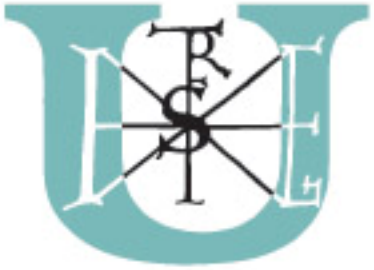


SZENT ISTVÁN EGYETEM

Hálózatbiztonság növelése,
automatikusan konfigurálódó access portok

Cseh Vendel, HBONE Workshop, 2011 november, Mátrafüred

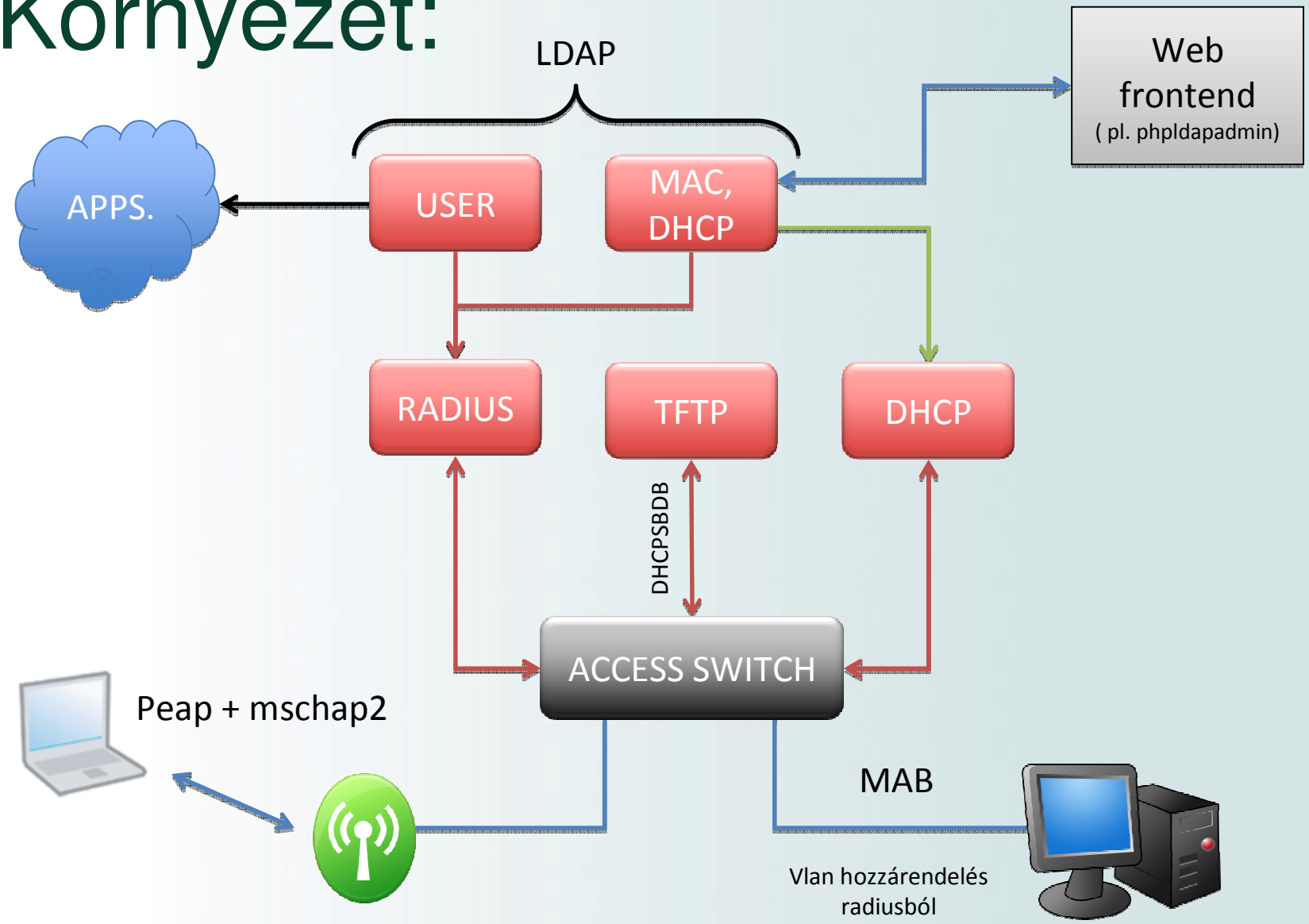
Célok:

- 1db dhcp szerver amit a kari rendszergazdák weben tudnak konfigurálni
- Védjük meg a hálózatot a rosszul csatlakoztatott „véletlenül odakerült” SOHO routerektől (jellemzően kollégium)
- Legyen valamiféle authentikáció a vezetékes hálózaton is
- Idegen gép a „bünti” vlan-ba kerüljön
- Ismert gép a saját vlan-jába kerüljön fali aljzattól függetlenül
- Ne kelljen konfigurálni az ismert gépeket
- Az egészet illesszük hozzá a meglévő radius -hoz

Előzmény:

Ethernet hálózatok tervezése (Balla Attila – Synergon)
http://hbone.hu/Workshop2007/ballaa-ethernet.pdf

Környezet:


LDAP
Web
frontend
(pl. phpldapadmin)
APPS.
USER
MAC,
DHCP
RADIUS
TFTP
DHCP
DHCPSBDB
ACCESS SWITCH
Peap + mschap2
MAB
Vlan hozzárendelés
radiusból

DHCP + LDAP

Előnyök:

•Konfiguráció változás esetén nem kell újraindítani a dhcp démont.
•Akár webről is konfigurálható (pl.: phpldapadmin).
•„realtime” nyilvántartás a delegált ip címekről.

Hátrányok:

•Nehéz bekonfigurálni.
•Stabil kapcsolat kell a dhcp és ldap között.

Megfontolandó:

•DHCP szerver és az ldap management vlanban kommunikáljon?
•Hogyan bontsuk az ldap fát? (nagyon hisztis)

DHCP + LDAP

Példa LDIF:

```
dn: ou=Dhcp-servers,dc=szie,dc=hu
objectclass: organizationalUnit
objectclass: top
ou: Dhcp-servers

dn: cn=dhcp.szie.hu,ou=Dhcp-servers,dc=szie,dc=hu
cn: dhcp.szie.hu
dhcpservicedn: cn=szie.Dhcp.Config,ou=Dhcp-configs,dc=szie,dc=hu
dhcpstatements: authoritative
objectclass: dhcpServer
objectclass: top

dn: ou=Dhcp-configs,dc=szie,dc=hu
objectclass: organizationalUnit
objectclass: top
ou: Dhcp-configs

dn: cn=szie.Dhcp.Config,ou=Dhcp-configs,dc=szie,dc=hu
cn: szie.Dhcp.Config
dhcpprimarydn: cn=dhcp.szie.hu,ou=Dhcp-servers,dc=szie,dc=hu
objectclass: dhcpService
objectclass: top

dn: cn=Subnets,cn=szie.Dhcp.Config,ou=Dhcp-configs,dc=szie,dc=hu
cn: Subnets
objectclass: dhcpGroup
objectclass: top
```

DHCP + LDAP

Példa LDIF:

dn: cn=192.168.1.0,cn=Subnets,cn=szie.Dhcp.Config,ou=Dhcp-configs,dc=szie,dc =hu
cn: 192.168.1.0 dhcpnetmask: 24
dhcpoption: routers 192.168.1.1
dhcpoption: subnet-mask 255.255.255.0
dhcpoption: domain-name-servers 192.168.1.251
dhcpoption: domain-name „plvlan.szie.hu"
dhcpstatements: default-lease-time 14399
dhcpstatements: max-lease-time 28799
objectclass: dhcpSubnet objectclass: top

dn: cn=Known Pool,cn=192.168.1.0,cn=Subnets,cn=szie.Dhcp.Config,ou=Dhcp-conf igs,dc=szie,dc=hu
cn: Known Pool
dhcprange: 192.168.1.2 192.168.1.250
objectclass: dhcpPool
objectclass: top

DHCP + LDAP

Dhcpd.conf:

```
ldap-server „ip ip ip ip";
ldap-port 389;
ldap-username "uid= ,ou= ,dc= ,dc= ";
ldap-password „szupertitok";
ldap-base-dn "dc= ,dc= ";
ldap-method dynamic;
ldap-debug-file "/var/log/dhcp-ldap-startup.log";
```

Ip cím delegálása:

```
dn: cn=011.Cseh.Vendel,cn=192.168.1.0,cn=Subnets,cn=noc.Dhcp.Config,ou=Dhcp -configs,dc=szie,dc=hu
cn: 011.Cseh.Vendel
dhcphwaddress: ethernet 00:1a:6b:d4:e6:e8
dhcpstatements: fixed-address 192.168.1.11
objectclass: dhcpHost
objectclass: top
```

(web felületen pár kattintás)

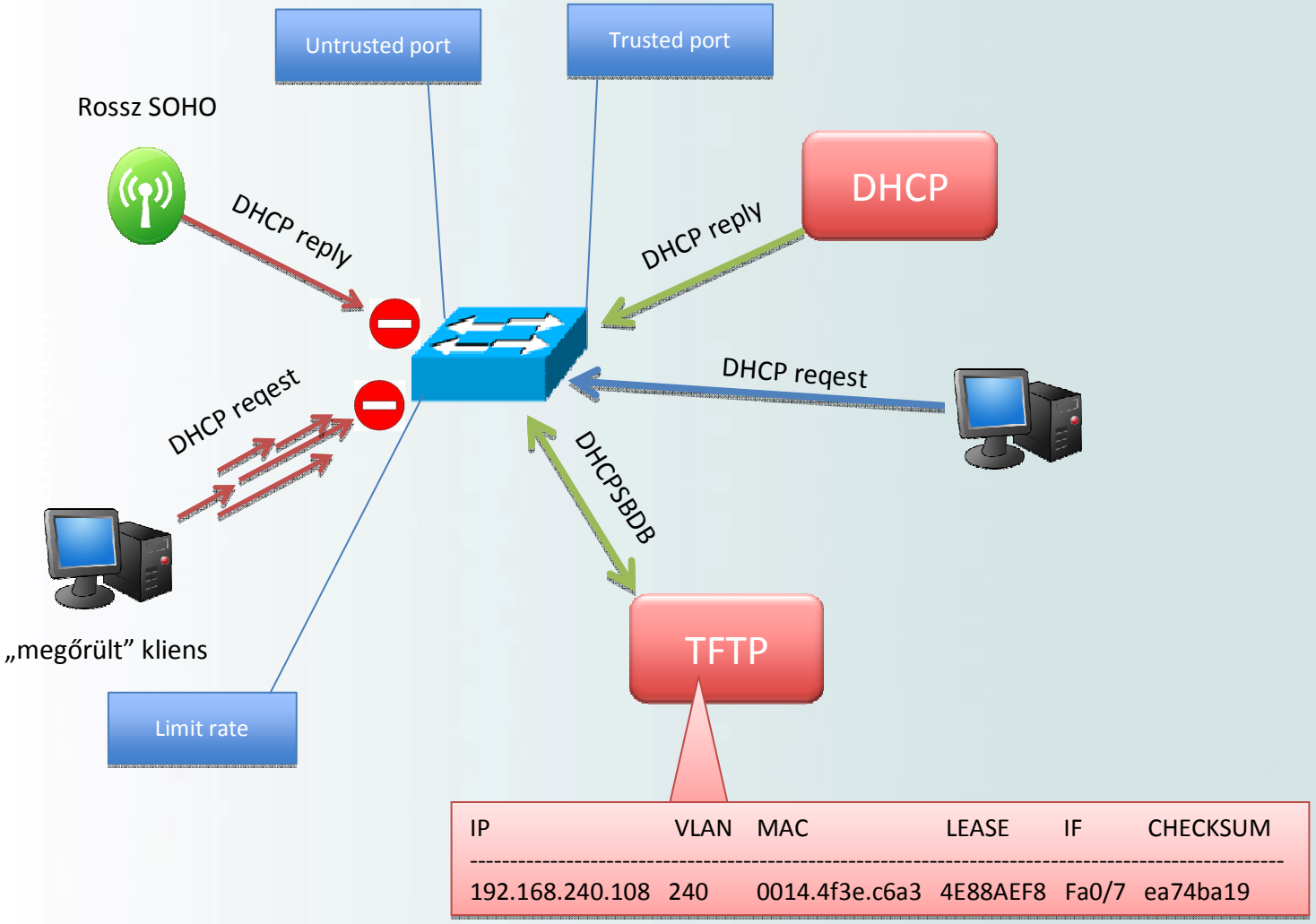
DHCP Snooping

Kollégiumokban tipikus probléma a gyári konfiguráción hagyott rosszul bedugott „véletlenül” odakerült SOHO router!

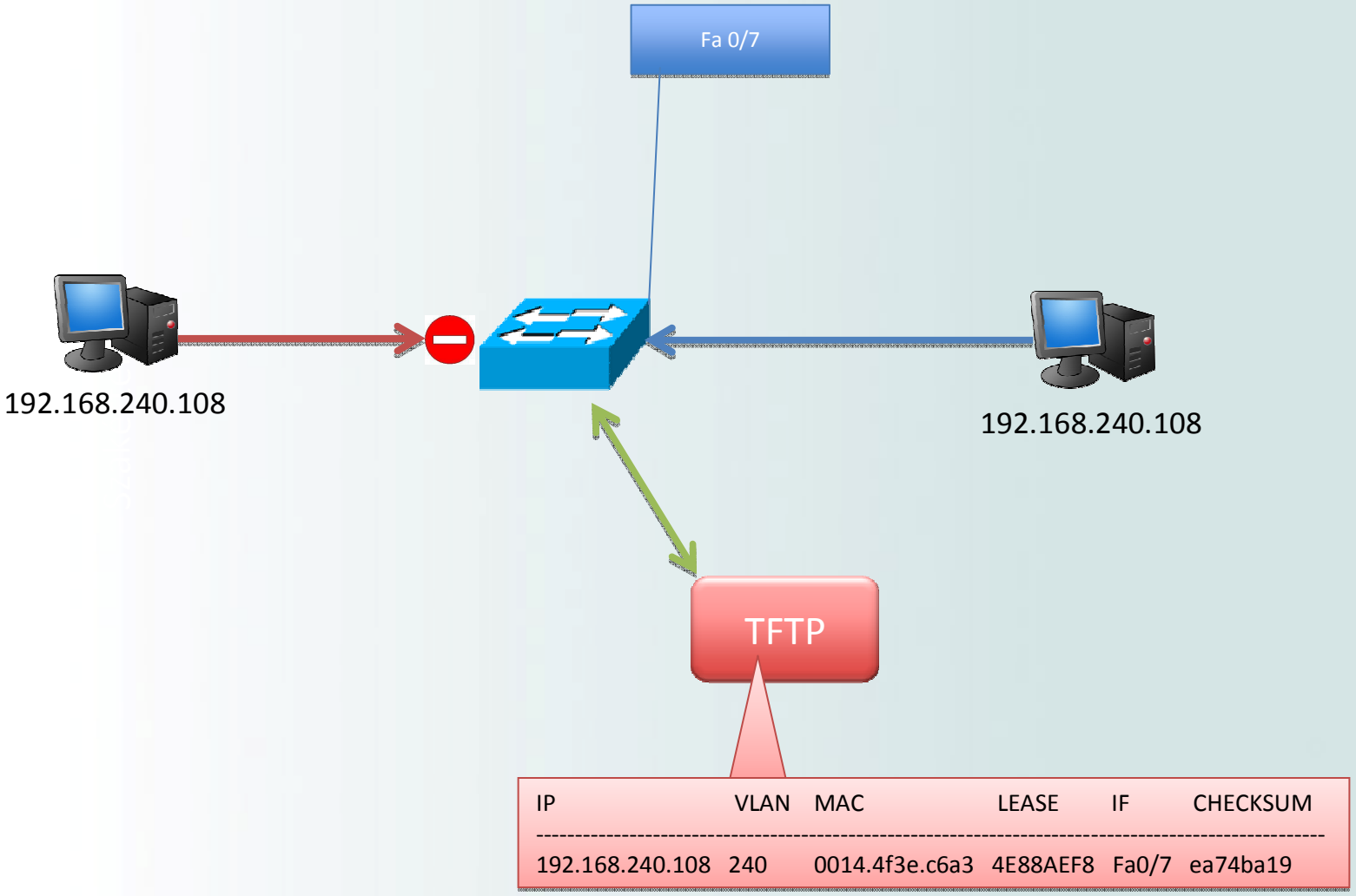
Problémát okozhat egy „megőrült” kliens is aki a túl sok kéréssel Dos-olja a dhcp szerverünket.

99%, hogy a 4 LAN port valamelyikét csatlakoztatják bekapcsolt DHCP –vel!

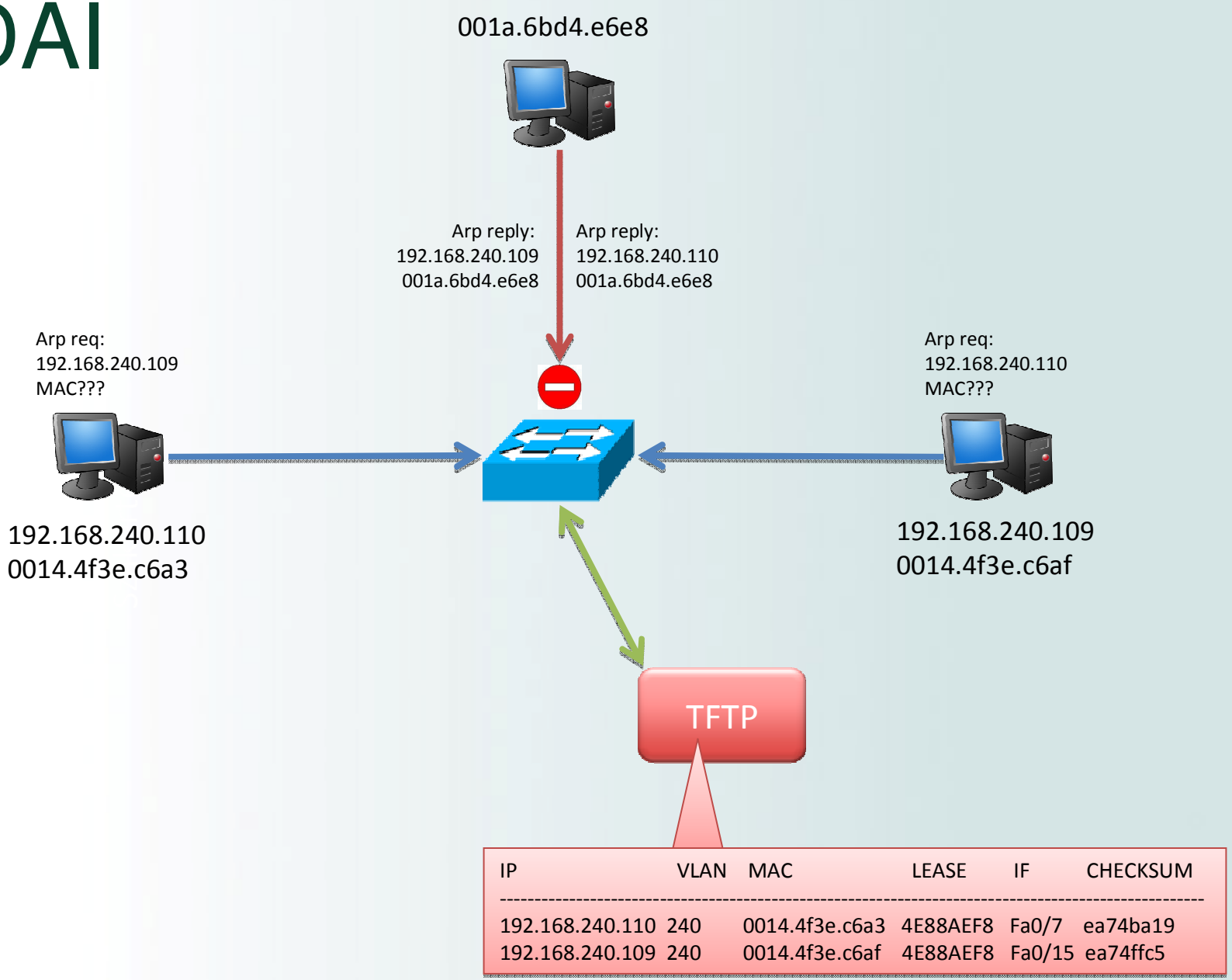
DHCP Snooping



IPSG


Fa 0/7
192.168.240.108
192.168.240.108
TFTP
IP VLAN MAC LEASE IF CHECKSUM
192.168.240.108 240 0014.4f3e.c6a3 4E88AEF8 Fa0/7 ea74ba19

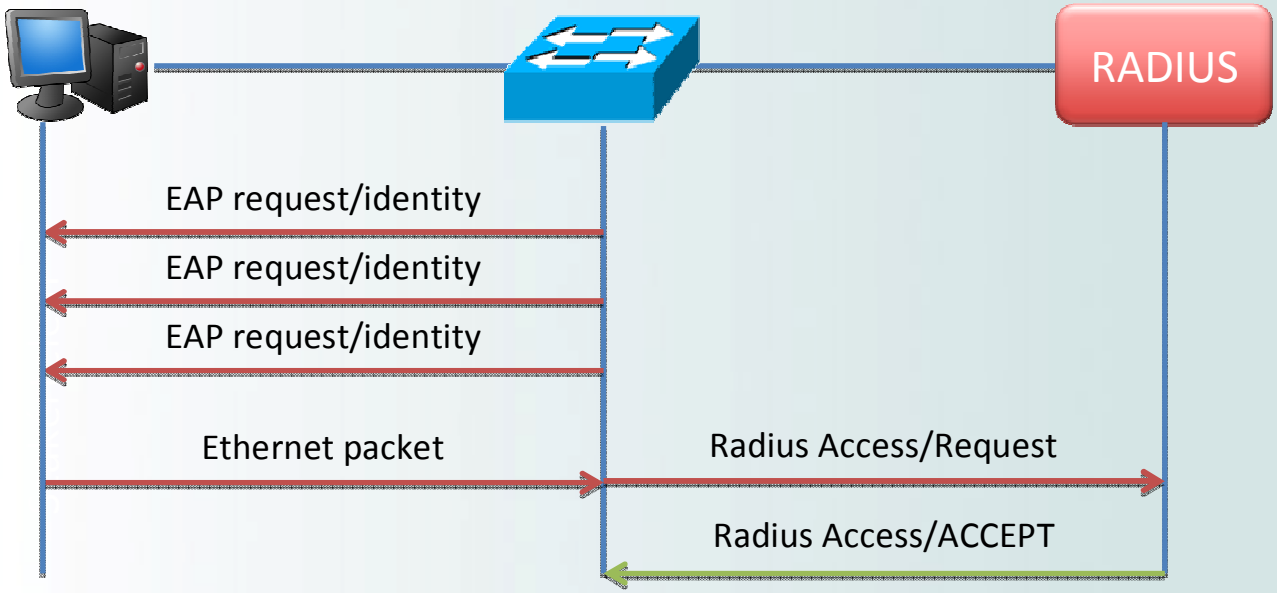
DAI


001a.6bd4.e6e8
Arp reply:
192.168.240.109
001a.6bd4.e6e8
Arp reply:
192.168.240.110
001a.6bd4.e6e8
Arp req:
192.168.240.109
MAC???
Arp req:
192.168.240.110
MAC???
192.168.240.110
0014.4f3e.c6a3
192.168.240.109
0014.4f3e.c6af
TFTP
IP VLAN MAC LEASE IF CHECKSUM
192.168.240.110 240 0014.4f3e.c6a3 4E88AEF8 Fa0/7 ea74ba19
192.168.240.109 240 0014.4f3e.c6af 4E88AEF8 Fa0/15 ea74ffc5

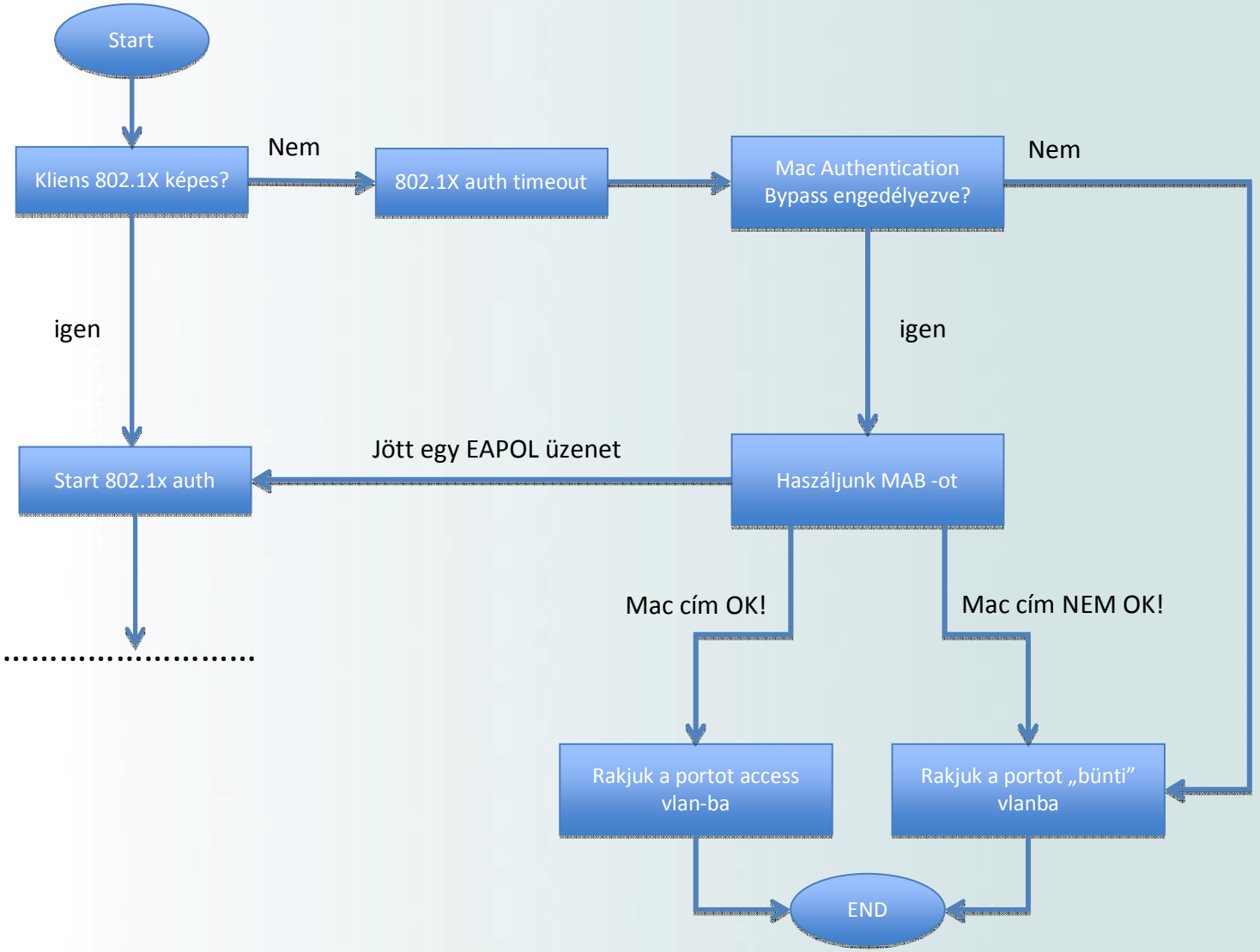
802.1x vs MAB

802.1x (kliens oldalon konfigurálni kell)	MAC authentication bypass
• VLAN assignment • Per-user ACL • Filter-ID attribute • Downloadable ACL • Redirect URL	• **VLAN assignment** • Per-user ACL • Filter-ID attribute • Downloadable ACL • Redirect URL

MAB


RADIUS
EAP request/identity
EAP request/identity
EAP request/identity
Ethernet packet
Radius Access/Request
Radius Access/ACCEPT

MAB



Szent István Egyetem, 2100 Gödöllô, Páter Károly utca 1. Tel.: 06-28-522-000. Fax: 06-28-410-804. E-mail: info@szie.hu

Radius igazítás 2x LDAP

```
ldap mac {
        server = „ipipipip"

        identity =  "uid=,ou=,ou=,dc=,dc="
        password =
        basedn = "ou=,dc=,dc="

        base_filter = "(cn=%{Stripped-User-Name:-%{User-Name}})"
        start_tls = no
        access_attr = "cn"
        dictionary_mapping = ${raddbdir}/ldap.mac.attrmap
        authtype = ldap
        ldap_connections_number = 5
        timeout = 4
        timelimit = 3
        net_timeout = 1
        }
```

Radius igazítás 2x LDAP

```
ldap wifi {
        server = „ipipipip"

        identity = "uid=,ou=,o=,o=,c="
        password =
        basedn = "ou=,o=,o=,c="

        base_filter = ""
        start_tls = no
        access_attr = "uid"
        dictionary_mapping = ${raddbdir}/ldap.attrmap
        authtype = ldap
        ldap_connections_number = 5
        timeout = 4
        timelimit = 3
        net_timeout = 1
        }
```

Radius igazítás 2x LDAP

```
authorize {
        redundant {
                wifi {
                        fail = 1
                        noop = 2
                        notfound = 3
                        ok = return
                        reject = return
                        userlock = return
                        invalid = return
                }
                mac {
                        fail = 1
                        noop = 2
                        notfound = 3
                        ok = return
                        reject = return
                        userlock = return
                        invalid = return
                }
}
```

Példa LDIF

dn: uid=001a6bd4e6e8,ou=Vlan23,ou=Mac-addresses,dc=szie,dc=hu
cn: 001a6bd4e6e8
objectclass: account
objectclass: simpleSecurityObject
objectclass: top
objectclass: uidObject
objectclass: radiusprofile
radiustunnelmediumtype: IEEE-802
radiustunnelprivategroupid: 20
radiustunneltype: VLAN
uid: 001a6bd4e6e8
userpassword: 001a6bd4e6e8

Példa swhtchkonf:

```
ip dhcp snooping vlan 2-1000
ip dhcp snooping database tftp://ipipip/snoop-databases/asw-flexdesk
ip dhcp snooping
!
 switchport mode access
 authentication event fail action authorize vlan buntivlan
 authentication event no-response action authorize vlan buntivlan
 authentication order mab dot1x
 authentication port-control auto
 mab
 spanning-tree portfast
 ip verify source
 ip dhcp snooping limit rate 50
!
interface GigabitEthernet0/1
 description uplink
 switchport mode trunk
 ip arp inspection trust
 ip dhcp snooping trust
!
radius-server host …. auth-port …. acct-port …. key ….
radius-server vsa send authentication
```