1. Aufbau der Testumgebung

It’s important that the clock for the serial interface has to be configured on the DCE (data communication endpoint) device.

Concerning OSPF routing every router assigns it’s known networks to the OSPF routing process with area 0.

As webserver nginx has been set up on an linux pc with default configuration over http. Ping and webserver access from the user pc to the webserver has been successful.

1. Router Spoofing

The ping between the user pc and the good webserver has been measured and is 18ms. TTL is 61. Theoretically, the ping from the user pc to the good webserver must be shorter and TTL must also be higher.

The ping from user pc to bad webserver is <1ms and TTL is 62.

RouterC is now storing the route to RouterX 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.

1. Router Authentication

**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.

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.

**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