

一种多业务以太网接入交换机的关键技术^{*}

张晓哲 刘 琼 方贵明

(中国科学院软件研究所 北京100080)

摘 要 宽带社区接入网是下一代网络研究的主要领域之一。RBISN(社区宽带综合业务网络系统)研究使用交换式以太网提供数字电视、IP 电话和 Internet 接入服务。需要解决用户隔离、组播、服务质量的问题。本文介绍了这一系统中交换机采用的关键技术。

关键词 宽带社区接入网,以太网接入交换机,非对称 VLAN,IGMP snooping,服务质量

Key Technologies in an Ethernet Access Switch Providing Multiple Services

ZHANG Xiao-Zhe LIU Qiong FANG Gui-Ming

(Institute of Software, Chinese Academy of Sciences, Beijing 100080)

Abstract Nowadays, broadband residential access networks remain one of the major research areas for NGN. RBISN (Residential broadband Integrated Services Network) is the research work on providing TV, VoIP and Internet Services with Switched Ethernet. There are many problems to be resolved such like isolation of users, multicast and QoS. This paper introduces the key technologies used in the switches in this system.

Keywords Broadband residential access network, Ethernet access switch, Asymmetric VLAN, IGMP snooping, QoS

在过去的几年中,各种宽带接入技术竞相登场。在有线接入领域,流行的技术是 xDSL(数字用户环路)、HFC(光纤同轴混合网)和 PON(无源光网络)。交换式以太网由于具有经

济、简单、高效率 and 易扩展等特点,成为一种前景看好的接入技术。

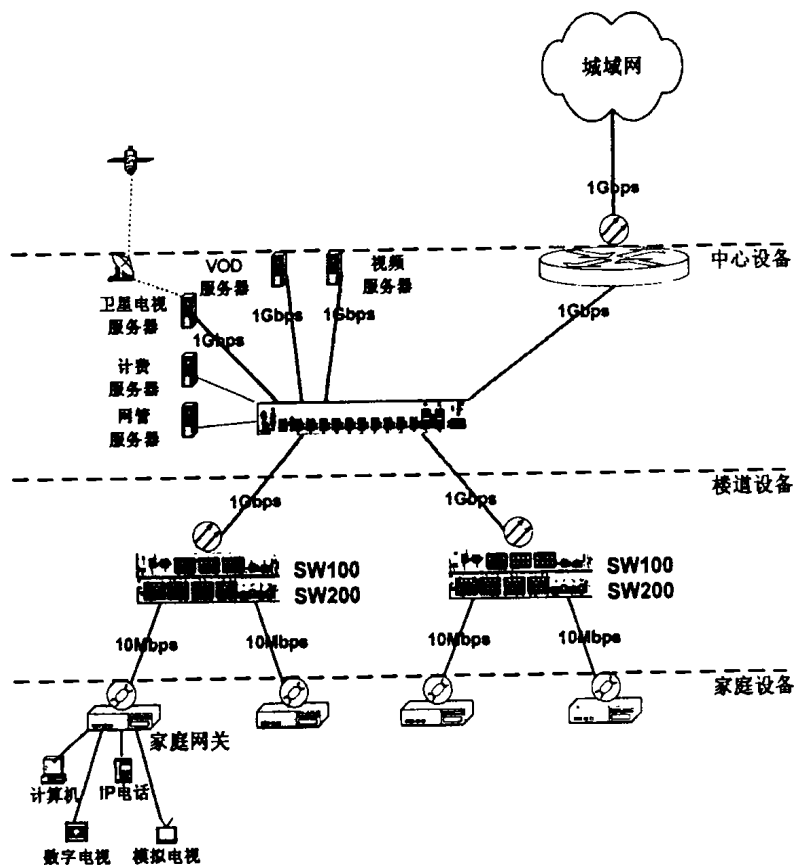


图1 社区宽带综合业务网络系统的网络拓扑

随着网络融合成为趋势,建立基于以太网的宽带社区网,为用户提供多业务接入提上了议事日程。一些标准组织和团体,如 IEEE 和 EFM 研究组、以太网在第一英里联盟 EFMA

和城域以太网论坛 MEF 正在研究以太网用于城域网和接入网的相关问题。

以太网与其他局域网技术一样,是针对私有网络环境而

^{*}北京市科学技术委员会项目(H020120120530)。张晓哲 硕士,研究方向是交换技术和三网融合的软件设计;刘 琼 研究员,研究方向是交换技术;方贵明 研究员,研究方向是多媒体通信与网络工程。

设计的,目的是解决办公设备的资源共享问题。其特点是简单高效,对网络安全、网络管理、传输质量等方面考虑较少。将这种技术应用于社区这种公用环境,需要解决的问题有以下几个:

用户隔离:一方面,社区的用户间是互不信任的关系。如果允许用户得到其他用户收发数据包,会危害用户的数据安全。另一方面,从管理的角度出发,不允许用户间私自通信。因此以太网必须具备用户隔离的能力。

组播传输:宽带接入提供多种媒体的服务,其中视频流对带宽的要求较高。如果采用单播方式进行传输,则会大大增加对带宽的需求。采用组播技术可以将带宽的要求降到最低,提高网络的可用性。因此以太网必须具备组播的能力。

保证服务质量:宽带接入提供多种媒体的服务,媒体流如视频和音频等服务不仅对带宽有要求,还要求网络保证其传输参数如时延、抖动、包丢失率不能超出允许范围。因此以太网必须具备一定的保证服务质量的能力。

RBISN(社区宽带综合业务网络系统)研究使用交换式以太网为社区用户提供数字电视、IP 电话和 Internet 接入服务,探索电视网、电话网和计算机网三网融合的实现。社区网络使用交换机以树形拓扑连接,核心三层交换机 SW1200 位于社区中心,通过光纤连接楼道交换机。楼道使用二层交换机 SW100/SW200,这两种交换机可通过多种形式级连,以支持不同数量的用户。用户设备使用家庭网关通过五类线接入楼道交换机。在社区网络边缘,IP 电话和 Internet 接入的流量汇聚后通过路由器连入外网,数字电视的流量从外网流入,通过组播技术分发到各个用户(由于数字电视目前没有标准的传输源,系统中暂时使用视频服务器和卫星电视服务器代替),如图1所示。

本文论述了楼道交换机采用的关键技术。

1 用户隔离

多个用户的家庭网关都与楼道交换机相连,用户可以侦听到其他用户的部分信息,用户间也可以进行通信。从安全和管理的角度出发,不允许用户的信息未经授权被其他用户得到,也不允许用户私自通信。因此楼道交换机必须实现用户隔离功能,这可以通过 VLAN 技术实现。标准的 VLAN 对应于二层域,用户使用标准 VLAN 隔离后,必须通过三层设备访问共享资源^[1]。按照标准的作法,每一个用户会分配一个网关 IP,十分麻烦。采用非对称 VLAN 控制协议进行用户隔离,不存在以上问题。而且在没有三层设备的情况下,也可以访问共享资源。

1.1 非对称 VLAN 控制模型

将连接通信主机 A、通信主机 B 和通信主机 C 的端口缺省 VLAN 号设为 $VLAN_A$ 、 $VLAN_B$ 和 $VLAN_C$ 之后,交换机可以自动学习到三条地址: $\langle MAC_A, VLAN_A \rangle$, $\langle MAC_B, VLAN_B \rangle$, $\langle MAC_C, VLAN_C \rangle$ 。这时如果 A 向 B 发送数据包,根据交换机的转发原理(广播包发送到 VLAN 的成员端口,单播包匹配 $\langle MAC_B, VLAN_A \rangle$ 没找到发送到 VLAN 的成员端口),数据包最终会被发送到 $VLAN_A$ 包含的端口。通过设定 $VLAN_A$ 包含/不包含连接通信主机 B 的端口,可以放行/阻塞 A 到 B 的单向流量。这里还存在一个问题,就是 A 到 B 的单向流量中,单播包也通过广播形式发送,通过加入地址 $\langle MAC_B, VLAN_A \rangle$ 可以解决这一问题。综合起来, A 到 B 的单向流量可用下列设定控制:

放行:设定 $VLAN_A$ 包含连接通信主机 B 的端口,添加地址 $\langle MAC_B, VLAN_A \rangle$ 。

阻塞:设定 $VLAN_A$ 不包含连接通信主机 B 的端口,删除地址 $\langle MAC_B, VLAN_A \rangle$ 。

组合这个基本设定,可以控制任何通信主机对间的通信。

非对称 VLAN 控制模型可用如下两个集合定义:

端口和端口 Pvid 二元组集合:

$$\{\langle P_i, Pvid_i \rangle | i=1 \cdots N\}$$

放行单向流量的 Pvid 二元组集合,是下面集合的一个子集:

$$\{\langle Pvid_i, Pvid_j \rangle | i, j=1 \cdots N, Pvid_i \neq Pvid_j\}$$

1.2 非对称 VLAN 控制协议

在社区宽带综合业务网络系统中,需要阻塞所有用户间的流量,放行用户和服务器之间的流量,可以使用文[1]中介绍的方法进行设置。实际上,这是非对称 VLAN 控制模型的一个特例,其定义为:

端口和端口 Pvid 的二元组集合:

$$\{\langle P_i, Pvid_i \rangle | i=1 \cdots N\}$$

服务 VLAN 和用户 VLAN:

服务 VLAN $\rightarrow Svid$; 用户 VLAN $\rightarrow Pvid_i, i=1 \cdots N, Pvid_i \neq Svid$

服务端口和用户端口:

服务端口 $\rightarrow P_i, i=1 \cdots N, Pvid_i = Svid$; 用户端口 $\rightarrow P_i, i=1 \cdots N, Pvid_i \neq Svid$

放行单向流量的 Pvid 二元组集合:

$$\{\langle Pvid_i, Pvid_j \rangle | i, j=1 \cdots N, Pvid_i \neq Pvid_j, Pvid_i = Svid$$

或者 $Pvid_j = Svid\}$

我们使用非对称 VLAN 控制协议来实现这个特例。非对称 VLAN 控制协议根据交换机硬件报告的 MAC 地址学习消息向 MAC 地址表添加/删除静态地址,使 MAC 地址表满足断言“用户 VLAN 学习到的地址同时存在于服务 VLAN 中,服务 VLAN 学习到的地址同时存在于所有用户 VLAN 中”。添加/删除静态地址时,会根据硬件学习到该地址的 VLAN 进行不同的处理。如果是服务 VLAN,应该在所有用户 VLAN 中添加/删除静态地址。如果是用户 VLAN,应该在服务 VLAN 中添加/删除静态地址。

1.3 全局/局部非对称 VLAN 控制

当交换机级连起来后,有两种方法保持整个交换机网络用户隔离的特性。一是级连端口间的流量维持 VLAN 的标志,这样实现的是全局非对称 VLAN 控制。另一种方式是将级连端口作为普通端口对待,级连端口间的流量进入交换机后,被重新标志到本地的 VLAN 中,这样实现的是局部非对称 VLAN 控制。

可以证明,采用两种方法都可以满足社区宽带综合业务网络隔离用户的要求。但前者比后者有如下两处劣势:

全局非对称 VLAN 控制需要每一个交换机知道整个网络中 VLAN 设置情况,采用静态配置十分麻烦,如果要交换机自动识别还需在非对称 VLAN 控制协议中增加新的功能。

全局非对称 VLAN 控制占用的 MAC 地址表项较多。以负荷最大的最高层交换机做比较,假设系统中有 N_s 台服务器, N_c 个用户,交换机设定 N_w 是个用户端口。

全局非对称 VLAN 使用的表项数为

$$N_s * (N_c + 1) + 2 * N_c = (N_s + 2) * N_c + N_s$$

局部非对称 VLAN 使用的表项数为

$$N_s * (N_w + 1) + 2 * N_c = 2 * N_c + N_s * (N_w + 1)$$

N_s 和 N_w 是常量, N_c 是变量。两者都随 N_c 线性增长,但斜率不同。

2 组播

在以太网中实现二层组播,可选的协议有 GMRP、CGMP 和 IGMP snooping。GMRP 不仅需要交换机支持,还需要主机支持并在路由器上部署 IGMP 和 GMRP 的转换协议^[2]。CGMP 不仅需要交换机支持,还需要路由器支持^[3]。IGMP-snooping 只需交换机支持,对于主机和路由器来说是透明的^[4]。由于硬件支持抓取 IGMP 包,我们选择了 IGMP snooping 协议,并根据实际环境改进其机制。

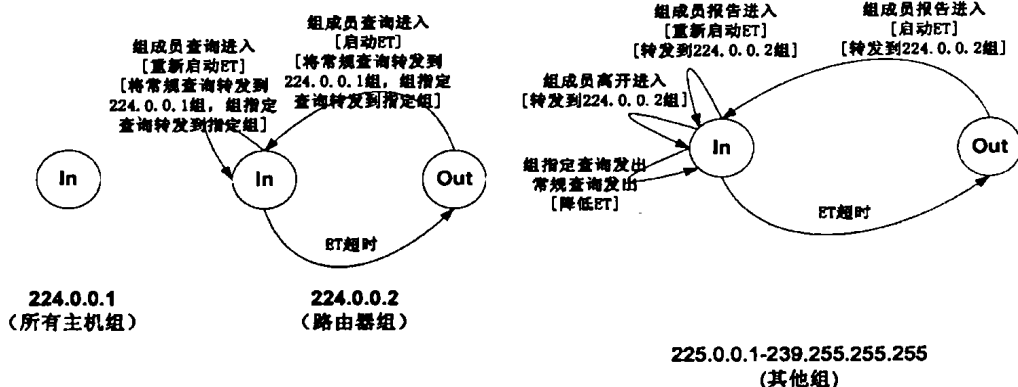


图2 每组播组每端口的成员状态机

状态机有两个状态“in”和“out”,前者表示端口有该组成员,后者表示没有。定时器 ET 表示该端口组成员的生存时间。所有主机组包含每个端口,ET 值为无穷大。路由器组通过组成员查询发现有路由器的端口。其他组通过组成员报告发现有成员的端口,收到组成员查询时,将所有端口的 ET 值降低,一旦没有组成员报告,端口因 ET 超时被踢出。

控制数据包转发的二层组播表由以上状态机的状态推出。对于发往组播组 G 的数据包,不但要发往组播组 G 的成员端口,还要发往路由器组的成员端口。这是因为缺省情况下路由器必须接收所有组播包,进行三层组播,组播组 G 的转发端口集合可以形式化地描述为:

{端口 i | 组播组 G 或者路由器组的端口 i 的状态机为“in”} - {输入端口}

2.2 存在的问题

在社区宽带综合业务网络系统中,我们为每个电视频道分配一个组播组,家庭网关选择/离开某个电视频道相当于加入/离开某个组播组。为通用环境设计的 IGMP snooping,存在以下需要改进的地方:

- 家庭网关离开某个电视频道时,发出组成员离开消息,该消息被向上递交到路由器后,触发组指定查询消息,组指定查询消息向下传送到所有收看该频道的家庭网关。最初发出组离开消息的家庭网关不再发组成员报告消息,最终 ET 超时端口被踢出,其他家庭网关发出组成员报告消息,保持原状态。该机制不但响应较慢,而且影响到其他家庭网关。

- IGMP 消息的传输没有可靠性的保证。当网络负荷较重时,IGMP 消息会发生随机性的丢失,导致 IGMP snooping 协议在整个网络内出现不连续的情况,组播数据不能够送到家庭网关。

第一个问题的根源在于 IGMP 协议的设计。IGMP 关心的是二层域中是否有接收者,而不关心接收者的个数及位置。收到一个组成员报告消息时,IGMP 可以确定二层域内有接收者;而收到一个组成员离开消息时,IGMP 不能确定所有组成员都已离开,因此需要再做查询。在社区宽带综合业务网络

2.1 IGMP snooping 协议

以 IGMPv2 为例,主机和路由器之间交换的 IGMP 消息有如下三种:由路由器发出的组成员查询,由主机发出的组成员报告和组成员离开。组成员查询又分为常规查询和组指定查询。前者是周期性的,后者由组成员离开消息触发^[5]。

IGMP snooping 协议为每个组播组的每个端口维护一个成员状态机和一个定时器 ET (Expire Timer),通过侦听 IGMP 消息和查看定时器状态修改这些状态机,如图2所示。

系统中,交换机的拓扑结构是树形的,叶子交换机的一个端口连接一个家庭网关。对于叶子交换机来说,组成员离开消息是一个确定性的信号,表明该端口已没有该组成员。对于非叶子交换机来说,如果在以其为根的子树内没有组成员的时候才向父亲交换机发送组成员离开消息,那么组成员离开消息也可以作为一个确定性信号。这样在收到组成员离开消息时,只需将端口直接踢出。

第二个问题的根源在于交换机的转发特性。交换机具有一定数量的数据包缓冲,当网络负荷较大的时候,可能因为缓冲不足丢失包。采用 ACK+重传是一个比较好的解决方法。接收交换机收到邻居的消息后,发送 ACK 包作为应答;发送交换机向邻居发送消息后,启动定时器等待邻居的 ACK 包,定时器超时则重传,由于家庭网关的路由器都不具备 ACK 的功能,还需考虑交换机与这两者的交互。交换机发送 ACK 包给家庭网关和路由器,该包被丢弃,不存在大的问题。交换机向家庭网关和路由器发送消息后,如果期待对方发送 ACK 包,则会导致不断的重传。这个问题在交换机和路由器之间显得最为严重。因此,还需加入邻居 ACK 能力的识别机制,对于不具备 ACK 功能的设备不期待 ACK 包。

2.3 改进的 IGMP snooping 协议

2.3.1 ACK 包的定义 ACK 包要被 IGMP snooping 协议收到仍要依靠硬件抓取 IGMP 包的功能,ACK 包采用了 IGMP 包的包头,只是在类型字段进行了修改。

IGMPv2 包类型字段为 0x11 表示该消息是组成员查询,0x16 表示该消息是组成员报告,0x17 表示该消息是组成员离开。相应的 ACK 包类型字段取值 0xA1、0xA6、0xA7。

2.3.2 状态机的定时器 每端口维持一个 ACK 能力状态机和相应的定时器 ANT (Ackable Neighbor Timer),状态机有两个状态“yes”和“no”,前者表示邻居具备 ACK 能力,后者表示不具备。ANT 表示邻居该能力的生存时间。端口收到任何一种 ACK 包,状态置为“yes”并刷新 ANT,ANT 超时则将状态置为“no”。

每组播组每端口成员状态机修改成如图3所示。由于对组

指定查询消息不再有动作,组成员查询全部改为常规查询。每组增加一个报告状态,在未报告的情况下转发组成员报告消息

息;在本组成员变空的情况下发送组成员离开消息。

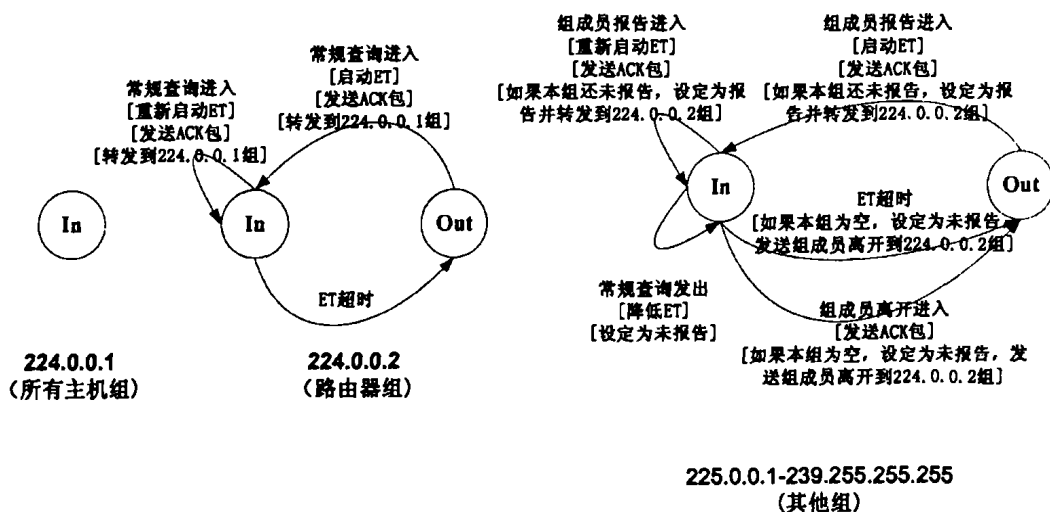


图3 每组每端口的成员状态机

每组播组每端口维持一个重传状态机、重传倒计时器 RTS (Retransmit Times) 和重传定时器 RT (Retransmit Timer)。所有主机组的状态机用于常规查询的重传,有两个状态“Wait”和“Idle”,前者表示等待常规查询 ACK 包,后者

表示无事。其他组的状态要用于组成员报告/组成员离开消息的重传,有三个状态“Wait1”、“Wait2”和“Idle”,“Wait1”表示等待组成员报告 ACK 包,“Wait2”表示等待组成员离开 ACK 包,“Idle”表示无事,如图4所示。

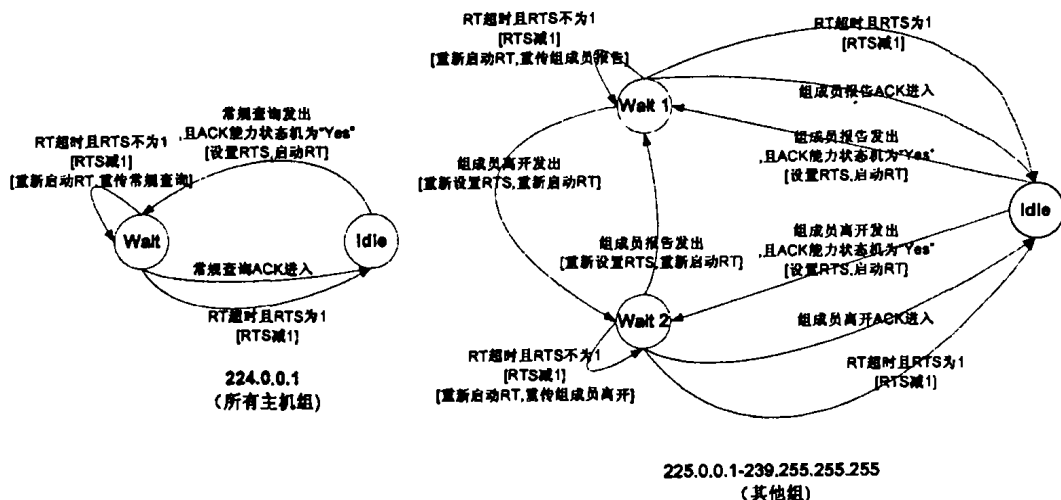


图4 每组播组每端口的重传状态机

所有主机组的 RT 重启后的值为常量。其他组的 RT 重启后的值为前一次的二分之一。其他组的成员状态机收到常规查询消息后必须考虑发生重传的情况,在降低后的 ET 值上增加一个常量,该常量等于 RT 初始值的两倍。

控制数据包转发的二层组播转发表与改进之前相同。

2.4 改进前后的比较

改进前后,家庭网关离开一个组的时间为

改进前 $T_{leaving} = RTT + ET$ 降低后的值

改进后 $T_{leaving} = LT$

RTT 是消息从家庭网关到根交换机的传输时间。 LT 是消息从家庭网关到叶子交换机的传输时间。可以粗略地认为 $RTT = 2 * \text{交换机层数} * LT$ 。

图5是一条组播组数为65的满负荷链路半小时内的重传统计,使用 ACK+重传机制后的协议可靠性增强。

3 QoS 的考虑

通常的 QoS(服务质量)机制是针对国际互联网和 IP 协议而言的,讨论的是如何在提供“尽力”、“公平”服务的 IP 协议基础上建立新的服务框架,以满足不同媒体对吞吐量、延时、抖动、包丢失率等方面的要求。较为常用的两个服务框架是 IS(集成服务)和 DS(区分服务),均由 IETF 提出^[6]。由于 QoS 机制的基础是 IP 协议,因此涉及的包转发设备都是路由器。二层交换机本质上是进行高速包转发的网桥,不在这一范

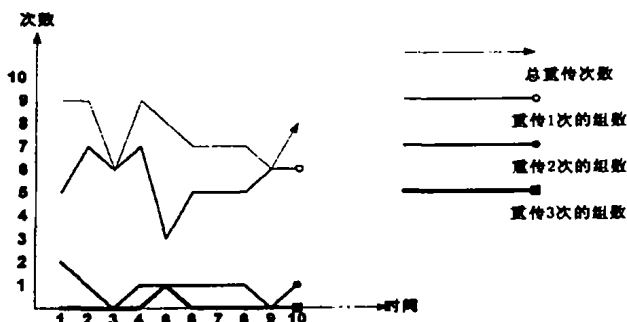


图5 一条组播组数为65的满负荷链路半小时内的重传统计

围之内。但其包交换的特性与路由器没有本质的差别,一些较为简单的 QoS 机制已经被引入这个环境,例如 802.1P 的 8 个优先级。

硬件支持的 QoS 机制参考的是 DS 模型。数据包进入交换控制芯片后,在输入处理中被映射到两个优先级队列之一;数据包离开交换控制芯片时,在输出处理中根据 WRR(加权轮转)和 SP(严格优先)出队列。此外,硬件还支持两处拥塞控制机制:FC(流控)和 HOL(线头阻塞)。

在社区宽带综合业务网络系统中,Internet 接入流量是弹性流,数字电视和 VoIP 的流是非弹性流。因此 Internet 流量使用低优先级而后两者使用高优先级。数字电视的控制包是 IGMP 包,缺省为高优先级;数据包是组播包,通过地址表项映射到高优先级。VoIP 的控制包和数据包由家庭网关和边缘路由器负责标识 ToS 字段,然后通过 ToS 映射到高优先级。

VRR 有预留带宽的作用,设置保证高优先级队列至少能够得到 12/13 的带宽,低优先级队列至少能够得到 1/13 的带宽;数字电视的流量在进入网络之前,先由服务器进行流量整形,使其尽量地接近 CBR 流。VoIP 的流量较小,可以忽略。保证高优先的流量使用的带宽不超出预留的范围,三种服务的服务质量可以得到保证。

对于拥塞控制机制,禁止 FC 开启 HOL。

结束语 基于以太网技术,提供多业务接入的宽带社区网已经提上议事日程。RBISN(社区宽带综合业务网络)研究使用交换式以太网提供电视、IP 电话和 Internet 接入服务。本文介绍了楼道交换机的关键技术。一是实现用户隔离的非对称 VLAN 技术,首先定义通用模型,然后根据实际环境实现,最后分析全局/局部控制的优劣。二是针对该环境改进的 IGMP snooping 协议,提高了响应时间和可靠性。最后是保证服务质量的措施。目前 RBISN 建有 200 用户的实验室测试网,已经稳定运行了两个月。实验表明,这些技术对该系统成为可用系统起到了关键的作用。

参考文献

- 1 IEEE Std 802.1Q-1998. IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks
- 2 IEEE Std 802.1D-1999. Standards for Media Access Control (MAC) Bridges
- 3 Beau Williamson. IP 组播网络设计开发. 电子工业出版社, 2000
- 4 Christensen M, Kimball K, Solensky F. Consideration for IGMP and MLD Snooping Switches (draft-ietf-magma-snoop-09.txt). Internet Draft, 2003
- 5 Fenner W. Internet Group Management Protocol, Version 2 (RFC 2236). Internet Draft, 1997
- 6 Stallings W. High-speed Networks and Internets—Performance and Quality of Service. Prentice Hall, 2002

(上接第 80 页)

$$i^*(\varphi) = \bigcup_{\varphi \in L(A)} \{w \in W \mid \pi_w(\varphi) = T\} \quad (3)$$

$$i^*(\varphi) = \bigcap_{\varphi \in L(A)} \{w \in W \mid \pi_w(\varphi) = \{T, I\}\} \quad (4)$$

显然,我们有 $i^*(\varphi) \subseteq i^*(\varphi)$, 则称 $[i^*(\varphi), i^*(\varphi)]$ 为命题 φ 的区间集合表示。

在文[6]中,假言推理规则扩展为:

$$\frac{[i^*(\varphi), i^*(\varphi)], [i^*(\varphi \rightarrow \psi), i^*(\varphi \rightarrow \psi)]}{i^*(\varphi) \cap i^*(\varphi \rightarrow \psi) \subseteq i^*(\psi) \subseteq i^*(\psi) \subseteq i^*(\varphi \rightarrow \psi)} \quad (5)$$

因为,如表 2 所示,当 $\varphi \rightarrow \psi$ 为 T 或 I 时, ψ 的所有为 T 或 I 的情况都包含进来,所以有 $i^*(\psi) \subseteq i^*(\varphi \rightarrow \psi)$; 当 $\varphi \rightarrow \psi$ 为 T 且 φ 为 T 或 I 时, ψ 必为 T , 所以有 $i^*(\varphi) \cap i^*(\varphi \rightarrow \psi) \subseteq i^*(\psi)$ 。综合起来,我们就得到了文[6]中的最终结论。其对应的概率推理规则为:已知 $P^*(\varphi \rightarrow \psi) (\varphi \rightarrow \psi) \leq P^*(\varphi \rightarrow \psi)$ 与 $P^*(\varphi) \leq P(\varphi) \leq P^*(\varphi)$, 我们可以推出:

$$P^*(\varphi) + P^*(\varphi \rightarrow \psi) - 1 \leq P^*(\psi) \leq P^*(\psi) \leq P^*(\varphi \rightarrow \psi) \quad (6)$$

但是,上述知识只定义了 $i^*(\psi)$ 的最佳下界与 $i^*(\psi)$ 的最佳上界,它不能比较精确地描述 $i^*(\psi)$ 与 $i^*(\psi)$ 的合适的取值范围。因此,我们需要对此范围进行进一步的研究。

再次回到表 2,我们来观察分析 $i^*(\psi)$ 与 $i^*(\psi)$ 各自的上下界。对于 $i^*(\psi)$,我们来找出它的合适的上界:由于当 $\varphi \rightarrow \psi$ 为 T 时, ψ 的所有为 T 的情况都包含进来,所以用 $i^*(\varphi \rightarrow \psi)$ 来作为 ψ 的上界,则有 $i^*(\varphi) \cap i^*(\varphi \rightarrow \psi) \subseteq i^*(\psi) \subseteq i^*(\varphi \rightarrow \psi)$; 对于 $i^*(\psi)$,找出其下界:当 $\varphi \rightarrow \psi$ 为 T , φ 为 T 或 I 时, ψ 一定为 T , 并且,当 $\varphi \rightarrow \psi$ 为 I , φ 为 T 时, ψ 一定为 I , 所以用 $(i^*(\varphi) \cap i^*(\varphi \rightarrow \psi)) \cup (i^*(\varphi) \cap i^*(\varphi \rightarrow \psi))$ 。因此,我们可以得出 $i^*(\psi)$ 的范围是 $[i^*(\varphi) \cap i^*(\varphi \rightarrow \psi), i^*(\varphi \rightarrow \psi)]$, $i^*(\psi)$ 的范围为 $[(i^*(\varphi) \cap i^*(\varphi \rightarrow \psi)) \cup (i^*(\varphi) \cap i^*(\varphi \rightarrow \psi)), i^*(\varphi \rightarrow \psi)]$ 。

则修改过的假言推理对应的概率推理为:已知 $P^*(\varphi \rightarrow \psi) \leq P(\varphi \rightarrow \psi) \leq P^*(\varphi \rightarrow \psi)$ 与 $P^*(\varphi) \leq P(\varphi) \leq P^*(\varphi)$, 我们可

以推出

$$P^*(\psi) + P^*(\varphi \rightarrow \psi) - 1 \leq P^*(\psi) \leq P^*(\varphi \rightarrow \psi) \quad (7)$$

$$P^*((i^*(\varphi) \cap i^*(\varphi \rightarrow \psi)) \cup (i^*(\varphi) \cap i^*(\varphi \rightarrow \psi))) \leq P^*(\psi) \leq P^*(\varphi \rightarrow \psi) \quad (8)$$

在三值逻辑的基础上,上述两种假言推理方法中,前者是后者的基础,后者是前者的扩展或细化。后者更精确地表示出作为结论的命题的确切发生率范围,或者确切的概率范围。

结论 发生率计算提供了与标准概率论的清晰明确的联系,同时,也确保了语义上等价的公式总是具有相同的相关概率,特别是其真值函数性,使得发生率可以表示命题间的独立性,它已经包含了命题间的联系。另一方面,该不确定性推理方法也增加了计算的复杂度。因为,使用该方法进行推理需要对集合进行操作,而这比用单独的数值方法进行推理复杂许多。这就意味着发生率计算在实用性方面,与已得到广泛应用的几种纯数值机制算法相比,还存在着相当的差距。因此,发生率计算算法还有待改进。本文对发生率计算理论进行了初步的研究,我们忠心地希望本文能够起到抛砖引玉的作用,为我国不确定性推理算法的研究起到推动作用。

参考文献

- 1 Nilsson N J. Probabilistic Logic. Artificial Intelligence, 1986, 28: 71~87
- 2 Bundy A. Incidence calculus: a mechanism for probabilistic reasoning. J. Automated Reasoning, 1985, 1: 263~283
- 3 Bundy A. Correctness criteria of some algorithms for uncertain reasoning using incidence calculus. J. Automated Reasoning, 1986, 2: 109~126
- 4 Liu W, McBryan D, Bundy A. The Method of Assigning Incidences. Applied Intelligence, 9, 2, Kluwer Academic, 1998. 139~162
- 5 Qi G. Probabilistic Inference on Three-valued Logic. In: Proc. of intl. conf. RSFDGr'2003, 2003. 690~693
- 6 Yao Y Y, Li X. Comparison of rough-set and interval-set models for uncertain reasoning. Fundamenta Informaticae, 1996, 27(2-3): 289~298