Fakulta elektrotechniky a informatiky
Vysoká škola báňská - Technická univerzita Ostrava

Semestrální projekt – 2. část

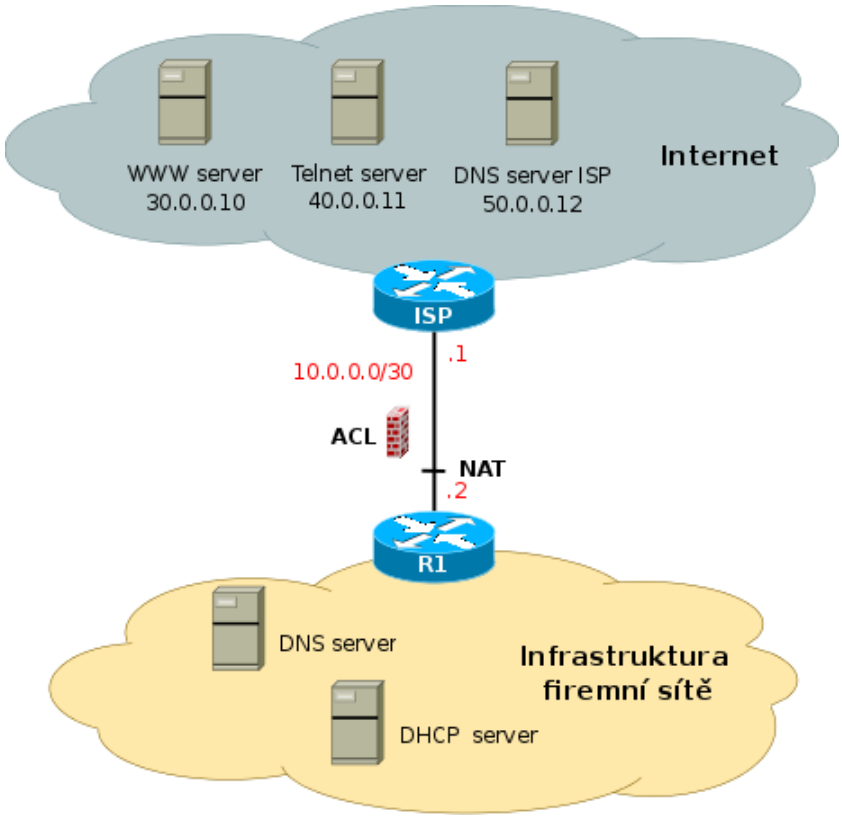
Počítačové sítě

Pavel Příkaský (PRI205)
Roman Zajíc (ZAJ134)
Martin Dočkal (DOC068)
Tomáš Jeřábek (JER042)

2008

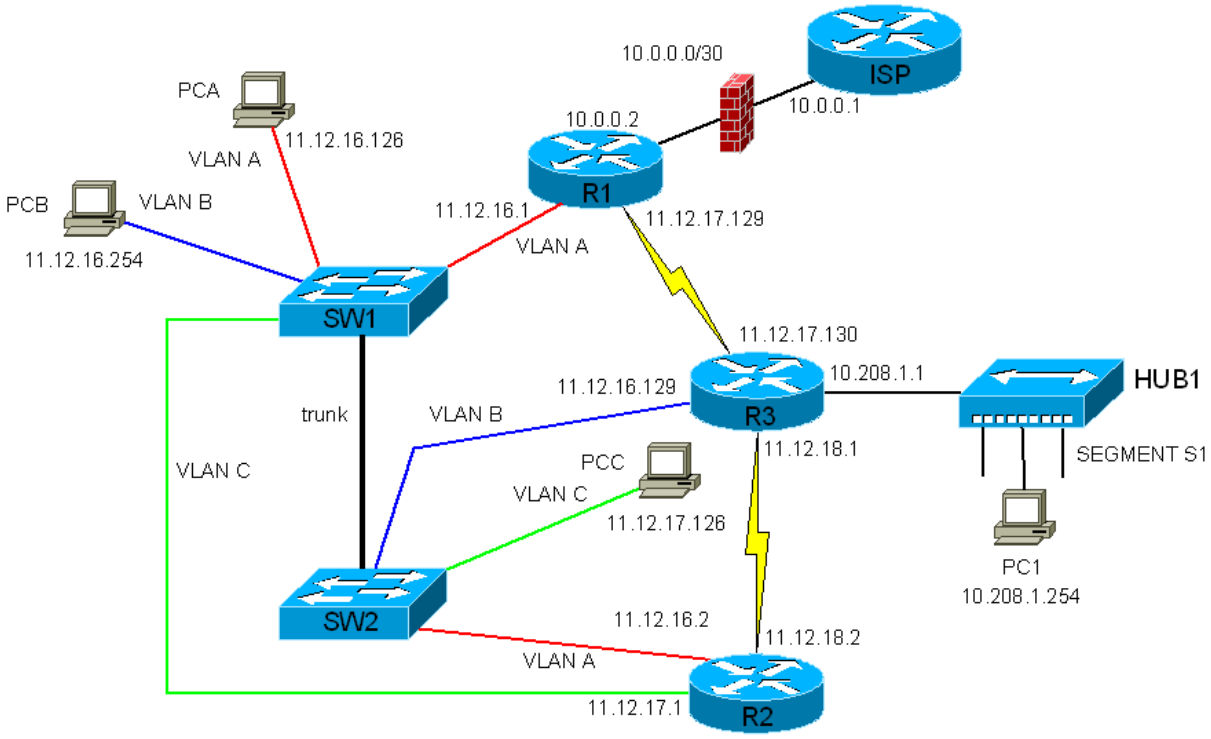
Zadání

Firma	**Apple**
Topologie	1
Počty stanic na podsítích	VLAN A - 63 VLAN B - 32 VLAN C - 16 S1 - 32
IP veřejné	11.12.16.0/22
IP privátní	10.208.1.0/24
Segment s NAT	S1
Velikost NAT poolu	32
Čísla VLAN	VLAN A - 101 VLAN B - 102 VLAN C - 103
Segment s DNS serverem	VLAN A
Segment s DHCP	VLAN A
Směrovací protokol	OSPF
ACL	T – VLAN B N – S1
Záznamy pro reverzní překlad v DNS poskytovatele (místo X.X.X.X patří IP adresa vašeho DNS serveru – uveďte v dokumentaci)	16.12.11.in-addr.arpa. NS X.X.X.X 17.12.11.in-addr.arpa. NS X.X.X.X 18.12.11.in-addr.arpa. NS X.X.X.X 19.12.11.in-addr.arpa. NS X.X.X.X



Adresní plán

Topologie

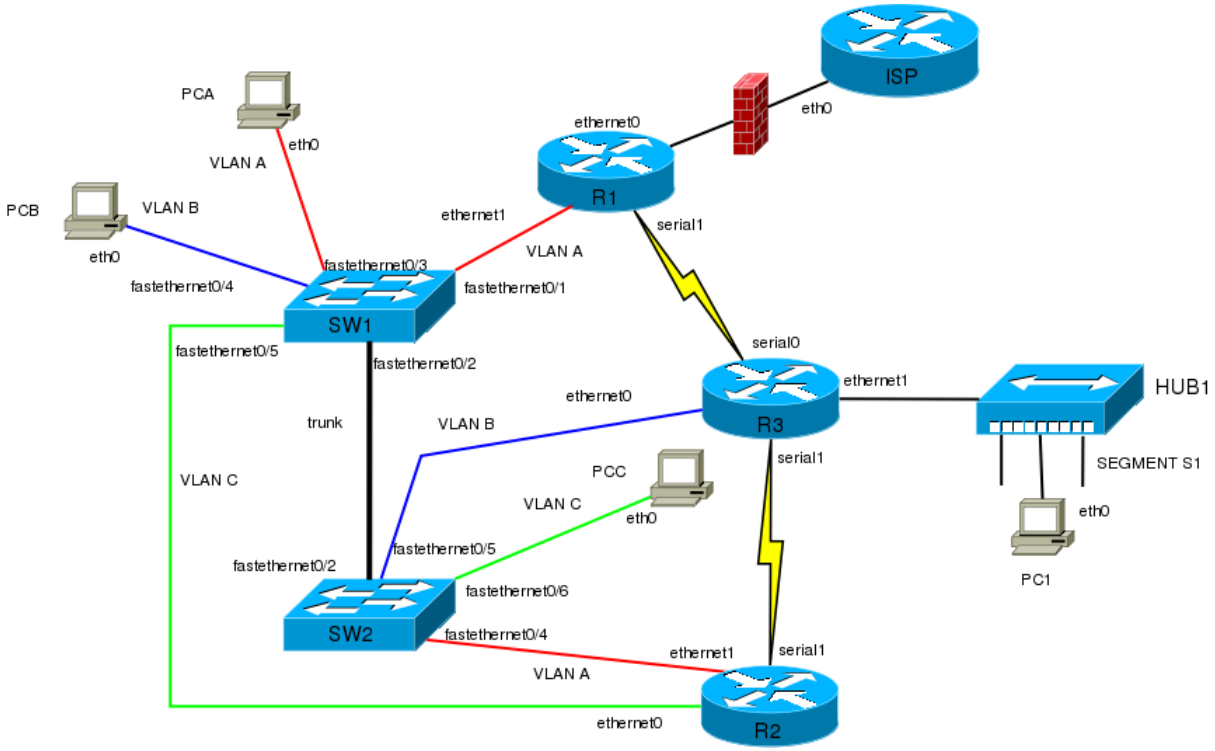


Netmask: 255.255.255.128 = 25, 255.255.255.0 = 24

Označení	Adresa/maska podsítě	Adresa výchozí brány (alternativní)	Rozsah použitelných IP adres stanic	Broadcast adresa
A	11.12.16.0/25	11.12.16.1 (11.12.16.2)	11.12.16.3 - 11.12.16.126	11.12.16.127
B	11.12.16.128/25	11.12.16.129	11.12.16.130 - 11.12.16.254	11.12.16.255
C	11.12.17.0/25	11.12.17.1	11.12.17.2 - 1.12.17.126	11.12.17.127
D	11.12.17.128/25	11.12.17.129 11.12.17.130	11.12.17.131 - 11.12.17.254	11.12.17.255
E	11.12.18.0/25	11.12.18.1 11.12.18.2	11.12.18.3 - 11.12.18.126	11.12.18.127
F (NAT)	11.12.18.128/25		11.12.18.129 - 11.12.18.254	11.12.18.255
G	10.208.1.0/24	10.208.1.1	10.208.1.2 - 10.208.1.254	10.208.1.255

Adresa DNS serveru: 11.12.16.3

Popis namapování síťových prvků



Propojení zařízení:

device:interface

ISP:eth0 -- ISP-R1 -- R1:ethernet0
PCC:eth0 -- SW2-PCC -- SW2:fastethernet0/6
PCB:eth0 -- SW1-PCB -- SW1:fastethernet0/4
PCA:eth0 -- SW1-PCA -- SW1:fastethernet0/3
PC1:eth0 -- R3-PC1 -- R3:ethernet1
R3:serial0 -- R1-R3 -- R1:serial1
R3:serial1 -- R2-R3 -- R2:serial1
R3:ethernet0 -- SW2-R3 -- SW2:fastethernet0/5
R2:ethernet0 -- SW1-R2 -- SW1:fastethernet0/5
R2:ethernet1 -- SW2-R2 -- SW2:fastethernet0/4
R1:ethernet1 -- R1-SW1 -- SW1:fastethernet0/1
SW2:fastethernet0/2 -- SW1-SW2 -- SW1:fastethernet0/2

Zabezpečení sítě – ACL

Tabulky pravidel

Ze sítě

Pořadí	Povolení/zákaz	L3/L4 protokol	Zdrojová adresa/maska	Zdrojový port	Cílová adresa/maska	Cílový port	Omezení
1	povolit	TCP	11.12.16.128/25	*	40.0.0.11/32	23	
2	zakázat	TCP	11.12.18.128/25	*	30.0.0.10/32	80	
3	zakázat	TCP	11.12.18.128/25	*	30.0.0.10/32	443	
4	povolit	TCP	*	*	*	80	
5	povolit	TCP	*	*	*	443	
6	povolit	UDP	11.12.16.3/32	53	*	*	
7	povolit	TCP	11.12.16.3/32	53	*	*	
8	povolit	UDP	*	*	*	53	
9	povolit	TCP	*	*	*	53	
10	povolit	ICMP	*		*		echo
11	povolit	ICMP	11.12.16.3/32		*		echo-reply
12	zakázat	IP	11.12.16.0/22		*		
13	zakázat	IP	10.208.1.0/24		*		
14	zakázat	IP	*		*		

Do sítě

Pořadí	Povolení/zákaz	L3/L4 protokol	Zdrojová adresa/maska	Zdrojový port	Cílová adresa/maska	Cílový port	Omezení
1	povolit	TCP	40.0.0.11/32	23	11.12.16.128/25	*	established
2	zakázat	TCP	30.0.0.10/32	80	11.12.18.128/25	*	
3	zakázat	TCP	30.0.0.10/32	443	11.12.18.128/25	*	
4	povolit	TCP	*	80	*	*	established
5	povolit	TCP	*	443	*	*	established
6	povolit	UDP	*	*	11.12.16.3/32	53	
7	povolit	TCP	*	*	11.12.16.3/32	53	
8	povolit	UDP	*	53	*	*	
9	povolit	TCP	*	53	*	*	established
10	povolit	ICMP	*		*		echo-reply
11	povolit	ICMP	*		11.12.16.3/32		echo
12	zakázat	IP	11.12.16.0/22		*		
13	zakázat	IP	10.208.1.0/24		*		
14	zakázat	IP	*		*		

Konfigurace

Vytvoření ACL pro odchozí směr

```
R1>enable
R1#configure terminal
R1(config)#access-list 101 permit tcp 11.12.16.128 0.0.0.127 host 40.0.0.11 eq 23
R1(config)#access-list 101 deny tcp 11.12.18.128 0.0.0.127 host 30.0.0.10 eq 80
R1(config)#access-list 101 deny tcp 11.12.18.128 0.0.0.127 host 30.0.0.10 eq 433
R1(config)#access-list 101 permit tcp any any eq 80
R1(config)#access-list 101 permit tcp any any eq 433
R1(config)#access-list 101 permit udp host 11.12.16.3 eq 53 any
R1(config)#access-list 101 permit tcp host 11.12.16.3 eq 53 any
R1(config)#access-list 101 permit udp any any eq 53
R1(config)#access-list 101 permit tcp any any eq 53
R1(config)#access-list 101 permit icmp any any echo
R1(config)#access-list 101 permit icmp host 11.12.16.3 any echo-reply
R1(config)#access-list 101 deny ip 11.12.16.0 0.0.3.255 any
R1(config)#access-list 101 deny ip 10.208.1.0 0.0.0.255 any
```

Vytvoření ACL pro příchozí směr

```
R1(config)#access-list 102 permit tcp host 40.0.0.11 eq 23 11.12.16.128 0.0.0.127 established
R1(config)#access-list 102 deny tcp host 30.0.0.10 eq 80 11.12.18.128 0.0.0.127
R1(config)#access-list 102 deny tcp host 30.0.0.10 eq 443 11.12.18.128 0.0.0.127
R1(config)#access-list 102 permit tcp any eq 80 any established
R1(config)#access-list 102 permit tcp any eq 443 any established
R1(config)#access-list 102 permit udp any host 11.12.16.3 eq 53
R1(config)#access-list 102 permit tcp any host 11.12.16.3 eq 53
R1(config)#access-list 102 permit udp any eq 53 any
R1(config)#access-list 102 permit tcp any eq 53 any established
R1(config)#access-list 102 permit icmp any any echo-reply
R1(config)#access-list 102 permit icmp any host 11.12.16.3 echo
R1(config)#access-list 102 deny ip 11.12.16.0 0.0.3.255 any
R1(config)#access-list 102 deny ip 10.208.1.0 0.0.0.255 any
```

Přiřazení ACL na rozhraní a určení směrů filtrace

```
R1(config)#interface ethernet 0
R1(config-if)#ip access-group 101 out
R1(config-if)#ip access-group 102 in
```

DNS server

Konfigurace (adresa DNS serveru: 11.12.16.3)

Soubor named.conf

```
zone "apple.isp.cz" {
      type master;
      file "apple.isp.cz.db";
};

zone "16.12.11.in-addr.arpa." IN {
      type master;
      file "16.12.11.in-addr.arpa.db";
};

zone "17.12.11.in-addr.arpa." IN {
      type master;
      file "17.12.11.in-addr.arpa.db";
};

zone "18.12.11.in-addr.arpa." IN {
      type master;
      file "18.12.11.in-addr.arpa.db";
};
```

Soubor apple.isp.cz.db

```
TTL 10800
$ORIGIN isp.cz.
apple       IN SOA      ( ns.apple office.apple.cz.
                    1
                    10800
                    3600
                    777600
                    3600);
$ORIGIN apple.isp.cz.
                        IN                NS          ns
ns                      IN                A           11.12.16.3
ethernet0-r2                        A           11.12.17.1
ethernet0-r3                        A           11.12.16.129
ethernet1-r1                        A           11.12.16.1
ethernet1-r2                        A           11.12.16.2
serial0-r3                          A           11.12.17.130
serial1-r1                          A           11.12.17.129
serial1-r2                          A           11.12.18.2
serial1-r3                          A           11.12.18.1
```

Soubor 16.12.11.in-addr.arpa.db

```
$TTL 10800
@           IN SOA      ( ns.apple.isp.cz office.apple.cz.
            1
            10800
            3600
            777600
            3600);
            IN              NS          ns
ns          IN              A           11.12.16.3
1           PTR         ethernet1-r1.apple.isp.cz.
2           PTR         ethernet1-r2.apple.isp.cz.
129         PTR         ethernet0-r3.apple.isp.cz.
```

Soubor 17.12.11.in-addr.arpa.db

```
$TTL 10800
@           IN SOA      ( ns.apple.isp.cz office.apple.cz.
                    1
                    10800
                    3600
                    777600
                    3600);
                        IN              NS          ns
ns                      IN              A           11.12.16.3
1           PTR         ethernet0-r2.apple.isp.cz.
130         PTR         serial0-r3.apple.isp.cz.
129         PTR         serial1-r1.apple.isp.cz.
```

Soubor 18.12.11.in-addr.arpa.db

```
$TTL 10800
@           IN SOA      ( ns.apple.isp.cz office.apple.cz.
                    1
                    10800
                    3600
                    777600
                    3600);
                        IN              NS          ns
ns                      IN              A           11.12.16.3
1           PTR         serial1-r3.apple.isp.cz.
2           PTR         serial1-r2.apple.isp.cz.
```

Spuštění:

```
named -g -c /etc/bind/named.conf

nslookup
server localhost
set type=A
apple.isp.cz.db
```

Prohlašuji že jsem se podílel na návrhu této části projektu a souhlasím s odevzdáním takto vypracované práce.

.....	.....
Pavel Příkaský	Roman Zajíc
.....	.....
Martin Dočkal	Tomáš Jeřábek