

Hogyan támadjunk és védjünk hálózati eszközöket?

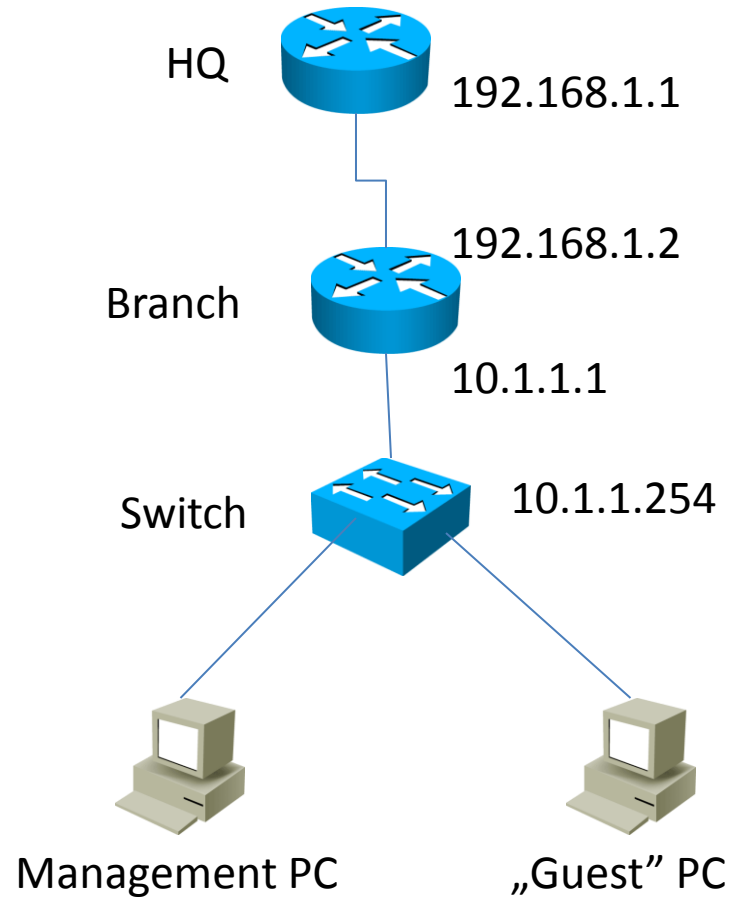
Beleznay Péter

pbeleznay@flane.com

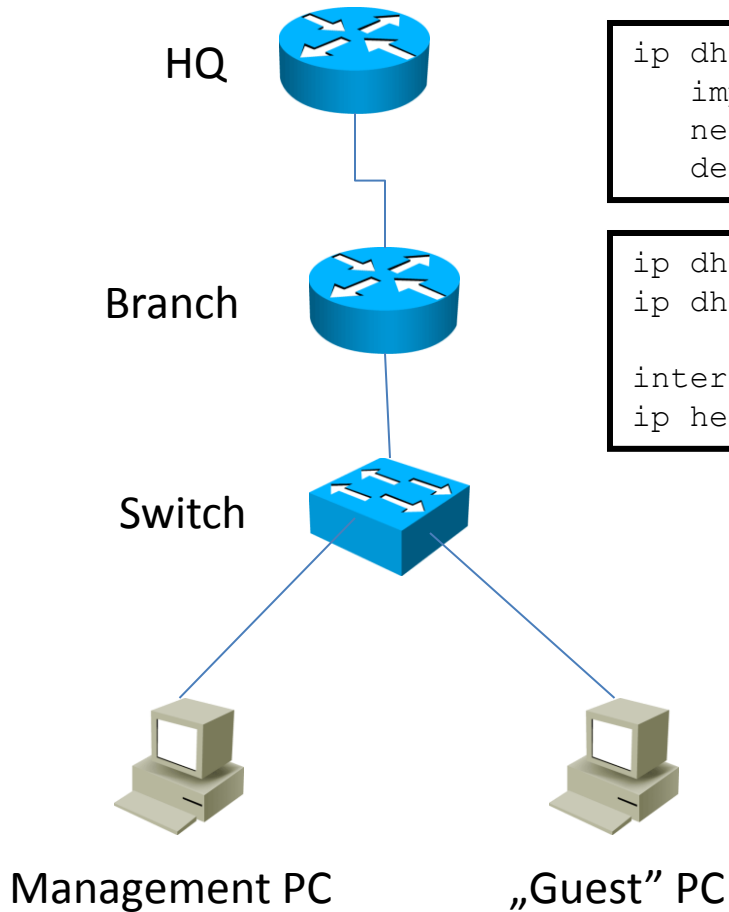
CCIE#10282, CCSI#31966

Fast Lane – Cisco Learning Solution Partner

Teszt labor



DHCP beállítások



```
ip dhcp pool TEST
import all
network 10.1.1.0 255.255.255.0
default-router 10.1.1.1
```

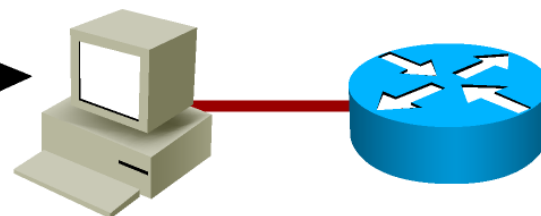
```
ip dhcp relay information option
ip dhcp relay information trust-all

interface Fastethernet 0/0
ip helper-address 192.168.1.1
```

Jelszó beállítások

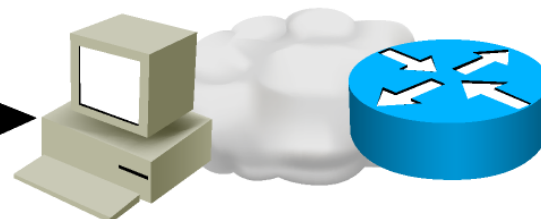
Console Password

```
RouterX(config) #line console 0  
RouterX(config-line) #login  
RouterX(config-line) #password cisco
```



Virtual Terminal Password

```
RouterX(config) #line vty 0 4  
RouterX(config-line) #login  
RouterX(config-line) #password sanjose
```



Enable Password

```
RouterX(config) #enable password cisco
```



Secret Password

```
RouterX(config) #enable secret sanfran
```

Service Password-Encryption Commands

```
RouterX(config) #service password encryption  
RouterX(config) #no service password-encryption
```

Jelszó támadások

Támadó eszközök:

- ❖ Getpass
- ❖ Cain

Védekezés:

- ✓ Minimum 8 karakter hosszú jelszavak használata (legyen benne szám, nagybetű, speciális karakter), de ennél is jobb nem használni olyan jelszót, ami a konfigurációba tárolódik el. Alkalmazzunk „AAA” megoldásokat, és RADIUS/TACACS szerveret!

De hogyan szerezhethetjük meg a konfigurációs beállításokat, vagy a jelszavakat?

Sniffer támadások...

Sniffer programok

❖ Eszköz: Wireshark

The screenshot displays the Wireshark interface with a list of captured packets. The selected packet (No. 507) is an HTTP ACK from 209.132.177.50 to 192.168.12.21. The detailed view shows the following information:

- Frame 507 (74 bytes on wire, 74 bytes captured)
- Ethernet II, Src: Amit_04:ae:54 (00:50:18:04:ae:54), Dst: Intel_e3:01:f5 (00:0c:f1:e3:01:f5)
- Internet Protocol, Src: 209.132.177.50 (209.132.177.50), Dst: 192.168.12.21 (192.168.12.21)
- Transmission Control Protocol, Src Port: http (80), Dst Port: 48890 (48890), Seq: 0, Ack: 1, Len: 0
 - Source port: http (80)
 - Destination port: 48890 (48890)
 - Sequence number: 0 (relative sequence number)
 - Acknowledgement number: 1 (relative ack number)
 - Header length: 40 bytes
 - Flags: 0x12 (SYN, ACK)
 - Window size: 5792
 - Checksum: 0x99db [correct]
 - Options: (20 bytes)
 - [SEQ/ACK analysis]

The packet bytes pane shows the following hex and ASCII data:

```
0000 00 0c f1 e3 01 f5 00 50 18 04 ae 54 08 00 45 00 .....P...T..E.
0010 00 3c 00 00 40 00 35 06 f6 47 d1 84 b1 32 c0 a8 <...@.5. .G...2..
0020 0c 15 00 50 be fa b5 36 ce 18 e0 bb b5 58 a0 12 ...P...6 ....X..
0030 16 a0 99 db 00 00 02 04 05 64 04 02 08 0a 10 1d .....d.....
0040 ee de 5b 81 15 29 01 03 03 02 ..[...]..
```

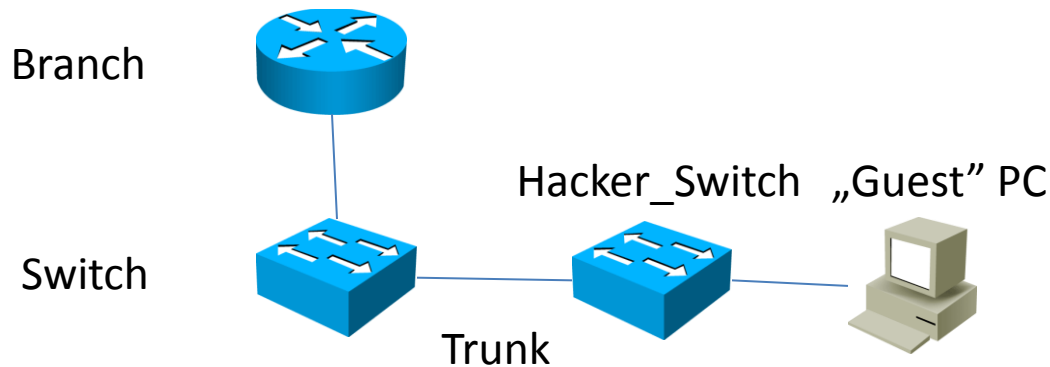
Source Port (tcp.srcport), 2 P: 1096 D: 1096 M: 0 Drops: 0

Egy mindennapos kép...



„Forgalom eltérítés” #1

- VTP és DTP



The screenshot shows a Wireshark capture of network traffic. The main pane displays a list of captured packets with columns for No., Time, Source, Destination, and Protocol. The packets are primarily ARP requests and replies between 192.168.1.101 and 192.168.1.102. The bottom pane shows the hex and ASCII representation of the selected packet.

No.	Time	Source	Destination	Protocol
12	0.04288	192.168.1.101	192.168.1.102	SNMP
13	0.05759	192.168.1.101	192.168.1.102	SNMP
14	0.07409	192.168.1.101	75.126.43.200	TCP
15	0.08760	192.168.1.101	192.168.1.102	SNMP
16	0.10409	192.168.1.101	75.126.43.200	TCP
17	0.11860	192.168.1.101	75.126.43.200	TCP
18	0.13509	192.168.1.101	75.126.43.200	TCP
19	0.15159	192.168.1.101	75.126.43.200	TCP
20	0.16809	192.168.1.101	192.168.1.102	SNMP
21	0.18459	192.168.1.101	192.168.1.102	SNMP
22	0.20109	192.168.1.101	192.168.1.102	SNMP
23	0.21759	192.168.1.101	192.168.1.102	SNMP
24	0.23409	192.168.1.101	192.168.1.102	SNMP

```
vtp mode server
vtp domain DEMO

interface Fastethernet 0/10
(switchport mode dynamic auto)
switchport mode access
switchport nonegotiate

Interface Fastethernet 0/11
```

```
Interface Fastethernet 0/1
Switchport mode trunk
```

„Forgalom eltérítés” #2

- Routing manipulálás

```
router ospf 1
network 10.1.1.0 0.0.0.255 area 0
```

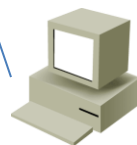
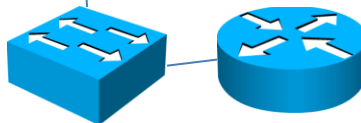
```
router ospf 1
passive-interface fastEthernet 0/0
area 0 authentication message-digest
```

```
router ospf 1
network 10.1.1.0 0.0.0.255 area 0
default-information originate always
```

Branch



Hacker_Router



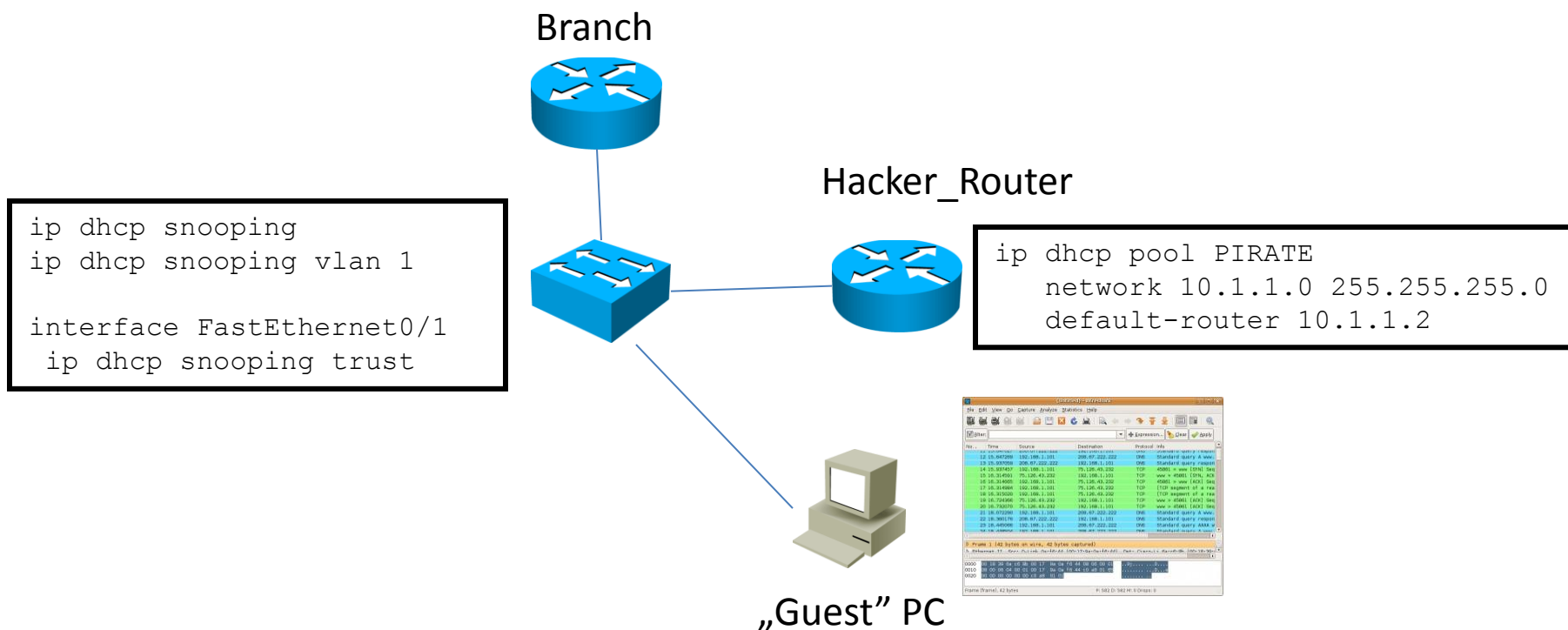
„Guest” PC

A screenshot of the Wireshark network protocol analyzer interface. The main pane shows a list of captured packets with columns for Time, Source, Destination, Protocol, and Info. The packet list includes various protocols such as Ethernet II, Internet Protocol Version 4, and Hypertext Transfer Protocol. The bottom pane shows the details of the selected packet, including the raw bytes and their hexadecimal representation.

No.	Time	Source	Destination	Protocol	Info
12	0.047296	192.168.1.101	192.0.2.222	OSPF	OSPFv2 Hello [R] 192.168.1.101
13	0.047300	192.0.2.222	192.168.1.101	OSPF	OSPFv2 Hello [R] 192.0.2.222
14	0.047457	192.168.1.101	75.126.46.230	TCP	4080 → www [EST] Seq=1010888888
15	0.047461	75.126.46.230	192.168.1.101	TCP	4080 → www [RST] Seq=1010888888
17	0.244048	192.168.1.101	75.126.46.230	TCP	1729 → www [RST] Seq=1010888888
18	0.244052	192.168.1.101	75.126.46.230	TCP	1729 → www [RST] Seq=1010888888
19	0.742646	75.126.46.230	192.168.1.101	TCP	www → 4080 [ACK] Seq=1010888888
20	0.742650	75.126.46.230	192.168.1.101	TCP	www → 4080 [ACK] Seq=1010888888
21	0.742654	192.168.1.101	192.0.2.222	OSPF	OSPFv2 Hello [R] 192.168.1.101
22	0.742658	192.0.2.222	192.168.1.101	OSPF	OSPFv2 Hello [R] 192.0.2.222
23	0.492006	192.168.1.101	192.0.2.222	OSPF	OSPFv2 Hello [R] 192.168.1.101
24	0.492010	192.0.2.222	192.168.1.101	OSPF	OSPFv2 Hello [R] 192.0.2.222

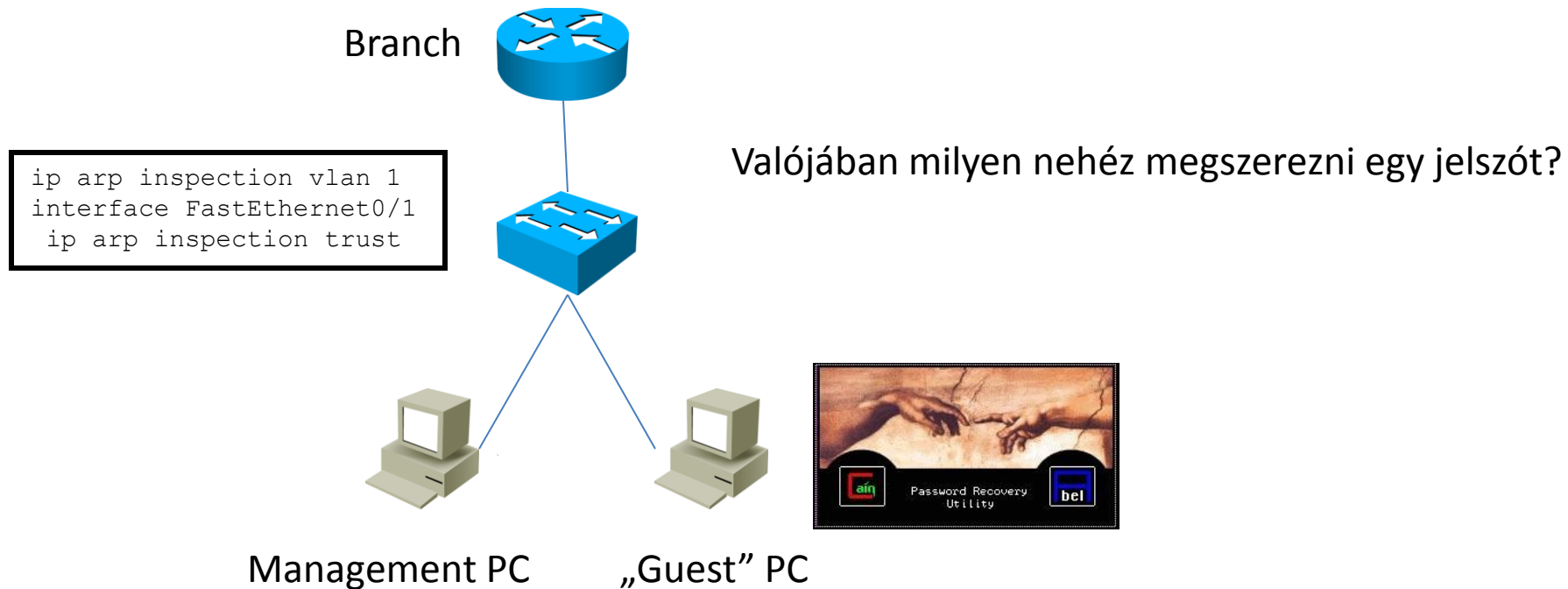
„Forgalom eltérítés” #3

- DHCP támadás



„Forgalom eltérítés” #4

- Man-in-the-middle támadás





Köszönöm!

