# PV177 – Cvičení z L2/L3 služeb sítí

Petr Holub, David Rohleder

jaro 2013

**Abstrakt**

Cílem předmětu je získat praktické zkušenosti se přepínacími a směrovacími protokoly, o nichž jste se teoreticky učili v rámci bakalářských a prvních magisterských sítí. Vyzkoušíte si práci s VLAN, různé varianty spanning-tree, agregace portů (LACP), návrh vhodných IP adresovacích schémat, směrování uvnitř autonomních systémů (OSPF, RIPv2) i mezi nimi (BGP), základy směrování multicastového provozu, vytváření tunelů mezi sítěmi (PPPoE, L2TP) a další. Vyzkoušíte si také základy filtrování provozu a pokud bude čas, podíváme se alespoň okrajově na naprosté základy MPLS.

## Obsah

## Vybavení laboratoře

- Zařízení Mikrotik
  - 6× Mikrotik RB433AH
  - 7× Mikrotik RB800
  - 1× Mikrotik RB1100AH
- Zařízení Cisco
  - 1× Cisco MDS 9216i
- Zařízení HP
  - 1× HP ProCurve 6108

# 1 L1 infrastruktura

## 1.1 Cíle cvičení

- Seznámit se se základy metalické kabeláže, krimpování konektorů, testování kabelů (test propojení, frekvenční testování).
- Osvojit si základy práce s CLI na vybavení dostupném v rámci laboratoře.
- Osvojit si základy práce s nástroji pro generování, monitorování a analýzu provozu (Wireshark, tcpdump, scapy, tcpreplay, iperf/netperf/nuttcp).
- Pochopit základy tvorby protokolů.

## 1.2 Zadání

1. Každý (!) nakrimpujte alespoň dva kabely, otestujte je a vypracujte protokol. Každý kabel bude obsahovat: krytky konektoru (pokud není součástí konektoru), jednoznačný identifikátor kabelu, označení délky.

2. Vytvořte z dostupných switchů dvě L2 podsítě propojené jednou linkou, kde každá z podsítí má fyzickou topologii hvězdy.

3. V síti bude připojen generátor rámců. Odchytněte náhodných 10 rámců a proveďte jejich analýzu.
   - Při odchytávání provozu dbejte na to, aby vaše počítače neposílaly do sítě zbytečné rámce.
   - Vyzkoušejte si zachycení provozu na počítači bez GUI a následnou analýzu na jiném počítači.

4. V síti přiřaďte L3 adresy (pro jednoduchost IPv4 a není třeba žádných sofistikovaných dělení) a pomocí některého z měřících programů proměřte propustnost sítě přes alespoň jednu z linek. O měřeních vypracujte protokol.

5. Opakujte zátěžový test sítě jako v předchozím bodě a při něm zachytávejte pakety. Zjistěte závislost výkonu zachytávání na velikosti zachytávaných částí rámců.

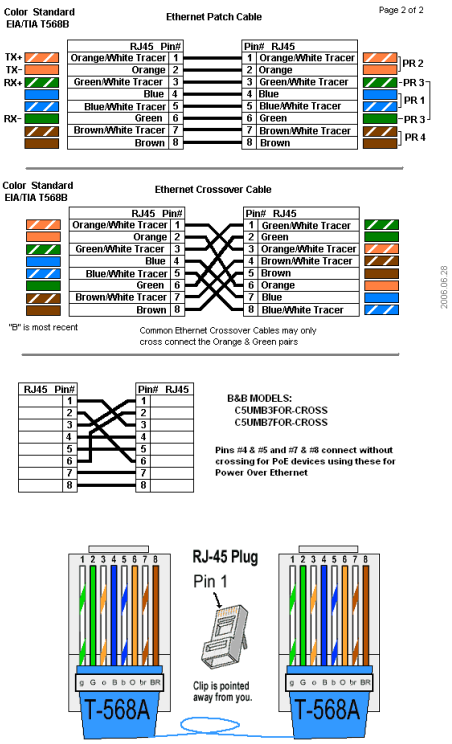
## 1.3 Protokol

Každý samostatně zpracuje a odevzdá protokol. Protokol musí obsahovat minimálně následující části:
- měření nakrimpovaných kabelů, specifikaci, které normě daný kabel vyhovuje
- analýzu obsahu zachycených paketů, součástí protokolu bude soubor obsahující analyzované pakety ve formátu PCAP,
- měření výkonnosti sítě,
- analýzu závislosti výkonu zachytávání na velikosti zachytávaných částí rámců.

Nezapomeňte, že každý protokol musí obsahovat informace o podmínkách, za nichž byly výsledky dosaženy!

## 1.4 Doplňující materiály

**Zapojení kabelů** Zapojení RJ45 kabelů pro Ethernet je uvedeno na obrázku 1. *Kabel nerozplétejte více, než je nezbytně nutné!*




Obrázek 1: Zapojení Ethernetových RJ45 konektorů. Převzato z: `http://www.bb-europe.com/images/EthernetRJ45B.gif` a `http://www.joncamfield.com/oss/schooltools/Reference/EthernetCabling_files/ethcable568a.gif`.

**Popisy CLI**

- Mikrotik:
  - http://wiki.mikrotik.com/wiki/Manual:Console
  - http://wiki.mikrotik.com/wiki/API_command_notes
- Cisco:
  - http://www.cisco.com/warp/cpropub/45/tutorial.htm
  -
- HP ProCurve:
  - ftp://ftp.hp.com/pub/networking/software/6200-5400-3500-CLI-k1201-Feb2007.pdf

**Příklady nástrojů pro konfiguraci a monitoring sítě**

- Základní konfigurace sítě

```
ifconfig eth0 inet 10.1.1.2 netmask 255.255.255.0 up
netstat -rn
```

- Konfigurace sítě na Windows pomocí příkazové řádky

```
ipconfig /all
netsh interface ip show config
netsh interface ip set address name="Local Area Connection"
        static 192.168.1.2 255.255.255.0 192.168.1.1 1
netsh interface ip set dns "Local Area Connection" static 192.168.1.1

netsh interface ip set address "Local Area Connection" dhcp
netsh interface ip set dns "Local Area Connection" dhcp
```

- Konfigurace bezdrátových sítí na Windows pomocí příkazové řádky http://technet.microsoft.com/cs-cz/library/cc755301%28v=ws.10%29.aspx

```
netsh wlan show all
netsh wlan show profiles
netsh wlan show interfaces
connect ssid="MojeWlan" name=Profil2 interface="Wireless Network Connection"

netsh wlan set hostednetwork mode=allow ssid=MojeSit key=MojeHeslo
netsh wlan start hostednetwork
netsh wlan stop hostednetwork
netsh wlan show hostednetwork
netsh wlan refresh hostednetwork MojeNoveHeslo
```

- Informace o Ethernetových rozhraních:

```
# ethtool eth2
Settings for eth2:
        Supported ports: [ FIBRE ]
        Supported link modes:   Not reported
        Supported pause frame use: No
        Supports auto-negotiation: No
        Advertised link modes:  Not reported
        Advertised pause frame use: No
        Advertised auto-negotiation: No
        Speed: 10000Mb/s
        Duplex: Full
```

```
        Port: FIBRE
        PHYAD: 0
        Transceiver: external
        Auto-negotiation: off
        Current message level: 0x00000004 (4)
                               link
        Link detected: yes
```

```
# ethtool -S eth2
NIC statistics:
     rx_packets: 16380239
     tx_packets: 23223570
     rx_bytes: 114521535441
     tx_bytes: 177575497708
     rx_errors: 0
     tx_errors: 0
     rx_dropped: 0
     tx_dropped: 0
     multicast: 0
     collisions: 0
     rx_length_errors: 0
     rx_over_errors: 0
     rx_crc_errors: 0
     rx_frame_errors: 0
     rx_fifo_errors: 0
     rx_missed_errors: 0
     tx_aborted_errors: 0
     tx_carrier_errors: 0
     tx_fifo_errors: 0
     tx_heartbeat_errors: 0
     tx_window_errors: 0
     tx_boundary: 4096
     WC: 1
     irq: 59
     MSI: 1
     MSIX: 0
     read_dma_bw_MBs: 1757
     write_dma_bw_MBs: 1736
     read_write_dma_bw_MBs: 3434
     serial_number: 366847
     watchdog_resets: 0
     dca_capable_firmware: 1
     dca_device_present: 0
     link_changes: 6
     link_up: 1
     dropped_link_overflow: 0
     dropped_link_error_or_filtered: 215425
     dropped_pause: 0
     dropped_bad_phy: 0
     dropped_bad_crc32: 0
     dropped_unicast_filtered: 215425
     dropped_multicast_filtered: 431472
     dropped_runt: 0
     dropped_overrun: 0
     dropped_no_small_buffer: 0
     dropped_no_big_buffer: 0
     ----------- slice ---------: 0
     tx_pkt_start: 23223570
     tx_pkt_done: 23223570
     tx_req: 61272593
     tx_done: 61272593
```

```
     rx_small_cnt: 3685681
     rx_big_cnt: 38056376
     wake_queue: 0
     stop_queue: 0
     tx_linearized: 0
     LRO aggregated: 0
     LRO flushed: 0
     LRO avg aggr: 0
     LRO no_desc: 0
```

- Statistiky o síťovém stacku

```
# netstat -s
Ip:
    13619568 total packets received
    149 with invalid addresses
    0 forwarded
    0 incoming packets discarded
    13617452 incoming packets delivered
    48708530 requests sent out
    6 reassemblies required
    1 packets reassembled ok
    503 fragments received ok
    3018 fragments created
Icmp:
    2464 ICMP messages received
    31 input ICMP message failed.
    ICMP input histogram:
        destination unreachable: 2132
        echo requests: 327
        timestamp request: 1
        address mask request: 3
    2034 ICMP messages sent
    0 ICMP messages failed
    ICMP output histogram:
        destination unreachable: 1706
        echo replies: 327
        timestamp replies: 1
IcmpMsg:
        InType3: 2132
        InType8: 327
        InType13: 1
        InType17: 3
        InType37: 1
        OutType0: 327
        OutType3: 1706
        OutType14: 1
Tcp:
    5 active connections openings
    79 passive connection openings
    2 failed connection attempts
    43 connection resets received
    2 connections established
    47721 segments received
    70260 segments send out
    29 segments retransmited
    3 bad segments received.
    4923 resets sent
Udp:
    12663934 packets received
    273654 packets to unknown port received.
```

```
    559246 packet receive errors
    48637539 packets sent
UdpLite:
TcpExt:
    2 resets received for embryonic SYN_RECV sockets
    8 ICMP packets dropped because they were out-of-window
    28 TCP sockets finished time wait in fast timer
    238 delayed acks sent
    2 delayed acks further delayed because of locked socket
    Quick ack mode was activated 8 times
    115 packets directly queued to recvmsg prequeue.
    4 bytes directly received in process context from prequeue
    3091 packet headers predicted
    1 packets header predicted and directly queued to user
    3830 acknowledgments not containing data payload received
    34802 predicted acknowledgments
    1 congestion windows recovered without slow start by DSACK
    4 congestion windows recovered without slow start after partial ack
    19 other TCP timeouts
    9 DSACKs sent for old packets
    5 DSACKs received
    1 connections reset due to early user close
    1 connections aborted due to timeout
    TCPDSACKIgnoredNoUndo: 1
    TCPSackShiftFallback: 3
    IPReversePathFilter: 1
    TCPRcvCoalesce: 187
    TCPChallengeACK: 2
IpExt:
    InMcastPkts: 1575
    InBcastPkts: 68792
    InOctets: -725770314
    OutOctets: -644689296
    InMcastOctets: 50400
    InBcastOctets: 12628875
```

- Nastavení MTU:
  `ifconfig eth0 mtu 9000`
- Kontrola síťových bufferů `sysctl`:

```
net.core.wmem_max
net.core.wmem_default
net.core.rmem_max
net.core.rmem_default
```

- Test průchodu paketů bez fragmentace:

```
ping -M do -s 8500 -c 5 1.2.3.4
From 1.2.3.4 icmp_seq=1 Frag needed and DF set (mtu = 1500)
```

- tcpdump

```
tcpdump -i eth0 -c 1000 -s 100 -w /tmp/file icmp
```

**Použití měřících nástrojů**

- Patch do `iperfu` pro vyšší rychlosti: `https://lkml.org/lkml/2007/9/26/215`
- iperf UDP

```
iperf -s -u -i 1 -l 8500
iperf -u -c hostname -i 1 -l 8500 -b 10M
```

- iperf TCP

```
iperf -s -i 1 -w 8M
iperf -c hostname -i 1 -w 8M
```

- netperf UDP

```
netserver -n 4
netperf -H 10.0.10.1 -n 4 -t UDP_STREAM -- -s 8M -S 8M -m nnnn -M nnnn
```

- netperf TCP

```
netserver -n 4
netperf -H 10.0.10.1 -n 4 -t TCP_STREAM -- -s 8M -S 8M -m nnnn -M nnnn
```

- nuttcp – trocha zábavy:

```
for h in 1.2.3.4 2.3.4.5; do for j in r t;
        do echo "";
        if [ "$j" = "r" ]; then echo "From $h to server";
        else echo "From server to $h"; fi;
                (for i in 200 400 600 800;
                        do ./nuttcp -i5 -T10 -u -R${i}M -v -v \
                                -${j} ${h};
                done ) | fgrep loss ;
        done;
done
```

# 2 Spojování sítí na L2: spanning-tree protokoly, LACP

## 2.1 Cíle cvičení

- Naučit se analyzovat provoz na síti na úrovni L2, prakticky si vyzkoušet fungování backward-learning protokolu.
- Vyzkoušet si a srovnat spanning-tree protokoly (STP 802.1D, RSTP 802.1w, v rámci jedné VLAN), pochopit a prakticky si vyzkoušet filtrování BPDU.
- Vyzkoušet agregaci linek pomocí protokolu LACP.

## 2.2 Zadání

1. Nakonfigurujte si přepínače pro základní přístup přes SSH.

   Cisco:

```
interface Vlan1
 ip address x.x.x.x y.y.y.y
 no shut
crypto key generate rsa general-keys modulus 1024

line vty 0 15
 transport input ssh
```

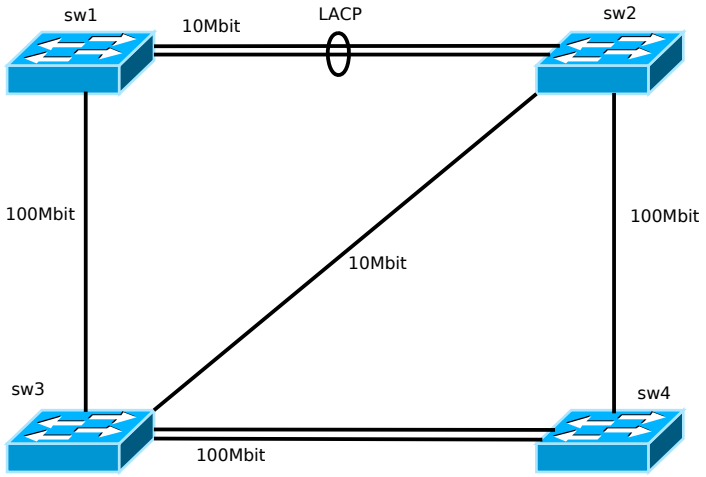
   Mikrotik:

```
ip address print
ip address add address=x.x.x.x netmask=y.y.y.y interface=ether1
ip service enable ssh
ip service disable telnet
export
```

   HP:

```
erase startup-config
show running-config
conf
hostname "mujswitch"
time timezone 60
time daylight-time-rule Middle-Europe-and-Portugal
console inactivity-timer 60
no telnet-server
no web-management
password manager
password operator
snmp-server community "PV177Community"
crypto key generate ssh
ip ssh
exit
show interfaces
show interfaces A1 hc
wr mem
```

2. Vytvořte síť se 4 přepínači zapojenými podle obrázku a na přepínačích nakonfigurujte protokoly STP a případně RSTP (pokud jej daná zařízení podporují). K dvěma přepínačům přípojte po jednom koncovém uzlu (např. notebook či Mikrotik nakonfigurovaný bez podpory switchování). Ověřte chování při zapojení sítě bez STP a se STP.




Cisco:

```
```

Mikrotik:

```
/interface bridge
add admin-mac=00:00:00:00:00:00 ageing-time=5m arp=enabled auto-mac=yes \
    disabled=no forward-delay=15s l2mtu=1600 max-message-age=20s mtu=1500 \
    name=bridge1 priority=0x8000 protocol-mode=none transmit-hold-count=6
/interface bridge port
add bridge=bridge1 disabled=no edge=auto external-fdb=auto horizon=none \
    interface=wlan2 path-cost=10 point-to-point=auto priority=0x80
add bridge=bridge1 disabled=no edge=auto external-fdb=auto horizon=none \
    interface=wlan1 path-cost=10 point-to-point=auto priority=0x80
add bridge=bridge1 disabled=no edge=auto external-fdb=auto horizon=none \
    interface=ether1 path-cost=10 point-to-point=auto priority=0x80
add bridge=bridge1 disabled=no edge=auto external-fdb=auto horizon=none \
    interface=ether2 path-cost=10 point-to-point=auto priority=0x80
add bridge=bridge1 disabled=no edge=auto external-fdb=auto horizon=none \
    interface=ether3 path-cost=10 point-to-point=auto priority=0x80
add bridge=bridge1 disabled=no edge=auto external-fdb=auto horizon=none \
    interface=wds1 path-cost=10 point-to-point=auto priority=0x80
/interface bridge settings
set use-ip-firewall=no use-ip-firewall-for-pppoe=no use-ip-firewall-for-vlan=\
    no
```

```
interface bridge set protocol-mode=[none|stp|rstp]
interface bridge port set bridge=bridge1 interface=ether2 \
        edge=[auto|no|no-discover|yes|yes-discover] \
        point-to-point=[auto|yes|no]
```

http://wiki.mikrotik.com/wiki/Manual:Interface/Bridge

HP:

```
conf
spanning-tree
spanning-tree force-version [stp-compatible|rstp-operation]
spanning-tree ethernet A1 point-to-point-mac [true|false|auto]
show spanning-tree
```

3. Zjistěte, kde leží root bridge.
4. Zjistěte, které porty jsou ve spanning-tree blokované.

   Cisco:

```
sw1# show spanning-tree blockedports
```

5. Připojte počítače k ke dvěma různým switchům. Zjistěte čas konvergence při výpadku některé z linek (linka mezi sw1 a sw3, linka mezi sw3 a sw4 a jedna z linek mezi sw1 a sw2). Liší se nějak?
6. Změňte root bridge na nejlepší variantu. Zdůvodněte, proč je to nejlepší varianta.
7. Odposlechněte pakety odpovídající spanning-tree protokolu (BPDU) a interpretujte je.
8. Na portech určených jako access porty zapněte BPDU guard, tj. pokud na daný port přijdou BPDU pakety, bude shozen. Ověřte fungování.

   Cisco:

```
interface FastEthernet0/1
 spanning-tree bpduguard enable
```

   Mikrotik: –

   HP:

```
spanning-tree ethernet A1 bpdu-protection
```

9. Nastavte filtrování BPDU na portech (tj. pouze likvidace příchozích/odchozích BPDU na daném portu). Navrhněte experiment, kterým ověříte jeho fungování.

   Cisco:

```
interface FastEthernet 0/1
 spanning-tree bpdufilter enable
```

   Mikrotik:

```
/interface bridge
filter add in-inteface=ether1 stp-*=*
```

http://wiki.mikrotik.com/wiki/Manual:Interface/Bridge#Bridge_Firewall

HP:

```
spanning-tree ethernet A1 bpdu-filter
```

10. Vytvořte síť ze svou přepínačů spojených agregovanými linky (alespoň dvěma). Ke každému z přepínačů připojte alespoň dva počítače. Zkonfigurujte protokol LACP a zjistěte, podle kterých parametrů je možné data mezi linky dělit.

11. Navrhněte a realizujte experiment, který ověří chování LACP protokolu, tj. že jeden datový tok jde vždy po jedné lince.

    Cisco:

```
interface Port-channel 1

interface FastEthernet 0/1
 channel-group 1 mode active
interface FastEthernet 0/2
 channel-group 1 mode active
```

    Mikrotik:

```
/interface bonding
        add slaves=ether2,ether3 mode=802.3ad lacp-rate=30secs \
        link-monitoring=mii-type1 \
        transmit-hash-policy=[layer-2|layer-2-and-3|layer-3-and-4]
```

    http://wiki.mikrotik.com/wiki/Manual:Interface/Bonding

    HP:

```
conf
interface A1 lacp active
exit
show lacp
show lacp distributed
show logging lacp
```

## 2.3 Zdroje

- Popis různých typu STP protokolů (Cisco) http://www.cisco.com/en/US/tech/tk389/tk621/tsd_technology_support_protocol_home.html

## 2.4 Protokol

Každý samostatně zpracuje a odevzdá protokol. Protokol musí obsahovat minimálně následující části:

- Popis konfigurace sítě se STP, na obrázku označte RP, DP, blokované porty, metriky na portech (zadání 2).
- výpis ze switche, kde leží STP root (zadání 3),
- výpisy ze všech switchů jejich blokovaných portů (zadání 4),
- tabulku časů konvergence pro jednotlivé linky. Vysvětlení, pokud se časy liší (zadání 5),

- vysvětlení vaší volby STP root bridge (zadání 6),
- Výsledky analýzy BPDU paketů (zadání 7).
- Popis konfigurací sítě a výsledky ověření fungování BPDUGuard a BPDU filtrování (zadání 8 a 9).
- Výsledky experimentálního ověření fungování LACP protokolu (popis experimentu, výsledky, diskuse; zadání 11).

# 3 Segmentace sítě pomocí VLAN, návrh adresovacích schémat IPv4/IPv6

## 3.1 Cíle cvičení

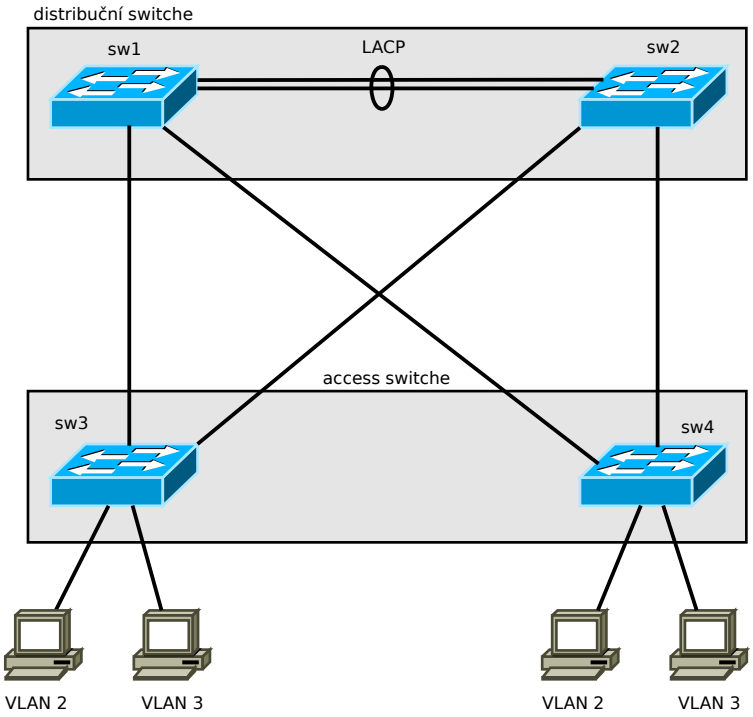
- Naučit se, kdy je třeba využívat segmentaci sítě do VLAN.
- Vyzkoušet si práci s per-VLAN spanning tree protokoly (PVST/PVST+,MSTP).
- Vyzkoušet si základy práce se směrovacími tabulkami.
- Vyzkoušet si návrh adresovacích schémat a rozmyslet jejich dopad na směrovací tabulky formou manuální údržby směrovacích tabulek.

## 3.2 Obvyklá topologie serverových sítí

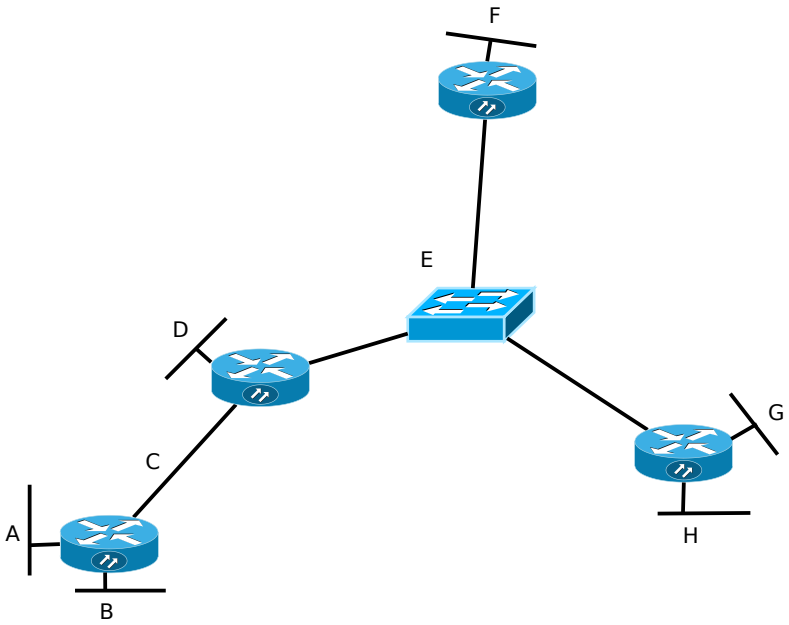
Více STP stromů je možné uplatnit např. u switchovaných sítí serverů. Následující obrázek představuje zjednodušenou topologii switchovaných sítí pro servery. Switche tady dělíme na access (přistupové) switche, do kterých jsou připojeny koncové servery a distribuční switche, které zajišťující připojení přístupových switchů. Rozdílné STP stromy umožňují rozdělit zátěž u různých VLAN na různé distribuční switche. Obdobnou topologii je možné uplatnit např. i u uživatelských stanic. MU používá tuto topologii např. v bohunickém kampusu. Více na toto téma můžete nalézt na `http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/campover.html`.

## 3.3 Zadání

- V obrázku 3 je znázorněna síť, pro kterou máte vytvořit adresní schema. Každá síť má různý počet počítačů, jak je uvedeno níže. Vaším úkolem je rozdělit přidělený adresový prostor tak, abyste co nejefektivněji přidělený prostor využili. Sítě B a H jsou pro tiskárny a podobná zařízení a nemusejí být přístupné z jiných lokalit. Počty potřebných IP adres pro sítě C a E odvoďte z diagramu.
  - Člověk 1 – NET: 13.12.1.0/23, A=12, B=17, D=37, F=87, G=15, H=4
  - Člověk 2 – NET: 201.6.8.0/24, A=60, B=7, D=51, F=5, G=6, H=3
  - Člověk 3 – NET: 4.3.2.0/22, A=271, B=154, D=162, F=20, G=21, H=6
  - Člověk 4 – NET: 87.3.11.128/25, A=12, B=2, D=37, F=7, G=15, H=5
  - Člověk 5 – NET: 144.67.3.192/26, A=12, B=17, D=5, F=8, G=12, H=3
  - Člověk 6 – NET: 121.7.34.128/25, A=12, B=5, D=3, F=54, G=12, H=3
  - Člověk 7 – NET: 45.250.0.0/23, A=62, B=4, D=133, F=60, G=12, H=4
  - Člověk 8 – NET: 78.1.1.128/25, A=18, B=14, D=30, F=13, G=5, H=7
  - Člověk 9 – NET: 131.10.0.0/23, A=32, B=4, D=128, F=48, G=10, H=4
  - Člověk 10 – NET: 24.36.10.10/25, A=4, B=10, D=62, F=3, G=26, H=24
  - Člověk 11 – NET: 13.12.1.0/23, A=31, B=12, D=37, F=87, G=15, H=4 ««««< zadani.tex
  - Tým 2 – NET: 201.6.8.0/24, A=60, B=7, C=2, D=51, E=3, F=5, G=6, H=3
  - Tým 3 – NET: 4.3.2.0/22, A=271, B=154, C=2, D=162, E=3, F=20, G=21, H=6
  - Tým 4 – NET: 87.3.11.128/25, A=12, B=2, C=2, D=37, E=3, F=7, G=15, H=5
  - Tým 5 – NET: 144.67.3.192/26, A=12, B=17, C=2, D=5, E=3, F=8, G=12, H=3
  - Tým 6 – NET: 121.7.34.128/25, A=12, B=5, C=2, D=3, E=3, F=54, G=12, H=3




Obrázek 2: Konfigurace sítě pro per-VLAN spanning tree.




Obrázek 3: Konfigurace sítě pro přidělování IP adres.

- Tým 7 – NET: 45.250.0.0/23, A=62, B=4, C=2, D=133, E=3, F=60, G=12, H=4
- Tým 8 – NET: 78.1.1.128/25, A=18, B=14, C=2, D=30, E=3, F=13, G=5, H=7
  =======
- Člověk 12 – NET: 201.6.8.0/24, A=60, B=72, D=1, F=5, G=6, H=3 »»»> 1.32

- Nakonfigurujte síť z obrázku 2 a pro různé VLANy zvolte různé kořeny STP stromu. Zdůvodněte vaši volbu.

  Jako přepínače použijte Cisco 2950, jako koncové prvky použijte Mikrotik s vypnutou funkcí bridge.

## 3.4 Protokol

- Popište konfigurace jednotlivých přepínačů v síti.
- Zanalyzujte, jak vypadají spanning tree pro jednotlivé VLANy.
- Popište, jak a proč jste navrhli adresní schémata.
- Popište, jaké IPv4 adresní rozsahy můžete používat v privátních sítích a jaké rozsahy nemůžete pro unicastové adresování používat vůbec?

# 4 Směrování uvnitř autonomních systémů

## 4.1 Cíle cvičení

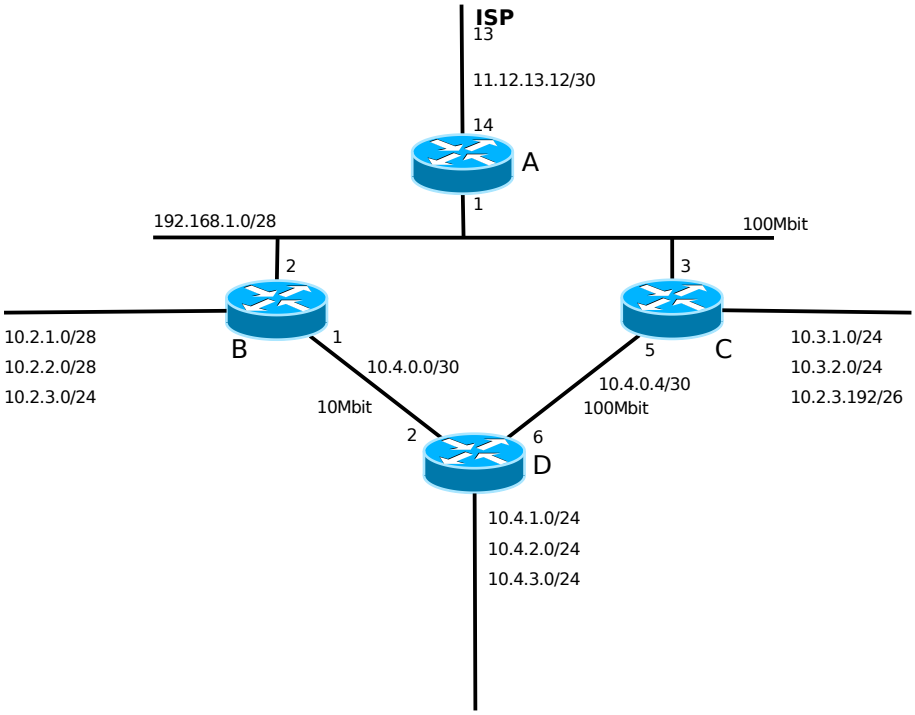
- Osvojit si konfiguraci běžných protokolů pro směrování v rámci autonomních systémů: OSPF
- Získat základní zkušenosti s laděním problémů směrování v rámci autonomních systémů.

## 4.2 Zadání

Jako směrovací protokol pro IPv4 vašeho vlastního AS jste si vybrali OSPFv2. Vaším cílem bude vyzkoušet několik scénářů tak, aby se OSPFv2 chovalo podle vašich představ.

## 4.3 Základní nastavení

Na následujícím obrázku máte váš AS. Nastavte všechny směrovače tak, aby byly všechny počítače v koncových sítích vzájemně dosažitelné. Do protokolu uveďte, kolik rout vidí směrovače A a D pomocí OSPF.




Příklady konfigurace OSPF na Mikrotiku:

```
/ip address add address=10.1.1.1/30 interface=ether1
/routing ospf instance
    add name=moje
```

Více na
http://wiki.mikrotik.com/wiki/Manual:OSPF-examples
http://wiki.mikrotik.com/wiki/Manual:Routing/OSPF

## 4.4 Rychlost konvergence

Na lince mezi směrovači C a D došlo k výpadku.

Zjistěte jak rychle síť zkonverguje. (tj. jak rychle mezi sebou dokáží počítače ze sítí NET-D1 a NET-C1 komunikovat).

1. v případě, kdy je směrovač schopen rozpoznat pád linky (třeba vytažením kabelu)
2. v případě, kdy není směrovač schopen rozpoznat pád linky

Úkol:

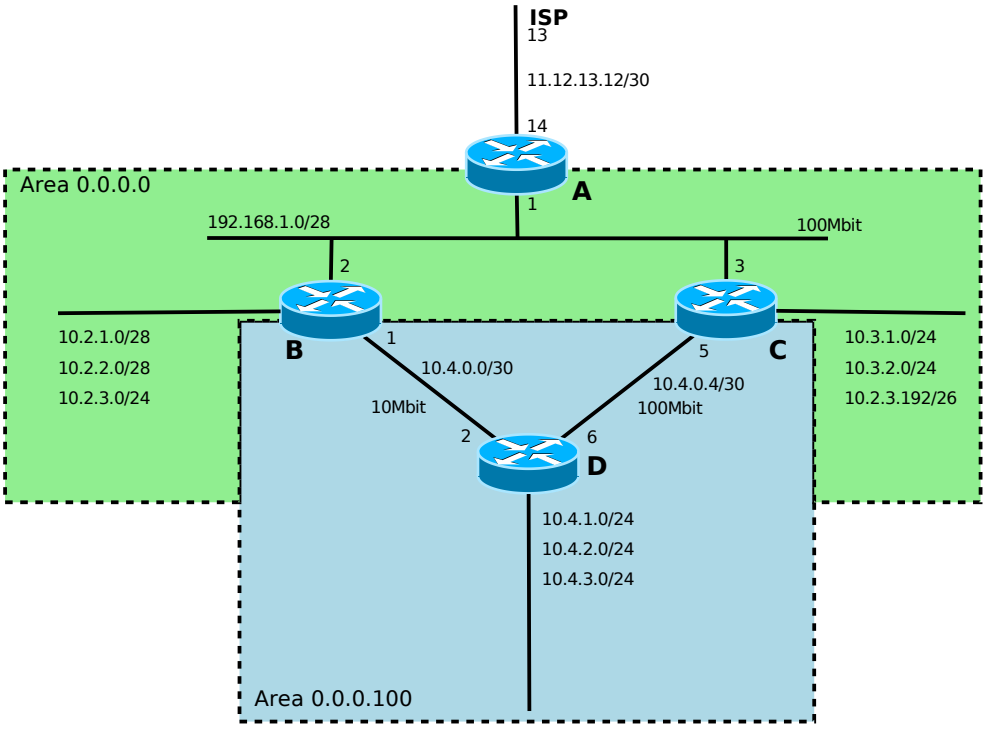
Minimalizujte dobu konvergence. Do protokolu uveďte, jaká je konvergence v případech 1 a 2. Uveďte na jakou nejnižší dobu konvergence jste se byli schopni dostat (a s jakým nastavením).

## 4.5 Rozdělení na oblasti

Do této chvíle jste měli všechny směrovače v jedné páteřní oblasti (backbone area 0.0.0.0). Protože se vám zdá, že síť je nestabilní a probíhá v ní příliš mnoho změn, pokusíte se rozdělit síť podle následujícího obrázku.

Vaše adresní schema jste si předem rozmysleli tak, že v lokalitě D budete přidělovat adresy ze sítí 10.D.Z.0/16 (Z=0. . . management síťových prvků, Z=1. . . klientské počítače, Z=2. . . tiskárny, atd.)

Nastavte směrovače B a C jako ABR a směrovač D jako vnitřní směrovač oblasti 0.0.0.100. Směrem do páteře šiřte pouze agregovanou síť 10.D.0.0/16.

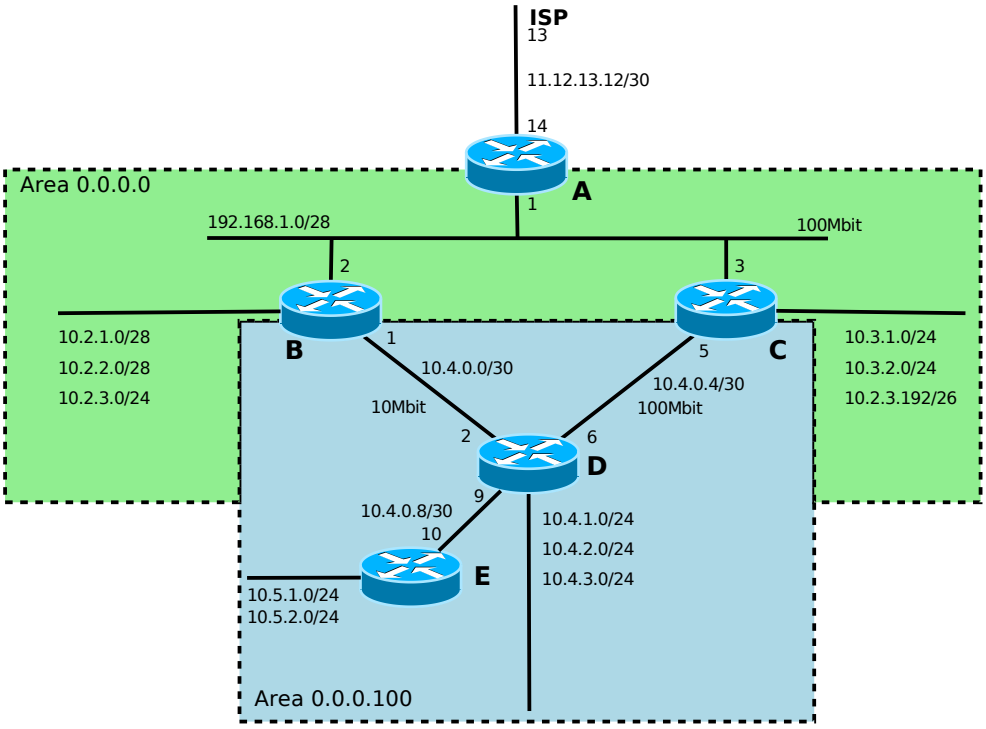



## 4.6 Stub area

Směrovač D je sice hardwarově poměrně silný stroj, ale má omezené kapacity pro počítání OSPF. Nezatěžujte jej tedy tím, že dostává všechny směrovací informace o ostatních sítích. Směrovače B a C budou směrovači D předávat pouze default routu. V protokolu uveďte kolik rout vidí směrovače A a D přes OSPF.

## 4.7 Redistribuce

Ke směrovači D byl připojen směrovač E, který neumí směrovací protokol OSPFv2. Nastavení směrování je tedy nutné udělat staticky. Nastavte statickou routu na síť 10.5.0.0/16. Zajistěte šíření této cesty do zbytku sítě. Zjistěte, jak je vidět tato cesta na směrovačích A a C (jakou má metriku).


ISP
13
11.12.13.12/30
14
A
1
Area 0.0.0.0
192.168.1.0/28
100Mbit
2
3
B
C
1
5
10.2.1.0/28
10.2.2.0/28
10.2.3.0/24
10.4.0.0/30
10Mbit
10.4.0.4/30
100Mbit
10.3.1.0/24
10.3.2.0/24
10.2.3.192/26
2
6
D
9
10.4.0.8/30
10
10.4.1.0/24
10.4.2.0/24
10.4.3.0/24
E
10.5.1.0/24
10.5.2.0/24
Area 0.0.0.100

## 4.8 Protokol

- 

# 5 Směrování mezi autonomními systémy

## 5.1 Cíle cvičení

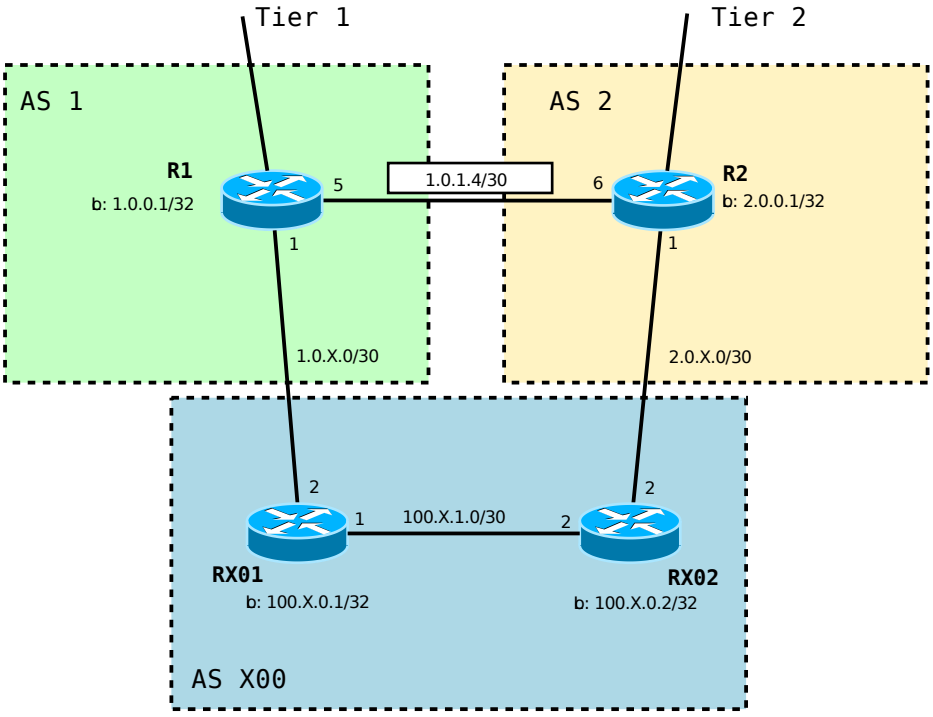
- Osvojit si konfiguraci směrovacího protokolu pro směrování mezi autonomními systémy: BGP.
- Získat základní zkušenosti s laděním problémů směrování mezi autonomními systémy.

## 5.2 Zadání

Každé skupině bude přiřazeno vlastní číslo X.

Nacházíte se v autonomním systému X00. Vaším úkolem je zprovoznění BGP směrování mezi vaším AS a AS vašich ISP (AS 1 a AS 2).

### Topologie a adresní schema




### Přidělené PI IP rozsahy

| | |
|---|---|
| **AS** | přidělený IP rozsah |
| **AS 1** | 1.0.0.0/16 |
| **AS 2** | 2.0.0.0/16 |
| **AS X00** | 100.X.0.0/20 |

**Adresy loopbacků**

| směrovač | IP |
|---|---|
| **RX01** | 100.X.0.1/32 |
| **RX02** | 100.X.0.2/32 |

**Adresy spojovacích sítí**

**R1 - RX01**
NET: 1.0.X.0/30
IP R1: 1.0.X.1
IP RX01: 1.0.X.2
**R2 - RX02**
NET: 2.0.X.0/30
IP R2: 2.0.X.1
IP RX02: 2.0.X.2
**RX01 - RX02**
NET: 100.X.1.0/30
IP RX01: 100.X.1.1
IP RX02: 100.X.1.2

**Vztahy pro navazování BGP relací**

- relace mezi AS jsou navazovány na adresy příslušných spojovacích sítí(v protokolu vysvětlete proč je to takto vhodné)
- relace v rámci AS jsou navazovány na adresy loopbackových rozhraní (v protokolu vysvětlete, proč je to takto vhodné - odhlédněte příliš jednoduché topologie příkladu)

## 5.3 Cvičení 1

AS X00 je multihome zákazník s PI IP adresami. AS X00 komunikuje přes AS 1, pouze v případě výpadku spojení s AS 1 dojde k přesměrování přes AS 2. Směrem k oběma poskytovatelům se bude šířit pouze jedna cesta s PI IP adresami přidělenými AS X00. AS X00 není tranzitní AS.

## 5.4 Cvičení 2

AS X00 je multihome zákazník s PI IP adresami. Zákazník by rád komunikoval s AS 2 a jinými zákazníky přímo připojenými k AS 2 přes AS 2. Zbytek provozu prochází přes AS 1. AS X00 není tranzitní AS.

## 5.5 Cvičení 3

Rozdělte PI IP adresy AS X00 na sítě /24. Liché sítě budou preferovat cestu přes AS 1, sudé sítě přes AS 2. AS X00 není tranzitní AS.

## 5.6 Cvičení 4

AS X00 poskytuje záložní konektivitu AS 2 pro případ výpadku jiných jeho linek. Zajistěte, aby AS 2 byl dosažitelný v případě tohoto výpadku. V případě, kdy je k dispozici jiná konektivita AS 2, nemělo by se komunikovat přes AS X00, ale přes linku některého jiného AS.

## 5.7 Protokol

- popište konfiguraci jednotlivých prvků v síti pro každé cvičení

# 6 Multicast

## 6.1 Cíle cvičení

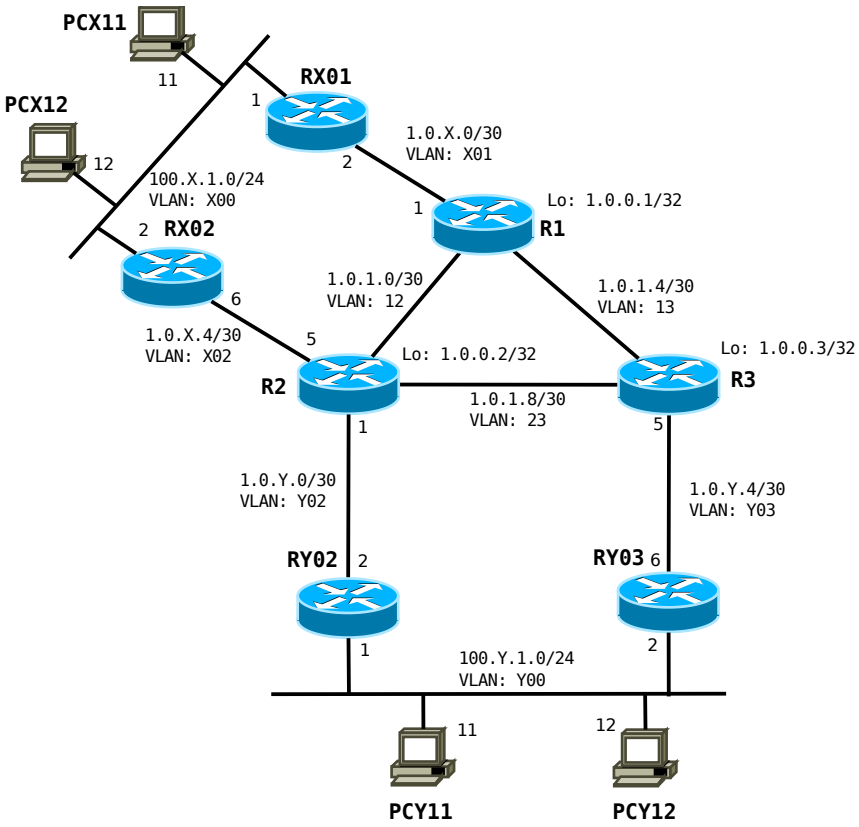
- Získat základní zkušenosti se směrováním multicastového provozu (PIM-SM).
- Naučit se základy analýzy multicastového provozu a detekování problémů.

## 6.2 Zadání

Mějme síť s topologií viz obrázek 4. V síti běží směrovací protokol OSPF, který nakonfigurujete na vám přidělených uzlech. Dále nakonfigurujete na vám přidělených uzlech PIM-SM s volbou RP pomocí BSR.

V topologii sítě jsou označeny vysílače, které budou vysílat multicastový provoz a přijímače, které budou multicastový provoz přijímat.

Rozdělte se na skupiny, každé skupině bude přiděleno jedinečné číslo X nebo Y.




Obrázek 4: Topologie multicastové sítě

### 6.2.1 Směrování

Mezi všemi směrovači běží směrovací protokol OSPFv2. Všechny směrovače jsou v backbone area. Nedochází k žádné redistribuci statických ani přímo připojených sítí. Metriky a další pa-

rametry OSPF jsou ponechány na defaultních hodnotách.

### 6.2.2 BSR

V síti jsou 2 BSR: R2 a R3.

### 6.2.3 Rendez-vous Pointy

- R1 – vyšší priorita
- R3 – nižší priorita

Adresy RP jsou vždy loopbackové adresy 1.0.0.X/32.

### 6.2.4 Vysílače a přijímače

Stanice **PCX11 a PCY11** jsou vysílače, které vysílají multicastový videostream na následujících multicastových adresách:

- PCX11: 239.0.X.11, port 1234, TTL=12
- PCY11: 239.0.Y.11, port 1234, TTL=32

Stanice **PCX12 a PCY12** přijímají a zobrazují multicastový videostream z obou streamů generovaných stroji PCX11 a PCY11.

### 6.2.5 IGMP

Na směrovačích R[XY]0[123] běží IGMPv2.

### 6.2.6 Vysílání a přijímání multicastového streamu pomocí vlc

```
$ vlc -vvv video.avi --sout
  '#transcode{vcodec=h264,vb=0,scale=0,acodec=mpga,ab=128,channels=2,
   samplerate=44100}:rtp{dst=239.0.X.11,port=1234,mux=ts,ttl=12}'
```

## 6.3 Protokol

- popište konfigurace jednotlivých prvků v síti, které jste nakonfigurovali
- vypište směrovací tabulku vám přidělených směrovačů
- vypište adresy PIM sousedů vám přidělených směrovačů
- vypište multicastové skupiny, které vám přidělené směrovače posílají do koncových sítí
- změřte konvergenci multicastového vysílání, když bude vypnut právě aktivní RP

# 7 Tunelování provozu

## 7.1 Cíle cvičení

- Osvojení si vytváření tunelů pomocí různých technologií: PPPoE, GRE, IPsec.
- Praktické používání aplikace OpenVPN.

## 7.2 Zadání

-

## 7.3 Protokol

-

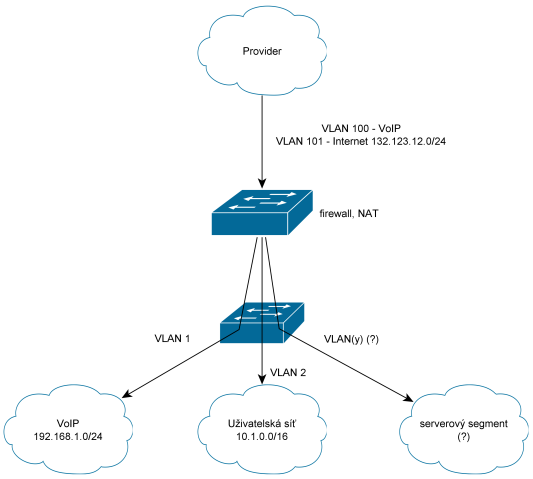
# 8 Filtrování provozu, překlad adres

## 8.1 Cíle cvičení

- Získat zkušenosti s bezstavovým a stavovým filtrováním.
- Návrh filtrovacích pravidel pro běžně se vyskytující praktické scénáře: firemní prostředí vs. akademické prostředí, požadavky nejběžnějších protokolů (DNS, HTTP/HTTPS, SMTP, POP3, IMAPv4, SAMBA, NFS), demilitarizované zóny, nároky multimediálních aplikací, atd.).
- Získat zkušenosti s různými variantami NAT.
- Probrat zajímavosti, které se v praxi vyskytují: uživatelem řízené firewally, port knocking, atd.
- Rozdiskutovat základní otázky: přiměřená ochrana sítě, přiměřená ochrana koncových zařízení, koncepční řešení vs. bastlení.

## 8.2 Zadání

- Máte firemní sít menší až střední firmy, pro jednoduchost připojenou k jednomu providerovi jedním uplinkem.
- Firemní síť se sestává ze tří logických částí, jak je patrné z následujícího schématu:




  - telefonní VoIP síť, obsahující SIP telefony tunelované k providerovi,
  - počítačovou síť uživatelských stanic,
  - serverový segment, který je třeba dále strukturovat, obsahující jak důvěrné služby určené dovnitř interní sítě:
    * databázový SQL server,
    * interní web server,
    * emailový server pro přístup k poště jednotlivými uživateli,

    tak služby, které musí být přístupné z internetu
    * DNS server,
    * emailovou relay,
    * web server,

- router/firewall/NAT.

Pro jednoduchost (a implementovatelnost v rámci cvičení) je rozvedení vnitřní sítě z firewallu realizováno pomocí VLAN, které jsou dále rozvedeny L2 infrastrukturou.

Cílem cvičení je rozmyslet, navrhnout a implementovat:

- adresní schéma pro serverový segment, jeho rozdělení na případné podsítě na L2 i L3 tak, aby bylo možné zajistit bezpečnost a požadovanou funkcionalitu jednotlivých serverů,
- pravidla pro směrování, jsou-li třeba,
- pravidla pro překlad adres s tím, že
  - musí být zajištěna dosažitelnost výše vyjmenovaných serverů z vnějšího internetu,
  - musí být zajištěna funkčnosti FTP klientů v síti uživatelských počítačů, a to i na internetové FTP servery (možných řešení je několik – vyberte si z nich, které považujete za nejlepší a svou volbu zdůvodněte).
- pravidla pro firewall s ohledem na zajištění bezpečnosti VoIP sítě, sítě uživatelských počítačů i serverů,
- pravidla pro síť uživatelských počítačů s tím, uživatelé musí mít přístup k interním serverům i k veřejnému internetu, avšak chcete minimalizovat rizika hrozeb z veřejného internetu.
- Rozmyslete a diskutujte, jak minimalizovat rizika spojená s útoky zevnitř sítě uživatelských počítačů.
- Diskutujte, k čemu a proč byste mohli využít DHCP snooping (bohužel není dostupný na platformě Mikrotik a tudíž nemůže být součástí cvičení).

Řešení můžete implementovat pomocí Mikrotiku, Linuxového PC s firewallem netfilter/iptables, nebo FreeBSD s firewallem PF.

## 8.3 Protokol

Bude obsahovat:

- Stručný popis zvolené platformy.
- Diskuse bezpečnostních rizik pro jednotlivé části sítě.
- Dokončené schéma sítě s doplněním chybějících informací.
- Adresní schéma serverového segmentu.
- Pravidla routeru, firewallu a NATu a jejich diskusi.
- Diskusi/zdůvodnění rozhodnutí, která jste v době návrhu museli provést.
- Diskusi zabezpečení vůči útokům zevnitř sítě a k využití DHCP snoopingu.
- Diskuse omezení funkcionality počítačové sítě, která je důsledkem implementace výše provedených a popsaných kroků.

# 9 Základy MPLS

## 9.1 Cíle cvičení

- Osvojení si teoretických základů MPLS (není pokryto přednáškami).
- Vyzkoušení si základní konfigurace sítě s CE/PE/P prvky.

## 9.2 Zadání

-

## 9.3 Protokol

-