一.基于SNMP的网络拓扑发现算法研究(纯手敲,学习总结)

学习的目的:实现网络管理,即对网络的运行状态进行监测和控制

1.对于物理网络拓扑的发现,主要是利用ARP协议和ICMP协议来发现局域网中的设备

2.目前对于物理网络拓扑发现算法的研究,主要有

a.基于端口流量的物理网络拓扑发现算法

b.基于地址转发表的物理网络拓扑发现算法

c.基于网桥生成树协议的物理网络拓扑发现算法,生成一个反映交换机之间关系的单路径树

所有条件的前提条件:要求网络中的交换机设备支持并开放SNMP服务

3.语术定义:

a.网元:网络中具体的通信设备或者逻辑实体称为网络元素,简称网元

b.管理信息库(MIB):被管理的对象的集合,所有网络被管理的对象信息都在其中,逻辑上的数据库

c.被管对象(MO):表示网络中的资源

网络管理系统的实现主要依赖MO和MIB

4.网络管理系统模型:

a.管理者(管理站,管理进程)

b.管理代理(代理,代理进程)

5.基本组成

a.网络管理者

b.被管节点

c.管理协议

d.网络管理信息库

----------------------------------------

操作管理 执行管理操作

网络---------->管理--------------被管

管理者 <---------代理<-------------对象

通知

----------------------------------------

6.网络拓扑发现是网络管理系统的基础,分层显示网络运行的拓扑结构,为后续的配置数据,监控提供支持:

a.网络拓扑自动发现工具:用于发现网络拓扑,识别网络中各种类型的设备

b.正确反映网元和网元之间的关系,并能顺利定位指定的设备,还能手动编辑关系图

7.网络拓扑发现对象主要分为两种

a.设备的发现,比如:子网,路由器,交换机,主机,接口

b.网络元素之间的物理布局与互连关系

8.网络拓扑发现前的准备工作

a.明确网络的层次,明确信息的采集

b.明确采用的是被动监控技术,还是主动监控技术来采集网络拓扑信息

b1.被动监控技术:为每个网络加入一个监测器,然后提交网络拓扑信息

b2.主动监控技术:网络管理主机向所有管理网络发送探测包

c.采用何种方式收集信息:

c1.采用网络管理信息协议来收集网络的信息

c2.采用通用的协议实现网络信息进行采集,ICMP,DNS等协议向网络上在线设备发送信息包/接收信息包

9.简单网络管理协议(Simple Network Management Protocol,SNMP)协议,应用层协议,属于TCP/IP协议族的一部分,

提供了底层网络管理系统的框架,采用优势:

a.SNMP易于实现,设备支持,运行占用资源少

b.开源

c.无连接协议,基于UDP传输服务来传递消息

d.可用于控制各种设备,比如电话,环境控制设备

e.在大网络环境中,提供了分区,为划分管理职责

10.SNMP概念

a.代理(agent),网络部件上的一个软件模型,收集并维护这个网络部件的管理信息

b.被管理对象(MO):一个MO描述网络部件的某一个可被管理的特性

c.管理信息库(MIB),概念上一个存放被管对象的库

d.管理信息结构SMI,定义了描述管理信息的规则定义语言:ASNA的子集

e.管理站(NMS),负责执行网络管理任务的设备

f.管理协议:NMS和代理之间通信使用的网络协议

管理站,代理,信息库,协议

11.图片

SNMP管理站 SNMP管理代理

管理应用程序<---------->管理信息库-被管对象

- 进程 -

通信原语 通信原语

- -

SNMP管理 SNMP管理

UDP UDP

IP IP

依赖网络协议<--------->依赖网络协议

a.核心是管理者,负责完成网络管理的各个功能,位于一个主机节点,代理一般有多个,管理工作站,一个设备或系统的功能

网络管理员和系统的接口,它的基本构成

a1.一个具有分析数据,发现故障等功能的应用程序

a2.一个用于网络管理员监控网络的接口

a3.将网络管理员的要求转化成远程网络元素的实际监控能力

a4.一个从所有被管理网络实体的MIB中抽取信息的数据库

b.管理代理,设备的平台,主机,网桥,路由器,集线器,支持网络的设备等可以开启SNMP的代理者,实际上是一个守护线程

记录这设备的运行情况,并异步向管理站报告意外事件,并支持查询

c.管理信息库,管理网络资源的方法就是将他们表示为对象,所谓对象是一个表示被管理资源某个方面的属性

,对象的集合被称为管理信息库MIB,任何支持SNMP协议的代理都应该能对MIB中定义的对象信息的查询做出响应

MIB设在代理处,管理站通过读取MIB中的对象值进行网络监控

d.网络管理协议,管理站与代理之间通过SNMP网络管理协议连接的,SNMP是一个应用层协议,使用网络层提供的

UPD传输服务来传递服务来传递信息,标准的代理监听端口为161

总体的流程:当一个网管应用程序要求从代理端信息的时候,它就向SNMP核心进程提出这个请求,核心进程从本地

的MIB中得到所需的对象的信息,然后构成SNMP请求的报文,最后将此报文使用UPD协议发送给代理进程161端口上,

代理进程收到做个请求后,访问其本地的MIB库以取得管理站所需信息,然后构造SNMP响应报文,最后使用UDP协议

将此报文发送给管理站,管理站的SNMP核心进程再将得到的信息传递给管理站上的网管应用程序就完成了一次信息交换

12.SNMP的五中协议数据单元(SNMP报文),进行消息交换:

a.get-request操作:从代理进程处提取一个或多个参数值

b.get-next-request操作:从代理进程处提取紧跟当前参数值的下一个参数值

c.set-request操作:设置代理进程的一个或多个参数值

d.get-reponse操作:返回一个或多个参数之,由代理进程发起,她是前面三中操作的响应操作

e.trap操作:代理进程主动发起的报文,通知管理进程有某些事情发生

a,b,c是管理进程发起的,d,e由代理进程发起的,a,b,c的操作简称,get,set.get-next,都是由161端口get或set报文

13.一个SNMP报文由三个部分组成,公共SNMP首部,get/set首部以及trap首部,变量绑定

a.公共SNMP首部:

a1.版本:版本号减一

a2.共同体(community):字符串,明文口令,常用的是6个字符"public"

a3.PDU类型:0-4,get-request,get-next-request,get-response,set-request,trap

b.get/set首部

b1.请求标识符(request ID),由管理进程设置的一个整数,代理进程在发送get-response报文时

也必须返回此请求标识符,管理进程可以同时向多个代理发出get报文,都是UDP传送,先发送的可能后到达

设置了请求标识符可以使管理进程识别返回的响应报文对应哪个请求报文

b2.差错状态(error status),代理进程回答填入0-5中的一个数字,noError(一切正常),tooBig(代理无法将回答装入到一个SNMP报文中)

noSushName(操作指明了一个不存在的变量),badValue(一个set操作指明了一个无效值或无效语法),readOnly(管理进程试图修改一个只读变量),

genErr(某些其他的差错)

b3.差错索引(error index),当出现noSuchName,badValue或者readOnly的差错时,由代理进程在回答时设置的一个整数,它指

明了有差错的变量在变量列表中的偏移

c.trap首部

企业(enterprise):填入trap报文的网络设备的对象标识符

trap类型:此字段正式的名称是generic-trap,共有七种,coldStart(0,代理进行了初始化),warmStart(1,代理进行了重新初始化),

linkDown(2,一个接口从工作状态变为故障状态),linkUp(3,一个接口从故障状态变为工作状态),authenticationFailure(4,从SNMP管理进程接收到具有一个无效共同体的报文)

egpNeighborLoss(5,一个EGP相邻路由器变为故障状态),enterpriseSpecific(6,代理自定义的事件,需要用后面的"特定代码"来指明)

c1.当使用上述类型2,3,5时,在报文后面变量部分的第一个变量应标识响应的接口

c2.特定代码(specific-code),指明代理自定义的时间(若trap类型为6),否则为0

c3.时间戳(timestamp),指明自代理进程初始化到trap报告的事件发生所经历的时间,单位为10ms,

d.变量绑定(variable-bindings)

指明一个或者多个变量的名和对应的值,在get或者get-next报文中,变量的值应该被忽略

14.管理信息结构SMI是管理信息库中对象定义和编码的基础,用于描述MIB中的对象采用抽象语法记法1(ASN.1)来

形式化定义管理对象

a.数据类型:INTEGER(可有范围限制,或特定范围),OCTERSTRING(0或多个8bit字节,每个字节值在0-255之间),DisplayString(和OCTERSTRING一样,不过每个字节必须是ASCII码),

OBJECTIDENTIFIER(对象的名字,用点分十进制数字表示,反映了它在互联网全局命名树中的位置),NULL(代表相关的变量没有值),IpAdress,PhysAddress,Counter,Gauge(非负整数,比如TCP连接数),

TimeTicks(时间计数器,以0.01秒为单位递增,不同的变量可以有不同的递增幅度,所以需要指定递增幅度),SEQUENCE(和C语言的结构体(structure)类似),SEQUENDEOF(这是一个向量的定义,其所有元素具有相同的类型),

15.管理信息库(Management Information Base)是不同层次上对被管理资源的抽象信息描述的集合

a.数据结构,作为一个公用的数据存放区域,采用了和域名系统DNS类似的树型结构,根节点没有名字

aa1.ROOT为MIB树的根节点,它有三个子树:ISO(1,ISO管理),CCITT(0,由CCITT管理),ISO-CCITT(2,由ISO和CCITT共同管理)

1下有其它子树,其中org(3)是ISO为其它组织定义的子树,org(3)下,特殊点是dod(6)下的一个子树internet(1)分配Internet体系结构委员会来管理,

包含4个子树:

aa1.directory(1,保留给OSI目录服务,以备将来使用),

aa2.mgmt(2,给IAB(Internet体系结构委员会)所批准认可的管理信息库的定义,目前有两个版本:MIB-I,MIB-II),由于任何配置中只能有一个MIB存在,因此俩个版本

MIB提供了相同的对象标识符,大多数用的是MIB-II,Mgmt(2)子树定义了目前最广泛的各种对象,一般称它们"组",定义的组分别为:

aaa1.System组:提供被管理设备的总体信息

aaa2.Interface组:提供网络实体的物理层接口的信息,包括配置信息和每个接口上发生事件的统计信息

aaa3.Ip组:提供了一个网络节点中有关IP实现和操作的信息

aaa4.At组:设备的地址转换信息,MIB-II下,改组内容在Ip下

aaa5.Icmp组:包括了有关ICMP的实现和操作的信息,保存了对各种类型的ICMP信息的接收和发送的统计结果

aaa6.Tcp组:主要用于对流量控制,丢失重传和网络拥挤等问题的解决

aaa7.Udp组:提供了有关UDP发送和接收数据包的信息

aaa8.Egp组:由有关实体的EGP信息和一个记录每个EGP邻居信息的表组成

aaa9.Snmp组:包括有关SNMP实现和操作的信息

aa3.experimental(3,包含了Internet试中使用的对象)

aa4.private(4,定义用户扩展的对象)

定义最多的部分是该子树下的enterprises(1)节点,该节点下的每个子树分配给了一个企业,而企业必须先向IAB登记注册

它们自己的厂商代码,然后就可以在该代码下创建她们自己的对象

b.从代理获得MIB变量值的实现,主要是受到来自服务请求经过语法分析,消息认证等过程,得到值,具体步骤:

b1.建立管理者和代理之间的连接,使用无连接的数据报层,构造Socket,使用bind系统调用进行地址绑定

是用来给自己建立的socket分配任意地址和端口号,把internet地址设置为INADDR-ANY,系统将会在可选择的本机地址中选择

一个可用的地址进行绑定,绑定后,就可以利用此套接口进行通信

b2.构造协议数据单元(PDU),根据用户输入信息,构造一个PDU数据结构,构造一个可以用来传送消息的PDU,将所请求对象放入变量绑定列表

,并将变量绑定加入到PDU中,协议数据单元构造好后,发送消息,Send to西工调用将获取目的地址并发送报文,接受代理的响应,读取数据

16.生成树协议(Spanning Tree Protocol,STP),是一种链路管理协议,为网络提供了路径冗余同时防止产生环路,为使以太网更好地工作,两个工作站之间只能

有一条活动路径,网络环路的发生有多种原因,最常见的一种的是有意生成的冗余,万一一个链路或交换机失败,会有另一个链路或交换机代替,STP允许网桥之间互相

通信以发现网络物理环路,定义了一种算法,网桥能够使用它创建无环路(loop-free)的逻辑拓扑结构,换句话说,STP创建了一个由无环路树叶和树枝构成的树结构

,其跨越了整个第二层网络,生成树操作对终端站透明,就是终端不知道

17.STP工作原理通过桥接协议数据单元(Bridge Protocol Data Unit-BPDU)交换各自状态信息,选出网络中根交换机和根节点,并为每个网段(switched segment)

选出根节点端口和指定端口,类似于最小生成树的算法,利用生成树的算法可以决定网络(哪台计算机主机在哪个区段),并通过BPDU信息交换以上数据

a.通过评估它所接收到的所有配置和选择最优选项,来决定一个网桥可发送的最佳信息

b.一旦选定某网桥发送的消息,网桥将该信息与来自无跟(non-root)连接的可能配置信息比较,如果a中选择的最佳选项并不优于可能配置信息,便删除该端口

18.生成树协议拓扑结构的思路是:网桥能够自动发现一个没有环路的拓扑结构的子网,也就是生成树,生成树协议还能够确定有足够的连接通向这个网络的每一个部分

它将建立整个局域网的生存树,当首次连接网桥或者发生拓扑结构变化时,网桥都将进行生成树拓扑的重新计算,当一个网桥收到某种类型的"设置信息"(一种特殊类型的桥接协议数据单元,BPDU)

时,网桥就开始从头实施生成树算法,这种算法从根网桥的选择开始的,根网桥(root bridge)是整个拓扑结构的核心,所有的数据实际上都要通过根网桥,下一步就是让每一个网桥

确定通向根网桥的最短路径,这一步会在每一个局域网进行,它选择指定的网桥,或者与根网桥最接近的网桥,指定的网桥将把数据从局域网发送到根网桥,最后一步是每个网桥要选择

一个根端口,所谓根端口也就是"用来向根网桥发送的数据的端口"

18.三种基于SNMP的网络拓扑发现算法的研究,为实现网络拓扑的自动生成,首先收集构造网络拓扑图的各种必要信息,利用各种网络路由搜索算法和相关协议

来获取整个网络中每个设备的路由信息,然后利用获取的路由信息来自动实现拓扑的生成,网络拓扑发现的算法主要发生在网络层和数据链路层,网络层通过每个路由器的MIB-II

库的ipRouterTable中获取,比较简单,对于指定深度的网络,基于SNMP的拓扑发现算法通常是使用一个种子路由器,通常使用本机网关的IP地址,获取其路由表内记录的所有可达

网段,以及到达网段所经过的下一跳路由器的端口和IP地址以及相关路由信息,并且它将继续扩展搜索,一直达到用户指定的深度为止,同时它还鞥获取每个路由设备上所有端口的直连子网

以及相应的子网掩码,采用类似广度优先搜索算法,主要用到了三条链表:

a.待检路由设备网关链表,拓扑信息链表,子网信息链表,指定深度内,总是将待检路由设备的网关信息放入待检设备网关链表,处理完后即将其从该链表删除,并将

已经取得的路由设备的网关信息放入拓扑信息链表,将这些网关对应的子网信息放入子网信息链表,算法会在搜索过程中指定深度后停止,最后只需要通过检索拓扑信息链表,就可以

获得指定深度范围的所有路由设备以及其互相连接的关系,通过检索子网信息链表又可以获得路由设备连接的子网以及子网内所有的活动主机的信息

b,需要的路由相关信息:

bb1.ipRouteIfIndex(网关的接口号,1.3.6.1.2.1.4.21.1.2)

bb2.ipRouteNextHop(下一跳网关的IP地址,1.3.6.1.2.1.4.21.1.7)

bb3.ipRouteType(路由类型,1.3.6.1.2.1.4.21.1.8)direct(3),indirect(4)

bb4.ipRouteMask(网段的子网掩码,1.3.6.1.2.1.4.21.1.11)

bb5.ipAdEntAddr(网关的IP地址,1.3.6.1.2.1.4.20.1.1)

bb6.ifDescr(接口的描述(指定了VLAN号),1.3.6.1.2.1.2.2.1.2)

c.流程:

c1.初始化待检路由设备网关链表,拓扑信息链表,子网信息链表

c2.向种子路由设备发送PDU征询数据包,从返回的数据包中解析每条记录中的路由相关信息,如果ipRouteType值为3,则

ipRouteNextHop值加入拓扑信息链表,将ipRouteNextHop,ipRouteDest,ipRouteMask,ipRouteIfIndex,ipDescr值加入子网信息链表

若ipRouteType值为4,则将ipRouteNextHop和ipAdEntAddr值加入拓扑信息链表,若子网信息链表中无节点的IP地址与ipRouteNextHop相同,则

将ipRouteNextHop加入待检设备网关链表,将该节点的跳数加一

c3.从待检路由设备网关链表中删除当前已经被处理过的节点并判断是否继续处理

19.链路层拓扑的获取算法,基于SNMP:

a.确定子网内需要探测的节点,对于支持SNMP协议的节点,根据MIB-II中信息(system组的ipForwarding和sysService变量来确定)确定类型,区别交换机和主机

,不支持SNMP协议的节点,根据节点分类

b.确定交换机和交换机之间的连接关系:

bb1.基于交换机地址转发表的拓扑发现和基于交换机生成树的拓扑发现

c.确定交换机与主机之间的关系

20.利用SNMP主要是基于交换机地址转发表的拓扑发现和基于交换机生成树的拓扑发现

21.实现网络拓扑发现的算法很多,判断优劣的指标参数主要有:

a.网络负荷:应不能增加太多流量

b.发现延迟:发现时间应该最大限度地减少

22.相关术语

a.交换机的端口与其他交换机相连,称为中继端口,反之为叶端口

b.接手来自根节点的数据包的中继端口称为上行端口,其余的中继端口为下行端口

c.第i台交换机Si的第j个端口为Sij

d.Aij表示交换机的地址转发表中通过端口Sij收到的数据帧的源MAC地址集合

e.简单连接:俩个交换机Si和Sk通过端口x和端口y简单连接仅当它们彼此通过端口和端口直接连接或者中间经过多个其它交换机后

间接连接

f.端口Sij的地址转发表是完整的,是指在给定子网中若交换机Sk发出的数据帧可以通过端口Sij到达Si,则Sk的MAC地址必然出现在

Aij中

g.对于交换机Si的任意端口x,T(x/i)表示穿过交换机Si的端口x后所能转发的MAC地址集合(即交换机Si中的除了端口x外的其余各端口的所有能转发的MAC地址的集合)