Dante®

使用 SaaS 工具和 Dante Director 保护 Dante 网络

在过去几十年中，许多人都在将传统的 AV 网络从模拟网络转向 AV-over-IP 网络。这种转变的好处非常广泛，包括提高信号路由的灵活性，方便多个制造商技术的互操作使用，以及显著减少完成任何任务所需的布线量。所有这一切都得益于内置在数百家制造商的数千台设备中的 Dante 技术。

由于所有这些设备现在都已完全联网，因此我们曾经认为只与计算机和其他终端相关的风险，现在也适用于我们的 AV 设备。作为 IT 和 AV 专业厂商，我们担心潜在的黑客攻击、未经授权的访问，甚至善意用户可能造成的负面影响。

现在常用的 AV-over-IP 安全的方法是将 AV 设备隔离在一个独立的网络上，而该网络不能访问 AV 网络之外的任何内容。在许多情况下，这意味着对网络进行“物理隔离”，阻止访问任何企业网络甚至互联网。

在本文中，我们将介绍如何通过开放互联网访问以与 Dante Director 等新兴工具配合使用，从而提高 Dante 网络的安全性，为网络可视性和安全性提供新的优势。

物理隔离网络的问题

物理隔离网络是指任何独立运行的网络，不与包括互联网在内的任何外部网络相连接。这一直是保护 AV 网络安全的首选方法，因为它在设计上限制了大多数访问。

创建一个完全隔离的网络（物理隔离）初看起来似乎很容易，但实际上却会阻碍 AV 系统的发展。在许多情况下，它还忽略了可能导致不稳定和其他网络问题的现有问题。

物理隔离网络的第一个问题是，大多数网络并没有真正做到与互联网 100% 隔离。由于设备的数字化特性，大多数设备都需要定期接受固件和软件更新，使其能够正常运行并保持最佳安全性。这些更新可能是为了修复软件错误、提高稳定性，甚至是维护当前的许可证。为了满足这些需求，大多数管理员会插入物理 AV 网络，并使用单独的 WIFI 连接以连接到互联网，因此违背了物理隔离网络的本质。

> 在优先考虑物理隔离媒体流量的同时，往往需要控制和配置信号来弥合物理隔离，使得能够混合使用和控制表面访问设备。

其次，任何 AV-over-IP 网络都依赖于与任何其他网络相同的以太网和交换机类型。如果这些交换机、电缆或网络连接处于开放区域，附近的任何人都可以插入，那么这个物理隔离网络就失去了安全性。此外，根据安装位置类型的不同，有些网络的风险要高得多。例如，大学、音乐院校、技术学院、教会和表演艺术场所。通常，这些机构趋向于培养学生和招募志愿者管理 AV-over-IP 网络。这固然能节省成本，但也是潜在风险的重要来源。只要有一个好奇的学生或好心的志愿者不小心改变了某些参数，就会对整个 AV 网络产生负面影响。在最坏的情况下，机密信息可能会通过错误路由的 AV 信号泄露。

另外一个挑战是，虽然人们倾向于使用物理隔离媒体流量，但往往需要控制和配置信号来弥合物理隔离，以允许混合使用和控制表面访问设备。虽然这方面的问题可以利用 VLAN 解决，但设置起来比较复杂，而且无法提供真正物理隔离系统所需的隔离级别。

最后，当网络被完全隔离时，管理员就不可能对其进行观察、监控和管理。禁止监控设备性能，也就无法进行远程诊断和维修。隔离还会防止创建审计跟踪，这在某些地区可能会导致违规行为。

确保 Dante 网络安全并允许访问互联网

将网络接入互联网是启用 Dante Director 等高级管理工具的必要步骤。如果操作得当，它可能比运行一个非管理型的本地 Dante 网络更安全。

如果你已经将网络接入互联网，无论是使用与其他互联网流量汇聚的网络，还是直接将 Dante 网络本身接入互联网，你还需要完成以下额外的设置，以确保网络安全，防止篡改和信号窃听。

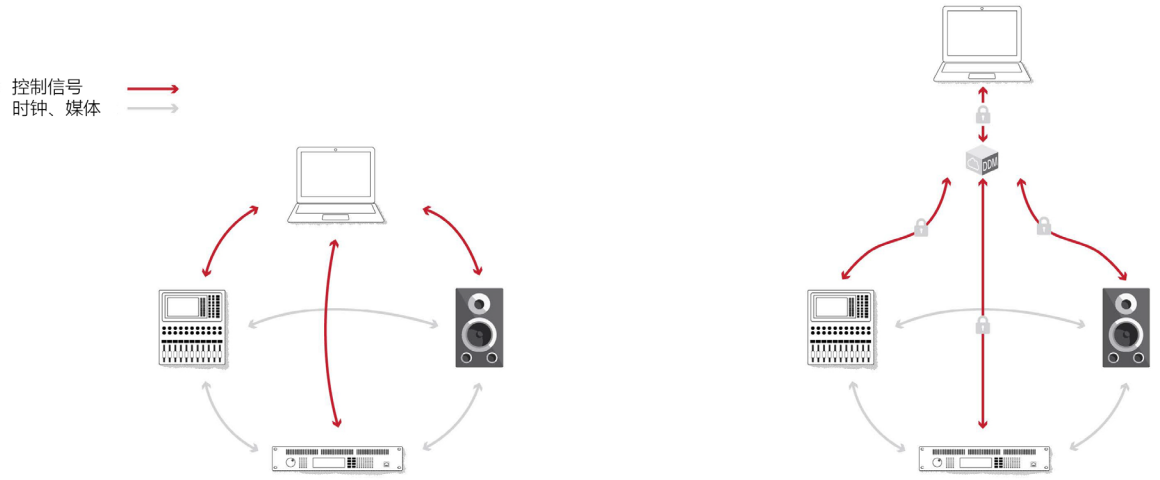
要确保 Dante 网络安全：

1. 通过将设备注册到 Dante 网络管理器（如 Dante Director）中来管理 Dante 网络
2. 打开防火墙和/或交换机中的选定端口
3. 限制已知来源的流量
4. 创建用户账户，并为受信任的用户和管理员提供访问权限

管理 Dante 网络

Dante 网络有两种类型：非管理型和管理型。

Dante 网络的默认配置为非管理型。在这种状态下，设备之间相互发送媒体（音频/视频/时钟）和信号数据。任何人都可以使用 Dante Controller 配置控制数据（信号路由和订阅、采样率设置等）。



非管理型　　管理型

在管理状态下，所有控制数据都通过单独的管理应用程序，如 Dante Director 或 Dante Domain Manager 路由。当 Dante 设备在管理应用程序中注册时，管理应用程序会对设备的所有控制通信进行安全加密，从而增加了额外的安全层。用户由 Director 管理员授予访问权限，并需要通过身份验证才能获得访问权限，媒体通信将按照管理应用程序的定义在设备之间继续流动。

管理 Dante 网络可防止任何无意或恶意的更改。用户对 Dante 网络的所有操作和更改都会被 Dante Director 记录在案，确保能够完全追溯到与发生的任何网络更改相关的特定用户和更改时间。

此外，在任何提供 Dante 网络访问权限的防火墙中，只需打开特定的 URL 和端口。该端口的流量也可限制在一定范围内。这可确保只有有效的控制信号才能按要求进出网络。

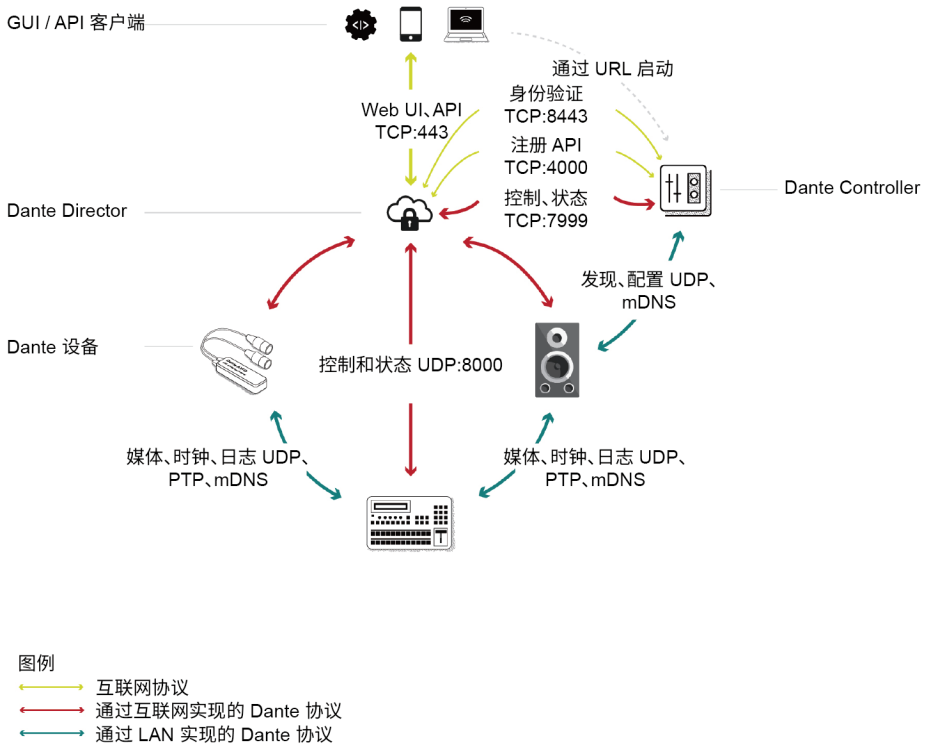
使用 Dante Director 管理网络

对于 Dante Director 的初始设置，在注册设备时，运行 Dante Controller 的计算机需要与 Dante 设备连接到相同的本地网络子网。如果你想限制对设备网络的访问，可以让你的计算机使用另一个网络（公司 WIFI、蜂窝网络等）访问 Director 中的注册设备。只有计算机需要这种直接访问，而且只有在设备注册时才需要。所有设置后的访问都可以通过互联网完成。

要将 Dante 设备注册到 Dante Director：

1. 将所有 Dante 设备连接至 AV 交换机
2. 将装有 Dante Controller 的计算机插入与 Dante 设备相同的子网中
3. 确保你的计算机可以通过端口 8443、4000 和 7999 访问 Dante Director
4. 将设备注册到 Dante Director
5. 确保在连接 Dante 网络和互联网的防火墙中打开端口 8000
6. 现在可以安全地将计算机从子网中拔出，然后就能够在任何互联网连接上使用 Dante Director 管理 Dante 网络。

场景：使用 Dante Controller 注册设备



打开防火墙中的端口

在向互联网开放物理隔离 AV 网络时，必须确保方法符合组织的安全需求。

无论是使用硬件或软件防火墙，还是在网络交换机层面进行端口过滤，第一步都必须是了解必要的端口。包括 Dante Director 在内的大多数 SaaS 应用程序都会在其产品文档、接线图和其他支持库中包含必要的信息。

以下是 Dante Director 和相关应用程序使用的端口列表。这些端口也可以在本文件的图表中找到。

注册设备后，Dante Director 唯一绝对需要的端口是端口 8000。如果你打算使用 Dante Controller 添加新设备并访问其他资源，则需要打开下面列出的其他端口。

Dante Director GUI 和 API 使用的端口和 URL		
地址	端口	用途
director.dante.cloud	TCP 443	网络用户界面
api.director.dante.cloud	TCP 443	外部 GraphQL API 客户端
在 Dante Director 中注册的设备使用的端口和 URL		
device.director.dante.cloud IP：15.197.156.165 或 3.33.153.19	UDP 8000	与 Dante Director 通信的设备
与 Dante Director 搭配使用时，Dante Controller 使用的端口和 URL		
device.director.dante.cloud	TCP 8443	Dante Controller 对 Dante Director 的身份验证
device.director.dante.cloud	TCP 7999	与 Dante Director 通信的 Dante Controller
api.director.dante.cloud	TCP 4000	Dante Controller API 访问 Dante Director
其他资源使用的端口和 URL		
www.audinate.com	TCP 443	常见问题解答
my.audinate.com	TCP 443	下载 Dante Controller
dev.audinate.com	TCP 443	用户指南
audinate.onfastspring.com	TCP 443	账户订阅

设备安全和控制数据

Dante 的设计以安全性为核心。最新的 Dante 硬件设备具有 Dante Updater 提供的安全启动和安全固件更新功能。在 Dante 设备之间传输以及传输到 Dante Director 的控制数据在传输过程中会被加密。这可确保控制数据在传输过程中不会被拦截、欺骗或篡改，从而保证网络配置的完整性，并防止媒体被重定向到或来自非预期端点。

根据来源限制流量

通过只打开防火墙中的特定端口，你已经将访问权限限制在了可以严密监控的特定区域。为了增加额外的安全层，你可能希望限制流量只能用于已知来源。

例如，如果使用 Dante Director，在注册所有设备后，可以限制端口 8000 的流量，只允许 Dante Director 与 Dante 网络通信。

要将流量限制在 Dante Director，请将 https://director.dante.cloud/ 设置为端口 8000 上所有流量的来源。

请记住，如果你需要在插入 Dante 网络时注册更多设备，则需要为 Dante Controller 与 Dante Director 的出站通信打开更多端口。Dante Director 和 Dante Controller 的所有远程访问都通过 8000 端口进行，但插入网络时的出站通信则需要通过上图中列出的其他端口进行。

启用用户访问控制

Dante Director 可限制只有经过批准的用户才能访问并管理 AV 网络。具体做法是在 Dante Director 中创建用户账户，然后只对必要的网站授予受限访问权限。

看似微小的改变却能带来巨大的收益。传统上，AV 网络信号路由、监控和控制都是通过 Dante Controller 等应用程序提供的。由于这是一款免费应用程序，因此任何人都可以下载并使用它来修改 Dante 网络。Dante Controller 的即插即用特性为许多新的 AV-over-IP 用户提供了使用方便，但是，对于不断发展的系统来说，不受限制的访问很快就会成为潜在的安全噩梦。

通过启用用户访问控制，Dante Controller 等工具现在需要登录才能访问或修改任何信号路由。用户无法访问的任何网络和设备现在都不可用，并保持当前状态，直到授权用户登录进行更改。

用户受到限制，并且只能管理由管理员授予的特定站点。这样，团队成员就可以被分配到特定的管理区域，防止无意中更改网络。

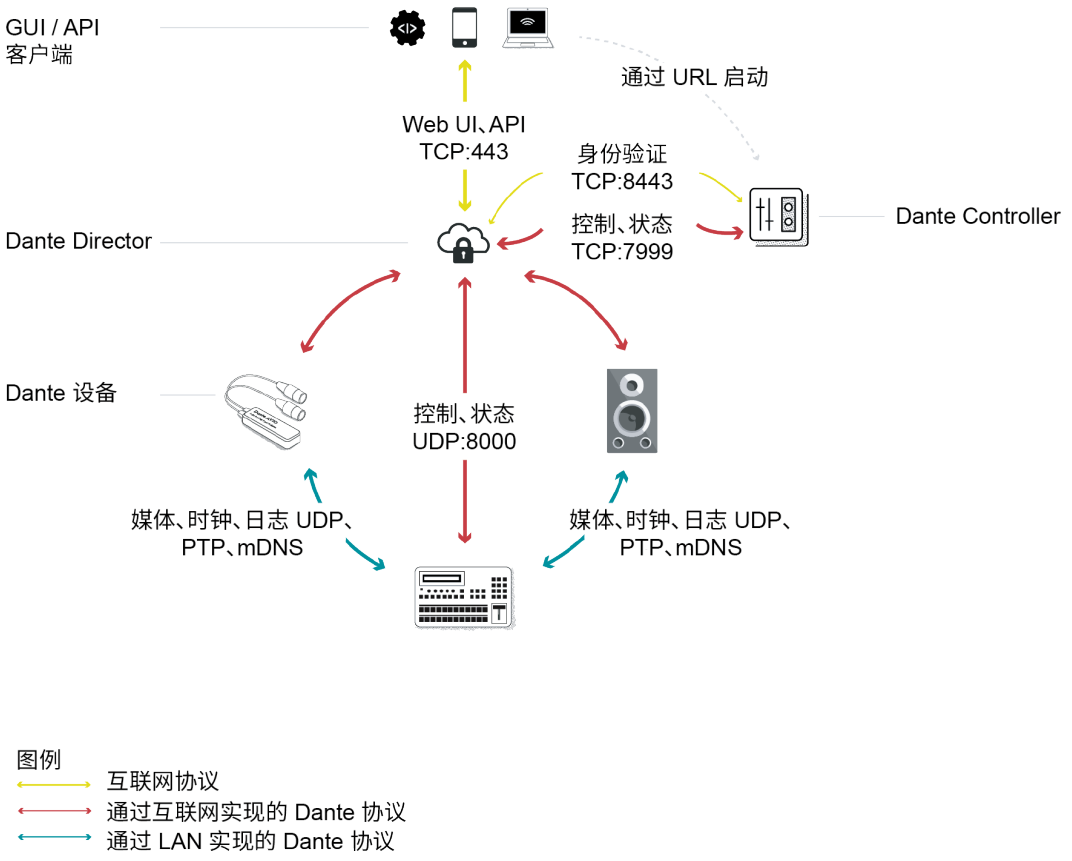
Dante Director 可限制只有经过批准的用户才能访问并管理 AV 网络。

注册设备后使用 Dante Director 管理 Dante 网络

将 Dante 网络中的设备注册到 Dante Director 后，设备访问互联网只需要一个端口，即端口 8000。使用 Dante Director 控制网络的所有流量都将通过该端口路由。这包括在远程计算机上使用 Dante Controller 进行的任何管理。远程计算机需要访问其他几个端口才能访问 Dante Director 本身，但所有这些都将通过 Director 的 8000 端口传递给设备。

如上所述，如果需要直接插入本地子网，Dante Controller 和其他应用程序将需要额外的端口进行出站通信。当然，这一切都取决于你的安全态势，并且可以在防火墙或交换机级别进行管理。

与 Dante Controller 配对的 Dante Director 的标准使用方法



使用 SaaS 产品的优势

像 Dante Director 这样的软件即服务 (SaaS) 产品是 AV 行业的下一个发展方向。与传统的软件部署模式相比，使用 SaaS 产品有许多好处。

这些好处包括：

- 快速设置和配置服务，无需在使用应用程序前启动自己的服务器、容器或管理程序。
- 与传统软件发布周期过长相比，可以更快地推出和采用定期功能改进。
- 对云应用程序进行频繁的质量控制更新。
- 具有关注软件安全性和合规性的责任分担模式，即软件供应商负责应用程序的安全性，你只需解决本地问题。
- 摆脱昂贵的定期硬件更新周期，以及对可能无法直接支持项目最终目标的硬件的持续维护。

总结

Dante Director 和其他 SaaS 工具可为 AV 网络的管理、监控和维护带来诸多好处。只要稍加规划，你的网络就能比以往更加安全和易于管理。如需了解更多信息，请参阅以下在线资源。

- Dante Director 常见问题解答 - 常见问题快速解答
- Dante 专业服务 - 需要更多帮助？与 Audinate 签订合同，获得定制培训和专家建议。
- Dante Managed API - 通过定制集成扩展你的 Dante 网络
- Dante Director 支持 - 联系我们并提交支持请求