RoMON

Summary

RoMON stands for "Router Management Overlay Network". RoMON works by establishing an independent MAC layer peer discovery and data forwarding network. RoMON packets are encapsulated with EtherType 0x88bf and DST-MAC 01:80:c2:00:88:bf and its network operate independently from L2 or L3 forwarding configuration. When RoMON is enabled, any received RoMON packets will not be displayed by sniffer or torch tools.

Each router on the RoMON network is assigned its RoMON ID. RoMON ID can be selected from the port MAC address or specified by the user.

RoMON protocol does not provide encryption services. Encryption is provided at the "application" level, by e.g. using ssh or by using a secure Winbox.

Secrets

RoMON protocol secrets are used for message authentication, integrity check and replay prevention by means of hashing message contents with MD5.

For each interface, if the interface-specific secret list is empty, a global secret list is used. When sending out, messages are hashed with the first secret in list if list is not empty and first is not "empty secret" (empty string = ""), otherwise, messages are sent unhashed. When received, unhashed messages are only accepted if a secret list is empty or contains "empty secret", hashed messages are accepted if they are hashed with any of the secrets in list.

This design allows for the incremental introduction and/or change of secrets in-network without RoMON service interruption and can happen over RoMON itself, e.g.:

- initially, all routers are without secrets;
- configure each router one by one with secrets="","mysecret" - this will make all routers still send unprotected frames, but they all will be ready to accept frames protected with secret "mysecret";
- configure each router one by one with secrets="mysecret","" - this will make all routers use secret "mysecret", but also still accept unprotected frames (from routers that have not yet been changed);
- configure each router with secrets="mysecret" - this will make all routers use secret "mysecret" and also only accept frames protected with "mysecret";

Changing of secret in a network should be performed in a similar fashion where for some time both secrets are in use in network.

Peer discovery

In order to discover all routers on RoMON network RoMON discover command must be used:

```
[admin@MikroTik] > /tool/romon/discover
Flags: A - active
Columns: ADDRESS, COSt, Hops, PATH, L2MTu, IDENTITY, VERSION, BOARD
   ADDRESS            COS  H  PATH               L2MT  IDENTITY   VERSION    BOARD
A  6C:3B:6B:48:0E:8B  200  1  6C:3B:6B:48:0E:8B  1500  hEX        6.47beta7  RB750Gr3
A  6C:3B:6B:ED:83:69  200  1  6C:3B:6B:ED:83:69  1500  CCR1009    6.47beta7  CCR1009-7G-1C-1S+
A  B8:69:F4:B3:1B:D2  200  1  B8:69:F4:B3:1B:D2  1500  4K11       6.47beta7  RB4011iGS+5HacQ2HnD
A  CC:2D:E0:26:22:4D  200  1  CC:2D:E0:26:22:4D  1500  CCR1036    6.47beta7  CCR1036-8G-2S+
A  CC:2D:E0:8D:01:88  200  1  CC:2D:E0:8D:01:88  1500  CRS328     6.47beta7  CRS328-24P-4S+
A  E4:8D:8C:1C:D3:0E  200  1  E4:8D:8C:1C:D3:0E  1500  MikroTik   6.47beta7  RB2011iLS
A  E4:8D:8C:49:49:DB  200  1  E4:8D:8C:49:49:DB  1500  hAP        6.47beta7  RB962UiGS-5HacT2HnT
```

Configuration Examples

In order for a device to participate in the RoMON network, the RoMON feature must be enabled and ports that participate in the RoMON network must be specified.

```
/tool romon set enabled=yes secrets=testing
```

Ports that participate in the RoMON network are configured in **the RoMON port** menu. Port list is a list of entries that match either specific port or all ports and specifies if matching port(s) is forbidden to participate in the RoMON network and in case port is allowed to participate in RoMON network entry also specifies the port cost. Note that all specific port entries have higher priority than the wildcard entry with **interface=all**.

For example, the following list specifies that all ports participate in RoMON network with cost 100 and ether7 interface with cost 200:

```
[admin@MikroTik] > /tool/romon/port/print
Flags: * - default
Columns: INTERFace, FOrbid, COSt
#     INTERF  FO  COS
0  *  all     no  100
1     ether7  no  200
```

By default one wildcard entry with **forbid=no** and **cost=100** is created.

Applications

Multiple applications can be run over the RoMON network.

In order to test the reachability of specific router on RoMON network RoMON ping command can be used:

```
[admin@MikroTik] > /tool/romon/ping id=6C:3B:6B:48:0E:8B count=5
  SEQ HOST                                    TIME  STATUS
    0 6C:3B:6B:48:0E:8B                       1ms
    1 6C:3B:6B:48:0E:8B                       0ms
    2 6C:3B:6B:48:0E:8B                       1ms
    3 6C:3B:6B:48:0E:8B                       0ms
    4 6C:3B:6B:48:0E:8B                       1ms
    sent=5 received=5 packet-loss=0% min-rtt=0ms avg-rtt=0ms max-rtt=1ms
```

In order to establish a secure terminal connection to router on RoMON network RoMON SSH command can be used:

```
[admin@MikroTik] > /tool/romon/ssh 6C:3B:6B:48:0E:8B
```

Run RoMON in Winbox by using CLI

In order to establish the RoMON session directly by using the command line on a computer, you must specify RoMON agents and desired routers addresses. RoMON agent must be saved on Managed routers list in Winbox in order to make a successful connection:

```
winbox.exe --romon 192.168.88.1 6C:3B:6B:48:0E:8B admin ""
```