(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 101075911 B
(45)授权公告日 2010.05.26

(21)申请号 200710008383.7

(22)申请日 2007.01.29

(30)优先权数据
138661/2006 2006.05.18 JP
324200/2006 2006.11.30 JP

(73)专利权人 阿拉克斯拉网络株式会社
地址 日本神奈川县

(72)发明人 正村雄介 渡边义则 柴田刚志

(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 12/24(2006.01)
H04L 12/26(2006.01)
H04L 12/56(2006.01)
H04L 12/46(2006.01)
H04L 29/06(2006.01)

(56)对比文件
CN 1567828 A,2005.01.19, 全文.
CN 1636387 A,2005.07.06, 全文.
CN 1713617 A,2005.12.28, 全文.

审查员 赵晶晶

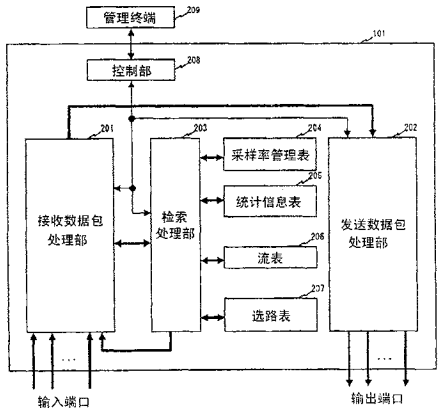
权利要求书 3 页 说明书 14 页 附图 12 页

(54)发明名称

统计信息收集系统及统计信息收集装置

(57)摘要

本发明为了详细把握在网络内流过的业务量，将从统计信息收集装置向采集装置发送的统计信息的业务量有效地削减。本发明是一种通信信息收集系统，具有统计信息收集装置和采集装置，上述统计信息收集装置接收数据包，收集上述接收数据包的统计信息，将上述所收集的统计信息发送给上述采集装置，该通信信息收集系统的特征在于，上述统计信息收集装置存储有流信息，该流信息包含用于识别上述接收数据包所属的流的流识别条件，按由上述流识别条件识别的每个流将上述所收集的数据包的统计信息分类，参照按上述每个流分类的统计信息，按上述每个流决定上述统计信息收集装置将上述统计信息发送给上述采集装置的发送间隔。



CN 101075911 B

1. 一种统计信息收集系统，具有统计信息收集装置和采集装置，

该统计信息收集装置具有：进行运算处理的第 1 处理器、连接到上述第 1 处理器的第 1 存储区、和连接到上述第 1 处理器的第 1 接口；

该采集装置具有：进行运算处理的第 2 处理器、连接到上述第 2 处理器的第 2 存储区、和连接到上述第 2 处理器并且连接到上述统计信息收集装置的第 2 接口；

上述统计信息收集系统的特征在于，

上述第 1 处理器接收数据包，收集上述接收数据包的统计信息，将上述所收集的统计信息发送给上述采集装置；

在上述第 1 存储区存储有流信息和按每个上述流信息发送给上述采集装置的发送间隔，该流信息包含用于识别上述接收数据包所属的流的流识别条件；

上述第 1 处理器：

按由上述流识别条件识别的每个流，将上述所收集的数据包的统计信息分类，

参照按上述每个流分类的统计信息和所存储的上述发送间隔，按上述每个流决定将上述统计信息发送给上述采集装置的发送间隔，以所决定的该发送间隔发送上述统计信息。

2. 如权利要求 1 所述的统计信息收集系统，其特征在于，

上述第 1 存储区存储收集上述统计信息的条件，

上述第 1 处理器根据上述所存储的收集统计信息的条件，收集上述统计信息。

3. 如权利要求 1 所述的统计信息收集系统，其特征在于，

上述统计信息包括上述流的频带，

上述第 1 处理器：

根据在上述统计信息中包含的上述流的频带，决定上述接收数据包的采样间隔；

按上述所决定的采样间隔，对上述接收数据包进行采样；

将上述所采样的数据包的报头信息作为上述统计信息，发送给上述采集装置。

4. 如权利要求 1 所述的统计信息收集系统，其特征在于，

上述第 1 处理器：

根据分析按上述每个流所分类的统计信息的结果，决定上述接收数据包的采样间隔；

按上述所决定的采样间隔，对上述接收数据包进行采样；

将上述所采样的数据包的报头信息作为上述统计信息，发送给上述采集装置。

5. 如权利要求 4 所述的统计信息收集系统，其特征在于，

上述第 2 处理器：

若从上述第 1 处理器接收到统计信息，则对按上述每个流所分类的统计信息进行分析，

将上述统计信息的分析结果发送给上述第 1 处理器；

上述第 1 处理器若接收到上述统计信息的分析结果，则根据上述所接收到的分析结果，决定上述接收数据包的采样间隔。

6. 如权利要求 4 所述的统计信息收集系统，其特征在于，

上述第 1 处理器：

对按上述每个流所分类的统计信息进行分析，

根据上述统计信息的分析结果，决定上述接收数据包的采样间隔。

7. 如权利要求 4 所述的统计信息收集系统，其特征在于，

按每个流设定与按上述每个流所分类的统计信息相关的阈值；

上述第 1 处理器若接收到上述数据包，则根据对上述接收数据包所属的流设定的阈值，判断是否对按上述每个流所分类的统计信息进行分析。

8. 如权利要求 4 所述的统计信息收集系统，其特征在于，

按每个流设定与按上述每个流所分类的统计信息相关的阈值；

上述第 2 处理器若从上述第 1 处理器接收统计信息，则根据对上述所接收的统计信息的流设定的阈值，判断是否对按上述每个流所分类的统计信息进行分析。

9. 如权利要求 7 所述的统计信息收集系统，其特征在于，

上述统计信息包括上述流的频带，

上述第 1 处理器根据上述统计信息的分析结果及上述流的频带中的至少一个，更新与按上述每个流所分类的统计信息相关的阈值。

10. 如权利要求 8 所述的统计信息收集系统，其特征在于，

上述统计信息包括上述流的频带，

上述第 2 处理器根据上述统计信息的分析结果及上述流的频带中的至少一个，更新与按上述每个流所分类的统计信息相关的阈值。

11. 一种统计信息收集装置，具有：进行运算处理的处理器、连接到上述处理器的存储区、和连接到采集装置并且连接到上述处理器的接口；该统计信息收集装置接收数据包，收集上述接收数据包的统计信息，将上述所收集的统计信息发送给上述采集装置；其特征在于，

在上述存储区存储有流信息和按每个上述流信息发送给上述采集装置的发送间隔，该流信息包含用于识别上述接收数据包所属的流的流识别条件，

上述处理器：

按由上述流识别条件识别的每个流，将上述所收集的数据包的统计信息分类，

参照按上述每个流分类的统计信息和所存储的上述发送间隔，按上述每个流决定将上述统计信息发送给上述采集装置的发送间隔，以所决定的该发送间隔发送上述统计信息。

12. 如权利要求 11 所述的统计信息收集装置，其特征在于，

上述存储区存储收集上述统计信息的条件，

上述处理器根据上述所存储的收集统计信息的条件，收集上述统计信息。

13. 如权利要求 11 所述的统计信息收集装置，其特征在于，

上述统计信息包括上述流的频带，

上述处理器：

根据在上述统计信息中包含的上述流的频带，决定上述接收数据包的采样间隔；

按上述所决定的采样间隔，对上述接收数据包进行采样；

将上述所采样的数据包的报头信息作为上述统计信息，发送给上述采集装置。

14. 如权利要求 11 所述的统计信息收集装置，其特征在于，

上述处理器：

根据分析按上述每个流所分类的统计信息的结果，决定上述接收数据包的采样间隔；

按上述所决定的采样间隔，对上述接收数据包进行采样；

将上述所采样的数据包的报头信息作为上述统计信息，发送给上述采集装置。

15. 如权利要求 14 所述的统计信息收集装置，其特征在于，

上述处理器：

对按上述每个流所分类的统计信息进行分析，

根据上述统计信息的分析结果，决定上述接收数据包的采样间隔。

16. 如权利要求 14 所述的统计信息收集装置，其特征在于，

按每个流设定与按上述每个流所分类的统计信息相关的阈值；

上述处理器若接收到上述数据包，则根据对上述接收数据包所属的流设定的阈值，判断是否对按上述每个流所分类的统计信息进行分析。

17. 如权利要求 16 所述的统计信息收集装置，其特征在于，

上述处理器根据上述统计信息的分析结果，更新与按上述每个流所分类的统计信息相关的阈值。

统计信息收集系统及统计信息收集装置

技术领域

[0001] 本发明涉及一种对所传送的数据包的数据包数及字节数等统计信息进行收集的通信统计收集装置，特别涉及一种向采集装置发送统计信息的统计信息收集装置。

背景技术

[0002] 现今，因特网被确定为重要的社会基本设施。因此，不仅是以往的尽力服务型数据通信，还开始对必须保证通信质量的数据进行通信。例如，在必须保证通信质量的数据中有声音、动画及核心业务的事务数据等。此外，通过 ADSL(Asymmetric Digital SubscriberLine :非对称数字用户环线）及 FTTH(Fiber To The Home :光纤到户）技术，访问线路被宽带化，所通信的数据的容量也增大。

[0003] 从这样的背景出发，对于通信业者及 ISP(Internet ServiceProvider :因特网服务供应商）来说，为了把握网络内的通信的状态，需要下述功能，即，收集网络内通信的数据的容量的统计，并通过分析所收集的统计，来监视网络。

[0004] 在监视网络的功能中，特别要求按根据数据的发送源、数据的发送目的地、应用以及质量等级等进行分类的每个数据组（以下称为流）收集统计信息的功能、以及分析每个流的统计信息的功能。

[0005] 通信业者及 ISP 通过利用每个流的统计信息，可以在提供通信的质量保证服务时确认是否保证了通信质量的状况。此外，由于通过利用每个流的统计信息，在有限的网络资源中增大所通信的数据的容量，所以可以利用用于有效活用网络资源的流量工程 (TE)。

[0006] 此外，通过使用每个流的统计信息，可以执行下述供应，即，预测客户的需求，预先准备网络资源，并对应来自客户的需求，迅速提供网络资源。此外，通过使用每个流的统计信息，可以检测、分析对网络的非法攻击。并且，通过使用每个流的统计信息，可以对每个流进行收费。

[0007] 此外，在网络上传送数据包的路由器及交换机等节点装置中具有收集统计信息的功能。

[0008] 统计信息收集系统具有 :多个统计信息收集装置，分散配置在网络上 ;采集装置，根据从这些统计信息收集装置发送来的统计信息，分析网络整体的业务量。

[0009] 作为收集每个流的统计信息的方法，公知有采样型的流统计技术（参照非专利文献 1)。在非专利文献 1 中记载的统计信息收集系统中，作为统计信息收集装置的路由器复制所接收的数据包，选择性地将所复制的数据包传送给采集装置。并且，在采集装置侧从所传送来的数据包中识别出流，并且收集、分析统计信息。

[0010] 统计信息收集系统中所具有的路由器根据由网络管理者预先设定的采样率，对所接受的数据包进行采样，通过预先规定的封装格式，将执行采样处理之后的数据包的复制进行封装，并传送到采集装置。

[0011] 采集装置从路由器传送来的数据包中提取所复制的数据包，根据所复制的数据包的报头信息、以及用于对根据需要而追加的流进行识别的信息，识别流，并更新每个流的统

计信息。

[0012] 此外，作为采样型统计信息收集系统的扩展，公知有以流为单位进行采样的技术（参照专利文献 1）。在非专利文献 1 中记载的流统计技术以一定的比例从路由器所发送的数据包中采样数据包，与此相对，在专利文献 1 中记载的流统计技术从路由器所发送的数据包的报头信息中识别流，以对每个流设定的比例，采样数据包。

[0013] （专利文献 1）日本特开 2006-5402 号公报

[0014] （非专利文献 1）IETF RFC3176”InMon Corporation’s sFlow：AMethod for Monitoring Traffic in Switched and Routed Networks”

[0015] 在非专利文献 1 中记载的流统计技术为，将路由器所接收的数据包的报头信息和一部分数据信息进行封装，并发送给采集装置。因此，为了使路由器详细地监视流的统计信息，需要将采样率设定得很大，频繁地对数据包进行采样，并发送给采集装置。

[0016] 但是，若采样率变大，则路由器的处理负载增大。此外，路由器和采集装置之间的通信量及采集装置的处理负载增大。

[0017] 因此，在通信量大的核心路由器中，很难高精度地收集流信息。此外，即使在通信量比较少的路由器中，也很难把握频带 (band) 小的流。

[0018] 由于在专利文献 1 中记载的流统计技术以流为单位进行采样，所以仅对想要监视的流进行采样，并发送给采集装置。因此，通过限定要采样的流，可以减轻路由器的处理负载、路由器和采集装置之间的通信量及采集装置的处理负载。

[0019] 但是，根据所采样的流的选择，有时不能检测异常的业务量 (traffic)，并且有时不能减轻统计信息的业务量。因此，在专利文献 1 中记载的流统计技术很难适当地选择要监视的流。

发明内容

[0020] 根据代表本发明的一个形态，本发明是一种通信信息收集系统，具有统计信息收集装置和采集装置，该统计信息收集装置具有：进行运算处理的第 1 处理器、连接上述第 1 处理器的第 1 存储区、和连接上述第 1 处理器的第 1 接口；该采集装置具有：进行运算处理的第 2 处理器、连接上述第 2 处理器的第 2 存储区、和连接上述第 2 处理器并且连接上述统计信息收集装置的第 2 接口；上述统计信息收集系统的特征在于，上述第 1 处理器接收数据包，收集上述接收数据包的统计信息，将上述所收集的统计信息发送给上述采集装置；在上述第 1 存储区存储有流信息和按每个上述流信息发送给上述采集装置的发送间隔，该流信息包含用于识别上述接收数据包所属的流的流识别条件；上述第 1 处理器：按由上述流识别条件识别的每个流，将上述所收集的数据包的统计信息分类，参照按上述每个流分类的统计信息和所存储的上述发送间隔，按上述每个流决定将上述统计信息发送给上述采集装置的发送间隔，以所决定的该发送间隔发送上述统计信息。

[0021] 发明效果

[0022] 根据本发明的一个形态，由于按照流的频带和种类自动控制采集装置所接收的统计信息，所以可以削减统计信息收集装置和采集装置之间的通信量，并且降低统计信息收集装置和采集装置的处理负载，提高统计信息的分析精度。

附图说明

[0023] 图 1 是表示本发明的第 1 实施方式的通信统计信息收集系统的框图。

[0024] 图 2 是本发明的第 1 实施方式的路由器的功能框图。

[0025] 图 3 是本发明的第 1 实施方式的流表的示意图。

[0026] 图 4 是本发明的第 1 实施方式的统计信息表的示意图。

[0027] 图 5 是本发明的第 1 实施方式的采样率管理表的示意图。

[0028] 图 6 是本发明的第 1 实施方式的检索处理部的动作的流程图。

[0029] 图 7 是本发明的第 1 实施方式的采样率控制处理的流程图。

[0030] 图 8 是本发明的第 1 实施方式的采集装置的功能框图。

[0031] 图 9 是本发明的第 2 实施方式的路由器的功能框图。

[0032] 图 10 是本发明的第 2 实施方式的项目集表的示意图。

[0033] 图 11 是本发明的第 2 实施方式的统计信息表的示意图。

[0034] 图 12 是本发明的第 2 实施方式的阈值管理表的示意图。

[0035] 图 13 是本发明的第 2 实施方式的业务量统计分析处理部的功能框图。

[0036] 图 14 是本发明的第 3 实施方式的信息统计收集装置的功能框图。

[0037] 图 15 是本发明的第 1 实施方式的采样信息发送格式的示意图。

[0038] 图 16 是本发明的第 2 实施方式的统计信息发送格式的示意图。

具体实施方式

[0039] 使用附图说明本发明的实施方式。

[0040] （第 1 实施方式）

[0041] 使用图 1 至图 8、图 15 说明本发明的第 1 实施方式。

[0042] 图 1 是本发明的第 1 实施方式的通信统计信息收集系统的示意图。

[0043] 统计信息收集系统具有路由器 101、服务器 102、终端 103 以及采集装置 104。经由网络连接这些装置。例如，由 ISP(InternetService Provider：因特网服务供应商）提供网络。此外，网络也可以是企业内网络。

[0044] 具体来说，终端 A103、终端 B103 以及终端 C103 与路由器 A101 连接。服务器 A102 与路由器 B101 连接，服务器 C102 与路由器 C101 连接。采集装置 A104 与路由器 A101 连接。此外，路由器 A101、路由器 B101 及路由器 C101 分别连接。

[0045] 路由器 101 是将在网络内通信的信息传送到其信息的发送目的地的装置。具有处理器、存储装置及通信接口。此外，路由器 101 收集所通信的信息的统计信息，将所收集的统计信息发送给采集装置 104。

[0046] 图 2 是本发明的第 1 实施方式的路由器 101 的功能框图。

[0047] 路由器 101 具有接收数据包处理部 201、发送数据包处理部 202、检索处理部 203、采样率管理表 204、统计信息表 205、流表 206、选路表 207 以及控制部 208。

[0048] 管理终端 209 连接到控制部 208。管理者可以经由管理终端 209 变更在接收数据包处理部 201、发送数据包处理部 202、检索处理部 203 中设定的各种参数。此外，管理终端 209 也可以经由网络连接到控制部 208。

[0049] 接收数据包处理部 201 经由输入端口接收数据包。接收数据包处理部 201 将所接

收的数据包存储在缓冲器中，将所存储的数据包的报头信息发送给检索处理部 203。

[0050] 检索处理部 203 若从接收数据包处理部 201 接收到报头信息，则执行检索处理，将检索处理的结果发送给接收数据包处理部 201。此外，关于检索处理，在图 6 中进行详细的说明。

[0051] 接收数据包处理部 201 若从检索处理部 203 接收检索结果，则基于在检索结果中包含的输出端口，向发送数据包处理部 202 发送数据包。

[0052] 此外，在接收数据包处理部 201 所接收的检索结果中包含对数据包进行采样的指示时，接收数据包处理部 201 将封装的指示、用于采样处理的采样率以及封装报头信息包含在相应的数据包中，将包含有封装的指示、用于采样处理的采样率以及封装报头信息的数据包的报头信息发送给相应的发送数据包处理部 202。此外，在接收数据包处理部 201 所接收的检索结果中包含用于采样处理的采样率以及封装报头信息。

[0053] 说明发送数据包处理部 202 的动作。发送数据包处理部 202 若从接收数据包处理部 201 接收数据包及检索结果，则向检索结果中包含的输出端口发送数据包。

[0054] 此外，在发送数据包处理部 202 所接收的检索结果中包含封装的指示时，发送数据包处理部 202 根据检索结果中包含的封装报头信息制作 IP 数据包，将采样处理所执行的数据包包含在数据部分，发送给采集装置 104。

[0055] 图 15 表示通过发送数据包处理部 202 发送给采集装置 104 的数据包的格式的一个例子。采样信息发送格式 1501 包括 sFlow 报头 1502、取得参数 1503 以及数据包数据 1504。将采样信息发送格式 1501 作为 UDP 的数据报 (datagram) 进行发送。发送数据包处理部 202 在取得参数 1503 的“sampling rate”中设定从接收数据包处理部 201 接收的、用于采样处理的采样率。

[0056] 采样率管理表 204 管理与流的频带和流的种类相对应的采样率，并且检索处理部 203 实际执行采样率控制处理 (图 7) 时参照采样率管理表 204。

[0057] 统计信息表 205 管理所收集的每个流的统计信息。流表 206 包括作为对路由器所接受的数据包的流进行确定的条件的信息、以及表示在流中所执行的处理的信息。选路表 207 注册有与发送源的 IP 地址和发送目的地的 IP 地址相对应的输出端口。

[0058] 图 3 是本发明的第 1 实施方式的流表 206 的示意图。

[0059] 流表 206 包括流识别条件 302 和统计控制信息 303。流识别条件 302 包括发送源 IP 地址 311、发送目的地 IP 地址 312、上层协议 313、发送源端口号 314、发送目的地端口号 315 以及其他信息 316。

[0060] 在发送源 IP 地址 311 中注册有发送路由器 101 所接收的数据包的发送源的 IP 地址。在发送目的地 IP 地址 312 中注册有路由器 101 所接收的数据包的发送目的地的 IP 地址。在上层协议 313 中例如注册有 TCP 及 UDP 等。

[0061] 在发送源端口号 314 中注册有发送路由器 101 所接收的数据包的发送源的端口号。在发送目的地端口号 315 中注册有路由器 101 所接收的数据包的发送目的地的端口号。

[0062] 在其他信息 316 中例如注册有数据包的输入输出端口号、发送源的 MAC 地址、发送目的地的 MAC 地址、TAG 协议的标识符、VLAN(Virtual LAN :虚拟局域网) 的标识符、优先级、TOS 以及 TCP 标志的一部分等。

[0063] 统计控制信息 303 包括注册处理 321、注册处理率 322、统计收集 323、采样处理

324、发送控制 325、流种类 326、采样率 327 以及其他信息 328。

[0064] 在注册处理 321 中注册有是否在流表 206 中注册新的条目的信息。若在注册处理 321 中注册了“1”，则检索处理部 203 注册新的条目。另一方面，若在注册处理 321 中注册了“0”，则检索处理部 203 不注册条目。

[0065] 在注册处理率 322 中注册有在流表 206 中注册新的条目时条目被注册的比率。若在注册处理率 322 中注册了“1/1”，则检索处理部 203 一定注册新的条目。此外，在注册处理 321 中注册了“0”时，由于不新注册条目，所以在注册处理率 322 中注册为“-”。

[0066] 此外，在流 ID“F12”的注册处理率 322 中注册有“1/1”。如果流 ID“F12”与任一个流识别条件都不一致，并且上层协议 313 是 TCP，则自动向流表 206 中追加新的条目。

[0067] 在统计收集 323 注册有是否收集统计信息的信息。在统计收集 323 中注册有“1”时，收集所对应的条目的统计信息。另一方面，在统计收集 323 中注册了“0”时，不收集所对应的条目的统计信息。

[0068] 在采样处理 324 中注册有是否执行采样处理的信息。采样处理是发送数据包处理部 202 根据采样率复制数据包并将所复制的数据包发送给采集装置 104 的处理。

[0069] 若在采样处理 324 中注册了“1”，则利用在采样率 327 中注册的值执行采样处理。若在采样处理 324 中注册了“0”，则不执行采样处理。

[0070] 在发送控制 325 中注册有是否执行发送控制处理的信息。此外，发送控制处理是变更采样率 327 中注册的值的处理。在图 7 中说明细节。若在发送控制 325 中注册有“1”，则执行发送控制处理。

[0071] 在流种类 326 中注册有流种类。例如，在流种类 326 中注册有“0”、“1”以及“2”中的某一个。“0”表示未知流。在流表 206 中新注册的流是未知流。此外，“1”表示已分析的流。被判断为安全的流是已分析的流、“2”表示异常流。被判断为异常的流是异常流。

[0072] 此外，在流种类 326 中也可以注册有“3”以上的值，表示异常流的异常程度。

[0073] 采集装置 104 参照每个流的统计信息，决定流种类，将所决定的流种类发送给路由器 101。路由器 101 若从采集装置 104 接收到流种类 326，则经由控制部 208 注册流表 206 的流种类 326。此外，可以由路由器 101 注册流种类 326，也可以经由管理终端 209 由管理者注册流种类 326。

[0074] 在采样率 327 中注册有执行采样处理的比例。例如若在采样率 327 中注册有“1/1000”，则以相应流的每 1000 个数据包 1 个的比例执行采样处理。

[0075] 在其他信息 328 中例如注册有采样开始条件及采样结束条件等。

[0076] 图 4 是本发明的第 1 实施方式的统计信息表 205 的示意图。

[0077] 统计信息表 205 包括流 ID301 及统计信息 401。

[0078] 流 ID301 是与流表 206 的流 ID301 通用的 ID，使流识别条件 302 和统计信息 401 对应。除了使用通用的 ID 使流识别条件 302 和统计信息 401 对应的方法之外，还可以利用使用指针使流识别条件 302 和统计信息 401 对应的方法、以及将流表 206 和统计信息表 205 作为一个表进行保持的方法等。

[0079] 统计信息 401 包括数据包数 411、字节数 412、频带 (bps)413、频带 (pps)414、开始时刻 415、阈值 416 以及其他信息 417。

[0080] 在数据包数 411 中注册有累计路由器 101 所接收的数据包数的值。若路由器 101

接收到与流 ID301 对应的数据包，则向数据包数 411 中加 1。

[0081] 在字节数 412 中注册有累计路由器 101 所接收的数据包中包含的数据包长度的值。若路由器 101 接收到与流 ID301 对应的数据包，则路由器 101 将所接收到的数据包的报头信息中包含的数据包长度加入字节数 412。

[0082] 在频带 (bps)413 中注册有流专用的频带 (bps)。在频带 (pps)414 中注册有流专用的频带 (pps)。

[0083] 在开始时刻 415 中注册有数据包数 411 被注册为 1 的时刻。即，注册有路由器 101 最初接收到于流 ID 相应的数据包的时刻。

[0084] 在阈值 416 中注册有是否为了分析统计信息而向采集装置 104 发送统计信息的条件即阈值。通常，在阈值 416 中注册有数据包数 411 的阈值。若数据包数 411 达到在阈值 416 中注册的值，则路由器 101 将该流的统计信息发送给采集装置 104。并且采集装置 104 的流分析处理部 805 分析流的统计信息。

[0085] 此外，在阈值 416 中也可以注册有与字节数 412 及开始时刻 415 相关的阈值。

[0086] 在其他信息 417 中注册有并没有包含在流 ID 中的项目出现的种类数、路由器 101 最后接收数据包的时刻等。此外，所出现的种类数表示例如在发送源 IP 地址包含在流表 206 的流识别条件 302 中时发送目的地 IP 地址出现了何种种类。

[0087] 图 5 是本发明的第 1 实施方式的采样率管理表 204 的示意图。

[0088] 采样率管理表 204 包括频带 (pps)501 及采样率 502。

[0089] 频带 (pps)501 与统计信息表 205 的频带 (pps)414 相对应。此外，也可以不是频带 (pps)，而是使用与统计信息表 205 的频带 (bps)413 相对应的频带 (bps)。

[0090] 采样率 502 对流表 206 的每个流种类 326 注册有在采样率 327 中注册的值。具体来说，采样率 502 包括与已分析的流 (0)511、未知流 (1)512 以及异常流 (2)513 相对应的注册在采样率 327 中的值。

[0091] 检索处理部 203 为了根据频带及流种类适当地将采样率 327 注册到流表 206 中，而参考采样率管理表 204。

[0092] 此外，采样率管理表 204 可以从管理终端 209 经由控制部 208 变更注册内容。

[0093] 图 6 是本发明的第 1 实施方式的检索处理的流程图。

[0094] 检索处理部 203 从接收数据包处理部 201 接收报头信息 (步骤 601)。

[0095] 检索处理部 203 若接收到报头信息，则检索流表 206(步骤 602)。此外，检索处理部 203 若接收到报头信息，则检索选路表 207(步骤 621)。此外，并列执行步骤 602 ～步骤 611 的处理和步骤 621 ～步骤 622 的处理。

[0096] 具体来说，在步骤 602 的处理中，检索处理部 203 根据包含在所接收的报头信息中的发送源 IP 地址、发送目的地 IP 地址、发送源端口号以及发送目的地端口号等，检索流表 206 的流识别条件 302，确定流 ID301。

[0097] 并且，检索处理部 203 根据所确定的流 ID301 的统计控制信息 303，执行步骤 603 ～步骤 611 的处理的统计处理。

[0098] 首先，检索处理部 203 参照流表 206，取得注册在注册处理 321 中的信息 (步骤 603)。

[0099] 接着，检索处理部 203 判断是否追加新的条目 (步骤 604)。具体来说，在步骤 603

的处理中所取得的注册在注册处理 321 中的信息为“1”的情况下，检索处理部 203 判断为追加新的条目，进入步骤 605 的处理。另一方面，在步骤 603 的处理中所取得的注册在注册处理 321 中的信息为“0”的情况下，检索处理部 203 判断为不追加新的条目，进入步骤 606 的处理。

[0100] 检索处理部 203 根据注册处理率 322，向流表 206 中追加新的条目（步骤 605）。

[0101] 接着，检索处理部 203 参照流表 206 的统计收集 323 及采样处理 324（步骤 606）。其后，处理分为步骤 607 的处理和步骤 610 的处理。

[0102] 检索处理部 203 参照流表 206 判断是否执行统计收集处理（步骤 607）。具体来说，检索处理部 203 在注册在统计收集 323 中的信息为“1”的情况下判断为执行统计收集处理，进入步骤 608 的处理。另一方面，检索处理部 203 在注册在统计收集 323 中的信息为“1”以外的情况下判断为不执行统计收集处理，结束统计处理。

[0103] 在步骤 607 的处理中，在判断为执行统计收集处理时，检索处理部 203 更新统计信息表 205（步骤 608）。

[0104] 具体来说，检索处理部 203 在所确定的流 ID 的数据包数 411 上加 1，在字节数 412 上加上报头信息中包含的数据包长度。并且，检索处理部 203 注册有频带 (bps)413 及频带 (pps)414 中所测量的频带 (bps) 及频带 (pps)。

[0105] 此外，与步骤 607 的处理并行，检索处理部 203 参照流表 206，判断是否执行采样处理（步骤 610）。具体来说，检索处理部 203 在注册在采样处理 324 中的信息为“1”以外的情况下判断为不执行采样处理。另一方面，检索处理部 203 在注册在采样处理 324 中的信息为“1”的情况下判断为执行采样处理，进入步骤 611 的处理。

[0106] 在步骤 610 的处理中，在判断为执行采样处理时，检索处理部 203 利用在采样率 327 中注册的值，执行采样处理（步骤 611）。具体来说，检索处理部 203 将执行采样处理的指示追加到发送给接收数据包处理部 201 的检索结果中。此外，检索处理部 203 在发送数据包处理部 202 执行采样处理时，将封装数据包的报头信息追加到检索结果中。

[0107] 检索处理部 203 若在步骤 601 的处理中接收到报头信息，则检索选路表 207（步骤 621）。检索处理部 203 检索选路表 207，并取得输出端口（步骤 622）。

[0108] 并且，检索处理部 203 将在步骤 622 的处理中取得的输出端口的信息追加到检索结果中，并结束检索处理（步骤 623）。此外，在步骤 611 的处理中执行了采样处理的情况下，检索处理部 203 将执行采样处理的指示、用于采样处理的采样率以及封装的报头信息追加到检索结果中。

[0109] 若结束了检索处理（步骤 623），则检索处理部 203 执行采样率控制处理（步骤 624）。此外，在图 7 中详细说明采样率控制处理。此外，若结束了检索处理（步骤 623），则检索处理部 203 将检索结果发送给接收数据包处理部 201（步骤 625）。

[0110] 图 7 是本发明的第 1 实施方式的采样率控制处理（步骤 624）的流程图。

[0111] 首先，检索处理部 203 参照流表 206 取得在发送控制 325 中注册的信息（步骤 701）。

[0112] 接着，检索处理部 203 根据所取得的在发送控制 325 中注册的信息，判断是否执行发送控制处理（步骤 702）。具体来说，在所取得的在发送控制 325 中注册的信息为“1”的情况下，检索处理部 203 判断为执行发送控制处理，并进入步骤 703 的处理。另一方面，在

所取得的在发送控制 325 中注册的信息为“1”以外的情况下，检索处理部 203 判断为不执行发送控制处理，并结束采样率控制处理。

[0113] 在判断为执行发送控制处理时，检索处理部 203 取得流表 206 的流种类 326 及统计信息表 205 的频带 (pps)414（步骤 703）。

[0114] 并且，检索处理部 203 参照采样率管理表 204，计算与所取得的流种类 326 及频带 (pps)414 相对应的采样率（步骤 704）。

[0115] 此外，在没有测量到频带 (pps)414 的情况下，参照与采样率管理表 204 的频带 (pps)501 的“缺省值”相对应的采样率。

[0116] 将在步骤 704 的处理中计算出的采样率的值注册到流表 206 的相应的流 ID301 的采样率 327 中（步骤 705）。

[0117] 若在流表 206 中注册新的采样率，则结束采样控制处理。

[0118] 此外，在本实施方式中，检索处理部 203 参照采样率管理表 204，计算采样率，但也可以使用计算公式根据频带及流种类计算采样率。

[0119] 此外，说明了路由器 101 的检索处理部 203 动态变更采样率的例子，但采集装置 104 也可以动态变更采样率 327。在图 8 中详细说明采集装置 104 变更采样率 327 的方法。此外，管理者可以经由管理终端 209 手动变更采样率。

[0120] 图 8 是本发明的第 1 实施方式的采集装置 104 的功能框图。

[0121] 采集装置 104 包括数据包收发处理部 801、统计信息数据包解析部 802、数据库管理部 803、采样设定处理部 804、流分析处理部 805、流信息显示处理部 806、输入输出处理部 807 以及采样率管理表 204。

[0122] 此外，采集装置 104 的输入输出处理部 807 连接到输入输出装置（鼠标 821、键盘 822 以及显示器 823）。此外，也可以是终端计算机经由网络连接到采集装置 104，通过该终端计算机所具有的输入输出装置进行输入输出。

[0123] 数据包收发处理部 801 从路由器 101 接收统计信息数据包。此外，数据包收发处理部 801 发送控制信息数据包。

[0124] 统计信息数据包解析部 802 提取在统计信息数据包中包含的被执行了采样处理的数据包的报头信息。并且，统计信息数据包解析部 802 将所提取的报头信息发送给数据库管理部 803。

[0125] 数据库管理部 803 根据从统计信息数据包解析部 802 接收到的报头信息，更新统计信息数据库 811。此外，数据库管理部 803 测量执行了采样处理的数据包所属的流的频带。并且，数据库管理部 803 将采样率、流种类以及所测量的流的频带发送给采样设定处理部 804。

[0126] 此外，数据库管理部 803 在执行了采样处理的数据包所属的流满足在阈值中设定的条件的情况下，将统计信息数据库 811 的相应的流的信息发送给流分析处理部 805。在阈值中设定的条件有流的数据包数为规定的数以上的情况以及流的频带 (bps 或 pps) 为规定的值以上的情况等。

[0127] 数据库管理部 803 根据对从流分析处理部 805 发送的统计信息数据库 811 进行检索的条件，检索统计信息数据库 811，将所检索的结果发送给流分析处理部 805。

[0128] 此外，数据库管理部 803 从流分析处理部 805 接收分析结果，根据所接收的分析结

果，注册或更新统计信息数据库 811 的流种类。

[0129] 采样设定处理部 804 参照采样率管理表 204，根据从数据库管理部 803 接收的采样率、流种类以及频带，计算相应的流的采样率。并且，采样设定处理部 804 向数据包收发处理部 801 发送将所算出的采样率作为控制信息数据包发送给路由器 101 的指示。

[0130] 此外，管理者可以通过鼠标 821 或键盘 822 的输入装置直接设定采样率。采集装置 104 可以将所设定的采样率发送给路由器 101。

[0131] 流分析处理部 805 从数据库管理部 803 接收执行了采样处理的数据包所属的统计信息数据库 811 的信息。并且，流分析处理部 805 根据所接收的统计信息数据库 811 的信息，分析相应的流的流种类。流分析处理部 805 将分析相应的流的流种类的结果发送给数据库管理部 803。

[0132] 此外，如果必要，流分析处理部 805 将从统计信息数据库 811 检索与相应的流关联的信息的条件发送给数据库管理部 803。

[0133] 流信息显示处理部 806 从统计信息数据库 811 接收统计信息。并且，流信息显示处理部 806 对统计信息执行分组，或者将统计信息图表化。

[0134] 采样设定处理部 804 计算采样率，通过将所计算出的采样率发送给路由器 101，采集装置 104 变更流表 206 中包含的采样率 327。

[0135] 接收到由采样设定处理部 804 计算出的采样率的路由器 101 经由控制部 208 及检索处理部 203 更新流表 206 的采样率 327。在流表 206 中不含有与所更新的流相对应的流 ID 时，路由器 101 在流表 206 中追加的新的条目。

[0136] 此外，在采集装置 104 更新流表 206 的采样率 327 时，路由器 101 将发送控制 325 设定为“0”，从而不能通过路由器 101 更新采样率。

[0137] （第 2 实施方式）

[0138] 使用图 9 ～图 13 以及图 16 说明本发明的第 2 实施方式。此外，对与第 1 实施方式相同的结构要素赋予相同的符号，并省略说明。

[0139] 本实施方式的路由器 101 具有第 1 实施方式的路由器 101 分析流统计信息的功能。

[0140] 图 9 是本发明的第 2 实施方式的路由器 101 的功能框图。

[0141] 路由器 101 具有接收数据包处理部 201、发送数据包处理部 202、检索处理部 203、业务量统计分析处理部 901、采样率管理表 204、统计信息表 205、流表 206、选路表 207、项目集 (item set) 表 902、阈值管理表 903 以及控制部 208。

[0142] 通过检索处理部 203 及业务量统计分析处理部 901 参照统计信息表 205。

[0143] 业务量统计分析处理部 901 生成对构成业务量信息的各项目任意组合之后的项目集表 902，通过收集项目集表 902 的条目的统计信息，提取特征业务量。

[0144] 项目集表 902 表示构成业务量信息的各项目的任意组合。此外，在图 10 中详细说明项目集表 902。在根据流的频带及流的种类变更统计信息表 205 的阈值 1206 时参照阈值管理表 903。此外，在图 12 中详细说明阈值管理表 903。

[0145] 图 10 是本发明的第 2 实施方式的项目集表 902 的示意图。

[0146] 在本实施方式中，构成业务量信息的项目是发送源 IP 地址、发送目的地 IP 地址、发送源端口号以及发送目的地端口号这 4 种。此外，作为其他的构成业务量信息的项目，例

如也可以使用发送源 MAC 地址、发送目的地 MAC 地址、VLAN-ID、协议号、优先级、TOS 以及 TCP 标志等。

[0147] 项目集表 902 包括任意组合构成业务量信息的项目所生成的各个表。

[0148] 在本实施方式中，项目集表 902 包括表 A1101、表 B1102、表 C1103 以及表 D1104。表 A1101 中构成业务量信息的项目为一个项目。表 B1102 中构成业务量信息的项目为二个项目。表 C1103 中构成业务量信息的项目为三个项目。表 D1104 中构成业务量信息的项目为四个项目。

[0149] 此外，在本实施方式中说明了在项目集表 902 中包含的表数为四个的情况，但项目集表 902 至少包括一个表，由于构成业务量信息的项目是四种，所以项目集表 902 最大包括四个表。在项目集表 902 中包含的各个表包括条目号 1111 及项目 1112。

[0150] 条目号 1111 是在项目集表 902 中包含的条目的唯一标识符。项目 1112 包括种类 1121 及值 1122。在种类 1121 中注册有构成业务量信息的项目。在值 1122 中注册有在种类 1121 中注册的构成业务量信息的项目的值。

[0151] 图 11 是本发明的第 2 实施方式的统计信息表 205 的示意图。

[0152] 通过业务量统计分析处理部 901 及检索处理部 203 参照统计信息表 205。

[0153] 统计信息表 205 包括条目号 1111、数据包数 1201、字节数 1202、频带 (bps)1203、频带 (pps)1204、开始时刻 1205、阈值 1206 以及其他信息 1207。

[0154] 条目号 1111 是与项目集表 902 及流表 206 的条目号通用的标识符，使项目集表 902 和统计信息表 205 对应。

[0155] 此外，在本实施方式中，业务量统计分析处理部 901 及检索处理部 203 参照一个统计信息表 205，但也可以相互独立地保持业务量统计分析处理部 901 参照的统计信息表和检索处理部 203 参照的统计信息表。

[0156] 在数据包数 1201 中注册有累计路由器 101 所接收的数据包数的值。具体来说，若路由器 101 接收到与条目号 1111 对应的数据包，则路由器 101 向数据包数 1201 中加 1。

[0157] 在字节数 1202 中注册有累计路由器 101 所接收的数据包中包含的数据包长度的值。若路由器 101 接收到与条目号 1111 对应的数据包，则路由器 101 将所接收到的数据包的报头信息中包含的数据包长度加入字节数 1202。

[0158] 在频带 (bps)1203 中注册有相应的条目号专用的频带 (bps)。在频带 (pps)1204 中注册有相应的条目号专用的频带 (pps)。

[0159] 在开始时刻 1205 中注册有数据包数 1201 被注册为 1 的时刻。即，注册有路由器 101 最初接收到与流 ID 相应的数据包的时刻。

[0160] 在阈值 1206 中注册有统计表制作部 1002 向流分析部 1003 发送信息时的条件。通常，在阈值 1206 中注册有数据包数 1201 的阈值。若数据包数 1201 达到在阈值 1206 中注册的值，则统计表制作部 1002 向流分析部 1003 发送信息。

[0161] 此外，在阈值 1206 中也可以注册有与字节数 1202 及开始时刻 1205 相关的阈值。

[0162] 在其他信息 1207 中注册有并没有包含在项目集表 902 的项目 1101 中的项目出现的种类数、和路由器 101 最后接收数据包的时刻等。此外，所出现的种类数是在发送源 IP 地址包含在项目集表 902 中时在项目集表 902 中不包括的项目即发送目的地 IP 地址出现的种类数。

[0163] 图 12 是本发明的第 2 实施方式的阈值管理表 903 的示意图。

[0164] 阈值管理表 903 包括频带 (pps)1401 及阈值 1402。

[0165] 频带 (pps)1401 与统计信息表 205 的频带 (pps)1204 相对应。此外，频带使用 pps，但也可以使用 bps。

[0166] 在阈值 1402 中对每个流种类注册有阈值的比率。在统计信息表 205 的阈值 1206 是数据包数 1201 的阈值时，在统计信息表 205 的阈值 1206 中设定将在阈值 1402 中注册的比率乘以按由项目集表 902 确定的每个条目号 1111 决定阈值之后的值。

[0167] 为了根据频带及流种类在统计信息表 205 的阈值 1206 中注册适当的值，参照阈值管理表 903。此外，可以从管理终端 209 通过控制部 208 变更阈值管理表 903。

[0168] 图 13 是本发明的第 2 实施方式的业务量统计分析处理部 901 的功能框图。

[0169] 业务量统计分析处理部 901 包括报头信息存储部 1001、统计表制作部 1002、流分析部 1003、统计信息数据包生成部 1004 及阈值设定部 1005。

[0170] 报头信息存储部 1001 从接收数据包处理部 201 接收报头信息，将所接收的报头信息发送给统计表制作部 1002。

[0171] 统计表制作部 1002 生成在所接收的报头信息中包含的构成业务量信息的项目（发送源 IP 地址、发送目的地 IP 地址、发送源端口号及发送目的地端口号）的任意组合。并且，统计表制作部 1002 参照项目集表 902，检索与所生成的组合一致的条目。

[0172] 在存在与项目集表 902 一致的条目时，统计表制作部 1002 根据一致的条目的条目号 1111，更新统计信息表 205 的相应的数据包数 1201、字节数 1202、频带 (bps)1203、频带 (pps)1204、开始时刻 1205、阈值 1206。

[0173] 另一方面，在不存在与项目集表 902 一致的条目时，统计信息表制作部 1002 向项目集表 902 和统计信息表 205 中追加新生成的组合的条目。

[0174] 在不能向项目集表 902 或统计信息表 205 中追加新的条目时，用新追加的条目改写已注册的条目。作为选择所改写的已注册的条目的方法，有选择统计信息表 205 的数据包数 1201 少的条目的方法、选择最后更新的时刻最早的条目的方法、以及随机选择条目的方法等。

[0175] 在追加新的条目时，在项目集表 902 中注册所生成的构成业务量信息的项目的组合。在统计信息表 205 的数据包数 1201 中注册“1”，在字节数 1202 中注册在报头信息中包含的数据包长度。此外，在频带 (bps)1203 及频带 (pps)1204 中注册由路由器 101 检测的频带。

[0176] 在开始时刻 1205 中注册数据包 1201 被注册为 1 的时刻。在阈值 416 中注册预先设定的值。此外，对项目集表 902 的每个组合设定在阈值 416 中注册的预先设定的值，并且管理者可以经由控制部 208 变更该值。

[0177] 说明统计表制作部 1002 更新统计信息表 205 的条目的方法。此外，以图 1 中的从终端 1 到服务器 1 的数据包的流为例进行说明。这里，设终端 1 的 IP 地址为 X1，服务器 1 的 IP 地址为 Y1，发送源端口号为 A1，发送端口号为 B1。

[0178] 统计表制作部 1002 若从报头信息存储部 1001 接收到报头信息，则分别将发送源 IP 地址及 X1 注册到表 A1101 的种类 1121 及值 1122 中，从而注册发送源 IP 地址为 X1 的条目。同样，统计表制作部 1002 在表 A1101 中注册发送目的地地址为 Y1 的条目、发送源端口

号为 A1 的条目以及发送目的地端口号为 B 1 的条目。因此，更新或新制作表 A1101。

[0179] 此外，统计表制作部 1002 分别将发送源 IP 地址及 X1 注册到表 B1102 的项目 A 中包含的种类 1121 及值 1122 中，并将发送目的地 IP 地址及 Y1 注册到项目 B 中包含的种类 1121 及值 1122 中，从而注册发送源 IP 地址为 X1 并且发送目的地 IP 为 Y1 的条目。同样，在表 B1102 中注册发送源 IP 地址为 X1 并且发送源端口号为 A1 的条目、发送源 IP 地址为 X1 并且发送目的地端口号为 B1 的条目、发送目的地 IP 地址为 Y1 并且发送源端口号为 A1 的条目、发送目的地 IP 地址为 Y1 并且发送目的地端口号为 B1 的条目、以及发送源端口号为 A1 并且发送目的地端口号为 B1 的条目。因此，更新或新制作表 B1102。

[0180] 同样，统计表制作部 1002 在表 C1103 中注册发送源 IP 地址为 X1 并且发送目的地 IP 地址为 Y1 并且发送源端口号为 A1 的条目、发送源 IP 地址为 X1 并且发送目的地 IP 地址为 Y1 并且发送目的地端口号为 B1 的条目、发送源 IP 地址为 X1 并且发送源端口号为 A1 并且发送目的地端口号为 B1 的条目、以及发送目的地 IP 地址为 Y1 并且发送源端口号为 A1 并且发送目的地端口号为 B1 的条目。因此，更新或新制作表 C1103。

[0181] 同样，统计表制作部 1002 在表 D1104 中注册发送源 IP 地址为 X1 并且发送目的地 IP 地址为 Y1 并且发送源端口号为 A1 并且发送目的地端口号为 B1 的条目。因此，更新或新制作表 D1104。

[0182] 此外，在本实施方式中，统计表制作部 1002 将所有项目的组合注册在项目集表 902 中，但可以根据需要进行省略。

[0183] 例如，在表 B1102 中仅注册发送源 IP 地址 X1 和发送目的地端口号 B1 的条目，并且表 B1102 中不注册其他组合。此外，管理者经由控制部 208 设定在各表中注册的组合。

[0184] 此外，统计表制作部 1002 若更新项目集表 902 和统计信息表 205，则参照统计信息表 205 的阈值 1206，并且判断是否将信息发送给流分析部 1003。

[0185] 通常，统计表制作部 1002 对统计信息表 205 中包含的数据包数 1201 和阈值 1206 进行比较。具体来说，若数据包数 1201 为阈值 1206 以上，则统计表制作部 1002 判断为将项目集表 902 及统计信息表 205 的相应的条目的信息发送给流分析部 1003，并且在流分析部 1003 中判断该信息。

[0186] 此外，统计表制作部 1002 在将信息发送给流分析部 1003 的同时，在统计信息表 205 的相应的条目（数据包数 1201、字节数 1202、开始时刻 1205 及其他信息 1207）中注册“0”。此外，在阈值 1206 中注册预先设定的值。

[0187] 另一方面，若数据包数 1201 不足阈值 1206，则统计表制作部 1002 判断为不将项目集表 902 及统计信息表 205 的相应的条目的信息发送给流分析部 1003。

[0188] 此外，也可以在阈值 1206 中注册字节数 1202 的阈值、开始时刻 1205 的阈值或其他信息 1207 的阈值。此时，统计表制作部 1002 对应阈值 1206，参照字节数 1202、开始时刻 1205 或其他信息 1207，判断是否将信息发送给流分析部 1003。

[0189] 在统计表制作部 1002 参照开始时刻 1205 判断是否将信息发送给流分析部 1003 时，从当前时刻减去开始时刻 1205，算出持续时间。并且，统计表制作部 1002 比较所算出的持续时间和阈值 1206。如果所算出的持续时间为阈值 1206 以上，则统计表制作部 1002 判断为将信息发送给流分析部 1003。另一方面，如果所算出的持续时间不足阈值 1206，则统计表制作部 1002 判断为不将信息发送给流分析部 1003。

[0190] 此外，统计表制作部 1002 保持有阈值 1206 是统计信息表 205 中包含的哪个信息的阈值的情况，并且管理者可以通过控制部 208 变更该情况。

[0191] 此外，在本实施方式中，统计表制作部 1002 参考一个阈值 1206，但也可以参照多个阈值。

[0192] 此时，统计信息表 205 包括多个阈值。若满足多个阈值中的预先设定的数量的阈值，则统计表制作部 1002 将相应的条目的信息发送给流分析部 1003。

[0193] 例如，在第 1 阈值中注册有数据包数 1201 的阈值，在第 2 阈值中注册有与开始时刻 1205 相关的阈值。统计表制作部 1002 在满足第 1 阈值并且满足第 2 阈值的情况下，将相应的条目的信息发送给流分析部 1003。此外，统计表制作部 1002 也可以在满足第 1 阈值及第 2 阈值中的至少一个的情况下，向流分析部 1003 发送。

[0194] 此外，在阈值 1206 是所有的条目所通用的值时，即不对每个流设定阈值时，也可以是统计表制作部 1002 保持所有的条目所通用的阈值，并且统计信息表 205 不保持阈值 1206，从而节约所使用的存储量。

[0195] 流分析部 1003 根据从统计表制作部 1002 发送的项目集 902 及统计信息表 205 的相应的条目的信息，判断业务量的频带和种类。

[0196] 此外，流分析部 1003 根据需要从项目集 902 及统计信息表 205 检索其他条目信息，分析条目的种类。

[0197] 在流分析部 1003 中分析的结果及相应条目的统计信息被发送到统计信息数据包生成部 1004。此外，还将条目的频带、条目的种类以及条目号 1111 发送给阈值设定部 1005。此外，流分析部 1003 若对条目的种类分析出异常，则将该条目的统计信息发送给控制部 208。

[0198] 统计信息数据包生成部 1004 将从流分析部 1003 接收到的分析结果及统计信息修整为发送格式，发送给路由器 101 的接收数据包处理部 201。

[0199] 图 16 表示由统计信息数据包生成部 1004 向接收数据包处理部 201 发送的统计信息发送格式 1601 的一个例子。统计信息发送格式 1601 包括报头信息 1602 及统计信息 1603。统计信息发送格式 1601 作为 SCTP、TCP 或 UDP 的数据报进行发送。

[0200] 在统计信息 1603 中包含有用于收集统计信息的采样率、由统计信息表 205 收集的统计信息以及项目集 902 的项目 1102。此外，由管理者通过控制部 208 在统计信息数据包生成部 1004 中预先设定作为统计信息的发送目的地的采集装置 104 的地址。

[0201] 阈值设定部 1005 参照阈值管理表 903，根据从流分析部 1003 接收到的条目的频带及条目的种类，计算阈值 1206，该阈值 1206 决定接着从统计表制作部 1002 向流分析部 1003 发送的间隔。具体来说，阈值设定部 1005 参照阈值管理表 903，计算出与相应的条目的频带 (pps) 及相应的条目的种类相对应的比率。并且，阈值设定部 1005 将所算出的比率发送给统计表制作部 1002。

[0202] 统计表制作部 1002 将所接收的比率乘以在相应的条目的阈值 1206 中注册的值，计算出新的阈值 1206。将计算出的阈值注册在相应的条目的阈值 1206 中。

[0203] 接着，说明在第 1 实施方式的接收数据包处理部 201 上追加的功能。

[0204] 本实施方式的接收数据包处理部 201 在接收到数据包的情况下，在将报头信息发送给检索处理部 203 的同时，还向业务量统计分析处理部 901 发送报头信息。此外，接收数

据包处理部 201 将从业务量统计分析处理部 901 接收到的统计信息数据包发送给发送数据包处理部 202。接收数据包处理部 201 的其他动作和第 1 实施方式相同。

[0205] 本实施方式的控制部 208 将从业务量统计分析处理部 901 的流分析部 1003 接收到的、条目的种类为异常的信息发送给检索处理部 203。此外，接收到异常的信息的检索处理部 203 在流表 206 中检索是否存在相应的条目，在存在相应的条目的情况下，在流种类 326 中设定为异常流。

[0206] 发送数据包处理部 202、检索处理部 203 的其他动作和第 1 实施方式相同。

[0207] （第 3 实施方式）

[0208] 使用图 14 说明本发明的第 3 实施方式。

[0209] 本发明的第 3 实施方式在网络控制装置 1301 上安装对第 2 实施方式的业务量统计进行分析的功能。

[0210] 图 14 是本发明的第 3 实施方式的网络控制装置 1301 的功能框图。

[0211] 网络控制装置 1301 包括 CPU(Central Processing Unit：中央处理器)1302、网络存储器 1303、程序存储 1304、统计信息数据库 1305、通信接口（通信 I/F)1306 以及输入输出装置 1307。此外，这些分别通过总线 1308 连接。

[0212] 在程序存储器 1304 中存储数据包收发处理部 1311、统计信息数据包解析处理部 1312、业务量统计分析处理部 1313。CPU1302 将程序存储器 1304 中存储的各种程序等加载到网络存储器，并执行。

[0213] 数据包收发处理部 1311 收发 IP 数据包。统计信息数据包解析处理部 1312 取得从路由器 101 发送的数据包中包含的报头信息。业务量统计分析处理部 1313 执行与第 2 实施方式的业务量统计分析处理部 901 相同的处理。业务量统计分析处理部 1313 的不同点在于：第 2 实施方式的业务量统计分析处理部 901 将统计信息数据包生成部 1004 生成的数据包发送给接收数据包处理部 201，与此相对，本实施方式的业务量统计分析处理部 1313 将统计信息数据包生成部 1004 生成的数据包发送给数据包收发处理部 1311。

[0214] 统计信息数据库 1305 包括项目集表 902 及统计信息表 205。此外，通过业务量统计分析处理部 1313 参照统计信息数据库 1305。

[0215] 路由器 101 是与第 1 实施方式相同的结构。通过路由器 101 执行了采样处理之后的数据包的报头信息被发送到网络控制装置 1301 及采集装置 104。

[0216] 此外，也可以在通过路由器 101 的数据包数较少的情况下，复制数据包，将所复制的数据包发送给网络控制装置 1301。

[0217] 工业实用性

[0218] 本发明可以用于网络的运营管理。特别是在详细管理网络上流经的业务量的情况下及使用大规模网络的情况下很有效。

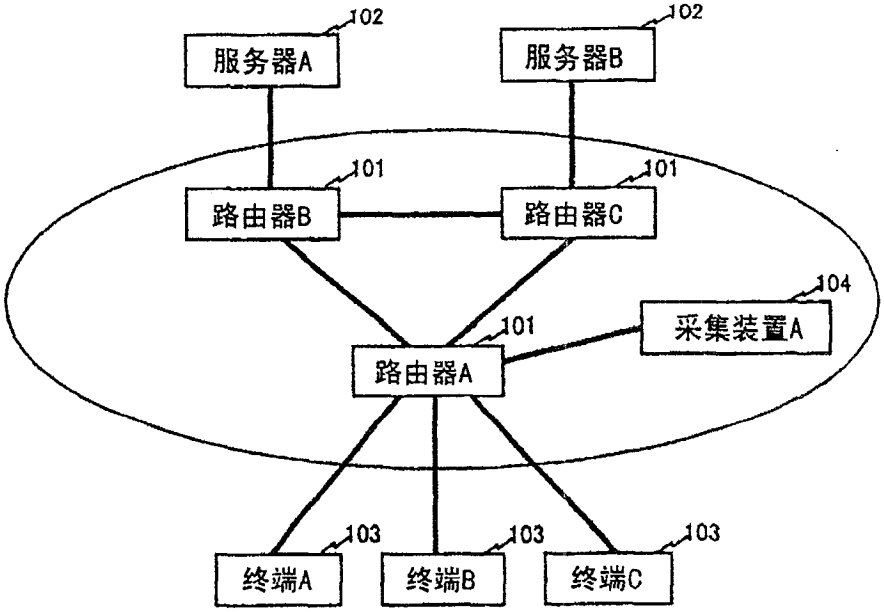

服务器A
服务器B
路由器B
路由器C
路由器A
采集装置A
终端A
终端B
终端C
102
102
101
101
101
104
103
103
103

图 1

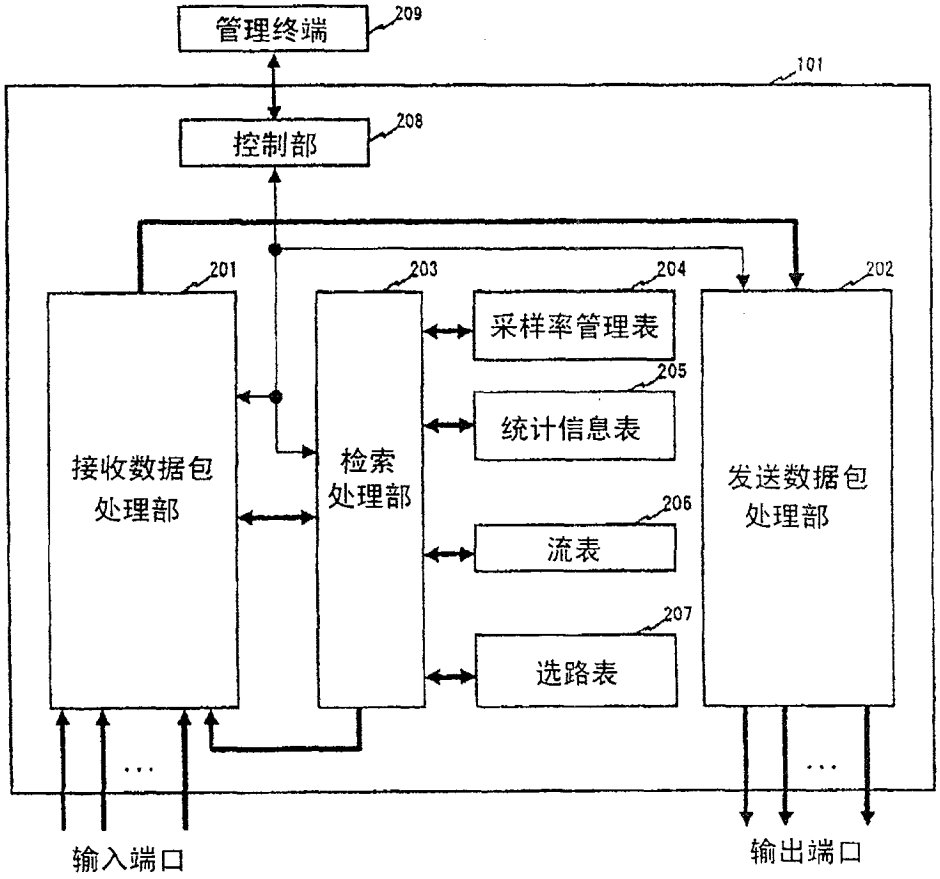

管理终端
209
101
控制部
208
201
203
204
202
采样率管理表
205
统计信息表
接收数据包
处理部
检索
处理部
发送数据包
处理部
206
流表
207
选路表
输入端口
输出端口

图 2

流表

流ID	流识别条件							统计控制信息							
	发送源IP地址	发送目的地IP地址	上层协议	发送源端口号	发送目的地端口号	其他信息		注册处理	注册处理率	统计收集	采样处理	发送控制	流种类	采样率	其他信息
F1	IP_S1	IP_D1	TCP	SPORT1	DPORT1	*		0	-	1	1	1	0	1/1,000	…
F2	IP_S2	IP_D2	TCP	SOPRT2	DPORT2	*		0	-	1	1	1	0	1/10,000	…
F12	*	*	TCP	*	*	*		1	1/1	1	1	1	0	1/1,000	…

301 302 303 206 311 312 313 314 315 316 321 322 323 324 325 326 327 328

图 3

统计信息表

流ID	统计信息						
	数据包数	字节数	频带 (bps)	频带 (pps)	开始时刻	阈值	其他信息
F1	P1	B1	25Mbps	30kpps	T1	Th1	…
F2	P2	B2	10Mbps	10kpps	T2	Th2	…
F12	-	-	-	-	-	-	…

301 401 205 411 412 413 414 415 416 417

图 4

采样率管理表

频带 (pps)	采样率		
	已分析的流（0）	未知流（1）	异常流（2）
Default	1/10,000	1/1,000	1/100
~100	1/10,000	1/1,000	1/10
101~1,000	1/10,000	1/1,000	1/100
1,001~10,000	1/100,000	1/10,000	1/1,000
10,001~100,000	1/1,000,000	1/100,000	1/10,000
100,001~1,000,000	1/10,000,000	1/1,000,000	1/100,000
1,000,001~10,000,000	1/100,000,000	1/10,000,000	1/1,000,000
10,000,001~100,000,000	1/1,000,000,000	1/100,000,000	1/10,000,000

501 502 204 511 512 513

图 5

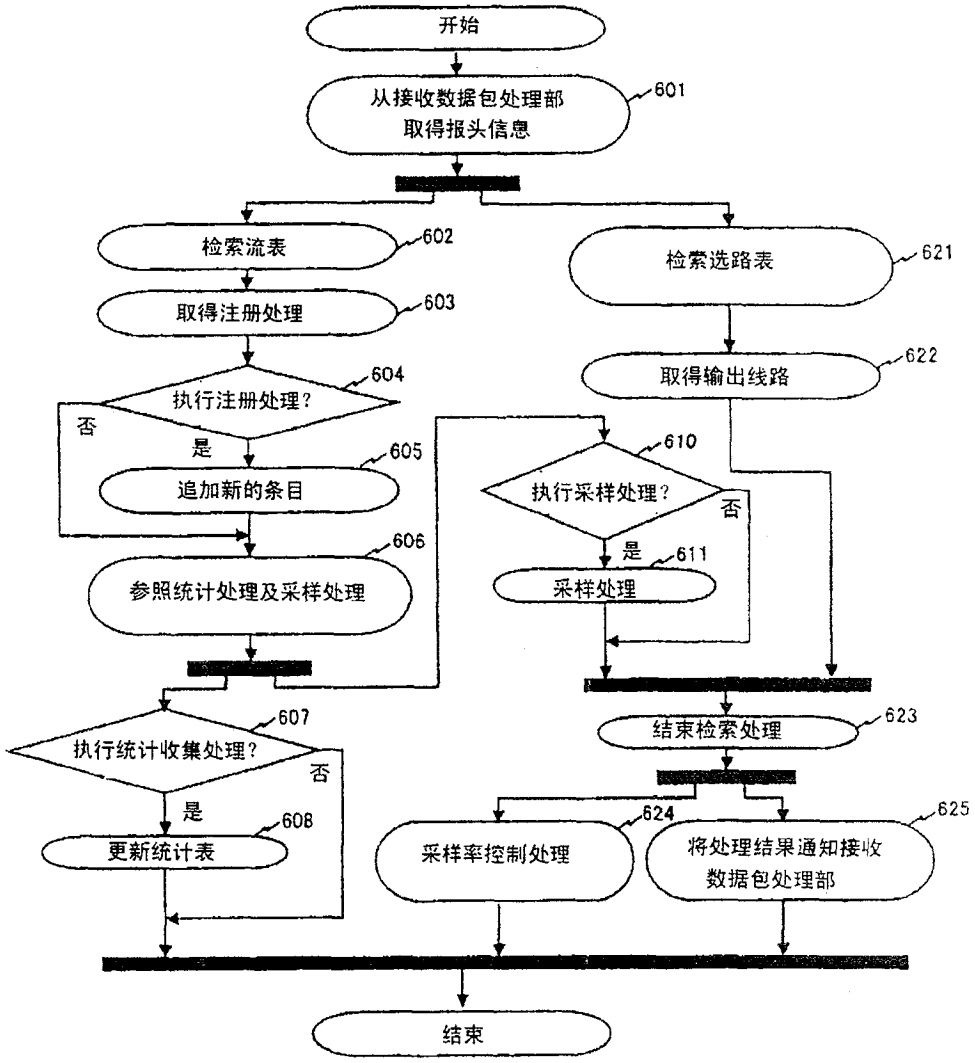

开始
从接收数据包处理部
取得报头信息
601
检索流表
602
取得注册处理
603
执行注册处理?
604
否
是
追加新的条目
605
参照统计处理及采样处理
606
执行统计收集处理?
607
否
是
更新统计表
608
检索选路表
621
取得输出线路
622
执行采样处理?
610
否
是
采样处理
611
结束检索处理
623
采样率控制处理
624
将处理结果通知接收
数据包处理部
625
结束

图 6

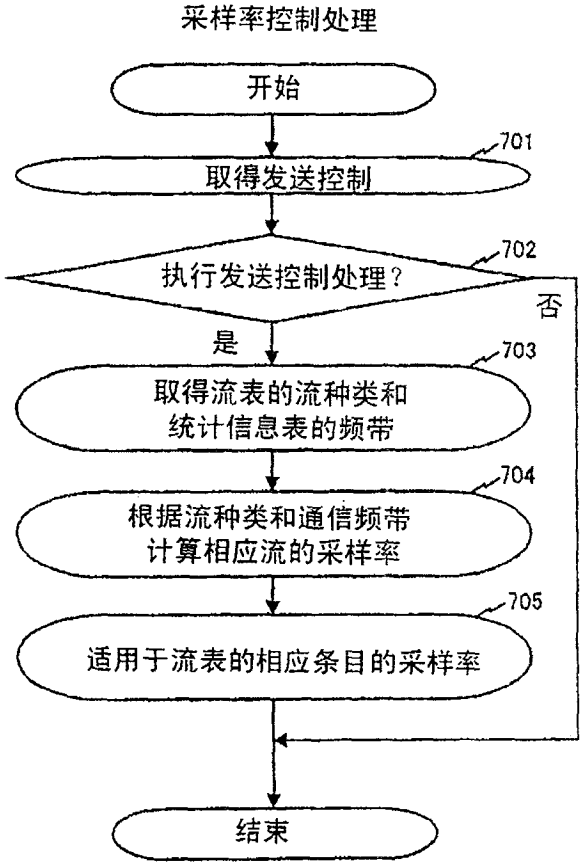

采样率控制处理
开始
701
取得发送控制
702
执行发送控制处理？
否
是
703
取得流表的流种类和
统计信息表的频带
704
根据流种类和通信频带
计算相应流的采样率
705
适用于流表的相应条目的采样率
结束

图 7

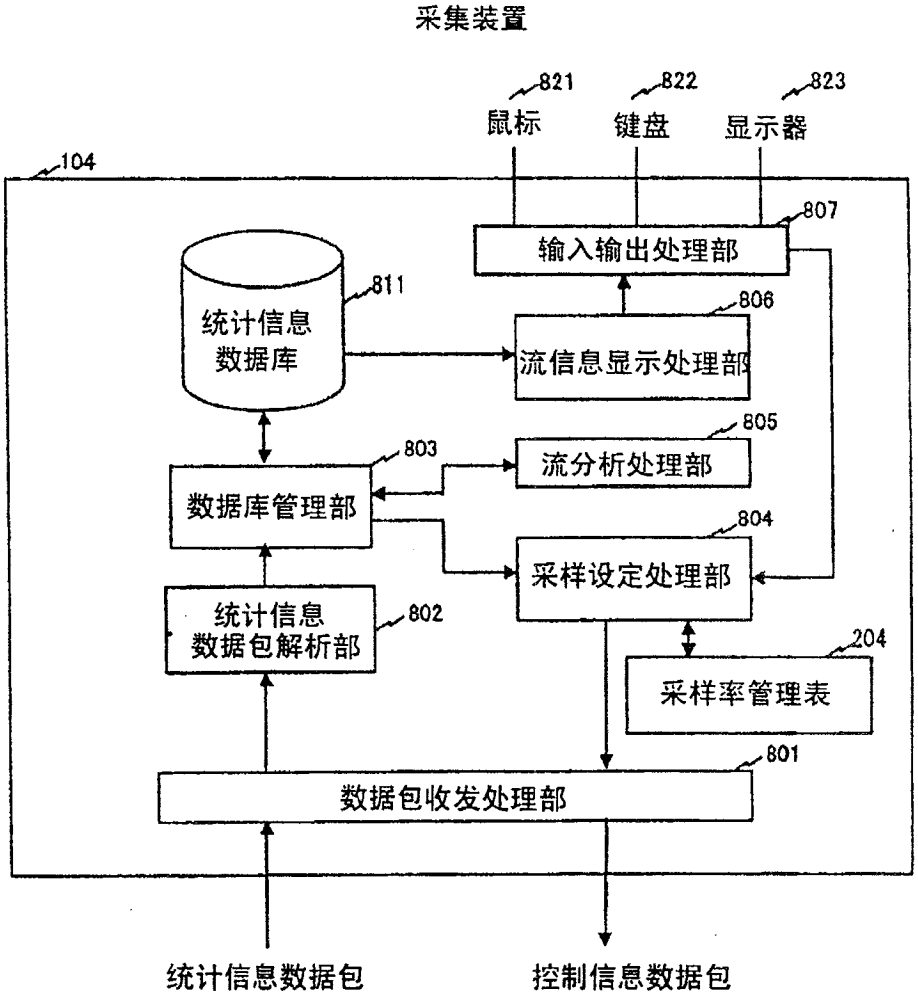

采集装置
821
鼠标
822
键盘
823
显示器
104
807
输入输出处理部
811
统计信息
数据库
806
流信息显示处理部
805
流分析处理部
803
数据库管理部
804
采样设定处理部
802
统计信息
数据包解析部
204
采样率管理表
801
数据包收发处理部
统计信息数据包
控制信息数据包

图 8

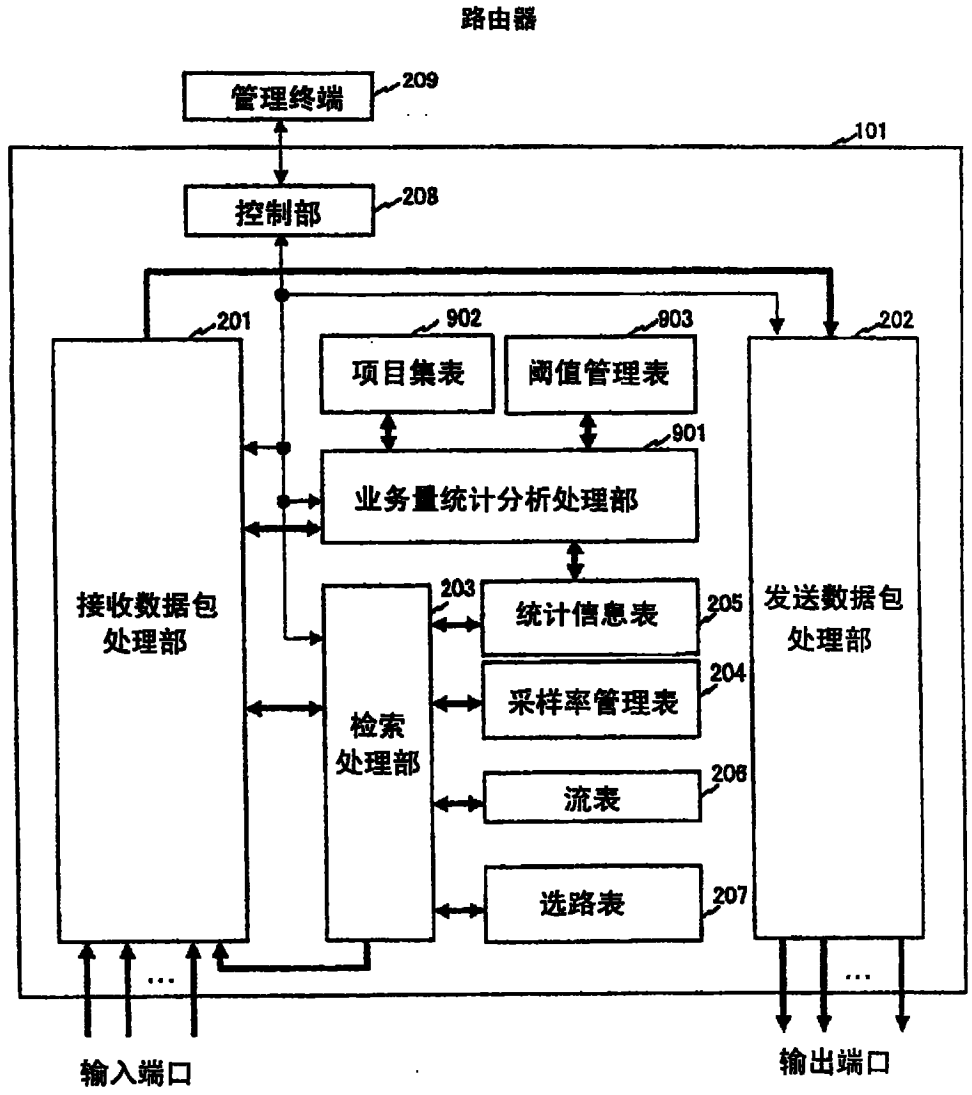

路由器
管理终端
209
101
控制部
208
201
902
903
202
项目集表
阈值管理表
901
业务量统计分析处理部
接收数据包
处理部
203
统计信息表
205
发送数据包
处理部
检索
处理部
采样率管理表
204
流表
206
选路表
207
...
...
输入端口
输出端口

图 9

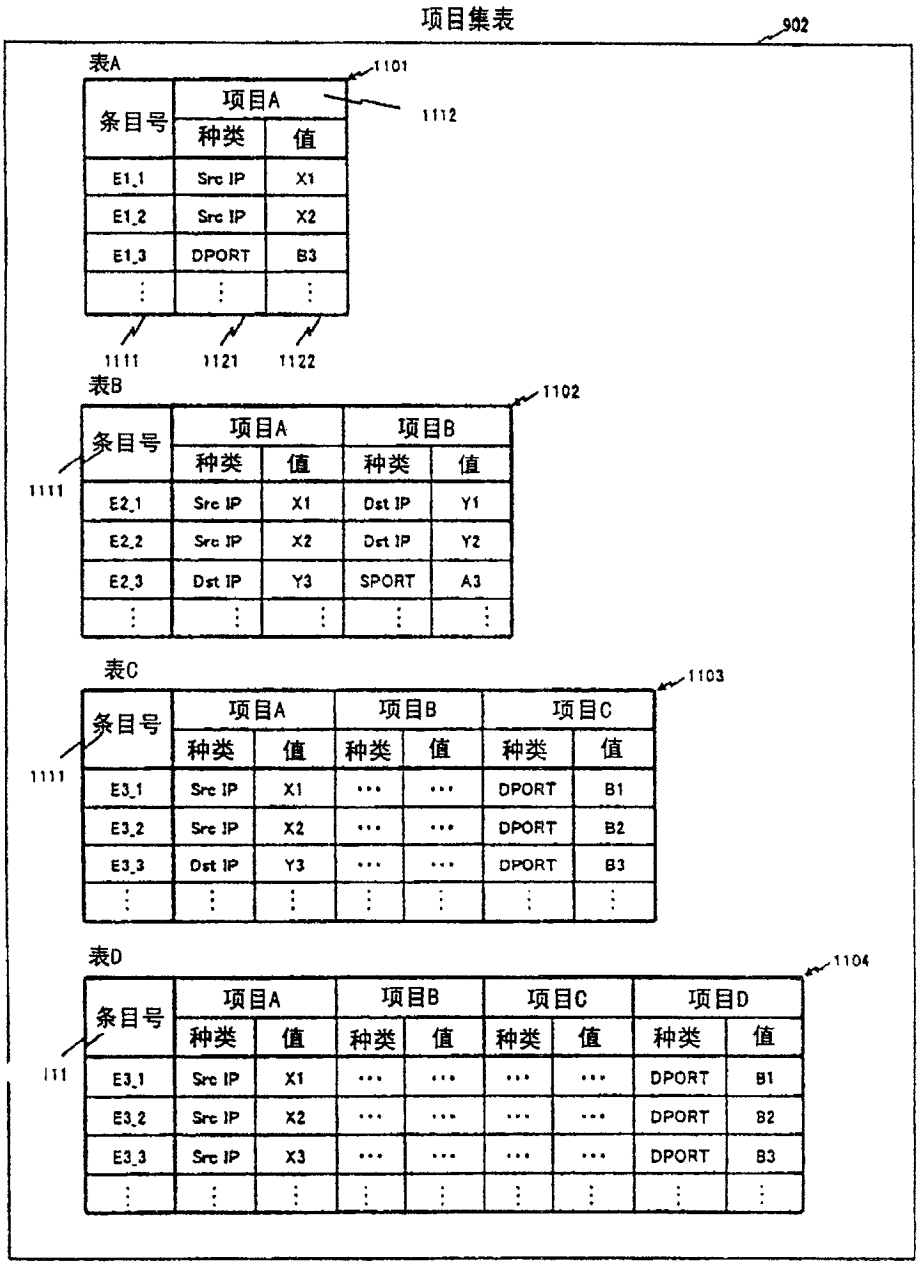

项目集表
902
表A
1101
1112
条目号
项目A
种类
值
E1_1 Src IP X1
E1_2 Src IP X2
E1_3 DPORT B3
1111
1121
1122
表B
1102
条目号
项目A
项目B
种类
值
种类
值
E2_1 Src IP X1 Dst IP Y1
E2_2 Src IP X2 Dst IP Y2
E2_3 Dst IP Y3 SPORT A3
1111
表C
1103
条目号
项目A
项目B
项目C
种类
值
种类
值
种类
值
E3_1 Src IP X1 ... ... DPORT B1
E3_2 Src IP X2 ... ... DPORT B2
E3_3 Dst IP Y3 ... ... DPORT B3
1111
表D
1104
条目号
项目A
项目B
项目C
项目D
种类
值
种类
值
种类
值
种类
值
E3_1 Src IP X1 ... ... DPORT B1
E3_2 Src IP X2 ... ... DPORT B2
E3_3 Src IP X3 ... ... DPORT B3
111

图 10

统计信息表

1111 条目号	1201 数据包数	1202 字节数	1203 频带（bps）	1204 频带（pps）	1205 开始时刻	1206 阈值	1207 其他信息
E1_1	P1_1	B1_1	BPS1_1	PPS1_1	t1_1	Th1_1	…
E1_2	P1_2	B1_2	BPS1_2	PPS1_2	t1_2	Th1_2	…
E1_3	P1_3	B1_3	BPS1_3	PPS1_3	t1_3	Th1_3	…
	⋮	⋮	⋮	⋮	⋮	⋮	⋮
E2_1	P2_1	B2_1	BPS2_1	PPS2_1	t2_1	Th2_1	…
E2_2	P2_2	B2_2	BPS2_2	PPS2_2	t2_2	Th2_2	…
E2_3	P2_3	B2_3	BPS2_3	PPS2_3	t2_3	Th2_3	…
	⋮	⋮	⋮	⋮	⋮	⋮	⋮
E3_1	P3_1	B3_1	BPS3_1	PPS3_1	t3_1	Th3_1	…
E3_2	P3_2	B3_2	BPS3_2	PPS3_2	t3_2	Th3_2	…
E3_3	P3_3	B3_3	BPS3_3	PPS3_3	t3_3	Th3_3	…
	⋮	⋮	⋮	⋮	⋮	⋮	⋮

205

图 11

阈值管理表

1401 频带 (PPS)	1402 阈值（比率）		903
	已分析的流（0）	未知流（1）	异常流（2）
Default	10	1	1/10
～100	10	1	1/100
101～1,000	10	1	1/10
1,001～10,000	100	10	1
10,001～100,000	1,000	100	10
100,001～1,000,000	10,000	1,000	100
1,000,001～10,000,000	100,000	10,000	1,000
10,000,001～100,000,000	1,000,000	100,000	10,000
	1411	1412	1413

图 12

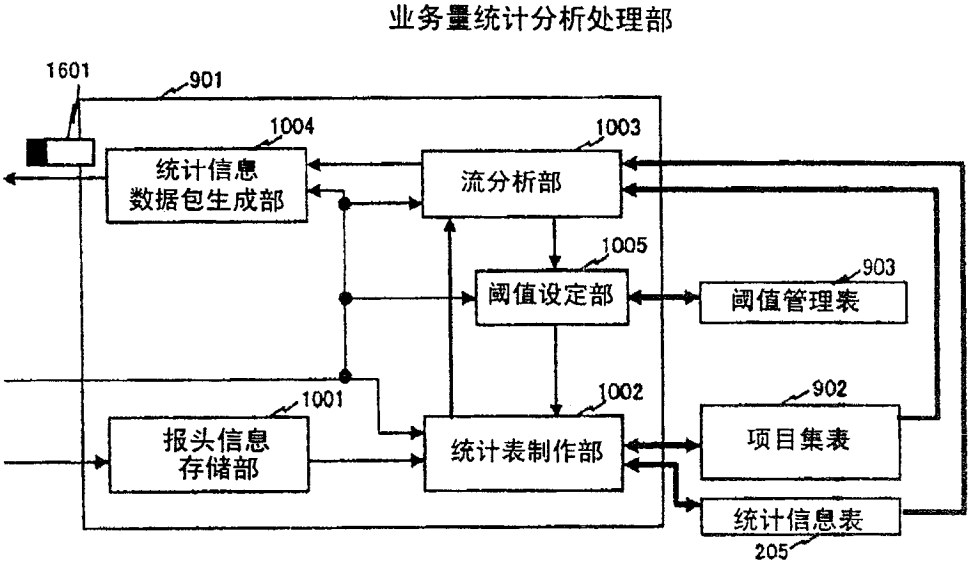

业务量统计分析处理部
1601
901
1004
统计信息
数据包生成部
1003
流分析部
1005
阈值设定部
903
阈值管理表
1001
报头信息
存储部
1002
统计表制作部
902
项目集表
统计信息表
205

图 13

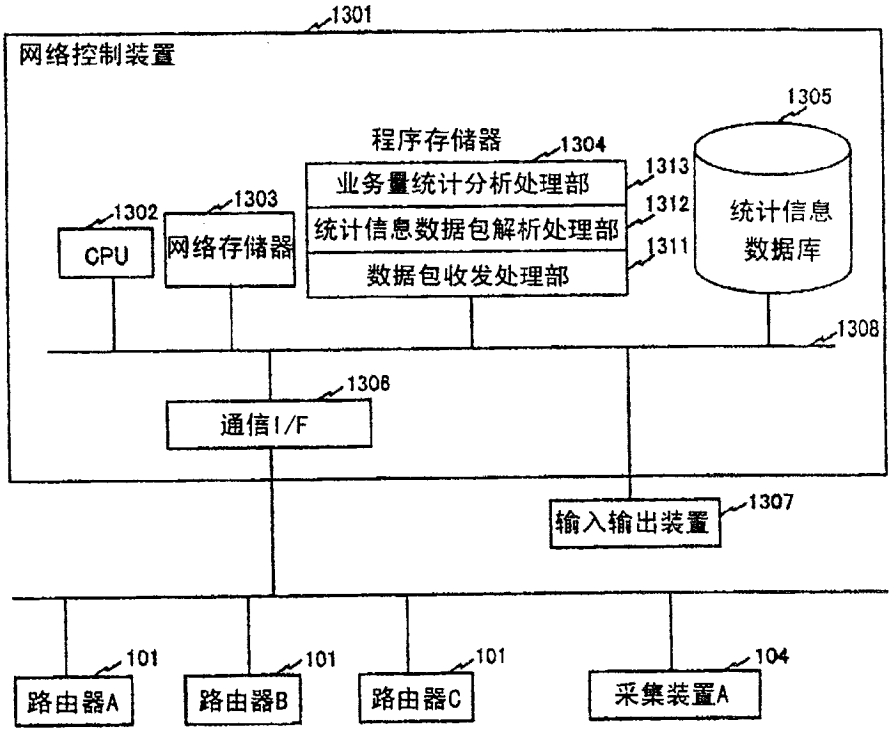

1301
网络控制装置
1305
程序存储器
1304
业务量统计分析处理部
1313
统计信息数据包解析处理部
1312
数据包收发处理部
1311
统计信息
数据库
1302
CPU
1303
网络存储器
1308
1306
通信I/F
1307
输入输出装置
101
路由器A
101
路由器B
101
路由器C
104
采集装置A

图 14

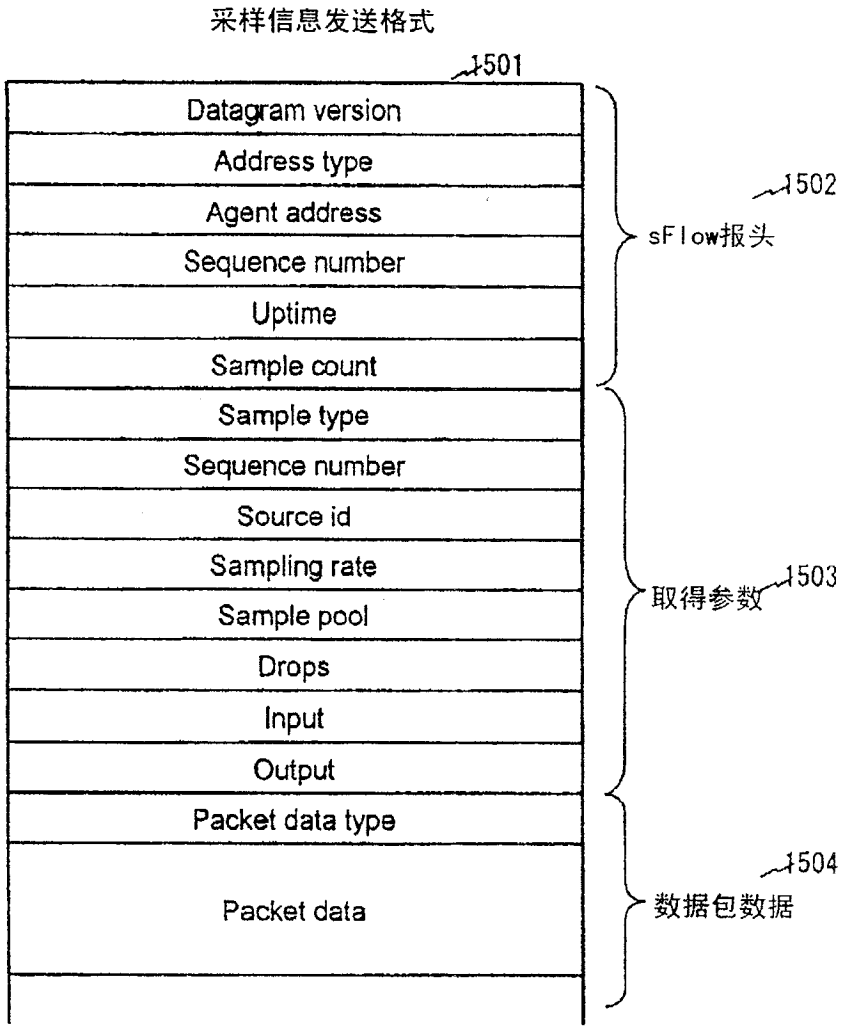

采样信息发送格式
1501
Datagram version
Address type
Agent address
Sequence number
Uptime
Sample count
Sample type
Sequence number
Source id
Sampling rate
Sample pool
Drops
Input
Output
Packet data type
Packet data
1502
sFlow报头
1503
取得参数
1504
数据包数据

图 15

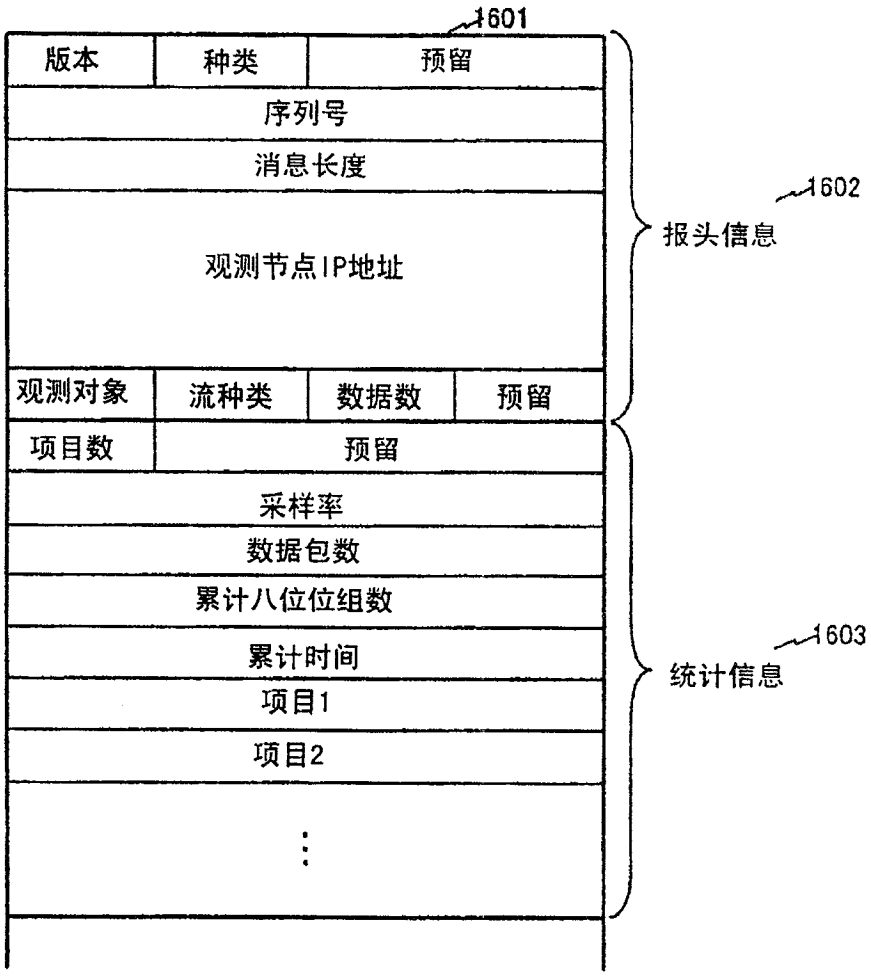

统计信息发送格式
1601
版本
种类
预留
序列号
消息长度
观测节点IP地址
观测对象
流种类
数据数
预留
项目数
预留
采样率
数据包数
累计八位位组数
累计时间
项目1
项目2
1602
报头信息
1603
统计信息

图 16