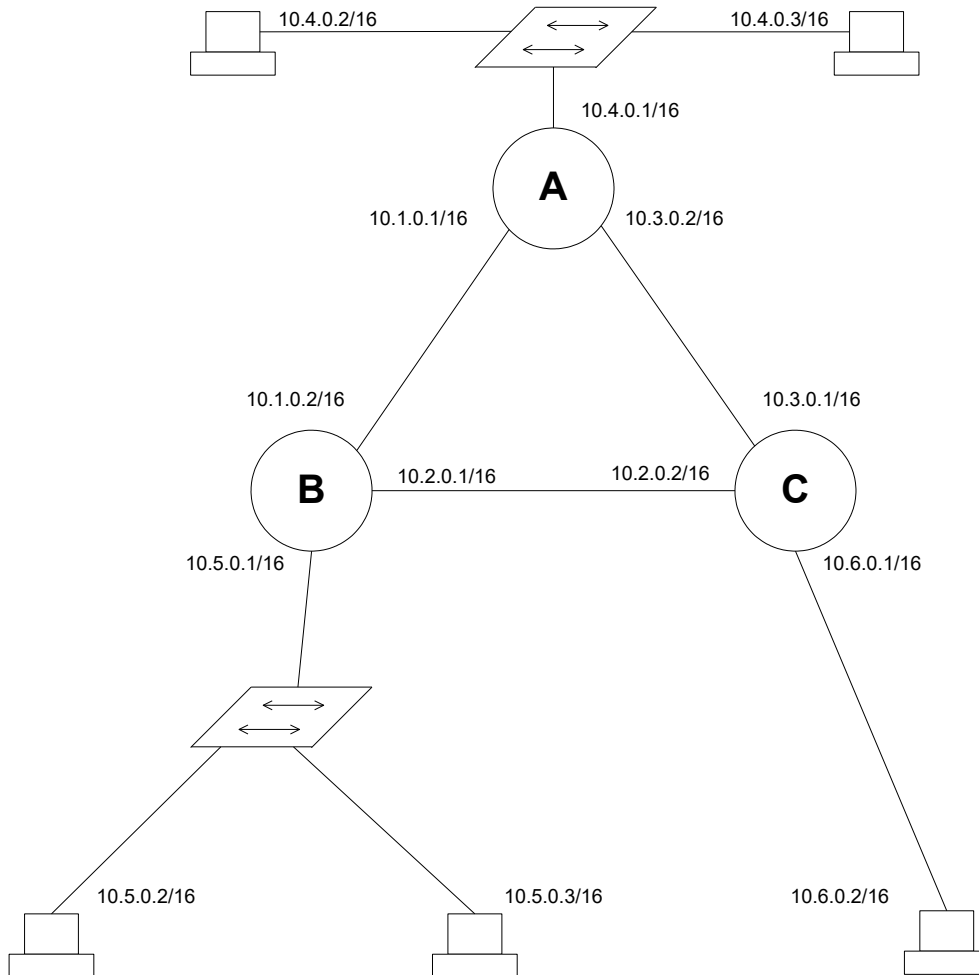


# OSPF

Nakonfigurujte směrovače dle schéma zapojení. Jako směrovací protokol použijte OSPF. Pomocí programu Ethereal odchyťávejte HELLO pakety, nejdříve s vypnutým šifrováním a poté se zapnutým šifrováním. Poukažte na možnosti odhalení hesla pomocí výše zmíněného programu.



Obr. 0 Schéma zapojení směrovačů

# 1 Konfigurace směrovače

Nastavení zabezpečení komunikace mezi směrovači a pomocí hesla *cisco* jsem provedl pomocí příkazů:

```
C(config-if)#ip ospf authentication-key cisco
```

```
C(config)#router ospf 1
```

```
C(config-router)#area 0 authentication
```

Příkazem `C# show running-config` jsem zjistil konfiguraci směšovače:

```
Building configuration...
Current configuration : 741 bytes
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
hostname C
logging queue-limit 100
ip subnet-zero
call rsvp-sync
```

## **interface Ethernet0/0**

```
ip address 10.6.0.1 255.255.0.0
half-duplex
```

## **interface Serial0/0**

```
ip address 10.3.0.1 255.255.0.0
ip ospf authentication-key cisco
clockrate 56000
```

## **interface Serial0/1**

```
ip address 10.2.0.2 255.255.0.0
ip ospf authentication-key cisco
router ospf 1
log-adjacency-changes
area 0 authentication
network 10.2.0.0 0.0.0.255 area 0
network 10.3.0.0 0.0.0.255 area 0
network 10.6.0.0 0.0.0.255 area 0
```

```
ip classless
no ip http server
dial-peer cor custom
line con 0
line aux 0
line vty 0 4
end
```

Při této konfiguraci byly odchyťvány pakety programem Ethereal. Výsledek je na obrázku Obr.2. Jak je vidět (červený text v obrázku), odchycený HELLO paket nese přímo heslo bez jakéhokoliv zabezpečení.

No. -	Time	Source	Destination	Protocol	Info
1	0.000000	Cisco_28:b4:e0	Cisco_28:b4:e0	LOOP	Loopback
2	0.356676	10.6.0.1	224.0.0.5	OSPF	Hello Packet
3	10.000986	Cisco_28:b4:e0	Cisco_28:b4:e0	LOOP	Loopback
4	10.357512	10.6.0.1	224.0.0.5	OSPF	Hello Packet
5	20.001676	Cisco_28:b4:e0	Cisco_28:b4:e0	LOOP	Loopback
6	20.358374	10.6.0.1	224.0.0.5	OSPF	Hello Packet
7	30.002521	Cisco_28:b4:e0	Cisco_28:b4:e0	LOOP	Loopback

Frame 2 (78 bytes on wire, 78 bytes captured)

- Ethernet II, Src: 00:05:5e:28:b4:e0, Dst: 01:00:5e:00:00:05
- Internet Protocol, Src Addr: 10.6.0.1 (10.6.0.1), Dst Addr: 224.0.0.5 (224.0.0.5)
- Open Shortest Path First
  - OSPF Header
    - OSPF Version: 2
    - Message Type: Hello Packet (1)
    - Packet Length: 44
    - Source OSPF Router: 10.6.0.1 (10.6.0.1)
    - Area ID: 0.0.0.0 (Backbone)
    - Packet Checksum: 0xe790 (correct)
    - Auth Type: Simple password
    - Auth Data: cisco
  - OSPF Hello Packet
    - Network Mask: 255.255.0.0
    - Hello Interval: 10 seconds
    - Options: 0x2 (E)
    - Router Priority: 1
    - Router Dead Interval: 40 seconds
    - Designated Router: 10.6.0.1
    - Backup Designated Router: 0.0.0.0

0000	01 00 5e 00 00 05 00 05 5e 28 b4 e0 08 00 45 c0	..A.... ^C....E.
0010	00 40 47 ff 00 00 01 59 86 9a 0a 06 00 01 e0 00	..@G....Y .....
0020	00 05 02 01 00 2c 0a 06 00 01 00 00 00 00 e7 90	..... .....
0030	00 01 63 69 73 63 6f 00 00 00 ff ff 00 00 00 0a	..cisco. ....
0040	02 01 00 00 00 28 0a 06 00 01 00 00 00 00 00	.....(.. .....

File: (Untitled) 610 bytes 00:00:30 Drops | P: 7 D: 7 M: 0

**Obr. 1 Odchycený HELLO paket bez šifrování**

Abychom předešli takto jednoduchému odhalení hesla, musíme použít nějakou formu šifrování. K tomuto účelu je možné použít například hashování funkci MD5. tuto funkci aktivujeme následujícím příkazem pro každé rozhraní:

```
C(config-if)#ip ospf message-digest-key 2 md5 cisco
```

a dále zadáme příkazy:

```
C(config)#router ospf 1
C(config-router)#area 0 authentication message-digest
```

Opět zjistíme konfiguraci routeru:

```
Building configuration...
Current configuration : 835 bytes
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
hostname C
logging queue-limit 100
ip subnet-zero
call rsvp-sync
```

```

interface Ethernet0/0
ip address 10.6.0.1 255.255.0.0
ip ospf message-digest-key 2 md5 cisco
half-duplex

```

```

interface Serial10/0
ip address 10.3.0.1 255.255.0.0
ip ospf message-digest-key 2 md5 cisco
clockrate 56000

```

```

interface Serial10/1
ip address 10.2.0.2 255.255.0.0
ip ospf message-digest-key 2 md5 cisco
router ospf 1
log-adjacency-changes
area 0 authentication
network 10.2.0.0 0.0.0.255 area 0
network 10.3.0.0 0.0.0.255 area 0
network 10.6.0.0 0.0.0.255 area 0

```

```

ip classless
no ip http server
dial-peer cor custom
line con 0
line aux 0
line vty 0 4
end

```

Opět jsem aktivoval zachytávání paketů v programu Ethereal. Výsledek je vidět na Obr.3  
 Jak je nyní vidět, paket HELLO nese v sobě přímo heslo, nýbrž jeho hash hodnotu.

No. -	Time	Source	Destination	Protocol	Info
1	0.000000	10.6.0.1	10.6.0.1	LOOP	Loopback
2	0.004891	10.6.0.1	224.0.0.5	OSPF	Hello Packet
3	10.000678	10.6.0.1	10.6.0.1	LOOP	Loopback
4	10.006163	10.6.0.1	224.0.0.5	OSPF	Hello Packet
5	20.001508	10.6.0.1	10.6.0.1	LOOP	Loopback
6	20.005765	10.6.0.1	224.0.0.5	OSPF	Hello Packet
7	30.028885	10.6.0.1	10.6.0.1	LOOP	Loopback
8	30.030728	10.6.0.1	224.0.0.5	OSPF	Hello Packet
9	40.027206	10.6.0.1	10.6.0.1	LOOP	Loopback
10	40.031466	10.6.0.1	224.0.0.5	OSPF	Hello Packet
11	41.666531	10.6.0.1	CDP/VTP	CDP	Cisco Discovery Protocol

[Frame 2 (94 bytes on wire, 94 bytes captured)  
 Ethernet II, Src: 00:05:5e:28:b4:e0, Dst: 01:00:5e:00:00:05  
 Internet Protocol, Src Addr: 10.6.0.1 (10.6.0.1), Dst Addr: 224.0.0.5 (224.0.0.5)  
 open Shortest Path First  
   OSPF Header  
     OSPF Version: 2  
     Message Type: Hello Packet (1)  
     Packet Length: 44  
     Source OSPF Router: 10.6.0.1 (10.6.0.1)  
     Area ID: 0.0.0.0 (Backbone)  
     Packet Checksum: 0x0000 (none)  
     Auth Type: cryptographic  
     Auth Key ID: 2  
     Auth Data Length: 16  
     Auth Crypto Sequence Number: 0x2b92951c  
     Auth Data: 4904EB69440553587C77EAD8C1499C6D  
   OSPF Hello Packet

0000	01 00 5e 00 00 05 00 05 5e 28 b4 e0 08 00 45 c0	..A.... A(....E.
0010	00 50 49 92 00 00 01 59 84 f7 0a 06 00 01 e0 00	..PI....Y .....
0020	00 05 02 01 00 2c 0a 06 00 01 00 00 00 00 00	.....+.....
0030	00 02 00 00 02 10 2b 92 95 1c ff ff 00 00 00 0a	.....(.....I.
0040	02 01 00 00 00 28 0a 06 00 01 00 00 00 00 49 04	.....(.....I.
0050	0b 60 41 05 52 58 7c 77 00 d8 c1 49 0c 6d	.....I.....

File: sifra 1274 bytes 00:00:41 | P: 11 D: 11 M: 0

Obr. 3 Odchycený HELLO paket se šifrováním