11.5.1 站点基线

站点基线的目的是获得网络上每个物理站点的整体流量快照。理想情况下，这将是 WAN 内的每一个段。

这个基线应该包含以下几个组件。

1．使用的协议

在网络边缘（路由器/防火墙）捕获网段上所有设备的流量时，请使用协议分层统计窗口（**Statistics->Protocol Hierarchy**）来查看所有设备的流量。然后，你可以对照查看是否缺少本应出现的协议，或者网络上是否出现了新的协议。你也可以在协议的基础上，用它来发现高于正常数量的特定类型的流量。

2．广播流量

这包含网段上的一切广播流量。在站点内任一点监听都可以捕获所有广播流量，通过它可以了解正常情况下谁将大量广播流量发送到网络中，这样你将很快确定是否出现了过多（或过少）的广播流量。

3．身份验证序列

这包括任意客户端到所有服务的身份验证过程的流量，比如动态目录、Web 应用程序，以及特定组织的软件。身份验证通常是服务运行缓慢的一个方面。通过基线你可以确定身份验证是否是通信缓慢的原因。

4．数据传输率

这通常包括在网络上测量这个站点到其他站点的大量数据传输。你可以使用 Wireshark 的捕获概述和绘图功能来确定传输速率和连接的一致性。这可能是你的一个很重要的站点基线。每当在网段上建立或拆除连接速度很慢时，你就可以运行与基线同样的数据传输并比较结果。这会告诉你连接是否真的很慢，甚至可能帮助你查找缓慢的原因。