

白皮书

## 您为什么需要带外管理

网络攻击、人为错误或任意环境状况都可能会造成系统中断。

许多网络要素也可能会导致中断。电缆互连、电源、交换机、密集的计算机箱、存储阵列甚至空调都可能会是问题来源。如果软件堆栈经常更新并且易于受到错误、漏洞利用和网络攻击的影响，那么只会增加网络设备的复杂性。

## 随时访问您的网络设备

如果主网络变得不可用,从数据中心和分支机构到边缘网络和 IoT 设备的所有网络部分是否都具有连接弹性?随着业务的发展,网络变得越来越复杂,新的部署或并购可能缺乏通过 Internet 无缝连接的能力。

考虑以下最近发生的严重中断和黑客攻击示例:

- **2015 年发生,并且在 2018 年再次发生 – Google:** 盗窃 Google+ 个人资料中的私人信息,包括姓名、雇主和职务、电子邮件地址、出生日期、年龄和婚姻状况。违规事故导致 Google 永久关闭了 Google+ 服务。
- **2018 年 – 英国航空:** 黑客攻击了 BA 网站和应用程序,盗取了超过 380,000 名客户的财务和个人数据。
- **2019 年 – Target:** 公司的注册中断了两个小时,导致销售额损失 5 千万美元。
- **2019 年 – Facebook:** 出现多次网络中断,Facebook 每小时的停机时间损失为 630 万美元。这包括公司由于股票受到重创而遭受的额外损失。

没有企业能够承担得起中断带来的后果,但是网络越庞大,发生中断的可能性就越大。中断的成本高昂,可能需要现场技术人员随时解决。即使为了纠正错误而进行固件更新、配置更改和重启,也需要人工服务。您需要通过辅助连接进行远程访问,以便随时可以访问网络设备。

### 什么造成中断?

网络攻击、人为错误或任意环境状况都可能会造成系统中断。

网络硬件故障和频繁更新的软件堆栈中的漏洞也可能导致中断。

2019 年 6 月,由于持续数小时的网络拥塞,在美国多个地区运行服务的 Google Cloud 项目的丢包率不断升高。在分析中断情况后,他们报告:“在中断发生两分钟后,Google 工程师就接收到故障警报,并迅速根据应对最严重生产事故的事故管理协议采取措施。

由于使用工具时需要争用原本已拥堵的网络带宽,调试问题的过程变得异常艰难。”他们意识到遇到了大麻烦,但是缺乏解决该问题的辅助方法。

造成中断的最常见原因之一是主要网络最后一英里的漏洞。尽管 ISP 连接在过去几年中有所改善,但这些服务无法克服的一个弱点是最后一英里问题。这指的是生产网络的最后一部分,它将您的网络连接到 ISP。这是连接中最薄弱的环节。

单个办公室、商店、分支机构或分发中心的所有网络流量都通过单个链路进行分配。这些链路的带宽实实在在地限制了可传输到您的 ISP 的数据量。这种瓶颈使您容易遭受 DDoS 攻击并且易出现低级人为错误,最终导致中断。最后一英里可能会成为物理故障的受害者。意外光纤切断可能会摧毁您的整个网络,并使您在相当长的一段时间内无法连接到 Internet 服务。

### 带内和带外管理

贵公司拥有用于传输网络流量(包括 VPN、Web、电子邮件、云应用程序等)的生产 ISP 连接。通常,只有一个主要网络管道(T1、有线电视网络、SD-WAN 或 MPLS)将这种流量路由到 Internet。管理信息采用与用户数据相同的接口传输。如果管理信息和数据共用同一层面,您最终将使用数据层面访问网络设备。这称为带内管理。如果使用带内网络来管理设备,数据和控制命令将通过相同的网络路由传输,因此管理层面与数据层面面临着同样的安全漏洞。您可能会发现自己由于网络中断而无法访问管理层面。

---

“您能够连接到所需的设备;能够进行管理,无论您是否通过常规方式进行连接。因此,4G、无线连接,各种连接方式都可以。”

**Steve DiCicco**  
高级网络工程师

---

带内管理的优点是便宜而且简单, 因为您只需要一个网络。但是它也不太安全, 因为您将用户流量与通常不太严格的访问规则和管理流量混合在一起。中断和攻击不仅可能会危害用户数据, 还可能会损害网络设备的管理和完整性。此外, 如果发生网络中断, 您将无法与设备进行通信。

另外一种方法是, 您可以通过仅处理管理流量的独立网络来运行管理流量。这是带外管理 (OOB)。OOB 提供了一种替代方法, 您可以独立于公司使用的主要 ISP 连接, 通过管理层面连接到远程设备 (例如路由器、交换机和服务器), 而不是直接在数据层面中访问设备的生产 IP 地址。带外路径与生产网络完全分离, 这样管理员能够安全地监控、访问和管理所有设备而不会干扰正常操作, 更重要的是, 不允许在数据层面级别访问管理层面。

由于带外网络将用户流量与管理流量分离, 因此您可以锁定、限制访问并全面保护管理层面。此外, 即使数据层面处于关闭状态, 您也可以对设备进行配置、管理和故障排除。OOB 解决方案通常通过 4G LTE 提供辅助连接, 使得网络技术人员能够在任何地方解决问题, 最重要的是, 可以为公司节省时间和金钱。

带外管理的缺点是需要为管理工作设置单独的网络, 这会产生额外的费用, 但是正如本文后面介绍的那样, ROI 很快就会抵消这项费用。

## 从三个层面, 轻松化解单个层面难解之题

将网络想象为三个层面<sup>1</sup>:

**数据层面**由承载用户数据的基础设施组件构成。举例而言, 其目的是允许数据在 Web 服务器与客户计算机之间流动。

**控制层面**负责保持数据流动。该层面包含允许将信息从一个地方路由到另一个地方的规则。例如, 网络路由器可在其中找到一条路径, 将数据从 Web 服务器传送到客户计算机。

**管理层面**用于配置和管理网络交换机和路由器。

在许多配置中, 管理层面与数据层面结合在一起, 如果数据层面出现问题, 这样做就可能会产生问题。

<sup>1</sup> [了解有关各个网络层面的更多信息。](#)

## 为什么需要 OOB?

您是否真的需要增加成本和复杂性来作为连接到设备的辅助方法?

是的, 您需要。即使会产生额外的成本, 也有多个理由选择 OOB。

首先, 提高安全性。如果不使用带外管理, 控制台端口将连接到带内生产网络, 因此, 如果病毒、机器人程序或黑客入侵您的网络, 那么整个网络都将受到威胁。

---

*“我们在使用交换机堆栈, 但是升级失败, 因此我们无法再使用堆栈了。实际上, 我们无需开车抵达办公室然后通过控制台端口进行连接, 而可以使用 Opengear 通过蜂窝模块进行连接, 并在 10 分钟内恢复正常运行。它为我们节省了大量时间, 过程也不那么艰难。”*

**Evans Vogas**  
网络运营分析师

---

其次,您将能够承受 ISP 中断并保持组织正常运转。您的主要 Internet 连接受“最后一英里”漏洞的影响。简单至铲子这样的工具就可能切断您的线路,此时您的主要连接(无论是光纤、电缆还是其他任何方式)将无法使用。借助高级 OOB 控制台,几乎可以立即远程管理网络中断。

对于拥有远程办公室的公司来说,采用带外管理是毋庸置疑的。无需将网络技术人员派遣到现场,即可通过集中的管理系统随时随地对设备进行故障排除和管理。

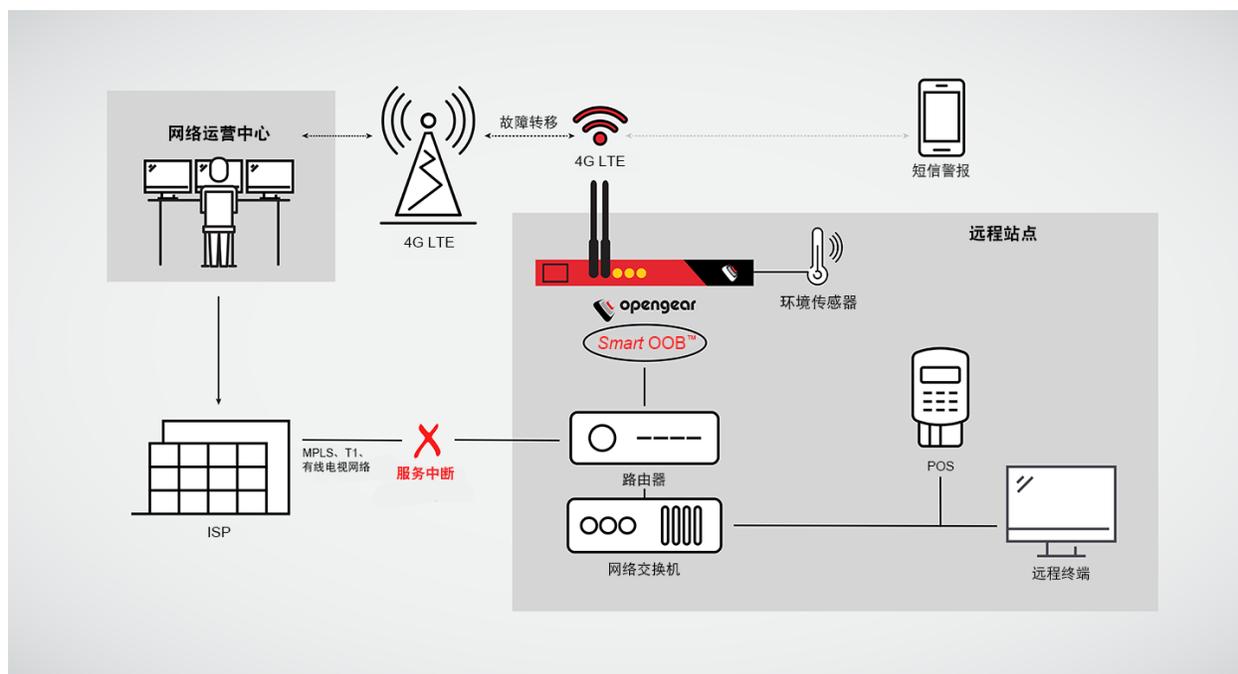
请记住,用于执行管理任务的 LTE 带宽非常小。基本上,网络技术人员通过终端发送文本命令,并获取从这些命令返回的信息。或者,他们或许能够使用集中管理软件,这种软件在后台仍不会占用过多带宽,从而使 LTE 费用保持在较低水平。

最终,这些优势将为您节省大量资金,远远超出对 OOB 所做的投资。

## 当今的高级带外管理控制台

带外管理控制台提供的功能可最大限度地减少停机时间并显著降低运营成本:

- 独立于带内网络运行,这种链路多样性可以实现真正的网络弹性。
- 自动蜂窝网故障转移。如果主要链路变得不可用,将通过远程 LAN 和设备 4G LTE 网络提供 Internet 连接。
- 提供零接触配置 (ZTP)。通过 ZTP,管理员可以自动执行部署过程。反过来,您可以自动执行重复任务,减少人工接触点,减少错误并将部署过程扩展到任何规模。
- 通过电子邮件或短信发送自动警报,以通知任何网络问题。
- 识别温度条件、柜门位置和 network 可用性方面的任何不符情况或异常活动。
- 允许远程恢复网络并运行,而无需从统一管理界面进行现场访问。



---

“您应该能够在中断后恢复正常运行。这就是我们设计站点的方式,让任何人都可以进入并重新启动。Opengear 拯救了我们很多很多次。”

**Landon Orr**

生产网络工程师

---

## OOB 投资回报

OOB 控制台可以通过降低运营成本和潜在的灾难性停机时间损失来快速收回成本。在运营成本方面,请考虑单个边缘站点的成本降低。

上门服务的费用大概为 500 美元。高级 OOB 控制台的费用大概为 1500 美元。只要网络发生 3 次中断,就已达到 OOB 成本。如果是乘坐飞机去解决问题,费用可能会更高,只要发生一次事故,就足以抵消成本。这还只是一个边缘站点的情况。

运营损失也会降低,原因是[根据 Gartner 的数据,停机一分钟的平均成本为 5,600 美元](#)。考虑包含 10 个物理站点的网络。

为网络配备一个典型的带外管理部署(具有 10 个站点)和一个集中管理系统,目前的成本大约是 2.5 万美元。平均而言,只要停机五分钟就能够抵消成本。

## 结论

带外管理无需上门服务,网络工程师也不需要访问数据中心、分支机构、信息亭、遍布各地的办公室或 POS 零售地点。您可以远程上载配置和 OS 映像,简化备份和还原功能,重启路由器以重置设备,并减少中断修复时间。OOB

可以为贵公司节省大量时间并提高生产率。对客户来说,带外管理可能意味着平稳运行和灾难性故障之间的区别。如果客户无法访问您的业务,则会带来基本的信任和忠诚度危机,从而导致较高的客户流失率。