INTERNET-DRAFT Kohei Ohta [kohei@nemoto.ecei.tohoku.ac.jp]
draft-kohei-rmon-svcloc-00.txt Tohoku University.
Tomohiro Ika [ika@nemoto.ecei.tohoku.ac.jp]
Tohoku University
Glenn Mansfield [glenn@wide.ad.jp]
Cyber Solutions Inc.
November 1997

Network Service Discovery using RMON-MIB.

Status of this Memo

Abstract

The Remote network monitoring MIB may be conveniently utilised to discover network services. This memo briefly outlines the technique of carrying out the discovery.

Table of Contents

1. Introduction

Remote network monitoring devices are probes that are deployed to look at all packets in a connected network segment(s). These are generally dedicated devices with dedicated resources to carry out traffic capture, filter and analysis at a Managers bidding. The Remote Network Monitoring Management Information Base, RMON-MIB [RFC1757] , provides an interface to a remote networking device which is called an RMON-agent. The more recent Remote Network Monitoring Management Information Base version 2, RMON2-MIB [RFC2021] has even more efficient and sophisticated facilities. Both can be conveniently used to to discover various network services. In this memo we show a simple mechanism to discover network services by using the RMON-MIB which is more widely deployed.

2. The Network Service Discovery Algorithm

An RMON-agent can be configured to filter the probed network traffic by protocol and send a notification to a manager in case a packet passes the filter. A protocol directory containing the essential details required to identify a network service in a packet is required. It will essentially tell the position and value of the corresponding assigned portnumber [RFC1700]. The RMON2-MIB has a built-in protocol directory.

The RMON agent will be probing the traffic and watching for packets which correspond to any of the network services listed in the protocol directory, by applying the corresponding "service filters". If a packet passes the filter, it is "captured" and a "network service discovered" notification is sent to the Network Manager which is performing in the role of a network service discoverer.

When the network manager receives a "network service discovered" notification it fetches the captured packet(s) from the RMON-agent. determines the corresponding server address from the packet (IP-Source). And updates the network service directory appropriately. To reduce load on the system, the network manager may also apply a suppress filter to suppress similar packets (describing the same service on the same server) from being captured.

Fig. 1 shows the algorithm schematically.

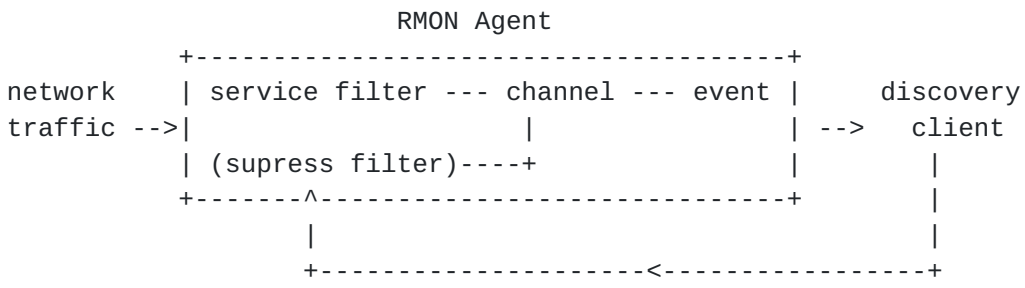

Fig. 1. Network Service Discovery using an RMON Agent

3. Details.

3.1 Filter Definitions for discovering network services.

The definition of filters to be used in the RMON probe essentially comprises three Managed Objects - filterPktData, filterPktDataMask, and filterPktDataNotMask. Each of these are bit patterns and are briefly explained below. For detailed descriptions refer to RFC1757.

- o filterPktData is the data that is to be matched with the input packet.
- o filterPktDataMask is the mask that is applied to the match process.
- o filterPktDataNotMask is the inversion mask that is applied to the match process.

For example the following filter is applied to discover an HTTP service related packet.

```
        IP                      TCP                      HTTP
-----------------------------------------------------------------
filterPktData =
          8 0 0 0 0 0 0 0 0 0 0   6 0 0 0 0 0 0 0 0 0 0   0  80
filterPktDataMask =
        255 0 0 0 0 0 0 0 0 0 0 255 0 0 0 0 0 0 0 0 0 0 255 255
filterPktDataNotMask =
        255 0 0 0 0 0 0 0 0 0 0 255 0 0 0 0 0 0 0 0 0 0 255 255
```

Note, for divide and conquer, above filter is configured as SUPRESS filter by filterPktDataNotMask object.

These filters are needed for each service and associated to channels.

3.2 Scope of Discovery

It is straightforward to restrict the discovery to a specific network or networks. A target network is specified by a network number and mask. For each target network a filter is configured and associated to the channel.

Example: Say we want to restrict the discovery to the following networks defined by a network number and mask,

130.34.199.0/26

The corresponding filter configuration is as follows:

```
          IP                            IP source addr
-------------------------------------------------------------------
filterPktData =
           8 0 0 0 0 0 0 0 0 0 0 0 0 0 130  34 199   0 0 0 0 0 0 0
filterPktDataMask =
        255 0 0 0 0 0 0 0 0 0 0 0 0 0 255 255 255 192 0 0 0 0 0 0
filterPktDataNotMask =
        255 0 0 0 0 0 0 0 0 0 0 0 0 0 255 255 255 192 0 0 0 0 0 0
```

These filters are also configured as SUPRESS filter as same as above service filter.

4. Examples of Discovered services

The following is an example of the network services directory which is dicovered by employing the filters shown in examples of 3.1 And 3.2.

	service name	server address
	www-http	130.34.199.4
	www-http	130.34.199.35
target network	www-http	130.34.199.8
130.34.199.0/26	ftp	130.34.199.8
	domain	130.34.199.2
	domain	130.34.199.2
	pop3	130.34.199.2
	ntp	130.34.199.2
:	:	:

The discovery time-stamp is also available.

5. Pros and Cons.

The technique proposed is useful as it is automatic and passive. It does not count on any other service and is thus more robust. If there is a service and if it is being used via the segment on which the RMON agent is attached, it will be detected.

On the other hand the technic is passive. If the service is not used it will not be detected. And, the technic can be used only in places where an RMON probe can be attached.

6. Acknowledgements.

This draft is the product of discussions and deliberations carried out in the NetMan working group of Tohoku University.

7. References

[1] CCITT Blue Book, "Data Communication Networks: Directory", Recommendations X.500-X.521, December 1988.

Security Considerations

In deploying the proposed mechanism, care will need to be taken to ensure the authenticity of the sources of information viz. the DNS servers and the WHOIS servers.

It needs to be noted that information from these sources do not

in generally carry any guarantee about the integrity or consistency of the contents.

Clients availing of the directory services will need ensure the authenticity of the corresponding servers.

Authors' Addresses

Kohei Ohta
GSIS, Tohoku University
Aoba-ku, Sendai
Japan

Phone: +81-22-217-7140
EMail: kohei@nemoto.ecei.tohoku.ac.jp

Tomohiro Ika
GSIS, Tohoku University,
Aoba-ku, Sendai 989-32
Japan

Phone: +81-22-217-7140
EMail: ika@nemoto.ecei.tohoku.ac.jp

Glenn Mansfield
Cyber Solutions Inc.
6-6-3 Minami Yoshinari
Aoba-ku, Sendai 989-32
Japan

Phone: +81-22-303-4012
EMail: glenn@wide.ad.jp