神州云科
Yunke China

数据表

DCYK 2930F 交换机系列

产品概述

DCYK 2930F 交换机系列专为创建数字工作场所的客户而设计，工作场所通过集成有线和无线方式为移动用户进行了优化。这些基本三层接入交换机可以通过高级安全和网络管理工具，如 DCYK ClearPass Policy Manager 和 DCYK AirWave，进行轻松部署和管理。在基于云的 DCYK Central 支持下，您只需少量甚至无需 IT 支持就可快速设置远程分支机构站点。强大的 DCYK ProVision ASIC 提供性能和价值，支持最新的软件定义网络（SDN）应用程序，为未来的应用程序提供面向未来的可编程性。具有虚拟交换框架（VSF）的堆叠提供了简单性和可扩展性。2930F 支持内置 1GbE 或 10GbE 上行链路、PoE+、接入 OSPF 路由、隧道节点、更好的服务质量、RIP 路由和 IPv6，无需软件许可。DCYK 2930F 交换机系列提供了一种便捷且具有成本效益的接入交换机解决方案，可以通过零接触配置和内置 10GbE 上行链路进行快速设置。强大的基本三层功能集包括有限的终身保修。

主要功能

- DCYK 基本三层交换机，带有 VSF 堆叠、静态、RIP 和接入 OSPF 路由、ACL 和更好的 QOS
- 使用 DCYK AirWave 和 DCYK ClearPass Policy Manager 获得一致的有线 / 无线体验
- 方便的内置 1GbE 或 10GbE 上行链路和高达 370 W PoE+
- 凭借 REST APIs 和 OpenFlow 支持，为创新的 SDN 应用程序作好准备
- 凭借零接触配置和基于云的 DCYK Central 支持实现简单部署

功能和优势

统一的有线和无线

- DCYK ClearPass Policy Manager 使用 DCYK ClearPass Policy Manager 支持统一的有线和无线策略
- 当检测到 DCYK接入点时，交换机自动配置会自动为交换机配置不同的设置，如 VLAN、CoS、PoE 最大功率和 PoE 优先级
- 本地用户角色在安全性、认证和 QoS 等方面定义了一组基于交换机的策略。使用交换机配置或 ClearPass，用户角色可以分配给一组用户或设备
- 提供动态分配的安全隧道，以基于每端口或每个用户角色将网络流量传输到 DCYK控制器。用户通过 ClearPass 策略管理器进行身份验证，该策略管理器将流量通过隧道传输到 DCYK控制器或本地交换机
- HTTP 重定向功能支持智能管理中心（IMC）自带设备（BYOD）解决方案
- 新的静态 IP 可见性允许 ClearPass 对具有静态 IP 地址的客户端进行计费

软件定义网络

- 支持多种编程接口，包含 REST APIs 以及 OpenFlow 1.0 和 1.3 规范，实现自动化网络运营，监控和故障排除。

服务质量（QoS）

- 流量优先级（IEEE 802.1p）允许将实时流量分类为八个优先级，映射到八个队列
- 第 4 层优先级支持基于 TCP/UDP 端口号进行优先级排序
- 服务等级（CoS）根据 IP 地址、IP 服务类型（ToS）、三层协议、TCP/UDP 端口号、源端口和 DiffServ 来设置 IEEE 802.1p 优先级标签
- 速率限制设定每端口入口强制执行最大值，以及每端口、每队列最小值
- 大型缓冲区提供完美的拥塞管理
- 未知的单播速率限制会限制具有未知目标地址的单播数据包，并限制 VLAN 上的泛洪

连接

- 灵活的 10 Gb/s 以太网连接，可提供四个固定的 10 千兆位端口（SFP+）
- Auto-MDIX 可在所有 10/100 和 10/100/1000 端口上进行直通或交叉电缆的自动调整
- IEEE 802.3at 以太网供电（PoE+）可提供高达 30 W 的端口，可支持最新的、支持 PoE+ 的设备，如 IP 电话、无线接入点和安全摄像头，以及符合 IEEE 802.3af 标准的终端设备；消除了在 IP 电话和 WLAN 部署中另外需要的附加电缆和电路的成本
- 先于标准的 PoE 支持检测先于标准的 PoE 设备并为之提供电源
- IPv6
  - IPv6 主机使交换机能够在 IPv6 网络中进行管理
  - 双栈（IPv4 和 IPv6）允许从 IPv4 过渡到 IPv6，支持两种协议的连接
  - MLD Snooping 将 IPv6 组播流量转发到相应的接口
  - IPv6 ACL/QoS 支持 IPv6 网络流量的 ACL 和 QoS
  - IPv6 路由支持静态和 RIPng 协议
  - 安全提供 RA 保护，DHCPv6 保护，动态 IPv6 锁定和 ND Snooping

性能

- 节能设计
  - 80 PLUS 银牌认证电源提高了电源效率并节约能源
  - 节能以太网（EEE）支持可以根据 IEEE 802.3az 降低功耗
- DCYK Provision ASIC 架构拥有最新的 DCYK Provision ASIC 设计，提供非常低的延迟，增加的数据包缓冲和自适应功耗
- 可选择的队列配置允许通过选择最能满足网络应用程序要求的队列数量和相关内存缓冲来提高性能

聚合

- IP 组播侦听和数据驱动的 IGMP 自动防止 IP 组播流量泛洪
- LLDP-MED（媒体端点发现）定义了 LLDP 的标准扩展，用于存储 QoS 和 VLAN 等参数的值，以自动配置网络设备，如 IP 电话
- IEEE 802.1AB 链路层发现协议（LLDP）通过使用带有 LLDP 自动设备发现协议的网络管理应用程序来促进轻松映射
- PoE 和 PoE+ 分配支持多种方法 - 自动、IEEE 802.3at 动态、LLDP-MED 细粒度、IEEE 802.3af 设备类，或用户指定，来分配和管理 PoE/PoE+ 功率，以实现更高效节约能源
- 本地 MAC 认证使用本地配置的配置文件分配诸如 VLAN 和 QoS 的属性，而配置文件可以是 MAC 前缀列表
- 新的 IP 组播路由包括 PIM 稀疏和密集模式，以路由 IP 组播流量（限于 16 个接口）
- 用于 IPv6 的协议独立组播支持一对多和多对多媒体转换，例如 IPv6 网络上的 IPTV

弹性和高可用性

- 新的虚拟交换框架（VSF）从多达八 * 个交换机创建一个虚拟弹性交换机；服务器或交换机可以使用标准 LACP 进行连接，以实现自动负载平衡和高可用性；通过减少对诸如生成树协议（STP）、等价多路径（ECMP）和 VRRP 等复杂协议的需求来简化网络操作
- IEEE 802.1s 多生成树通过允许多个生成树在多个 VLAN 环境中提供高链路可用性；为 IEEE 802.1d 和 IEEE 802.1w 提供传统支持
- 新的虚拟路由器冗余协议（VRRP）允许两个路由器组可以动态地相互备份，以为 IPV4 和 IPV6 网络创建高可用的路由环境（限于 128 个虚拟路由器）
- IEEE 802.3ad 链路聚合控制协议（LACP）和端口中继支持多达 128 个静态、动态或分布式中继线（在堆叠中活动的），每个中继线有每个静态中继线多达有八个链路（端口）；并对整个堆叠中的成员提供中继支持。
- SmartLink 提供活动和备用链路的简单配置链路冗余

管理

- SNMPv1、v2 和 v3 完全支持 SNMP；提供对行业标准管理信息库（MIB）和私有扩展的全面支持；SNMPv3 支持使用加密来增加安全性
- DCYK Central 基于云的管理平台提供了一种简单，安全且经济高效的交换机管理方式
- 零接触配置（ZTP）使用 AirWave 网络管理，通过使用基于 DCYK Activate 或基于 DHCP 的进程，简化了交换机基础设施的安装
- 支持多种编程接口，包括 REST APIs 和 Openflow 1.0 和 1.3，以实现网络操作，监控和故障排除的自动化

*需要ArubaOS-Switch 16.06软件

可管理性

- 双闪存镜像提供独立的主和副操作系统文件，以在升级的同时进行备份
- 便于使用的端口命名允许向端口分配描述性名称
- Find-Fix-Inform 自动发现并修复常见的网络问题，然后通知管理员
- 多配置文件允许将多个配置文件存储到闪存映像
- 软件更新可以从互联网上免费下载
- RMON、XRMON 和 sFlow® 为统计、历史、报警和事件提供高级监控和报告功能
- 故障排除入口和出口端口监控允许解决网络问题
- 单向链路检测（UDLD）监视两个交换机之间的链路，如果两个设备之间的任何点链路断开，则阻塞链路两端的端口
- 针对语音的新 IP SLA 使用 UDP 抖动及用于 VoIP 测试的 UDP 抖动来监控语音流量质量

第二层交换

- VLAN 支持和标记同时支持 IEEE 802.1Q（4094 VLAN ID）和 2K VLAN
- 巨型数据包支持提高了大数据传输的性能；支持高达 9,220 字节的帧大小
- IEEE 802.1v 协议 VLAN 隔离将非 IPv4 协议自动选择至自己的 VLAN 中
- 快速的每 VLAN 生成树（RPVST+）允许每个 VLAN 构建单独的生成树，以改善链路带宽使用；与 PVST+ 兼容
- GVRP 和 MVRP 允许自动学习和动态分配 VLAN
- 用于覆盖网络的 VxLAN 封装（隧道）协议，实现更可扩展的虚拟网络部署

第三层服务

- DHCP 服务器集中并降低 IPv4 地址管理的成本

第三层路由

- 静态 IP 路由提供手动配置的路由；包括 ECMP 功能
- 256 个静态和 10000 个 RIP 路由便于隔离用户数据，而无需添加外部硬件
- 路由信息协议（RIP）提供 RIPv1、RIPv2 和 RIPng 路由
- 接入 OSPF
  - 提供 OSPFv2 和 OSPFv3 协议，用于在接入和 LAN 下一层之间的路由。仅支持一个 OSPF 区域和多达 8 个接口。
- 新的基于策略的路由根据网络管理员设置的策略使用分类器来选择可以转发的流量（限于 16 个下一跳路由）

安全

- 控制平面策略设置交换机控制协议层面的速率限制，以保护 CPU 过载免受 DOS 攻击
- 多种用户认证方式
  - IEEE 802.1X 在客户端使用 IEEE 802.1X 请求者与 RADIUS 服务器一起根据行业标准进行认证
  - 基于 Web 的身份验证提供了类似于 IEEE 802.1X 的基于浏览器的环境来验证不支持 IEEE 802.1X 请求者的客户端
  - 基于 MAC 的认证使用 RADIUS 服务器，根据客户端的 MAC 地址对客户端进行认证
- 认证灵活性
  - 每个端口的多个 IEEE 802.1X 用户提供每端口多个 IEEE 802.1X 用户的认证；防止用户以另一用户的 IEEE 802.1X 身份验证进行“蹭网”
  - 每个端口交换机端口的并发 IEEE 802.1X、Web 和 MAC 认证方案最多可接受 32 个 IEEE 802.1X、Web 和 MAC 认证
- 访问控制列表（ACL）提供基于源 / 目标 IP 地址 / 子网和源 / 目标 TCP/UDP 端口号的 IP 第 3 层过滤
- 源端口过滤只允许指定的端口相互通信
- RADIUS/TACACS+ 通过使用密码认证服务器简化交换机管理的安全管理
- 安全外壳加密所有传输的数据，以通过 IP 网络进行安全远程 CLI 访问
- 安全套接层（SSL）加密所有 HTTP 流量，允许对交换机中基于浏览器的管理 GUI 进行安全访问
- 端口安全性仅允许访问指定的 MAC 地址，这可以予以学习或由管理员指定
- MAC 地址锁定防止特定配置的 MAC 地址连接到网络
- 安全 FTP 允许安全地向（从）交换机传输文件；防止不需要的文件下载或交换机配置文件未经授权的复制
- 交换机管理登录安全性可以通过可选地要求 RADIUS 或 TACACS+ 认证来安全地切换 CLI 登录

- 当用户登录交换机时，自定义横幅（Banner）显示安全策略
- STP BPDU 端口保护在不需要桥接协议数据单元（BPDU）的端口上阻止 BPDU，以防止伪造 BPDU 的攻击
- DHCP 保护阻止来自未经授权 DHCP 服务器的 DHCP 数据包，防止拒绝服务攻击
- 动态 ARP 保护功能阻止来自未授权主机的 ARP 广播，防止网络数据的窃听或窃取
- STP 根保护（STP Root Guard）保护根网桥（Root Bridge）免受恶意攻击或防止配置错误
- 身份驱动的 ACL 允许实现高度细粒度和灵活的访问安全策略和针对每个经过身份验证的网络用户的 VLAN 分配
- 每端口广播抑制在繁忙流量端口上行链路上选择性配置广播控制
- 私有 VLAN 通过限制对等通信来防止各种恶意攻击来提供网络安全；通常，交换机端口只能与同一社区和 / 或上行链路端口中的其他端口通信，而不管 VLAN ID 或目标 MAC 地址
- 开放式身份验证角色通过允许故障客户端的完全网络访问简化了棕色地带部署中 AAA 的首次部署，并在客户端插入后立即提供即时连接

监控和诊断

- SFP+ 和 1000BASE-T 收发器的数字光学监控允许详细监控收发器设置和参数

保修和支持

- DCYK有限终身质保

标准和协议（适用于所有系列产品）

拒绝服务保护

- CPU DoS 保护

设备管理

- RFC 1155 结构和管理信息（SMIv1）
- RFC 1157 SNMPv1/v2c
- RFC 1591 DNS（客户端）
- RFC 1901（基于社群的 SNMPv2）
- RFC 1901-1907 SNMPv2c，SMIv2 和修订的 MIB-II
- RFC 1908（SNMPv1/v2 共存）
- RFC 2576（SNMPv1, v2, v3 版本之间共存）
- RFC 2578-2580 SMIv2
- RFC 2579（SMIv2 文本约定）
- RFC 2580（SMIv2 一致性）
- RFC 2819（RMON 组报警、事件、历史和统计信息）
- RFC 3416（SNMP 协议操作 v2）
- RFC 3417（SNMP 传输映射）
- HTML 和 Telnet 管理
- HTTP、SSHv1 和 Telnet
- 多个配置文件
- 多个软件映像
- SNMPv3 和 RMON RFC 支持
- SSHv1/SSHv2 安全外壳
- TACACS/TACACS+
- Web 用户界面

通用协议

- IEEE 802.1AX-2008 链路聚合
- IEEE 802.1d MAC Bridges
- IEEE 802.1p 优先级
- IEEE 802.1Q VLANs
- IEEE 802.1s 多生成树
- IEEE 802.3ad 链路聚合控制协议（LACP）
- IEEE 802.3af 以太网供电
- IEEE 802.3at PoE+
- IEEE 802.3az 能效以太网
- IEEE 802.3x 流量控制
- RFC 768 UDP
- RFC 783 TFTP 协议（修订 2）
- RFC 792 ICMP
- RFC 793 TCP
- RFC 826 ARP
- RFC 854 TELNET
- RFC 868 时间协议
- RFC 951 BOOTP
- RFC 1058 RIPv1
- RFC 1256 ICMP 路由器发现协议（IRDP）
- RFC 1350 TFTP 协议（修订 2）
- IEEE 802.1v 按协议和端口进行 VLAN 分类
- RFC 1519 CIDR IEEE 802.1w 生成树快速重新配置
- RFC 1542 BOOTP 扩展
- IEEE 802.3ab 1000BASE-T
- RFC 1918 私有网络地址分配
- RFC 2030 简单网络时间协议（SNTP）v4
- RFC 2131 DHCP
- RFC 2236 IGMP 监听
- RFC 2453 RIPv2
- RFC 2865 远程认证拨号用户服务（RADIUS）
- RFC 2866 RADIUS 计费
- RFC 3046 DHCP 中继代理信息选项
- RFC 3411 用于描述简单网络管理协议（SNMP）管理框架的架构
- RFC 3412 针对简单网络管理协议（SNMP）的消息处理和调度
- RFC 3413 简单网络管理协议（SNMP）应用程序
- RFC 3414 针对简单网络管理协议版本 3（SNMPv3）的基于用户的安全模式（USM）
- RFC 3415 针对简单网络管理协议（SNMP）的基于视图的访问控制模式（VACM）
- RFC 3416 针对 SNMP 的协议操作
- RFC 3417 针对简单网络管理协议（SNMP）的传输映射
- RFC 3418 针对简单网络管理协议（SNMP）的管理信息库（MIB）
- RFC 3575 针对 RADIUS 的 IANA 注意事项
- RFC 3576 对 RADIUS 的扩展（仅 CoA）
- RFC 4541 互联网组管理协议（IGMP）和组播侦听者发现（MLD）侦听交换机的注意事项
- RFC 4675 RADIUS VLAN 和优先级
- RFC 4861 IP 版本 6（IPv6）的邻居发现
- RFC 4862 IPv6 无状态地址自动配置
- RFC 5905 网络时间协议版本 4：协议和算法规范
- UDLD（单向链路检测）

IP组播

- RFC 1112 IGMP
- RFC 2236 IGMPv2
- RFC 2710 IPv6组播侦听器发现（MLD）
- RFC 3376 IGMPv3
- RFC 4541互联网组管理协议（IGMP）和组播侦听者发现（MLD）侦听交换机的注意事项

IPv6

- RFC 1981 IPv6路径MTU发现
- RFC 2080针对IPv6的RIPng
- 协议适用性声明
- RFC 2082 RIP-2 MD5
- RFC 2460 IPv6规范
- RFC 2464以太网上的IPv6传输
- RFC 2710 IPv6组播侦听器发现（MLD）
- RFC 2925远程Ping、跟踪路由和查找操作（仅限PING）的管理对象定义
- RFC 2925远程操作MIB（仅限Ping）
- RFC 3019 MLDv1 MIB
- RFC 3315 DHCPv6（客户端和中继）
- RFC 3484针对IPv6的默认地址选择
- RFC 3513 IPv6寻址架构
- RFC 3596针对IPv6的DNS扩展
- RFC 3810针对IPv6的MLDv2
- TCP 4022针对TCP的MIB
- RFC 4113针对UDP的MIB
- RFC 4251 SSHv6架构
- RFC 4252 SSHv6认证
- RFC 4253 SSHv6传输层
- RFC 4254 SSHv6连接
- RFC 4291 IP版本6寻址架构
- RFC 4293针对IP的MIB
- RFC 4419针对SSH的密钥交换
- RFC 4443 ICMPv6
- RFC 4541 IGMP和MLD侦听开关
- RFC 4861 IPv6邻居发现
- RFC 4862 IPv6无状态地址自动配置
- RFC 5095在IPv6中弃用类型0路由标头
- RFC 6620 FCFS SAVI
- IETF工作组文稿

MIB

- IEEE 802.1ap（仅MSTP和STP MIB）
- IEEE 8021-桥接-MIB（2008）
- IEEE 8021-Q-桥接-MIB（2008）
- RFC 1155针对TCP/IP互联网的管理信息结构和ID
- RFC 1156（TCP/IP MIB）
- RFC 1,157 A 简单网络管理协议（SNMP）
- RFC 1213 MIB II
- RFC 1493桥接MIB
- RFC 1724 RIPv2 MIB
- RFC 2021 RMONv2 MIB
- RFC 2578管理信息版本2（SMIv2）的结构
- RFC 2579 SMIv2的文本约定
- RFC 2580 SMIv2的一致性声明
- RFC 2613 SMON MIB
- RFC 2618 RADIUS客户端MIB
- RFC 2620 RADIUS计费MIB
- RFC 2665以太网型接口类型MIB
- RFC 2668 802.3 MAU MIB
- RFC 2674 802.1p和IEEE 802.1Q桥接MIB
- RFC 2737 Entity MIB (version 2)
- RFC 2819 RMON MIB
- RFC 2863接口组MIB
- RFC 2925 Ping MIB
- RFC 2932 IP（组播路由MIB）
- RFC 2933 IGMP MIB
- RFC 3414基于SNMP用户的SM MIB
- RFC 3415基于SNMP视图的ACM MIB
- RFC 3417 IEEE 802网络上的简单网络管理协议（SNMP）
- RFC 3418针对SNMPv3的MIB
- RFC 4836针对802.3介质连接单元（MAU）的管理对象

网络管理

- IEEE 802.1AB 链路层发现协议（LLDP）
- RFC 1155 管理信息的结构
- RFC 1157 SNMPv1
- RFC 2021 使用 SMIv2 的远程网络监控管理信息库版本 2
- RFC 2576 SNMP 版本之间的共存
- RFC 2578 管理信息版本 2（SMIv2）的结构
- RFC 2579 SMIv2 的文本约定
- RFC 2580 SMIv2 的一致性声明
- RFC 2819 RMON 的四个组：1（统计）、2（历史）、3（报警）和 9（事件）
- RFC 2819 远程网络监控管理信息库
- RFC 2856 附加大容量数据类型的文本约定
- RFC 2925 远程 Ping、跟踪路由和查找操作应用的管理对象定义
- RFC 3164 BSD 系统日志协议
- RFC 3176 sFlow
- RFC 3411 SNMP 管理框架
- RFC 3412 针对简单网络管理协议（SNMP）的消息处理和调度
- RFC 3413 简单网络管理协议（SNMP）应用程序
- RFC 3414 针对简单网络管理协议版本 3（SNMPv3）的基于用户的安全模式（USM）
- RFC 3415 针对简单网络管理协议（SNMP）的基于视图的访问控制模式（VACM）
- RFC 3418 针对简单网络管理协议(SNMP)的管理信息库(MIB)
- RFC 5424 系统日志协议
- ANSI/TIA-1057 LLDP 媒体端点发现（LLDP-MED）
- SNMPv1/v2c/v3 XRMON

QoS/CoS

- IEEE 802.1p（CoS）
- RFC 2474 DiffServ 优先级，包括 8 个队列 / 端口
- RFC 2475 DiffServ 架构
- RFC 2597 DiffServ 确保转发（AF）
- RFC 2598 DiffServ 快速转发（EF）
- 入口速率限制

安全

- IEEE 802.1X 基于端口的网络访问控制
- RFC 1321 MD5 消息摘要算法
- RFC 1334 PPP 认证协议（PAP）
- RFC 1492 访问控制协议，有时被称为 TACACS
- RFC 1492 TACACS+
- RFC 1994 PPP 质询握手认证协议（CHAP）
- RFC 2082 RIP-2 MD5 认证
- RFC 2104 用于消息认证的哈希密钥
- RFC 2138 RADIUS 认证
- RFC 2139 RADIUS 计费
- RFC 2246 传输层安全（TLS）
- RFC 2548 Microsoft® 厂商特定的 RADIUS 属性
- RFC 2618 RADIUS 认证客户端 MIB
- RFC 2620 RADIUS 计费客户端 MIB
- RFC 2716 PPP EAP TLS 认证协议
- RFC 2818 TLS 之上的 HTTP
- RFC 2865 RADIUS（仅客户端）
- RFC 2865 RADIUS 认证
- RFC 2866 RADIUS 计费
- RFC 2867 针对隧道协议支持的 RADIUS 计费修正
- RFC 2868 针对隧道协议支持的 RADIUS 属性
- RFC 2869 RADIUS 扩展
- RFC 2882 NAS 要求：扩展 RADIUS 实践
- RFC 3162 RADIUS 和 IPv6
- RFC 3576 对 RADIUS 的动态授权扩展
- RFC 3579 RADIUS 对可扩展认证协议（EAP）的支持
- RFC 3580 IEEE 802.1X RADIUS
- RFC 3580 IEEE 802.1X 远程认证拨号用户服务（RADIUS）使用指南
- RFC 4576 RADIUS 属性访问控制列表（ACL）
- draft-grant-tacacs-02 (TACACS)
- 针对 802.1X 的访客 VLAN
- MAC 认证
- MAC 加锁
- MAC 锁定
- 端口安全
- RFC 安全套接层（SSL）
- SSHv2 安全外壳
- Web 认证

神州云科 Yunke China
北京市海淀区上地九街9号数码科技广场
吴寄遥: +86.13693208636l wujyj@digitalchina.com
汪要娣: +86.18721819116l wangydw@digitalchina.com