

DANTE 认证项目

第3级 – 高级 DANTE 联网

高级

DANTE 联网

DANTE 认证项目

第3 级

DANTE 认证项目

Audinate 培训项目

•
获得官方认证可以使客户相信您具备实施 Dante 网络所需的专业知识和技能

•
确保获得一套一致的的方法和知识



© Audinate Pty Ltd. All rights reserved

<http://www.audinate.com/resources>

- Dante 认证项目是由 Audinate 提供的一个培训项目。
- 获得官方认证可以使客户和同行相信您具备成功设计并推出 Dante 网络所需的专业知识和技能
- 我们通过此次培训提供一套一致的的音频联网方法和知识。随着这项技术的广泛应用并被越来越多的卖家、安装商和客户所采纳，认证的重要性也一定会不断提高。

DANTE 认证项目

获得 **Dante** 认证后，
您将获得：

- 第1级、第2级和第3级“Dante Certified (Dante 认证)”徽标的使用权
- 通过各个等级的认证的证书。



© Audinate Pty Ltd. All rights reserved

<http://www.audinate.com/resources>

获得 Dante 认证后，您可以使用自己的已通过等级的“Dante Certified (Dante 认证)”徽标。

DANTE 认证项目

第1级：Dante 简介

- 100% 在线授课
- 背景知识
- 基础信号路径布线
- 在简单系统（约 6 个设备 · 1 台交换机）中设置 Dante



© Audinate Pty Ltd. All rights reserved

<http://www.audinate.com/resources>

- 第1级 DANTE 认证项目在线授课
- 该项目提供关于数字音频概念的背景知识
- 项目涵盖基本的自动化和 Dante 中的信号路径布线
- 第1级认证可以提供成功使用小型 Dante 网络（通常具有 6 个左右设备和 1 台网络交换机）所需的一切知识。

DANTE 认证项目

第2级：中级

Dante 概念

- 可现场和在线完成
- 大型系统（约 12 个设备）
- 时钟选项
- 了解单播和组播
- 延时
- 冗余
- Dante Virtual Soundcard 和 Dante Via



© Audinate Pty Ltd. All rights reserved

<http://www.audinate.com/resources>

- 第2级 DANTE 认证项目面向运行较大型系统且经验更为丰富的用户
- 本项目会详细介绍 Dante 时钟选项
- 其中会简要介绍单播和组播网络流量以及如何通过 Dante 使用这两种模式
- 项目会介绍 Dante 延时的调节和监控
- 项目会介绍冗余 Dante 网络
- 同时还会介绍 Dante 软件，例如 Dante Virtual Soundcard 和 Dante Via。

DANTE 认证项目

所需步骤：

- 第1级：通过第1级在线考试
- 第2级：通过2级在线考试以及现场或在线技能考核



© Audinate Pty Ltd. All rights reserved

<http://www.audinate.com/resources>

理解可扩展的 DANTE 网络

Dante 主题

- 兴趣点
 - Audinate 是哪家公司
 - 为什么要使用 Dante
 - Dante 在哪里使用
 - 什么是 Dante
 - 如何使用 Dante
- 建构原则
- 评估和优化网络组件
- 故障排除
- 在统合式网路中使用 Dante



常规知识联网

- 兴趣点
 - 为什么要使用网络服务
 - 什么是网络
 - 网络在哪里使用
 - 如何理解网络
- 建构原则
- 了解网络组件功能
- 涵盖在网络课程和基本信息中



© Audinate Pty Ltd. All rights reserved

<http://www.audinate.com/resources>

Dante第3级培训模块重点是在大型网络中运行 Dante。

首先必须将“Dante”这个在商用成品 (COTS) 网络上运行的服务与网络本身区分开

基本知识联网跟踪是 Audinate 提供的通用信息和指导，而由硬件供应商（Cisco HP Juniper 等）提供的培训对于相应的制造商产品线来说更加全面和实用，也更有针对性

第3级培训课程提供的工具能帮助您做出这样的区分

关于 **AUDINATE**



总部位于澳大利亚
悉尼市



最初由网络工程师
创立

Dante™

将 Dante 开发为
的 **100%互操作**
性解决方案

面向所有音响厂商



© Audinate Pty Ltd. All rights reserved

<http://www.audinate.com/resources>

9

首先，简单介绍 Audinate。

- 我们的总部位于澳大利亚悉尼市。
- Audinate 最初由网络工程师创立并且聘请了很多网络工程师，因此，我们对联网和网络标准如何工作以及如何获得最佳的音响性能有深刻认识。
- 我们将 Dante 开发为面向所有音响厂商的 100% 互操作的解决方案。在这一方面，我们是独一无二的。我们将这项技术提供给所有人，确保使用 Dante 的所有产品都可以自由互连，不会产生任何问题。

业务范围

Dante 技术

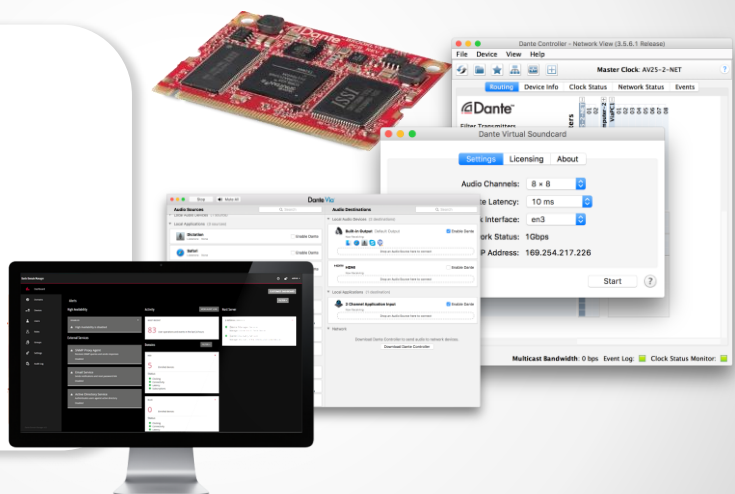
(包括所有相关产品)

硬件模块

开发工具

软件产品：

- Dante Controller
- Dante Virtual Soundcard
- Dante Via
- Dante Domain Manager



© Audinate Pty Ltd. All rights reserved

<http://www.audinate.com/resources>

10

我们的产品是什么？

我们是 Dante 音频联网技术的唯一创造者和开发者。我们生产所有相关产品，包括：

- 硬件模块和芯片组，这些产品销售给厂商，以快速容易地将 Dante 整合到他们各自的产品中。
- 为厂商提供的开发工具，因而厂商们可以对 Dante 进行定制，以满足他们的需求和设计要求。
- 软件产品，专业音响工作人员可以利用这些软件使用 Dante；
- Dante Controller，这是管理 Dante 网络的必备工具
- Dante Virtual Soundcard，您可以通过这款软件直接在 Dante 网络上使用任何您希望使用的 Digital Audio Workstation 软件；和
- Dante Via，您可以通过这款软件将连接的音响产品和应用直接连接到 Digital 网络。
- Dante Domain Manager，全面的 Dante 网络管理系统。

为什么要使用 DANTE？



11

为什么要使用 Dante？为什么我们想要更熟悉 IP 网络？为什么不使用 MAD1 等现有的多声道标准？这是因为 IP 网络提供了许多优点，它们不仅适用于电脑，还适用于所有设备。

如果您曾阅读过有关联网的任何技术文档、书籍或参加过任何相关课程，您很快就会意识到需要学习很多技术术语。如果您想成为一名 IT 管理员，那么就需要记忆很多首字母缩略词和缩写。作为 IT 管理员，您肩负着巨大的压力，因为您所服务的公司或机构完完全全依赖于网络运作。如果网络出现故障，公司的盈利就会停止，而且会开始亏损！

作为音频专业人员，我们始终都是尽力而为，但是到头来，我们还是希望从系统里把声音弄出来。而不管信不信，IT 管理员们实际上也都希望 IT 系统能够发挥作用。

因此，我们首先要了解的是 IP 网络实际运作的基础，这样我们就可以对 IT 管理员的用语有初步的认识。我们将打破一些迷思，看看我们怎样理解一些流行的术语，这样就不会被 IT 部门弄得团团转。

在这之后是关于 Dante 内部底层服务功能的更具体的内容。

然后则是 Dante 一些常见问题的解答

为什么使用 **DANTE** ?

网络是一组相互连接的事物

•
关键是互操作性

•
市场上有 1400 多款 Dante 产品

•
超过 350 家 OEM 制造商

•
超过 100 万台支持 Dante 的终端已经发货



© Audinate Pty Ltd. All rights reserved

<http://www.audinate.com/resources>

网络是一组相互连接的事物

- 要连接和组建网络，其中的关键是互操作性
- 有超过 1000 台支持 Dante 的产品（并不断增长）
- 迄今为止，已有 350 多家 OEM 制造商采用 Dante（并不断增长）
- 超过 100 万台支持 Dante 的端点已经发货

为什么使用 DANTE？

如果产品上有 Dante 标志，它就能连接到其他任何带有 Dante 标志的设备

Dante 是高度商业成熟并得到广泛支持的解决方案 – 而且改进和功能还在不断增加

最广泛采用的音频网络解决方案



© Audinate Pty Ltd. All rights reserved

<http://www.audinate.com/resources>

- Dante 就是 Dante – 如果产品上有 Dante 标志，它就能连接到其他任何带有 Dante 标志的设备 – 没有如果，也没有但是
- Dante 是高度商业成熟并得到广泛支持的解决方案 – 而且改进和功能还在不断增加（使用者超过 100 万，存在维护互操作性的既得利益）
- Dante 是有史以来最被广泛采用的音频网络解决方案
- 在联网方面 – 最大的就是最好的

DANTE 在哪里使用？



14

使用 Dante 的各种应用程序概述。

现场音乐

美国航空中心 - 佛罗里达州迈阿密



商业安装

切萨皮克球馆- 美国俄克拉荷马州俄克拉荷马市





广播

维多利亚州国会大厦- 澳大利亚墨尔本

17

教育

总督州立大学 - 伊利诺斯州大学园



礼拜堂

柳溪社区教会- 伊利诺斯州南巴灵顿







后期制作

GOLDCREST 电影 - 英国伦敦



录音

SYNCHRON STAGE- 奥地利维也纳

什么是 **DANTE?**

什么是 DANTE？

- **Dante** 是一种联网技术
 - 提供给 OEM 制造商的硬件解决方案
 - 软件解决方案 – DVS、Dante VIA、Dante Controller、DDM
- **Dante** 技术提供：
 - IP 网络中每个端点紧密同步（优于 1 μ s）的媒体播放
 - 在所有专业采样率下的未压缩数字音频
 - 在局域网及路由 IP 网络上可实现简单即插即用发现和路由
- **Dante** 可以配置在商用成品 (COTS) 的网络基础架构上



© Audinate Pty Ltd. All rights reserved

<http://www.audinate.com/resources>

Dante 是一种运行于以下设备的网络技术：

- 提供给 OEM 制造商的硬件解决方案
- 软件解决方案 – DVS、Dante VIA、DDM

Dante 技术提供

- IP 网络中每个端点紧密同步（优于 1 μ s）的媒体传送
- 在所有专业采样率下的未压缩数字音频
- 在局域网及路由 IP 网络上可实现简单即插即用发现和路由

Dante 可以配置在商用成品 (COTS) 的网络基础架构上 – 不需要特殊的基础架构硬件

高级 DANTE 联网：第 1 节

在本节中...

联网

- 什么是网络？
- 比较连接音频设备的各种方法：
 - TDM 联网技术（以时间为中心）
 - 分组交换（以地址为中心）联网技术



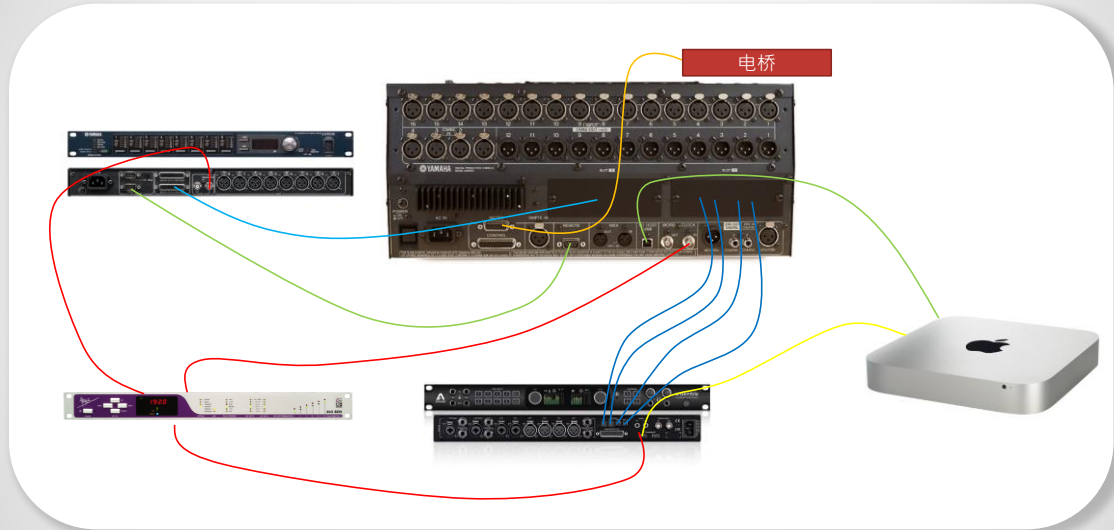
在本节《什么是网络》中，我们一起来了解如何将音频设备连接到网络上。

我们将回顾和比较一些历史，以便了解为什么这项技术在行业中占据主导地位

。

我们将回顾 TDM 网络，这是一种在网络中传输数据和音频的较老的方式，然后看看我们后来为什么改用了分组交换模式。

连接“老式”数字音频系统



Dante
by audinate

© Audinate Pty Ltd. All rights reserved

<http://www.audinate.com/resources>

27

每个人都可能建立过这样的系统

我们有：

数字音频和控件从舞台音箱连接到调音台，

然后从调音台连接到电脑的音频接口

全部与外部字时钟保持同步

当然，每个模块都需要单独的独立线缆。

从人理解的角度来看 – 每个模块各自分配一根线缆可能会让您感到舒适。

但对于 Dante 网络，我们需要做的仅仅是...

使用 DANTE



Dante
by audinate

© Audinate Pty Ltd. All rights reserved

<http://www.audinate.com/resources>

28

...这样。前一张幻灯片上的所有模块现在全部连到同一根线缆上。

连接要求

“旧式”数字系统

- 1 根 9 针串行 (HA 控制)
- 1 根 专用的电桥线缆
- 3 根 75 欧姆 BNC 线缆 (字时钟)
- 1 根 25 针 D-SUB M-M (AES)
- 1 根 USB 线缆
- 1 根 Thunderbolt 线缆
- 4 根 TOS-LINK 线缆



“使用 DANTE”

- 4 根 Cat5e 线缆



© Audinate Pty Ltd. All rights reserved

<http://www.audinate.com/resources>

29

因此，当我们比较两种系统的接线时，可以看到使用 Dante 的优势，我们只需要四根 CAT-5e 线缆就可以将系统连接在一起。

但是这些布线示例跟 IP 网络的主题有什么关系呢？

这个例子恰恰很好地说明了为什么它跟 IP 网络有着精准的对应关系。

我们都已经习惯了用我们的笔记本电脑运行电子邮件、一次浏览多个网页、畅享流媒体音乐、观看 Netflix 电视剧、不断刷新 Facebook...这些操作都是同一时间进行的。

我们实际上是在一个平台上同时运行大量不同的应用程序。在这个例子里面，这个平台正好是一台电脑。但这跟我们在 Dante 网络上所做的完全一样 - 在一个平台上同时运行大量不同的功能模块。

网络是什么意思？

- Dante 网络是**通过 IP 连接的一组设备集合**，设备之间可以相互交换音频信息。
- Dante 能做到的比这还要多：
 - 为达到现代网络的易用性，设备均可自动发现
 - 设备使用的是让人容易理解的名称 – 包括设备及其通道标签
 - 设备可提供诊断信息给控制器应用程序
 - 设备和通道可以由系统管理员管理，并且可以建立安全的生态系统
- Dante 设备通过 IP（**互联网协议网络**）交换信息
 - 在其他一切生活领域，“网络”一词已经成为 IP 网络的代名词
 - 世界上最大的网络就是公共互联网 – 当然，这个网络也使用 IP



那么，我们说的网络意思是什么...网络就是一组能够相互通信的设备...对我们来说，Dante 网络是通过 IP 连接的一组设备集合，设备相互之间可以交换音频信息

当然，Dante 不仅仅是将音频传递给线路。

- 它允许自动发现设备
- 在 Dante 当中，设备使用的是让人容易理解的名称 – 包括设备及其通道标签（而不是 MAC 地址）
- 设备可提供诊断信息给控制器应用程序
- 设备和通道可以由系统管理员管理，并且可以构建安全的生态系统

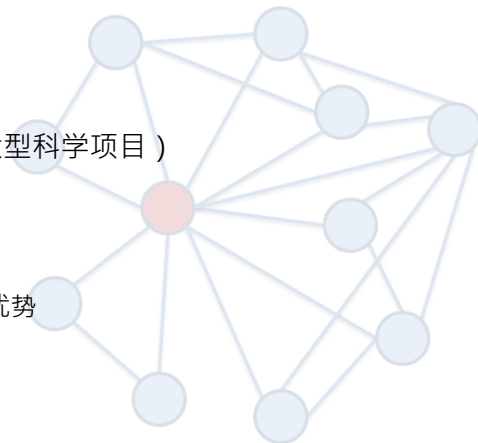
Dante 设备通过 IP 也即互联网协议网络交换信息

今时今日，在其他一切生活领域，“网络”一词已经成为 IP 网络的代名词

世界上最大的网络就是公共互联网 – 当然，这个网络也使用 IP

所以...“联网”是指 IP？

- IP 网络是当今世界上最普遍的网络类型
- IP 为什么成为了主要的联网技术？
 - 大多数制造商支持（无论是软件还是硬件）
 - 已经应用于所有行业（从银行到太空火箭到大型科学项目）
 - IP 非常灵活：
 - 网络是“中性”的
 - IP 网络达到真正的全球规模
 - 设备和布线以前所未有的方式利用“规模经济”的优势
 - IP 遵循的模式比其他方案更具可扩展性
 - 全球数百万工程师和技术人员都能理解
 - 每一天每个小时都有数十亿终端用户使用它



那么，联网是不是指 IP – 诚然，IP 网络是当今世界上最受广泛使用的一个网络但情况并非总是如此，

那么为什么 IP 成为了主要的网络技术呢？

- 大多数制造商支持（无论是软件还是硬件）
- 已经应用于所有行业（从银行到太空火箭到大型科学项目）
- IP 非常灵活，这里的意思是
 - 网络是“中性”的，我们稍后会进一步谈论网络的“中性”，但基本上这里的意思是我们不关心通过 IP 网络发送什么类型的数据，它可以是文档、网页、流媒体音频、电话、视频等
 - IP 网络规模扩展之广，几乎已经达到全球规模
 - 设备和布线以前所未有的方式利用“规模经济”的优势
 - IP 遵循的模式比其他方案更具可扩展性
 - 全球数百万工程师和技术人员都能理解
 - 每一天每个小时都有数十亿终端用户使用它

IP 的替代方案（历史）

- 一开始就需要给每项任务都分配专用线缆
- 线缆是通信系统的重要组成部分
 - “更快”更昂贵的线缆承担“高带宽”任务
 - “更便宜”更普通的线缆承担“低带宽”任务
- 来自模拟线路的逻辑演进
 - 布线变得非常复杂
 - 存在距离的限制
 - 配置时间长
 - 希望减少布线

在 IP 网络真正成为电信行业的关键一环之前，我们采用的是一种叫做时分复用或 TDM 的技术。

TDM 很好，因为用模拟世界来打比方就很容易理解，比如说可以手动用电话线来彼此连接，就像老式电话交换机操作员那样。这也是 AES-3、AES-10 或 MADI，以及 AES-50 使用的方法。

它的工作原理是设备之间的通信在主时钟上运行，然后将该主时钟细分为多个空档。之后将数据放入每个空档。只要发送端将数据放入接收端可以读取的空档中，就可以将数据再次取出。从概念上来说很简单。这就像在旧式的电话交换机中切换线路一样。

重点是，这种模式在点对点系统中运行得非常好，分配均匀。所以如果要运行电话网络的话，这样很好。我可以有一个快速的时钟，并且可以将一定数量的电话线插入这些时间空档里面。这样非常有效。我的电话流量全部都相同、间隔相等，一切都是均一的。TDM 网络后来之所以在电信方面不再那么流行，主要是由于互联网的出现。互联网数据并不是均一的。您编写电子邮件的速度不

可能比网络连接的传输速度更快，除非您运行大量的垃圾电子邮件操作。

所以实际情况是，只有在我发送东西的时候才会出现数据高峰。消息发送完成后，我就不再发送数据了。在 TDM 系统中，我已经预约了时间空档，为该功能预留了带宽，这种情况自始至终不会改变。如果我一直没有使用它，我的效率就会下降。

所以跟我们谈到网络是中性的时候不一样，电信 TDM 系统的主要用途是语音通信。说白了，这个原因是在 70 年代、80 年代和 90 年代早期，这就是您使用电话网络的主要用途。您拿起电话，就是为了打电话和某人交谈。

随着互联网的出现，我们在此之上又有了更加庞大的流量需求。所以人们首先尝试的是将数据流量挤进语音流量里面，但电信主要是语音提供商。拨号服务。你们有多少人还记得这一点？

它跟分组交换网络的区别在于它是面向地址的。如果我们简要回顾一下我们的沟通历史，就会发现声音并不一直是电信网络的主要服务内容。最早服务于消息传递的第一批网络是电报网络。历史上曾经短暂出现过一些有着多达 35 个线对的疯狂系统（用来代表字母表上的每个字母和数字，这个系统在 19 世纪 40 年代之前存在了大约 9 个月），后来有个聪明人出现了：“哦，我们可以用这种叫做摩斯电码的玩意儿，这对人类来说很好理解。”

摩斯电码配置在电报机或电报系统中时，是一种以地址为导向的系统。

也就是说，我击打摩斯键，要表述的第一件事就是“我想把这封电报寄给比尔琼斯，寄到他的家庭住址”。这样骑自行车的人就可以把电报送给正确的人。IP 网络的工作原理跟这个类似。它们都是面向地址的。

那么您是说过去 150 年来，我们从发送电报进化成了现在的发送数据报？

您可以看看所有的论点都在不断绕圈，这其中基本规则仍然适用。

后来电报网络上就出现了这个闯入者。这就是语音。这跟历史上亚历山大·格雷厄姆·贝尔发明电话如出一辙。多年后，语音再次成为数据网络上的闯入者。这听起来也很熟悉。这就是 90 年代发生的 VoIP 事件。大家本来用他们的 IP 网络愉快地共享文件、发送电子邮件，然后有一天突然出现了语音。

所以用于处理网络上语音的方案再次应运而生。

回顾这些事情，并了解过去发生的历史，也就不难预测未来会发生什么了。
拥有一个中性的网络非常棒，因为一切（所有数据）都是一样的。由用户来决定什么是重要的。

IP 的替代方案 (历史)

- IP 网络在电信中普及之前，TDM – 分時多工网络很常见
 - TDM 是旧式数字音频格式使用的方法 (AES3, AES10 (MADI) AES50)
 - TDM 网络在设定好的一个速率下运行 – 它被认为是“同步”网络
 - “时间空档”中或填充了数据，或没有数据，然后只要发送端将“正确的”数据放入“正确的”时间空档中（相对于接收者而言），那么输出的结果数据与输入的数据就能相匹配
 - 网络的容量取决于时钟频率，通过推断也不难理解“时间空档”的数量也取决于它

IP 网络在电信中普及之前，TDM – 分時多工网络很常见

- TDM 是旧式数字音频格式使用的方法 (AES3, AES10 (MADI) AES50)
- TDM 网络在设定好的一个速率下运行 – 它被认为是“同步”网络
- “时间空档”中或填充了数据，或没有数据，然后只要发送端将“正确的”数据放入“正确的”时间空档中（相对于接收者而言），那么输出的结果数据与输入的数据就能相匹配
- 网络的容量取决于时钟频率，通过推断也不难理解“时间空档”的数量也取决于它

IP 的替代方案 (历史)

- TDM 网络不是“中性”的
 - 在电信领域，只要流量是单纯的语音的话，就很简单
 - 一旦电信公司开始提供其他服务，TDM 模式就显现出其效率低下的一面

TDM 网络不是“中性”的

- 在电信业务中，只要流量是单纯语音的话，处理起来很简单
- 一旦电信公司开始提供其他服务，TDM 模式就显现出其效率低下的一面

将这与 TDM 比较

TDM 系统仅在有用容量为 100% 时才有高效率

24 位通道数	“闲置”位 Dante 单播	“闲置”位 64 通道 MADI	100mbps 链路 MADI 上的带宽百分比	100mbps 链接 Dante 上的带宽百分比
1	104	1512	100%	6%
2	80	1488	100%	6%
4	32	1440	100%	6%
64	128	0	100%	88%
65	104	1512*	200%	94%



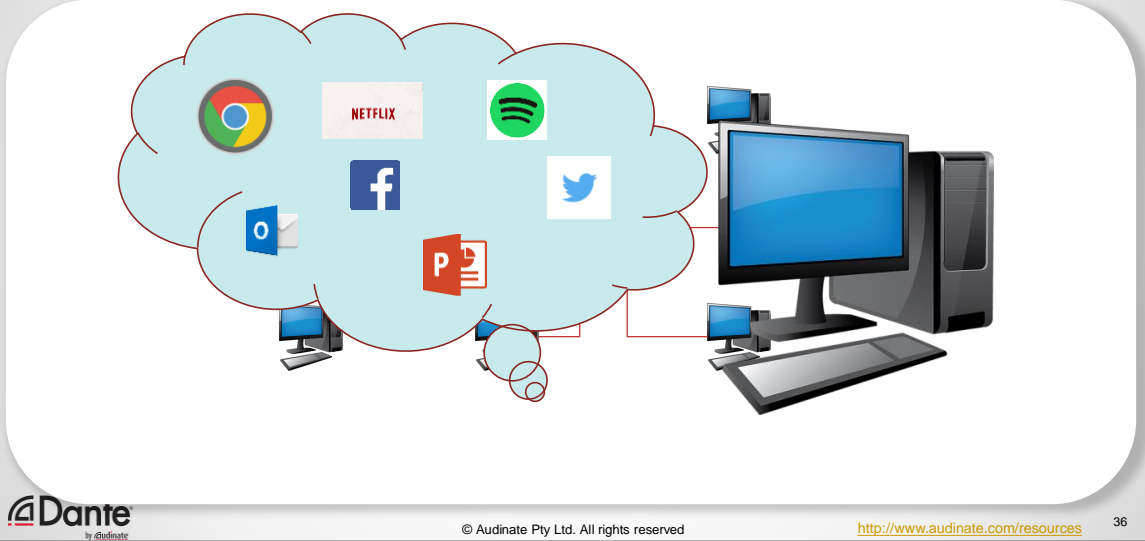
这是 TDM 效率扩展的示例。

如果我始终在使用 TDM 系统上所有的点对点链路，那么这可以说是非常高效的。它会不断前进。

问题是，当我想要比 TDM 再多用一个音频通道时，我必须再增加 100% 来实现这个目标。

而正常数据则存在间歇性高峰。我们运行的服务并不总是使用恒定带宽。所以当您既有周期性又有非周期性流量时，IP 分组交换网络实际上比 TDM 系统更有效率优势。

为什么电脑上使用“封包交换”网络？



这对瑞士国旗来说是一次非常糟糕的尝试，因为毕竟网络是中性的。

那么为什么在电脑上使用分组封包交换网络(packet switched)呢？

我们会在电脑上运行各种应用程序。非常正常，不是吗。我们每天都这样做。

并且这些应用程序中每一个都有一个地址。

某些应用程序可能需要在电脑的处理内部彼此对话，所以它们必须具备地址来进行内部通信。现在有很多应用程序需要通过网络接口(network socket)进行外部对话。

那么让我们通过示例来看看我们如何在不同位置之间建立会话以及如何通过互联网来发现对方。

应用程序地址



我打开谷歌浏览器并决定访问 YouTube.com。可是，电脑并不懂英语，所以：好的，我不知道 YouTube 的 IP 地址，这可能是个问题。要是电话号码簿这样的东西，我就可以查了。幸好真的有。如果我配置过我的电脑，它就会知道域名系统 (DNS)。

所以 Google 的 DNS，就像谷歌的大电话本一样，是 8.8.8.8。那么，让我们打电话给查号服务。

我们上到公共互联网，找到 Google DNS。对话如下：嗨，我正在寻找一个名为 YouTube.com 的 IP 地址，您知道吗？它说知道，地址是这个。它把它发送回电脑。

电脑将缓存（或存储）这些信息，因为有很高的几率我们下次还会再观看 YouTube。我不想一直打查号服务。”就像在过去一样，它将它记录下来并存储在某个地方。

所以现在我要打电话给 YouTube。我需要组织一下语言。我不希望打个电话过去，听到电话响了，却不知道该说什么。那么为了打这个电话，我需要知道些什么？好吧，我的电脑系统内部正在进行大量的工作。我有其他东西连接到其他互联网服务。所以它们在电脑里面都有内部地址。我的内部地址就是这个特定的网络浏览器。哦，好的。（这是来自一名同事电脑的真实例子）。他的机器

正在使用 TCP 套接字 53618。所以我得到了这个属于当天当时我的网络浏览器所使用的具体地址。而且我也知道我自己的 IP 地址，这非常方便。而且我也知道我想要安全地连接到 YouTube。所以 HTTPS 的标准端口号是 443。那么我就可以继续打电话了。

嗨 (YouTube 的 IP 地址)

这是我 (在我的 IP 地址)，您能给我的 TCP 端口 53618 回个电话吗？

那么这个消息就发出去了。它抵达了 YouTube。YouTube 会说：嗨，并发回一条回应消息：我能为您做什么？那很好，因为我们都知道我们为什么要使用 YouTube，不是吗？

猫的视频。

这只是 DNS。这是一个简单的发现过程，我们在 Dante 内部就使用这套理念来发现设备。

现在我们不需要在本地子网中使用静态服务器来实现这一点。

我们使用一种称为组播 DNS 的组件，它现在允许多个服务器接听和聆听人们说“嗨”的信息。

这是发现的基础。我们大家都有输入网址或其他东西的经验，这件神奇的事情在后台进行，而我则是顺利在电脑上播放了猫的视频。

这真的很简单，这只是使用电话簿的外推罢了。

应用程序地址

- 每个应用程序都重复相同的过程
- 每个应用程序都有其独特的内部（端口）地址
- 在音频设备中，这可能是：

应用程序	本地端口	远程 IP	远程端口
PTP	UDP	224.0.1.129	UDP 319
音频流	UDP 14340	192.168.1.56	UDP 14390
音频流	UDP 14350	192.168.1.60	UDP 14367
增益控制	UDP 50135	192.168.1.56	UDP 50231



举个例子，我们有 YouTube、Facebook、Outlook、Spotify.....他们都有本地的 TCP 端口地址，这就是它们要使用的远程地址。

因为这些通常都是 HTTPS 服务，所以远程套接字是 443，除了 Outlook 会使用 389（这是 Exchange 服务器的标准套接字）。

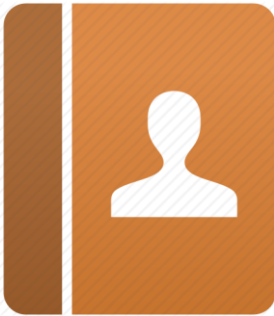
理解这一点的最佳思路是：每个人都在使用多芯线缆，里面很多对芯。一般来说，您可以使用数字来标识线缆中的线对。这就是这些套接字地址。

它实际上就像一个跳板一样。只不过在基于 IP 的系统中，我们每个传输协议有 16 位地址容量。这对于 TCP 来说有 16,535 个不同地址，UDP 也一样多的数量。

。

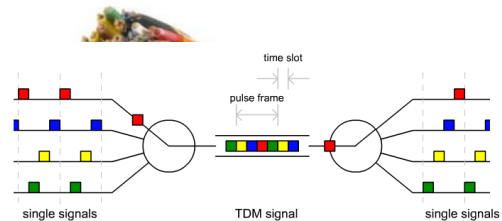
所以，这就像是我从我的电脑里拿出了这条巨大的多芯线缆，然后我可以将应用程序放到线缆的末端。这真的很简单。这就是音频视频人员能担当非常好的网络工程师的原因。您只不过还不知道而已。

我们怎么把它放在一起...
但让其保持彼此独立？



IP 网络地址簿

和



专用“线缆”



寻址的概念是 IP 网络的关键

这就跟邮件系统一样。我们将大量不同邮件压缩到一起，将它放入一个袋子中，再将它从袋子中取出，然后放到正确的位置。

在模拟系统中，我们使用“专用线缆”，很容易从系统流量本身看到“线对”

在 TDM 系统中，我们使用一种在更高速度的背板中将不同信号进行多路传输的过程，并在另一端进行反多路转换，希望它们在接收器处与在发送器处解释出的时间位置相同。

在 TDM 系统中，流量处于特定的时间空档中（只要每个端点设置正确并且同步...问题就解决了）

在分组交换 IP 网络中，流量具有自己的专用地址
我们用来定义这个过程就称为“封装”

高级 DANTE 联网：第 2 节

在本节中...

网络的分层模型

- 封装
 - 我们如何组织要发送的数据
 - 我们如何建立以地址为中心的线路与应用程序连接
 - 了解网络分层 – 邮政模式



网络的分层模型

封装

- 我们如何组织要发送的数据
- 我们如何建立以地址为中心的线路与应用程序连接
- 了解网络分层 – 邮政模式

分层模式



OSI 模型

- 较旧
- 擅长定义此部分
- 较不相关

TCP/IP 模型

- 较新
- 擅长定义此部分
- 缺乏细节



整个通信概念可以用多种模型来描述。

描述分层模型有两种常见方式：OSI 模型（开放系统互连）和 TCP/IP 模型 (DoD)

OSI:于七十年代初提出。

好处是它是硬件独立的，是一个概念模型。

概念模型跟具体模型相比，好处在于它可以持续很长时间。

擅长定义网络堆叠的较低层。我们如何发出信号，我们如何处理端口寻址，我们如何处理网络地址。

但对于上层而言并不太好。在过去，我们必须在表示层上有一个单独的应用层，而这个层现在已经不再存在了。

在较旧的设备中，必须确保数据的格式对于接收设备是可以理解的，因此有时必须将数据转向等等。

描述它的最好方法是：表示层基本就像是一个“会话层和应用程序之间的联网代理。目前，会话层之间的通信在某些通信模式中非常有用，而在其他通信模式中则不那么重要。

今时今日，传输层已经变得非常复杂。

DoD 模型，对于网络访问有点偏弱。

封装 – “网络堆叠”



- OSI 模型非常庞大，并且包含构建许多不同通信方法的范围
- 在实践层面上，这意味着可用的工具包非常大
- 网络中实际的简化（和准确）模型如下：

我们从一些数据堆叠的顶部开始。这些可能是任何数据。音频样本、视频数据帧、文字处理文档等等。

然后我们把它放在传输层周围。所以我的应用程序连接到一个端口。或者也可以称之为接口。这就是我们用作端口地址的那些地址。这些就像是我们多芯线缆中的一对对线。我们把这些数据放进一个特定的编号端口。

然后我们在它的前端添加一个数据头，说我有我的本地端口，并且我知道我需要将它发送到哪里，因此我将目标端口放在那里，因为接触另一端的将是多芯线缆中的其他线对。而且，出于礼貌，我也把返回地址也就是发出信息的源端口放了进去，所以我可以开始设置某种认证。

然后，这只是前面的一些东西，后面就是数据了。这是我们称之为封装的第一阶段。

然后，我们需要获取端口号，就在那里，并且我们需要获得网络层地址，也就是 OSI 模型的第 3 层。

这就是我们获得 IP 地址的地方。因此，我们的 IP 地址将目标 IP 地址，也就是实际发送数据的设备放进去，我把我的返回 IP 地址放在上面。封装的前端保存着目标端口（它的前往位置）和源端口（它来自哪里）。就像在邮政系统中发送一封信一样。

然后我希望能够处理它经过的设备之间的线路。我们在第 2 层做到这一点。也就是数据链路层。

那么，我们再次构建封装。我有目标 MAC 地址，它是 IP 地址的物理地址。可以有多个 IP 地址位于同一个 MAC 地址。所以这基本上就是我们经历的线路。首先是我的源 MAC 地址，然后是我的目标 IP 地址、我的源 IP 地址、我的目标端口和我的源端口。然后当然是数据。

为什么我们要用两种方法在这里写入一个地址？

因为，当我们建立一个庞大的网络时，我们希望把它细分为多个部分。我们可能在同一局域网中直接连接设备之间的存在线路，但我们不需要将线路地址连接到世界的另一端。这样的扩展效果并不好。

所以我们将 IP 地址放在最上面。那么这个系统中的一台电脑会问：这个 IP 地址是本地的还是远程的？

所以我们产生了子网划分的想法，即通过网关来实现。即使在家里，您也可以使用网关路由器。

基本上电脑知道它属于哪个 IP 子网。如果它要把数据发往一个远程子网，它会知道“啊，这个线路的 MAC 地址是路由器的 MAC 地址，因为我不能直接在本地发送它。将它发送到路由器，然后它在路由器的线路上，通过路由器将其传递。我们用另一张幻灯片来描述这个过程。

封装 - 模拟

IP 堆叠是抽象的



1. 我建立了一些数据（写一封信）
2. 我把信放在信封里（打包）
3. 我在信封上写下地址
4. 在邮局，信封进入邮袋（数据帧(MAC)封装）
5. 邮袋被放在卡车中，并被带到下一个分拣设施（物理层）

IP 堆叠是抽象的。这个模型也有不奏效的时候。没有东西是完美的。

分层模型的思想是，如果您是一名开发人员，您可以专注于一个特定的层面，只需关注从上层获得的数据以及如何将其呈现给下一层就可以了。

这意味着并不了解物理布线的人仍然可以更底层的 IP 堆叠上工作。这是一个非常有效的改进设备的方法。

至于出现问题的时候...您知道我们随时可以获得更新吗？它由许许多多的软件团队完成，团队之间并不知道其他人在做什么。

好，那么让我们回顾一下摘要：

这个跟邮政服务很像

我写了一封信（一些数据）

我把这封信放在一个信封里，并注明“我”是端口地址，“您”是端口地址
我在信封上写了给我的回信地址 – 这是“我”的 IP 地址

我在信封上写下您的收信地址 – 这是“您”的 IP 地址

我把信封交到邮局，他们把它放在一个邮包里 – 国际邮寄地址放在一个袋子里，“本地”邮箱则放在另一个袋子里 – 这就是源 MAC 地址和目标 MAC 地址

装有这封信的信封在系统中被“分类”几次 – 信件不会被打开，源和目标 IP（街道）地址也永远不会改变

信封随着邮包被多次转发（MAC 地址）

邮包可以随火车、飞机、船和面包车旅行 – “物理层”

当最后一个邮包到达目标时，信封将被解包（从数据帧中取出包裹）

信封由街道地址的某个人交给收件人并打开（数据从信息包中删除）

高级 DANTE 联网：第 3 节

在本节中...

不同的通信模式

- 广播
- 单播

它们在何处适用

- 冲突域
- 广播域

路由器和交换机

- 冲突域分段 – 交换
- 广播域分段
- 地址解析协议(ARP)
- VLAN
- IP 子网
- 路由器



我们会介绍网络内部不同的通信模式。

我们会讲到广播和单播，这些非常容易理解。

它们对应的就是冲突域和广播域的概念。

我们会讲到交换机和路由器的作用。它们对网络分段的时候，首先是冲突域，然后才是广播域。

这些都是网络世界的主流用语。所以我们正在深入研究可以用来说服 IT 管理员的技术。希望我们能清楚地解释好这些概念，这样您就会说：“啊哈，就是这样的意思。这并不可怕。”

我们还会提到 ARP、VLAN、IP 子网和路由器。

两种（或 3 种）消息

- “标明地址的”消息具有巨大灵活性的优势
- 在 TDM 网络中，不需要使用任何形式的地址
 - 目标位置由其时间位置来解释
- 在分组交换网络中（就像邮件系统），收件人是唯一的
 - 也可以将“未经请求的”邮件从发件人发送到多个或所有地址
 - 这是非常有用的，不过同时也可能很令人恼火

标明地址的消息具有巨大灵活性的优势。

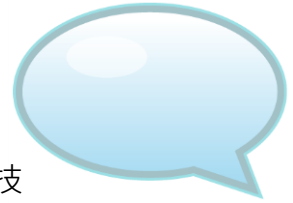
即使在古老的电报时代，在您需要把电报发送到一个地址时，这个信息也被包含在发信人消息中。

在 TDM 网络中，不需要使用任何形式的地址。它只是一个点对点的通信。外部协议会认可各个时间空档的含义，不一定需要是我们所说的同带信号。

在分组交换网络中，正如您在封装的那一页幻灯片中看到的那样，我们能够非常精确地处理在不同地址之间发送和接收的信息。

两种（或 3 种）消息

- IP 网络非常擅长通过管理技术来限制“未经请求的邮件”
- IP 网络中的三种消息类型是：
 - 单播 – 一对一通信
 - 组播 – 一对多通信
 - 广播 – 对所有人的通信
- 相比之下，TDM 网络只是真正的单播（但通过“接线技巧”可以实现类似于广播的功能） – 无论哪种方式都没有严格的区别



幸运的是，IP 网络非常擅长通过管理技术来限制“未经请求的邮件”

IP 网络中的三种消息类型是：

单播 – 一对一通信

组播 – 一对多通信

广播 – 对所有人的通信

相比之下，TDM 网络只是真正的单播（但通过“接线技巧”可以实现类似于广播的功能） – 无论哪种方式都没有严格的区别

消息类型的不同原理

- 旧式 IP 网络使用“集线器”或单根线缆将电脑连接在一起
 - 基于“第 1 层”的网络
 - 所有消息都是网络中有效的“广播”消息
 - 我们可以非常精确地处理一条消息
 - 使用一个集线器或单个“令牌环”连接，我们就能有效地从邮政系统中去掉“邮件分拣处”
 - 所有电脑都会收到每一封邮件，并且必须丢弃它们自己不感兴趣的所有内容
- 分组交换网络为 IP 广播消息使用特定 IP 地址，
 - 该地址会映射到特定的广播目标 MAC 地址
- 为了使它发挥作用，我们需要网络中的某些东西来“分拣”邮件



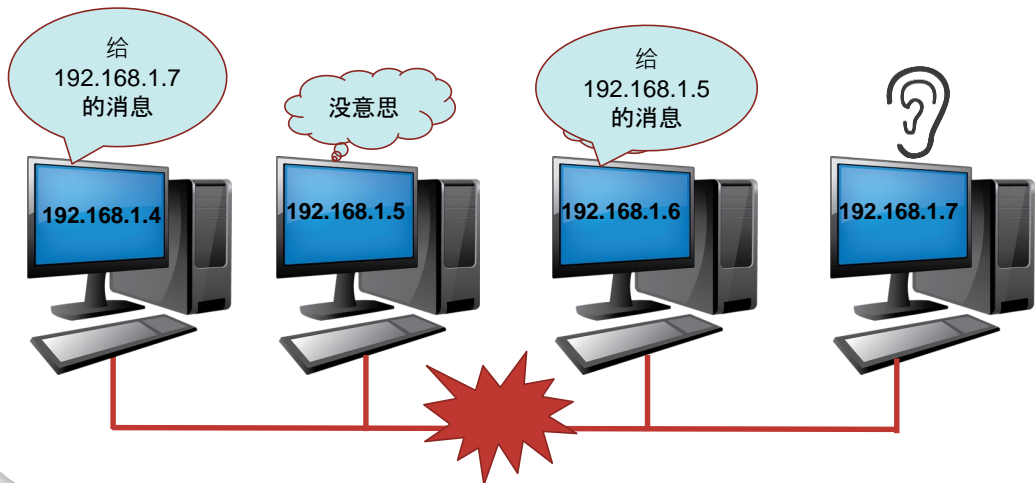
旧式 IP 网络使用“集线器”或单根线缆将电脑连接在一起

- 这被认为是基于“第 1 层”的网络
- 在这种网络中，所有消息都是网络内有效的“广播”消息
- 正如我们从封装过程中看到的那样，我们可以非常精确地处理消息
- 使用一个集线器或单个“令牌环”连接，我们就能有效地从邮政系统中去掉“邮件分拣处”
- 因此，所有电脑都会收到每一条消息，并且必须丢弃它们自己不感兴趣的一切内容（否则可能会打开不是发送给它们的信息或者恶意内容...导致安全问题）

分组交换网络为 IP 广播消息使用特定 IP 地址，该 IP 地址映射到特定的广播目标 MAC 地址

为了使它发挥作用，我们需要网络中的某些东西来“分拣”邮件

冲突域



这是冲突域的一个例子。

在旧式的集线器系统中，我们认为任何连接到集线器的对象都位于同一个冲突域

如果两个或多个设备可以同时传输到网络的同一个网段，这个位置就是冲突域发生这种情况时 – 正在传输的数据会出现“混乱”，基础架构无法将它们分开。

结果 = 信息完全无意义

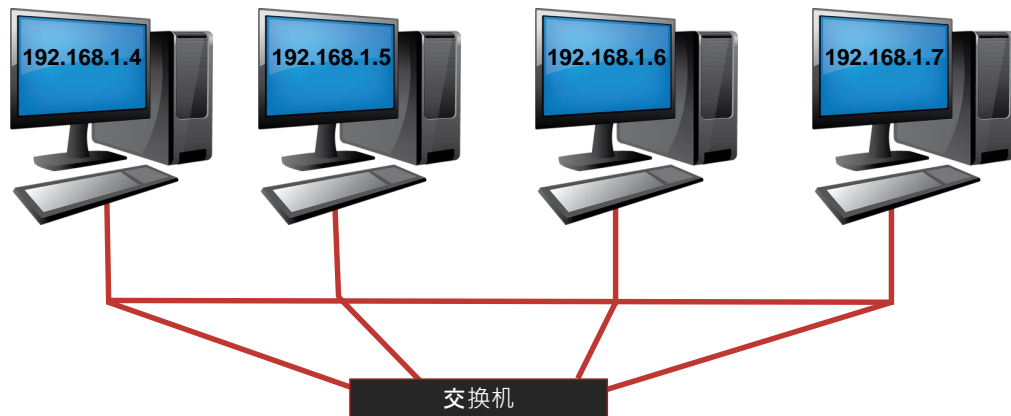
人们最终制定了协议来防止这种情况发生：带冲突检测的载波侦听多路访问 (CSMA/CD)

这种方法基本上是等待冲突发生，然后让发送设备等待一段随机时间，再重新发送信息。而且，理想情况下每台电脑的“随机”时间都有所不同，这样数据最终就能成功发送。这不适用于对时间敏感的内容，比如尝试发送时钟或实时媒体等情况。当您开始引入“随机时间”时，它并不会起作用，也正因为如此，Dante 不能运行在集线器网络上。时间是随机的。

这也是 Dante 不能运行在无线网络上的原因。Wi-Fi 也使用载波侦听多路访问/冲突避免 (CSMA/CA)。这导致 Wi-Fi 很难用于实时媒体。

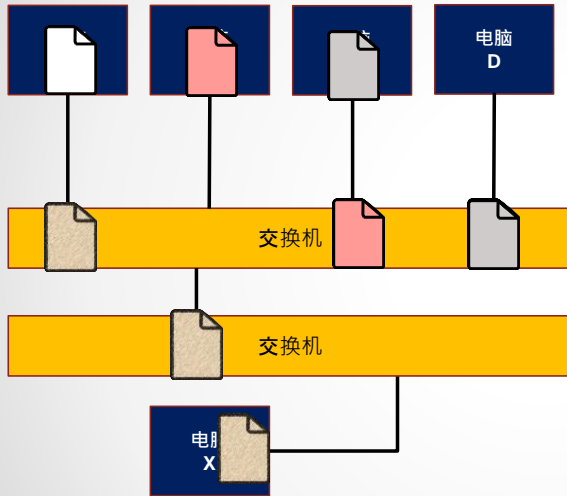
请注意，Wi-Fi 与专用无线链路不同。

冲突域 – 分段



交换机比单纯接线或“糊涂的”集线器更聪明 – 后者现在几乎已经不存在了。
交换机会查看以太网数据帧（第 2 层）上的目标 MAC 地址，并将其仅转发到物理接口，连接到具有所述目标 MAC 地址的设备
由于数据帧仍然是连贯的（不存在冲突混乱），如果发出信息的接口在那一精确时刻处于“繁忙”状态的话，交换机可以“缓冲”夫一数据框
这样就维持了数据的完整性
因此交换机被认为是对“冲突域进行分段”

单播传输



单播期间是源和目标之间的私有对话。

。



© Audinate Pty Ltd. All rights reserved

<http://www.audinate.com/resources>

(点击动画)

这个例子中的每个会话都是单播的，并且是源和目标之间的私有对话。

您可能会认为“这很好，我们正在使用 MAC 地址在设备之间进行通信。我们为什么要使用 IP 地址？”

我们来看看网络堆叠。请记住，我们在电脑上运行的应用程序需要与世界另一端的其他设备及其应用程序进行通信。所以它需要接口和 IP 地址的组件，以便进行远程通信。它也需要 MAC 地址的概念，因为它需要一块物理硬件来发送消息。

(我认为不需要读出来)

1. 网络连接如图所示
2. 电脑 A 将消息发送到电脑 D - 会话开始
3. 会话完成 (会话结束时网络是安静的)

4. 电脑 B 将消息发送到电脑 C-会话开始
5. 电脑 C 将消息发送到电脑 D-会话开始
6. 电脑 B 和 C 之间的会话完成
7. 网络被扩展
8. 电脑 X 将消息发送到电脑 A
9. 电脑 C 和 D 之间的会话完成
10. 电脑 X 和 A 之间的会话完成

“第 2 层”网络

- 交换机只关心 MAC 地址
- MAC 地址分三种类型
 - 主机（设备 IP 堆叠第 2 层的 MAC 地址）
 - 组播 – 指示交换机从所有接口发出的一组特定的目标 MAC 地址（除非被管理）
 - 广播 – 指示交换机从所有接口转发出去的一个目标 MAC 地址
- 某些网络技术仅使用第 2 层
 - MAC 地址到 MAC 地址
 - 这种网络技术比单纯使用无法识别设备的技术要好
 - 然而，这种方法不能像“完整堆叠”一样扩展
 - 需要为操作系统编写特定的驱动程序来处理堆叠的“缺失部分”

交换机只关心 MAC 地址

MAC 地址分三种类型：

主机（设备 IP 堆叠第 2 层的 MAC 地址）

组播 – 指示交换机从所有接口发出的一组特定的目标 MAC 地址（除非被管理）

广播 – 指示交换机从所有接口转发出去的一个目标 MAC 地址

某些网络技术仅使用第 2 层 – MAC 地址到 MAC 地址

这种网络技术比单纯使用无法识别设备的技术要好

然而，这种方法不能像“完整堆叠”一样扩展

需要为操作系统编写特定的驱动程序来处理堆叠的“缺失部分”

局域网 中的 IP 地址？为什么？

- 电脑操作系统中的“标准”网络堆叠，通过 IP 地址将端口连接到运行在其上的应用程序软件
- 我们假定与周边设备以及与世界另一端的设备通信都是采用一样的方法 – “细节”交给网络基础架构去完成。
- **重要提示**：理解网络“多层”共同运作的原理与理解各层本身一样重要
- 为了令设备了解如何与网络中的其他设备进行通信，我们使用一种称为 **ARP – 地址解析协议**将 IP 地址解析为 MAC 地址



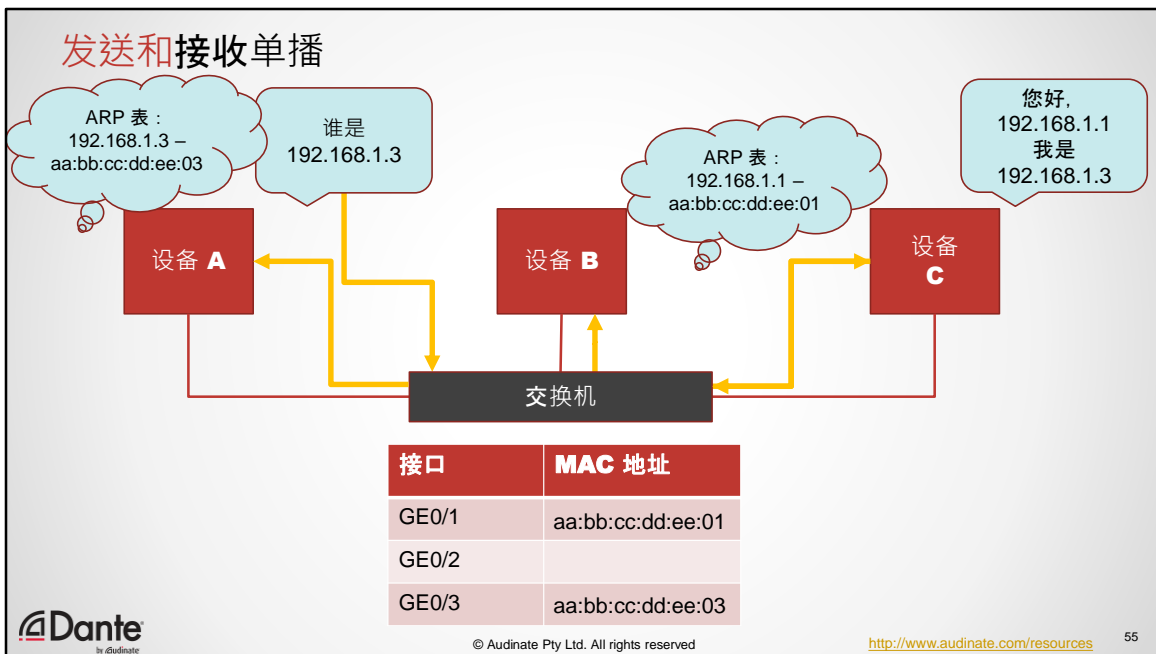
非常好。我们只需要 MAC 地址就可以在这样的网络中对话。为什么我们还需要 IP 地址？这更复杂，不是吗？

电脑操作系统中的“标准”网络堆叠通过 IP 地址将端口连接到运行在其上的应用程序软件

我们假定与周边设备以及与世界另一端的设备通信都是采用一样的方法 – “细节”交给网络基础架构去完成。

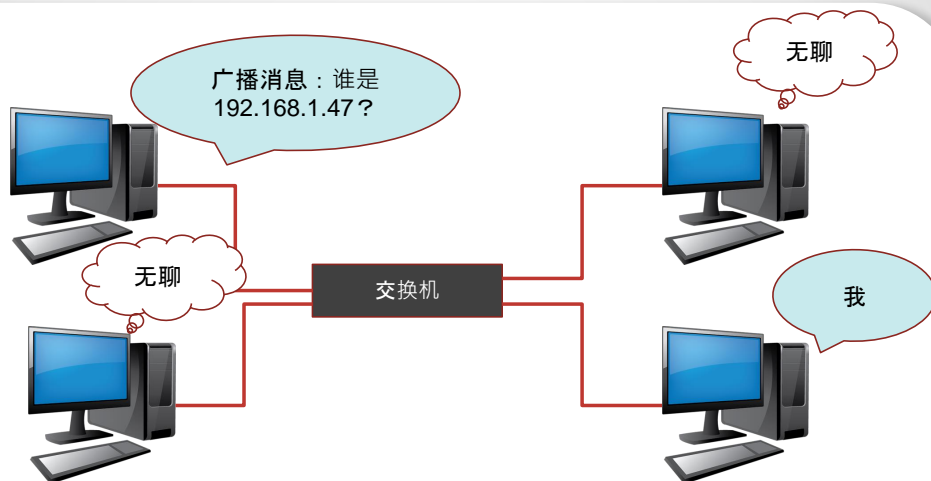
重要提示：理解网络“多层”共同运作的原理与理解各层本身一样重要

为了令设备了解如何与网络中的其他设备进行通信，我们使用一种称为 **ARP – 地址解析协议**的过程将 IP 地址解析为 MAC 地址



1. 设备 A 中的应用程序决定需要向设备 C 发送消息
2. 设备 A 知道设备 C 的 IP 地址（我们不关注这个例子中是怎么知道的）
3. 网络刚刚开启 – 尚未开始通信
4. 为了“找到”设备 C，设备 A 发出“ARP”（地址解析协议）请求（广播消息）
5. 这个广播信息发到了所有地方
6. ARP 消息中有一些标准的有用信息：
 1. 源 MAC 地址
 2. 源 IP 地址
7. 交换机记录源 MAC 地址，并填充其 MAC 地址表
8. 设备 B 接收并忽略该消息
9. 设备 C 接收并响应该消息（单播）
10. 设备 C 从包含分组的数据帧中知道了目标 MAC 地址，从中知道从设备 A 发送的发送 IP 地址
11. 设备 C 填充其 ARP 表
12. 交换机通过查看返回的消息来填充 MAC 地址表

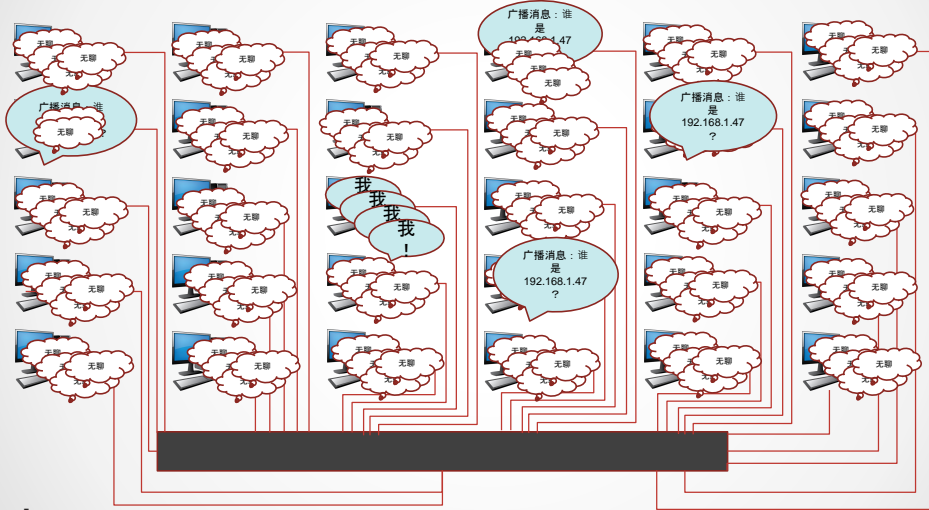
广播域



那么让我们来看看为什么 IT 管理员们害怕广播。

这是一个小型网络。我们将发布 ARP。这个人响应了。我们只需要发送几个 ARP，那么每个人都会发现对方。但是当网络变大时会发生什么？

广播域



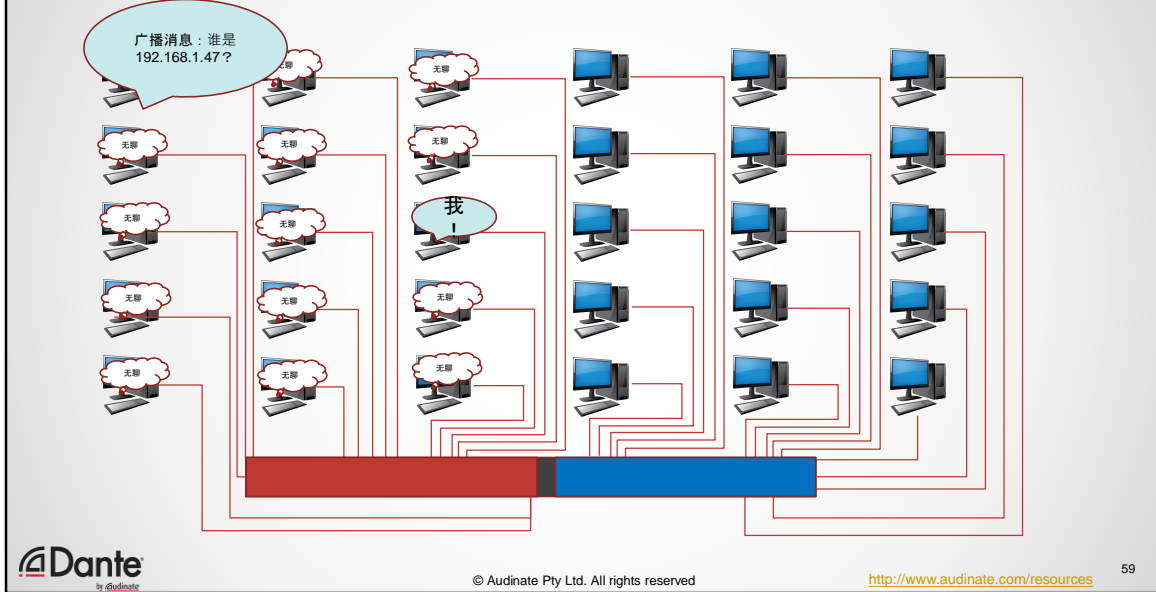
这个人发送出一个 ARP，每个人都认为这很无聊。除了这个人。
然后这个人发送一个 ARP，每个人都认为这很无聊，除了这个人。
然后这个人发送一个 ARP，这个人，这个人.....



有更好的方法来解决这个问题吗？

当然有更好的方法来做到这一点。您可以看到网络上有很多根本没人感兴趣的信息在发送。

分段广播域 – 良好的做法



所以我们做的是对广播域进行分段。我们需要做的是将这个交换机一个切成俩。现在，当我发出 ARP 时，只有这台交换机上的人才能听到它。

作为一般规则，有“充分理由”经常要相互通信的设备应该归为同一广播域的成员在音频网络中，调音台不太可能与办公室经理的电脑进行通信因此明智的做法是 将这些设备放入不同的广播域

如何做到这一点？

我们可以有一个完全独立的布线基础架构中，将它们分隔在两个物理局域网

更高效的做法是将它们分入不同的 VLAN – 虚拟局域网

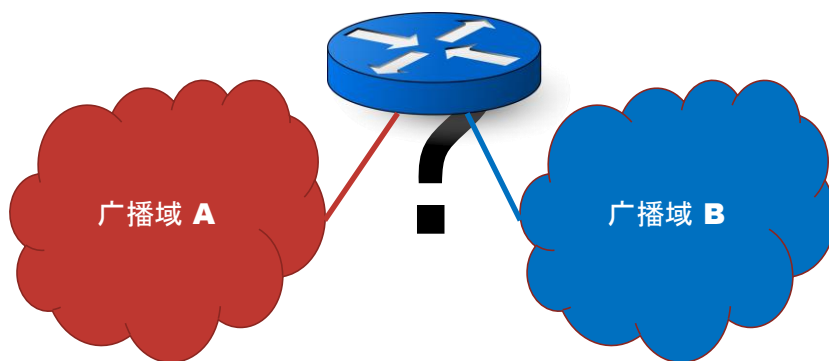
但是如果我们需要偶尔通信呢？

我们可以使用路由器来连接两个（虚拟）局域网

路由器不会传递广播流量

路由器只关心 IP 地址 (OSI 模型的第 3 层)

广播域分段 - 保持连接



所以现在有了两个不同的广播域。它们被分段了。我们接下来在中间安进一个路由器。路由器不传递广播信息。这样，路由器监听 IP 地址并查看源 IP 地址和目标 IP 地址，并且这些地址可通过路由器传递。这样就将那些有很多广播流量的区域分割成了更小的空间。

这也是人们喜欢按功能拆分 IP 子网的原因。如果我想要让所有的销售部门共享一个网络，最好是让它们很快能发现对方。这样它们就可以在彼此之间使用广播消息。但是它们并不一定要跟制作部门一直对话。所以没有必要向制作部门的网络发送广播消息。而制作员工可以专注于自己的事情。

以这种方式进行分段还可以让我们在路由器中进行过滤从而阻止连接，因为两个独立的广播域相互无法进行通信。

由于这一切都是在逻辑层完成的，所以我们的布线基础架构仍可以用常见的产品，用软件更改这些设置就可以，而不必拉线缆。

某些网络功能需要广播消息

从 ARP 的例子中我们可以看出为什么这是必要的

广播消息被局域网中的每个设备接收

这种特点对于建立全球可扩展的网络至关重要

考虑一下 ARP 是否可以发给连接到公共互联网的全部数十亿台设备

即使一台设备只发少量消息，也会使整个网络停顿

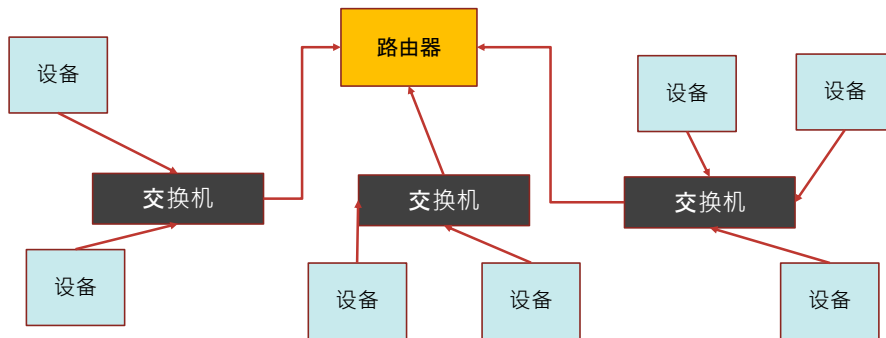
为了在局域网之外进行通信，就需要路由器

路由器不会传递广播流量

因此路由器是对广播域进行分段

虚拟局域网(VLAN)-历史

最初，当网络管理员对网络分段的时候没有虚拟局域网(VLAN)。每“组”电脑使用不同的路由器



但是如果我们需要偶尔通信呢？

我们可以使用路由器来连接两个（虚拟）局域网

路由器不会传递广播流量

路由器只关心 IP 地址（OSI 模型的第 3 层）

路由器维护 ARP 表 - 终端不（一定）维护

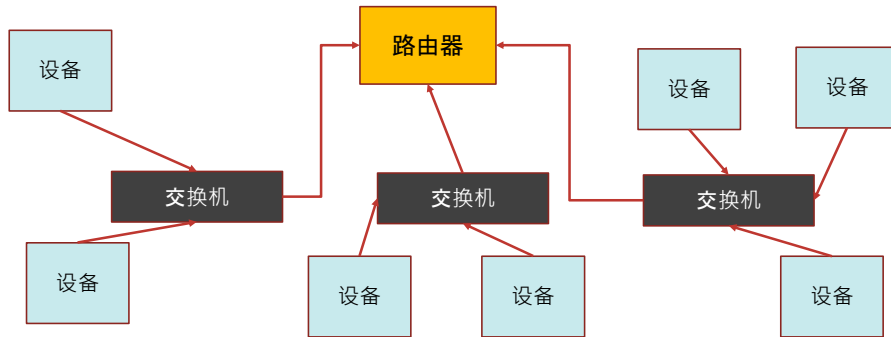
在我们了解 VLAN 上这一点是如何完成的之前，我们先来回顾一下它们的历史。

因此，当 IT 管理员想要给网络分段时，他们必须为每个部门购买不同的交换机。这没问题，只要您的各个团队的地理位置都彼此类似就行。如果您使用了交换机上几乎所有的端口，那也没关系。

但不幸的是，现实情况并不是这样。

虚拟局域网(VLAN) -历史

现实中交换机上有大量“闲置”端口，以及大量额外的接线
闲置端口=浪费金钱！

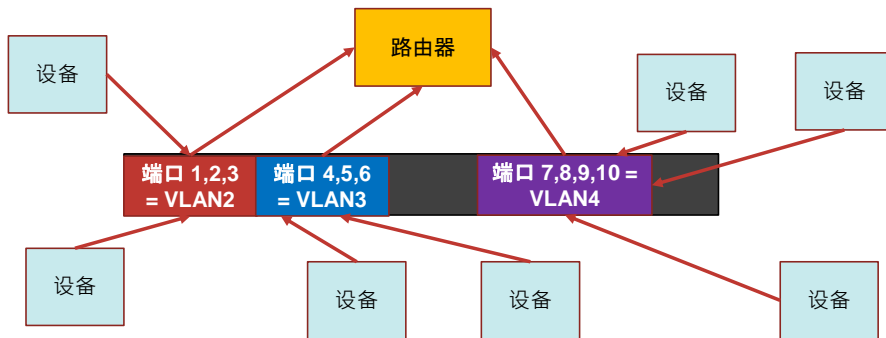


我们最终面对的现实是用上了很多交换机，交换机上有很多闲置端口。没有人喜欢闲置端口，因为它通常都意味着浪费金钱。那么我们如何更有效地做到这一点？

虚拟局域网(VLAN) -历史

为什么不把这些物理局域网全都放在同一台交换机上？

节约“闲置”端口 – 布线仍然相同



那么第一步就是弄来一个大交换机，把端口合并到一起。这样我们就有了基于端口的 VLAN。

我们可以用红色 VLAN 将所有电脑连接在一起，然后将线缆连接到路由器。

将蓝色 VLAN 的电脑连接在一起，然后将另一根线缆连接到路由器，把三台电脑连接到紫色 VLAN，再将它也连接到路由器上。

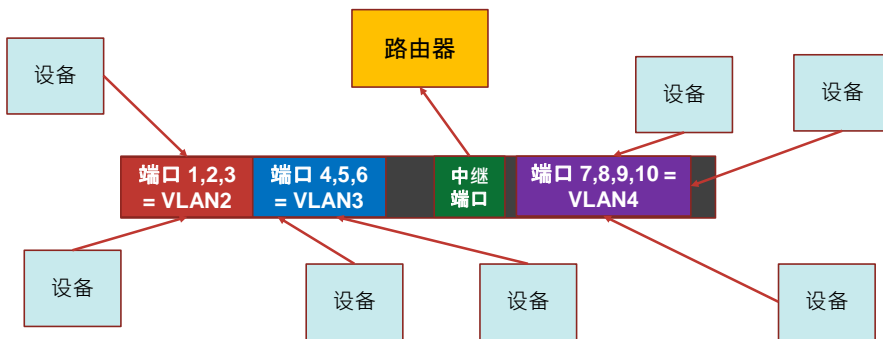
这很棒。这样就基本解决了我的交换机端口问题。但是在这个例子中，我从每个虚拟局域网用一个交换机端口连接到路由器，等于是三重布线。

这是一个好的开始，我在交换机上节省下了一些钱。但我们可以做得更好，我们是聪明的 IT 人员。

虚拟局域网(VLAN) -历史

端口的 VLAN 确实为昂贵的交换机端口节省了金钱

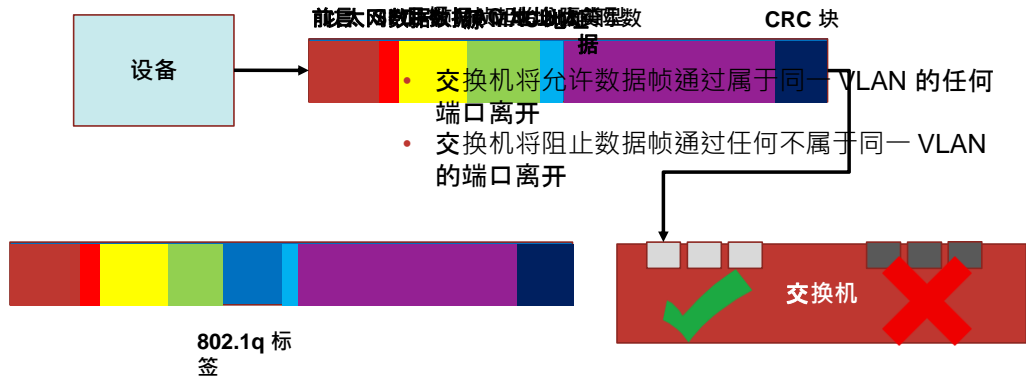
现在 802.1q“标签”解决了重复布线的问题 – 这个标签允许数据帧出现在相同的线路上



所以我们产生了建立一个中继端口的想法。

我们在流量中放置一个标签来表明这个特定的流量属于这个特定的 VLAN。

VLAN 标签 和 PVID (PORT VLAN ID)



VLAN 标签以这种方式工作：

我们把封装的概念用在 VLAN 上面。

要用在 VLAN 上，我们必须使用必要的 VLAN 编号来标记数据帧

1. 所以，我们要在设备中构建一个以太网数据帧-
2. 一个以太网数据包以一个前导码开始，其中包含一个交替的 1 位和 0 位（7 字节）数字，方便网络上的设备同步接收器时钟，实现位级同步。
3. 接下来是 SFD- 数据帧起始分隔符 (10101011)，这标志着有用数据的开始和前导码的结束。
4. 接下来我们添加目标 MAC 地址
5. 随后是源 MAC 地址
6. 然后是以太类型-用于指示哪个协议被封装在数据帧的实际数据中
7. 之后是实际数据- 所有的数据！它包含 IP 数据包 - 交换机不关心 IP 地址。路

由器才关心。

8. 最后是 CRC 块（循环冗余校验），以便检测出错误。
9. 该数据帧进入交换机的交换机端口。交换机端口被设置为接受“无标签”的数据帧（但是属于 VLAN 的成员）
10. 交换机将 802.1q 标签放入数据帧中
11. 交换机将允许数据帧通过属于同一 VLAN 的任何端口离开
12. 交换机将阻止数据帧通过任何不属于同一 VLAN 的端口离开

IEEE802.1q 下有 4096 种可以用的 VLAN 标签



边界设备（台式电脑、Dante 设备等）通常会发送“无标签”数据帧



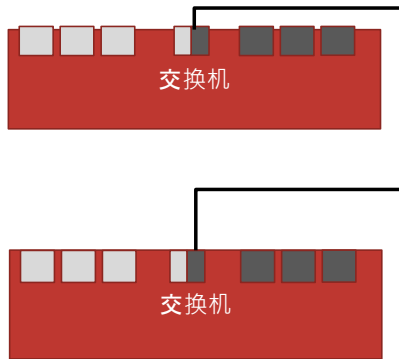
交换机会被设置为在这些设备连接的接口上接收无标签的数据帧（它还会“去掉”通过“未标签”的接口离开的数据帧的标签）

当无标签的数据帧进入设置为“在 VLAN 中无标签”的接口时，接口将为该数据帧的后续传输应用 VLAN 标签



交换机只允许匹配 VLAN 的标签进入或离开其接口

VLAN 标签 - 和 PVID (PORT VLAN ID)



- 要访问另一台交换机上同一 VLAN 中的端口，要建立一个使用多个 VLAN“标签”的端口
 - 思科称之为“中继”端口
- 中继或多标签连接允许具有不同 VLAN 标签的数据帧使用相同的物理接口
- 带标签的数据帧仅允许通过同一 VLAN 中的端口离开交换机
- 当带标签的数据帧离开正常的本地接入层 VLAN 端口时，该标签被移除。
- 在中继端口中，标签不会被移除。

1. 如果我们想要访问另一台交换机上同一个 VLAN 中的端口，我们怎么做 - 我们可以建立一个带有多个 VLAN “标签”的端口（思科称之为“中继”端口）
2. 中继连接（或称多标签连接）允许具有不同 VLAN 标签的数据帧使用同一个的物理接口（它们的标签仍然必须匹配该接口的允许标签）
3. 标有该 VLAN 标签的数据帧只能通过这些端口离开交换机
4. 同样，标有其他 VLAN 标签的数据帧也只能通过这些端口离开
5. 带标签的端口不会删除 802.1q 标签，因此具有不同标签的流量可以在同一物理连接上加载

要记住的重要一点是当标签数据帧离开正常的本地接入层 VLAN 端口时，该标签会被删除。在中继端口中，标签不会被删除。所以您会听到有人说标签和非标签（思科）也有人说访问和中继（惠普的叫法）。这说的是同一件事。

IPV4 IP 地址 – 主机和网络

- 路由器对广播域分段 – 因为它们不会转发广播流量
 - 路由器不关心 MAC 地址（它们会掩盖地址 – 这是很好的安全功能）
- VLAN 可以用 802.1q 标签分隔广播域
- 路由器可以将 IP 子网连接在一起
- “IP 地址”有 2 种
 - “主机”地址 – 设备的 IP 地址
 - “网络”地址 – 描述一组主机的 IP 地址
- IP 子网的大小由子网掩码定义。子网掩码：
 - 是通过 DHCP 提供的 4 个八位字节号码，也是静态 IP 配置的重要组成部分
 - 让设备知道哪些 IP 地址属于“本地”（相同的子网）哪些属于“远程”
 - 本地 IP 地址会令设备发出 ARP
 - 远程 IP 地址则被转发到“默认网关”的 MAC 地址（如果有定义）
 - 如果没有定义的“默认网关”，则该消息将被丢弃



在 IPV4 中，我们有两个并行的概念在运行。大家都听说过 IP 地址。我们的主机，可以是一台电脑，一台 Dante 设备或其他设备，主机有 IP 地址，然后我们也有一个网络地址。

毕竟，由于路由器会对广播域分段，并且它们不会转发广播流量，正如我们所看到的，我们需要一种方法来确保我们能够进入正确的子网。

正如我们所见，路由器不会转发 MAC 地址。它们不关心这些信息。

我们可以使用 VLAN 来分隔广播域。毕竟，我们会根据行政决定阻止不同交换机端口之间的设备互通。当我们想再次将这两件事重新结合在一起时，就要使用路由器。

由于 VLAN 处于第 2 层 MAC 地址级别，IP 子网处于数据包级别或 IP 级别（第 3 层）。

“IP 地址”有 2 种

- “主机”地址 – 设备的 IP 地址
- “网络”地址 – 描述一组主机（或机器）的 IP 地址

设置扩展广域网最重要的是子网掩码。

而在讨论子网掩码时，常常会涉及到定义中的冲突。以前，我们认为 IPV4 已经足够大，能够容纳整个世界（实际上不能），那时候我们提出了分类 IP 地址的想法。不知何故，某些机构占用了其中很大一部分。这就导致留给其他人的不够了。

分类 IP 地址非常好，因为它们位于八位字节边界处，但它们的效率不高。

后来我们即将用完 IPV4 地址这个问题越来越突出，于是我们也转而开始采用无类系统。

问题是，人们一开始谈到一个 A 类子网，然后却用无类的方式来描述它。其实，这两种术语在某种程度上是互不兼容的。现在对于 A 类、B 类、C 类网络的公认定义存在若干界限，但是如果您要从无类的角度来使用它，就会导致混乱。因为子网掩码长度由类定义。所以在现代网络的说法中，我们先说网络地址，然后是斜杠，后面是描述我们 IP 子网的多个位。

IP 子网的大小由子网掩码定义。子网掩码：

- 是通过 DHCP 提供的 4 个八位字节号码，也是静态 IP 配置的重要组成部分
- 让设备知道哪些 IP 地址属于“本地”（相同的子网）哪些属于“远程”
- 本地 IP 地址会令设备发出 ARP
- 远程 IP 地址则被转发到“默认网关”的 MAC 地址（如果有定义）
- 如果没有定义的“默认网关”，则该消息将被丢弃

IP 子网掩码

- IPv4 地址有 32 位 – 也就是 1 个网络当中有 43 亿台设备
- 想象一下如果单个广播域有这么大会怎么样！
- 这就是为什么我们有 IP 子网（来对这个广播域分段）
- 子网掩码是 IP 地址的“网络”地址部分和 IP 地址的“主机地址”部分之间的“边界”
- 有效的子网掩码是一行连续的二进制‘1’，直到达到掩码以后变为‘0’

子网掩码 (十进制)	子网掩码 (二进制)	子网掩码 CIDR	每个网络的主机数量	可能的网络数量
255.255.255.0	11111111.11111111.11111111.00000000	/24	254	1670 万
255.0.0.0	11111111.00000000.00000000.00000000	/8	1670 万	256
255.255.255.248	11111111.11111111.11111111.11111000	/29	6	5.37 亿

一共是由 32 位构成一个 IPV4 地址。

IP 子网掩码告诉设备 IP 地址的哪一部分是它“关心”的“本地”部分

由于是二进制组成，所以它被称为掩码

它不是网络信息，而是在对特定子网感兴趣的设备之间达成的约定。

IP 子网掩码由 4 个“八位字节”构成，以匹配 IPV4 地址

有效的掩码可以是：

255 254 252 248 240 224 192 128 (0)

为什么？

在二进制中 255 = 11111111 254 = 11111110 252 = 11111100 248
= 11111000 240 = 11110000 224 = 11100000 192 = 11000000 128
= 10000000 0 = 00000000

由 1 构成的“屏障”告诉设备匹配被 1“掩蔽”的任何二进制值，如果匹配是“成功”，则地址属于本地 – 如果存在不匹配 – 则转发

到网关（交给别人处理）

例如 – 我发送给目标 IP 地址 192.168.1.10，我的子网掩码是 255.255.255.0，我的 IP 地址是 192.168.1.12 我的设备会去匹配 192.168.1 – 这是一个“良好的匹配”，所以我知道它是本地地址
如果我发送给 192.168.2.10，那么 2（第三个）八位字节就不匹配，那么我就知道它会被发送到网关

VLAN 和子网

- 单个 VLAN 是单个广播域
- IP 子网也是一个广播域
- 因此，VLAN 也可以向路由器描述为 IP 子网
- 警告！– 在同一 VLAN 中对两个 IP 子网进行静态 IP 寻址并不明智！
 - 在 VLAN 中建立 IP 广播数据包时，它将被静态映射到广播 MAC 地址
 - 在第 2 层，设备无法区分来自另一个 IP 子网的广播数据帧
 - 因此，在同一 VLAN 中的不同 IP 子网的 IP 广播仍然去到“其他”IP 子网中的设备 – 这就存在潜在的安全风险
- 提示 – 使每个 VLAN 都拥有自己的 IP 子网



单个 VLAN 是单个广播域

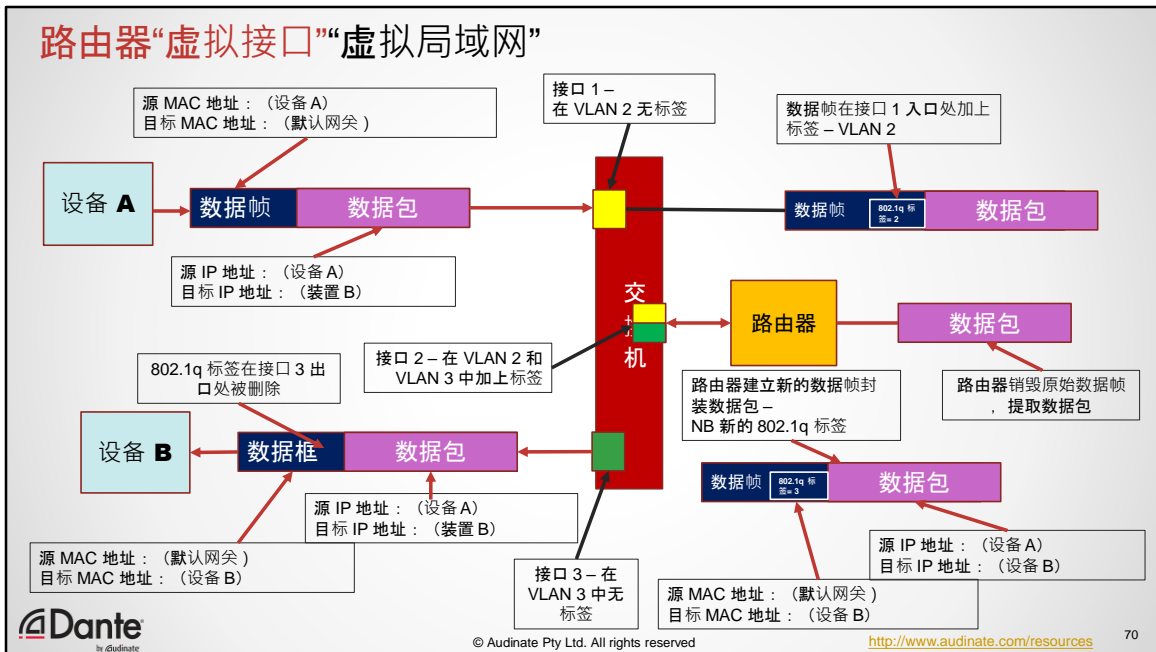
IP 子网也是一个广播域

因此，VLAN 也可以向路由器描述为 IP 子网

警告！– 在同一 VLAN 中对两个 IP 子网进行静态 IP 寻址并不明智！

- 在 VLAN 中建立 IP 广播数据包时，它将被静态映射到广播 MAC 地址
- 在第 2 层，设备无法区分来自另一个 IP 子网的广播数据帧
- 因此，在同一 VLAN 中的不同 IP 子网中的 IP 广播仍然去到“其他”IP 子网中的设备 – 这就存在潜在的安全风险

提示 – 使每个 VLAN 都拥有自己的 IP 子网



这是一个在具有 VLAN 的路由器中的图形化流程示例。

设备 A 发送一条消息，一开始包含我们的源 MAC 地址和目标 MAC 地址的数据包，然后它被封装到一个数据帧中，之后我们可以将其发送给交换机。

然后交换机将 VLAN 标签放入数据帧中。然后我们想把它发送到不同的子网。那么，我们有一个连接到路由器的中继端口，现在大多数路由器都不能理解 802.1Q VLAN 标签，也就是您在路由器内部将 VLAN 映射到 IP 子网的位置。

路由器提取数据帧、丢弃数据帧头，并查看数据包。这就是路由器对第 3 层感兴趣的原因。

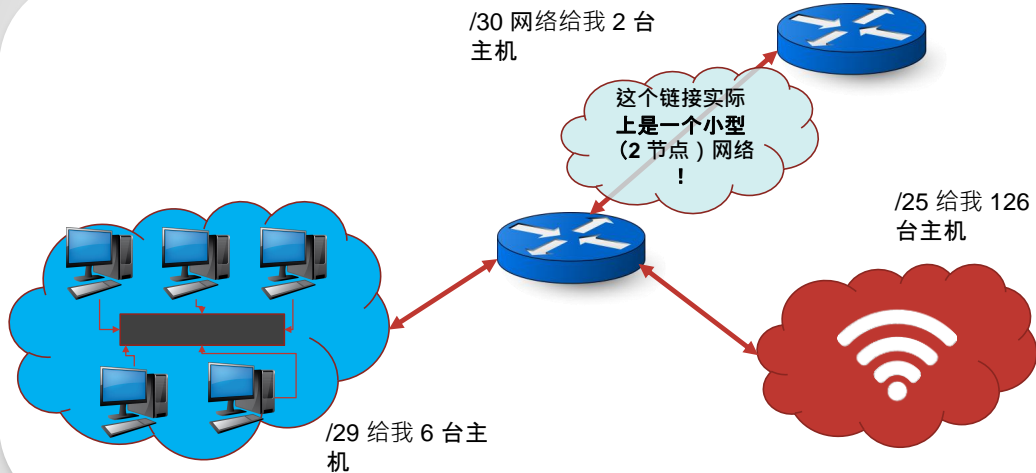
查看源 IP 地址和目标 IP 地址，并且知道目标 IP 地址位于其他子网中，并且它也连接到该子网。

获取数据包，并且因为它知道最终目标的 MAC 地址，所以它重建了一个数据帧，但是这次目标 MAC 地址现在是另一个子网内设备的地址。所以它实际上会重建该数据报的外部，然后知道要加上哪个 VLAN 标签来确保它从正确的端口发出

并抵达那台机器。

当然，我们在这里可以看到，在它离开交换机的时候因为是接入层交换机端口，802.1Q 标签被删除，那么我们又回到了设备 B 可以读取的数据帧和数据包中。

为什么子网大小不同？



那么，为什么我们要有不同大小的子网呢？

因为我们的地址数量有限，所以我们必须有效地使用它们。

那么在这里我可以用到 6 台使用 /29 位子网的主机。

这个链接基本上是将此设备连接到此设备。两台路由器连在一起。只有两个节点参与其中。它仍然是一个网络，虽然它只有两台设备。我可以使使用 /30，这样我有 2 台主机。2 个 IP 地址，链路两端各一个。

然后我可能会在这里建立一个 Wi-Fi 子网。我有来宾 Wi-Fi，我可以用一个 /25，这样我就有 126 个 IP 地址，我可以分配给那些只想使用我的来宾 Wi-Fi 的人

。

对于最有效的 IP 方案从最大到最小分段

子网 ID	第一台主机	最后一台主机	广播 IP	子网掩码	主机数量
192.168.1.0	192.168.1.1	192.168.1.126	192.168.1.127	255.255.255.128	126
192.168.1.128	192.168.1.129	192.168.1.134	192.168.1.135	255.255.255.248	6
192.168.1.136	192.168.1.137	192.168.1.138	192.168.1.139	255.255.255.252	2

我应该使用静态还是动态 IP 地址？

- 通常情况下，动态地址更简单，也更不容易出现人为错误
- 静态地址一般更适合用于服务器（但不是必需的）
- 在使用组织 SSL 证书时，静态 IP 地址是必不可少的（在欧洲，这是获得公共静态 IPV4 地址唯一可接受的“借口”）



所以这里的诀窍是，如果我要建立一个大规模的网络，我应该从一开始就使用最大的网络，然后再缩小。这意味着我实际上可以将这些 IP 地址块串在一起。

为什么这个很重要呢，比如说当我进入到其他人的 IT 基础架构，然后要求连通多个 VLAN，或者我想使用不同的 IP 子网的时候。这是绝对会让 IT 管理员发狂。因为他们有一份像这样的巨大电子表格，精心组织好各个 IP 子网的大小来适合这个位置。他们将所有的 IP 地址都排在一条长线上，高效率地使用它们。

然后您出现了，然后说“嘿，我想要做些不一样的事情”，他们一听到这个立刻就会摆出一副我不想跟您打交道的表情。

其实很简单。在很多网络上，您不一定要连接到公共互联网。

这样您就可以在自己的一组 IP 子网中使用自己的 VLAN。只要路由器没有指向其他子网，您可以使用任何您喜欢的方案。这是完全可扩展的，所以只要有管理员给您分出来一小部分自己的空间，您就可以为所欲为。只有当您开始想要加入更多不同的网络时，您才没有完全控制权，这个时候您必须与管理员联系。

所以实际上，在跟 IT 人员谈到这个问题的时候，首先第一个问题是要厘清“访问其他网络”实际上指的是什么。

例如，您可以向他们说明您想要公共互联网连接。您实际上只需要一个 IP 地址

来连接公共互联网，这实际上是一件很容易的事情。
这是知己知彼，百战百胜。

高级 DANTE 联网：第 4 节

在本节中...

服务质量

- 什么是 QoS，什么不是
- 您什么时候要使用它？

“第三种”通信

组播

- 为什么组播有用
- 我们如何管理组播？
- 网路群组管理协定(IGMP) – 深潜



在本节中，我们将介绍服务质量和组播。

之后我们将进一步讲解这两个概念的细节。

我们经常被问到服务质量的问题，因为人们认为您需要在这方面下很多工夫。我们将揭开关于 QoS 的一些迷思。

对于组播，我们将讨论何时使用组播、如何处理它、如何管理它，以及如何在大规模环境中处理 IGMP 侦听。

服务质量 (QOS)

什么是服务质量 (QoS) ?

- 服务质量 (QoS) 是流量优先和管理的方法
- 其目的是为使用网络的应用程序提供特定级别的服务
- 我如何指定一个服务级别？
 - 吞吐量
 - 延迟
 - 延迟变化
 - 数据包丢失



服务质量 (QoS) 是流量优先化和和管理的方法。

这是一套您可以部署在网络基础架构中的技术，可帮助您以不同方式区分和处理不同类型的流量。

其理念是，您可以为网络上的不同应用程序提供不同级别的服务。

那么，Dante 是一个运行在网络上的应用程序，因此您可以将 Dante 与其他流量进行区别对待。电子邮件是另一项服务猫视频又是另外一个。

目的是为使用网络的应用程序提供特定级别的服务。

- 与“自由模式”的最佳效果系统相比，这样的效果可能更好，也可能更差

这是如何指定的呢？

- 吞吐量、延迟、延迟变化（每个数据包的延迟有多少变化）、数

据包丢失等。

IP 传输音频(AoIP)实际上只关注其中的某些方面

- 延迟变化 – 有助于最大限度地减少延迟并获得良好的 PTP 性能
- 总吞吐量 – 我们需要网络承载大量的音频数据包
- 数据包丢失 – 我们需要所有音频都能成功传输

什么是服务质量 (QoS) ?

- QoS 有两种基本形式：
 - 基于类别的，使用排队和优先级排序等方法（例如 Diffserv）
 - 相对
 - 指定哪些重要、哪些不重要
 - 实行容易
 - 基于预订的，使用速率控制、流量整形和准入控制的方法（例如，QoS NSLP 或 Intserv）
 - 绝对
 - 指定数量、频率以及方法 – 然后在可能的情况下做出决定
 - 实行复杂



服务质量 (QoS) 是流量优先化的方法。

目的是为使用网络的应用程序提供特定级别的服务。

- 与“自由模式”的最佳效果系统相比，这样的效果可能更好，也可能更差

那么 QoS 有两种基本形式。我在这里说的只是笼统的概念，如果您已经对 QoS 有深入了解，非常抱歉，但这里只是一种笼统的表述。

首先是基于类别的方法。

基于类别的 QoS 方案使用的是非常简单的方法，例如管理队列，优先处理这些队列或进入这些队列的数据包，以便在服务中提供差异化。您看到了 Diffserv 这个词，这可能是最常使用和最广泛部署的基于类别的系统。

它是相对的：A 类、B 类、C 类、D 类，这些类别之间的差异很重要。但不是绝对的。它不会强调 A 类得到什么，而是说 A 类得到的是 B 类没有得到的。这对于帮助识别重要事项、处理重要事项以及排除重要性较低的事项非常有用。实行起来也很简单。

另一类 QoS 机制就是所谓的基于预订。这个用的是更高级的方法，如速率控制、准入控制、流量整形等一大堆复杂的学术领域和技术，以便更好地处理流量问题。在这里您会听到“交通工程”这个词。

这可以帮助您在两个网络之间提供速率有限的链接，例如，您可以限制基础架构中的人员访问 Netflix 的可用带宽量。

这是一套非常强大的工具。

您需要非常非常仔细地指定您要实施的数字：我要控制带宽吗？我要控制高峰速度吗？我要处理什么流量参数？然后完成整个设置过程。端到端，贯穿整个链路。这非常复杂。只有当您知道自己在做什么，或者您认为自己知道自己在做什么时，才能触摸这一块！

这是如何指定的呢？

- 吞吐量、延迟、延迟变化、数据包丢失等

IP 传输音频(AoIP)实际上只关注其中的某些方面

- 延迟变化 – 有助于最大限度地减少延迟并获得良好的 PTP 性能
- 总吞吐量 – 我们需要网络承载大量的音频数据包
- 数据包丢失 – 我们需要所有音频都能成功传输

QoS 有两种基本形式

- 基于类别，使用排队和优先级排序等方法（例如 Diffserv）
 - 指定哪些重要、哪些不重要
- 使用速率控制和准入控制之类的方法（例如 QoS NSLP）
 - 指定数量、频率以及方法 – 然后在可能的情况下做出决定

什么是服务质量 (QoS) ?

IP 传输音频(AoIP)实际上只关注其中的某些方面：

- 延迟变化 – 有助于最大限度地减少延迟，并在更广泛的条件下实现良好的 PTP 性能
- 总吞吐量 – 我们需要通过网络获取大量音频数据包
- 数据包丢失 – 我们需要所有音频都能成功传输



服务质量 (QoS) 是流量优先化的方法。

在音频 IP (AoIP)方面，我们只着重关注少数几个方面。

IP 音频在现代网络上真的是一个非常宽容的应用程序。由于现在网络速度如此之快，因此音频应用并不需要用到网络所能提供的一切。之前在 100M 和 10M 网络中，我们几乎占满了网络的全部功能。但是，今天已经有了千兆网甚至更高的速度，这个已经不再是我们的瓶颈。

那么我们关心什么？

- 延迟变化 – 有助于最大限度减少整体延迟低，并获得良好的时钟 (PTP) 性能。一致性是关键。
- 总吞吐量 – 我们需要网络承载大量的音频数据包
- 数据包丢失 – 我们需要所有音频都能成功传输。我们不希望音频丢失。

QoS 有两种基本形式

- 基于类别，使用排队和优先级排序等方法（例如 Diffserv）
 - 指定哪些重要、哪些不重要

- 使用速率控制和准入控制之类的方法（例如 QoS NSLP）
 - 指定数量、频率以及方法 – 然后在可能的情况下做出决定

为什么要这么做？

- QoS 技术有助于将性能进一步扩展，令带宽限制不再成为问题
 - 帮助基础架构发挥更大的功效
 - 以超过 60–70% 的利用率运行链接
 - 在同一网络中混合 100Mbps 和 1Gbps
 - 运行共享服务网络（例如音频和视频、企业 IT 等）
- QoS 不是魔法，它不能创造出更好的性能

那为什么要用它呢？

QoS 技术有助于将性能进一步扩展，令带宽限制不再成为问题

帮助基础架构发挥更大的功效

以超过 60–70–80% 的利用率运行链接

如果您在同一个网络中混合 100Mbps 和 1Gbps，这就很有用

或者如果您要运行共享服务网络（例如音频和视频、企业 IT 等）

QoS 不是魔法，它不能创造出更好的性能事实上，反而在 QoS 关闭了之后，才能获得最佳性能。而插入 QoS 之后，性能反而开始下降。

所以从 QoS 开始。看看您是否真的需要它，然后再使用。

为什么要这么做？

- 简单的事实：现有最好的 QoS 是带宽
 - 成本低廉，资源丰富，易于使用
 - Dante 将向系统提供可预测的峰值负载 – 这应该使您能够确保网络的用量适当
- 关键事项：
 - Dante 设备发送相对较小且固定大小的数据包，这些数据包由发送设备“合理”分布
 - 这样有助于最大程度上减少交换机上的队列，从而大大降低对 QoS 的需求，进而获得优秀的性能



简单的事实：可用的最佳 QoS 是带宽

成本低廉，资源丰富，易于使用

Dante 将向系统提供可预测的峰值负载 – 这应该使您能够确保网络的用量适当

关键事项：

- Dante 设备发送相对较小且固定大小的数据包，这些数据包由发送设备“合理”分布

- 这样有助于最大程度上减少交换机上的队列，从而大大降低对 QoS 的需求，进而获得优秀的性能

我们的工程副总裁讲述的一个故事是他获得博士学位时在服务质量的故事。在他开始攻读博士学位、他的博士生导师告诉他：“你在做的事实际上是徒劳的。快加速度吧。”

Dante 设备提供的流量实际上是以不会使交换机超负荷的方式进行设计的。不会对交换机造成压力。

基于类别的 QoS

- 基于类别的 QoS 是 COTS 以太网交换机中部署最广泛的技术
 - 这可以归功于 VoIP !
- 使用写入每个数据包的 IP 或以太网报头的标签
 - 只是一个数字，没有特别的意义
- 交换机需要检查每个数据包并映射到输出端口上的指定队列
- 然后按照管理过程的一组规则清空队列
 - 这些规则定义了每个类别的流量所经历的服务水平

基于类别的 QoS 是 COTS 以太网交换机中部署最广泛的技术。这是 VoIP 的功劳

。

使用写入每个数据包的 IP 或以太网报头的标签。报头中已经有空间来支持这一点。交换机仅仅需要查看这些信息并看到一个数字。如果它看到数字 7，它将把它发送到这个队列，或这个队列，或另一个队列。这种办法简单又高效。

只是一个数字，没有特别的意义

交换机需要检查每个数据包并映射到输出端口上的指定队列

然后按照管理过程的一组规则清空队列

这些规则定义了每个类别的流量所经历的服务水平

基于类别的 QOS

- 有许多优势
 - 简单
 - 每个数据包的附加位较低
 - 在交换机芯片中实行
 - 分布式
 - 灵活 - 网络可以应用标签，改变它们，使用系统特定的政策来解释它们等等
 - 非常擅长保护高优先级流量不受低优先级流量的影响
- 缺点
 - 在一个流量类别内可能过载 - 例如，所有均为高优先级...
 - 所有东西都很重要的时候...就没有真正重要的东西了
 - 在大多数情况下不是限制条件



- 有许多优势
 - 简单
 - 每个数据包的附加位较低
 - 在交换机芯片中实行
 - 分布式
 - 灵活 - 网络可以应用标签，改变它们，使用系统特定的政策来解释它们等等
 - 非常擅长保护高优先级流量不受低优先级流量的影响
- 缺点
 - 在一个流量类别内可能过载 - 例如，所有均为高优先级...
 - 所有东西都很重要的时候...就没有真正重要的东西了
 - 在大多数情况下不是限制条件

DIFFSERV

- DSCP 值映射到交换机中每个输出端口的队列
 - 在 Dante 中心网络，最高优先级队列用于 PTP 流量（非常小的实际数据）
 - 下一级的优先级用于音频数据 -实际数据稍大
 - 在此之下的优先级用于时间关键控制数据
 - 最后一个队列可用于其他任何事情
- 应用此“排序”标准后，交换机中的队列将数据帧发送到线路上
 - 不要忘记这是针对单个交换机的，所以如果想要一致的行为，则所有的交换机都应该有相同的配置
- 非常适合确保高优先级流量不受较低优先级的影响
 - 在每台设备上，PTP 每秒只有几个数据包
 - 而在每个数据流中，音频每秒有几千个数据包

DSCP 值映射到交换机中每个输出端口的队列

在 Dante 中心网络中，最高优先级队列用于 PTP 流量（非常小的实际数据）

下一级的优先级用于音频数据 -实际数据稍大

在此之下的优先级用于时间关键控制数据

最后一个队列可用于其他任何事情

应用此“排序”标准后，交换机中的队列将数据帧发送到线路上

不要忘记这是针对单个交换机的，所以如果想要一致的行为，则所有的交换机都应该有相同的配置

非常适合确保高优先级流量不受较低优先级的影响

在每台设备上，PTP 每秒只有几个数据包

而在每个数据流中，音频每秒有几千个数据包

示例

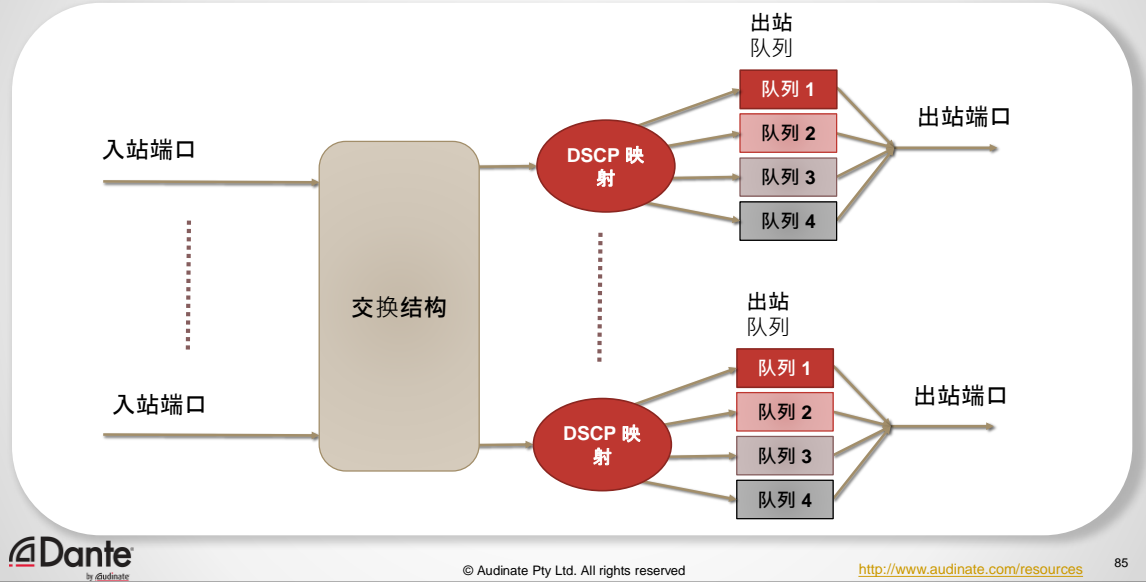
- 航空公司登记柜台或登机通道
 - 根据对航空公司的重要性，客户被分配到一个类别（白金、黄金、其他...）
 - 等同于 DSCP 标签
 - 重要客户有优先值机柜台
 - 等同于专用队列
 - 不繁忙的时候，所有客户都迅速获得服务
 - 繁忙的时候，重要客户迅速获得服务
- 为什么可以这样？
 - 优先客户相对于其他类型较少
 - 优先客户值机和登机时的等待时间最少...
- 在什么时候会失效？
 - 在芝加哥奥黑尔机场国内航站楼，每个人都是铂金客户
 - 如果每个人都很重要，那就没人重要...



航空公司登记柜台或登机通道

- 根据对航空公司的重要性，客户被分配到一个类别（白金、黄金、其他...）
（就像 Diffserve !）
 - 等同于 DSCP 标签
 - 重要客户有优先值机柜台
 - 等同于专用队列
 - 不繁忙的时候，所有客户都迅速获得服务
 - 繁忙的时候，重要客户迅速获得服务
- 为什么可以这样？
- 优先客户相对于其他类型较少
 - 优先客户值机和登机时的等待时间最少...
- 在什么时候会失效？
- 在芝加哥奥黑尔机场国内航站楼，每个人都是铂金客户
 - 如果每个人都很重要，那就没人重要...

简化队列模型



这是一个简化队列模型。

数据包从左侧进入，从右侧离开。

数据包通过交换机。它们到达输出端口，里面有一点小东西，一个小精灵，它看着数据包说，这是 27 号，应该进入 1 号队列。然后有一个算法运行，确保如果 1 号队列收到数据包，则首先服务 1 号队列。如果队列 1 没有内容，就转到队列 2。如果队列 2 没有内容，就转到队列 3。这是一种严格的优先级算法。

队列模式

交换机可以配置为使用不同的算法管理队列：

- 严格优先 - 始终服务最重要的类别
- 加权循环 - 按队列权重分配队列的服务时间
- 成形循环(SRR) - 以统计上成形的形式分配队列的服务时间（思科使用此术语）

如果您要配置 QoS，这些算法非常重要。这一点很重要。在为 Dante 配置 Diffserv 时，人们总是在这里出错。如果您打算使用 Diffserv 或 DSCP，那么您必须确保您使用严格的优先级。因为这是确保 PTP 数据在通过交换机时不会受到阻碍的唯一方式。

还有其他类型的算法：

加权循环：您可以在队列中设置权重，比如说，我给您 20%，给您 20%，给您 60%。它更偏向于一种带宽操纵算法。并且最终会为您的重要流量稍微延迟一段时间，等待下一次到达时再发送。这实际上是消极的。如果您设置错误，它会导致您的网络突然开始表现出非常不同的行为，因为它故意拖延数据包。

在思科，您将会看到 SSR 或成形循环，后者更加复杂。我们不会详细讨论这一点。

队列模式

- Dante 需要对 PTP 流量使用严格的优先级队列
 - 这将确保如果标记为 DSCP 56 的同步数据包到达，它将始终尽快被传递
 - 使用严格优先级可以最大限度地减少 PTP 流量通过系统时遇到的延迟变化，特别是在重负荷情况下
 - WRR 或 SRR 将增加延迟变化并降低 PTP 性能
- 许多数据中心交换机默认设置为 SRR 或 WRR 模式 - 如果在更高规格的交换机产品上使用 QoS，则需要检查此情况

许多数据中心交换机将默认启用该模式。因此，您需要确定您是否使用 QoS，如果您正在使用交换机制造商产品组合中较高级别的交换机，则您可能会发现启用了该功能。或者如果正在使用，您就需要确保它不会造成妨碍。

这是针对具体交换机的。如何配置，如何关闭。您必须联系交换机的具体制造商，了解如何驱动。

DANTE DSCP 值

优先级	使用	DSCP 标签	十六进制	十进制	二进制
高	时间关键的 PTP 事件	CS7	0x38	56	111000
中	音频 · PTP	EF	0x2E	46	101110
低	(预留)	CS1	0x08	8	001000
无	其他流量	BestEffort	0x00	0	000000

选择这些值以便与许多交换机中的默认映射保持一致



Dante 使用的 Diffserv 代码点，我们一开始时已使用了。而这些选择是因为它们映射到大多数交换机的默认号码。

所以我们针对 PTP 使用的十进制数字 56。另一个是用于音频的 46。其他都不重要。

因此，如果您只想在 QoS 世界中进行一项配置，那么您需要配置的只有 PTP。您甚至不用担心音频。

CISCO SG300

- 像Cisco SG300这样的交换机可以非常简单地设置QoS 队列
- 所有出站队列都可以设置为严格优先级
 - 最高优先级队列首先清空，然后是下一个优先级
- 设置起来很简单 - 将交换机设置为 Trust DSCP，然后根据之前的表格分配 DSCP 标记...工作就完成了



SG300 这样的交换机具有非常简单的 QoS 设置，而且功能非常强大及实用。

您可以轻松地将所有出站输出队列设置为严格优先级。如果这样设置，将首先遵循最高优先级，这个队列清空时，转到下一个优先级，清空后再转到下一个优先级。这就可以确保它正常运转。设置起来非常简单。

肯定不是设置复杂的交换机。

其他规格 - TRUST DSCP ?

- 告诉交换机相信终端将正确标记流量，而不是滥用高优先级
- 对于像 Dante 这样的不需要用户配置的服务很有用 - 终端只能生成正确的 DSCP 标签
- 如果我把这个关掉会怎么样？ - 交换机将从所有数据包上“剥离”DSCP 标签并忽略它们
- 大多数校园、企业和运营商网络都不会信任终端 DSCP 标签，而是应用系统管理员定义的策略



那么 Trust DSCP 是什么意思呢？

它非常重要。因为如果您是网络管理员，您每天大部分时间都在思考可能出现的问题。

可能出现问题的是有人将某种东西插入网络中；那种试图假装是别的东西的流量。或者说，“嘿，我是高优先级的，所以我需要得到一种特别的对待，这可能不合适的。”

因此，默认情况下，大多数交换机都设置为不实际信任终端放在数据包上的 Diffserv 代码点。对于 IT 部门来说这是很有用的，因为它可以防止有人做错事，防止有人在网络上造成问题，并且还允许他们在网络上定义策略。但是在设置简单的 Dante 系统时，您需要确保您信任 Diffserv 代码点。因为如果您不这样设置，Dante 系统就会剥离代码点，就不会有任何 QoS。

大多数校园、企业类型的网络都设置为不信任 Diffserv 代码点。在任何情况下，它们会在当数据包第一次到达交换机时将之重新映射到其他一些方案。

其他规格 - DSCP 重新映射

- 许多交换机允许您在入口上剥离或重新映射 DSCP 标签
- 在入口处定义 ACL 并处理匹配的数据包
- 在网络之间的边界非常普遍
- 可用于保护不可信环境中的 PTP，或使 PTP 适合在该网络中运行的方案
- 示例：配合 UDP 端口 319、320、321 上的 PTP 流量，并应用 DSCP 56



重新映射是什么意思？这是指清零数据包中的 Diffserv 值，并将其替换为其他值。这只是一个数字，没有关系，但在那个系统中，他们说数字，比如说 27 是重要的，但是我们的数字是 56。他们会说我们需要把数字 56 变成 27，他们会这样做。这就是他们会做的。这是一个在交换机中编写过滤程序来查找这些数据包的过程，然后通过匹配该过滤程序对它们做些什么。这在网络之间的边界非常普遍。因此，网络服务提供商会在与其他网络运营商共享边界时默认执行此操作。这是控制自己政策的一种方式。当我想要改变某些东西或做一些不同的事时，不需要打电话给另一个网络上的人。

如果您在大型校园环境中运行，并且您确实需要使用 QoS 来保护 PTP，那么这非常有用。您可以对 IT 部门说，“没关系，把它映射到您想要的地方。”我们的数字是 56，如果您可以映射的话；另外，流量在端口 319、320 和 321 上。然后您应用另一个数字。您可以在这里映射任何东西，这就是您需要做的。因此这样会很灵活。

常常会有人问到 Diffserv 代码点值配置。我们会听到，“这个人想要一个不同的数字。”处理方法就是这样做。SG300 就能这样做。这是个以相对较低的价格在

交换机上提供的功能。大多数 IT 管理员都可以操作。

其他规格 - 服务类别 (COS)

- COS, 或者说服务类别, 是什么?
 - COS 依靠第 2 层方法来标记数据帧
 - 802.1q 报头的一部分 (还记得 VLAN 吗?)
 - 只有已标记的 VLAN 流量才会有 802.1q 报头
 - 大多数端点不能生成 802.1q 标记
 - 不是有用的端到端标记, 很可能在流量达到网关的时候会被剥离
 - 注: 即使它们可能发生变化, 但无论链路类型如何, DSCP 值都可以保持端到端
- IPP 或者 IP 优先级又是什么?
 - 支持比 DSCP 更低的分辨率, 因此在较大的系统中使用频率较低



还有一些需要讨论的重点。

在思科交换机中, 您可能会看到有使用服务类别。

COS 依靠第 2 层方法来做 DSCP 和 Diffserv 做的事。它只在以太网层部署。

它是我们之前讨论过的在 VLAN 中使用的 802.1Q 报头的一部分。

如果您还记得之前的内容, 大多数端点不会对它们的数据包标记。

所以, 这意味着这是一个 QoS 机制, 使用起来有点难度。您必须做更多工作来配置。您必须启用标签, 您必须进行处理。

由于 802.1Q 标签被剥离, 它不能进行端到端的工作。它们不会使其脱离 VLAN。它们会进入 VLAN, 但不会出来。因此, 如果您使用服务类别版本而不是 Diffserv 版本, 就难以建立系统。

唯一重要的区别是 Diffserv 将其放入 IP 数据包报头中, 服务级别将其放入以太网报头中。

还有一种称为 IP 优先级或 IPP，支持比 DSCP 更低的分辨率，因此在较大的系统中使用频率较低。网络提供了什么，会决定交换机厂商，决定行业的发展方向，所以您不会在任何地方看到这种情况。

企业级交换机功能

- 在更大（更强大，更昂贵）的企业级交换机上，QoS 可能更“灵活”（也就是很复杂）
- 此类交换机允许网络运营商满足许多不同的业务
 - 利用 IP 中固有的灵活性和功能
- 确切了解特定平台的 QoS 设置如何实施非常重要
 - 最好选择制造商培训课程
 - 这里可能有很多细节



因此，我刚才提到的一个问题是，当您开始使用越来越强大的以太网交换机和路由器时，它们开始导入越来越多的企业类型、数据中心类型的功能，并且有些东西对于 AoIP 不是必需的，而且需要有相当多技能的人来驱动它们或将它们放在一起。

它们可以做很多事情。利用思科队列管理模块，可以实现一些非常强大的功能。但是您不需要对 AoIP 使用这些功能，并且根据我们的经验，它们会导致问题，因为您会过度配置，最终会干扰流量而不是保护流量。这里的目标是保护，而不是阻碍。

所以我要说的是，如果您打算这样做，您就有必要了解这些 QoS 配置将如何影响您的音频。做一些测试。设置，进行配置，并使用 Dante Controller 中显示时钟和延迟的测试工具，以及其他稳定性工具，帮助您确定是否对网络有任何影响。因此，如果您要进行这些配置，请返回并检查并测试，确定您没有损坏它。

在这个特定的领域里有很多细节，这是和特定产品相关的。如果您有 Juniper 的知识，就知道它可能不会全部转移到思科。

它可能会带来不同吗？

- 使用 QoS 将“捕捉”需求中的瞬间“高峰”
 - 这些通常是由未标记的 DSCP 流量造成的
- 如果您通过相关网络链接移动 512 个 Dante 通道，您仍然有“空间”来容纳其他服务（超过 100mbps）
 - 有多少人拥有 100mbps 的互联网连接？
 - 有多少人拥有与 AV 相同的网段上的 100mbps 的互联网流量？
- 您通常需要在网络的某个地方设置一个窄点，才能从 QoS 配置中获得积极的好处
- 在 QoS 配置不必要的环境中，您也可能会看到过度配置的负面影响



那么 QoS 是否会带来不同？

它肯定有助于捕捉需求中的瞬间高峰和保护 PTP。所以如果有人创造了大量的流量，制造大量组播，那么它有助于保护 PTP。这是很值得的。

所以我想提出的一点是，如果通过相关网络链接移动 512 个 Dante 通道 - 那是最大的 Dante 端点，我们的 Dante HC 芯片为 512x512。在那个链路上的速度为 700-750Mbps 左右。您仍然有空间来容纳其他服务（超过 100mbps）

要记住，100mbps 仍然是很多数据。有多少人拥有 100mbps 的互联网连接？有多少人拥有与 AV 相同的网段上的 100mbps 的互联网流量？

您可以使用 QoS 在非常高的饱和点（例如接近 95%）运行链路并保护 Dante 音频。但我会问您为什么要这样做。您可以使用一个 10G 的交换机。这样更便宜，更简单。

但您通常需要在网络的某个地方设置一个窄点，才能从 QoS 配置中获得积极的好处。

如果您能用得上千兆位数据传输通道，那么使用 10G Core 的价格就相当便宜。现在很多交换机都有 10G 上行链路端口。或者建立一个链路聚合组也可以。结合两个链路，建立一个链路，就能有 2G、4G 或者 6G。所以有很多方法可以解决这个问题，不一定需要涉及复杂的 QoS，试图利用链路的最后 10%。

最后一点，如果在复杂而不必要的 QoS 配置中出现问题的话，那么您将看到负面影响。

根据我们提供支持的经验和这个一直以来的问题，这个问题一直是这种支持的重要组成部分。

只需要拿个回形针，重置开关，就能解决，谢谢。

组播

围绕组播，总是有很多问题。组播寻址，组播流量，它是如何工作的，它有什么作用...

我们来回顾一下组播是什么，然后看看我们用来管理组播的技术。

组播 IP 寻址

- 组播组由“组播目的地 IP 地址”来定义
 - 地址范围内的任何主机都可以“侦听”组地址
 - 当接收器数量比发射机多时，就非常有用
- 特别保留的 IP 和 MAC 地址表示组播目的地
 - 以 01:00:5E 开头的 MAC 地址
 - IPv4 范围：224.0.0.0 – 239.255.255.255
 - IPv6 范围：FF00::/8
- 组播 IPv4 地址不会 1:1 映射到组播 MAC 地址
 - 每个组播 MAC 地址最多 32 个组播 IP 地址
- 这使得 L2 交换机难以识别组播流
 - 因此我们要使用“IGMP 侦听”



组播组不是一个“物件”，它只是一个地址，一个组地址。您决定是否作为一个接收设备来侦听这个地址，或者不 - 如果您需要的话。

它可以将音频从一个发射器发送到更多的接收器。

有专门为组播保留的 MAC 地址和 IP 地址 (IPV4 和 IPV6) 特殊地址范围 (IEEE 面向 MAC, IP 面向 IANA)。而当您使用其中一种组播时，就意味着这里的任何数据都将被视为组播而不是单播。

以 01:00:5E 开头的 MAC 地址

IPv4 范围：224.0.0.0 – 239.255.255.255

IPv6 范围：FF00::/8

现在，将 IPV4 地址映射到 MAC 地址时存在一些问题。如果您还记得，您建立的数据包，MAC 地址是由您要发送到的地址决定的，IP 地址也是这个人的 IP 地址。我们必须用组播来复制它。这样每个 IP 地址才能有一个组播 MAC 地址。它们应该是独一无二的，这样您才可以在交换机中管理各种事物。很不幸，这是不

可能的，因为有组播 IP 地址比组播 MAC 地址多。

每个组播 MAC 地址最多 32 个组播 IP 地址

这使得 L2 交换机难以识别组播流。

这就是 IGMP 侦听存在的原因。

它存在于第 2 层，但实际上是第 3 层。有点像 ARP，ARP 也是必须在第 2 层和第 3 层运行。

互联网组管理协议 (IGMP)

- 互联网组管理协议 (IGMP) 是用于在 IPv4 路由网络中管理组播流量的协议
 - IPv6 将 IGMP 替换为“组播侦听器发现 (MLD)”
- 用于帮助管理组播泛滥
 - 没有它，组播流量需要前往所有地方 - 不理想
 - 对于高速率媒体流量来说，组播管理通常是一件好事
- 协议负责确定哪些网络或主机需要特定的组播组
 - 路由器将查询消息发送到每个网络上的所有主机
 - 主机回应它们想加入的群组
 - VLAN 里面有什么？
- 所有 Dante 设备均实施 IGMP（作为主机）



互联网组管理协议 (IGMP) 是用于在 IPv4 路由网络中管理组播流量的协议
IPv6 将 IGMP 替换为“组播侦听器发现 (MLD)”

在 IPV4 中，IGMP 被主机用来对路由器说明，“嘿，我要那个 IP 地址。”

它被用于帮助管理组播泛滥

因为如果我有一个组播数据包，并且我是一个路由器；在我面前有三个网络，并且我知道每个网络上都有一个主机想要这个组播数据包，我会将它发送给这三个 VLAN。一个新的 VLAN 被配置，没有主机需要组播地址，所以我不需要发送。这就是 IGMP 允许我作为路由器执行的操作。

在 VLAN 内，我们尝试使用第 2 层复制相同的内容来尝试建立这些组。然后，以太网交换机可以决定，“哦，这台交换机上只有一台主机需要这个特定的地址，所以我只会将它转发出该端口。”

通过网络传播的位置，它可以帮助管理和控制组播流量。哪些设备最终收到它，哪些设备不会收到。

所以这是一组所有 IP 栈实施的消息。所有 Dante 设备都实施，所有计算机都实施，它是所有 IP 协议栈的标准组成部分。只要您在一个应用程序中执行一些操作，表示：“嘿，我想在 239.254.5.1 上获得流量”，就会有一条消息进入网络并被发送到一个特定的地址。这条消息说：“我是这个主机，我需要这些流量，开始吧。”然后流量就会开始朝您这边过来。

而这个过程还有另一部分保持活跃。所以有计时器参与，这是我们要讲到的重点。最后，第 2 层交换机会监听这些消息，并尝试在第 2 层复制第 3 层的内容。

IGMP 查询器

- 如今的大多数交换机都可以充当 IGMP 查询器
 - 查询器定期向 224.0.0.1 上的所有主机发送查询消息
 - 您想要什么群组地址？
 - 主机以“成员报告”回复至 224.0.0.2（或 224.0.0.22）
 - 我想要 A.B.C.D
 - 每个 VLAN 只能有一个活跃查询器
 - *可以*在一些制造商设备中配置多个查询器
- 中间层 L2 交换机在 IGMP 流量上侦听
 - 成员报告标识哪些接口需要每个组播组
 - 然后交换机将组映射到端口并构建组播转发表
 - 组播流量仅出现在需要的端口上

推动这个过程的就是所谓的 IGMP 查询器。他是那个在网络上工作的人，常常会说：“嘿，谁在听什么？你对什么感兴趣？你对什么感兴趣？”它会到处问这个问题。所有主机都发回信息说：“我还在侦听这个。我还在侦听那个。这个没有了。”这就使查询器能够在网络上产生这些流量。然后系统中的交换机和路由器就可以使用这些消息确定它们需要转发的位置。

大多数以太网交换机都可以充当 IGMP 查询器。如果它们支持 IGMP 的话。大多数都可以。这很重要，因为您需要在网络上有一个查询器才能让 IGMP 工作。所以如何您没打开这个，配置一个查询器，那 IGMP 就不会工作。

查询器定期向 224.0.0.1 上的所有主机发送查询消息

您想要什么群组地址？

主机以“成员报告”回复至 224.0.0.2（或 224.0.0.22）

我想要 A.B.C.D

每个 VLAN 只能有一个活跃查询器

*可以*在一些制造商设备中并行配置多个查询器。

例如，思科拥有可以管理哪个查询器是任何给定系统中的活跃查询器的算法。但重要的是，在任何时间点，任何特定的 VLAN 上只有一个活跃的查询器，这是为了帮助您防止问题并在出现问题时进行调试。

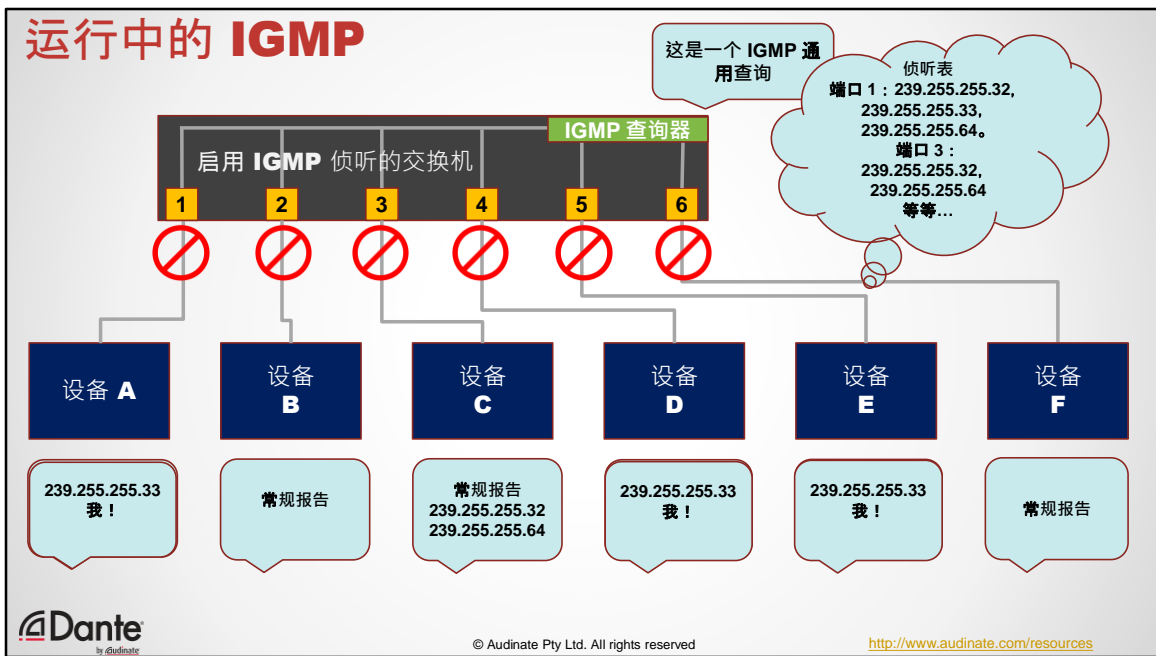
IGMP 侦听部分这个短语是因为第 2 层交换机，即以太网交换机而出现的。它们监测正在通过网络的第 3 层流量，侦听、窥探。它们获取其中的信息，然后将其映射到交换机中获得的 MAC 地址。这意味着它们可以为流经的组播媒体建立转发表，然后决定哪个端口需要接收该数据包。

在默认情况下，当组播数据包进入此交换机时，它会将其转发出所有端口。但是现在我已经构建了这张表，我知道只有 3 个端口需要这个组播流量。我可以做出这个决定，并在其他端口屏蔽它。

这可以非常有效地防止设备接到不想接收的过多流量。

目前在广播领域，关于这一点的重要性就有一个很好的例子。他们正在将生产设施转移到 IP。他们试图通过使用组播在网络上发送未压缩的 4k 广播质量的视频。这就是每秒 6、7、8 千兆。您不希望这些视频到达您的电脑，或任何不想接收它的设备。这就像试图从消防喉喝水一样！

所以他们依靠 IGMP 来管理网络上的组播。



1. 打开 IGMP 侦听将导致交换机屏蔽所有组播
2. IGMP 查询消息必须存在，才能为 IGMP 侦听提供“侦听”对象
3. 在许多现代交换机上，打开 IGMP 侦听也会打开交换机内部的查询器（如在 SG300 上）
4. 查询器发送查询，设备（接收器）发送“报告”
5. “侦听器”根据查询和报告构建转发表
6. 查询器发送两种主要类型的查询
 1. 一般查询 - 询问接收设备感兴趣的组播组
 2. 组特定查询 - 询问谁对特定组播组感兴趣
7. 设备发送报告以回应查询
8. 当设备连接时，它会发送一个“未经请求”的报告
9. 这意味着一旦设备连接，IGMP 侦听器就会转发组播组（无需等待查询器）

优化 IGMP 侦听

- 运行 IGMP 来管理 IPv4 组播涉及：
 - 网络查询器中的特定角色
 - 计时器：查询间隔·超时等
 - 特定组播地址：224.0.0.1, 224.0.0.2, 224.0.0.22 等
 - 多个版本：IGMPv2, IGMPv3 等
 - 来自不同交换机厂商的协议实施 - 厂商特定的优化：例如 fast leave, 查询代理等。
- 这可能很复杂...
 - 特别是如果您开始随机更改定时器或交换机配置
 - 随机变化将产生随机效应



那么我刚才讲的听起来非常简单、稳定。我作为查询器，每隔一段时间发送一条消息，作为主机，我侦听消息，然后将它们发回，然后因此，我得到我想要的内容。

但要实现这一点，就需要用很多定时器。并在 IGMP 实施中使用控制和参数。

以 SG300 为例，可以看出都包括些什么。您必须全部设置，并且要设置正确。默认值对大多数事情而言是可用的。但我们经常接到这样的支持电话 - 人们会说：“音频需要很长时间...，有些东西发生了变化，有些事情要再等 30 秒才能发生。”这一般是因为计时器时间太长、太短、超时等等的结果。

调整网络协议中的定时器是一项具有挑战性的任务。

要运行 IGMP 来管理 IPv4 地址。它在网络中具有特定的角色：

您必须选择某个人作为查询器。您要为这个人设置特定的参数。您必须选择：查询间隔，即我发送查询的频率。

为了等待每个人的回复，我要等多久？或等待这个人回复？或这个人？

我该如何处理网络中已知的特殊地址？组播 DNS 就是其中之一。M-DNS 使用该组播范围内的特殊地址。它由 IANA - 互联网寻址人员分配。您必须将其与其他组播流量区别开来。我还必须处理不同版本的 IGMP：v2 和 v3。大多数人认为版本号越高越好。并不总是这样。IGMPv3 听起来很不错，但是您会意识到它实际上并没有给您额外的好处，所以为什么要自找麻烦呢。

您会发现最重要的事情就是 IGMP，因为它是专为在路由基础设施中使用而设计的第 3 层协议。这个没关系，因为在这方面是有标准的。但是，涉及到侦听元素，以及如何将该协议映射到第 2 层交换机时，就要视具体的厂商而定了。它们会以适合其特定交换机体系结构的方式配置。因此，惠普、博科、瞻博网络、思科等等设备的行为会略有不同。有很多可以调整的地方。

所以我的意思是，如果您开始调整各种配置，这就可能会很复杂。

所以我想谈谈您可以做哪些简单的工作来帮助您的 IGMP 系统工作。高效，快速，避免所有陷阱和问题。

简化的处方

- 将查询器间隔设置得较短 - 15 或 30 秒即可
 - 最大限度地减少音频间隙，提高响应速度
- 保留默认设置的超时值
 - 在大多数情况下，越长越好
- 确保每个 VLAN 只有一个活跃查询器。
 - 理想情况下，这是一个核心网络交换机或路由器端口
 - 症状：音频断断续续
 - 诊断：Wireshark 显示来自多个来源的 IGMP 查询消息



© Audinate Pty Ltd. All rights reserved

<http://www.audinate.com/resources>

下面是简化的处方：

使用较短的查询间隔即可。对于很多应用程序来说，这不是您该做的事情，但在 Dante 的音频应用程序中，这很好。因此，运行一个非常短的查询间隔，比如 30 秒，是可以的。

这将有助于保持系统状态的更新。这样一来，当事情发生变化时，会很快得到反映。如果缺少了某些东西，或者出了什么问题，就有机会修复它。

不要在任何实施中改变超时值。不要改变。如果您已经这样做了，我们会要求您将回形针放入交换机中。通常，更长的时间会更好，让超时需要更长时间才发生，但更改超时对响应性并没有帮助。这会增加事情失败的可能性。到时候就没有音频了。

您需要确保每个 VLAN 只有一个活跃查询器。我说这点的原因是在这里涉及定时器。如果它们的配置不同，并且网络中存在不同的转发行为，则最后可能会是

不同的状态。这样一来，物件可能会在短时间内消失或永不消失。（您想要组播流，然后取消订用）。

所以最好的做法是每个 VLAN 只有一个查询器。思科提供了用于管理这方面的工具。其他厂商也有。还有一点需要补充的是，如果您要在 VLAN 中运行 IGMP 侦听，请使用常见的交换机厂商的设备。可以只用思科，只用惠普，只用瞻博网络。不要混搭。

VLAN 上有多个活跃查询器可能导致第 2 层网段出现我们称之为“组播路由翻转”的情况。

理想情况下，您应该将 IGMP 查询器作为核心交换机或路由器端口。

您必须使用 Wireshark 来诊断这个问题。如果您遇到问题，并且您怀疑是 IGMP 导致此问题。而您要寻找的是来自多个来源的多个查询消息。

简化的处方

- 避免使用 fast leave
 - 不能带来任何好处
- 避免使用 IGMP 代理
 - 除非您确定知道它会有何表现
- 确保 Netgear 交换机上未设置“阻止未注册的组播”
 - 阻止不应该阻止的流量 (mDNS, PTP)
- Dante 设备支持 IGMPv3



© Audinate Pty Ltd. All rights reserved

<http://www.audinate.com/resources>

避免使用称为 Fast Leave 的功能。这个功能不会给您带来任何好处。

IGMP 也允许您写代理。什么是代理？代理服务器是以捕获从一个方向来的信息并缓存，然后查看反方向的信息，然后说“哦，我知道，我会为您回答...”，而您就不必回答了。这个功能很好，但它不起作用的时候就不行了。当代理不起作用时，那就问题大了。因为您可以想象，如果您缓存每一个长时间停滞的单个 IGMP 查询，您就会累积很多问题。所以不要使用 IGMP 代理。有实行代理的交换机，请关闭其中的 IGMP 代理功能。

我对 Netgear 的意思是相同的，所以我想对在 Netgear 工作的任何人表示歉意，但请解决这个问题。在 Netgear IGMP 实施中有一项功能叫做“组织未注册的组播”。我之前提到了特殊的组播地址。M-DNS, PTP。它们是互联网部门分配给这些服务的地址。您不应该注册这些地址。事实上，我们的本意也不是让您注册这些地址。而当您在交换机中启用组播过滤时，您也不应阻止它们。但是这在 Netgear 交换机中的作用是阻止 M-DNS、PTP 等等。如果您在运行 Netgear 交换机时看到一个症状，然后您说“我有 Dante 设备，但是我能看到它，然后我不能”，或者“我看不到其他东西。我只能看到这个名字，但之后不能...”这很可能就是

原因。所以请务必关掉它。

请注意，Dante 设备支持 IGMPv3，但我们不使用任何 v3 功能。

IGMP 侦听性能考虑因素

- 请记住 - 交换机使用 MAC 地址表进行操作
- 每个 MAC 地址可能有多个 IP 地址
 - 工作需要由交换机完成，以便解决这个问题
- 一些交换机还使用 CPU 来转发组播流量
 - 这可能导致转发延迟发生变化
 - 随着组播量的增加，可能会导致过载
- 这意味着一些交换机可能在处理组播时很慢
 - 可能会导致组播音频或 PTP 无法接受的延迟
- 常见症状包括：
 - 设备周期性失去同步
 - 收到组播流时音频不稳定



© Audinate Pty Ltd. All rights reserved

<http://www.audinate.com/resources>

运行 IGMP 的交换机上进行着大量工作。如果您仔细想想，现在必须寻找特定类型的消息。它必须捕捉它们，解释它们，研究如何改变它的路由表。然后更改路由表，并确保一切都保持最新状态。

因此，如果涉及交换机 CPU，可能会影响交换机的性能。因此，如果组播管理涉及通过交换机的管理 CPU（不幸是，这的确发生在很多交换机中），那么就转发延迟或延迟可变性而言，这便是性能下降。

在这张幻灯片上，我们记录了这些信息。使用 CPU 转发组播流量对整体性能不利。价格更昂贵的交换机有禁用此功能的选项。例如博科的交换机就可以。按照默认设置，它们会使用 CPU 转发组播。但是您可以把它关掉，然后放回到硬件中。而这样做会给您与单播相同的性能，这就是您所需要的。

这对事情的影响大多数在 PTP 方面。您可能会注意到 PTP 直方图中的某些时钟传播。它不会是一条直线，而是会上下浮动。或者在极端的情况下，音频中可能出现一些漏失。

这种情况是需要留心并避免的。

在这方面，不是所有交换机都一样。一般而言，价格越高，交换机就越好。

组播传播

- 网络通过 L3 核心网络提供 L2 VLAN 是常见的要求
 - 在这些环境中，组播有时是一个挑战
 - 许多系统管理员都不喜欢组播流量出现
- PTP 希望网络的转发延迟保持一致和对称
- 有些情况下，可能不会这样
 - 非对称非组播技术，如 MPLS、GPON 等
 - ACL 配置不正确等
- 常见症状包括：
 - 多个 PTP 主时钟
 - 设备无法保持同步
- 打开所有设备的单播延迟请求有助于诊断并可能解决问题



© Audinate Pty Ltd. All rights reserved

<http://www.audinate.com/resources>

组播的另一个挑战领域是当您尝试通过路由器核心穿通 VLAN 时。正如我之前提到的，IT 部门真的不喜欢这样。他们会对此感到有点恼火。但思科拥有一种非常好的技术，叫做 VXLAN。

组播在这些环境中可能是一个挑战，通常情况是，通过 2 层中继、隧道或其他实施方式，您无法获得所有的组播。

这是一个方面，您可能会看到 PTP 性能的某些变化，或者您可能会看到比如 Dante 报告说网络中有多个时钟主控的情况。而这里的症状实际上是与组播流量不通过这些链路传播有关。

现在还有像 GPON、MPLS 这样的网络连接技术。这些技术通常是不对称的，不是为组播或反向组播设计的。有许多不同的应用程序可能会阻止组播从网络中间的某个地方通过，到达边缘，然后再返回。

您可能还会遇到一个 IT 人员成为安全方面的纳粹，对一切应用 ACL，而这会造成破坏。

因此，您可以在组播环境中看到这些情况，通常会导致：

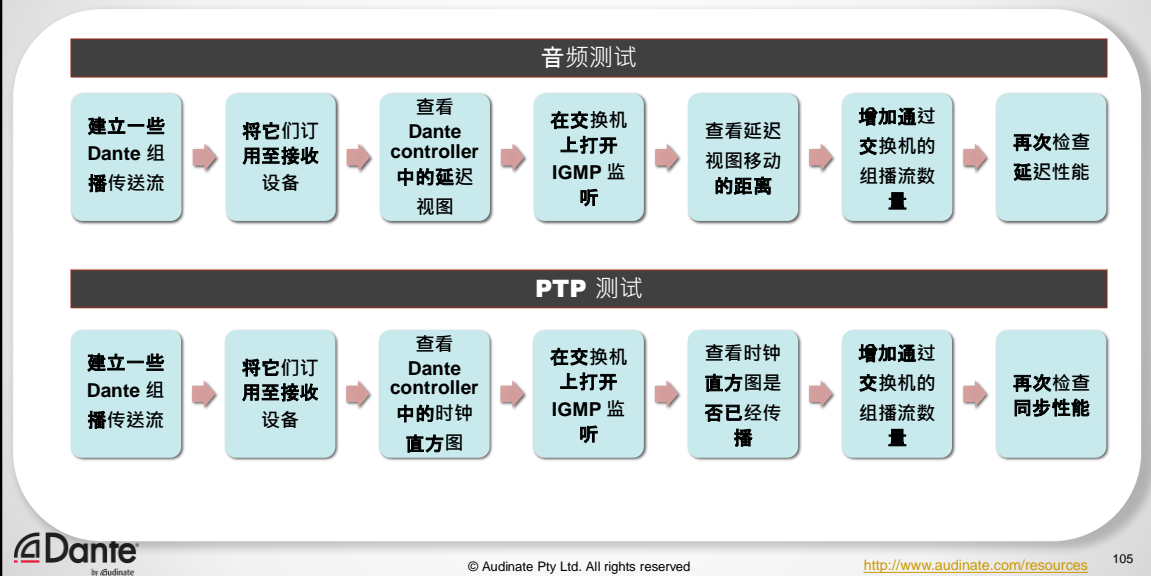
PTP 中断
音频漏失

Dante 设备出现或消失

要记住这三种症状。

帮助诊断这些问题的一种方法是使用 Dante 内置的新功能，现在称为“单播延迟请求”。您将在任何设备的“设备配置”选项卡的“设备视图”中看到。您可以打开此功能，在所有设备上打开，如果突然开始计时，您就知道该网络中存在组播分发问题。因为它将 PTP 转换为使用单播。这是一个帮助诊断这些类型问题的功能。

测试组播交换机性能



如果您的交换机可以执行转发组播流量的任务，那么这里是一个诊断方法。使用延迟图和时钟直方图测试音频，然后测试 PTP。

音频测试

- 建立一些 Dante 组播传送流
- 将它们订用至接收设备
- 查看 Dante controller 中的延迟视图
- 在交换机上打开 IGMP 监听
- 查看延迟视图移动的距离
- 增加通过交换机的组播流数量
- 再次检查延迟性能

PTP 测试

- 建立一些 Dante 组播传送流

将它们订用至接收设备

查看 Dante controller 中的时钟直方图

在交换机上打开 IGMP 监听

查看时钟直方图是否已经传播

增加通过交换机的组播流数量

再次检查同步性能

高级 DANTE 联网：章节 5

在本节中...

了解 **Dante** 的网络资源

- Dante 使用的带宽
- 拓扑对带宽使用的影响



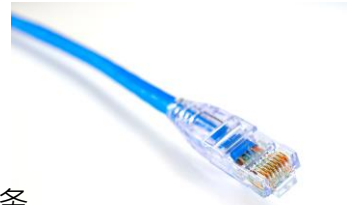
定义资源要求

- 任何项目都需要这一阶段的规划
- Dante 网络所需的资源：
 - ✓ 足够的传输流，以便为所有接收器提供服务
 - ✓ 足够的带宽，以便传输流量
 - ✓ 畅通无阻的逻辑连接（“连线”未切断，并“插入”）
 - ✓ 连接到发射机的设备上有足够的接收流量可用



DANTE 放到线路上的数据

- 为了制作完整的音频网络解决方案，我们需要：
 - 音频传输
 - 时钟
 - 设备发现
 - 设备和路由控制
- 使用以太网 IP 模式可以让我们在 1 根电缆上完成此任务
- 有些设备也使用同一根线缆供电！
- OSI 模型提供了一个非常整齐的框架

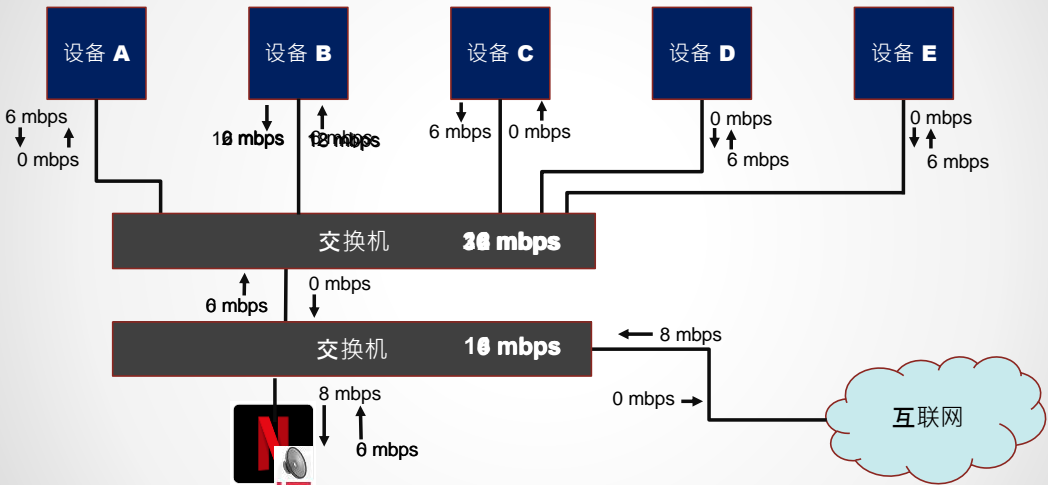


构建原则

- 构建网络时需要考虑的主要因素是什么？
 - 确定所需的服务
 - 带宽利用率
 - 为预测的带宽需求指定最佳基础架构
 - 识别潜在的“瓶颈” - 在设计中避免或管理
 - 确保架构可扩展（网络将随着时间的推移而增长）
 - 了解可能的未来服务要求
- 这个列表较长，难度较高 - 但幸运的是，我们有既定的“规则”



带宽利用率 - DANTE 流量



- 1.设备 A 向设备 B 发送信号
- 2.设备 C 向设备 B 发送信号
- 3.设备 B 向设备 D 发送信号
- 4.设备 B 向设备 E 发送信号
- 5.我们扩展网络 (添加 Internet 连接)
- 6.我们从互联网上传输 Netflix
- 7.我们将 Netflix 的音频发送到设备 B (DVS)

了解资源 - 带宽

- 流是发送到某个 IP 地址/端口的一系列数据包
- 单播流包含 4 条通道
 - Ultimo2 设备上有 2 条通道
 - 采样率为 48KHz 时，单播流使用 6Mbps 带宽
 - 如果只有一条通道被“订用”，则其他 3 条通道被“发送”为静音
 - 随着其他通道被添加到 2 个设备之间，来自连续通道的音频内容“转储”到流中
 - 如果现有流存在“空白”，则不会建立新流
- 一个组播流最多包含 8 条通道
- 采样率为 48KHz 时，组播流使用最多 12Mbps 带宽
 - 流中只包含选定的通道
 - 无法在现有的组播流中添加新的通道
 - 避免建立多个遵循相似路径的“单通道”组播流

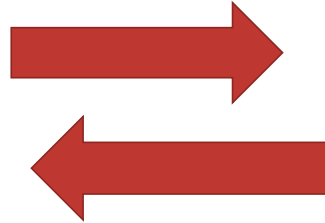
了解资源 - 流



- 流的限制是内部设备资源的限制
- 不同的设备类型有不同的限制
- 对于设备而言，无论流是单播还是组播都无关紧要（因为目标 IP 地址只是简单地改变）

了解资源 - 流

- 每个 Dante 设备都有一些可用的“发送流”和“接收流”
 - Ultimo 设备有 2 个发送流和 2 个接收流
 - Dante Virtual Soundcard 具有 16 个发送流和 16 个接收流
 - Brooklyn II 设备具有 32 个发送流和 32 个接收流
 - Dante PCIe 卡具有 32 个发送流和 32 个接收流
 - Dante HC 设备具有 128 个发送流和 128 个接收流
- 流被用于提高系统的整体效率



了解资源 - TX 流

- Tx 流的建立方式有两种

在单播模式下 -

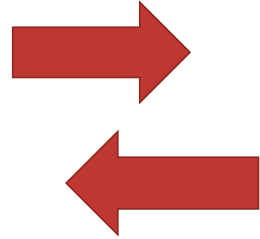
- 当接收设备请求一个 (或多个) 通道时, 建立 Tx 流
- 如果存在空间, 通道被添加到现有的 TX 流
- 一个单播流最多可以包含四个通道

在组播模式下 -

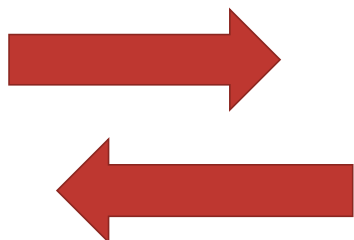
- Tx 流会立即建立 (不需要接收设备来请求)
- 一个组播流最多可以包含八个通道
- 无法将通道添加到组播流

- 所有 Dante 流默认都是单播

- 只有有意编程才能建立组播流 - 在 Dante controller 中 - 这是由人工完成的



了解资源 - TX 流



- Dante 流默认为单播
- 向多台设备分发相同内容时可以使用组播实现优化
- 当通道成为组播时 - 这些通道将在新的组播流中传输
- 如果设备正在使用全部流 - 接收设备不能再订用
- Tx 流使用情况在 Dante Controller 的“传输”选项卡上显示



© Audinate Pty Ltd. All rights reserved

<http://www.audinate.com/resources>

当您将一个通道添加到已有的组播流时，接收器将切换到使用组播流。订用单播，建立组播，接收器设备切换。删除组播，接收器恢复为单播。在删除组播流之前将有一个警告，告诉您会发生这种情况，包括音频中断。值得展示。

了解资源 - RX 流

- 每次建立以下订用时，接收设备都将使用新的 RX 流资源：

- 需要发射机上新的单播流，或者
- 是一个已经在组播流中的通道的第一个订用



- Rx Flow 使用情况在 Dante Controller 的“接收”选项卡中显示



这里需要一个例子...第二个单播通道对比第五个单播通道和新的子到组播通道

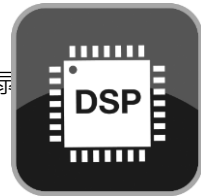
简单的网络资源利用



回顾

音频网络由三个元素组成：

- 建立流的设备（麦克风、音箱、DSP、播放源等）
- 承载数据的基础架构
- 接收流的设备（DSP、放大器、有源扬声器、录像机等）



© Audinate Pty Ltd. All rights reserved

<http://www.audinate.com/resources>

音频网络由三个元素组成

建立流的设备（麦克风、音箱、DSP、播放源等）

承载数据的基础架构

接收流的设备（DSP、放大器、有源扬声器、录像机等）

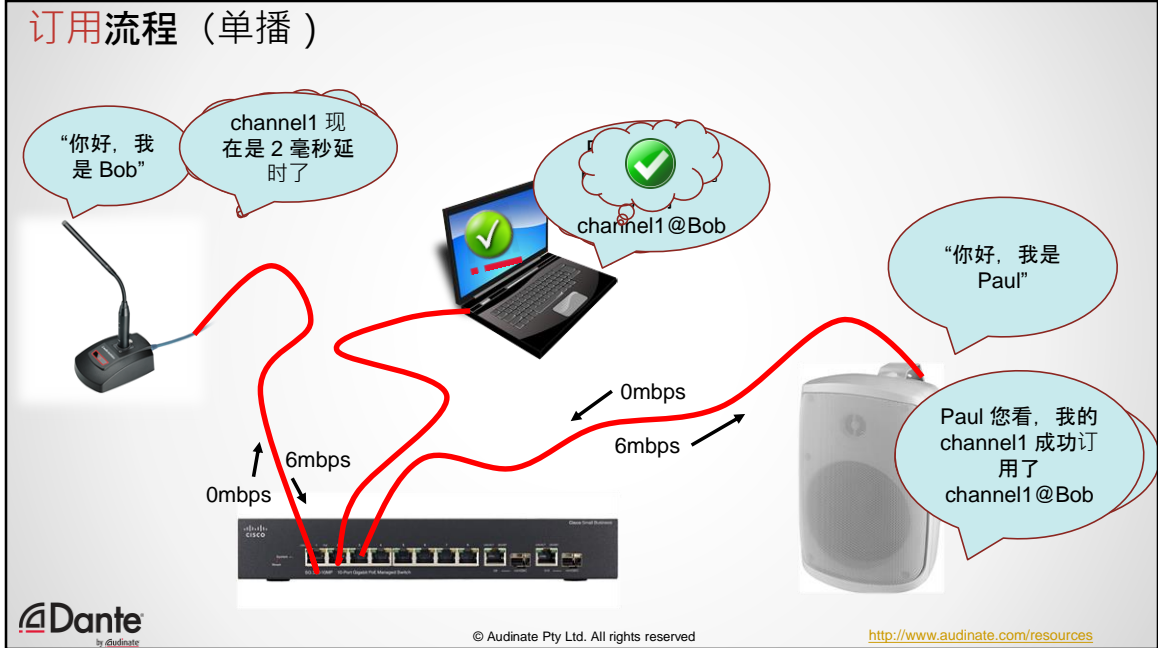
高级 DANTE 联网：章节 6

在本节中...

在 **Dante** 中订用

- 订用流程
- 组播订用
- 拓扑和 QoS



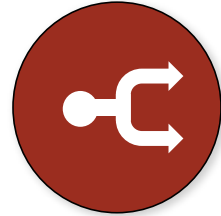


1. 将笔记本电脑 (运行 Dante controller) 插入交换机
2. 将麦克风插入交换机
 1. 麦克风“公布”自己 (组播)
 2. Dante controller“得悉”通知并填充路由页面
3. 将扬声器插入交换机
 1. 扬声器“公布”自己 (组播)
 2. Dante controller“得悉”通知并填充路由页面
4. 我们决定将 Paul 订用到 Bob (从 Dante Controller)
5. Dante Controller “告诉”Paul 向 Bob 索取 channel1
6. Paul 向 Bob 询问 channel1 的延时设置
7. Bob 检查并确定延迟设置 = 或 > 自己的设置
8. 如果是这样, 则 Paul 的延时会产生流
9. 如果不是, 则使用 Bob 的延时建立流

10. Bob 和 Paul 之间使用 6mbps 带宽 (单向)
11. 交换机和计算机之间的线缆使用 0mbps 带宽
12. Paul 报告订用“良好” (组播)
13. Controller 更新记录 (绿色勾号)

组播订用

- Dante 流默认为单播 (有充分理由)
- 在单播中 - 仅在接收器和发射器之间使用带宽 :
 - 当进行有效订用时
 - 并且在接收器和发射器之间的最短路径上
- 当建立组播流时
 - 它不关心接收器
 - 如果没有用户 - 它仍然使用带宽 - 无处不在 (在非管理网络中)
- Dante 不能从单播动态切换到组播
 - 但是如果在单播订用已经建立之后再建立组播流 , 则切换为使用新的组播流



- Dante 流默认为单播 (有充分理由)
- 在单播中 - 仅在接收器和发射器之间使用带宽 :
 - 当进行有效订用时
 - 并且在接收器和发射器之间的最短路径上
- 当建立组播流时

- 它不关心接收器
 - 如果没有用户 - 仍然随处使用带宽
(在非管理网络中)
- Dante 不能从单播动态切换到组播
 - 但是如果在单播订用已经建立之后建立组播流，则它们将切换为使用新的组播流

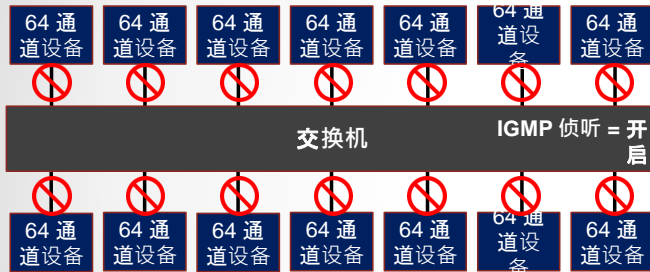
示例 - 在 DANTE 网络中



- 如果所有设备都设置为完全组播
- 交换机仍能承受...但设备就不能了!
- 每个最多32个流受每个节点的单播带宽限制了
- 8x12 mbps 组播流 = 96mbps x 14 节点 = 1.344 gbps
- 超过每条电缆的接收带宽仍然
- 但仍然只占4.8%的背板带宽
- 交换机承载通道到一个网络,就会“泛滥”,最大可能接收64个通道似乎是一个巨大的问题...
- 可能的“最差”流结构 = 一个设备上 有 32 x 2 个通道流
- 单播只能实现“2路”分裂

1. 14 台设备，每台设备 64 个通道，每个通道 32 个流
2. $32 \times 6 =$ 每节点最大单播带宽 = 每节点 192mbps
3. $192 \times 14 = 2688\text{mbps} =$ 超过一千兆比特
4. 单播每节点最大 Rx 带宽仍然是 192 mbps (流不足)
5. 交换机的最低背板带宽为 28 gbps (仍超过 10 倍的实际带宽)
6. 可能的“最差”流结构 = 一个设备上有 32 x 2 个通道流 (仍然发送 64 个通道)
7. 单播只能实现“2路”分裂
8. 如果所有设备设置为完全组播 - 交换机仍能承受...但设备就不能了!
9. $8 \times 12 \text{ mbps}$ 组播流 = $96\text{mbps} \times 14$ 节点 = 1.344 gbps = 超过每条电缆的承受力! 但仍然只占 4.8% 的背板带宽
10. 发送 832 个通道到一个网络, 就会“泛滥”, 最大可能接收 64 个通道似乎是一个巨大的问题...

我们来修改一下原始示例



- 在 IGMP 侦听关闭、所有设备组播的情况下 - 我们试图在每个千兆位线缆传输 1.344 gbps
- 很明显这是做不到的！
- 打开 IGMP 侦听
- 每个设备只能订用 32 个流 - 这是最大带宽，每个端口 384 mbps
- 背板带宽保持不变，约占 4.8% 的容量
- 这就是为什么组播管理总是优先于 QoS 的原因

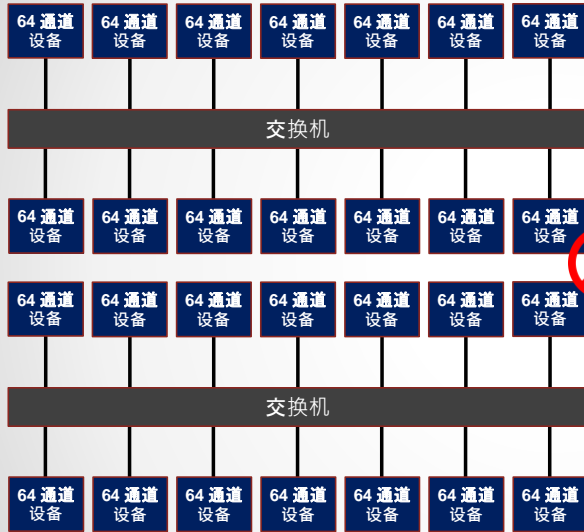


© Audinate Pty Ltd. All rights reserved

<http://www.audinate.com/resources>

- 请记住 - 在 IGMP 侦听关闭、所有设备组播的情况下 - 我们试图在每个千兆位线缆传输 1.344 gbps
- 很明显这是做不到的
- 打开 IGMP 侦听（假设查询器正在工作）
- 每个设备只能订用 32 个流
- 这是最大带宽，每个端口 384 mbps（在现实中这是不可能的）
- 背板带宽保持不变，约占 4.8% 的容量（没有竞争）
- 这就是为什么组播管理总是优先于 QoS 的原因（按重要顺序）

DANTE 与 QoS



- 假设顶部交换机上的所有 14 个设备正在以 1:1 映射传输到底部交换机上的 14 个设备
- $14 \times 64 = 896$ 个通道
- 每个设备 16 个流 @ $6\text{mbps} \times 14 = 1344\text{mbps}$
- 简单来说 - 在千兆级链路上... 带宽耗尽了！
- **解决方案是什么？10 千兆级链路 - 问题解决了！**
- 所有这些设备都在传输恒定的数据速率
- **QoS 在这里毫无作用！**



假设顶部交换机上的所有 14 个设备正在以 1:1 映射传输到底部交换机上的 14 个设备

$14 \times 64 = 896$ 个通道

每个设备 16 个流 @ $6\text{mbps} \times 14 = 1344\text{mbps}$

简单来说 - 在千兆级链路上...

带宽耗尽了！

解决方案是什么？10 千兆级链路（绝不荒唐）

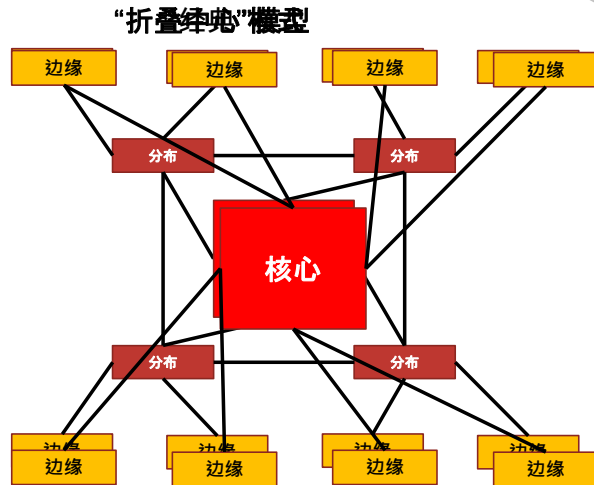
问题解决了！

所有这些设备都在传输恒定的数据速率

QoS 在这里毫无作用（它不是解决方案）

拓扑和 QOS

- 前面的示例显示了由次优拓扑建立的瓶颈
- 幸运的是，已经有成熟的网络拓扑结构设计方法
- “三层分层模型”描述了这个概念
- 随着交换机和路由器速度的增加，“折叠中心”(collapsed core)已经变得更加正常



- 前面的示例显示了由次优拓扑建立的瓶颈
- 幸运的是，已经有成熟的网络拓扑结构设计方法
- “三层分层模型”描述了这个概念
- 随着交换机和路由器速度的增加，“折叠中心”已经变得更加正常

高级 DANTE 联网：章节 7

在本节中...

高阶时钟

- 网络如何与媒体时钟同步？
- 外部时钟有什么作用？
- 网络同步
- 时间同步
- PTP 中的时间



高阶时钟

网络如何与媒体时钟同步？

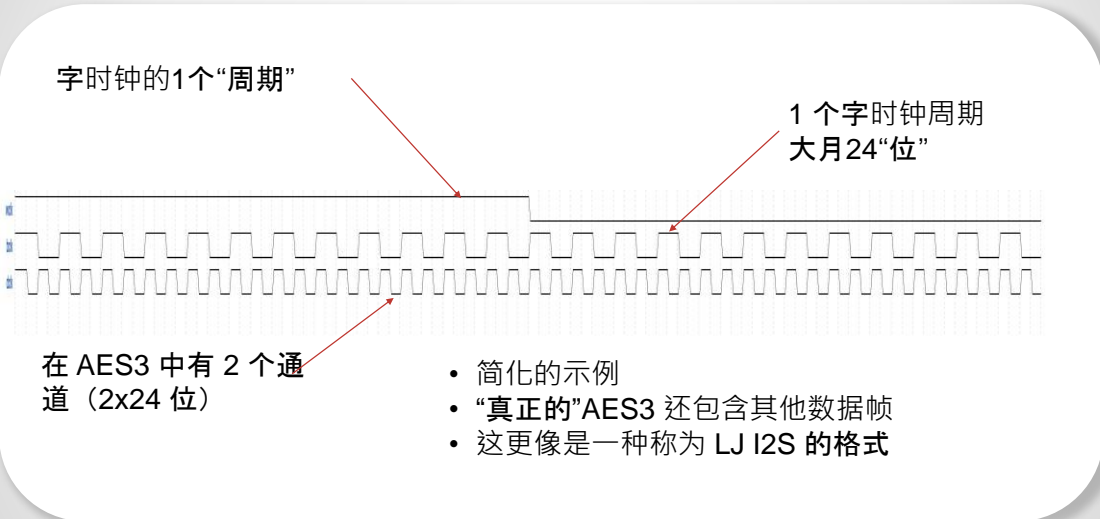
外部时钟有什么作用？

网络同步

时间同步

PTP 中的时间

网络如何与媒体时钟同步？



在第1级中，我们介绍了在基本数字音频部分中需要“字时钟”的问题

字时钟定义了“字”的开始，它是组成数字样本的二进制数字组

字时钟不定义“比特深度”，仅仅定义比特串的开始

字时钟处于采样率

那么...我们的“传统”数字设备如何理解这一点？

人们普遍认为，给设备赋予“外部”字时钟取代了其“内部”时钟

并没有！

请考虑 24 位的 48KHz AES 音频对

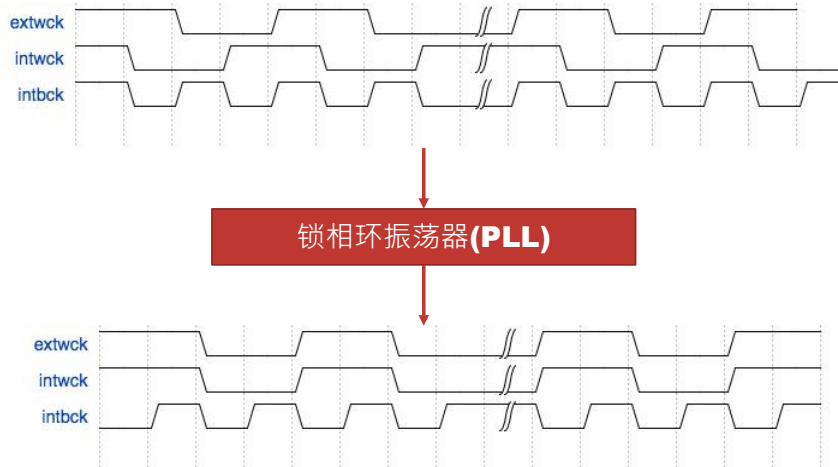
字时钟将每秒钟脉冲 48,000 次

但数据是 $24 \times 2 \times 48000$ (位 x 通道 x 采样率)

这意味着 2 个音频通道的数据速率为 2.3Mbps

这意味着要运行一个计数器来捕获这些位，接收数据的设备必须有一个更高频率的时钟

外部时钟有什么作用？



外部字时钟肯定是有作用的！

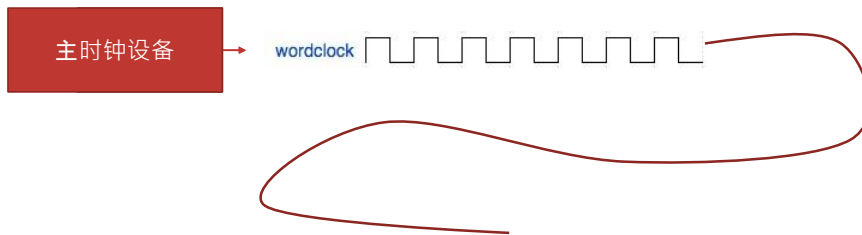
我们从基础实验中了解到了这一点

如果我们没有主时钟和从时钟，我们会收到爆裂声和/或没有音频

外部时钟更像是一个同步参考

外部时钟允许从设备将其内部时钟振荡器与主设备的内部时钟振荡器对准

分布式字时钟如何工作



- 速度=距离/时间 信号在 1uS 内传播多远？
 - $2.8 \times 10^8 \times 1 \times 10^{-6} = 280\text{m}$
- 我们多久需要在这段距离上同步一次？
- 在直播声音和广播中 - 很多时候（比如高尔夫、足球、体育场演唱会、赛车运动...等）
- Dante 保证网络中任意点的微秒同步...。如何做到这一点？

通常，主时钟设备向线缆发送脉冲

该设备可以是音频设备，也可以是专用主时钟

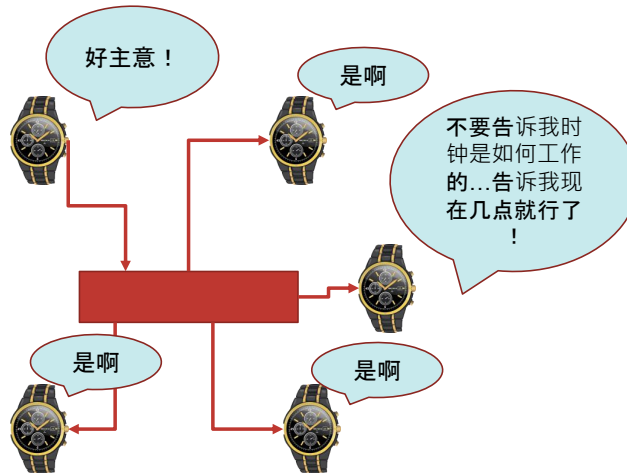
主时钟设备必须连接到其所有从设备

如果主设备被移除/失败，则从设备将停止同步

考虑通过线缆的传播时间

补偿这个时间不是“标准”字时钟的一部分

网络同步



数字时钟的概念是为了保持设备的时间正确

传统系统上分配了时钟

在现代网络系统中 - 时间可以分布

分布式“时间”具有许多独特的优点

时间是以小时、分钟、秒、毫秒为单位表示的（正如我们理解的那样）

时钟只是一秒钟的脉冲数 - 没有“挂钟”时间的概念

同步时间



- 通过网络分配时间的想法始于英国铁路公司
- 随着铁路网络的增长 - 有必要制定时间表
- 一辆火车随便出现，在任何时间离开，这是不能接受的 - 想想这是多么麻烦的事！
- 这个问题是如何解决的？（记住 - 当时没有电话！）

通过网络分配时间的想法始于英国铁路公司

随着铁路网络的增长 - 有必要制定时间表

一辆火车随便出现，在任何时间离开，这是不能接受的 - 想想这是多么麻烦的事！

这个问题是如何解决的？（记住 - 当时没有电话！）

同步时间



Dante
by audinate

© Audinate Pty Ltd. All rights reserved

<http://www.audinate.com/resources>

134

简单...

他们会在火车上放一个“参考时钟”

每个火车站都有一个车站时钟

车站站长尽可能精确地对准火车上的钟（真正的时钟，并带进他的办公室）设置车站时钟

火车继续前行 - 在下一站重复这个过程

每隔一段时间都会重复这个过程以保持车站“时间正确”

“标准时间”就是这么来的

PTP 的工作原理也差不多！

PTP 中的时间

- 当然 - 在几秒钟内同步远不足以满足音频传输的需要！
- 幸运的是, IEEE1588 (又名 PTP 精确时间协议) 好多了！
- IEEE1588 的准确率为纳秒
- PTP 主设备提供参考时间
- 它将这个参考时间传输到网络上 (相当于列车)



当然 - 在几秒钟内同步远不足以满足音频传输的需要！

幸运的是, IEEE1588 (又名 PTP 精确时间协议) 好多了！

IEEE1588 的准确率为纳秒

PTP 主设备提供参考时间

它将这个参考时间传输到网络上 (相当于列车)

PTP 中的时间

- 铁路系统的问题是，时钟必须放到列车上，然后从列车上拿下来 - 一次只能有一个火车站同步
- 如果我们能够同时同步，会不会更好？
- 幸运的是，在网络上，这正是我们所做的
- 就像铁路一样 - 消息在网络上传播需要时间 - 而 PTP 也照顾到了这一点！



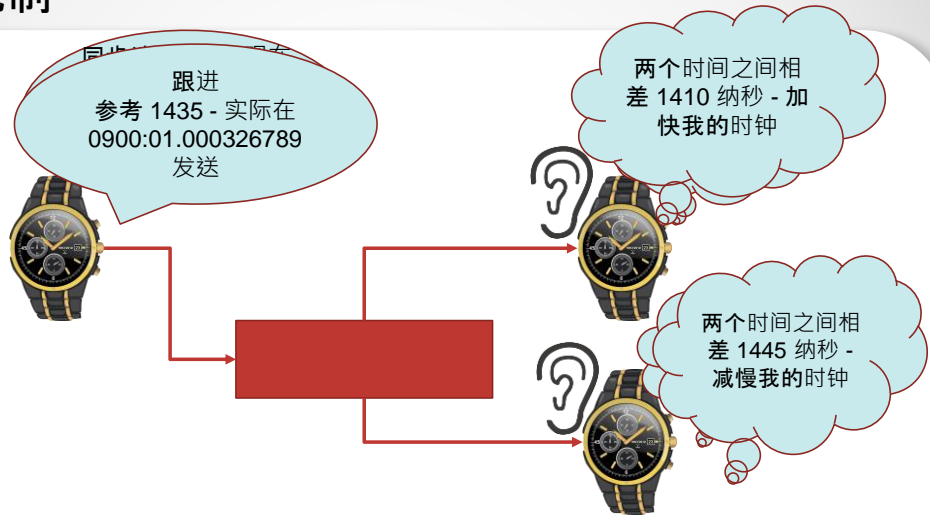
铁路系统的问题是，时钟必须放到列车上，然后从列车上拿下来 - 一次只能有一个火车站同步

如果我们能够同时同步，会不会更好？

幸运的是，在网络上，这正是我们所做的

就像铁路一样 - 消息在网络上传播需要时间 - 而 PTP 也照顾到了这一点！

PTP 机制



主时钟发送同步消息

基本上就是：“你好，这是同步消息 1435，现在是 2017 年 5 月 8 日星期一 09:00:01.000325364”

然后，从设备就可以设置它们各自的计时器

但是 - 我们试着让这些计时器一致

每一次，都会有一个计时器的“速度”与其他略有偏差

如果我们能传达这些信息，不是会更好吗？

PTP 就思考过这一点！

主时钟发送同步跟进消息

该消息表示 - 参考消息 1435, 实际上是在 2017 年 5 月 8 日星期一 09:00:01.000326789 发送的

然后, 接收时钟可以将接收到 *同步* 消息的时间与 *跟进* 消息说明的实际时间进行比较, 以确定其是否比主时钟运行速度更快或更慢

PTP 必须在整个网络上运行

- 我们了解到，数据帧可能相互带来轻微的阻碍
- 对于 PTP 数据帧也是这样的（它们并不会魔法）
- 实际上，从设备需要对从主设备收到的消息“取平均值”，而不是“直接下结论”
- PTP 也考虑如何在网络中保持稳定

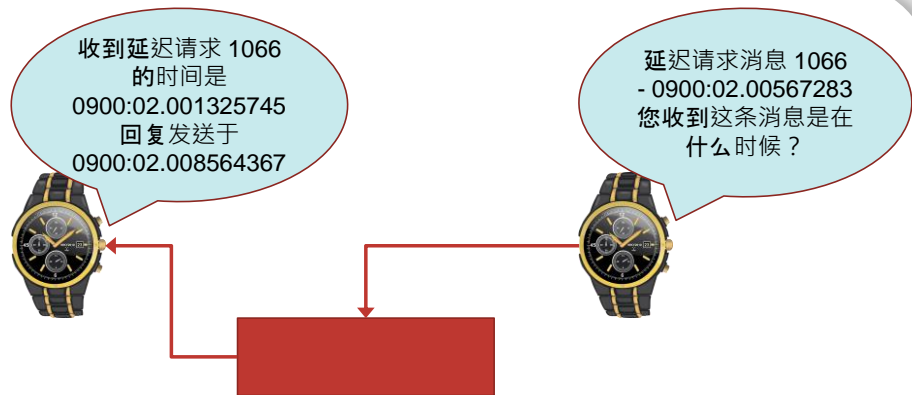
我们已经了解到，数据帧可能相互带来轻微的阻碍

对于 PTP 数据帧也是这样的（它们并不会魔法）

实际上，从设备需要对从主设备收到的消息“取平均值”，而不是“直接下结论”

PTP 也考虑如何在网络中保持稳定

PTP 必须在整个网络上运行



如果没有“真实”的信息 - 从设备仍然要“猜测”主设备的时间（意识不到网络延迟）

如果大家都知道网络延迟的想法，不是会更好吗？

这就是为什么一旦从设备将其“速度”关闭（记住 PLL），它就开始向主设备发送“延迟请求”消息

从设备向主设备发送延迟请求消息

“你好，这是一个延迟请求信息，于 2017 年 5 月

8 日星期一 09:00:02.000567283 发送 - 你是什么时候收到这条消息的？”

主设备回复

“这是主设备 - 我在 2017 年 5 月 8 日星期一
0900:02.001325745 收到此消息，我在 2017 年 5
月 8 日星期一 0900:02.008564367 回复此消息”

然后，从设备就能了解到网络造成的延迟 - 它可以使用这些信息，以及同步数据包来预测它应该如何调整它的本地时钟以保持一致

继续...

- 主设备继续发送同步和跟进消息
- 从设备继续发送延迟请求消息
- Dante 的“同步间隔”为 0.25 秒 - 每秒 4 个数据包
- 从设备快速地获得紧密的同步

- 主设备继续发送同步和跟进消息
- 从设备继续发送延迟请求消息
- Dante 的“同步间隔”为 0.25 秒 - 每秒 4 个数据包
- 从设备快速地获得紧密的同步

继续...

- 现在...如果我们在一段时间后删除主时钟
 - 从设备对主时钟的“相对速度”有着很好的理解（并且可以自己维持这一点）...就像是高速公路上的限速标志（并假设您遵守规则）
 - 从设备对主设备的时间也有非常准确的认识 - 并且会相应地设置自己的时钟
- 这就是说
 - 现在，任何从设备都可以轻松（并且快速）地成为主设备
 - 跟进的从设备与“新主设备”足够同步，音频时钟不受影响
 - 系统的同步不依赖于单个永久固定的主设备
 - 时间就是时间 - 我可以随意将它“砍”成很多部分 (Hz)
 - 毕竟，音频和视频时钟完全就是相反的时间 - $1\text{Hz} = 1\text{S}^{-1}$

- 现在...如果我们在一段时间后删除主时钟
 - 从设备对主时钟的“相对速度”有着很好的理解（并且可以自己维持这一点）...就像是高速公路上的限速标志（并假设您遵守规则）
 - 从设备对主设备的时间也有非常准确的认识 - 并且会相应地设置自己的时钟
- 这就是说
 - 现在，任何从设备都可以轻松（并且快速）地成为主设备
 - 跟进的从设备与“新主设备”足够同步，音频时钟不受影响
 - 系统的同步不依赖于单个永久固定的主设备
 - 时间就是时间 - 我可以随意将它“砍”成很多部分 (Hz)
 - 毕竟，音频和视频时钟完全就是相反的时间 - $1\text{Hz} = 1\text{S}^{-1}$

高级 DANTE 联网：章节 8

在本节中...

故障排除

- 故障排除的基础
- Dante 端口地址
- 网络端口
- IP 地址
- MAC 地址
- 常见症状和原因
- 联系 IT 部门



故障排除

- 故障排除的基础
- Dante 端口地址
- 网络端口
- IP 地址
- MAC 地址
- 常见症状和原因
- 联系 IT 部门

故障排除

- 网络就是将设备连接在一起
 - 了解连接如何“中断”是解决问题的关键
- 回顾 - Dante 将以下“流量”放入网络中
 - 时间 - PTP IEEE1588
 - 音频数据
 - 用于建立路线和控制 Dante 功能的命令
 - 发现服务 (以便命令可以发送到设备)
- 仅仅因为您不能“看到它”，并不意味着它不能被看到！
 - 请思考使用“端口地址”附加到网络堆叠的应用程序
 - 许多操作系统使用“防火墙”软件来阻止某些应用程序访问网络堆叠
 - 如果您可以“看到”主时钟 (在 Dante controller 路由屏幕顶部标识) ，但看不到设备或设备名称不带任何信息，99% 的情况是 - 运行 Dante controller 的计算机上的防火墙阻止了某些东西



- 网络就是将设备连接在一起
 - 了解连接如何“中断”是解决问题的关键
- 回顾 - Dante 将以下“流量”放入网络中
 - 时间 - PTP IEEE1588
 - 音频数据
 - 用于建立路线和控制 Dante 功能的命令
 - 发现服务 (以便命令可以发送到设备)
- 仅仅因为您不能“看到它”，并不意味着它不能被看到！
 - 请思考使用“端口地址”附加到网络堆叠的应用程序
 - 许多操作系统使用“防火墙”软件来阻止某些应用程序访问网络堆叠
 - 如果您可以“看到”主时钟 (在 Dante controller 路由屏幕顶部标识) ，但看不到设备或设备名称不带任何信息，99% 的情况是 - 运行 Dante controller 的计算机上的防火墙阻止了某些东西

故障排除 - DANTE“端口”地址

Dante 使用的流量如下：

mDNS	224.0.0.251:5353
控制和监测	224.0.0.230 – 232:8007-8706
PTP	224.0.1.129 – 132:319-320
组播音频	239.255.0.0/16:4321
单播音频	RX 单播 IP : 14336 – 14600
AES67 组播音频	239.XX.0.0/16:5004



- 所有 Dante 流量都是 UDP/IP
- 这意味着如果这些端口和 IP 地址往来的流量被阻止，那么承载该特定服务的“电线”可被视为“被切断”！



Dante 使用的流量如下：

mDNS：224.0.0.251:5353

控制和监测：224.0.0.230 – 232:8007-8706

PTP：224.0.1.129 – 132:319-320

组播音频：239.255.0.0/16:4321

单播音频：RX 单播 IP：14336 – 14600

AES67 组播音频：239.XX.0.0/16:5004

所有 Dante 流量都是 UDP/IP

这意味着如果这些端口和 IP 地址往来的流量被阻止，那么承载该特定服务的“电线”可被视为“被切断”！

网络端口 - 切断线缆的两种方式

- 计算机的操作系统可能使用“防火墙”
 - 查看操作系统中的哪些应用程序试图访问网络
 - 将规则应用于这些连接（允许或拒绝）
 - 查看哪些目标IP地址（和端口）正在被使用 - 可以在此基础上允许/拒绝
 - 可以确定网络是“私人”还是“公共”，并在此基础上决定允许/拒绝
 - 可以查看已经特定端口和/或 IP 地址传输/接收了多少数据，并决定在“阈值”触发规则
- 防火墙设备只是网关处的计算机 - 它们的工作方式与操作系统防火墙类似



- 计算机的操作系统可能使用“防火墙”
 - 查看操作系统中的哪些应用程序试图访问网络
 - 将规则应用于这些连接（允许或拒绝）
 - 查看哪些目标IP地址（和端口）正在被使用 - 可以在此基础上允许/拒绝
 - 可以确定网络是“私人”还是“公共”，并在此基础上决定允许/拒绝
 - 可以查看已经特定端口和/或 IP 地址传输/接收了多少数据，并决定在“阈值”触发规则
- 防火墙设备只是网关处的计算机 - 它们的工作方式与操作系统防火墙类似

网络端口 - 切断线缆的两种方式

- 网络交换结构可以应用 ACL（访问控制列表）
 - ACL 是用于过滤网络流量的强大工具
 - 许多高级 IT 网络都将应用 ACL
 - 通常 IT 部门不希望公开或讨论这些（潜在的安全问题）
- 期望所需服务配备所需资源是合理的 - 在端口级别，这点已经在之前的幻灯片中定义



- 网络交换结构可以应用 ACL（访问控制列表）
 - ACL 是用于过滤网络流量的强大工具
 - 许多高级 IT 网络都将应用 ACL
 - 通常 IT 部门不希望公开或讨论这些（潜在的安全问题）
- 期望所需服务配备所需资源是合理的 - 在端口级别，这点已经在之前的幻灯片中定义

IP 地址

- 需要关注的 2 种 IP 地址：
 - 在 Dante 中，组播 IP 地址只能在一个 IP 子网中工作
 - 跨越多个子网的 Dante 网络上的所有通信都是单播的（设备 IP 到设备 IP）
- 组播 IP 地址
 - 某些交换机默认阻止 IP 组播（这将阻止以下功能正常工作）：
 - 局域网中的 Dante Discovery
 - Dante Clock（按照标准，PTP 作为组播发送）
 - 组播 Dante 音频

- 需要关注的 2 种 IP 地址：
 - 在 Dante 中，组播 IP 地址只能在一个 IP 子网中工作
 - 跨越多个子网的 Dante 网络上的所有通信都是单播的（设备 IP 到设备 IP）
- 组播 IP 地址
 - 某些交换机默认阻止 IP 组播（这将阻止以下功能正常工作）：
 - 局域网中的 Dante Discovery
 - Dante Clock（按照标准，PTP 作为组播发送）
 - 组播 Dante 音频

IP 地址

- 需要关注的 2 种 IP 地址：
 - 在 Dante 中，组播 IP 地址只能在一个 IP 子网中工作
 - 跨越多个子网的 Dante 网络上的所有通信都是单播的（设备 IP 到设备 IP）
- 单播 IP 地址
 - 要让单播通信成功：
 - 在局域网中 - 两台设备必须位于同一个 IP 子网内
 - 在路由网络中 - 包含要连接的设备的局域网必须由 IP 路由器连接在一起
 - 路由器的 IP 子网配置必须正确（接口正确寻址）
 - 相关 IP 子网之间必须存在路由
 - 更高级的路由器可以像交换机或防火墙一样使用 ACL 来过滤流量

- 需要关注的 2 种 IP 地址：
 - 在 Dante 中，组播 IP 地址只能在一个 IP 子网中工作
 - 跨越多个子网的 Dante 网络上的所有通信都是单播的（设备 IP 到设备 IP）
- 单播 IP 地址
 - 要让单播通信成功：
 - 在局域网中 - 两台设备必须位于同一个 IP 子网内
 - 在路由网络中 - 包含要连接的设备的局域网必须由 IP 路由器连接在一起
 - 路由器的 IP 子网配置必须正确（接口正确寻址）
 - 相关 IP 子网之间必须存在路由
 - 更高级的路由器可以像交换机或防火墙一样使用 ACL 来过滤流量

MAC 地址

- MAC 地址很少会导致任何问题（除非 ACL 或安全设备配置了拒绝规则）
- 在第 2 层 - 确保交换机上的所有接口都处于预期的 VLAN 中,这是最常见的配置问题
- 最后说说第 1 层
 - 线缆是否被切断？
 - 接口是否开放？（管理型交换机可以使用软件命令关闭其接口）
 - 如果使用光纤 - 信号完整性是否良好（光纤端头是否清洁？接口是否无灰尘？）
 - 使用可靠的测试设备来验证线缆（Cat 5/6/7 等）并检查信号完整性和光纤组件的损耗

- MAC 地址很少会导致任何问题（除非 ACL 或安全设备配置了拒绝规则）
- 在第 2 层 - 确保交换机上的所有接口都处于预期的 VLAN 中,这是最常见的配置问题
- 最后说说第 1 层
 - 线缆是否被切断？
 - 接口是否开放？（管理型交换机可以使用软件命令关闭其接口）
 - 如果使用光纤 - 信号完整性是否良好（光纤端头是否清洁？接口是否无灰尘？）
 - 使用可靠的测试设备来验证线缆（Cat 5/6/7 等）并检查信号完整性和光纤组件的损耗

常见症状和原因

设备名称显示在
Dante Controller
中 - 没有显示用于扩展
通道的 +，状态视图缺
失数据

- 检查计算机操作系统上的防火墙设置
- 检查并确认计算机上由 Dante controller 使用的接口与您希望控制的 Dante 设备处于同一 IP 子网中

常见症状和原因

时钟发出解锁/锁定警告

- 可能的组播拦截 - 检查 Dante controller 中的时钟直方图以确认
- 单播延迟请求可以作为快速测试是否属于这种情况的工具
- Dante 时钟可以运行极长时间才会再次出现影响音频的同步失败...小时

常见症状和原因

显示多个主时钟

- 设备“无法得悉”来自其他设备的组播同步消息 - 假设它们是主设备
- 通常由网络中受阻的组播流量引起

联系 IT 部门

- 本课程详细介绍了 Dante AoIP 网络的要求
- 特定 IT 基础架构厂商设备的配置细节是特定且独特的
- 然而 - 本课程涵盖的概念在 IP 网络中是通用的（对于不同的基础架构厂商，术语可能略有不同）
 - 了解如何建立 IP 连接（端口、IP 地址、路由、交换、组播、广播等）有助于解释需求
 - 了解带宽需求很有用
 - 了解可以应用 QoS 规则来优化性能
 - 了解 IGMP 可用于缓解组播的负面影响



本课程详细介绍了 Dante AoIP 网络的要求

特定 IT 基础架构厂商设备的配置细节是特定且独特的

然而 - 本课程涵盖的概念在 IP 网络中是通用的（对于不同的基础架构厂商，术语可能略有不同）

- 了解如何建立 IP 连接（端口、IP 地址、路由、交换、组播、广播等）有助于解释需求
- 了解带宽需求很有用
- 了解可以应用 QoS 规则来优化性能
- 了解 IGMP 可用于缓解组播的负面影响

联系 IT 部门

- 联网是指使许多块独特的“拼图”一起工作
- 本课程解释了拼图的“Dante 部分”的要求和性能
- 请记住 - IT 部门必须将许多部分组合在一起 - 保持耐心，它可以并且将会很好地配合在一起。



联网是指使许多块独特的“拼图”一起工作

本课程解释了拼图的“Dante 部分”的要求和性能

请记住 - IT 部门必须将许多部分组合在一起 - 保持耐心，它可以并且将会很好地配合在一起。

下
一步

接受 第3 级测试

<http://www.audinate.com/certify>

- 如果您没有 Audinate 账户，请先建立账户
- 登录到您的账户
- 接受第3 级测试
- 证书会自动产生



谢谢