11.5.3 应用程序基线

最后一个网络基线类别是应用程序基线。这个基线应该用于所有基于网络的关键业务应用程序。

应用程序基线包含以下几个组件。

1．使用的协议

我们在这个基线中再次使用了 Wireshark 的协议分层统计窗口，但这次是在运行应用程序的主机上捕获流量。然后，你可以通过比较这个列表，发现依赖于这些协议的应用程序是否正常运转。

2．启动/关闭

这个基线需要捕获应用程序启动和关闭时生成的流量。一旦应用程序不能启动、不能关闭，或这两个过程都异常缓慢，你就可以使用它确定原因。

3．关联/依赖

这个基线需要持续更久的捕获，以通过会话窗口确定这个应用程序依赖的其他主机和应用程序。有时我们会意识不到应用程序间的一些潜在依赖关系，这时应用程序基线便能派上用场。通过这个，你可以确定应用程序不能正常运转，是因为配置错误还是因为所依赖应用程序的高延迟。

4．数据传输率

你可以在应用程序服务器正常运转期间，使用 Wireshark 的捕获概述和绘图功能确定数据传输率和连接一致性。每当有人报告应用程序缓慢时，你就可以使用这个基线来确定当前问题是否是高利用率或高用户负载造成的。