# Síť LAN

- semestrální práce X32PRS
- Ondřej Caletka
- caleto1@fel.cvut.cz

# Zadání

- Z CSV souboru generovat konfigurační soubory pro služby sítě LAN:
  - DHCP server
  - DNS server
  - NAT 1:1 (volitelně)
- CSV soubor musí obsahovat záhlaví, být lidsky čitelný

# Řešení - uživatelský pohled

- skript *parsecsv.sh* nemá parametry
  - konfigurační volby je možno upravit na začátku skriptu
  - na standardní chybový výstup jsou posílána různá hlášení podle nastavené DEBUG úrovně
- Každý konfigurační soubor se skládá z šablony hlavičky, šablony patičky a vlastního obsahu
  - v hlavičkách a patičkách jsou nahrazeny %PROMĚNNÉ%
- Pro funkci NAT 1:1 je vygenerován skript, který nadefinuje potřebné záznamy do dvou uživatelsky definovaných řetězů v *nat* tabulce.

# Řešení - struktura programu

- načtení proměnných, úprava jejich formátu (sed)
- příprava sed-skriptu pro náhradu %PROMĚNNÝCH% v šablonách
- založení výstupních souborů podle šablon hlaviček
- iterace přes všechny řádky CSV souboru
  - kontrola, zda řádky obsahují platné IP a MAC adresy
  - rozdělení řádku na jednotlivá pole
  - přidání záznamů do všech konfiguračních souborů
- přidání patiček na konec konfiguračních souborů

# Příklady

- Vstupní CSV soubor
- Šablona dopředného DNS záznamu
- Výstup dopředné a reverzní DNS konfigurace
- Šablona dhcpd.conf
- Příklad výstupu dhcpd.conf
- Příklad výstupu ip_nat.sh

# Vstupní CSV soubor

"Jméno uživatele","IP adresa","DNS jméno","MAC adresa","veřejná IP"
"admin","192.168.0.254","router","004f4e001122",
"user1","147.32.127.241","shdns","ffffff000000",
"user2","192.168.0.138","zyxel","00ab0e12df5a",

# Příklad šablony dopředné DNS

```
%LAN_DNS%            IN SOA  gw.%LAN_DNS% root.gw.%LAN_DNS% (
                     %SERIAL%   ; serial
                     10800      ; refresh (3 hours)
                     900        ; retry (15 minutes)
                     604800     ; expire (1 week)
                     86400      ; minimum (1 day)
                     )
                NS      ns.%LAN_DNS%

localhost            IN      A       127.0.0.1

;nasleduje automaticky generovany obsah
;---------------------------------------
```

# Příklad doma.net.zone

```
doma.net.               IN SOA  gw.doma.net. root.gw.doma.net. (
                                2007122823   ; serial
                                10800      ; refresh (3 hours)
                                900        ; retry (15 minutes)
                                604800     ; expire (1 week)
                                86400      ; minimum (1 day)
                                )
                        NS      ns.doma.net.
;nasleduje automaticky generovany obsah
;---------------------------------------
router          IN      A       192.168.0.254
shdns           IN      A       147.32.127.241
zyxel           IN      A       192.168.0.138
;-----------------------------------------------
;konec generovaneho obsahu

;definice aliasu
gw              IN      CNAME   router
ns              IN      CNAME   router
```

# Příklad 0.168.192.in-addr.arpa.zone

```
0.168.192.in-addr.arpa.    IN SOA  gw.doma.net. root.gw.doma.net. (
                                   2008010323   ; serial
                                   10800      ; refresh (3 hours)
                                   900        ; retry (15 minutes)
                                   604800     ; expire (1 week)
                                   86400      ; minimum (1 day)
                                   )
                           NS      ns.doma.net.

;nasleduje automaticky generovany obsah
;---------------------------------------

254             IN      PTR     router.doma.net.
138             IN      PTR     zyxel.doma.net.

;-----------------------------------------
;konec generovaneho obsahu
```

# Šablona dhcpd.conf

```
option domain-name "%LAN_DNS%";
option domain-name-servers ns.%LAN_DNS%;

default-lease-time 600;
max-lease-time 7200;

# If this DHCP server is the official DHCP server for the local
# network, the authoritative directive should be uncommented.
#authoritative;

subnet %LAN_IP%.0 netmask 255.255.255.0 {
  option routers gw.%LAN_DNS%;
#  range %LAN_IP%.200 %LAN_IP%.250;
}

#Nasleduje automaticky generovany seznam definic hostu
##################################################
```

# Příklad dhcpd.conf

```
subnet 192.168.0.0 netmask 255.255.255.0 {
  option routers gw.doma.net.;
#  range 192.168.0.200 192.168.0.250;
}
#Nasleduje automaticky generovany seznam definic hostu
#####################################################
host router {
  hardware ethernet 00:4f:4e:00:11:22;
  fixed-address 192.168.0.254;
}
host zyxel {
  hardware ethernet 00:ab:0e:12:df:5a;
  fixed-address 192.168.0.138;
}
#####################################################
#Konec automaticky generovaneho seznamu
```

# Příklad skriptu ip_nat.sh

```
#!/bin/bash
# Skript pro automatickou konfiguraci NATu 1:1

IPT=`which iptables`
#IPT=iptables  #alternativne
#IPT=/sbin/iptables #dalsi alternativa

#vymazani predchozich pravidel
${IPT} -t nat -F extip_snat
${IPT} -t nat -F extip_dnat

#Nasleduji vygenerovana pravidla
#################################
${IPT} -t nat -A extip_snat -s 192.168.0.1 -d \! 192.168.0.0/24 -j SNAT
   --to-source 147.32.127.252
${IPT} -t nat -A extip_dnat -d 147.32.127.252 -j DNAT --to-destination
   192.168.0.1
#################################
#Konec vygenerovanych pravidel
```

# Závěr

- Funkčnost skriptu je omezena pouze na sítě s maskou C (255.255.255.0)
- Pokud bude skript spouštěn častěji než 1x za hodinu, nebude patřičně zvýšeno sériové číslo databáze DNS
- Pro funkčnost NAT 1:1 je třeba zajistit projití uživatelských řetězů *extip_snat* a *extip_dnat* z hlavních řetězů *POSTROUTING* a *PREROUTING* tabulky *nat*.
  - iptables -t nat -A POSTROUTING -j extip_snat
  - iptables -t nat -A PREROUTING -j extip_dnat

# Závěr

Děkuji za pozornost