OSPF & Security

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Version #   |     Type      |         Packet length         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          Router ID                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           Area ID                             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           Checksum            |             Autype            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Authentication                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Authentication                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Currently defined:

0 No authentication

1 Simple password

This is silly:

- Simple to attack,
- Need something better.

The proposal: use MD5, as in SNMPv2.

- MD5:
  - One way function of message + password.
  - Do not transmit password, but only result.
- What is the protection:
  - + Messages cannot be forged,
  - + Messages cannot be changed,
  - - Messages can be replayed,
  - ? Messages stay in the clear.
- The rationales:
  - Used in SNMPv2: present in routers.
  - No encryption: no export control.
  - Password management is already present.

The implementation:

- Emission:
  - prepare OSPF packet (with password),
  - compute MD5 of packet,
  - erase password,
  - insert MD5 check.
- Reception:
  - save MD5 check,
  - insert password,
  - compute MD5 of packet,
  - compare with received value.
- One big problem: need 16 octets.
  - Either extend the OSPF packet size,
  - Or provide OSPF "trailer",
  - Or only use 8 out of 16:
    - easy to implement,
    - subject to crypto-analysis,
    - still better than clear text...
- Also needed:
  - MIB variable,
  - Secure set up of password.