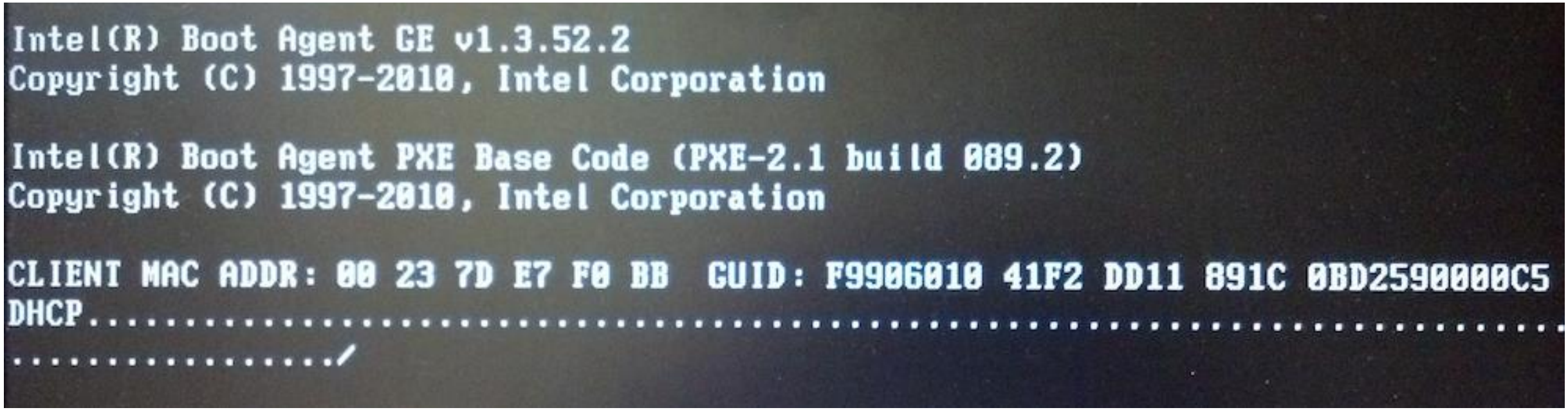
A szerverimplementációk bizonyos korlátozásokat tesznek lehetővé:

- csak bizonyos fájlokhoz
- csak bizonyos IP címekről
- csak olvasási joggal

lehet hozzáférni.

Hol használunk TFTP-t?

- Routerek, switchek operációs rendszerének frissítésekor
- Routerek, switchek konfigurációs fájljainak mentésére, tárolására
- PC-k bootolására:



#05/5 – Összefoglalás

Fogalmak	TFTP rendeltetése
	Bűvészinas szindróma
Eljárások	TFTP adatátvitel

VÉGE

PÁZMÁNY

Pázmány Péter Katolikus Egyetem

Információs Technológiai és Bionikai Kar