神州云科
Yunke China

数据表

DCYK 5400R ZL2 交换机系列

产品概述

使用针对高速 IEEE 802.11ac 设备的 DCYK智能速率多千兆位端口，DCYK 5400R zl2 交换机系列是业界领先的移动园区访问解决方案。产品为创建数字工作场所客户提供了企业级的弹性，具有创新的灵活性和可伸缩性，而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。这一系列产品通过虚拟交换框架（VSF）堆叠技术、无中断故障切换和针对 5400R VSF 堆叠的快速软件升级，带来了可伸缩的聚合。高级第 2 层和第 3 层功能集包括 OSPF、IPv6、IPv4 BGP、隧道节点、强大的 QoS 和基于策略的路由，无需软件许可。

基于强大的 ProVision ASIC，DCYK 5400R zl2 交接机系列拥有带有 2 Tbps 纵横交换结构（2.1µ 低延迟、前所未有可编程性）的高速、大容量的架构，并支持创新的软件定义网络（SDN）应用。这一系列配有 6 或 12 插槽紧凑型机箱，提供灵活的连接选项，线速 40GbE，多达 96 个 10GbE 线速端口及多达 288 个 PoE +端口。5400R 可以使用高级的安全和网络管理工具，例如 DCYK ClearPass Policy Manager、DCYK AirWave 和基于云平台的 DCYK Central，予以轻松部署和管理。

主要功能

- 强大的 DCYK 第 3 层模块化交换机系列，具有 VSF 堆叠、动态分包技术、低延迟和弹性。
- 针对高速多千兆带宽的 DCYK智能速率（IEEE 802.3bz）和PoE+ 功率。
- 针对无线流量聚合的可扩展线速 40GbE。
- 凭借 REST API 和 OpenFlow 的支持，为 SDN 做好准备。
- 凭借 ClearPass 策略管理器、AirWave 以及 Central 支持的安全和网络管理工具。

功能和优势

软件定义网络

- 支持多种可编程接口，包括 REST API 和 Openflow 1.0 和 1.3，来开启自动的网络维护、监测和故障诊断

统一的有线和无线

- 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
- 用户角色定义了一系列的基于交换机的策略，关于安全性、认证和 QoS 等方面。用户角色可以分配给一组用户或设备，用户角色可以是交换机本地用户角色也可以是 ClearPass 下发角色
- 动态分包技术提供了安全隧道，以基于每端口或每用户角色的方式将网络流量传输到 DCYK控制器。对于基于每用户角色的隧道节点（PUTN），用户通过 ClearPass 策略管理器进行身份验证，并根据身份验证情况决定数据流量是通过隧道转发到 DCYK控制器还是通过交换机本地进行转发
- 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

服务质量（QoS）

- 基于高级分类器的 QoS，根据第 2 层、第 3 层和第 4 层信息，使用多个匹配标准对流量进行分类；应用 QoS 策略，例如基于每端口或每 VLAN 为所选流量设置优先级和速率限制
- 流量优先级允许将实时流量分类为八个优先级，而这八个优先级映射到八个队列

- 带宽整形
  - 基于端口的速率限制提供每端口入口 / 出口强制增加的带宽
  - 基于分类器的速率限制使用访问控制列表（ACL）来为每个端口上的入口流量强制带宽增加
  - 降低的带宽提供每端口、每队列基于出口的带宽减少
- 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
- 未知单播速率限制功能压制未知目的地址的单播数据包，限制 VLAN 上的报文风暴

管理

- DCYK Central 基于云的管理平台，为管理交换机提供了简单、安全和具有成本效益的方法
- 零接触配置（ZTP）通过使用基于 DCYK Activate 或基于 DHCP 的方式来注册到 AirWave 网络管理系统，从而简化了交换机基础设施的安装
- 针对相同硬件的灵活管理 - 针对相同硬件既支持基于云平台的 Central 管理也支持本地 Airwave 管理，确保管理平台变更时不需要拆除和更换交换基础设施
- 针对语音的 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（需要 v3 模块）
- 内置可编程和易于使用的 REST API 接口为移动优先（Mobile-first）的园区网提供配置自动化
- 远程智能镜像可以基于 ACL、端口、MAC 地址或 VLAN，将指定的入口 / 出口流量镜像到网络中任何地方的本地或远程 8200 zl、6600、6200 yl、5400 zl、5400R、3500 或 3800交换机
- RMON、XRMON 和 sFlow® v5 为统计、历史、报警和事件提供高级监控和报告功能
- IEEE 802.1AB 链路层发现协议（LLDP）从网络上的相邻设备发布和接收管理信息，便于网络管理应用程序的简单映射
- 单向链路检测（UDLD）支持慧与公司（DCYK ）UDLD和 DLDP 协议，以监控两台交换机之间的电缆，如果电缆断开，则关闭两端的端口
- 管理简单性为所有基于 DCYK ProVision 的交换机（包括 zl 和 yl交换机）提供通用软件功能和 CLI 实施
- 命令授权利用 RADIUS 将 CLI 命令的自定义列表链接到单个网络管理员的登录；审计跟踪文件活动
- 友好的端口名称允许为端口指定描述性名称
- 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
- 多个配置文件轻松存储到闪存映像
- Comware CLI
  - Comware 兼容的 CLI 为使用 DCYK OS-Switch CLI 的慧与公司用户提供体验
  - 显示和基本的 Comware CLI 命令本身嵌入交换机 CLI 中；显示输出格式为基于 Comware 的交换机；基本命令提供了熟悉的 Comware 初始交换机设置
  - 在 Comware 命令输入时配置 Comware CLI 命令，引出 CLI 帮助，以表达正确的 DCYK OS-Switch 软件 CLI 命令

连接

- IEEE 802.3az 节能以太网在低链路使用期间降低功耗（支持 v2 zl 10/100/1000 和 10/100 模块）
- IEEE 802.3at PoE+ 提供每端口高达 30W 的功率，从而支持最新的 PoE+ 受电设备，如 IP 电话、无线接入点和安防监控摄像头，同时兼容 IEEE 802.3af 的受电设备；节约了 IP 电话和 WLAN 部署中的电缆和线路的额外开支
- 先于标准的 PoE 支持检测先于标准的 PoE 设备并为之提供供电
- 高密度端口连接性提供多达 12 个接口模块插槽及多达 288 个支持 PoE 的 10/100/1000 速率有线接口或每系统 96 个 10GbE 端口
- 千兆以太网和万兆以太网端口上的巨型帧，巨型帧允许高性能远程备份和灾难恢复服务
- 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
- IPv6
  - IPv6 主机使交换机能够在 IPv6 网络中进行管理
  - 双栈（IPv4 和 IPv6）将 IPv4 转换为 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 流量的 ACL 和 QoS
  - IPv6 路由支持静态、RIPng、OSPFv3 路由协议
  - 6in4 隧道支持 IPv6 流量封装于 IPv4 数据包中
  - 安全提供 RA 保护，DHCPv6 保护，动态 IPv6 锁定和 ND Snooping

性能

- 高速、高容量架构 2 Tbps 纵横交换结构在专用的 ProVision ASIC 上提供了模块内和模块间交换，吞吐量为 785,700,000 PPS。
- 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

弹性和高可用性

- 虚拟交换框架（VSF）从两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 等的复杂协议的需求来简化网络操作（需要 v3 模块）
- 快速软件升级可以通过顺序升级堆叠中的成员将停机时间缩短到几秒钟（需要 v3 模块），从而减少升级过程中 VSF 堆栈的停机时间。
- 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
- 不间断交换可提高网络可用性，以更好地支持关键应用程序，如统一通信和移动性；接口和结构模块在从主管理模块到备用管理模块故障切换期间继续交换流量
- 不间断路由增强了第三层高可用性；OSPFv2/v3 和 VRRP 将在从主管理模块切换到备用管理模块的故障切换期间继续操作和路由网络流量
- 冗余的管理和功率提供了增强的系统可用性和运行的连续性
- IEEE 802.1s 多生成树协议通过允许多个生成树在多个 VLAN 环境中提供高链路可用性；包括 IEEE 802.1D 生成树协议和 IEEE 802.1w 快速生成树协议
- IEEE 802.3ad 链路聚合控制协议（LACP）支持多达 144 个中继，每个中继最多可以有 8 个链路（端口）
- 分布式中继使用无循环冗余网络拓扑，无需使用生成树协议；允许服务器或交换机使用一个逻辑中继线连接到两个交换机，以进行冗余和负载共享
- 可选冗余电源提供不间断电源，并在安装时允许冗余电源热插拔
- 热插拔模块允许不同的模块，冗余电源配置中的电源要添加或更换，不会中断网络
- 十分简便的 DCYK zl 通用附件（接口模块和电源）
- 上行链路故障检测为那些为主要备用 NIC 分组而配置的服务器提供主要备用网路径冗余
- SmartLink 提供主用和备用链路的简单配置链路冗余

第二层交换

- VLAN 支持和标签同时支持 IEEE 802.1Q 标准和 4094 VLAN
- IEEE 802.1v 协议 VLAN 隔离将非 IPv4 协议自动选择至自己的 VLAN 中
- 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（需要 v3 模块）
- GVRP 和 MVRP 允许自动学习和动态分配 VLAN
- IEEE 802.1ad Q-in-Q 通过提供分层结构来提高以太网网络的可扩展性；连接高速园区或城域网上的多个 LAN
- 基于 MAC 的 VLAN 提供了细粒度的控制和安全性；使用 RADIUS 将 MAC 地址 / 用户映射到特定的 VLAN（要求 V2 或更高版本的模块）
- 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
- DCYK 交换机网状化在多个主动冗余链路之间动态地绑定负载平衡，以增加可用的总带宽；使用 V2 或更高版本的模块允许并发三层路由

第三层服务

- 双向转发检测（BFD）支持链路连通性监控，减少 OSPFv2 和 VRRP 的网络聚合时间（需要 v3 模块）
- 用户数据报协议（UDP）帮助功能允许 UDP 广播通过路由器接口定向到特定的 IP 单播或子网广播地址，并防止 UDP 服务（如 DHCP）的服务器欺骗
- 环回接口地址定义了路由信息协议（RIP）和开放最短路径优先（OSPF）中的地址，从而提高了诊断能力
- 路由图在路由再分配期间提供更多的控制；允许过滤和更改路由指标
- 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 路由为 IPv4 和 IPv6 网络提供手动配置的路由
- 路由信息协议（RIP）提供 RIPv1、RIPv2 和 RIPng 路由
- OSPF 为 IPv4 路由提供 OSPFv2，为 IPv6 路由提供 OSPFv3
- 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（需要 v2 或更高版本的模块）
- 边界网关协议（BGP）提供 IPv4 边界网关协议路由，这种路由可扩展、健壮和灵活

安全

- Control Plane 策略通过设置控制协议的速率限制来避免因为 DOS 攻击导致 CPU 过载
- 访问控制列表（ACL）以每个 VLAN 或每个端口方式，基于 IP 字段、源 / 目标 IP 地址 / 子网以及源 / 目标 TCP/UDP 端口号提供过滤
- 多种用户认证方式
  - 每端口 IEEE 802.1X 用户提供每端口多个 IEEE 802.1X 用户的认证
  - 基于 Web 的身份验证，对不支持 IEEE 802.1X 请求者的客户端从 Web 浏览器进行身份验证
  - 基于 MAC 的认证客户端使用 RADIUS 服务器，根据客户端的 MAC 地址对客户端进行认证
  - 基于端口的并发 IEEE 802.1X、Web 和 MAC 认证方案允许每个端口最多可接受 32 个 IEEE 802.1X，Web 和 MAC 认证
- 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
- 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
- 安全管理访问通过 SSHv2、SSL 和 / 或 SNMPv3 为所有访问方法（CLI、GUI 或 MIB）提供安全加密
- 交换机 CPU 保护提供自动保护，防止恶意网络流量尝试关闭交换机
- 通过启用任何交换机端口自动抑制 ICMP 流量，ICMP 抑制将击败 ICMP 拒绝服务攻击
- 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
- 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
- 动态 IP 锁定可以通过 DHCP 保护来阻止来自未经授权的主机流量，从而防止 IP 源地址欺骗
- 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
- 恶意攻击检测监控 10 种网络流量，并在可能由恶意攻击造成的异常被检测到时发送警告
- 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
- 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
- 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
- 开放身份认证角色简化了在棕色地带的首次 AAA 部署，在客户端认证失败时提供完全的网络访问权限并提供即时连接
- 关键身份认证角色确保像 IP 电话等重要设备即时在 RADIUS 服务器不通时也一样可以访问网络
- MAC 绑定通过将终端 MAC 地址绑定到端口的方式，允许传统终端即使处于非通信状态也同样保持认证通过的状态，直到终端注销或断开网络
- 管理界面向导可以帮助确保管理界面如 SNMP、Telnet、SSH、SSL、Web 和 USB 处于所希望的等级
- 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
- 当用户登录到交换机时，安全横幅会显示自定义的安全策略
- IEEE 802.1AE MACsec 使用标准加密和认证（需要 v3 模块）在两个交换机端口（1Gbps 或 10Gbps）之间的链路上提供安全性

标准和协议（适用于所有系列产品）

BGP

- RFC 1997 BGP 社区属性
- RFC 2918 路由刷新能力
- RFC 4271 边界网关协议 4（BGP-4）
- RFC 4456 BGP 路由反射：全网状内部 BGP 的替代（IBGP）
- RFC 5492 使用 BGP-4 的能力通告

设备管理

- RFC 1591 DNS（客户端）
- HTML 和 telnet 管理
- RFC 2576（SNMP V1、V2、V3 之间共存）
- RFC 2579（SMIv2 文本约定）
- RFC 2580（SMIv2 一致性）
- RFC 3416（SNMP 协议操作 v2）

通用协议

- IEEE 802.1ad Q-in-Q
- IEEE 802.1AX-2008 链路聚合
- IEEE 802.1D MAC 桥接
- IEEE 802.1p 优先级
- IEEE 802.1Q VLAN
- IEEE 802.1s 多生成树
- IEEE 802.1v 按协议和端口进行 VLAN 分类
- IEEE 802.1w 生成树快速重新配置
- IEEE 802.3ad 链路聚合控制协议（LACP）
- IEEE 802.3af 以太网供电
- IEEE 802.3az 高效以太网
- IEEE 802.3bz 2.5 Gbps 和 5 Gbps 接口
- 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 1350 TFTP 协议（修订 2）
- RFC 1519 CIDR
- RFC 1542 BOOTP 扩展
- 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 2453 RIPv2
- RFC 2548（仅 MS-RAS- 厂商）
- RFC 3046 DHCP 中继代理信息选项
- RFC 3575 针对 RADIUS 的 IANA 注意事项
- RFC 3576 对 RADIUS 的扩展（仅 CoA）
- RFC 3768 VRRP
- RFC 4675 RADIUS VLAN & 优先级 UDLD（单向链路检测）
- RFC 5880 BFD
- RFC 5905 NTP 客户端

IP 组播

- RFC 3376 IGMPv3
- RFC 3973 PIM 密集模式
- RFC 4601 PIM 稀疏模式

IPv6

- RFC 1981 IPv6 路径 MTU 发现
- RFC 2375 IPv6 组播地址
- RFC 2080 针对 IPv6 的 RIPng
- RFC 2081 RIPng 协议适用性
- RFC 2082 RIP-2 MD5 分配
- 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 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 3587 IPv6 全局单播地址格式
- RFC 3596 针对 IPv6 的 DNS 扩展
- RFC 3810 针对 IPv6 的 MLDv2
- TCP 4022 针对 TCP 的 MIB
- RFC 4087 IP 隧道 MIB
- RFC 4113 针对 UDP 的 MIB
- RFC 4213 IPv6 主机和路由器的基本转换机制
- 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 4294 IPv6 节点要求
- 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 5340 针对 IPv6 的 OSPFv3
- RFC 5453 保留的 IPv6 接口标识符
- RFC 5519 组播组成员发现 MIB（仅限 MLDv2）
- RFC 5722 重叠的 IPv6 碎片处理
- RFC 6620 FCFS SAVI
- IETF 工作组文稿

MIBs

- 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 1213 MIB II
- RFC 1493 桥接 MIB
- RFC 1724 RIPv2 MIB
- RFC 1850 OSPFv2 MIB
- RFC 2021 RMONv2 MIB
- RFC 2096 IP 转发表 MIB
- RFC 2578 管理信息版本 2（SMIv2）的结构
- 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 实体 MIB（版本 2）
- RFC 2787 VRRP MIB
- RFC 2863 接口组 MIB
- RFC 2925 Ping MIB
- RFC 2932 IP（组播路由 MIB）
- RFC 2933 IGMP MIB
- RFC 4292 IP 转发表 MIB
- RFC 4836 针对 802.3 介质连接单元（MAU）的管理对象
- RFC 7331 BFD MIB

网络管理

- IEEE 802.1AB 链路层发现协议（LLDP）
- RFC 2819 RMON 的四个组：1（统计）、2（历史）、3（报警）和 9（事件）
- 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
- XRMON

OSPF

- RFC 2328 OSPFv2
- RFC 3101 OSPF NSSA
- RFC 5340 针对 IPv6 的 OSPFv3

QoS/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）

安全

- IEEE 802.1AE MAC 安全标准（MACSec）
- IEEE 802.1X 基于端口的网络访问控制
- RFC 1492 TACACS+
- RFC 1321 MD5 消息摘要算法
- RFC 2698 A 双速率三色标记
- RFC 2818 TLS 之上的 HTTP
- RFC 2865 RADIUS（仅客户端）
- RFC 2866 RADIUS 计费
- RFC 3579 RADIUS 对可扩展认证协议（EAP）的支持
- 安全套接层（SSL）
- SSHv2 安全外壳

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: +86.13693208636I wujyj@digitalchina.com
汪要娣: +86.18721819116I wangydw@digitalchina.com