



(12) 发明专利

(10) 授权公告号 CN 1713617 B

(45) 授权公告日 2012.05.16

(21) 申请号 200510005964.6

第 37 行 - 第 6 栏第 46 行 .

(22) 申请日 2005.01.31

US 6098157 A, 2000.08.01, 全文 .

(30) 优先权数据

审查员 赖异

176535/2004 2004.06.15 JP

(73) 专利权人 株式会社日立制作所

地址 日本东京都

(72) 发明人 赤羽真一 长坂充 须贝和雄

石川有一

(74) 专利代理机构 永新专利商标代理有限公司

72002

代理人 胡建新

(51) Int. Cl.

H04L 12/56 (2006.01)

H04L 12/24 (2006.01)

(56) 对比文件

US 2002141343 A1, 2002.10.03, 全文 .

US 6473400 B1, 2002.10.29, 说明书第 4 栏

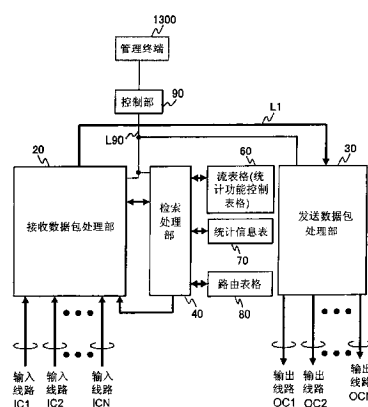
权利要求书 4 页 说明书 23 页 附图 17 页

(54) 发明名称

通信统计收集装置

(57) 摘要

本发明提供一种可动态选择统计对象包、收集不同数据包流的统计信息的通信统计信息收集装置。具有：流表格检索部，从流表格中检索对应于检索关键字的流项目；对不同流收集统计信息的统计收集处理部；统计信息通知包生成部，生成用于将存放的统计信息通知给收集装置的包；项目管理部，按照从流表格中检索到的统计控制项目表示的统计控制信息，更新流表格；和拷贝生成部，按照从流表格中检索到的特定项目表示的统计控制信息，以规定的采样速率来生成应传送给收集装置的采样包。



1. 一种通信统计信息收集装置,具有:由定义了用于识别数据包流的流识别条件的多个流项目构成的流表格;以及检索处理部,将从网络接收数据包的标题中提取的多个标题信息项目的组合作为流检索关键字,从上述流表格中检索具有与上述流检索关键字对应的流识别条件的流项目,该通信统计信息收集装置利用上述流表格的检索结果,收集不同数据包流的统计信息,其特征在于:

所述通信统计信息收集装置具有统计功能控制表格,该统计功能控制表格包含至少一个统计控制项目,该统计控制项目与流识别条件对应地定义了用于限定应成为统计对象的数据包的统计控制信息;

上述检索处理部根据由各接收数据包的标题信息生成的上述流检索关键字,检索上述流表格,在没有对应于上述流检索关键字的流项目的情况下,检索上述统计功能控制表格,在检索到对应于上述流检索关键字的统计控制项目时,根据该统计控制项目所表示的统计控制信息,执行与该统计控制项目的流识别条件对应的数据包流的统计信息的收集处理。

2. 根据权利要求1所述的通信统计信息收集装置,其特征在于:

所述检索处理部具备变更单元,该变更单元用于在检索到作为与上述流检索关键字对应的项目的上述统计控制项目时,根据该统计控制项目所表示的统计控制信息,变更所述流表格或统计功能控制表格的内容。

3. 根据权利要求1或2所述的通信统计信息收集装置,其特征在于:

具有统计信息表,该统计信息表由与所述流表格和统计功能控制表格的各项目对应的用于存放统计信息的多个统计信息项目构成,

所述检索处理部具备统计收集处理部,该统计收集处理部对于通过所述流检索关键字检索到的流项目或与统计控制项目对应的统计信息项目,执行伴随着数据包接收的统计信息的更新处理。

4. 根据权利要求1或2所述的通信统计信息收集装置,其特征在于:

所述统计功能控制表格包含第1、第2统计控制项目,该第1、第2统计控制项目对于成为上述流检索关键字的多个标题信息项目中的至少一个,指定成为统计对象的数据包应具备的标题信息值来作为流识别条件,

上述第1统计控制项目的统计控制信息对于与流识别条件对应的数据包流,指定对通过上述流检索关键字识别的不同数据包流应收集统计信息;上述第2统计控制项目的统计控制信息对于与流识别条件对应的数据包流,指定应以规定的采样速率来生成接收数据包的拷贝,

所述检索处理部具备:追加单元,在检索到作为与上述流检索关键字对应的项目的上述第1统计控制项目时,向所述流表格追加将上述流检索关键字设为流识别条件的新的流项目;和开始单元,在检索到作为与上述流检索关键字对应的项目的上述第2统计控制项目时,开始控制动作,该控制动作用于以规定的采样速率来生成与流识别条件对应的接收数据包的拷贝,并传送到特定的统计信息处理装置。

5. 根据权利要求1或2所述的通信统计信息收集装置,其特征在于:

所述统计功能控制表格包含第1统计控制项目,该第1统计控制项目对于成为上述流检索关键字的多个标题信息项目中的至少一个,指定成为统计对象的数据包应具备的标题信息值来作为流识别条件,并且包含作为统计控制信息的一部分的表示应登录新的流项目

的登录标志,

所述检索处理部具有项目管理部,该项目管理部在从上述统计功能控制表格中检索到作为与上述流检索关键字对应的统计控制项目的上述第 1 统计控制项目时,把新的流项目追加到所述流表格中,该新的流项目将从接收数据包的标题中提取出的多个标题信息项目的组合作为流识别条件。

6. 根据权利要求 5 所述的通信统计信息收集装置,其特征在于:

所述第 1 统计控制项目包含作为统计控制信息的一部分的统计处理的开始条件,

所述项目管理部在从上述统计功能控制表格中检索到上述第 1 统计控制项目时,对照上述统计处理的开始条件和与该第 1 统计控制项目对应的统计信息项目所表示的统计信息,在满足统计处理的开始条件的时刻,将所述新的流项目追加到所述流表格中。

7. 根据权利要求 3 所述的通信统计信息收集装置,其特征在于:

所述统计功能控制表格包含作为统计控制信息的一部分的第 2 统计控制项目,该第 2 统计控制项目包含将按规定的采样速率生成的接收数据包的拷贝传送到事先指定的统计信息处理装置的采样处理的开始条件和表示是否执行采样处理的采样处理标志,

所述检索处理部具备:

采样判定部,在从上述统计功能控制表格中检索到作为与上述流检索关键字对应的统计控制项目的上述第 2 统计控制项目时,若采样处理标志为关闭状态,则对上述采样处理的开始条件和与该第 2 统计控制项目对应的统计信息项目所表示的统计信息进行对照,在满足采样处理的开始条件的时刻,将上述采样处理标志变更成打开状态;和

采样处理部,在采样处理标志为打开状态时,按规定的采样速率产生用于生成接收数据包的拷贝的控制信号。

8. 根据权利要求 7 所述的通信统计信息收集装置,其特征在于:

所述第 2 统计控制项目包含作为统计控制信息的一部分的采样处理的结束条件,

所述采样判定部在从所述统计功能控制表格中检索到上述第 2 统计控制项目时,若采样处理标志为打开状态,则对上述采样处理的结束条件和与该第 2 统计控制项目对应的统计信息项目所表示的统计信息进行对照,在满足采样处理的结束条件的时刻,将上述采样处理标志恢复成关闭状态。

9. 根据权利要求 7 所述的通信统计信息收集装置,其特征在于:

由数据包流的频域值来指定所述采样处理的开始条件,与所述第 2 统计控制项目对应的统计信息项目包含有作为统计信息项目的一部分的频域。

10. 一种通信统计信息收集装置,具有:由定义了用于识别数据包流的流识别条件的多个流项目构成的流表格;以及检索处理部,将从网络接收数据包的标题中提取的多个标题信息项目的组合作为流检索关键字,从上述流表格中检索具有与上述流检索关键字对应的流识别条件的流项目,该通信统计信息收集装置利用上述流表格的检索结果,收集不同数据包流的统计信息,其特征在于:

上述流表格包含至少一个统计控制项目,该统计控制项目与流识别条件对应地定义了用于限定应成为统计对象的数据包的统计控制信息,

在从上述流表格中检索到作为与由各接收数据包的标题信息生成的流检索关键字对应的项目的上述统计控制项目时,上述检索处理部根据该统计控制项目所表示的统计控制

信息,执行与该统计控制项目的流识别条件对应的数据包流的统计信息的收集处理,并且根据该统计控制项目所表示的统计控制信息,变更上述流表格的内容。

11. 根据权利要求 10 所述的通信统计信息收集装置,其特征在于:

在检索到作为与上述流检索关键字对应的项目的上述统计控制项目时,所述检索处理部根据该统计控制项目所表示的统计控制信息,生成新的流项目,并向所述流表格中追加该流项目。

12. 根据权利要求 10 或 11 所述的通信统计信息收集装置,其特征在于:

具有统计信息表,该统计信息表由与所述流项目的各流项目对应的用于存放统计信息的多个统计信息项目构成,

所述检索处理部具备统计收集处理部,该统计收集处理部对于与从所述流表格中检索到的流项目对应的统计信息项目,执行伴随着数据包接收的统计信息的更新处理。

13. 根据权利要求 10 或 11 所述的通信统计信息收集装置,其特征在于:

所述流表格包含第 1 统计控制项目,该第 1 统计控制项目对于成为上述检索关键字的多个标题信息项目中的至少一个、指定成为统计对象的数据包应具备的标题信息值来作为流识别条件,并包含作为统计控制信息的一部分的表示应登录新的流项目的登录标志,

所述检索处理部在从上述流表格中检索到上述第 1 统计控制项目时,把新的流项目追加到所述流表格中,该新的流项目将从接收数据包的标题中提取出的多个标题信息项目的组合作为流识别条件。

14. 根据权利要求 12 所述的通信统计信息收集装置,其特征在于:

所述流表格包含第 2 统计控制项目,该第 2 统计控制项目作为统计控制 信息的一部分,包含按规定的采样速率将接收数据包的拷贝传送到事先指定的统计信息处理装置的采样处理的开始条件和表示是否执行采样处理的采样处理标志,

所述检索处理部具备:

采样判定部,在从上述流表格中检索到上述第 2 统计控制项目时,若采样处理标志为关闭状态,则根据上述采样处理的开始条件和与该第 2 统计控制项目对应的统计信息项目所表示的统计信息,判定采样处理是否开始,并在满足采样处理的开始条件的时刻,将上述采样处理标志变更成打开状态;和

采样处理部,在采样处理标志为打开状态时,按规定的采样速率产生用于生成接收数据包的拷贝的控制信号。

15. 根据权利要求 14 所述的通信统计信息收集装置,其特征在于:

所述第 2 统计控制项目包含作为统计控制信息的一部分的采样处理的结束条件,

所述采样判定部在检索到所述第 2 统计控制项目时,若采样处理标志为打开状态,则根据上述采样处理的结束条件和与该统计控制项目对应的统计信息项目所表示的统计信息,判定采样处理是否结束,在满足采样处理的结束条件的时刻,将上述采样处理标志恢复成关闭状态。

16. 根据权利要求 14 所述的通信统计信息收集装置,其特征在于:

由数据包流的频域值来指定所述采样处理的开始条件,与所述第 2 统计控制项目对应的统计信息项目包含有作为统计信息项目的一部分的频域。

17. 一种与网络连接的通信统计信息收集装置,其特征在于,具有:

流表格,由与用于识别数据包流的流识别条件对应地定义了统计控制信息的多个流项目构成;

统计信息表,由与上述流表格的各项对应地存放统计信息的多个统计信息项目构成;

流表格检索部,将从接收自上述网络的数据包的标题中提取的多个标题信息项目的组合作为流检索关键字,从上述流表格中检索具有与上述流检索 关键字对应的流识别条件的流项目;

统计收集处理部,在与通过上述流表格检索部检索到的流项目对应的统计信息项目中,收集不同数据包流的统计信息;

统计信息通知包生成部,生成用于将存放在上述统计信息表中的统计信息通知给事先指定的其它统计信息处理装置的数据包;和

拷贝生成部,根据由上述流表格检索部检索到的特定的流项目所表示的统计控制信息,以规定的采样速率来生成应传送给上述其它统计信息处理装置的接收数据包的拷贝。

18. 根据权利要求 17 所述的通信统计信息收集装置,其特征在于:

所述流表格包含至少一个统计控制项目,该统计控制项目与流识别条件对应,定义了用于限定应成为统计对象的数据包的统计控制信息,其中,该流识别条件为对于成为上述流检索关键字的多个标题信息项目中的至少一个,指定了成为统计对象的数据包应具备的标题信息值,

所述通信统计信息收集装置具有项目管理部,该项目管理部在由所述流表格检索部检索到作为与上述流检索关键字对应的项目的上述统计控制项目时,根据该项目表示的统计控制信息,把新的流项目追加到上述流表格中,该新的流项目将上述流检索关键字的内容设为流识别条件。

19. 根据权利要求 18 所述的通信统计信息收集装置,其特征在于:

所述项目管理部监视所述统计信息表的状态变化,检测超过规定时间时统计信息没有变化的统计信息项目,并从上述统计信息表和所述流表格中读出该统计信息项目所表示的统计信息和与该项目对应的流识别条件,提供给所述统计信息通知包生成部。

20. 根据权利要求 18 所述的通信统计信息收集装置,其特征在于:

所述项目管理部在向所述流表格追加新的流项目时,根据需要选择应从上述流表格中删除的流项目,并从上述流表格和所述统计信息表中读出该流项目表示的流识别条件和与该流项目对应的统计信息项目所表示的统计信息,并提供给所述统计信息通知包生成部。

通信统计收集装置

[0001] 本发明涉及一种通信统计收集装置,具体而言,是涉及一种作为节点装置连接于通信网络上、对不同数据包流来分别收集数据包数量、字节数量等统计信息的通信统计收集装置。

背景技术

[0002] 因特网作为重要的社会基础设施而存在,不仅应用于以前的 Best-Effort 型数据通信,还开始应用于声音、动态图像等实时数据、或基础业务的事务数据等需要保证通信品质的数据通信中。另外,伴随基于 ADSL(Asymmetric Digital Subscriber Line) 或 FTTH(Fiber To The Home) 技术的访问线路的宽频带化,被通信的数据量也倾向于增大。

[0003] 在这种背景下,媒介或 ISP(Internet Service Provider) 等通信服务商为了把握网络上的通信状态,需要执行通信数据量等统计信息的收集或分析的网络监视功能。尤其是,对按数据的发送源或目的地、应用、品质等级等分类的不同通信数据群(下面称为流)分别收集、分析统计信息的功能的高度化要求很高。

[0004] 媒介或 ISP 通过利用这种每个流的统计信息,在提供品质保证的通信服务时,能确认通信品质的保证状况。另外,能有效使用有限的网络资源,执行对应于数据量增大的通信工程(下面简称为 TE)。此外,还能进行供应,预测顾客的需要,有计划地准备网络资源,对通信频带或服务用户请求迅速地提供网络资源,或检测不正当用户对网络资源的攻击,并进行分析、收费等。通常将统计信息收集功能装备在网络上执行数据包传送控制的路由器、开关等节点装置中。

[0005] 作为流统计信息的收集方式,已知例如 http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/nflov_pg.ppt 中记述的高速缓冲存储器(cache)型流统计技术(非专利文献1)。使用上述现有技术的统计信息收集系统由分散配置在网络上的多个统计信息收集装置、和根据从这些统计信息收集装置定期通知的统计信息来分析网络整体的通信量的收集(collector)装置构成。

[0006] 具有高速缓冲存储器型统计信息收集功能的路由器具备识别接收数据包的所属流用的流表格,按照组合接收数据包的标题信息项目或数据包的输入线路接口序号等构成的检索关键字,检索流表格。流表格由对每个流准备的多个流项目(flow entry)构成,各流项目例如通过发送源 IP 地址、目的地 IP 地址、协议种类、TOS(Type of Service) 值、发送源 TCP(TransmissionControl Protocol)/UDP(User Datagram Protocol) 端口序号、目的地 TCP/UDP 端口序号、输入线路界面序号等的组合,定义流识别条件。

[0007] 在接收数据包与登录在协议中的某个流识别条件一致的情况下,对于与该流识别条件对应准备的统计信息项目,更新数据包数量或字节数量等统计数据。上述流表格检索的结果,在接收数据包与协议上的任一流识别条件都不一致的情况下,将把构成检索关键字的标题信息项目与输入界面序号等的组合作为流识别条件的新的流项目追加到流表格中。定期监视统计信息项目的内容,例如将一定期间以上、统计数据没有变化的统计信息项目的内容作为统计信息数据发送到收集装置。另外,通过老化处理,从表格中删除已通知给

收集装置的统计信息项目、和与之对应的流项目。

[0008] 作为流统计信息的其它收集方式,已知例如 Internet Engineering TaskForce(IEFT) 的 RFC3176(非专利文献 2)中记载的采样型流统计技术。在采样型统计信息收集系统中,各路由器有选择地将接收数据包的拷贝传送到收集装置,收集装置侧从这些拷贝数据包中识别流,执行统计信息的收集与分析。

[0009] 构成采样型统计信息收集系统的各路由器按照事先由网络管理者设定的采样速率,采样接收数据包,按事先规定的封装(capsule)化格式,将采样到的接收数据包的拷贝(拷贝数据包)传送到收集装置。有时也向各封装化数据包追加例如接收数据包的输入线路界面序号、根据接收数据包的标题信息特定的输出线路界面序号、下一传送对象路由器的 IP 地址(Nest Hop IP 地址)等、流识别用的信息。收集装置从由路由器传送的封装化数据包中提取拷贝数据包,根据拷贝数据包的标题信息、和必要时追加的流识别用信息,识别流,更新不同流的统计信息。

[0010] 在上述封装型的现有统计信息收集系统中,使用于流识别条件与检索关键字的信息要素的组合是固定的,收集统计信息的各路由器对全部接收数据包一律收集不同流的统计信息。因此,存在登录在流表格中的流项目数量和统计信息项目数量增加的问题。

[0011] 通常,流识别所需的流识别条件信息为 200-600 比特左右。作为将这种多个比特信息作为检索关键字来高速执行表格检索的方式,有使用 CAM(Content Addressable Memory)的检索方式。CAM 方式可高速匹配表示登录在存储器中的流识别条件的位模式、和作为检索关键字提供的位模式。但是,CAM 与通常的半导体存储器相比,位单价高,所以如高速缓冲存储器型统计信息收集系统所示,若各路由器的流项目数量增加,则流表格的构成中需要大量的 CAM 芯片,存在路由器价格变高的问题。

[0012] 另外,在高速缓冲存储器型的现有统计信息收集系统中,作为流识别条件,由于只能使用固定的标题信息项目的组合,所以难以将上述信息项目之外的其它信息要素、例如用于识别 TCP 连接的控制包种类的 TCP 标志、或以太网(Ethernet;注册商标名)标题内的目的地 MAC(Media Access Control)地址、发送源 MAC 地址、用于识别虚拟 LAN 的 VLAV(Virtual LAN)识别符等用于流识别。

[0013] 另一方面,在采样型统计信息收集系统中,由于在收集装置侧进行流识别,所以可执行由路由器侧进行流识别的高速缓冲存储器型所不能进行的使用高协议层标题信息的流分类、和基于包数据的内容分析的统计信息的收集。另外,在采样型中,由于能对每个接收数据包的输入线路界面指定是否执行拷贝数据包生成用的采样,所以例如可通过将统计对象包限定成来自特定输入线路的接收数据包,提高流统计精度。

[0014] 但是,在采样型的现有统计信息收集系统中,因为不能指定是否进行基于输入线路界面之外的单位、例如协议种类的采样,所以限制了收集装置的流统计精度的提高。另外,在现有技术中,是否采样需要由网络管理者事先设定,存在不能根据通信量状况来动态改变是否采样的设定的问题。

发明内容

[0015] 本发明的目的在于提供一种可动态选择统计对象包、收集不同数据包流的统计信息的通信统计信息收集装置。

[0016] 本发明的另一目的在于提供一种可对于具有事先指定的属性的数据包流、在流表格中灵活登录流识别项目的通信统计信息收集装置。

[0017] 本发明的再一目的在于提供一种可根据数据包流来选择地使用高速缓冲存储器型和采样型统计信息收集功能的通信统计信息收集装置。

[0018] 为了实现上述目的,本发明的统计信息收集装置具有由定义用于识别数据包流的流识别条件的多个流项目构成的流表格;统计功能控制表格,与流识别条件对应,包含定义了用于限定应成为统计对象的数据包的统计控制信息的至少一个统计控制项目;和检索处理部,将从网络接收数据包的标题中提取的多个标题信息项目的组合作为流检索关键字,从上述流表格和统计功能控制表格中检索具有对应于流检索关键字的流识别条件的流项目,

[0019] 上述检索处理部按照根据各接收数据包的标题信息生成的流检索关键字,检索流表格,在没有对应于流检索关键字的流项目的情况下,检索统计功能控制表格,在检索到对应于上述流检索关键字的统计控制项目时,按照该统计控制项目表示的统计控制信息,执行对应于该统计控制项目的流识别条件的数据包流的统计信息收集处理。

[0020] 本发明的特征之一在于,上述检索处理部在检索到统计控制项目、作为对应于流检索关键字的项目时,按照该统计控制项目表示的统计控制信息,变更上述流表格或上述统计功能控制表格的内容。

[0021] 上述统计控制项目与通常的流项目不同,作为流识别条件,对成为流检索关键字的多个标题信息项目中的至少一个,指定成为统计对象的数据包应具备的标题信息值。在本发明的最佳实施方式中,为了使表格检索高速化,将上述统计功能控制表格统一为流表格,在看不到与流检索关键字对应的流项目时,从流表格中检索与流检索关键字对应的统计控制信息项目。

[0022] 具体而言,本发明的通信统计信息收集装置具有由与各个流项目和统计控制项目对应、用于存放统计信息的多个统计信息项目构成的统计信息表,上述检索处理部具备统计收集处理部,对于通过流检索关键字检索到的流项目或与统计控制项目对应的统计信息项目,执行伴随数据包接收的统计信息的更新处理。

[0023] 本发明的一个特征在于,上述统计功能控制表格(或流表格)包含第1统计控制项目,作为统计控制信息的一部分,该第1统计控制项目包含表示应登录新的流项目的登录标志,具有项目管理部,当上述检索处理部检索到上述第1统计控制项目、作为对应于流检索关键字的项目时,为了收集由流检索关键字特定的不同数据包流的统计信息,将把从接收数据包的标题中提取出的多个标题信息项目组合设为流识别条件的新的流项目追加到上述流表格中。

[0024] 本发明的再一特征在于,上述统计功能控制表格(或流表格)包含第2统计控制项目,利用统计控制信息,对与流识别条件对应的数据包流指定应按规定采样速率生成接收数据包的拷贝,上述检索处理部在检索到上述第2统计控制项目、作为对应于流检索关键字的项目时,开始控制动作,以规定的采样速率生成对应于流识别条件的接收数据包的拷贝,将拷贝数据包传送到特定的统计信息处理装置。

[0025] 在本发明的1实施例中,上述第2统计控制项目包含按规定的采样速率将生成的接收数据包的拷贝传送到事先指定的统计信息处理装置的采样处理的开始条件、和表示是

否执行采样处理的采样处理标志,作为统计控制信息的一部分,上述检索处理部具备采样判定部,在检索到上述第 2 统计控制项目作为对应于流检索关键字的项目时,若采样处理标志为关闭状态,则对照上述采样处理的开始条件、和对应于该第 2 统计控制项目的统计信息项目表示的统计信息,在满足采样处理的开始条件的时刻,将上述采样处理标志变更成打开状态;和采样处理部,在采样处理标志为打开状态时,按规定的采样速率产生用于生成接收数据包的拷贝的控制信号。

[0026] 在本发明的 1 实施例中,上述第 2 控制项目包含采样处理的结束条件,作为统计控制信息的一部分。此时,采样判定部在从统计功能控制表格中检索到第 2 控制项目时,若采样处理标志为打开状态,则对照上述采样处理的结束条件、和与该第 2 控制项目对应的统计信息项目表示的统计信息,在满足采样处理的结束条件的时刻,将上述采样处理标志恢复成关闭状态。例如由数据包流的频域值来指定采样处理的开始条件和结束条件。

[0027] 从其它观点看,本发明的通信统计信息收集装置具有流表格检索部,将从由网络接收到的数据包的标题中提取的多个标题信息项目的组合作为流检索关键字,从流表格中检索具有与流检索关键字对应的流识别条件的流项目或统计控制项目;

[0028] 统计收集处理部,在与通过上述流表格检索部检索的项目对应的统计信息项目中,收集不同数据包流的统计信息;

[0029] 统计信息通知包生成部,生成用于将存放在统计信息表中的统计信息通知给事先指定的其它统计信息处理装置的包;和

[0030] 拷贝生成部,按照由上述流表格检索部检索到的特定流项目表示的统计控制信息,以规定的采样速率来生成应传送给上述其它统计信息处理装置的接收数据包的拷贝。

[0031] 本发明的通信统计信息收集装置的一个特征在于,具有项目管理部,在所述流表格检索部检索到上述统计控制项目、作为对应于流检索关键字的项目时,按照该项目表示的统计控制信息,把将上述流检索关键字的内部设为流识别条件的新的流项目追加到上述流表格中。

[0032] 可通过上述项目管理部来执行向统计信息通知包生成部提供统计信息。在本发明的 1 实施例中,上述项目管理部监视所述统计信息表的状态变化,检测越过规定时间统计信息没有变化的统计信息项目,并从上述统计信息表与流表格中读出该统计信息项目表示的统计信息和与该项目对应的流识别条件,提供给上述统计信息通知包生成部。另外,在向流表格追加新的流项目时,所述项目管理部选择必要时应从流表格中删除的流项目,并从上述流表格和所述统计信息表中读出该流项目表示的流识别条件、和对应于该流项目的统计信息项目表示的统计信息,提供给所述统计信息通知包生成部。

[0033] 在本发明中,由各流项目定义的流识别条件除例如从接收数据包的 IP 标题中提取的标题信息项目外,还可设为 TCP 或 UDP 等从层 4 标题、或 Ethernet 等的层 2 标题中提取的标题信息项目、接收数据包的输入线路序号和输出线路序号的组合。

[0034] 根据本发明,因为可由统计控制项目表示的统计控制信息来限定成为统计对象的数据包流的种类,所以可抑制登录于流表格中的流项目数量的增加。因此,可减少流表格所需的高速存储器的容量,降低装置价格。

[0035] 另外,根据本发明的结构,可通过统计控制项目的统计控制信息来选择地执行高速缓冲存储器型和采样型的统计信息收集,也可指定为了采样型的统计信息收集而应传送

到收集装置的拷贝数据包的生成条件。例如,对于将成为监视对象的特定数据包流的属性设为流识别条件的统计控制项目,通过指定表示采样开始条件的频域值来作为统计控制信息的一部分,在上述特定数据包流的频域到达开始条件的时刻,开始接收数据包的采样,并开始向收集装置传送拷贝数据包。

[0036] 此时,因为可限定发送到收集装置的采样的母集团,所以收集装置中的统计信息的存放变容易,可提高分析精度。另外,由此例如可容易自动检测对特定服务器的攻击数据、病毒数据等、通信量图案有特征的数据包流,并进行分析。另外,由此可有效利用网络或收集装置的资源。

附图说明

[0037] 图 1 是表示使用本发明的统计收集装置的通信网络一例的图。

[0038] 图 2 是表示由图 1 的通信网络通信的数据包的格式图。

[0039] 图 3 是表示 Ethernet V2 的帧的标题格式的图。

[0040] 图 4 是表示 Tag VLAN 对应的 Ethernet V2 帧的标题格式的图。

[0041] 图 5 是表示 IPv4 数据包的标题格式的图。

[0042] 图 6 是表示 IPv6 数据包的标题格式的图。

[0043] 图 7 是表示 TCP 的标题格式的图。

[0044] 图 8 是表示图 7 中的 TCP 标志 133 的细节的图。

[0045] 图 9 是表示 UDP 标题的格式的图。

[0046] 图 10 是表示由图 1 的路由器 R1 收集的流识别条件一例的图。

[0047] 图 11 是表示由图 1 的路由器 R1 收集的统计信息的一例的图。

[0048] 图 12 是表示具备本发明的统计收集功能的路由器 R1 一实施例的结构图。

[0049] 图 13 是表示本发明的路由器 R1 与管理终端 1300 的连接关系的一例的图。

[0050] 图 14 是表示本发明的路由器 R1 与管理终端 1300 的连接关系的另一例的图。

[0051] 图 15 是表示在本发明的路由器内部处理的内部数据包的格式一例的图。

[0052] 图 16 是表示图 12 的接收数据包处理部 20 的一实施例的框图。

[0053] 图 17 是表示积累在图 16 的存储器 25A、25B 中的数据包数据管理信息块 200 的一例的图。

[0054] 图 18 是表示积累在图 16 的存储器 25A(或 25B) 中的数据包数据管理信息块、与积累在存储器 24 中的数据块的关系图。

[0055] 图 19 是表示图 16 的发送数据包处理部 30 的 1 实施例的框图。

[0056] 图 20 是表示图 16 的检索处理部 40 的 1 实施例的框图。

[0057] 图 21 是表示图 16 的流表格 60 的一例的图。

[0058] 图 22 是表示图 16 的统计信息表 70 一例的图。

[0059] 图 23 是表示图 20 的检索结果输出部 48 输出的检索结果通知 480 的一例的图。

[0060] 图 24 是表示图 16 的拷贝管理部 28 具备的地址释放控制表格 280 的一例的图。

[0061] 图 25 是表示图 20 的流管理表格 49 的一例的图。

[0062] 图 26 是表示图 20 的统计信息通知数据包生成部 53 输出的统计信息通知数据包 300 的格式一例的图。

[0063] 图 27 是用于说明图 12 所示的流表格 60 的另一实施例的图。

[0064] 图 28 是用于说明图 12 所示的统计信息表 70 另一实施例的图。

具体实施方式

[0065] 下面,参照附图来说明本发明的通信统计信息收集装置的实施例。

[0066] 图 1 表示使用本发明的通信统计信息收集装置的网络结构的一例。

[0067] 这里所示的网络 NW 由容纳了终端 T1、T2、T3、T4 的路由器 R1、容纳了服务器 S1 的路由器 R2、容纳了服务器 S2 的路由器 R3、和连接于路由器 R1 的统计信息的收集装置 C1 构成,路由器 R1 具备作为本发明的通信统计信息收集装置的功能。终端 T1、T2、T3、T4 分别经线路 C-T1、C-T2、C-T3、C-T4 连接于路由器 R1 上,路由器 R1 经线路 C-R2、C-R3 连接于路由器 R2、R3 上。

[0068] 在上述网络 NW 中,在终端 T1、T3 与服务器 S1、终端 T2、T4 与服务器 S2 进行通信中,将从服务器 S1 发送到终端 T1、T3 的 IP(Internet Protocol) 数据包的流分别称为“流 1”、“流 2”,将从服务器 S2 到终端 T2、T4 的 IP 数据包流分别称为“流 3”、“流 4”。

[0069] 这里,流 1 由 IP 的上位协议为 TCP、IP 标题内的 TOS(Type of Service) 为 TOS1、TCP 标题内的发送源端口序号与目的地端口序号分别为 SPRT1、DPRT1 的数据包串构成,流 2 由 IP 的上位协议为 TCP、TOS 为 TOS1、发送源端口序号与目的地端口序号分别为 SPRT1、DPRT3 的数据包串构成。另外,流 3 由 IP 的上位协议为 UDP、TOS 为 TOS2、UDP 标题内的发送源端口序号与目的地端口序号分别为 SPRT2、DPRT2 的数据包串构成,流 4 由 IP 的上位协议为 UDP、TOS 为 TOS2、发送源端口序号与目的地端口序号分别为 SPRT2、PRT4 的数据包串构成。

[0070] 图 2 表示在上述网络上通信的 IP 数据包 10 的结构。

[0071] IP 数据包 10 由对应于 OSI(Open System Interconnection) 参照模块的协议层的多个层的标题、具体而言为层 2 标题 11、层 3 标题 12 和层 4 标题 13、与数据 14 构成。

[0072] 作为层 2 的协议,例如可使用 Ethernet(注册商标名)、ATM(Asynchronous Transfer Mode)、MPLS(Multi-Protocol Label Switching) 等协议,作为层 3 的协议,可使用 IP version 4(IPv4)、IP version 6(IPv6) 等协议。另外,作为层 4 的协议,可使用 TCP、UDP 等协议。

[0073] 图 3 表示 Ethernet V2 帧的标题结构,作为层 2 标题 11 的一例。

[0074] 对 Ethernet V2 帧标题,设定表示帧的开始的前置码 /SFD111、层 2 中的目的地终端地址(目的地 MAC 地址)112 和发送源地址(发送源 MAC 地址)113、和表示层 3 的协议的种类 118。

[0075] 图 4 表示 Tag VLAN 对应的 Ethernet V2 帧的标题格式,作为层 2 标题 11 的另一例。对 Tag VLAN 对应的 Ethernet V2 帧标题,设定表示帧的开始的前置码 /SFD111、层 2 中的目的地终端地址(目的地 MAC 地址)112 和发送源地址(发送源 MAC 地址)113、表示是 Tag VLAN 对应的 TAG 协议 ID114、表示帧的传送优先级的优先级 115、表示存储层 2 的路由信息的 CFI(Cannonical Field Indicator)116、VLAN 识别符(VLAN ID)117、和表示层 3 的协议的种类 118。

[0076] 图 5 表示 IPv4 的标题结构,作为层 3 标题 12 的 1 例。

[0077] 在 IPv4 标题中包含表示数据包的传送品质的 ToS121、表示层 4 的协议的协议 122、发送源 IP 地址 126A、目的地 IP 地址 127A 等信息。ToS 和协议分别由 8 比特构成,发送源 IP 地址和目的地 IP 地址分别由 32 比特构成。

[0078] 图 6 表示 IPv6 的标题结构,作为层 3 标题 12 的另 1 例。

[0079] 在 IPv6 标题中,包含表示数据包的传送品质的等级 123、表示在该 IPv6 标题部之后的下一标题的种类的下一标题序号 125、发送源 IP 地址 126B、目的地 IP 地址 127B 等信息。下一标题例如为 TCP 或 UDP 的情况下,设定表示层 4 的协议的值,作为下一标题序号 125。等级 123 和下一标题序号分别由 8 比特构成,发送源 IP 地址和目的地 IP 地址分别由 128 比特构成。

[0080] 图 7 表示 TCP 的标题结构,作为层 4 标题 13 的一例。

[0081] 在 TCP 标题中,包含分别为 16 比特长的发送源端口序号 131A 和目的地端口序号 132A,作为上位层识别应用程序的逻辑端口序号。另外,包含表示 TCP 连接中的数据包种类的 TCP 标志 133 等信息。

[0082] 如图 8 所示, TCP 标志 133 由向接收终端指示将接收数据紧急传递到应用程序的紧急标志 (URG) 1331、通知发送终端接收终端接收到数据的 ACK1332、指示发送终端和接收终端不延迟地传递数据的 PUSH1333、指示 TCP 连接的复位的 RST1334、指示连接的结束的 FIN1335、和指示连接的确立的 SYN1336 的 6 个标志构成。

[0083] 图 9 表示 UDP 的标题结构,作为层 4 标题 13 的另一例。

[0084] 与 TCP 标题一样,在 UDP 标题中包含分别为 16 比特长的发送源端口序号 131B 和目的地端口序号 132B。

[0085] 图 10 表示图 1 的路由器 R1 中定义了成为统计信息的收集对象的流识别条件的流表格的一部分。这里,表示将统计信息的收集对象流限定为层 4 的协议为 TCP 流的情况。

[0086] 流表格的各项与流项目序号 61 相对应,表示流识别条件 62 和未图示的统计控制信息。流识别条件 62 由 IP 标题表示的发送源 IP 地址 621、目的地 IP 地址 622、上位协议 623 和 TOS624、及 TCP 或 UDP 标题中包含的发送源端口序号 625 和目的地端口序号 626 的值定义。另外,这里所示的标题信息的组合不过是流识别条件的一例,流识别条件也可以是与图 10 不同的标题信息的组合。

[0087] 在本发明的统计信息收集装置(路由器 R1)中,通过后述的检索处理部 40,动态执行项目向上述流表格的登录与删除、项目内容的部分纠正。在将向流表格的登录项目限定为协议种类为 TCP 的情况下,路由器 R1 仅将从线路 C-R2、CR-3 接收的数据包流中、上位协议为 TCP 的流 1 与流 2 登录在流表格中。

[0088] 图 11 表示收集在路由器 R1 的统计信息表中的统计信息的一例。

[0089] 统计信息表由与流表格的流项目序号 61 相对应的多个统计信息项目构成。

[0090] 在这里所示的实例中,作为统计信息 72,收集不同流的接收数据包数(下面称为数据包数)721、接收数据包的累计字节数(下面称为字节数)722、接收数据包的输入线路序号 723、成为接收数据包的传送目的地的输出线路序号 724 与其它信息 729。

[0091] 图 12 是表示具备本发明的统计收集功能的路由器 R1 一实施例的框图。

[0092] 路由器 R1 由连接于输入线路 ICn($n = 1-N$)上的接收数据包处理部 20、连接于输出线路 OCn($n = 1-N$)上的发送数据包处理部 30、连接于接收数据包处理部 20 上的检索处

理部 40、附带于检索处理部 40 上的流表格 60、统计信息表 70 和路由表格 80、和控制部 90 构成。流表格 60 如后所述,兼用作存储统计控制项目的统计功能控制表格。控制部 90 连接于管理终端 1300,按照来自管理终端 1300 的指示,对接收数据包处理部 20、检索处理部 40、发送数据包处理部 30 执行各种参数信息的设定。

[0093] 路由器 R1 也可以是分别由专用的 LSI 构成上述接收数据包处理部 20、发送数据包处理部 30、检索处理部 40 和控制部 90,并相互连接这些专用 LSI,为了减少 LSI 之间的布线,也可构成由一个专用 LSI 来实现多个处理部,相互连接少数的专用 LSI。另外,也可由通用的 MPU(Micro Processing Unit) 或 NP(Network Processor) 来实现路由器功能的一部分,来代替使用专用 LSI。

[0094] 图 12 中,示出由信号线 L1 连接接收数据包处理部 20 与发送数据包处理部 30 的结构,但装置也可构成分别将接收数据包处理部 20 与发送数据包处理部 30 的个数设为多个,通过纵横开关来连接接收数据包处理部与发送数据包处理部之间。另外,作为检索处理部 40 参照的流表格 60 用的存储器,在要求高速的检索处理性能的情况下,例如使用 CAM 或 SSRAM,在较低速的检索处理性能即可的情况下,可使用每比特的价格便宜、每比特的芯片面积也少的 DRAM。

[0095] 图 13 表示连接于路由器 R1 的控制部 90 上的管理终端 1300 的一例。

[0096] 管理终端 1300 由用于显示路由器 R1 内的各种表格的内容的显示画面 301、和用于选择、编辑显示于显示画面中的表格内容的任意部位的鼠标 1302、键盘 1303 等的输入单元构成。管理终端 1300 如图 14 所示,也可经网络 NW 连接于路由器 R1。另外,也可使收集装置 C1 具有管理终端 1300 的功能,从收集装置来更新路由器的表格信息。

[0097] 图 15 表示在路由器 R1 内部传送的内部数据包的格式一例。

[0098] 内部数据包构成在图 2 所示来自网络的接收数据包的开头附加内部标题 15。内部标题 15 包含表示数据包的接收线路的输入线路序号 151、分别由检索处理部 40 确定的数据包的输出线路序号 152、封装化指示标志 153、封装标题信息 154。

[0099] 在封装化指示标志 153 中,设定标志信息,用于在需要按规定速率将采样的接收数据包的拷贝传送到收集装置 C1 时,从检索处理部 40 向发送数据包处理部 30 指示接收数据包的封装化。另外,在封装标题信息 154 中,设置在将采样的接收数据包传送到收集装置 C1 时所需的封装化标题的内容(层 2 标题、层 3 标题、层 4 标题)。封装标题信息 154 的内容在封装化指示标志 153 为导通状态时有效。

[0100] 图 16 表示接收数据包处理部 20 的一实施例。

[0101] 接收数据包处理部 20 由分别连接于输入线路 ICi 上的多个线路终端处理部 21-i ($i = 1-N$)、暂时积累从线路终端处理部 21-i 输出的接收数据包的缓冲存储器 22-i ($i = 1-N$)、暂时积累从检索处理部 40 提供的统计信息通知数据包的缓冲存储器 22-(N+1)、连接于这些缓冲存储器上的数据包积累控制部 23、数据包数据积累存储器 24、输入数据包标题积累存储器 25A、输出数据包标题积累存储器 25B、存储器状态管理部 26、标题发送控制部 27、拷贝管理部 28、和数据包传送控制部 29 构成。

[0102] 各线路终端处理部 21-i 在从输入线路 ICi 接收数据包时,执行数据包数据的错误检测等数据包终端处理。各线路终端处理部 21-i 废弃检测到数据错误的接收数据包,将正常接收的数据包积累在缓冲存储器 22-i 中,将数据包接收通知给数据包积累控制部 23。数

据包积累控制部 23 在缓冲存储器 22-(N+1) 中也积累统计信息通知数据包时,从检索处理部 40 经信号线 L530 接收数据包接收通知。

[0103] 数据包积累控制部 23 按照预定的选择规则,从有数据包接收通知的缓冲存储器中读出接收数据包,并生成应附带于接收数据包上的内部标题 15。此时,内部标题 15 中,仅输入线路序号 151 的字段包含有效数据,其它字段 152-154 为空状态。由读出接收数据包的缓冲存储器 22-k($k = 1-N+1$) 来唯一确定输入线路序号 151 的值 k。

[0104] 数据包积累控制部 23 将包含生成的内部标题 15 和从接收数据包提取的层 2 标题 1-层 4 标题 13 的固定长度标题部分作为图 17 中说明的数据包数据管理信息块 200 的一部分,存储在输入数据包标题积累存储器 25A 中。将作为接收数据包的剩余部分的可变长度的数据部 14 存储在数据包数据积累存储器 24 中。

[0105] 在本实施例中,将数据包数据积累存储器 24 分割成固定长度的多个存储器块,由存储器状态管理部 26 来管理各存储器块的空状态(使用状态)。数据包积累控制部 23 在从缓冲存储器中读出一个接收数据包时,请求存储器状态管理部 26 分配个数对应于接收数据包的数据长度的空存储器块,并将接收数据包的数据部 14 分割存储在这些存储器块中。

[0106] 图 17 表示数据包数据管理信息块 200 的一例。

[0107] 数据包数据管理信息块 200 依次读出作为数据部积累用而分配给同一数据包的多个存储器块,由块种类标志 201、分配给同一数据包的存储器块数 202、表示存储在各存储器块中的有效数据长度的有效数据长度 203、存储器地址 204、和标题信息字段 205 构成。

[0108] 存储器地址 204 表示数据包数据积累存储器 24 中的各存储器块的开头地址。另外,对标题信息字段 205 设定图 15 中所示的内部数据包的标题 15、11-13。

[0109] 在本实施例中,如图 18 所示,在向一个接收数据包分配多个空存储器块、例如块 k、块 k+2、块 k+3 的情况下,数据包积累控制部 23 生成数量与分配存储器块数相同的数据包数据管理信息块 200-1 ~ 200-3,并将这些管理信息块以 FIFO 形式存储在输入数据包标题积累存储器 25A 中。块种类标志 201 表示该管理信息块 200 是否是附带于同一数据包的多个数据包数据管理信息块中的开头块。

[0110] 图 18 中,示出将各存储器块的尺寸假设为 L,将从缓冲存储器 22-i 中读出的接收数据包的数据部 14 的长度假设为 $2L + \Delta L$,分配块 k、块 k+2、块 k+3 的三个存储器块的情况。此时,与开头存储器块 k 对应的第 1 数据包数据管理信息块 200-1 对块种类标志 201 设定表示开头块的值,对存储器块数量 202 设定“3”,对有效数据长度 203 设定“L”,对存储器地址 204 如箭头 P1 所示,设定表示存储器块 k 的开头的指针地址值。

[0111] 对上述第 1 数据包数据管理信息块 200-1 的标题信息字段 205 设定内部标题 15、和层 2 标题 11-层 4 标题 13 的值。但是,内部标题 15 中仅输入线路序号 151 有效,输出线路序号 152-封装化标题信息 154 的值未定。如后所述,按照来自检索处理部 40 的检索结果来补充这些未定的标题信息要素。

[0112] 与第 2、第 3 存储器块 k+2、k+3 对应的第 2、第 3 数据包数据管理信息块 200-2、200-3 对块种类标志 201 设定表示该块是后续块的值,将存储器块数 202 与标题信息字段 205 设为未使用。对第 2 数据包数据管理信息块 200-2 的有效数据长度 203 设定“L”,对存储器地址 204 如箭头 P2 所示,设定表示存储器块 k+2 的开头的指针地址值。另外,对第 3 数

据包数据管理信息块 200-3 的有效数据长度 203 设定“ ΔL ”,对存储器地址 204 如箭头 P3 所示,设定表示存储器块 k+3 的开头的指针地址值。

[0113] 这样,在输入数据包标题积累存储器 25A 中,以 FIFO 形式存储数据包数据管理信息块 200-1 ~ 200-3,当由第 1 管理信息块 200-1 来指定构成组的存储器块的个数 204 与应附带于数据部 14 上的标题信息 205 时,依次读出这些 1 组数据包数据管理信息块 200-1 ~ 200-3,并按照各管理信息块表示的存储器地址 204,从数据包数据积累存储器 24 中依次读出分割后积累在多个块中的 1 数据包大小的数据。另外,必要时,通过利用第 1 管理信息块 200-1 所示的标题信息 205,可封装化接收数据包,传送给收集装置 C1。后面说明数据包接收处理部 20 的详细动作。

[0114] 图 19 表示发送数据包处理部 30 的 1 实施例。

[0115] 发送数据包处理部 30 由分别连接于输出线路 OC_i 上的多个线路终端处理部 31-i (i = 1-N)、数据包输出控制部 32、数据包数据积累存储器 33、输出数据包标题积累存储器 34、存储器状态管理部 35、和数据包接收部 36 构成。后面详细描述发送数据包处理部 30 的动作。

[0116] 图 20 表示检索处理部 40 的 1 实施例。

[0117] 检索处理部 40 包括:经信号线 L27 连接于接收数据包处理部的标题发送控制部 27 上的标题信息积累部 41、分别连接于标题信息积累部 41 上的流表格检索部 42、路由表格检索部 43 和流项目管理部 44、采样处理部 45、采样判定部 46、统计收集处理部 47、经信号线 L48 连接于标题发送控制部 27 上的检索结果输出部 48、附带于流项目管理部 44 上的流管理表格 49、统计信息通知数据包标题信息积累部 50、采样数据包标题信息积累部 51、流信息积累部 52、和统计信息通知数据包生成部 53。

[0118] 流表格检索部 42 根据从标题信息积累部 41 输出的标题信息,生成流表格 60 的检索关键字,并将从流表格 60 中检索到的统计控制信息输出到流项目管理部 44 和采样判定部 46。另外,按照来自流项目管理部 44 的指示,执行流表格项目的追加 / 删除,将成为删除对象的流项目的内容输出到流信息积累部 52。

[0119] 路由表格检索部 43 根据从标题信息积累部 41 表示的标题信息中提取的接收数据包的目的地 IP 地址,访问路由表格 80,将从路由表格 80 中检索到的路由信息通知给流表格检索部 42、采样处理部 45、统计收集处理部 47、检索结果输出部 48。

[0120] 统计收集处理部 47 对应于流表格检索部 42 与路由表格检索部 43 的检索结果,更新统计信息表的统计数据。另外,统计收集处理部 47 对应于来自流项目管理部 44 的指令,读出积累在统计信息表 0 的特定项目中的统计信息,将其输出到流信息积累部 52。

[0121] 检索结果输出部 48 当从路由表格检索部 43 接收路由表格 80 的检索结果时,生成图 23 中详细描述检索结果通知 480,并经信号线 L48 将其发送到接收数据包处理部 20 的标题发送控制部 27。

[0122] 本实施例中所示的检索处理部 40 的统计收集处理部 47 具备高速缓冲存储器型的统计功能,按规定定时将积累在统计信息表 70 中的统计数据发送到收集装置 C1;和采样型的统计收集功能,对特定流的接收数据包,按流表格 60 指定的采样速率生成采样(拷贝数据包),并将其发送给收集装置 C1。

[0123] 采样处理部 45 在从流表格(统计功能控制表格)中检索到的统计控制项目的统

计控制信息指示进行采样处理（向收集装置传送拷贝数据包）的情况下，对接收数据包处理部 20 指示生成采样。采样的生成指示信息以包含在检索结果输出部 48 输出到信号线 L48 的检索结果通知中的形式，通知给接收数据包处理部 20。另外，从采样数据包标题信息积累部 51 中读出在将采样发送给收集装置 C1 时所需的目的地 IP 地址等封装化标题信息，作为检索结果通知的一部分，通知给接收数据包处理部 20。

[0124] 采样判定部 46 如后所述，对应于流表格 60 的检索结果，检查接收数据包所属流的统计信息，在变为应开始采样处理的流状态时，执行作为统计控制信息的一部分的采样处理标志的改写。

[0125] 统计信息通知数据包生成部 53 根据积累在流信息积累部 52 中的流条件和统计信息、及统计信息通知数据包标题信息积累部 50 所示的封装化标题信息，生成统计信息通知数据包，经信号线 L53 输出到接收数据包处理部 20 的缓冲存储器 22-C。另外，在统计数据的通知对象与采样数据包的传送对象是同一收集装置的情况下，可由同一存储器来兼用作统计信息通知数据包标题信息积累部 50 与采样数据包标题信息积累部 51。

[0126] 网络管理者可经信号线 L90 与控制部 90 来执行对统计信息通知数据包标题信息积累部 50 与采样数据包标题信息积累部 51 的封装标题信息的设定、与对流表格 60、路由表格 80 的项目信息的设定。

[0127] 图 21 和图 22 表示路由器 R1 具备的流表格 60 与统计信息表 70 的具体内容的一例。

[0128] 流表格 60 如图 21 所示，由与流项目序号 61 相对应、表示流识别条件 62 和统计控制信息 63 的多个项目构成，统计信息表 70 如图 22 所示，由与流项目序号 61 相对应、表示统计信息 72 的多个项目构成。

[0129] 另外，流项目序号 61 表示为将流识别条件 62、统计控制信息 63、统计信息 72 彼此关联的信息，有时由于表格的结构而不需要流项目序号 61。另外，通过将流项目序号 61 用作指针，也可将由流表格 60 定义的 1 群的多个流识别条件与一个统计控制信息项目与一个统计信息项目关联。

[0130] 这里，示出作为流识别条件 62，向图 10 所示的信息要素 621-626 附加其它信息 629 的实例。作为其它信息 629，例如可使用数据包的输入、输出线路序号、图 3 所示的目的地 / 发送源 MAC 地址与种类、图 4 所示的 TAG 协议 ID、优先级、VLAN-ID、图 8 所示的 TCP 标志的至少一部分。

[0131] 从流表格 60 中，作为检索结果，如统计控制信息 63 所示那样，得到登录处理标志 631、登录处理速率 632、统计收集标志 633、频域计算标志 634、采样处理标志 635、采样速率 636、采样判定标志 637、采样开始频域 638、采样结束频域 639、其它信息 640。在这里所示的实例中，除图 11 所示的信息项目 721-724、729 外，向统计信息表 70 追加频域 725，作为统计信息 72。

[0132] 在图 21 所示的流表格 60 中，具有流项目序号 f1、f2 的项目 EN-1、EN-2 定义了图 10 所示的上位协议为 TCP 的流 1、流 2 的流识别条件 62 与统计控制信息 63。在接收数据包的标题信息与项目 EN-1、EN-2 的流识别条件一致的情况下，检索处理部 40 对统计信息表的项目 SE-1、SE-2 所示的信息项目收集统计信息。

[0133] 具有项目序号 F12 的项目 EN-x12 是一个统计控制项目，与其它的项目 EN-1、EN-2

不同,流识别条件 62 的上位协议 623 若为 TCP,则表示流识别条件 62 的其它信息要素 621、622、624-629 可以用任意 (“*”) 来表示。

[0134] 统计控制项目 EN-x12 在统计控制信息 63 的登录处理标志 631 为“1”,登录处理速率为“1/1”,输出项目 EN-x12 的统计控制信息作为流表格 60 的检索结果的情况下,按照上述登录处理标志 631,检索处理部 40 执行向流表格 60 的新的流项目的登录动作。即,上述统计控制项目 EN-x12 用作自动将与流识别条件 62 一致的新的流项目追加到流表格 60 中的流登录用项目。

[0135] 例如,在流表格 60 中,项目 EN-1、EN-2 为未登录状态、路由器 R1 接收了属于流 1 的数据包的情况下,流表格检索部 42 输出项目 EN-x12 的统计控制信息 63,作为基于该数据包的标题信息的流表格 60 的检索结果。如后所述,检索处理部 40 的流项目管理部 44 着眼于流表格检索部 42 输出的统计控制信息 63 的登录处理标志 631,在登录处理标志 631 为“1”时,向流表格检索部 42 指示基于标题信息积累部 41 表示的标题信息的新的流项目 EN-1 的登录。

[0136] 因此,通过在初始状态下对流表格 60 设定流登录用的统计控制项目 EN-x12,在满足该项目的流识别条件的接收数据包的处理时,可自动向流表格 60 追加统计收集用的新的流项目。项目 EN-1、EN-2 通过上述统计控制项目 EN-x12 自动追加到流表格 60 中。处于图 21 的状态时,路由器 R1 在接收到不符合项目 EN-1、EN-2 的流识别条件的新的 TCP 协议数据包的情况下,与该接收数据包相对应,向流表格 60 追加统计收集用的其它流项目。

[0137] 另外,通过将统计收集用的流项目 EN-1、EN-2 优先于统计控制项目 EN-x12 来检索流表格 60 的项目排列,可避免将相同内容的统计收集用流项目重复登录于流表格 60 中。另外,在将统计控制项目 EN-x12 登录在与流表格 60 不同的统计功能控制表格中、流表格 60 中没有对应于检索关键字的项目的情况下,也可检索统计功能控制表格。

[0138] 在本发明的实施例中,如上所述,流项目管理部 44 自动生成统计收集用的流项目,但统计功能控制项目以外的统计收集用的流项目群的一部分也可由管理者从管理终端 1300 手动设定。

[0139] 在图 21 所示的统计控制信息 63 中,登录处理速率 632 表示命中流登录用统计控制项目 EN-x12 时的登录处理的执行速率,登录处理速率的设定值在登录处理标志 631 的设定值为“1”时有效。登录处理速率的设定值“1/1”意味着在命中统计控制项目 EN-x12 的情况下,必需执行流登录处理。

[0140] 统计收集标志 633 在设定值为“1”的情况下,意味着更新该流的统计信息。频域计算处理标志 634 在设定值为“1”的情况下,意味着算出该流的频域 725。在图 21 所示实例中,统计收集用项目 EN-1、EN-2 与统计控制项目 EN-x12 将统计收集标志设定为“1”,将频域计算处理标志 624 设定成“0”。因此,就图 22 所示的统计信息 72 而言,频域 725 成为统计对象之外的项目。

[0141] 采样处理标志 635 的设定值为“1”时,意味着按照采样速率 636 生成接收数据包的拷贝,将其传送到收集装置 C1。采样速率 636 的设定值在采样处理标志 635 的设定值为“1”的情况下有效。采样速率 636 的设定值例如在“1/1000”的情况下,意味着对于该流的 1000 个数据包按 1 个的比例来生成拷贝。在图 21 的实例中,流项目 EN-1、EN-2、EN-x12 由于采样处理标志 635 为“0”,所以采样速率 636 的值无意义。

[0142] 采样判定标志 637 在其设定值为“1”时,向采样判定部 46 指示该流的采样的开始、结束的判定处理的执行。若设定值为“0”,则不执行采样判定处理。采样开始频域 638 表示成为该流的采样开始条件的流频域值,采样结束频域 639 表示成为采样结束条件的流频域值。

[0143] 采样判定部 46 在采样判定标志 637 为“1”的情况下,比较采样开始频域 638 与对应的统计信息项目表示的当前频域 725,并在当前频域比采样开始频域大的时刻,将采样处理标志 635 变更为“1”。另外,在采样处理标志 635 处于“1”状态时,比较当前频域 725 与采样结束频域 639,在当前频域比采样结束频域小的时刻,将采样处理标志 635 恢复成“0”。在图 21 中,项目 EN-1、EN-2、EN-x12 由于将采样判定标志设定成“0”,所以不执行基于接收数据包采样的拷贝的生成。

[0144] 下面,参照图 16、图 19、图 20 来详细说明本发明的路由器的动作。首先,说明在流表格 60 中仅存在流登录用项目 EN-x12,统计收集用的项目 EN-1、EN-2 未登录的状态下,数据包积累控制部 23 处理属于流 1 的接收数据包时的路由器动作。

[0145] 数据包积累控制部 23 当从缓冲存储器 22-1 ~ 22-(N+1) 之一读出接收数据包时,在生成内部标题 15 之后,指定接收数据包的数据部积累所需的存储器块的个数,请求存储器状态管理部 26 分配存储器块。存储器状态管理部 26 对于数据包数据积累存储器 24 中准备的多个存储器块(存储器地址),管理各自的使用状态,从处于空状态的存储器块中,向数据包积累控制部 23 分配必要个数的存储器块(存储器地址)。

[0146] 数据包积累控制部 23 按照从存储器状态管理部 26 分配的存储器地址,如图 18 所述,执行数据包数据管理信息块向输入数据包标题积累存储器 25A 的写入、和接收数据包数据部向数据包数据积累存储器 24 的写入。另外,在数据包数据积累存储器 24 中没有所需个数的空存储器块的情况下,数据包积累控制部 23 废弃接收数据包。

[0147] 在本实施例中,说明以 FIFO(Fast-In Fast-Out) 形式来执行数据包数据处理信息块向存储器 25A 的写入,但也可通过将输入数据包标题积累存储器 25A 分割成固定长度的多个存储器块,使各数据包数据管理信息块具有下一块的指针地址,将 1 组数据包数据管理信息块分散存储在存储器 25A 内的任意空存储器块中。

[0148] 数据包积累控制部 23 在向输入数据包标题积累存储器 25A 写入完数据包数据管理信息块时、或向数据包数据积累存储器 24 写入完数据包数据时,经信号线 L23,向标题发送控制部 27 发送数据包的接收通知。

[0149] 接收到上述数据包接收通知的标题发送控制部 27 从输入数据包标题积累存储器 25A 中读出开头的数据包数据管理信息块 200-1,经信号线 L27 将该数据包数据管理信息块表示的标题信息(内部标题 15、层 2 标题 11-层 4 标题 13)传送到检索处理部 40 的标题信息积累部 41。另外,标题发送控制部 27 根据开头的数据包数据管理信息块 200-1 所示的存储器块数(M),依次读出后续的 M-1 个数据包数据管理信息块 200-2、200-3、...,暂时保持这些内容。

[0150] 在图 20 中,检索处理部 40 的标题信息积累部 41 在暂时积累经信号线 L27 从标题发送控制部 27 接收到的标题信息之后,分配给流表格检索部 42、路由表格检索处理部 43、流项目管理部 44、统计信息处理部 47。

[0151] 流项目管理部 44 保持上述标题信息,等待接收来自流表格检索部 42 的统计控制

信息。路由表格检索处理部 43 根据上述标题信息,生成检索路由表格 80 所需的检索关键字,并从路由表格 80 中检索包含输出线路序号的路由信息。将检索结果分配给流表格检索部 42、采样处理部 45、检索结果输出部 48。

[0152] 流表格检索部 42 根据标题信息、和必要时路由表格检索处理部 43 输出的路由信息,提取成为流识别条件 62 的信息项目、即发送源 IP 地址、目的地 IP 地址、上位协议、TOS、发送源端口序号、目的地端口序号等信息,并将这些信息项目的组合作为检索关键字,检索流表格 60。

[0153] 这里,因为假设上述标题信息是属于流 1 的数据包的信息,并且,在流表格中仅登录项目 EN-x12 的状态,所以作为流表格 60 的检索结果,得到流项目 EN-x12 的流项目序号(或项目地址)f12、和表示登录处理标志为“1”、登录处理速率为“1/1”、统计收集标志为“1”、采样处理标志为“0”的统计控制信息。

[0154] 流表格检索部 42 将上述检索结果分配给流项目管理部 44、采样处理部 45、采样判定部 46、统计收集处理部 47。此时,因为采样处理标志为“0”,所以不产生采样处理部 45 与采样判定部 46 中用于生成采样的特别动作。

[0155] 从标题信息积累部 41 接收标题信息的统计收集处理部 47 等待接收来自流表格检索部 42 的统计控制信息。在本例中,因为表示统计控制信息的统计收集处理标志为“1”,所以统计收集处理部 47 根据从路由表格检索部 43 接收到的路由信息和从标题信息积累部 41 接收到的标题信息,更新具有统计信息表 70 中的流项目序号 F12 的表格项目 SE-x12 的统计信息 72。具体而言,将表格项目 SE-x12 的数据包数 721 加 1,将上述标题信息表示的接收数据包长度加到字节数 722 上,将上述标题信息表示的输入线路序号 151 的值记录在输入线路序号 723 中,将上述路由信息表示的输出线路序号记录在输出线路序号 724 中。

[0156] 另一方面,流项目管理部 44 通过从流表格检索部 42 接收到的统计控制信息,由于登录处理标志为“1”,登录处理速率为“1/1”,所以对具有从标题信息积累部 41 接收到的标题信息的流,判断为应将新的流项目登录到流表格 60 中。在例如处理速率为“1/k”(k 为比 1 大的值)的情况下,根据登录处理速率,判定是否应登录流。

[0157] 流项目管理部 44 管理流表格 60 的项目地址的使用状况。此时,流项目管理部 44 从上述标题信息中提取成为流识别条件的信息项目,生成具有项目序号 f1 的新的流识别条件,并将包含该流识别条件、部分纠正的统计控制信息和空项目地址的流登录指示提供给流表格检索部 42。在流表格 60 中没有新的流项目所需的空地址的情况下,流项目管理部 44 在执行后述的流项目删除处理之后,发出上述流登录指示。

[0158] 从流项目管理部 44 接收到流登录指示的流表格检索部 42 按照指定的项目地址、流识别条件、统计控制信息,将新的流项目追加到流表格 60 中。这里,因为假设接收属于流 1 的数据包的情况,所以响应上述流登录指示,向流表格 60 追加统计收集用的项目 EN-1。在接收到属于流 2 的数据包的情况下,通过与之一样的动作,向流表格 60 追加统计收集用的项目 EN-2。

[0159] 检索结果输出部 48 当从路由表格检索部 43 接收路由信息时,生成检索结果通知 480,并经信号线 L48 将其发送到接收数据包处理部 20 的标题发送控制部 27。检索结果通知 480 如图 23 所示,由输出线路序号 481、拷贝指示标志 482、封装化指示标志 483、封装化标题信息 484、其它信息 485 构成。

[0160] 这里,拷贝指示标志 482 是表示接收数据包处理部 20 必需拷贝接收数据包的标志,封装化指示标志 483 是表示应使用封装化标题信息 484 来封装化上述拷贝数据包的标志。拷贝指示标志 482 对于采样处理部 45 向信号线 L45 输出拷贝指示信号的時刻生成的检索结果通知,设定成“1”。封装化指示标志 483 如后所述,对于在将拷贝指示标志设定成“1”的检索结果通知之后生成的拷贝数据包发送用检索结果通知,设定成“1”。在封装化标题信息 484 中,设定从采样数据包标题信息积累部 51 中读出的标题信息,仅在封装化指示标志 483 为“1”的情况下有效。

[0161] 在输出线路序号 481 与其它信息 485 中,在通常的检索结果通知的情况下,设定从由路由表格检索部 43 接收到的路由信息中提取的输出线路序号和其它信息。但是,对于拷贝数据包发送用检索结果通知,设定为了将拷贝数据包发送给收集装置所需的规定输出线路序号和其它信息。

[0162] 在本例的情况下,因为没有来自采样处理部 45 的拷贝指示,所以检索结果输出部 48 生成包含拷贝指示标志 482 为“0”、封装化指示标志 483 为“0”、封装化标题信息 484 为无效数据、输出线路序号 491 与其它信息 485 为有效数据的检索结果通知 480,发送到信号线 L48。

[0163] 返回图 16,标题发送控制部 27 当经信号线 L48 接收检索结果通知 480 时,向已从存储器 25A 读出的最初的数据包数据管理信息块 200-1 中,追加上述检索结果通知 480 表示的输出线路序号 481、封装化指示标志 483、封装化标题信息 484 的内容,作为输出线路序号 152、封装化指示标志 153、封装标题信息 154。将更新后的数据包数据管理信息块 200-1 写入输出数据包标题积累存储器 25B 中。另外,必要时,也可追加检索结果通知 480 表示的其它信息 485,作为数据包数据管理信息块 200-1 的内部标题 15 的一部分。

[0164] 如图 18 所述,不必向后续的数据包数据管理信息块 200-2、200-3、…追加标题信息。因此,标题发送控制部 27 对于这些后续的数据包数据管理信息块,将从存储器 25A 读出的信息原样写入输出数据包标题积累存储器 25B 中。

[0165] 之后,标题发送控制部 27 向拷贝管理部 28 通知写入上述输出数据包标题积累存储器 25B 中的各数据包数据管理信息块表示的存储器地址 204 的值、和根据检索结果通知 480 判明的拷贝数量,并请求数据包传送控制部 29 开始传送数据包。在本例的情况下,在从检索控制部 40 接收到的检索结果通知 480 中,由于拷贝标志 482 为“0”,所以标题发送控制部 27 将拷贝数量“0”通知给拷贝管理部 28。

[0166] 拷贝管理部 28 用于控制数据包数据积累存储器 24 的各存储器块的释放,例如如图 24 所示,具备与数据包数据积累存储器 24 的各存储器块(存储器地址)281 对应、存储积累数据的发送等待次数 282 的存储器地址释放控制表格 280。

[0167] 拷贝管理部 28 当从标题发送控制部 27 接收数据包数据积累存储器 24 的存储器地址 204 与拷贝数量时,对应于通知的拷贝数量,变更与上述存储器地址释放控制表格 280 中的上述存储器地址 204 对应的存储器块的发送等待次数 282。发送等待次数在从标题发送控制部 27 通知的拷贝数量为“0”时被设定为“1”,在拷贝数量为“1”时被设定为“2”。

[0168] 图 24 的表格状态与图 18 对应,表示将接收数据包的数据部分割存储在块 k、k+2、k+3 中的状态。此时,因为从标题发送控制部 27 通知的拷贝数量为“0”,所以设定“1”,作为与这些存储器块 k、k+2、k+3 对应的发送等待次数。

[0169] 数据包传送控制部 29 当从标题发送控制部 27 接收数据包传送开始请求时,从输出数据包标题积累存储器 25B 中读出开头的数据包数据管理信息块 200-1,并按照该块所示的存储器地址 204 与有效数据长度 203,从数据包数据积累存储器 24 的存储器块 k 中读出最初的数据块。数据包传送控制部 29 按照开头的数据包数据管理信息块 200-1 所示的存储器块数 202,以 FIFO 形式从输出数据包标题积累存储器 25B 中读出第 2、第 3 数据包数据管理信息块 200-2、200-3,按照这些信息块所示的存储器地址 204 与有效数据长度 203,依次从数据包数据积累存储器 24 的存储器块 k+2、k+3 中读出后续的数据块。

[0170] 数据包传送控制部 29 通过在从开头数据包数据管理信息块 200-1 中提取的标题信息 205 之后、将由这些数据块再构成的数据包数据部 14 发送给信号线 L1,将具有图 15 的格式的内部数据包传送给发送数据包处理部 30。数据包传送控制部 29 当完成一个内部数据包传送时,向拷贝管理部 28 通知表示数据读出完成的存储器块的地址的数据包传送完成通知。

[0171] 拷贝管理部 28 当接收上述数据包传送完成通知时,按照通知的存储器块地址,对存储器地址释放控制表格 280 的发送等待次数 282 执行减法运算。在本例中,将存储器块 k、k+2、k+3 的发送等待次数各减 1,结果,全部的发送等待次数为“0”。拷贝管理部 28 在每次更新发送等待次数时,都检查剩余次数,对发送等待次数为“0”的存储器块,判断为不用保存积累数据,指示存储器状态管理部 26 释放存储器地址。存储器状态管理部 26 管理有释放指示的存储器地址(存储器块),作为空状态,将这些存储器地址使用于此后的对数据包积累控制部 23 的分配地址中。

[0172] 对于图 19 所示的发送数据包处理部 30 而言,当数据包接收部 36 从信号线 L1 接收内部数据包时,将标题信息部分(标题 15、11-13)积累在输出数据包标题积累存储器 34 中,将数据包的数据部分 4 积累在数据包数据积累存储器 33 中。这些向存储器积累标题信息与数据包数据使用图 18 中说明的数据包数据管理信息块,以与接收数据包处理部 20 的输入数据包标题存储器 25A 和数据包数据积累存储器 24 一样的形式执行。数据包数据积累所需的存储器块的分配由存储器状态管理部 35 来执行。

[0173] 数据包接收部 36 当完成向输出数据包标题积累存储器 34 写入数据包数据管理信息块、和向数据包数据积累存储器 33 写入数据包数据时,向数据包输出控制部 32 输出数据包发送请求。

[0174] 当接收上述数据包发送请求时,数据包输出控制部 32 与接收数据包处理部 20 的数据包传送控制部 29 一样,通过从输出数据包标题积累存储器 34 读出的开头的数据包数据管理信息块所示的存储器块数 202,读出后续的数据包数据管理信息块,并按照各数据包数据管理信息块所示的存储器地址 204 与有效数据长度 203,从数据包数据积累存储器 33 中依次读出数据包的数据部。

[0175] 数据包输出控制部 32 在将从多个存储器块中读出的数据块再构成最初的数据包数据 14 之后,根据开头的数据包数据管理信息块表示的封装化指示标志 153 的值,判定是否要封装化输出数据包。在本例的情况下,因为上述封装化指示标志的值为“0”,所以不必封装化输出数据包。因此,数据包输出控制部 32 通过将从开头的数据包数据管理信息块中提取的层 2 标题 11、层 3 标题 12、层 4 标题 13 提供给上述再构成的数据包数据 14,生成输出数据包,并将该输出数据包输出到由上述数据包数据管理信息块所示的输出线路序号

152 特定的线路终端处理部 31-k。

[0176] 线路终端处理部 31-k 在向从数据包输出控制部 32 接收的输出数据包提供冗余编码等附加信息之后,发送给输出线路 0ck。

[0177] 接着,说明在已将统计收集用的流项目 EN-1 登录到流表格 60 中的状态下,数据包积累控制部 23 处理属于流 1 的接收数据包时的路由器 R1 的动作。

[0178] 标题发送控制部 27 从将接收数据包的标题信息传送给检索处理部 40 开始、至检索处理部中流表格检索部 42 检索流表格 60 的动作与流项目 EN-1 未登录时一样。这次由于是流项目 EN-1 已登录到流表格 60 中的状态,所以流表格检索部 42 输出流项目 EN-1 所示的统计控制信息,作为流表格 60 的检索结果。流项目 EN-1 的统计控制信息 63 如图 21 所示,登录处理标志 631 为“0”,统计收集标志 633 为“1”,采样处理标志 635 与采样判定标志 637 为“0”。

[0179] 因为登录处理标志为“0”,所以不执行流项目管理部 44 的流登录处理。另外,由于采样处理标志、采样判定标志为“0”,所以不产生采样处理部 45 与采样判定部 46 的特别动作。

[0180] 另一方面,因为统计收集处理标志为“1”,所以统计收集处理部 47 对流项目序号 f1 的统计信息项目 SE-1 更新统计信息。

[0181] 具体而言,将数据包数量 721 加 1,将从标题信息积累部 41 接收到的标题信息所示的接收数据包的字节数量与字节数 722 相加,将上述标题信息所示的输入线路序号记录在输入线路序号 723 中,并将从路由表格检索部 43 接收到的路由信息所示的输出线路序号记录在输出线路序号 724 中。检索结果输出部 48 的动作与接收数据包处理部 20 之后的动作与上述流项目 EN-1 未登录时一样。

[0182] 下面,说明流项目管理部 44 执行的从流表格中删除项目的动作。

[0183] 流项目管理部 44 将统计收集标志为“1”、登录处理标志、采样处理标志、采样判定标志为“0”的流项目作为删除对象,监视数据包的接收状况,从流表格 60 中删除在规定时间内中断了数据包接收的流项目。充项目管理部 44 在没有空项目区域的状态下,当必需将新的流项目登录到流表格 60 中时,也从上述删除对象项目中选择特定的项目,从流表格 60 中删除。

[0184] 成为删除对象的流信息被登录在流管理表格 49 中,定期监视数据包的接收状况。流管理表格 49 例如图 25 所示,对于成为删除对象的各项目,表示流项目序号 49、流表格 60 中的项目地址 492、数据包数量 493、更新时刻 494、非更新次数 495。这里,数据包数量 493 是为了监视删除对象流的通信状态而选择的代表统计信息,也可用字节数量代替数据包数量来作为监视对象。

[0185] 流项目管理部 44 对于具有登录在流管理表格 49 中的流项目序号的各数据包流,经统计收集处理部 47,按一定时间间隔从统计信息表 70 中读出数据包数量 721 的最新值,并与流管理表格 49 所示的上次监视时的数据包数量 493 进行比较。在最新数据包数量与上次值不同的情况下,将数据包数量 493 替换成最新值,同时,将更新时刻 494 替换成当前时刻。在最新数据包数量与上次值相同的情况下,不变更更新时刻 494,增加非更新次数 495 的值。也可在每次更新数据包数量 493 时,将非更新次数 495 恢复到最初值。

[0186] 流项目管理部 44 判断非更新次数通过上述增加而达到规定阈值的流项目为无用

项目,对流表格检索部 42 指定项目地址 492,指示删除无用流项目,并对统计信息处理部 47 指定流项目序号,指示删除统计信息项目。

[0187] 流项目管理部 44 通过从流表格检索部 42 接收流项目 EN-x12 的统计控制信息,在需要将新的流项目追加到流表格 60 中时,并且在流表格中没有空区域的情况下,从流管理表格 49 中选择更新时刻 494 最久的项目,作为无用项目,对流表格检索部 42 和统计信息处理部 47 指示与上述一样的项目删除。

[0188] 流表格检索部 42 当从流项目管理部 44 接收无用流项目的删除指示时,从流表格 60 的指定项目地址读出流识别条件 62。流表格检索部 42 在将读出的流识别条件传送到流信息积累部 52 后,删除该流项目,并通知流项目管理部 44 释放删除项目的地址。同样,统计信息处理部 47 也在从流项目管理部 44 接收无用流项目的删除指示时,从统计信息表 70 中读出具有指定项目序号的统计信息项目的内容,在将其传送到流信息积累部 52 后,删除该统计信息项目。

[0189] 流信息积累部 52 将伴随流项目的删除从流表格检索部 42 接收到的流识别条件、和从信息收集处理部 47 接收到的统计信息(下面将这两种信息合称为流信息)保持在存储器中。在将事先指定的流数量的流信息积累在流信息积累部 52 中的时刻,统计信息通知数据包生成部 53 从流信息积累部 52 中读出积累流信息,利用统计信息通知数据包标题信息积累部 50 表示的封装标题信息,生成统计信息通知数据包 300。统计信息通知数据包生成部 53 在将生成的统计信息通知数据包 300 输出到信号线 L53 的同时,将数据包的接收通知输出到信号线 L530。

[0190] 统计信息通知数据包 300 例如图 26 所示,由标题 301、和多个流记录 302 (302-1 ~ 302-N) 构成。标题 301 根据从标题信息积累部 50 中读出的封装化标题信息生成,包含收集装置 C1 的 IP 地址,作为目的地 IP 地址。统计信息通知数据包 300 例如可使用记载于 http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/nfc/nfc_3_0/nfc_ug/nfcform.htm 中的格式。

[0191] 在这里所示的实例中,各流记录 302 包含流识别符 303、采样速率 304、流识别标题信息 305、数据包数量 306A、字节数量 306B、输出线路序号 306C、输入线路序号 306D、其它信息 306E。对信息项目 306A-306E 设定从信息收集处理部 47 输出的统计信息。另外,在流识别符 303 中使用流项目序号 61,在采样速率 304 中使用被使用于统计控制信息的规定采样速率,在流识别标题信息 305 中使用流识别条件 62。收集装置在接收到上述统计信息通知数据包时,根据各流记录所示的采样速率 304,可推定在网络上实际通信的数据包数量。

[0192] 从统计信息通知数据包生成部 53 输出到信号线 L53 的统计信息通知数据包 300 被暂时积累在接收数据包处理部 20 的缓冲存储器 22-(N+1) 中,将输出到信号线 L530 的数据包接收通知输入到数据包积累控制部 23。因比,数据包积累控制部 23 可与积累在其它缓冲存储器 22-1 ~ 22-N 中的通常接收数据包一样处理积累在缓冲存储器 22-(N+1) 中的统计信息通知数据包 300。

[0193] 数据包积累控制部 23 在从缓冲存储器 22-(N+1) 中读出统计信息通知数据包 300 时,与来自网络的接收数据包的处理时一样,生成内部标题 15,向存储器状态管理部 26 请求必要个数的存储器块地址,如图 18 所述,按数据包数据管理信息块形式,将内部标题 15 与标题 301 积累在输入数据包标题积累存储器 25A 中,将统计信息通知数据包 300 的数据

部（流记录 302-1 ~ 302-N）分割成固定长度的多个块，积累在数据包数据积累存储器 24 中，向标题发送控制部 27 输出数据包接收通知。

[0194] 标题发送控制部 27 与检索处理部 40 的动作与通常的接收数据包处理时一样，与网络接收数据包的标题信息一样处理通知数据包 300 的标题信息。结果，按附加包含路由表格检索结果所示的输出线路序号 152 的内部标题的形式，将统计信息通知数据包 300 传送到发送数据包处理部 30，从发送数据包处理部 30 发送到与收集装置的连接线路上。

[0195] 下面，说明数据包积累控制部 23 处理与流登录用项目 EN-x12 所示的流识别条件不一致的数据包、例如属于图 1 中说明的上位协议为 UDP 的流 3 或流 4 的数据包时的检索处理部 40 的动作。

[0196] 路由表格检索部 43 与流识别条件无关，根据从标题信息积累部 41 接收到的标题信息，检索路由表格 80，并输出检索结果。另一方面，流表格检索部 42 根据标题信息、和必要时从路由表格 80 检测到的路由信息，生成流检索关键字，检索流表格 60。

[0197] 在本例中，因为接收数据包的上位协议为 UDP，所以在流表格 60 中完全不存在对应于上述检索关键字的项目（统计控制项目与流项目）。因此，流表格检索部 42 将表示没有对应的统计控制信息的检索结果输出到流项目管理部 44、采样处理部 45、采样判定部 46、统计收集处理部 47。

[0198] 在没有统计控制信息的情况下，流项目管理部 44 不执行流登录处理。采样处理部 45、采样判定部 46、统计收集处理部 47 也不执行各自固有的动作。因此，检索结果输出部 48 生成拷贝标志 482 与封装化指示标志 483 为“0”、封装标题信息 484 为无效、仅输出线路序号 481 和其它信息 485 中包含有效信息的检索结果通知 480，并将之输出到信号线 L48。响应于上述检索结果通知 480 执行的接收数据包处理部 20 的动作与属于流 1 的接收数据包的情况一样。

[0199] 下面，说明本实施例的路由器 R1 具备的采样型统计信息收集功能。这里，采样处理部 45 与采样判定部 46 利用登录在流表格 60 中的统计控制信息和积累在统计信息表 70 中的统计信息，检索处于特殊通信状况下的数据包流，在由采样速率指定的定时，指令接收数据包处理部 20 生成接收数据包的拷贝。

[0200] 例如，对于图 1 所示的网络，假设终端 T2 或终端 T4 通过向服务器 S2 发送 TCP(Transmission Control Protocol) 的 SYN 数据包，妨碍（SYN 命中）从服务器 S2 向其它终端的通信服务的情况。SYN 命中数据包将定义成 TCP 标题的代码比特中的 SYN 标志设定成“1”。

[0201] 在以下说明中，将从终端 T2 发送到服务器 S2 的一连串 SYN 数据包流称为流 Fs2，将从终端 T4 发送到服务器 S2 的一连串 SYN 数据包流称为流 Fs4。另外，假设从终端 T2、终端 T4 发送的 SYN 数据包的总计频域随着时间经过而增加，在本实施例中，说明检索处理部 40 在 TCP 的 SYN 数据包的总计频域为 50Mbps 以上的时刻，按采样速率 1/10 开始接收数据包的采样（拷贝数据包）生成，在总计频域为 40Mbps 以下的时刻，停止采样生成的情况。

[0202] 图 27 表示检测 SYN 命中用的流表格 60 的一例。

[0203] 为了监视 TCP 的 SYN 数据包并成为采样的对象，在流表格 60 中登录具有流项目序号 f24 的项目 EN-x24。项目 EN-x24 也是统计控制项目之一，作为流识别条件 62，指定上位协议 623 为“TCP”，SYN 标志 627 为“1”，此外项目 621、622、624-626、629 为任意值

(“*”)。

[0204] 上述项目 EN-x24 对作为检索结果输出的统计控制信息 63, 指定登录处理标志“0”、统计收集标志“1”、采样处理标志“0”、采样速率“1/10”、采样判定标志“1”、采样开始频域“50Mbps”、采样结束频域“40Mbps”。

[0205] 图 28 表示对统计信息表 70 准备的具有流项目序号 f24 的统计信息项目 SE-x24 的内容一例。作为当前时刻的统计信息, 例如数据包数量 721 为“P24”, 字节数量 722 为“B24”, 频域 735 为 10Mbps。

[0206] 接收数据包处理部 20 的数据包积累部 23 从任一缓冲存储器中读出接收数据包 (SYN 数据包), 标题发送控制部 27 将接收数据包的标题信息传送给检索处理部 40, 检索处理部 40 的路由表格检索部 43 与流表格检索部 42 执行各自表格检索之前的动作与上述流 1 的接收数据包处理时一样。

[0207] 在接收数据包是属于流 2 的 Fs2 的 SYN 数据包的情况下, 流表格检索部 42 根据标题信息生成的检索关键字与图 27 所示的项目 EN-x24 的流识别条件一致。因此, 流表格检索部 42 将项目 EN-x24 表示的统计控制信息作为检索结果, 分配给流项目管理部 44、采样处理部 45、采样判定部 46、统计收集处理部 47。

[0208] 这次, 由于检索到的统计控制信息的登录处理标志 631 与采样处理标志 635 为“0”, 所以流项目管理部 44 与采样处理部 45 不执行特别的响应动作。统计收集处理部 47 由于统计控制信息的统计收集标志 633 为“1”, 所以更新具有流项目序号 f24 的项目 SE-x24 的统计信息 72。因此, 数字包数量 721、字节数量 722、频域 725 的值都比图 28 所示的值有所增加。

[0209] 另一方面, 采样判定部 46 统计控制信息的采样判定标志 635 为“1”、采样处理标志 635 为“0”, 所以执行是否应开始接收数据包的处理的判定 (采样开始判定)。采样开始判定是指向统计收集处理部 47 请求流项目序号 f24 的统计信息, 比较当前频域 735 与统计控制信息表示的采样开始频域 638。这里, 频域 735 的当前值“10Mbps”比采样开始频域 638 的指定值“50Mbps”小, 所以采样判定部 46 判断为不要采样处理, 不执行特别的动作。因此, 在该时刻, 检索结果输出部 48 输出拷贝帧 482 与封装化指示标志 483 为“0”、输出线路序号 481 和其它信息 485 中包含有效信息的检索结果通知 480, 接收数据包处理部 20 不生成采样数据包。

[0210] 假设重复上述动作, 流项目 EN-24 的频域 735 的值逐渐增大, 为“51Mbps”。在该状态下, 数据包积累控制部 23 处理流 Fs2 的 SYN 数据包, 当标题发送控制部 27 将标题信息传送到检索处理部 40 时, 采样判定部 46 对流项目序号 f24 的流执行采样开始判定, 检索当前频域 735 超过由统计控制信息指定的采样开始频域 638。采样判定部 46 这次判断为需要开始采样处理, 对流表格检索部 42 指示将流项目序号 f24 的流项目 EN-x24 中的采样处理标志 635 改写“1”。流表格检索部 42 响应于上述改写指示, 将流项目 EN-x24 的统计控制信息中包含的采样处理标志 635 的值改写为“1”。

[0211] 此时, 仅更新统计信息表 70 的项目 SE-24 的统计信息 72、和流表格的流项目 EN-24 的统计控制信息, 采样处理部 45 的动作没有变化。因此, 检索处理输出部 48 将与此前一样的检索结果通知 480 输出到信号线 L48, 接收数据包处理部 20 不生成采样数据包。

[0212] 但是, 在将采样处理标志 635 的值改写为“1”后, 当接收处理属于流 Fs2 的下一

SYN 数据包时,检索处理部 40 的动作变化。采样判定部 46 对从流表格检索部 42 通知的统计控制信息,由于采样判定标志 637 与采样处理标志 635 双方都为“1”,所以对流项目序号 f24 的流,执行是否应结束接收数据包的采样处理的判定(采样结束判定)。采样结束判定是指向统计收集处理部 47 请求流项目序号 f24 的统计信息,并比较当前频域 735 与采样结束频域 639。这里,因为当前频域 735 超过采样结束频域 639,所以采样判定部 46 判断为不需要采样处理标志的改写,等待下一统计控制信息。

[0213] 另一方面,采样处理部 45 就从流表格检索部 42 通知的统计控制信息而言,由于采样处理标志 635 为“1”,所以例如使用数据包计数器,以基于采样速率 636 的频度,产生采样数据包生成指示(拷贝指示)。在本例中,采样处理部 45 以对 10 个 SYN 数据包产生 1 个拷贝指示的比例产生拷贝指示,经信号线 L45 将拷贝指示提供给检索结果输出部 48。不产生拷贝指示的周期中的检索结果输出部 48 的动作与上述采样处理标志 635 为“0”的情况一样。

[0214] 检索结果输出部 48 在从信号线 L45 接收拷贝指示的情况下,生成让接收数据包处理部 20 知道必需生成数据包拷贝的第 1 检索结果通知,并在将其输出到信号线 L48 之后,生成让接收数据包处理部 20 知道应将使用封装标题信息的封装化拷贝数据包发送到收集装置的第 2 检索结果通知,并将之输出到信号线 L48。

[0215] 第 1 检索结果通知与通常的检索结果通知 480 一样生成,将拷贝指示标志 482 设定成“1”。即,对封装化指示标志 483 设定“0”,对输出线路序号 481 和其它信息 485 设定从路由表格的检索结果中提取的输出线路序号与其它信息,封装标题信息 484 为无效。

[0216] 第 2 检索结果通知对拷贝指示标志 482 设定“0”,对封装化指示标志 483 设定“1”,对封装标题信息 484 设定用于将采样(接收数据包的拷贝)发送到收集装置的封装标题信息。从采样数据包标题信息积累部 51 中读出该封装标题信息。对第 2 检索结果通知的输出线路序号 481 与其它信息 485 设定在采样数据包标题信息积累部 1511 中事先准备的输出线路序号与其它信息。

[0217] 图 16 中,接收数据包处理部 20 的标题发送控制部 27 当接收上述第 1 检索结果通知 480 时,与通常数据包的处理时一样,将该检索结果通知表示的输出线路序号 481 ~ 封装化标题信息 484 设定成开头的数据包数据管理信息块 200-1 的内部标题 15,并将数据包数据管理信息块 200-1 写入输出数据包标题积累存储器 25B 中。因为这次接收到的检索结果通知中拷贝指示标志 482 为“1”,所以标题发送控制部 27 不废弃地保持已写入输出数据包标题积累存储器 25B 中的数据包数据管理信息块 200-1。在存在后续的数据包数据管理信息块 200-2、200-3、…的情况下,将这些信息块原样写入输出数据包标题积累存储器 25B 中,与数据包数据管理信息块 200-1 一样,不废弃地保持。

[0218] 之后,标题发送控制部 27 向拷贝管理部 28 通知拷贝数量、和上述各数据包数据管理信息表示的存储器地址 204 的值,并向数据包传送控制部 29 请求开始传送数据包。由于这次检索结果通知的拷贝指示标志 482 为“1”,所以向拷贝管理部 28 通知拷贝数量“1”。因此,拷贝管理部 28 对于图 24 所示的地址释放控制表格 280,将与从标题发送控制部 27 通知的存储器地址对应的存储器块 281 的发送等待次数 282 设定成“2”。

[0219] 数据包的传送控制部 29 响应上述数据包传送开始请求,从输出数据包标题积累存储器 25B 中读出数据包数据管理信息块 200-1、200-2、…,根据这些数据包数据管理信息

块,从数据包数据积累存储器 24 中读出数据包数据部分,将再编制的内部数据包(SYN 数据包)输出到信号线 L1。

[0220] 在数据包的传送控制部 29 完成内部数据包的传送时,拷贝管理部 28 对于地址释放控制表格 280,将结束数据发送的存储器块的发送等待次数各减 1。这次由于将结束数据发送的存储器块的发送等待次数的初始值设定成“2”,所以相减后的发送等待次数分别作为“1”保留。因此,对于这些存储器块而言,抑制向存储器状态管理部 26 发出地址释放通知,原样保存积累在数据包数据积累存储器 24 中的数据包数据。

[0221] 标题发送控制部 27 在上述第 1 检索结果通知之后,从检索结果输出部 48 接收第 2 检索结果通知。接收到第 2 检索结果通知的标题发送控制部 27 与接收第 1 检索结果通知时一样,将该检索结果通知表示的输出线路序号 481-封装化标题信息 484 设定成开头的数据包数据管理信息块 200-1 的内部标题 15,并将数据包数据管理信息块 200-1 写入输出数据包标题积累存储器 25B 中,在存在后续的数据包数据管理信息块 200-2、200-3、…的情况下,将这些信息块原样写入输出数据包标题积累存储器 25B 中。这次由于第 2 检索结果通知的拷贝指示标志 482 为“0”,所以废弃已写入输出数据包标题积累存储器 25B 中的数据包数据管理信息块 200-1、200-2、…。

[0222] 之后,标题发送控制部 27 向拷贝管理部 28 通知拷贝数量、和上述各数据包数据管理信息表示的存储器地址 204 的值,并向数据包传送控制部 29 请求开始传送数据包。由于这次拷贝指示标志 482 为“0”,所以拷贝管理部 28 对于地址释放控制表格 280,将与从标题发送控制部 27 通知的存储器地址对应的存储器块 281 的发送等待次数 282 设定成“1”。因此,当数据包的传送控制部 29 完成内部数据包的传送时,对于结束数据发送的存储器块,相减后的发送等待次数分别为“0”,向存储器状态管理部 26 发出地址释放通知。

[0223] 响应上述第 2 检索结果通知,从数据包传送控制部 29 传送到发送数据包处理部 30 的内部数据包(SYN 数据包的拷贝)中,内部标题 15 的封装化指示标志 153 被设定成“1”。发送数据包处理部 30 的数据包输出控制部 32 提取从输出数据包标题积累存储器 34 中读出的开头数据包数据管理信息块 200-1 中包含的作为标题信息 205 一部分的内部标题 15,检查封装化指示标志 153。由于这次封装化指示标志 153 为“1”,所以将内部标题信息 15 中包含的收集装置对象的封装化标题信息 154(层 2 标题-层 4 标题)提供给拷贝数据包的开头,并发送到由输出线路序号 152 特定的线路终端处理部 30-k。

[0224] 按基于采样速率 636 的频度,反复执行上述拷贝数据包的生成、和向收集装置发送封装化数据包,直到作为监视对象的 SYN 数据包的频域 725 比由流项目 EN-24 指定的采样结束频域 639 低为止。在将流项目 EN-24 的采样处理标志 635 设定成“1”的状态下,逐渐减少对应于流识别条件 62 的 SYN 数据包的送出量,在统计信息表 70 中的频域 755 的值比由采样结束频域 639 指定的“40Mbps”低的情况下,检索处理部 40 如下动作。

[0225] 接收数据包处理部 20 的数据包积累控制部 23 结束新的 SYN 数据包的积累处理,当从标题发送控制部 27 向检索处理部 40 的标题信息积累部 41 传送上述 SYN 数据包的标题信息时,流表格检索部 42 将从流表格 60 中检索到的流项目 EN-24 的统计控制信息 63 分配给流项目管理部 44、采样处理部 45、采样判定部 46、统计收集处理部 47。

[0226] 流项目管理部 44 由于统计控制信息 63 的登录处理标志为“0”,所以不执行特别的响应动作。统计收集处理部 1507 由于统计控制信息 63 的统计收集标志为“1”,所以按照从

标题信息积累部 41 接收到的标题信息,更新统计信息项目 SE-x24 的统计信息 72。采样处理部 45 由于统计控制信息 63 的采样处理标志 635 为“1”,所以与此前一样,重复基于采样速率 636 的拷贝指示动作。

[0227] 另一方面,采样判定部 46 由于统计控制信息 63 的采样判定标志 637 与采样处理标志 635 双方都为“1”,所以对流项目序号 f24 的流执行采样结束判定。这次由于当前的频域 735 比采样结束频域 639 低,所以采样判定部 46 对流表格检索部 42 指示将流项目序号 f24 的流 EN-24 中的采样处理标志 635 改写为“0”,流表格检索部 42 将项目 EM-24 的统计控制信息 63 恢复到初始状态。因此,SYN 数据包流的频域再次超过采样开始频域,在采样处理标志 635 被设定成“1”之前的期间,在 SYN 数据包处理时,不从采样处理部 45 产生拷贝指示,向收集装置发送封装化数据包成为停止状态。

[0228] 在本发明中,作为流识别条件的其它信息 629,例如通过指定 TCP 标志、或 Ethernet 标题的目的地 / 发送源 MAC 地址、VLAN ID 的值,可检测对使用 TCP 连接的特定控制数据包的服务器的 Denial of Service 命中 (attack) (DOS 命中),或可收集 VLAN-ID、MAC 地址以外的统计信息。

[0229] 在实施例,数据包积累控制部 23 生成应附加于各接收数据包的内部标题 15,将其设定给数据包数据管理信息块 200,积累在输入数据包标题积累部 25A 中,但也可由各线路终端处理部 21-1 ~ 21-N 生成内部标题,数据包积累控制部 23 以内部数据包形式从缓冲存储器 22-1 ~ 22-N 中读出接收数据包。此时,由于也必需向积累在缓冲存储器 22-(N+1) 中的统计信息通知数据包 300 提供内部标题 15,所以最好对统计信息通知数据包标题信息积累部 50 事先准备内部标题 15。

[0230] 另外,在实施例,说明当检索到流登录用的统计控制项目 EN-x12 时,无条件地向流表格 60 追加新的流项目的实例,但也可由统计控制项目 EN-x12 的统计控制信息 63 来指定新的流项目的登录条件,当满足该条件时,向流表格 60 追加新的流项目。

[0231] 例如,对于项目 EN-x12,如果将采样开始频域 638 约束为在采样判定标志 637 为“1”的情况下,表示采样处理的开始条件,而在采样判定标志 637 为“0”、登录处理标志 631 为“1”的情况下,表示新项目的登录开始条件,则通过统计控制项目 EN-x12 的统计控制信息,分别将登录处理标志 631、统计收集标志 633、频域计算标志 634 设定成“1”,将采样判定标志 637 设为“0”,对采样开始频域 638 设定登录开始频域,从而当 TCP 流中满足登录开始频域时,可使流项目管理部 44 启动向流表格 60 追加新项目的动作。

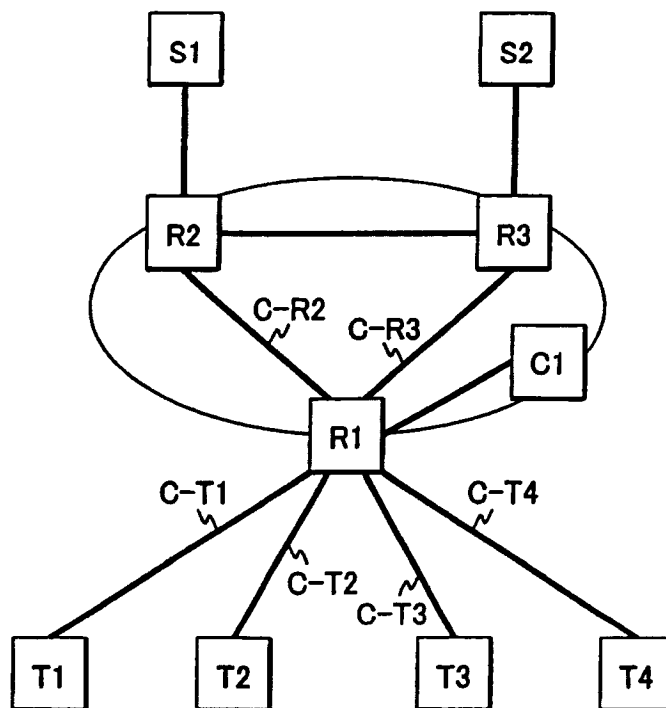


图 1

数据包10

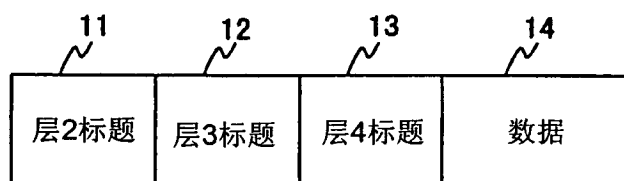


图 2

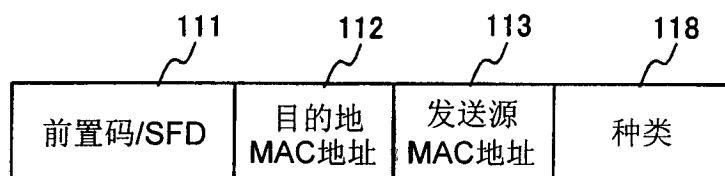


图 3

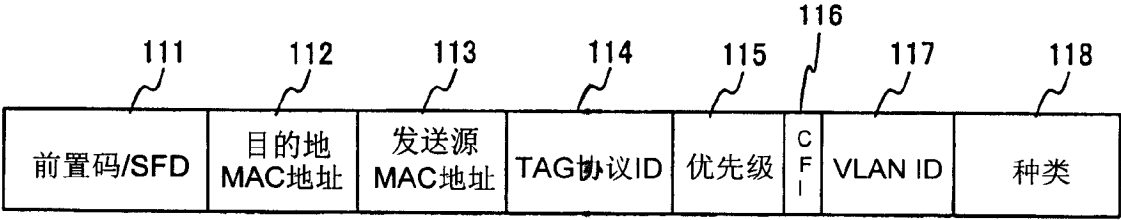


图 4

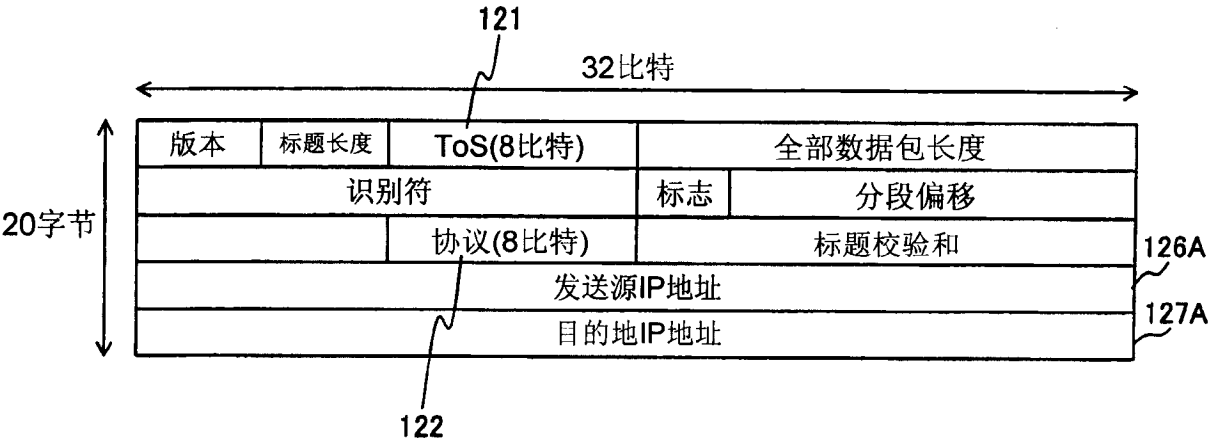


图 5

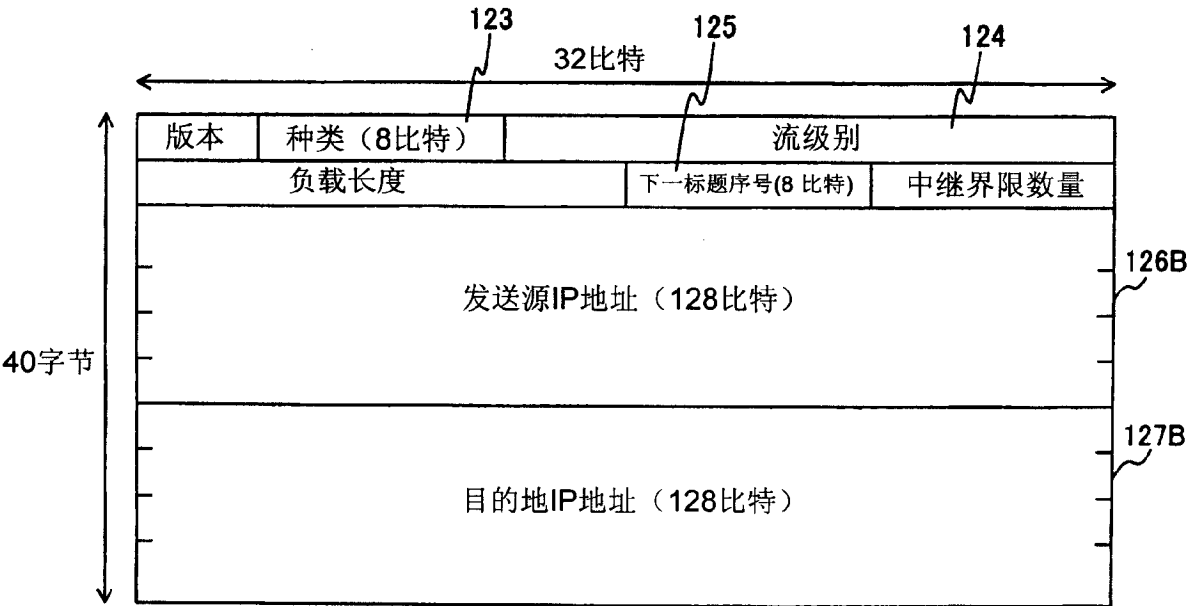


图 6

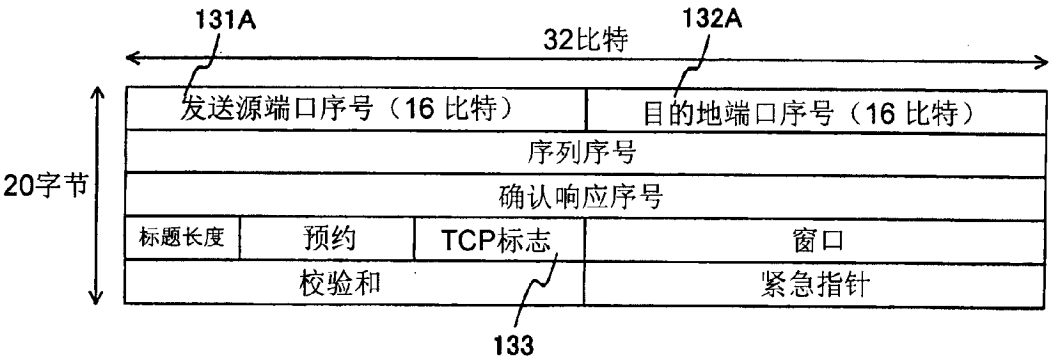


图 7

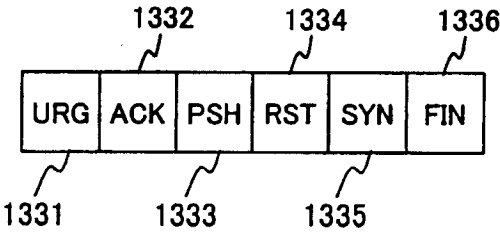


图 8

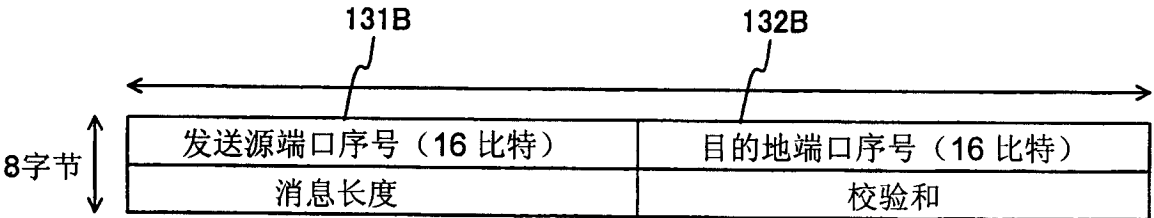


图 9

流项目 序号	流识别条件					
	发送源 IP地址	目的地 IP地址	上位协议	TOS	发送源 端口序号	目的地 端口序号
f1	IP-S1	IP-T1	TCP	TOS1	SPRT1	DPRT1
f2	IP-S1	IP-T3	TCP	TOS1	SPRT1	DPRT3

621
622
623
624
625
626

图 10

流项目 序号	统计信息				
	数据包 数量	字节数量	输入线 路序号	输出线 路序号	其它 信息
f1	10	2000	C-R2	C-T1	...
f2	20	2000	C-R2	C-T3	...

721
722
723
724
729

图 11

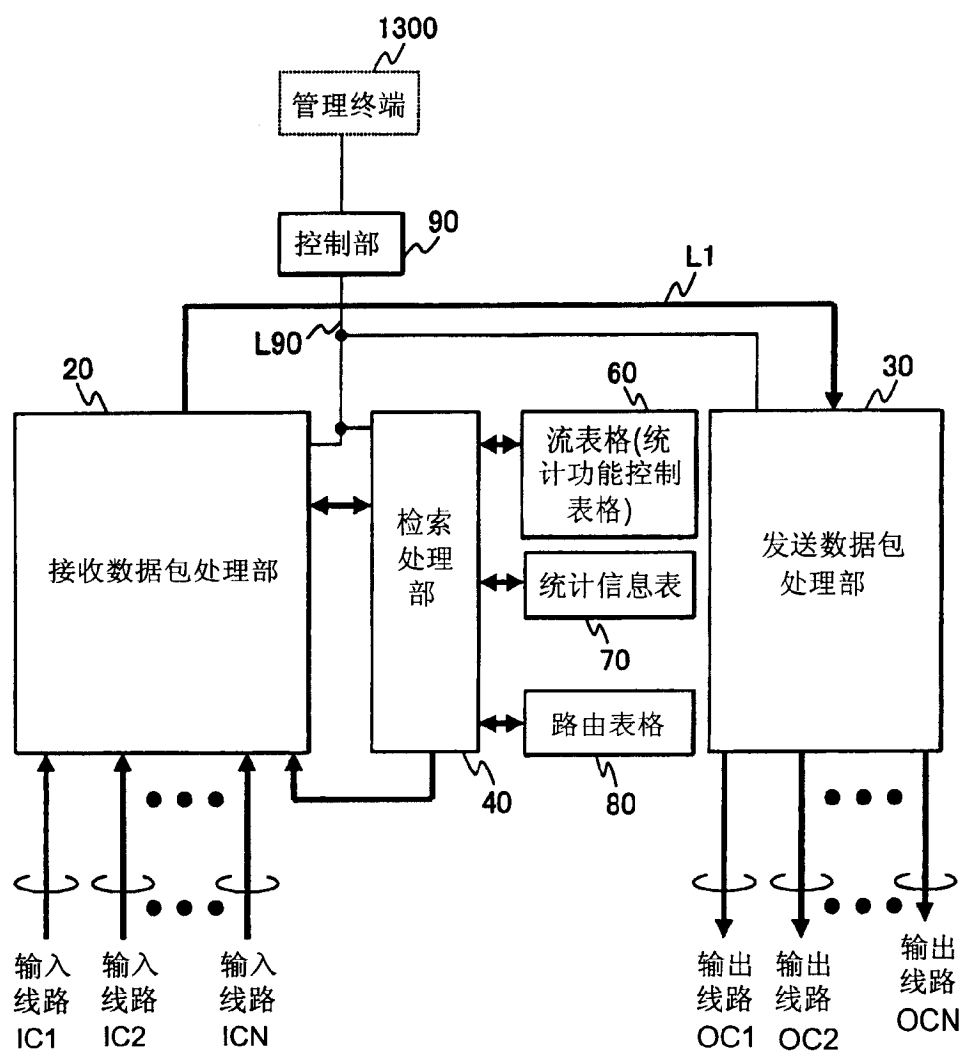


图 12

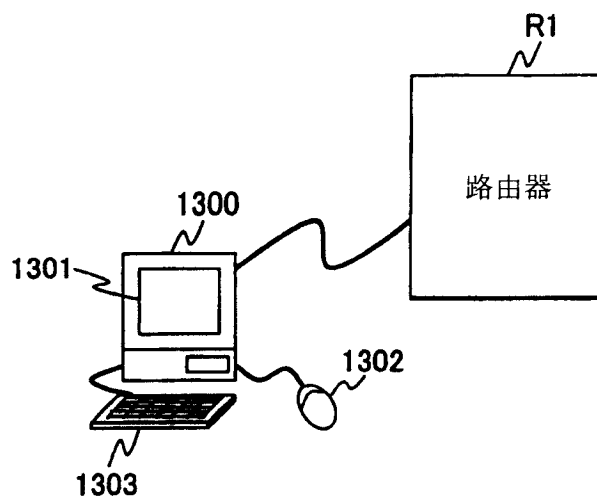


图 13

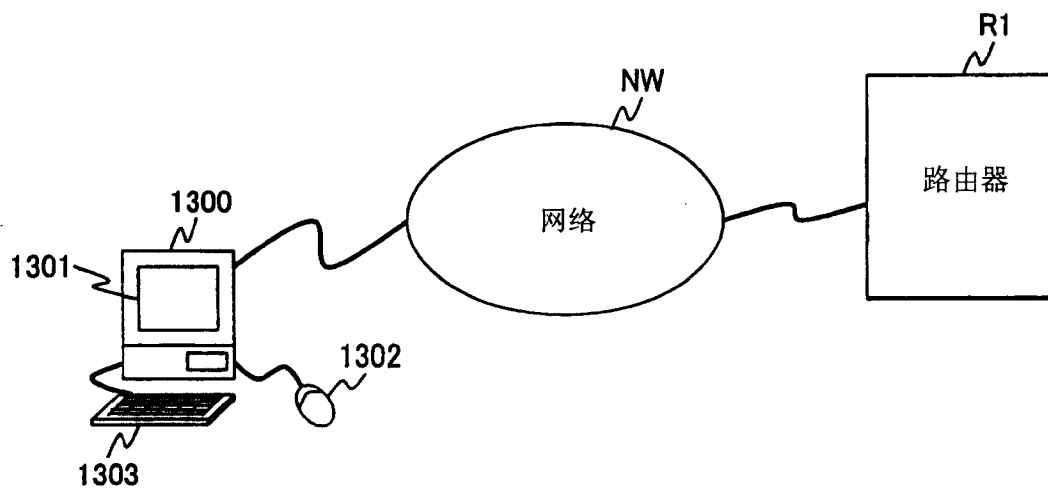


图 14

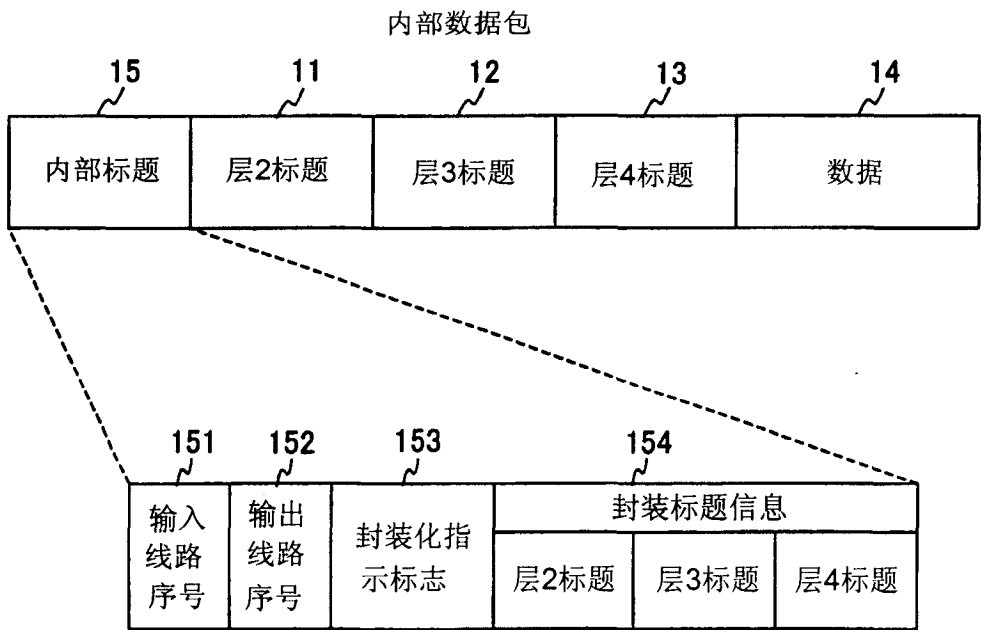


图 15

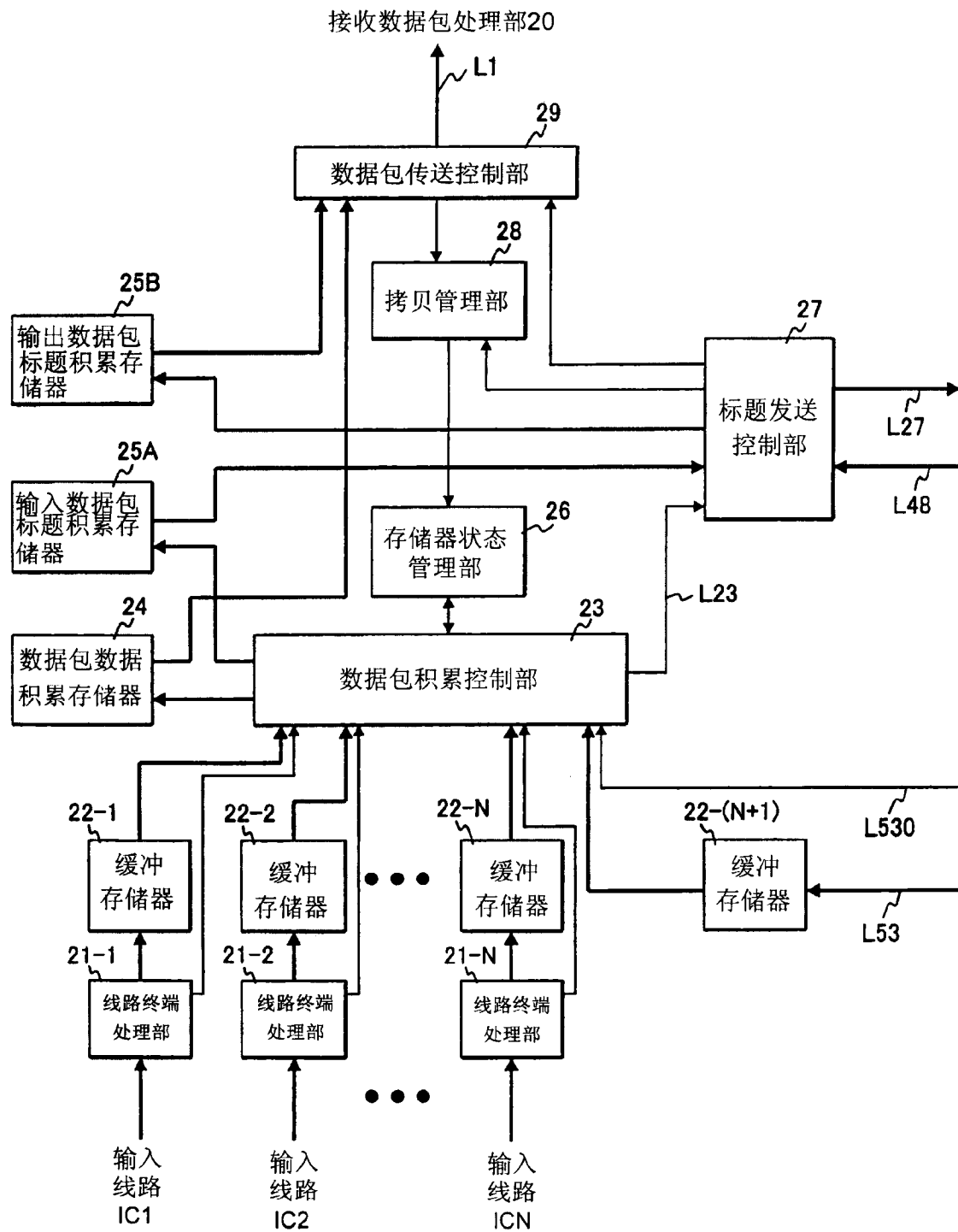


图 16

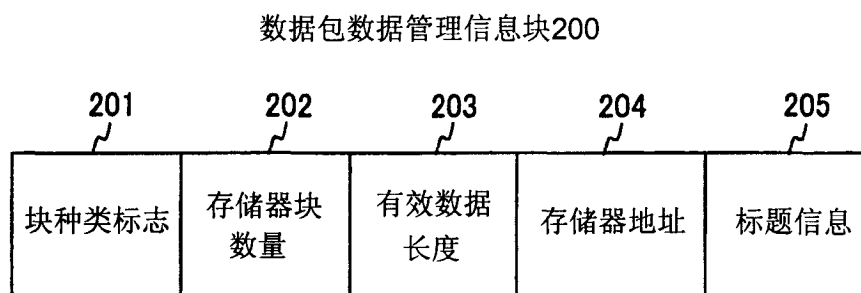


图 17

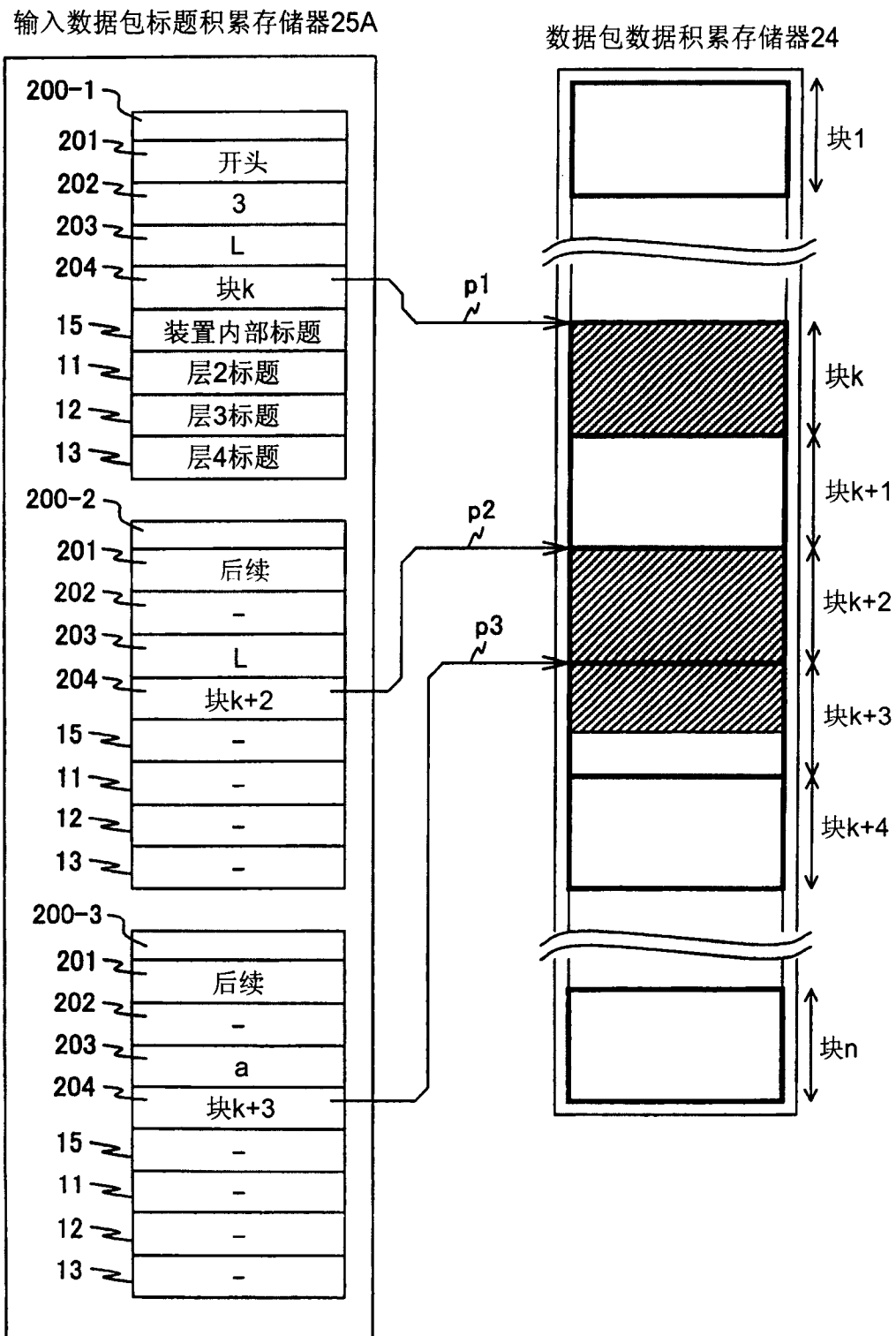


图 18

发送数据包处理部30

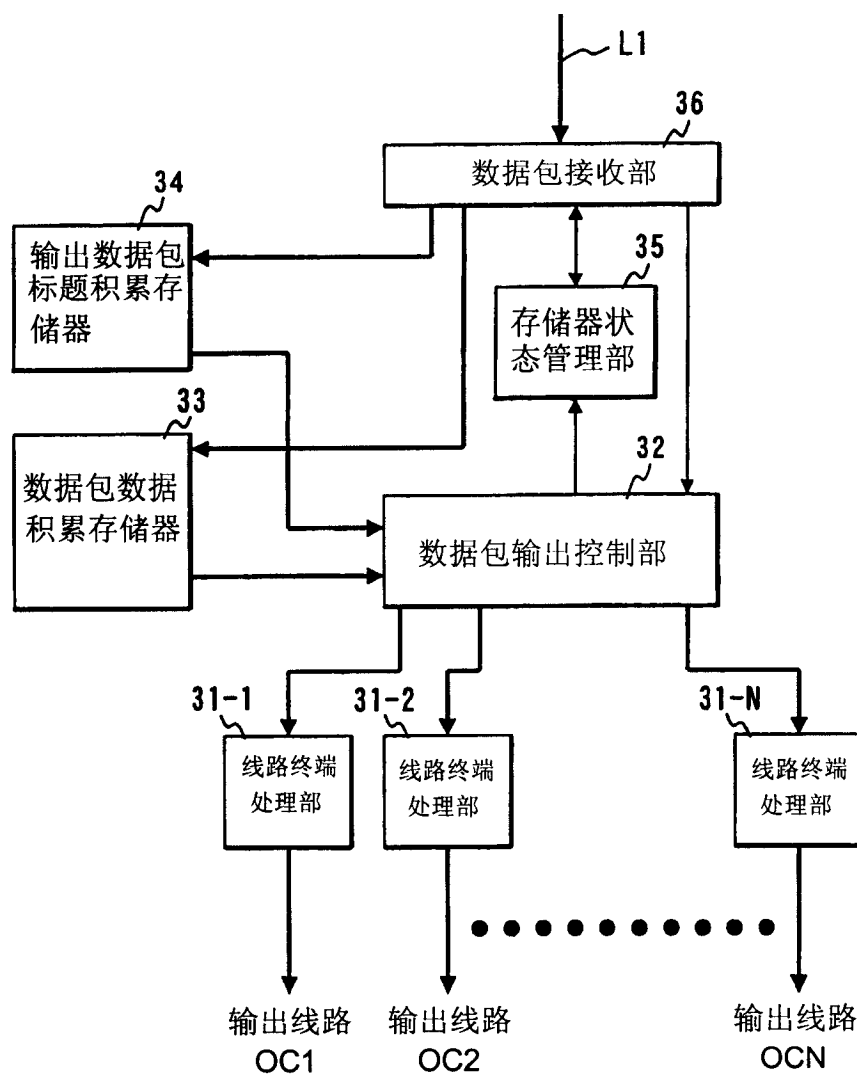


图 19

检索处理部40

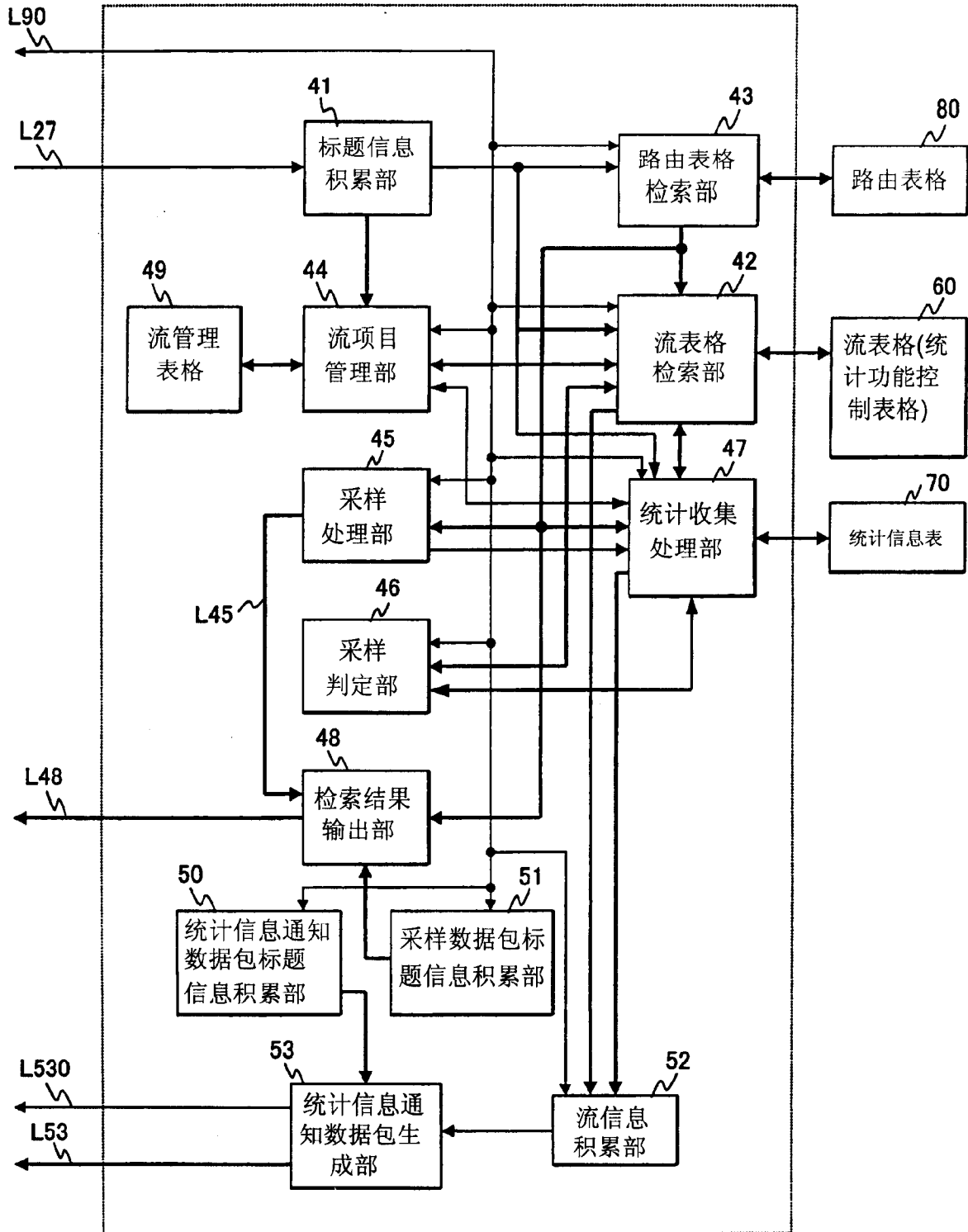
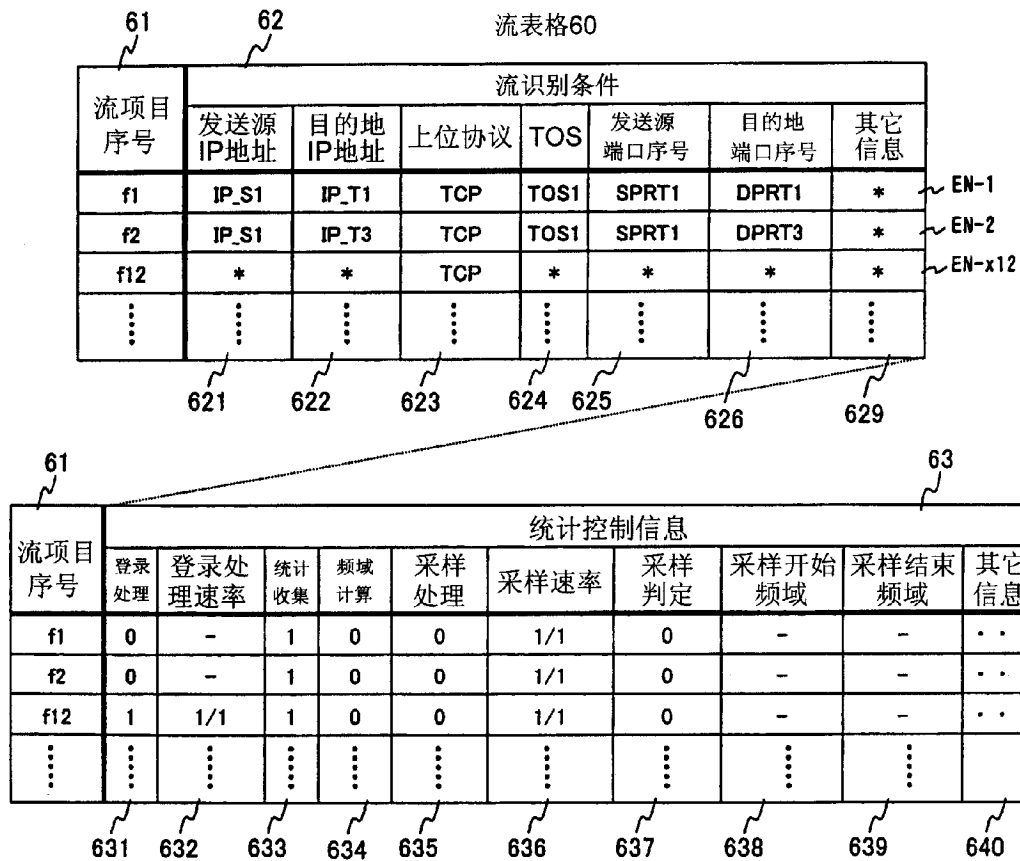


图 20



统计信息表70

流项目 序号	统计信息						
	数据包 数量	字节 数量	输入线 路序号	输出线 路序号	频域	其它 信息	
f1	P1	B1	C_R2	C_T1	-	...	SE-1
f2	P2	B2	C_R2	C_T3	-	...	SE-2
f12	P12	B12	xxx	xxx	-	...	SE-x12
⋮	⋮	⋮	⋮	⋮	⋮	⋮	

61 721 722 723 724 725 729

72

图 22

检索结果通知480

输出 线路 序号	拷贝 指示 标志	封装化 指示 标志	封装标题信息			其它信息
			层2标题	层3标题	层4标题	

481 482 483 484 485

图 23

地址释放控制表格280

281 块	282 发送等待次数
块1	0
...	...
块k	1
块k+1	0
块k+2	1
块k+3	1
...	...
块n	0

图 24

流管理表格49

491 流项目 序号	492 流表格项目 地址	493 数据包 数量	494 更新时刻	495 非更新 次数
f1	1	P1'	100	0
f2	2	P2'	200	1
⋮	⋮	⋮	⋮	⋮

图 25

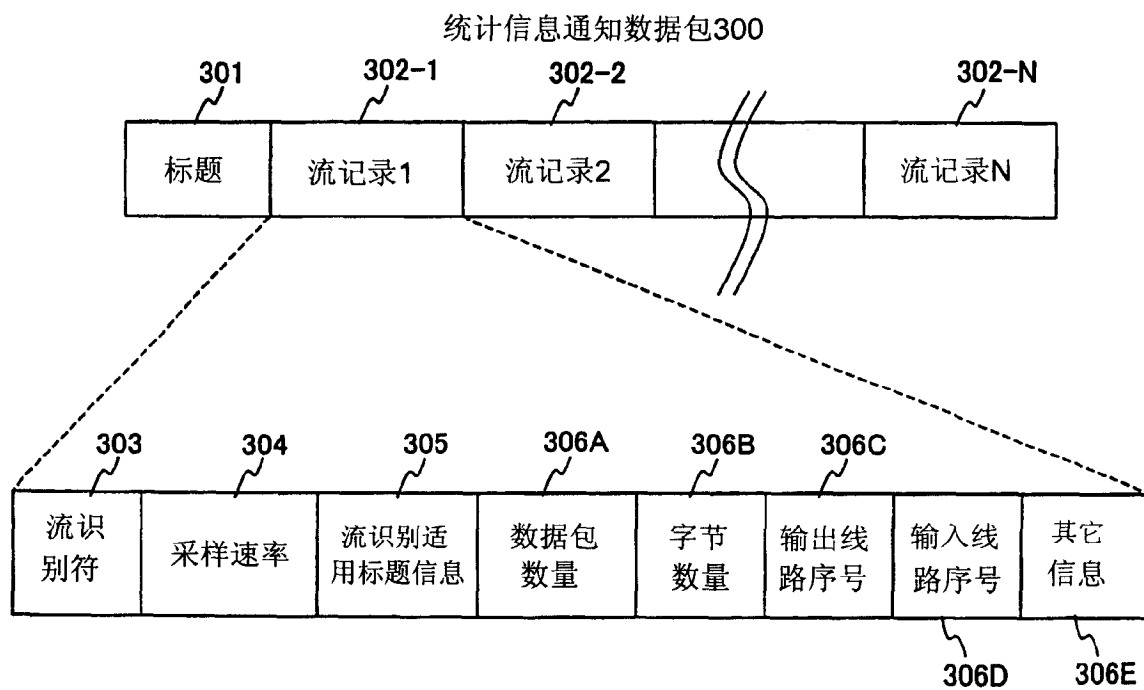


图 26

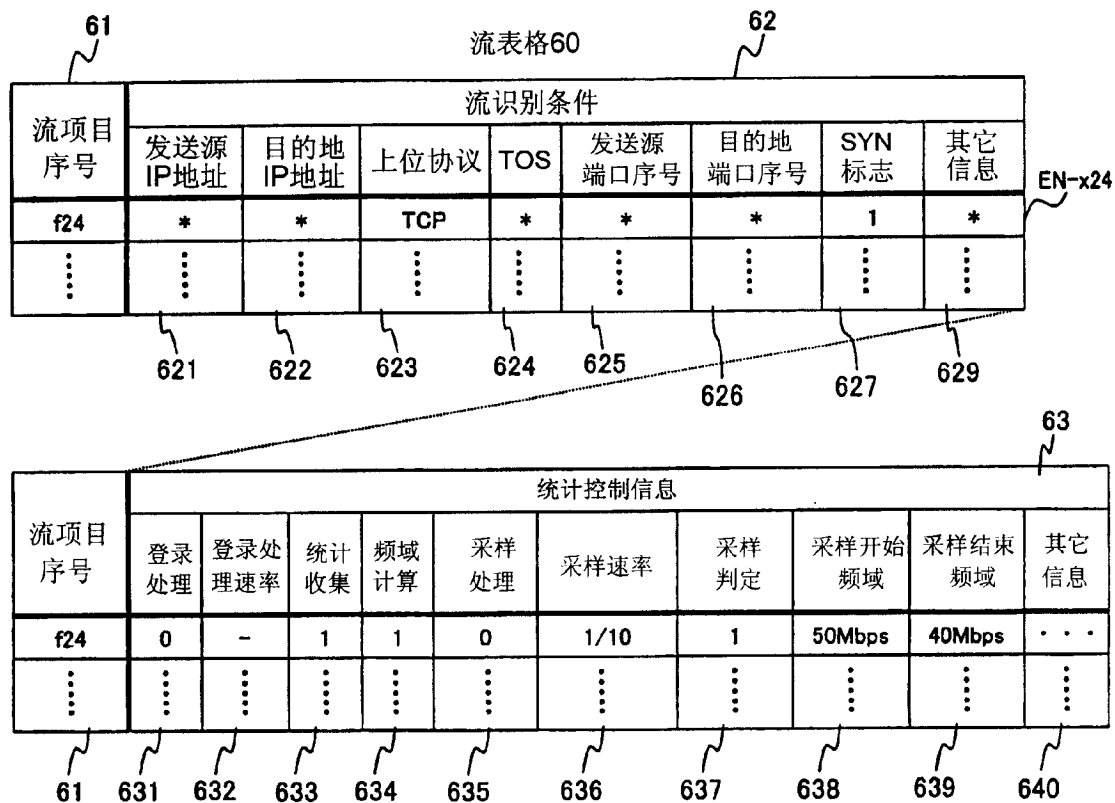


图 27

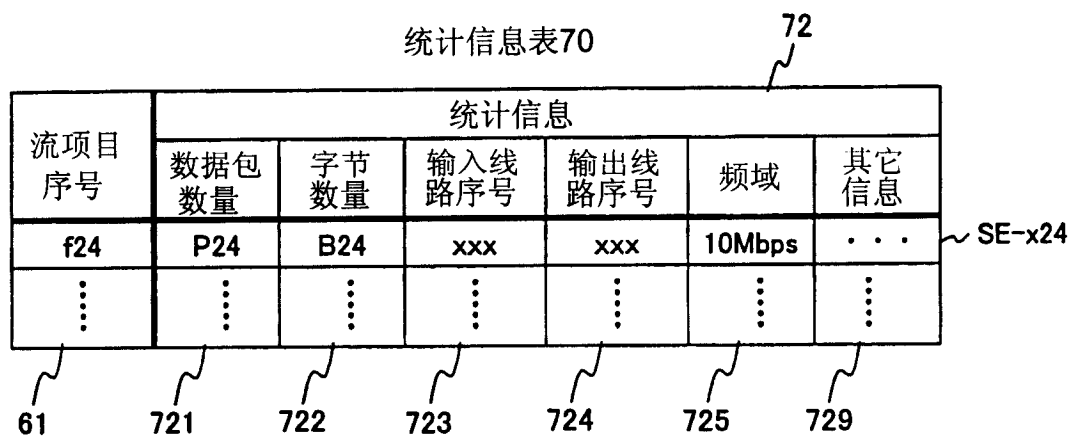


图 28