



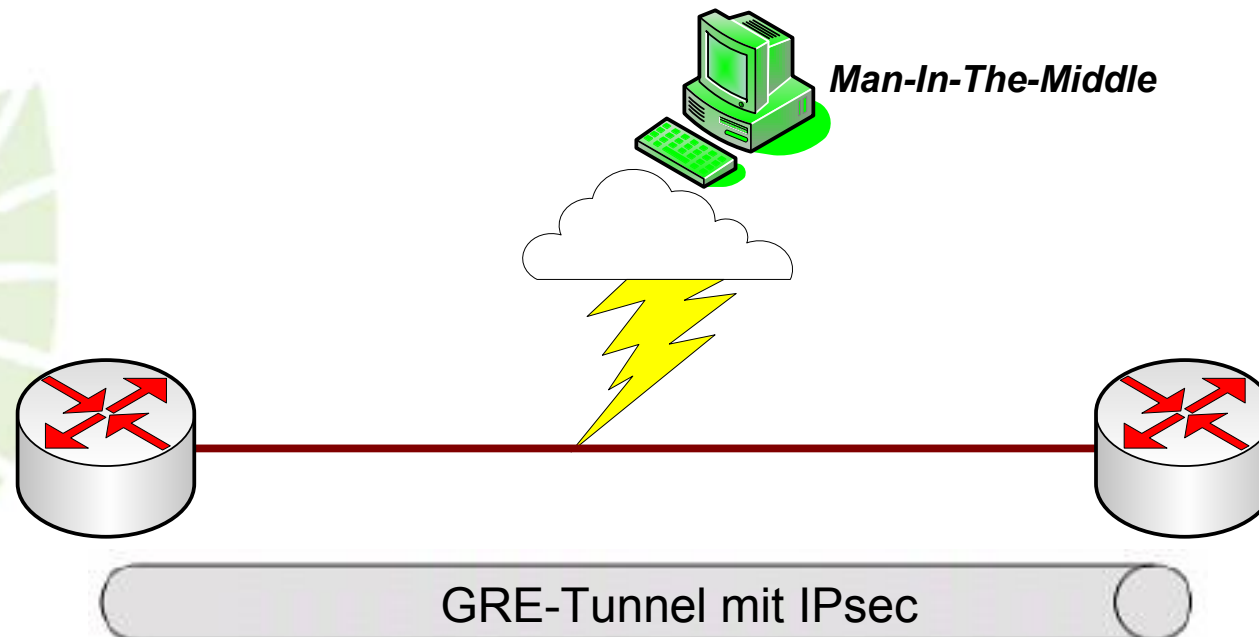
# VoIP Sicherheit

- Telefonie über einen GRE-Tunnel mit IPsec -



# Problemstellung

- Aufbau einer abhörsicheren Verbindung über einen GRE-Tunnel mit IPsec -





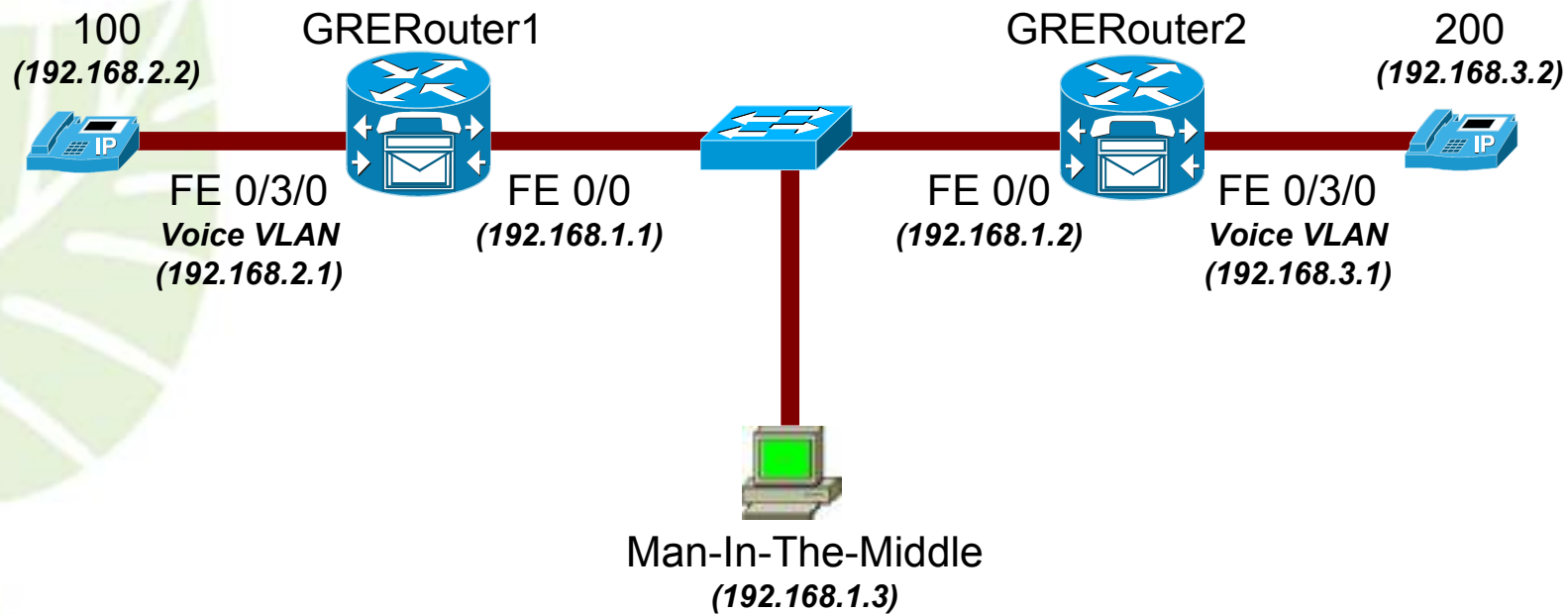
# Benötigte Komponenten

- 2 Router
  - CallManagerExpress
  - Router-IOS: ADVEnterprise
- 1 Switch
- 2 IP-Telefone
- 1 Workstation (Man-In-The-Middle)
  - Cain & Abel, Wireshark (Ethereal)



# Phase 1

- Aufbau einer gewöhnlichen VoIP Verbindung -





# Ergebnis

- Durch das Mitschneiden des Paketstromes erhält der Angreifer RTP-Daten, die er leicht in eine Audiosequenz umwandeln kann.

No.	Time	Source	Destination	Protocol
72	7.140816	192.168.1.2	192.168.1.1	RTP
73	7.147930	192.168.1.1	192.168.1.2	RTP
74	7.148210	192.168.1.1	192.168.1.2	RTP
75	7.150196	192.168.1.2	192.168.1.1	RTP
76	7.150889	192.168.1.2	192.168.1.1	RTP
77	7.157988	192.168.1.1	192.168.1.2	RTP
78	7.158267	192.168.1.1	192.168.1.2	RTP
79	7.159549	192.168.1.2	192.168.1.1	RTP
80	7.159804	192.168.1.2	192.168.1.1	RTP
81	7.159808	192.168.1.1	192.168.1.2	RTP
82	7.159842	192.168.1.1	192.168.1.2	RTP
83	7.200131	192.168.1.2	192.168.1.1	RTP
84	7.200000	192.168.1.1	192.168.1.1	RTP

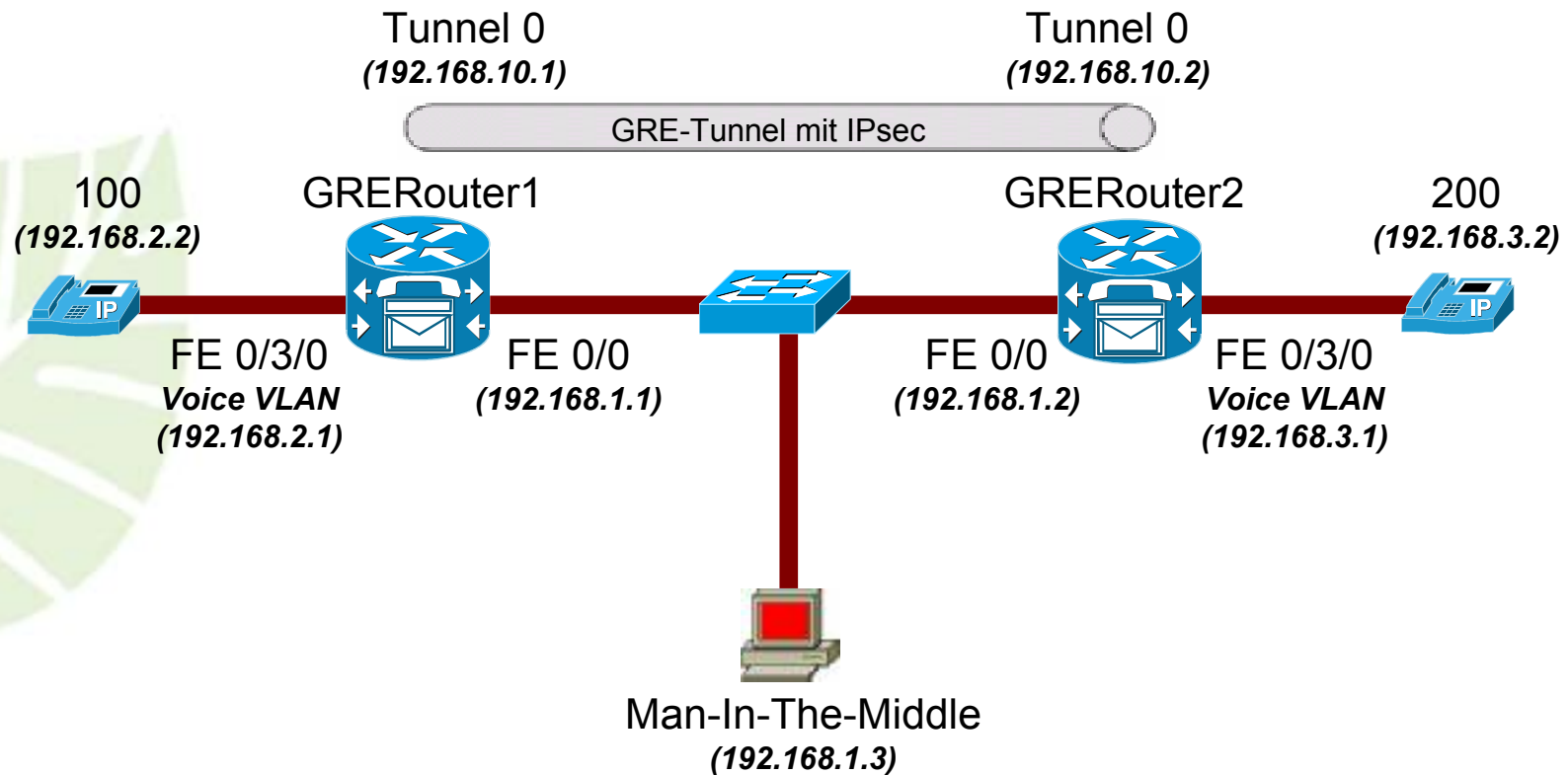
Frame 1 (50 bytes on wire, 60 bytes captured)  
Ethernet II, Src: Intel(R) Ethernet Controller (08:00:27:00:00:00), Dst: Intel(R) Ethernet Controller (08:00:27:00:00:00)  
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.2  
Logical-Link Control, Src: Intel(R) Ethernet Controller (08:00:27:00:00:00), Dst: Intel(R) Ethernet Controller (08:00:27:00:00:00)  
Spanning Tree Protocol

0000 01 80 c2 00 00 00 0e 83 72 c5 c3 00 26 42 42 .....  
0010 03 00 00 00 00 00 80 01 00 0e 83 71 c9 c0 00 00 .....  
0020 0c 00 80 01 00 0e 83 72 c5 c0 80 03 00 00 14 00 .....  
0030 02 00 0f 00 00 00 00 00 00 00 00 00 00 00 .....  
0040 .....



# Phase 2

- Aufbau eines GRE-Tunnel mit IPsec -





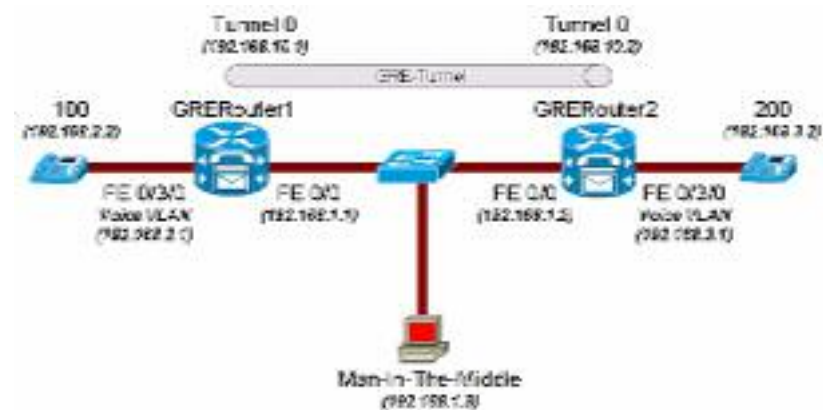
# Phase 2a

## - Konfiguration des GRE-Tunnel -

```
GRERouter1(config)# interface tunnel 0
GRERouter1(config-if)# ip address 192.168.10.1 255.255.255.0
GRERouter1(config-if)# tunnel source 192.168.1.1
GRERouter1(config-if)# tunnel destination 192.168.1.2
GRERouter1(config-if)# no shutdown
```

```
GRERouter2(config)# interface tunnel 0
GRERouter2(config-if)# ip address 192.168.10.2 255.255.255.0
GRERouter2(config-if)# tunnel source 192.168.1.2
GRERouter2(config-if)# tunnel destination 192.168.1.1
GRERouter2(config-if)# no shutdown
```

**Tunnel verhindert nicht die  
Auswertbarkeit der Daten!  
=> Verschlüsselung mit IPsec**





# Phase 2b

## Verschlüsselung mit IPsec - GRERouter1 -

```
GRERouter1(config)# access-list 100 permit gre host 192.168.1.1 host 192.168.1.2
```

```
GRERouter1(config)# crypto isakmp policy 1
```

```
GRERouter1(isakmp-config)# authentication pre-share
```

```
GRERouter1(config)# crypto isakmp key 6 cisco123 address 192.168.1.2 255.255.255.0
```

```
GRERouter1(config)# crypto ipsec transform-set strong esp-3des esp-md5-hmac
```

```
GRERouter1(cfg-crypto-trans)# mode tunnel
```

```
GRERouter1(config)# crypto map vpn 10 ipsec-isakmp
```

```
GRERouter1(cfg-crypto-map)# set peer 192.168.1.2
```

```
GRERouter1(cfg-crypto-map)# set transform-set strong
```

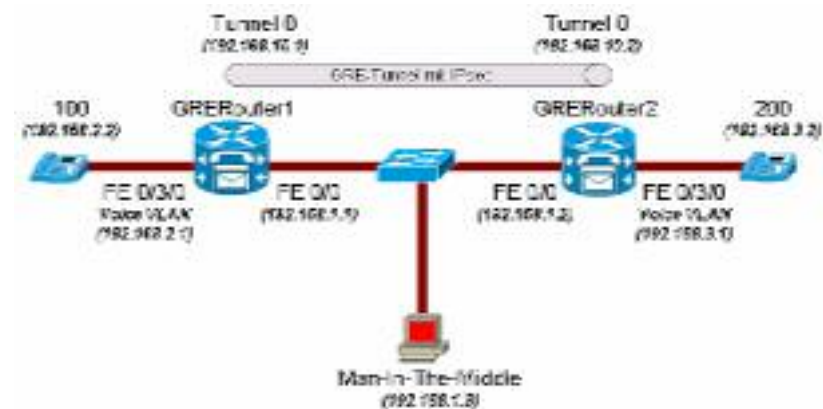
```
GRERouter1(cfg-crypto-map)# match address 100
```

```
GRERouter1(config)# interface tunnel 0
```

```
GRERouter1(config-if)# crypto map vpn
```

```
GRERouter1(config)# interface fastEthernet 0/0
```

```
GRERouter1(config-if)# crypto map vpn
```





# Phase 2b

## Verschlüsselung mit IPsec - GRERouter2 -

```
GRERouter2(config)# access-list 100 permit gre host 192.168.1.2 host 192.168.1.1
```

```
GRERouter2(config)# crypto isakmp policy 1
```

```
GRERouter2(isakmp-config)# authentication pre-share
```

```
GRERouter2(config)# crypto isakmp key 6 cisco123 address 192.168.1.1 255.255.255.0
```

```
GRERouter2(config)# crypto ipsec transform-set strong esp-3des esp-md5-hmac
```

```
GRERouter2(cfg-ctypto-trans)# mode tunnel
```

```
GRERouter2(config)# crypto map vpn 10 ipsec-isakmp
```

```
GRERouter2(cfg-ctypto-map)# set peer 192.168.1.1
```

```
GRERouter2(cfg-ctypto-map)# set transform-set strong
```

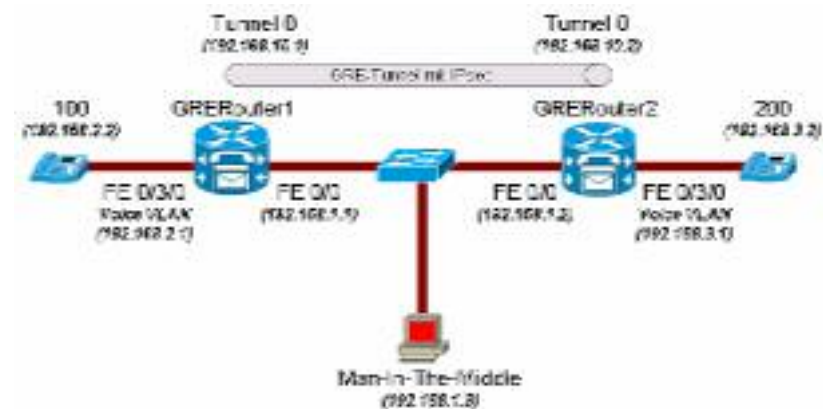
```
GRERouter2(cfg-ctypto-map)# match address 100
```

```
GRERouter2(config)# interface tunnel 0
```

```
GRERouter2(config-if)# crypto map vpn
```

```
GRERouter2(config)# interface fastEthernet 0/0
```

```
GRERouter2(config-if)# crypto map vpn
```





# Ergebnis

- Durch das Mitschneiden des Paketstromes erhält der Angreifer ESP-Daten, die durch ihre Verschlüsselung nicht auswertbar sind.

No.	Time	Source	Destination	Protocol
74	9.8049018	192.168.1.1	192.168.1.2	ESP
75	9.8049901	192.168.1.1	192.168.1.2	ESP
76	9.8079019	192.168.1.2	192.168.1.1	ESP
77	9.8089968	192.168.1.2	192.168.1.1	ESP
78	9.809173	192.168.1.1	192.168.1.2	ESP
79	9.809334	192.168.1.1	192.168.1.2	ESP
80	9.888013	192.168.1.2	192.168.1.1	ESP
81	9.889037	192.168.1.1	192.168.1.2	ESP
82	9.908059	192.168.1.2	192.168.1.1	ESP

Frame 1 (518 bytes on wire (414 bytes captured) on interface 0: [eth0] [0:8:0:0:0:0])

- Ethernet II, Src: Cisco72:c9:5c:00:0a:83 (08:00:0c:29:5c:00:0a:83), Dst: Endo
- Internet Protocol, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255
- User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps
- Bootstrap Protocol

0000 ff ff ff ff ff ff 00 48 83 72 c9 c0 08 00 45 00 .....

0010 02 5c 01 5f 00 00 ff 11 b8 32 00 00 00 00 ff .....

0020 ff ff 00 44 00 43 02 48 00 00 0c 01 06 00 60 00 .....D.C

0030 04 e9 00 00 80 00 00 90 00 00 00 00 00 90 00 .....00



# Fazit

- Daten sind auch nach Umleitung über den GRE-Tunnel noch auswertbar.
- Um eine Auswertung der Daten zu verhindern, ist eine Verschlüsselung (IPsec) erforderlich.



**Haben Sie noch Fragen?**