

Hostolt IP alközponti infrastruktúra provisioning rendszerének átalakítása

téma kutatói összefoglalója

Dr. Huszák Árpád

Hallgató: Egyed-Izsák Katalin

Céges konzulens: Szerényi Zsolt, NISZ Nemzeti Infokommunikációs Szolgáltató Zrt.

Egyetemi konzulens: Dr. Huszák Árpád

A provisioning kifejezés egy telekommunikációs szolgáltatás aktiválását vagy megváltoztatását jelenti, mely folyamat lefedi a felhasználói igény jelzésétől az összes szükséges változtatás megtételéig jelentkező feladatokat. Provisioning rendszereknek nevezik azokat a middleware rendszereket, amelyek az ügyféladminisztrációs rendszerek felől érkező kéréseket fogadják, értelmezik, és a meghatározott üzleti folyamatok mentén a különféle hálózati eszközök és adatbázisok felé az általuk értelmezhető rendszerspecifikus üzeneteket szétküldik

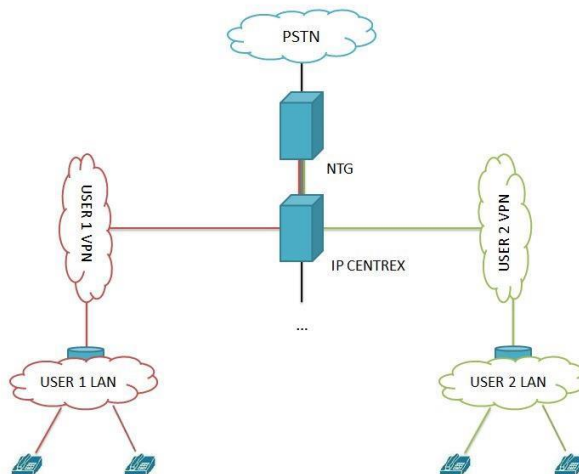
A NISZ által üzemeltetett hostolt IP alközponti infrastruktúra (IP Centrex) jelenleg integrált, azaz az IP Centrex rendszer szerves részét képező provisioning rendszerrel rendelkezik. Ez nehezíti az új végkészülékek (IP telefonok) illesztését az IP Centrex rendszerhez, mert minden esetben gyártói közreműködést igényel. Ezért a NISZ önálló, saját fejlesztésű és üzemeltetésű provisioning rendszert épít ki.

A félév folyamán elsősorban a rendszer felépítésének megismerése volt a cél, például hogy milyen lépésekből áll össze a provisioning folyamata, mely szerverek módosítására lesz szükség a provisioning különálló szerveren történő megvalósításához. A NISZ IP Centrex-en belül kialakításra került az éles rendszer mellett egy tesztrendszer is, mely szabad kísérletezési lehetőséget nyújt a véghezvinni kívánt változtatások kipróbálására.

Szolgáltatási modell

A NISZ által is használt, úgynevezett alap szolgáltatási modell esetén az intézményi LAN hálózaton az IP telefonok kiszolgálása az intézményi informatikai rendszerében az adat- és internetforgalom kezelésétől külön, attól elkülönült VLAN-on keresztül történik. Ekkor az IP telefonok minden forgalma az intézmény központi telephelyén elhelyezkedő tűzfal kihagyásával közvetlenül a hívásvezérlő eszközök felé történik. Ezzel az egyes telephelyek esetleges IP lezakadásakor, a többi telephelyen a szolgáltatás zavartalanul biztosítható.

A biztonságos működés biztosítása érdekében a Centrex rendszer két telephelyes, redundáns módon került kialakításra. A rendszer rendelkezik egy belső kommunikációs csatornával, mely a két telephely között L2 szintű összeköttetést biztosít, és melyen az egyes rendszerelemek egymással kommunikálnak. A névkiszolgáló, a hívásvezérlő és a média proxy eszközök az egyes intézményi MPLS VPN-ek felé közvetlen eléréssel rendelkeznek, azaz ezek az eszközök „belátnak” az intézményi VPN hálózatokba. Minden egyes intézményi VPN-ben ezek az eszközök ugyanazzal az IP címmel érhetők el. Egyes rendszerelemek az NTG IP hálózatából publikus IP címen is elérhetők (HVR). A 1. ábrán egy, a USER 1 VPN-je felől a USER 2 VPN-je felé menő hívás látható. Ilyen esetekben az IP Centrex proxy-ként működik.



1. ábra A window_df DataFrame első 5 eleme

Manuális provisioning

VoIP telefon vagy SIP telefon az internetes protokollon keresztül történő hangátvitelre, közismert nevén VoIP (voice over internet protocol) technológiára épül. Az IP Centrex rendszerben jelen pillanatban az alábbi IP telefonok használhatók: Cisco CP78xx és CP88xx, SPxxx, valamint Yealink T2xx készülékcsalád. A kézzel történő regisztráció megismerése céljából a folyamatot egy olyan Cisco 6841-3PCC telefonra vizsgáltuk, amely korábban nem volt a hálózatba regisztrálva.

A készüléken config beállításokat is végeztünk, hogy minél könnyebben kezelhető és személyre szabottabb legyen a készülék. Így többek között beállításra került a NISZ Centrex üdvözlőszöveg, a magyar nyelvű menü és az állandó háttérvilágítás. Mivel a beállítások eltárolódnak a szerveren, a jövőben már magától is be fog tudni regisztrálni a telefon, teljesen automatikusan. Mivel nincs külön alap, illetve MAC cím alapján kitöltött config fájl, ami a saját speciális jellemzőit tartalmazná, ezért minden, ebbe a készülékcsaládba tartozó telefon ezekkel a beállításokkal fog beregisztrálni a rendszerbe. Kevés számú eszköz esetén nem is lenne probléma, ám mivel a NISZ esetén általában több 1000 telefon egyidejűleg történő provisioning-járól beszélünk, ez a fajta regisztráció nem megvalósítható.

Auto provisioning

A Centrex rendszer provisioning folyamata lehetővé teszi, hogy az IP telefon a csatlakoztatás után automatikusan konfigurálja magát. Ez a folyamat a készülék többszöri újraindulásával jár. A provisioning folyamata:

- A DHCP szerver IP címet oszt az IP telefonnak. Ekkor megkapja a TFTP szerver nevét, valamint, hogy milyen IP címeiken érhető el a DNS névfeloldó szerverek.
- A telefon a TFTP szerverről egy minimális konfigurációt tölt le. Ez a minimális konfiguráció csupán annyit tartalmaz, milyen néven érhető el a provisioning szerver, ahonnan http/https protokollal le tudja tölteni a valódi konfigurációt. Mivel az átviteli útban tűzfal nem található, a TFTP portok nyitása nem jelent problémát.

- A provisioning során a telefon egy készülékfüggő (.xml alapú vagy plain text) template fájlt tölt le. Ez a template fájl makró utasításokat tartalmaz, mely utasítások hatására az IP telefon a MAC címétől, és a Centrex vonali beállításoktól függő, egyedi konfigurációt kap.

A provisioning folyamatát egy SPA504G készüléken keresztül mutatjuk be, a hálózatban ugyanis ebből a készüléktípusból található a legtöbb.

DHCP szerver

Az IP Centrex rendszerben az IP telefonok felől 100.64.165.10 és 100.64.165.74 IP címen elérhető Media Proxy (MP) kiszolgálókon került beállításra a DHCP kiszolgálás. A Centrex többi szerveréhez hasonlóan ez is redundánsan lett kialakítva (elsődleges és másodlagos szerver). Amennyiben az egyik szerver megválaszol egy kérést, akkor ezt jelzi a másik DHCP szervernek és az már nem válaszol a kérésre, valamint a kiosztott IP címet is feljegyzi, és nem osztja ki. Új ügyfél esetén tehát mindig be kell állítani a DHCP szerveren, hogy mely interfészen szolgálja ki a DHCP kéréseket. A dhcpd.conf fájlban található egy hivatkozás a dhcpd.ipranges fájlra. Ebben a fájlban található az az adatok, melyek zónánként eltérőek. Zóna alatt olyan logikai területeket értünk, melyek szerkezetileg összetartoznak, vagyis az ugyanazon CE vagy MCE eszköz (option router) által kiszolgált IP telefonok képeznek egy zónát.

IP cím kiosztás folyamata

Az IP telefon IP cím iránti igényét (DHCP request) először egy köztes routernek (az IP telefon szempontjából a gateway szerepét betöltő routernek) küldi, aki továbbítja a kérést, majd visszafelé irányban az erre érkező választ is (DHCP acknowledge).

NTP

Az IP telefonok számára az időszinkron (NTP) forrást alap esetben CE router biztosítja a telefonok felé mutatott gateway IP címén. A DHCP szerveren kerül beállításra, mely zónát kérdezzék a telefonok, illetve az NTP szerverek milyen IP címen érhetőek el. A

DNS

Az IP telefonok számára a névfeloldás (DNS) szolgáltatás a Centrex rendszerben két másodlagos (slave) DNS szerveren keresztül történik. Az elrendezés lehetővé teszi, hogy az elsődleges DNS módosításával a zónafájlok automatikusan frissítésre kerüljenek a másodlagos szervereken. Az elsődleges és a másodlagos szerverek közötti kommunikáció a menedzsment zónában történik. Az IP telefonok a DNS szolgáltatást a 100.64.165.30 illetve a 100.64.165.94 IP című „intézményi” interfészen kérdezik le, így a másodlagos névszerverek az intézményi hálózatok felé ezeken az IP címen szolgálják ki a névfeloldási kéréseket.

A DHCP szerveren kerül beállításra, mely zónát kérdezzék a telefonok, illetve a névfeloldó szerverek milyen IP címen érhetőek el. A jelenlegi DHCP beállítás minden subnet-re vonatkozóan ugyanazt a névfeloldást alkalmazza.

TFTP

A központi DHCP kiszolgáló OPTION üzenetben adja meg az IP telefonnak a TFTP kiszolgáló helyét. Az OPTION üzenetben csak egyetlen cím adható meg, ennek kiesése esetén pedig nem lenne backup. A név megadásával viszont (ami több IP címet is magába foglal) biztosítva van a szolgáltatás redundanciája.

Minden egyes IP telefontípus különböző konfigurációs fájlt igényel. Az alábbi kódrészletben látható, hogy az általam vizsgált készülék az SPA50x készülékcsaládra általánosan érvényes konfigurációs fájlt keresi, tölti le magára először.

```
Trivial File Transfer Protocol
Opcode: Read Request (1)
Source File: spa50x_30x_en_v755.xml
Type: octet
Option: timeout = 10
Option: tsize = 0
```

Port forwarding

A provisioning szerver és a template fájlok nem a proxy szerveren, hanem az MCCN eszközön található. Az MCCN az intézmények felől egy publikus IP címen érhető el. Az MCCN eszközök nem rendelkeznek az intézményi VPN felé interfésszel. Biztosítani kell, hogy az IP telefonok, melyek publikus IP című hálózatot nem érnek el, a provisioning szervert mégis elérjék. A megoldás, hogy a két proxy eszköz, mely rendelkezik a publikus HVR zóna felé IP eléréssel is, az MCCN HA IP címén elérhető 80-as http és a 443-as https portokat tükrözi az IP telefonok felé.

Template fájlok

Az MCCN eszközön makro vezérelt template fájlok (.xml) gondoskodnak arról, hogy minden készülék a készülék típusnak, a MAC címnek, és a Centrex beállításoknak megfelelő egyedi konfigurációt kapjon. Például, az SPA502G egy két nyomógombos, míg az SPA504G négy nyomógombos készülék, így eltérő template fájl tartozik hozzájuk. Emellett, a Centrex-ben beállítható, hogy mely nyomógombok milyen funkcióval rendelkezzenek, ezért készüléktípusonként is léteznek különböző konfigurációk.

A template-ek mérete fajtánként eltérő, és mi ezen belül is csak bizonyos részeket használunk. Mivel a telefonok gyártói minél több alközpontot (Centrex-et) üzemeltető cégnek szeretnének megfelelni, így a több száz soros fájlnak csak bizonyos részei lesznek érvényesek ránk, mások pedig más VoIP rendszerekben.

Miután az .xml template fájlt létrehoztuk, és az adatbázisba is betöltöttük, az MCCN web felületén elérhetővé válik a variáció hozzárendelése a vonalhoz, és ezzel az adott készülékhez. Ezt a konfigurációt egyszerűen le lehet kérdezni, a böngészőbe az alábbi sort beírva:

```
http://prov.t-cx.nisz.hu/provisioning/cisco/spa504G/381c1ab75191
```

Ez a parancs természetesen csak az adott MAC című, SPA504G fajtájú telefonra lesz érvényes. A 2. ábrán a még kitöltetlen és a már kitöltött fájl általános paramétereit leíró rész összehasonlítása látható.

```

<!-- General -->

<Station_Name ua="na">@@extensions.station_name@@</Station_Name>
<Station_Display_Name ua="na">@@extensions.station_name@@</Station_Display_Name>
<Voice_Mail_Number ua="na">@@domains.special_numbers_dialout_prefix@1717</Voice_Mail_Number>
<Text_Logo ua="na">$0a Centrex</Text_Logo>
<BMP_Picture_Download_URL ua="na"/>
<Select_Logo ua="na">Text Logo</Select_Logo>
<Select_Background_Picture ua="na">None</Select_Background_Picture>
<Softkey_Labels_Font ua="na">Auto</Softkey_Labels_Font>
<Screen_Saver_Enable ua="xm">No</Screen_Saver_Enable>
<Screen_Saver_Wait ua="xm">300</Screen_Saver_Wait>
<Screen_Saver_Icon ua="xm">Background Picture</Screen_Saver_Icon>

```

```

<!-- General -->

<Station_Name ua="na">SPA504G</Station_Name>
<Station_Display_Name ua="na">SPA504G</Station_Display_Name>
<Voice_Mail_Number ua="na"> 1717</Voice_Mail_Number>
<Text_Logo ua="na">$0a Centrex</Text_Logo>
<BMP_Picture_Download_URL ua="na"/>
<Select_Logo ua="na">Text Logo</Select_Logo>
<Select_Background_Picture ua="na">None</Select_Background_Picture>
<Softkey_Labels_Font ua="na">Auto</Softkey_Labels_Font>
<Screen_Saver_Enable ua="xm">No</Screen_Saver_Enable>
<Screen_Saver_Wait ua="xm">300</Screen_Saver_Wait>
<Screen_Saver_Icon ua="xm">Background Picture</Screen_Saver_Icon>

```

2. ábra Template-ek összehasonlítása

Eredmények, értékelés

A félévben a NISZ VoIP rendszer felépítésének megismerése volt a cél, hogy a későbbiekben egy autoprovisioning rendszert építhessünk ki. Ehhez szerverek módosítására lesz szükség a provisioning különálló szerveren történő megvalósításához. A NISZ IP Centrex-én belül kialakításra került az éles rendszer mellett egy tesztrendszer is, mely szabad kísérletezési lehetőséget nyújt a véghezvinni kívánt változtatások kipróbálására. Mivel a munkára csupán valamivel több, mint 3 hónap állt rendelkezésre, így ezalatt a jelenlegi rendszer alapos megismerésére, illetve az autoprovisioning megvalósításához szükséges módszerek áttekintésére volt lehetőség.