

# The Why and How of Full Service Monitoring

## Background

Without FSM™ monitoring any discussion as to the user Quality of Experience is meaningless. What can be more service affecting than a set-top box that is unable to decrypt a Premier League football match because the CA portal cannot be detected by the STB. This is why Bridgetech has always had as its remit to look to the transport layer and the protocols involved that literally make IPTV work (or not).

This short article is aimed at Bridgetech's business partners and will give a brief non-technical introduction to the background of this system and how it is implemented in our product line.

## The Simple Case

First of all let's start with some background on a normal IP-monitoring case. Usually an IP-Probe is inserted between a multicast server and some other device, for instance a set-top box as shown in Figure 1.

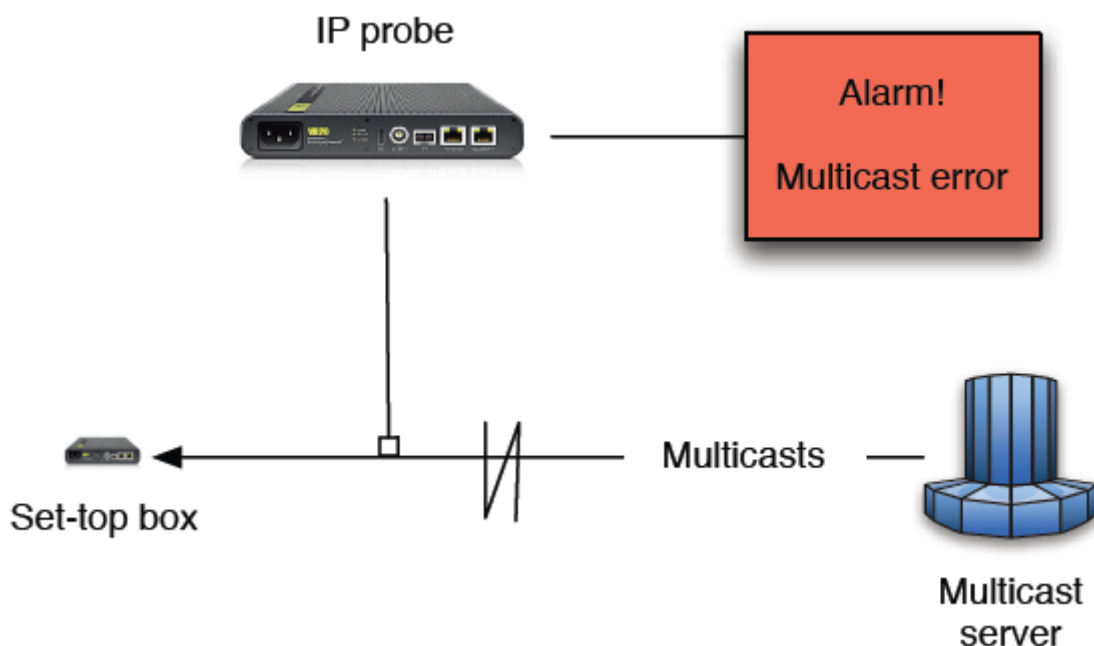


Figure 1: IP-probe monitoring multicasts sent to a set-top box.

The IP-Probe constantly monitors the multicasts going to the set-top box and will raise an alarm if any errors are detected. This case is, however, overly simplified. In a somewhat more real-life situation there will be a middleware component added to this scenario.

## The Glue Called Middleware

The term "middleware" is a container for any hardware or software components inserted between the set-top box and the multicast source. The reason for inserting these extra components in the multicast system is to add additional functionality such as electronic program guides, billing systems, access management etc.

In many cases these middleware components are just as important as the multicasts themselves from the end-users point of view. To clarify this we will take a video-on-demand system as an example, see Figure 2. In this case, if the set-top box is unable to access the conditional-access server the end user will not be able to watch an unencrypted multicast.

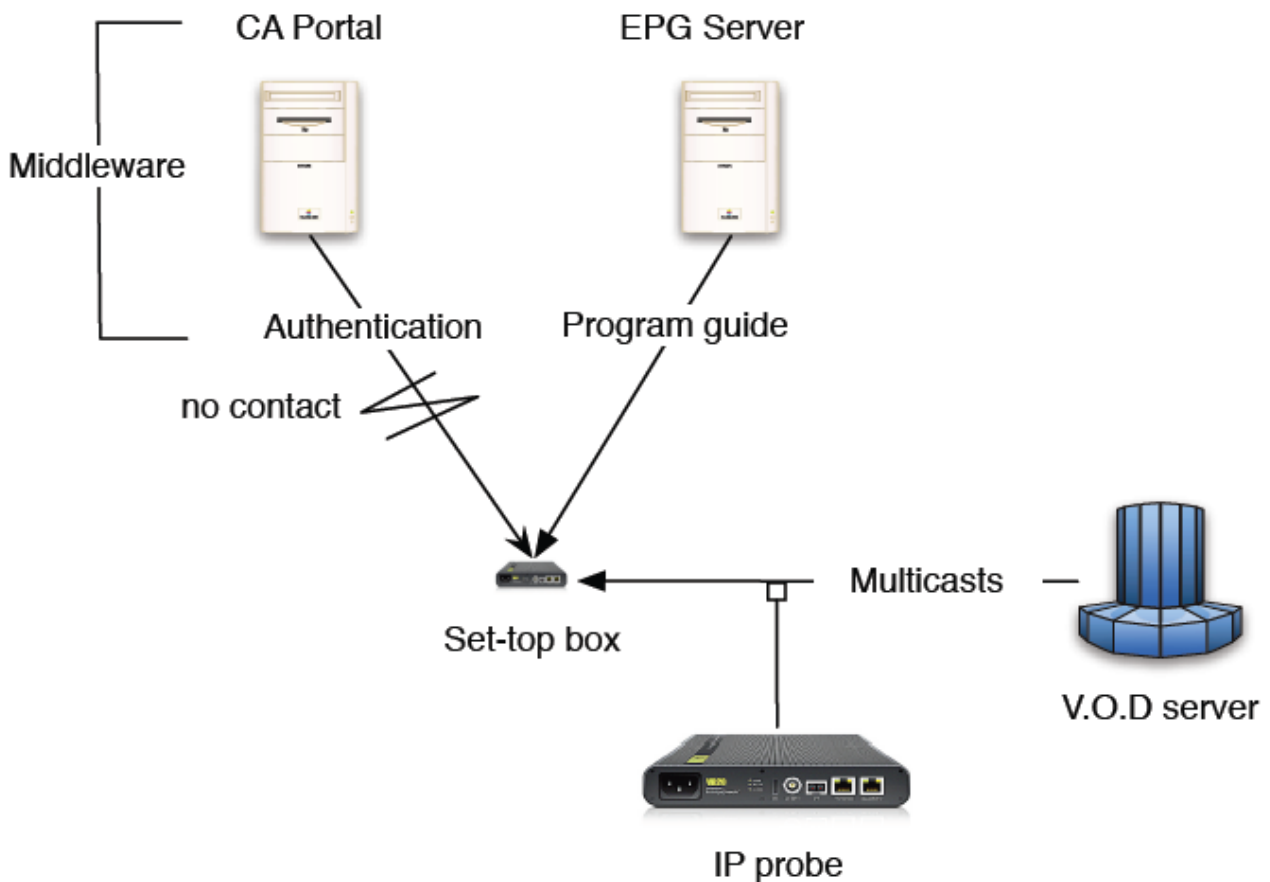


Figure 2: Conditional Access Server is not reachable by the set-top box.

Even though there is an IP-Probe monitoring the multicast, the case of the unavailable middleware server will not be detected and no alarms will be raised. Since the effect of this error is just as bad as multicast errors from the end-users point of view, it needs to be addressed in an IPTV monitoring system. Enter Full Service Monitoring.

### Total Control With FSM™

To further enhance the confidence level of our monitoring system we have included Full Service Monitoring in the VB2 series IP-Probes. FSM™ is targeted at middleware servers and other vital system components. Using the familiar monitoring concept developed and used to monitor multicasts in our earlier products, FSM™ monitors service availability in real-time and raises alarms on errors.

To illustrate a typical scenario involving Full Service Monitoring, Figure 3 shows the same case as discussed previously, only this time with FSM™ included in the IP-probe toolset. Now the probe will monitor the middleware servers in addition to just the multicasts. If, for some reason, the Conditional Access portal should suddenly become unavailable it will be detected by the probe and an alarm will be raised.

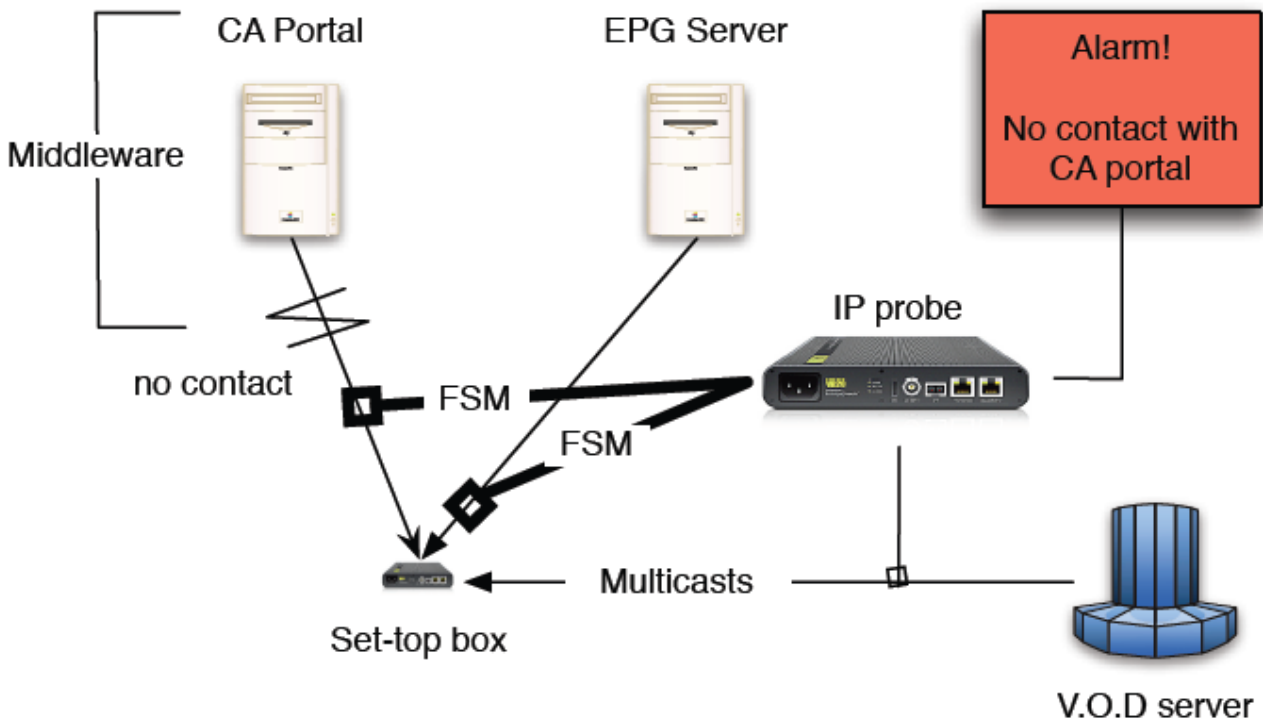


Figure 3: A video-on-demand system monitored with FSM™

## Configuration and Usage

FSM™ is configured in the 'Setup' section of the user-interface just as the other features of the IP-Probe. Up to 10 services may be monitored simultaneously. Each service can be probed by either an ICMP echo request (also known as ping) or by an HTTP get request. The type of protocol used to probe the target server should be chosen to best reflect how the service is used in the system. A ping might be sufficient to check the availability of simple services like gateways and routers but many services will be content specific and delivered over HTTP and therefore require the HTTP protocol.

Here is a screenshot of the actual FSM™ setup interface:

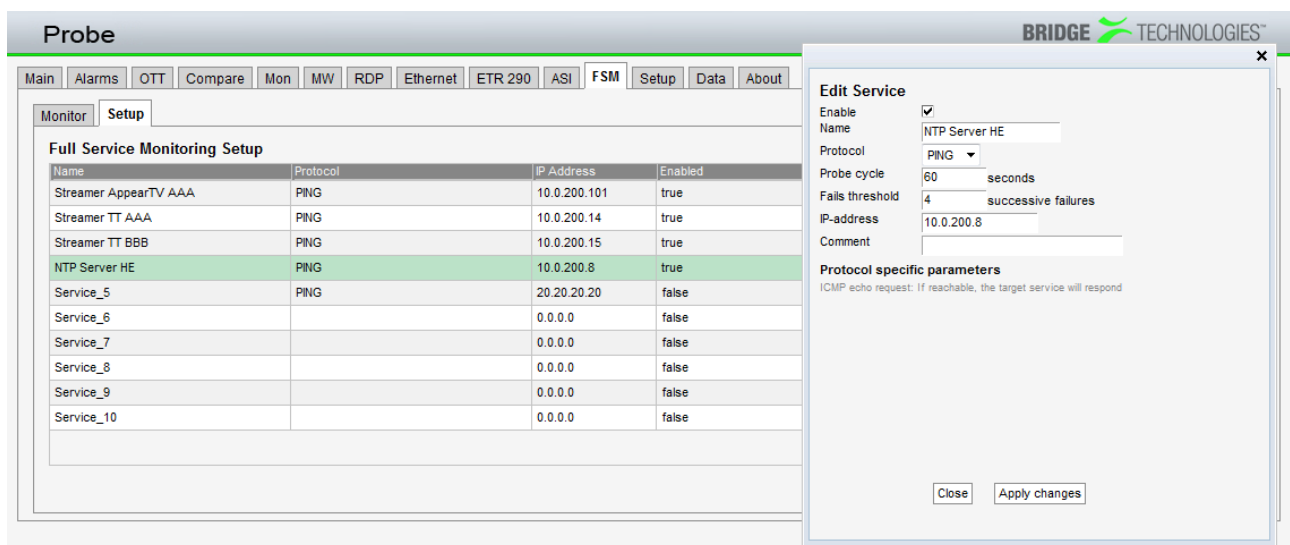


Figure 4: FSM™ setup interface.

How to choose the appropriate protocol depends on what is known about the target service. The HTTP option requires some knowledge about specific url's used to access the service and information about the content returned by the service. If this is unknown, or hard to obtain, ping will be a wiser choice since it will always work as long as the probe is able to reach the target server via Ethernet. The main difference between ping and HTTP is that ping only checks for server availability but HTTP verifies the content returned by the process running on the server.

Once the services are defined in 'Setup' they can be monitored in the main FSM tab. This pane shows the realtime status of each service monitored as shown in Figure 5.

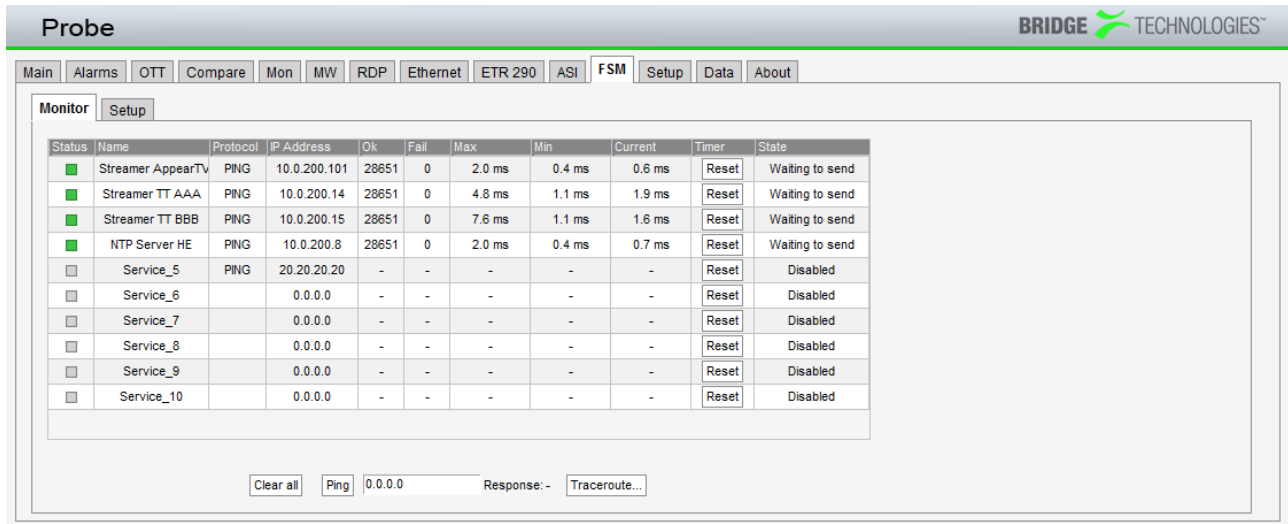


Figure 5: FSM™ realtime monitoring

For convenience a manual ping field is located below the status table. By entering a valid IP address and pressing the 'ping' button an arbitrary server in addition to the pre-defined services may be pinged.

## Conclusion

As discussed in this article, Full Service Monitoring is another great tool in the Bridge Technologies IP monitoring toolbox. The ability to monitor and report errors from middleware services is vital for complex IPTV systems already deployed by many of our customers. We therefore see this as a new but important area of interest for our VB-series of probes that will be further expanded in future releases.