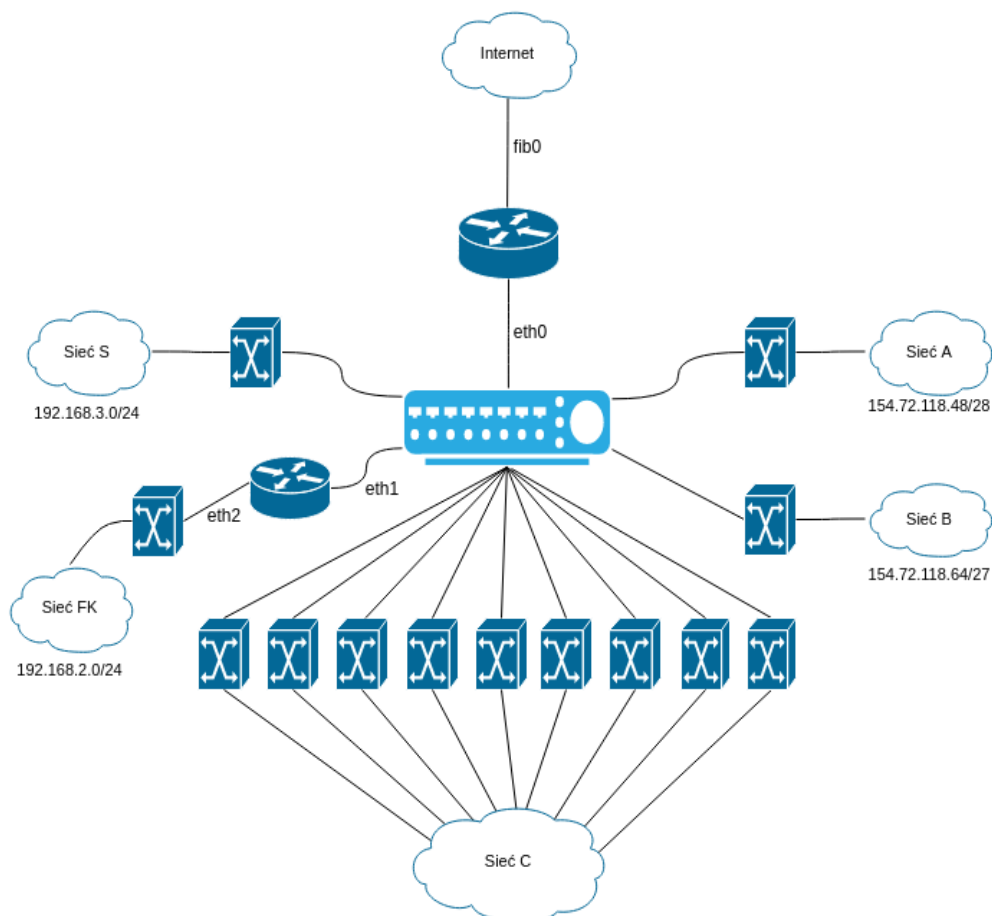


Projekt sieci komputerowej

Przedmiot SKM, lato 2020



Sieć	Adres	Maska	Zakres IP	Adres rozgłoszeniowy	Adres bramy domyślnej
Provider <=> router	154.72.118.40	255.255.255.248	154.72.118.41 - 154.72.118.46	154.72.118.47	154.72.118.41
A	154.72.118.48	255.255.255.240	154.72.118.49 - 154.72.118.62	154.72.118.63	154.72.118.49
B	154.72.118.64	255.255.255.224	154.72.118.65 - 154.72.118.94	154.72.118.95	154.72.118.65
C	192.168.1.0	255.255.255.0	192.168.1.1 - 192.168.1.254	192.168.1.255	192.168.1.1
FK	192.168.2.0	255.255.255.0	192.168.2.1 - 192.168.2.254	192.168.2.255	192.168.2.1
S	192.168.3.0	255.255.255.0	192.168.3.1 - 192.168.3.254	192.168.3.255	192.168.3.1
RTtoFK	192.168.4.0	255.255.255.0	192.168.4.1 - 192.168.4.254	192.168.4.255	192.168.4.1

Opis interfejsów routerów działających w sieci:

Router	Nazwa interfejsu	Opis
R0	fib0	Służy do połączenia z dostawcą internetu
R0	eth0	Do połączenia ze switchem zarządzanym
RFK	eth1	Do połączenia ze switchem zarządzanym
RFK	eth2	Do połączenia ze switchem niezarządzanym sieci FK

Opis portów switcha zarządzanego, porty typu 1000Base-T:

Nr	Nazwa	Opis
1	eth0	Do połączenia z routerem głównym
2	ethA	Do połączenia z niezarządzanym switchem sieci A
3	ethB	Do połączenia z niezarządzanym switchem sieci B
4	ethC1..9	Do połączenia z niezarządzanymi switchami sieci C
5	ethRFK	Do połączenia z routerem sieci FK
6	ethS	Do połączenia z niezarządzanym switchem sieci S

Sieci VLAN i ich przypisanie:

10 - A
20 - B
30 - C
40 - RToFK
50 - S

Plik konfiguracyjny switcha zarządzanego:

```
source /etc/network/interfaces.d/*
```

```
auto lo  
iface lo inet loopback
```

```
allow-hotplug eth0
```

```
auto eth0.10  
iface eth0.10 inet manual
```

```
auto eth0.20  
iface eth0.20 inet manual
```

```
auto eth0.30  
iface eth0.30 inet manual
```

```
auto eth0.40  
iface eth0.40 inet manual
```

```
auto eth0.50  
iface eth0.50 inet manual
```

```
allow-hotplug ethA  
iface ethA inet manual
```

Lukasz Pokorzyński, nr 300251

```
allow-hotplug ethB
iface ethB inet manual
```

```
allow-hotplug ethC1
iface ethC1 inet manual
#[...]
```

```
allow-hotplug ethRFK
iface ethRFK inet manual
```

```
allow-hotplug ethS
iface ethS inet manual
```

```
brctl addbr br0
brctl addif br0 eth0.10
brctl addif br0 ethA
```

```
brctl addbr br1
brctl addif br1 eth0.20
brctl addif br1 ethB
```

```
brctl addbr br2
brctl addif br2 eth0.30
brctl addif br2 ethC1
#[...]
```

```
brctl addbr br3
brctl addif br3 eth0.40
brctl addif br3 ethRTFK
```

```
brctl addbr br4
brctl addif br4 eth0.50
brctl addif br4 ethS
```

```
ip link set dev br0 up
ip link set dev br1 up
ip link set dev br2 up
ip link set dev br3 up
ip link set dev br4 up
```

Dodatki

1. Projekt sieci

1)

```
# loopback
auto lo
iface lo inet loopback
```

```
iface fib0 inet static
    address 154.72.118.42
    netmask 255.255.255.248
    gateway 154.72.118.41
```

```
iface eth0.10 inet static
    address 154.72.118.49
    netmask 255.255.255.240
    network 154.72.118.48
```

```
iface eth0.20 inet static
    address 154.72.118.65
```

Łukasz Pokorzyński, nr 300251

```
netmask 255.255.255.224
network 154.72.118.64
```

```
iface eth0.30 inet static
address 192.168.1.1
netmask 255.255.255.0
network 192.168.1.0
```

```
iface eth0.40 inet static
address 192.168.4.1
netmask 255.255.255.0
network 192.168.4.0
```

```
iface eth0.50 inet static
address 192.168.3.1
netmask 255.255.255.0
network 192.168.3.0
```

2)

```
# loopback
auto lo
iface lo inet loopback
```

```
iface eth1 inet static
address 192.168.4.2
netmask 255.255.255.0
network 192.168.4.0
```

```
iface eth2 inet static
address 192.168.2.254
netmask 255.255.255.0
network 192.168.2.0
```

2. Routing

3) Router główny

Cel	Gateway	Maska	Interfejs
154.72.118.40	0.0.0.0	255.255.255.248	fib0
154.72.118.48	0.0.0.0	255.255.255.240	eth0.10
154.72.118.64	0.0.0.0	255.255.255.224	eth0.20
192.168.1.0	0.0.0.0	255.255.255.0	eth0.30
192.168.2.0	192.168.4.2	255.255.255.0	eth0.40
192.168.3.0	0.0.0.0	255.255.255.0	eth0.50
192.168.4.0	0.0.0.0	255.255.255.0	eth0.40
0.0.0.0	154.72.118.41	0.0.0.0	fib0

Router dodatkowy FK

Cel	Gateway	Maska	Interfejs
192.168.4.0	0.0.0.0	255.255.255.0	eth1
192.168.2.0	0.0.0.0	255.255.255.0	eth2
0.0.0.0	192.168.4.1	0.0.0.0	eth1

4) Reguły iptables translacji adresów

```
iptables --table nat --append POSTROUTING --out-interface fib0 -j SNAT -- source 192.168.1.0/24 --to-source 154.72.118.42
iptables --table nat --append POSTROUTING --out-interface fib0 -j SNAT -- source 192.168.2.0/24 --to-source 154.72.118.42
iptables --table nat --append POSTROUTING --out-interface fib0 -j SNAT -- source 192.168.3.0/24 --to-source 154.72.118.42
```

5) Reguły iptables filtracji

```
iptables -A FORWARD -s 192.168.1.0/24 -d 0/0 -p tcp --match multiport --dports http,https,smtp,imap,pop3 -j ACCEPT
iptables -A FORWARD -s 192.168.1.0/24 -d 0/0 -p udp --match multiport --dports domain,bootps,bootpc -j ACCEPT
iptables -A FORWARD -s 192.168.1.0/24 -d 0/0 -p icmp -j ACCEPT
iptables -A FORWARD -s 192.168.1.0/24 -d 0/0 -j DROP

iptables -A FORWARD -s 154.72.118.48/29 -d 192.168.3.3 -p tcp --match multiport --dports ldaps -j ACCEPT
iptables -A FORWARD -s 154.72.118.64/27 -d 192.168.3.3 -p tcp --match multiport --dports ldaps -j ACCEPT
iptables -A FORWARD -s 192.168.2.0/24 -d 192.168.3.3 -p tcp --match multiport --dports ldaps -j ACCEPT
iptables -A FORWARD -s 192.168.2.0/24 -d 192.168.3.2 -p tcp --match multiport --dports mysql -j ACCEPT

iptables -A FORWARD -d 192.168.3.0/24 -j DROP
```

Aby możliwa była komunikacja między siecią FK, a siecią RtoFK (RouterToFK), wymagana jest reguła statycznego routingu:

```
ip route add 192.168.2.0/24 via 192.168.4.2
```

3. Konfiguracja usługi DHCP

6) Adres IP i MAC

Adres IPv4 192.168.1.30

Adres IPv6 fe80::bc4:eb5f:7cf3:584b

Adres sprzętowy 60:E3:27:00:0D:C5

7) /etc/dhcp/dhcpd.conf

```
# podsieć A
subnet 154.72.118.48 netmask 255.255.255.240 {
    option routers 154.72.118.49;
}

# podsieć B
subnet 154.72.118.64 netmask 255.255.255.224 {
    option routers 154.72.118.65;
}
```

Łukasz Pokorzyński, nr 300251

```
# podsieć C
subnet 192.168.1.0 netmask 255.255.255.0 {
    range 192.168.1.54 192.168.1.254;
    option routers 192.168.1.1;
}

# podsieć FK
subnet 192.168.2.0 netmask 255.255.255.0 {
    option routers 192.168.2.1;
}

# podsieć S
subnet 192.168.3.0 netmask 255.255.255.0 {
    range 192.168.3.10 192.168.3.14;
    option routers 192.168.3.1;
}
host dns-film-skm-tv {
    hardware ethernet 60:e3:27:d6:70:b3;
    fixed-address 154.72.118.50;
    server-name „ns.film.skm.tv”;
}

host dns-jigsaw-film-skm-tv {
    hardware ethernet 60:e3:27:cd:67:59;
    fixed-address 154.72.118.51;
    server-name „ns.jigsaw.film.skm.tv”;
}

host server-mail {
    hardware ethernet 60:e3:27:1e:c4:bc;
    fixed-address 154.72.118.53;
    server-name „mail.film.skm.tv”;
}

host server-www {
    hardware ethernet 60:e3:27:0a:e4:44;
    fixed-address 154.72.118.54;
    server-name „beta.film.skm.tv”;
}

host dbsrv {
    hardware ethernet 60:e3:27:6a:95:df;
    fixed-address 192.168.3.2;
    server-name „dbsrv.film.skm.tv”;
}

host ldapsrv-server {
    hardware ethernet 60:e3:27:99:9a:dc;
    fixed-address 192.168.3.3;
    server-name „ldapsrv.film.skm.tv”;
}

host Bclient1 {
    hardware ethernet 60:e3:27:d9:c5:86;
    fixed-address 154.72.118.66;
}

host Bclient2 {
```

Łukasz Pokorzyński, nr 300251

```
        hardware ethernet 60:e3:27:d9:c5:87;
        fixed-address 154.72.118.67;
    }

    host Bclient3 {
        hardware ethernet 60:e3:27:d9:c5:88;
        fixed-address 154.72.118.68;
    }
    #[...]
    host FKclient1 {
        hardware ethernet 60:e3:27:d9:c5:41;
        fixed-address 192.168.2.10;
    }

    host FKclient2 {
        hardware ethernet 60:e3:27:d9:c5:42;
        fixed-address 192.168.2.11;
    }

    host FKclient3 {
        hardware ethernet 60:e3:27:d9:c5:43;
        fixed-address 192.168.2.12;
    }
    #[...]
```

8) /etc/network/interfaces

source /etc/network/interfaces.d/*

```
auto lo
iface lo inet loopback

iface eth0 inet static
    address 154.72.118.52
    netmask 255.255.255.248
    network 154.72.118.49
```

4. Konfiguracja usługi DNS

Opcje, które są ważne dla obu serwerów DNS:

```
acl goodclients {
    192.168.1.0/24;
    localhost;
    192.168.2.0/24;
    192.168.3.0/24;
    192.168.4.0/24;
    154.72.118.48/28;
    154.72.118.64/27;
    154.72.118.40/29
};

options {
    directory "/var/cache/bind";
    forwarders {
        8.8.8.8;
    };
    recursion yes;
    allow-query { goodclients; };
    dnssec-validation auto;
    listen-on-v6 { any; };
}
```

Łukasz Pokorzyński, nr 300251

};

9) Pliki konfiguracyjne i administracyjne dla ns.film.skm.tv

```
zone "film.skm.tv" {
    type master;
    file "/etc/bind/film.skm.tv";
    notify yes;
    also-notify { 154.72.118.51; };
    allow-transfer { 154.72.118.51; };
};
```

```
zone "jigsaw.film.skm.tv" {
    type forward;
    forward only;
    forwarders { 154.72.118.51; };
};
```

```
zone "118.72.154.in-addr.arpa" {
    type master;
    file "/etc/bind/118.72.154";
    notify yes;
    also-notify { 154.72.118.51; };
    allow-transfer { 154.72.118.51; };
};
```

```
zone "3.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/3.168.192";
    notify yes;
    also-notify { 154.72.118.51; };
    allow-transfer { 154.72.118.51; };
};
```

```
/etc/bind/film.skm.tv:
film.skm.tv. IN SOA ns.film.skm.tv. hostmaster.film.skm.tv. (
    3 ;Serial
    86400 ;Refresh
    7200 ;Retry
    3600000 ;Expire
    172800 ) ; Negative Cache TTL
```

```
film.skm.tv. IN NS ns.film.skm.tv.
film.skm.tv. IN MX 100 mail.film.skm.tv.
```

```
ns.film.skm.tv. IN A 154.72.118.50
alfa.film.skm.tv. IN A 154.72.118.52
beta.film.skm.tv. IN A 154.72.118.54
www.film.skm.tv. IN CNAME beta
mail.film.skm.tv. IN A 154.72.118.53
dbsrv.film.skm.tv. IN A 192.168.3.2
ldapsrv.film.skm.tv. IN A 192.168.3.3
```

```
jigsaw.film.skm.tv. IN NS ns.jigsaw.film.skm.tv.
ns IN A 154.72.118.51;
```

```
/etc/bind/118.72.154:
118.72.154.in-addr.arpa. IN SOA ns.film.skm.tv. hostmaster.film.skm.tv. (
    2 ;Serial
    86400 ;Refresh
```


Łukasz Pokorzyński, nr 300251

```
7200 ;Retry
3600000 ;Expire
172800 ) ; Negative Cache TTL
```

```
118.72.154.in-addr.arpa. IN NS ns.film.skm.tv.
```

```
50.118.72.154.in-addr.arpa. IN PTR ns.film.skm.tv.
51.118.72.154.in-addr.arpa. IN PTR ns.jigsaw.film.skm.tv.
52.118.72.154.in-addr.arpa. IN PTR alfa.film.skm.tv.
54.118.72.154.in-addr.arpa. IN PTR beta.film.skm.tv.
53.118.72.154.in-addr.arpa. IN PTR mail.film.skm.tv.
```

```
/etc/bind/3.168.192:
```

```
3.168.192.in-addr.arpa. IN SOA ns.film.skm.tv. Hostmaster.film.skm.tv. (
    1 ;Serial
    86400 ;Refresh
    7200 ;Retry
    3600000 ;Expire
    172800 ) ; Negative Cache TTL
```

```
3.168.192.in-addr.arpa. IN NS ns.film.skm.tv.
```

```
2.3.168.192.in-addr.arpa. IN PTR dbsrv.film.skm.tv.
3.3.168.192.in-addr.arpa. IN PTR ldapsrv.film.skm.tv.
```

10) Pliki konfiguracyjne i administracyjne dla ns.jigsaw.film.skm.tv

```
zone "film.skm.tv" {
    type slave;
    masters { 154.72.118.50; };
};
```

```
zone "jigsaw.film.skm.tv" {
    type master;
    file "/etc/bind/jigsaw.film.skm.tv";
};
```

```
zone "118.72.154.in-addr.arpa" {
    type slave;
    masters { 154.72.118.50; };
};
```

```
zone "3.168.192.in-addr.arpa" {
    type slave;
    masters { 154.72.118.50; };
};
```

```
/etc/bind/jigsaw.film.skm.tv:
```

```
jigsaw.film.skm.tv. IN SOA ns.jigsaw.film.skm.tv. hostaster.film.skm.tv. (
    2 ;Serial
    86400 ;Refresh
    7200 ;Retry
    3600000 ;Expire
    172800 ) ;Negative Cache TTL
```

```
jigsaw.film.skm.tv. IN NS ns.jigsaw.film.skm.tv.
ns.jigsaw.film.skm.tv. IN A 154.72.118.51
www IN CNAME beta.film.skm.tv.
```

Serwer ns.jigsaw.film.tv pobiera rekordy z danych stref od serwera ns.film.skm.tv, stąd wystarczy jeden plik konfiguracyjny /etc/bind/jigsaw.film.skm.tv.