Hálózat menedzsment ahogy én gondolom

# Miért?

Jogos kérdés. Az internet tele van hálózat menedzsment programokkal. És jócskán van köztük olyan amelyik tökéletesen teszi a dolgát. Amire kitalálták, és amit a fejlesztő fontosnak tartott:

* Nagios Ha csak arra vagyunk kíváncsiak működik-e, akkor nagyon jó.
* Munin Ha a terhelések, érdekelnek, grafikonokat akarunk, akkor jó.
* Zabbix Szintén jó, amire kitalálták.
* GLPI Na ez végre a kliensekkel is foglalkozik.

Amire szerintem szükség van:

* Kéne valamilyen dokumentáció, vagy ha már XXI. század, egy adatbázis az egész hálózatról:
  + Szerverek, kliens gépek, egyéb hálózati elemek.
  + Csatlakozók, patch panelek, patch kábelek, fali kábelek.
  + Felhasználók (nem csak mint felhasználók)
  + Helyek, alaprajzok. Ki ill. mi hol van.
* Adatgyűjtés, nyomkövetés:
  + Címek változása
  + Eszközök mozgása
  + Eszközök, szolgáltatások állapota.
  + Szabályok.
* És persze kellhet az is, amit a többiek tudnak

Van igény, de azért ez kevés, nem szokás csak úgy belefogni egy ilyen munkába. Mi volt még?

Mint programozó meg akartam valósítani két dolgot:

Volt néhány ötletem az SQL és C++ összekapcsolásáról, ha objektumokat tárolunk az adatbázisban, akkor legyenek azok rendes objektumok a programban is, és csak a legkevesebb dolgot keljen kétszer megcsinálni, vagy ledefiniálni.

A program inkább csak módszereket tartalmazzon, hogy mit kell pontosan csinálni, hogyan viselkedjen, vagy jelenjen meg egy objektum, az az adatbázisban legyen definiálva.

Mondhatnám, hogy ennyi, de még volt egy fontos dolog. Fogalmam nem volt, hogy ez ekkora munka. Ráment egy kis idő, amit bélyeggyűjtésre is fordíthattam volna, de mára van egy rendszer, ami kipróbálható, működik: <https://github.com/csikfer/lanview2>

# Telepítés.

A rendszer elvileg multiplatformos. Tesztelve Ubuntu 18.04 és Windows rendszereken, de Windows alatt néhány funkció (jelenleg) hiányzik.

Az elsődleges platform Linux, és a dokumentáció részletesen tartalmazza a telepítési folyamatot Ubuntu 18.04 -re.

# A rendszer részei

* Adatbázis. PostgreSQL
* lv2 API
* lv2d lekérdező gyökér alkalmazás / daemon.
* Lekérdező alprogramok
* lv2g GUI API
* lv2gui GUI
* Vagyonvédelmi kiegészítő hardver elemek, és a lekérdező alprogram.
* Interpreter (CLI)

# Vagyonvédelem

Van egy napra, pontosabban percre kész adatbázisunk a lekérdezéseknek köszönhetően, így lehetőség nyílik egy, a hálózatfelügyelethez lazábban kapcsolódó, de ugyan olyan fontos funkció betöltésére.

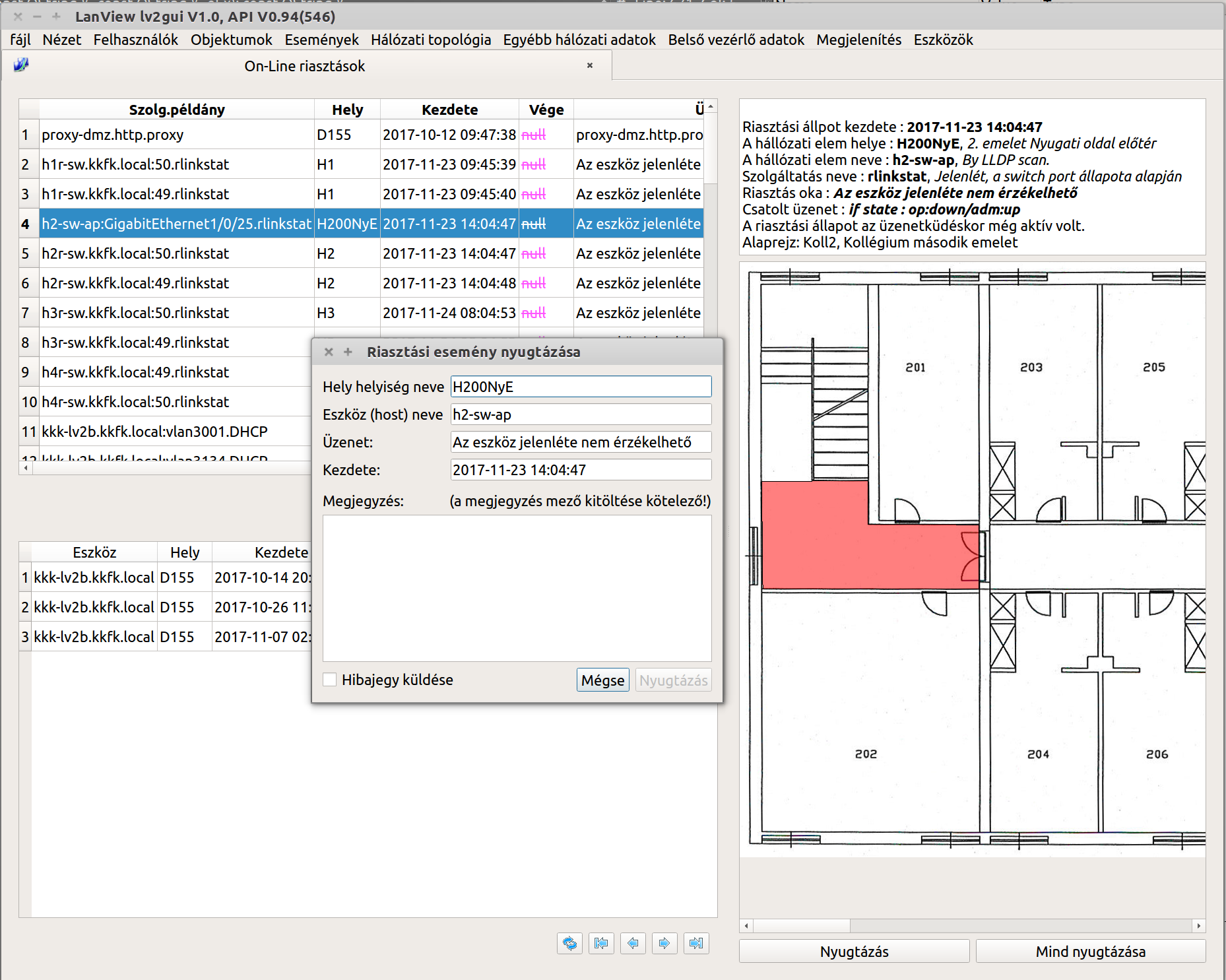
Vannak folyamatosan működő eszközeink, és a munkaállomások jelentős része, ha nem is folyamatos üzemű, de folyamatos tápellátású lehet, így perc pontossággal detektálható a jelenlétük, a switch port állapota alapján. Ha ezeket az eszközöket eltávolítják, a port állapot alapján (up → down) riasztás generálódhat, ami 1-2 perc késleltetéssel megjelenhet egy diszpécseri terminálon.

Viszonylag egyszerű és olcsó hardver elemekkel kibővítve a rendszert, biztosítható olyan elemek védelme is, melyek a hálózat szempontjából passzívak:

* Kontroller: Egy AtMega alapú intelligens eszköz(ök), ami RS485 buszon kommunikál(nak) a lekérdező szerverrel. Az RS485 port lehet a szerveren pl. egy USB átalakítóval, de használhatunk RS485 szerver modult is. Erre csatlakoznak az érzékelők, max. 16db/RS485 csatorna.
* Érzékelő Egy, a védendő eszközre ragasztható eszköz. A rendkívül egyszerű, és így olcsó kétpólusú elem mindössze 3 alkatrészből áll: 2 LED (zöld, vörös), és egy kontaktus. Az érzékelő állapotai: ok, leválasztva, nincs érzékelő (szakadás), rövid-zár, fordított bekötés, hiba.

# És vágjunk a közepébe, néhány funkció

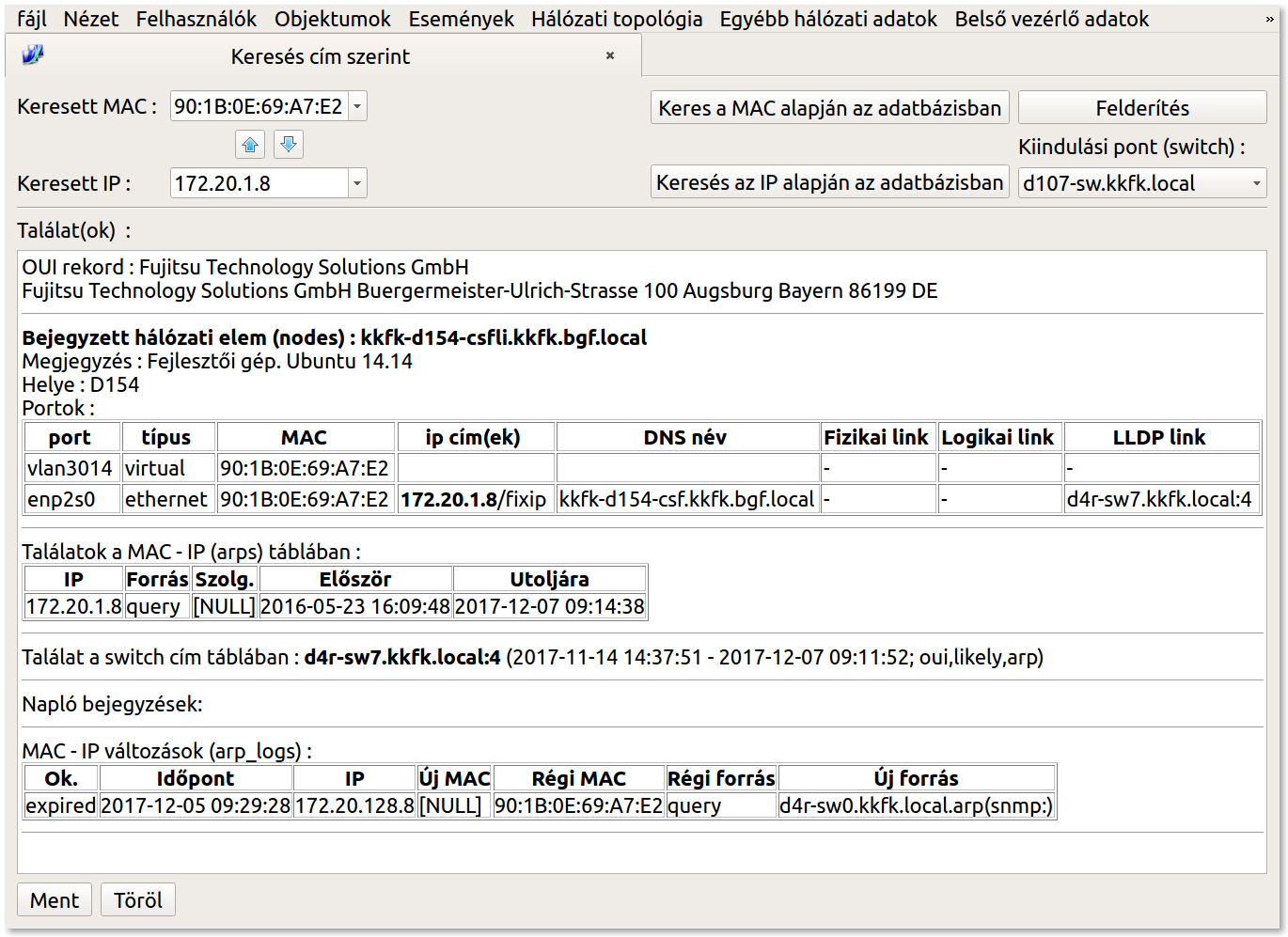
## On-line riasztás, diszpécseri terminál



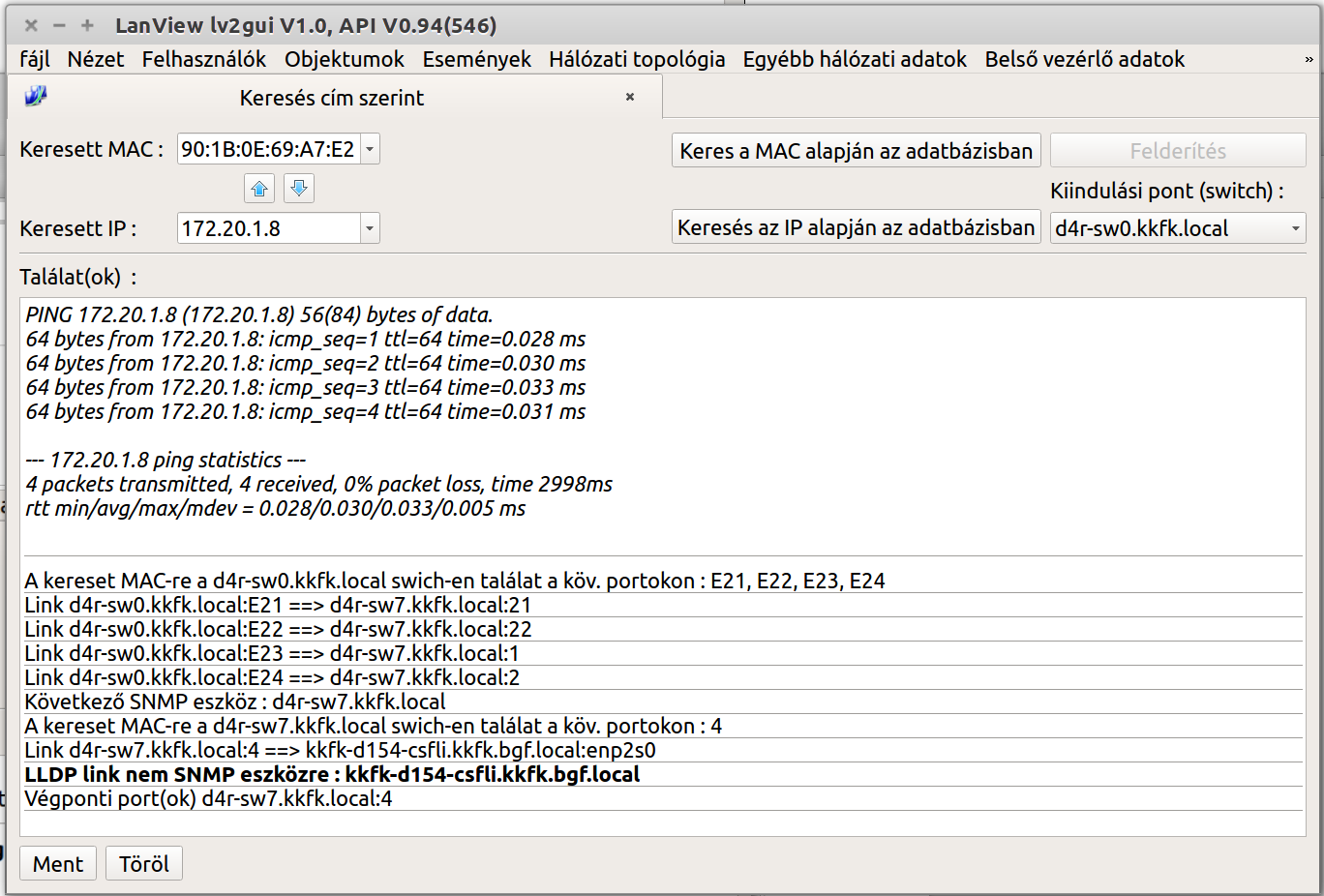
Közvetlen riasztások a diszpécser felé az aktuális zónában.

## Hálózati elem keresése

Az adatbázisban MAC vagy IP alapján, vagy közvetlen keresés a switch cím táblákban



Közvetlenül a switch címtáblákban:



## Hálózati elem(ek) felvétele

Erre több lehetőség van.

* Automatikus, ha az eszköz ismeri az SNMP protokollt. Továbbá, ha az eszközök ismerik (és engedélyezett) az LLDP, akkor a láncon végig haladva az összes SNMP eszköz regisztrálható automatikusan.
* Van egy CLI, több eszköz esetén ez a leghatékonyabb, ha az előző lehetőség nem adott.
* A GUI általános megjelenítő rendszerén keresztül, ez inkább módosítás, vagy javításkor hasznos, vagy ha nincs más lehetőség.
* Végül van egy pár egyedi adatlap:
  + Munkaállomások felvétele vagy módosítása
  + Patch panelek vagy falicsatlakozók felvétele.
  + SNMP eszközök felvétele, frissítése.

### LLDP képes eszközök feltérképezése

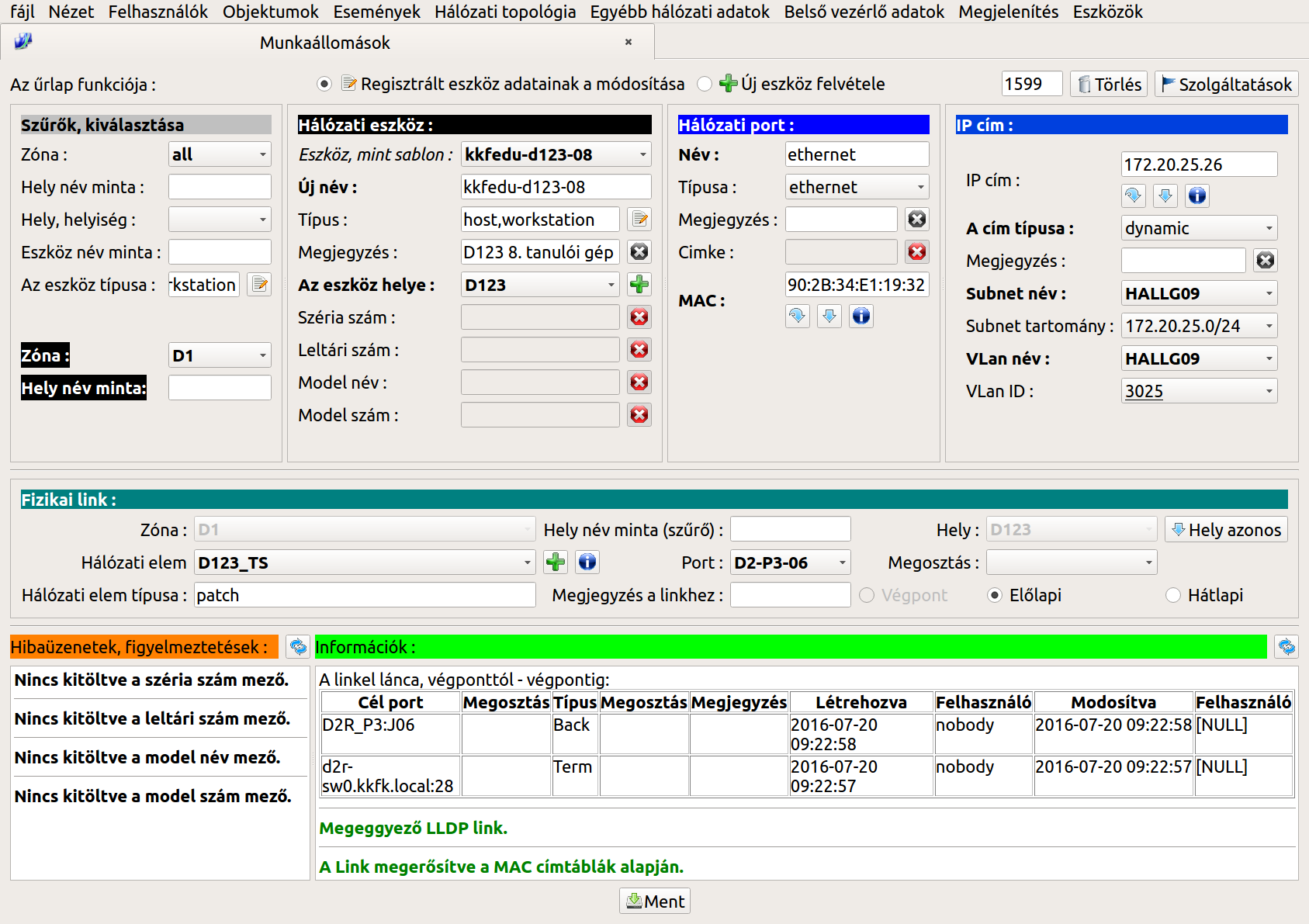
* + 1. A CLI-n keresztül lehetséges. A naplóban megjeleníti a lekérdezés eredményének, és az adatbázis tartalmának az összevetését, illetve a súlyosabb felfedezett problémákról külön bejegyzés készül.

### 

### SNMP eszköz felvétele, frissítése

* + 1. SNMP eszköz felvételének ill. frissítésének legegyszerűbb eszköze, feltéve persze, hogy a eszköz gyártója által implementált SNMP felület választ ad minden kérdésre, ami sajnos sok esetben nem igaz. Ha a lekérdezés eredménye hiányos, vagy esetleg egyes következtetések tévesek, ezeket utólag korrigálni kell. Pl. a HP19xx sorozata nem adja vissza a trönk-ök tagjait, vagy pl. Windows esetén nem állapítható meg egyértelműen az interfész kavalkádban melyek a fizikai interfészek. És vannak olyan eszközök pl. Hivision kamerák, amik elvileg ismerik az SNMP-t de nincs fellelhető MIB fájl, és nem ad vissza semmilyen értékelhető információt.

### Munkaállomások kezelése



Az adatlap olyan eszközök kezelésére alkalmas, melyek egy interfésszel, és egy IP címmel rendelkeznek, tipikusan munkaállomások. Az adatlap folyamatosan riportokban tájékoztatást ad a kitöltött adatokról, ill. Hibákról, segít az egyes adatmezők kitöltésében, ha ez az adatbázis alapján lehetséges, továbbá az egyes elemekről részletes riportot is megjelenít, ha kérjük:

Részletes riport a megadott elemről, vagy az adat alapján.

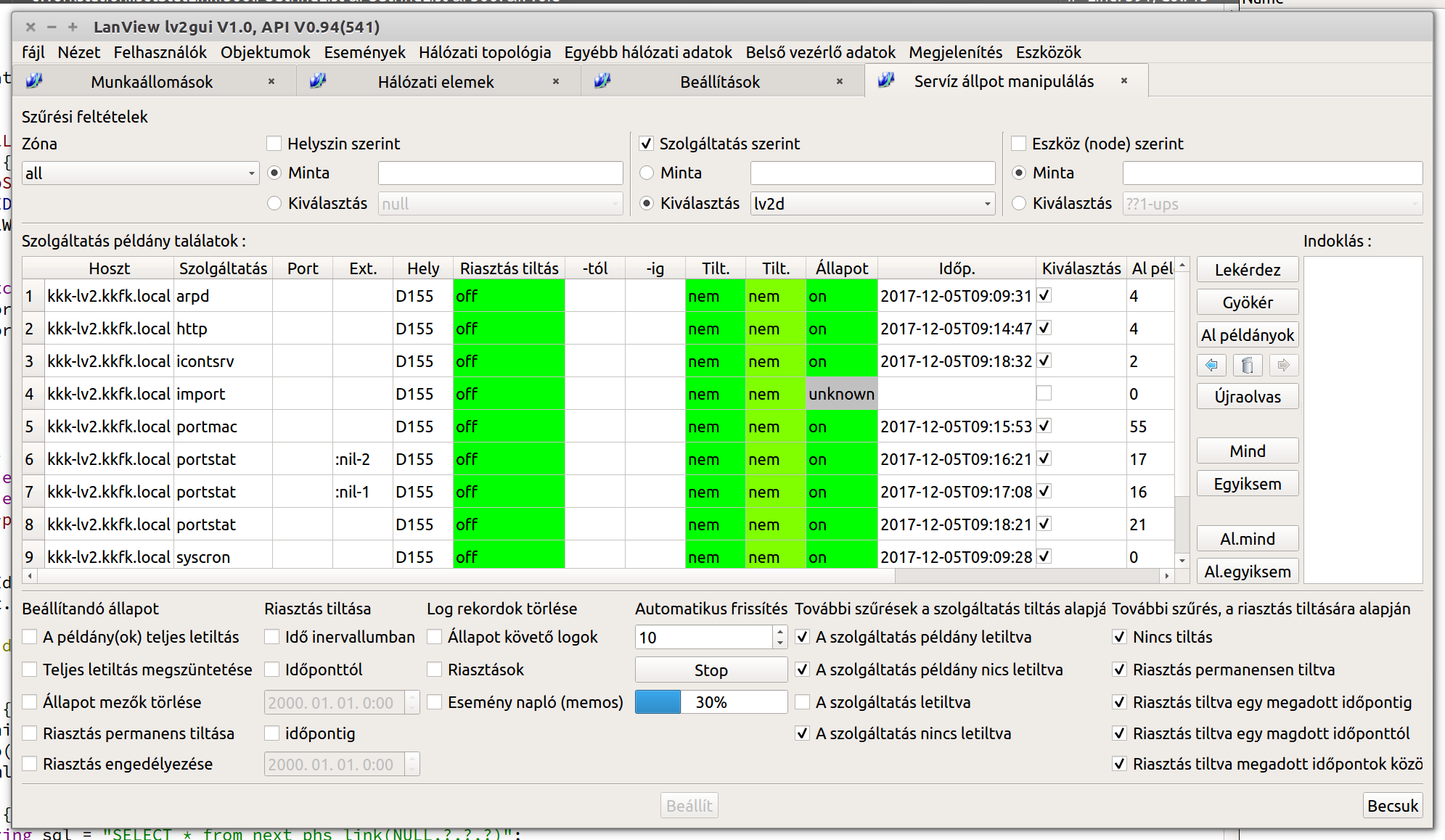
Regisztrált hálózati elem betöltése a megadott MAC vagy IP alapján

MAC vagy IP mező kitöltése a megadott IP ill. MAC alapján.

Új elem (helyiség, falicsatlakozó, vagy patch panel) felvétele.

## Szolgáltatások, lekérdezések

* 1. A Nagios-ból kölcsönzött fogalom, hasonló tulajdonságokkal. Viszont itt nem igazán arról van szó, hogy egy konkrét szolgáltatás elérhető-e, hanem ezen felül jelenthet egy lekérdezést, információ gyűjtést. Ezen felül a lekérdezések hierarchiájának is más az alapja.



### Fali kábelek felfedezése

Végül egy segédeszköz a fali kábelek felvételéhez, ami különböző szempontok alapján próbálja feltérképezni a fali vagyis nem látható összeköttetéseket, ill. ezeket a szempontokat össze is veti egymással.

