Laboratory II

Binna, Reschenhofer, Schörghofer

Course: Internet Infrastructure and Security

Lecturer: FH-Prof. DI Mag. Dr. Dominik Engel

23.11.2016

Table of Contents

List of Abbreviations

MOTD	Message of the Day
DCE	Data Communication Endpoint
OSPF	Open Shortest Path First
IP	Internet Protocol
LSR	Link State Routing
AS	Autonomous System
TTL	Time To Live

1 Topology

The following topology (figure 1.1, taken from the Moodle instructions) had to be recreated in the lab.

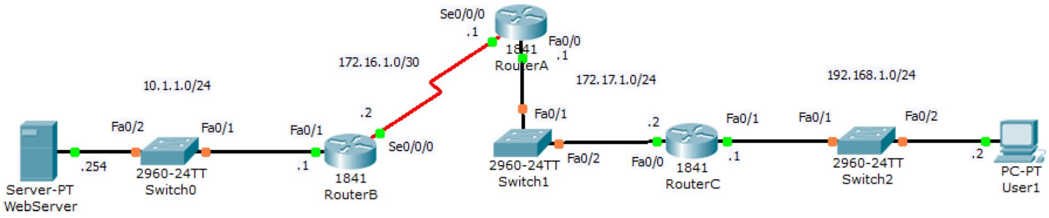


Figure 1.1: Topology (Moodle)

Each device was configured with basic settings like hostname, Message of the Day (MOTD), a secret enable password, disabled IP domain lookup, synchronous logging on line console 0 and the service password-encryption, which prevents passwords from being displayed in clear-text in the start-up and running configuration. The important part is that the clock-rate for the serial interface has to be configured on the Data Communication Endpoint (DCE) device.

```
interface Serial0/0/0
 bandwidth 64
 ip address 172.16.1.1 255.255.255.252
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 7 094F471A1A0A
 clock rate 64000
```

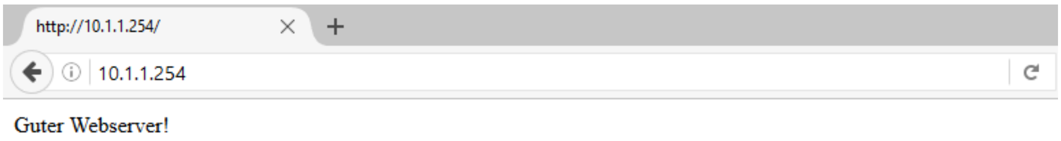
Listing 1.1: Setting the clock-rate on Router A

Open Shortest Path First (OSPF) is a routing protocol for Internet Protocol (IP) networks. It uses a Link State Routing (LSR) algorithm and falls into the group of interior routing protocols, operating within a single Autonomous System (AS). Concerning the OSPF routing, every router assigns its known networks to the OSPF routing process with area 0.

```
router ospf 1
 area 0 authentication message-digest
 network 172.16.1.0 0.0.0.3 area 0
 network 172.17.1.0 0.0.0.255 area 0
```

Listing 1.2: OSPF routing example router A

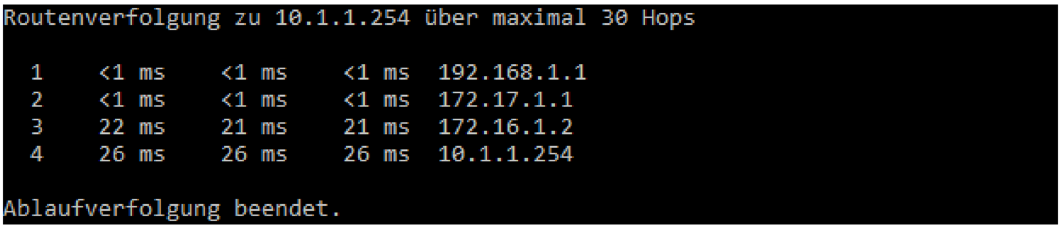
"nginx" has been set up as a webserver on a linux pc with default configuration for http (IP address for the webserver is "10.1.1.254"). Ping and webserver access from the user-pc to the webserver has been successful as shown in (figure 1.2). Be sure to disavle the windows firewall on both devices to allow ping.



Guter Webserver!

Figure 1.2: Webserver access

For this topology the ping command from the user pc to the webserver took on average 18ms and had a remaining Time To Live (TTL) of 61. The tracert command as shown in (figure 1.3) from the user pc to the webserver shows that a package needs 4 hops to reach the webserver.



```
Routenverfolgung zu 10.1.1.254 über maximal 30 Hops

  1    <1 ms    <1 ms    <1 ms  192.168.1.1
  2    <1 ms    <1 ms    <1 ms  172.17.1.1
  3    22 ms    21 ms    21 ms  172.16.1.2
  4    26 ms    26 ms    26 ms  10.1.1.254

Ablaufverfolgung beendet.
```

Figure 1.3: Tracert from user pc to good webserver

2 Router Spoofing

For the router spoofing attack another router has beed added to the network as seen in (figure 2.1, taken from the Moodle instructions). This router also operates in OSPF mode.

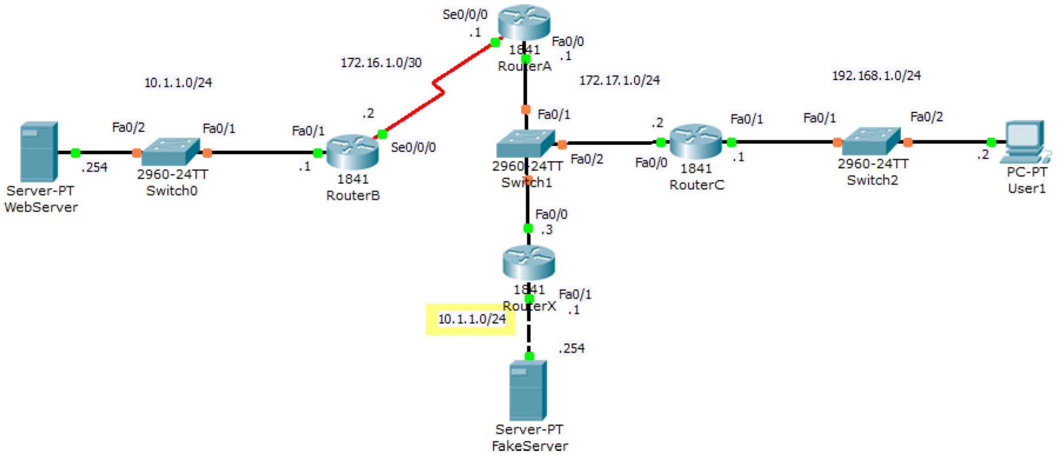


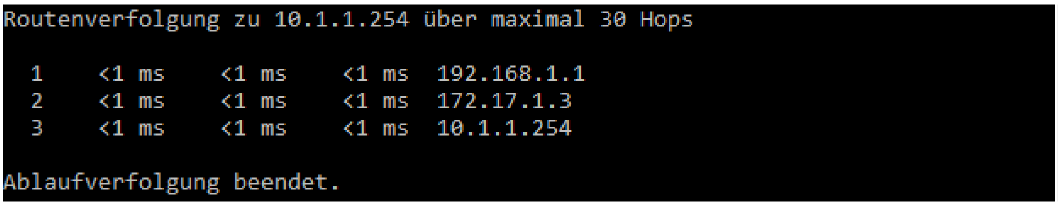
Figure 2.1: Router spoofing topology

Router X is now configured in a way that neighboring routers think this Router B with the webserver in his network.

```
router ospf 1
 network 10.1.1.0 0.0.0.255 area 0
 network 172.17.1.0 0.0.0.255 area 0
```

Listing 2.1: OSPF configuration on router X

OSPF detects changes in the topology it computes the shortest-path tree for each route using a method based "Dijkstra's algorithm". The bad Router X propagates that he has a network "10.1.1.0/24" with the webserver. This results in a shorter path from the user pc to the webserver. The user pc doesn't know that this is a bad webserver since OSPF only detected a shorter path to the webserver. Router C is now storing the route to Router X in the routing table, because this route has the lower path cost. Therefore, a ping from the user pc now goes to the bad server. The ping from the user pc to the bad webserver is <1ms with a TTL of 62. Because of the new route the package isn't sent over the serial link whichg results in a shorter response time for the ping command. The tracert command (figure 2.2) shows that the package only needs 3 hops to its destination and the averga response time is <1ms.



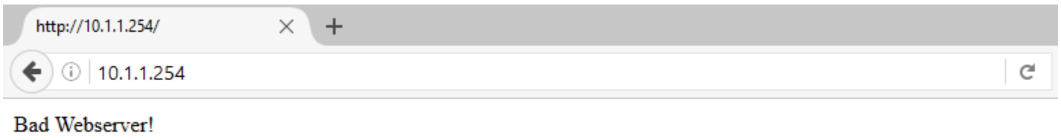
```
Routenverfolgung zu 10.1.1.254 über maximal 30 Hops

  1    <1 ms    <1 ms    <1 ms  192.168.1.1
  2    <1 ms    <1 ms    <1 ms  172.17.1.3
  3    <1 ms    <1 ms    <1 ms  10.1.1.254

Ablaufverfolgung beendet.
```

Figure 2.2: Tracert from user pc to bad webserver

If the user wants to access the webserver again, he will be redirected to the bad webserver, because of the routing table entry in router C which states that the shortest path to the network "10.1.1.0/24" with the webserver is the one via router X. (figure 2.3) shows the output when accessing the webserver.



Bad Webserver!

Figure 2.3: Bad webserver access

3 Router Authentication

In this chapter, the router authentication methods are explaned. Router authentication for OSPF allows to flexibly authenticate OSPF neighbours. This enables OSPF routing to exchange routing update information in a secure manner. There exist three different types of authentication in OSPF:

- Null authentication: Also called type 0 -> no authentication information is included in the packet header. This is also default.
- Plain text authentication: type 1 -> use of simple plain-text passwords
- Md5 authentication: typ2 -> use of md5 cryptographic passwords (also not secure anymore!)

OSPFv3 is capable of using SHA1 authentication, which is at least better than MD5 authentication.

3.1 Plain Text Authentication

At first, plain text authentication has been configured. The authentication key is configured for each interface separately by use of the following command:

```
ip ospf authentication-key cisco
```

Only interfaces, where the authentication key match, can participate in OSPF advertising. The following command then enables OSPF authentication for all interfaces inside area 0:

```
router ospf 1
        area 0 authentication
```

When the commands above are executed on only Router A and Router C, all OSPF routes that have previously been stated in the routing table (advertised from Router B) are now lost, because Router B doesn't have the authentication configuration. The big disadvantage of plain text authentication is, that the password can be clearly seen in the packet.

3.2 MD5 Authentication

First the md5 message digest has to be set on the interfaces:

```
Interface s0/0/0
      ip ospf message-digest-key 1 md5 cisco
```

After that, md5 authentication can either be enabled on a per interface basis with the following command:

```
Interface s0/0/0
      ip ospf authentication message-digest
```

Or globally for all interfaces belonging to a specific area:

```
router ospf 1
       area 0 authentication message-digest
```

4 Sniffing Attack and Clear Text Password Router Authentication