SIEMENS西门子 SCALANCE S615LAN路由器 6GK5 615-0AA00-2AA2

产品名称	SIEMENS西门子 SCALANCE S615LAN路由器 6GK5 615-0AA00-2AA2
公司名称	浔之漫智控技术(上海)有限公司
价格	.00/件
规格参数	西门子:代理经销商 交换机:全新原装 假一罚十 德国:正品现货 实体经营
公司地址	上海市松江区石湖荡镇塔汇路755弄29号1幢一层A区213室
联系电话	15801815554 15801815554

产品详情

服务质量Quality of Service (QoS) 是一种有助于高效利用网络中现有带宽的方法。QoS 通过排定数据传输的优先级来实现。传入帧根据特定优先级分类到 Queue 中，然后进行进一步处理。这为帧分配了特定的优先级。各种不同的 QoS 方法相互影响，并按下列顺序加以考虑：1. 交换机首先检查传入帧是广播帧还是代理帧。→ 第一个条件满足时，交换机将考虑 “ 常规 (页 279) ” 页上设置的优先级。交换机将根据 “ CoS 映射 (CoS Map) (页 281) ” 页面上的分配将帧分类到队列中。2. 如果第一个条件不满足，交换机将检查帧是否包含 VLAN 标记。→ 如果第二个条件满足，交换机将检查 “ 常规 (页 279) ” 页面上的优先级设置。交换机将检查是否为优先级设置了 “ 非强制 ” (Do not force) 以外的值。如果设置了优先级，交换机将根据 “ CoS 映射 (CoS Map) (页 281) ” 页面上的分配将帧分类到队列中。3. 如果第二个条件也不满足，则将根据信任模式对帧进行进一步处理。信任模式在 “ QoS 信任(QoS Trust) (页 284) ” 页面上组态。私有 VLAN借助私有 VLAN (PVLAN)，可将一个 VLAN 二层广播域划分为多个子区域。私有 VLAN 由以下单元组成： 主私有 VLAN（主 PVLAN）主私有 VLAN 是指被划分的 VLAN。 次私有 VLAN（次 PVLAN）次 PVLAN 只存在于主 PVLAN 内。每个次 PVLAN 都有一个特定的 VLAN ID，并且与主PVLAN 相连。次 PVLAN 分为以下两类： – Isolated Secondary PVLAN隔离次 PVLAN 内的各设备之间不能通过第 2 层进行通信。 – Community Secondary PVLAN公共次 PVLAN 内的各设备之间可直接通过第 2 层进行通信。隶属不同 PVLAN 团体的设备之间不能通过第 2 层进行通信。说明次 PVLAN 的 VLAN ID如果不同工业以太网交换机上的次 PVLAN 采用相同的 VLAN ID，则这些次 PVLAN 中的终端设备可以在不同交换机上通过第 2 层与其它设备进行通信。前提条件是将连接不同 IE 交换机的端口组态为混合端口。如果将这些端口组态为中继端口，并为隔离的各个次级 PVLAN 使用相同 VLAN ID，则终端设备仍然处于隔离状态。说明私有 VLAN 功能和 RADIUS 验证当通过 RADIUS 验证为 VLAN 的一个或多个端口启用 VLAN 分配时，不应将此 VLAN 另外组态为私有

VLAN。与通过 RADIUS 验证进行 VLAN 分配相关的私有 VLAN
功能可能会导致系统状态不一致。技术基础5.4 VLANSCALANCE
XB-200/XC-200/XF-200BA/XP-200/XR-300WG Web Based Management V4.3.182 配置手册, 11/2021,
C79000-G8952-C360-13Private VLAN VLAN YPrimary PVLAN XSecondary PVLAN 10IsolatedSecondary
PVLAN 20CommunitySecondary PVLAN 30Community 3URPLVFXRXV 3RUW 7DJJHG0HPEHU+RVW
3RUW 8QWDJJHG0HPEHU3URPLVFXRXV 3RUW 8QWDJJHG0HPEHUPC1PC2PC3PC4PC5在本
示例中，各工业以太网交换机之间使用混合端口进行互连。这些网络端口在所有 PVLAN（主 PVLAN
和所有次 PVLAN）中均为带标记的成员。用于连接 PC 的端口是主机端口。主机端口在主 PVLAN
及其次 PVLAN 中均为无标记的成员。用于连接服务器的端口是混合端口。该混合端口在所有
PVLAN（主 PVLAN 和所有次 PVLAN）中均为带标记的成员。在本示例中，所有 PC
均可与服务器通信，反之亦然。PC1 不能与任何其它 PC 通信。公共次PVLAN
内的设备之间可以相互通信，但不能与其它次 PVLAN 内的 PC 通信。5.4.4 VLAN 通道使用 Q-in-Q VLAN
隧道功能，可通过提供商网络转发具有 VLAN
隧道的各种客户网络的数据通信。每个客户网络均有完备的可用 VLAN。技术基础5.4 VLANSCALANCE
XB-200/XC-200/XF-200BA/XP-200/XR-300WG Web Based Management V4.3.1配置手册, 11/2021,
C79000-G8952-C360-13 83VLAN
隧道在提供商网络边界组态的交换机之间建立。一个提供商交换机具有以下端口类型：
访问端口提供商交换机通过访问端口连接到客户网络。 –
传入数据通信访问端口处的传入数据通信视为无标记 ①。所有的传入帧均由具有访问端口端口
VID的标签扩展②。所有帧均已标记，这意味着它们已由第二个 802.1Q 标签（外部 VLAN标签）③
扩展。附加字节中包含标记协议标识符 (TPID) 和标记控制信息 (TCI)。 标记协议标识符 (TPID)
前两个字节构成标记协议标识符 (TPID)，且始终包含值 0x8100。此值指定该数据包包含 VLAN
信息或优先级信息。 标记控制信息 (TCI) 两个字节的标记控制信息 (TCI) 包含以下信息： QoS 信任
技术基础 5.4 VLAN SCALANCE XB-200/XC-200/XF-200BA/XP-200/XR-300WG Web Based Management
V4.3.1 80 配置手册, 11/2021, C79000-G8952-C360-13 标记帧有 3 个位用于优先级，又称为服务类别 (Class of
Service, CoS)，另请参见 IEEE 802.1Q。 CoS 位 优先级 数据通信的类型 000 0（最低） Background 001 1 Best
Effort 010 2 Excellent Effort 011 3 Critical Applications 100 4 Video，< 100 ms 延时（延迟和抖动） 101 5
Voice（语言），< 10 ms 延时（延迟和抖动） 110 6 Internetwork Control 111 7（最高） Network Control
仅当组件中存在队列（可在其中缓冲优先级较低的数据包）时，方可实现数据包的优先级。
设备具有多个并行队列，可在其中处理各种优先级的帧。默认情况下，首先会处理具有最高
优先级的帧。此方法可确保即使在数据通信繁忙时，具有最高优先级的帧仍能得到发送。
规范格式标识符 (CFI) CFI 用于表示以太网与令牌环之间的兼容性。 其值的含义如下： 值 含义 0 MAC
地址格式符合规范。以规范形式表示 MAC 地址时，先传送最低有效位。以太 网交换机的标准设置。 1
MAC 地址格式不符合规范。 VLAN ID 在 12 位数据字段中，最多可构成 4096 个 VLAN
ID。存在以下惯例： VLAN ID 含义 0 帧中仅包含优先级信息（标记有优先级的帧），不包含任何有效的
VLAN 标识符。 1- 4094 有效 VLAN 标识符，该帧被分配给某 VLAN 并且也可以包含优先级信息。 4095
预留 – 传出数据通信使用访问端口的传出数据通信，将外部标签再次删除。
核心端口提供商交换机通过核心端口连接到提供商网络。核心端口为访问端口的端口 VLAN
的成员，或者使用端口类型 “ Switch-Port VLAN Trunk ” 组态。在本示例中，来自客户网络 A、B 和 C
的数据通信使用 VLAN 通道通过提供商网络转发。来自客户网络 A 的帧带有 VLAN ID
标记。来自客户网络 B 的帧带有优先级标记。来自客户网络 C的帧没有标记。技术基础5.4
VLANSCALANCE XB-200/XC-200/XF-200BA/XP-200/XR-300WG Web Based Management V4.3.184 配置手册,
11/2021, C79000-G8952-C360-13帧在到达相关访问端口时，即由具有访问端口端口 VID
的标签扩展，并通过提供商网络隧道化。帧离开提供商网络时，将立即再次删除外部 VLAN 标签
(PVID)。帧以其原始格式转发。保留帧的优先级。5.5 镜像设备提供了同时引导入站或出站数据流经过其
它接口以进行分析或监视的选项。这对受监视的数据流没有影响。此过程称为镜像。在此菜单部分，可
启用或禁用镜像并设置参数。镜像端口镜像端口是指将工业以太网交换机的某个端口（镜像端口）上的
数据通信复制到另一个端口（监视端口）。可以将一个或多个端口镜像到监视端口。如果协议分析器与
监视端口相连接，则可在不中断连接的情况下记录镜像端口的数据通信。这意味着可在不影响数据通信
的情况下对数据通信进行研究。只有设备有空闲端口可用作监视端口时，才能实现此功能。说明转发
RSPAN 流如果设备要转发 RSPAN 流，必须满足两个要求：

输入端口和输出端口必须属于同一个端口组。 对于输入端口，必须禁用“ 学习 ”功能。只能使用 CLI 命令 no unicast mac learning 实现此过程。5.6 SNMP简介借助 (Simple Network Management Protocol , SNMP)，可以监视和控制中央站中的网络元件，例如路由器或交换机。SNMP 控制被监视设备与监视站之间的通信。SNMP 的任务： 监视网络组件 远程控制网络组件，以及远程为网络组件分配参数 错误检测和错误通知技术基础5.6 SNMPSCALANCE XB-200/XC-200/XF-200BA/XP-200/XR-300WG Web Based Management V4.3.1配置手册, 11/2021, C79000-G8952-C360-13 85版本 v1 和 v2c 的 SNMP 没有安全机制。网络中的所有用户都可以访问数据，还可使用适当的软件来更改参数分配。如果只需对访问权限进行简单控制而无需考虑安全性，则可使用团体字符串。团体字符串与查询一起传送。如果团体字符串正确，SNMP 代理将做出响应并发送所请求的数据。如果团体字符串不正确，SNMP 代理将放弃查询。可以为读取和写入权限定义不同的团体字符串。团体字符串以明文形式传送。团体字符串的标准值： public具有只读权限 private具有读写权限说明由于 SNMP 团体字符串用于访问保护，请勿使用标准值“ public ”或“ private ”。请在初始调试之后更改这些值。设备级的更多简单保护机制： Allowed Host被监视系统知道监视系统的 IP 地址。 Read Only如果为被监视设备指定“ Read Only ”，则监视站只能读取数据，但无法更改。SNMP 数据包未加密，其他用户可轻松读取。中央站也称为管理站。SNMP 代理安装在与管理站交换数据的被监视设备上。管理站发送以下类型的数据包： GET向 SNMP 代理请求数据记录 GETNEXT调用下一条数据记录。 GETBULK （自 SNMPv2c 起可用）每次请求多条数据记录，例如，表中的多行。 SET包含相关设备的参数分配数据。SNMP 代理发送以下类型的数据包： RESPONSESNMP 代理返回管理器请求的数据。 TRAP如果发生特定事件，SNMP 代理将发送陷阱。SNMPv1/v2c/v3 使用 UDP（User Datagram Protocol，用户数据包协议）并使用 UDP 端口161 和 162。管理信息库 (Management Information Base, MIB) 对该数据进行了介绍。SNMPv3与先前版本 SNMPv1 和 SNMPv2c 比较，SNMPv3 引入了广义的安全概念。SNMPv3 支持： 完全加密的用户验证 对全部数据通信进行加密 在用户/组级别对 MIB 对象进行访问控制