(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 108965061 A
(43)申请公布日 2018.12.07

(21)申请号 201810877530.2

(22)申请日 2018.08.03

(71)申请人 上海欣诺通信技术股份有限公司
地址 201620 上海市松江区文翔东路58号11幢

(72)发明人 万仁勇 周华 吴志远 谢虎 李琳

(74)专利代理机构 上海光华专利事务所(普通合伙) 31219
代理人 高彦

(51)Int.Cl.
H04L 12/26(2006.01)
H04L 12/46(2006.01)

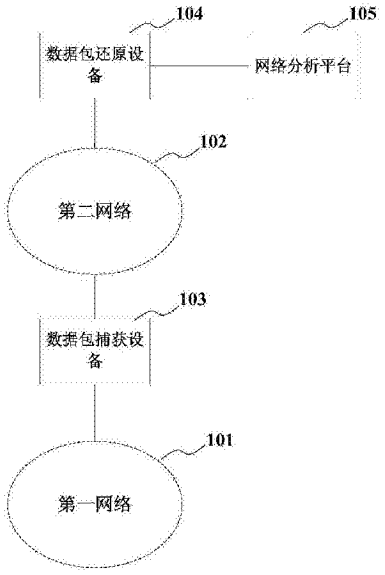
权利要求书3页 说明书8页 附图4页

(54)发明名称

数据包捕获设备及方法、还原设备及方法、系统和介质

(57)摘要

本发明的数据包捕获设备及方法、还原设备及方法、系统和介质，所述数据包捕获设备，包括：第一网络接口，通信连接第一网络；第二网络接口，通信连接第二网络，并用于通过所述第二网络通信连接数据包还原设备通信；数据处理电路，通信连接所述第一网络接口及第二网络接口，用于对从所述第一网络接口和/或第二网络接口捕获的原始网络数据包复制，且按预定格式封装所复制的原始网络数据包为封装数据包，并通过所述第二网络接口传送所述封装数据包至所述数据包还原设备，以供其还原为原始网络数据包；本发明实现利用轻量级数据包捕获设备将数据包发送远端集中分析处理，解决现有技术的问题。



CN 108965061 A

1.一种数据包捕获设备，其特征在于，包括：

第一网络接口，通信连接第一网络；

第二网络接口，通信连接第二网络，并用于通过所述第二网络通信连接数据包还原设备通信；

数据处理电路，通信连接所述第一网络接口及第二网络接口，用于对从所述第一网络接口和/或第二网络接口捕获的原始网络数据包复制，且按预定格式封装所复制的原始网络数据包为封装数据包，并通过所述第二网络接口传送所述封装数据包至所述数据包还原设备，以供其还原为原始网络数据包。

2.根据权利要求1所述的数据包捕获设备，其特征在于，还包括：线路切换单元，通信连接所述第一网络接口、第二网络接口及数据处理电路，用于切换第一网络接口与第二网络接口连通、或第一网络接口及第二网络接口同数据处理电路连通。

3.根据权利要求2所述的数据包捕获设备，其特征在于，所述线路切换单元包括控制端，用于在接收到表示所述数据包捕获设备处于正常工作状态的第一类型信号时，控制第一网络接口及第二网络接口同数据处理电路连通；或者，在接收到表示所述数据包捕获设备处于故障状态的第二类型信号时，控制第一网络接口与第二网络接口连通。

4.根据权利要求1所述的数据包捕获设备，其特征在于，所述第一网络及第二网络为互联网络；所述从所述第一网络接口和/或第二网络接口得到的原始网络数据包复制，且按预定格式封装所复制的原始网络数据包为封装数据包，包括：

若所述原始数据包接收自第一网络接口，则从对其复制得到的复制数据包中提取源MAC地址、目地MAC地址及源IP地址；

将所提取源MAC地址作为封装数据包的源MAC地址，将所提取目的MAC地址作为封装数据包的目的MAC地址，将所提取源IP地址作为封装数据包的源IP地址，将封装数据包的目的IP地址设为所述数据包还原设备的IP地址，将封装数据包的UDP目的端口设为指定的所述网络还源设备监听使用的端口，并将原始数据包装载于所述封装数据包的净荷中，而构造形成所述封装数据包。

5.根据权利要求1或4所述的数据包捕获设备，其特征在于，所述第一网络及第二网络为互联网络；所述从所述第一网络接口和/或第二网络接口得到的原始网络数据包复制，且按预定格式封装所复制的原始网络数据包为封装数据包，包括：

若所述原始数据包接收自第二网络接口，则从对其复制得到的复制数据包中提取源MAC地址、目地MAC地址及目的IP地址；

将所提取源MAC地址作为封装数据包的目的MAC地址，将所提取目的MAC地址作为封装数据包的源MAC地址，将所提取目的IP地址作为封装数据包的源IP地址，将封装数据包的目的IP地址设为所述数据包还原设备的IP地址，UDP目的端口使用指定的所述网络还源设备监听使用的端口，并将原始数据包装载于所述封装数据包的净荷中，而构造形成所述封装数据包。

6.根据权利要求1所述的数据包捕获设备，其特征在于，所述第一网络接口通信连接所述第一网络出口的网关设备。

7.一种数据包还原设备，其特征在于，通信连接第二网络并通过所述第二网络通信连接于数据包捕获设备，且通信连接于网络分析平台；所述数据包捕获设备还通信连接第一

网络，所述数据包还原设备包括：

第一网络接口，通信连接所述数据包捕获设备，以得到其发来的封装有捕获自第一网络或第二网络的原始数据包的封装数据包；

第二网络接口，通信连接所述网络分析平台；

数据处理电路，通信连接所述第一网络接口及第二网络接口，用于还原所述封装数据包以得到原始数据包，并通过所述第二网络接口发送到所述网络分析平台。

8.一种网络分析系统，其特征在于，包括：

一或多个如权利要求1至6中任一项所述的数据包捕获设备；每个数据包捕获设备通信连接于至少一第一网络并连接于一第二网络，用于生成所述封装数据包并通过所述第二网络发送；

如权利要求7所述的数据包还原设备，通过第二网络通信连接所述一或多个数据包捕获设备，用于接收所述封装数据包并还原得到原始数据包，并对外发送；

网络分析平台，通信连接于所述数据包还原设备，用于接收所述还原得到的原始数据包以并据以进行网络分析。

9.一种数据包捕获方法，其特征在于，包括：

对从连接于第一网络的第一网络接口和/或连接于第二网络的第二网络接口捕获的原始网络数据包复制，且按预定格式封装所复制的原始网络数据包为封装数据包；其中，所述第二网络接口通过所述第二网络通信连接数据包还原设备通信；

通过所述第二网络接口传送所述封装数据包至至数据包还原设备，以供其还原为原始网络数据包。

10.根据权利要求9所述的数据包捕获方法，其特征在于，所述对从连接于第一网络的第一网络接口和/或连接于第二网络的第二网络接口捕获的原始网络数据包复制，且按预定格式封装所复制的原始网络数据包为封装数据包，包括：

若所述原始数据包接收自第一网络接口，则从对其复制得到的复制数据包中提取源MAC地址、目地MAC地址及源IP地址；

将所提取源MAC地址作为封装数据包的源MAC地址，将所提取目的MAC地址作为封装数据包的目的MAC地址，将所提取源IP地址作为封装数据包的源IP地址，将封装数据包的目的IP地址设为所述数据包还原设备的IP地址，将封装数据包的UDP目的端口设为指定的所述网络还源设备监听使用的端口，并将原始数据包装载于所述封装数据包的净荷中，而构造形成所述封装数据包。

11.根据权利要求9或10所述的数据包捕获方法，其特征在于，所述第一网络及第二网络为互联网络；对从连接于第一网络的第一网络接口和/或连接于第二网络的第二网络接口捕获的原始网络数据包复制，且按预定格式封装所复制的原始网络数据包为封装数据包，包括：

若所述原始数据包接收自第二网络接口，则从对其复制得到的复制数据包中提取源MAC地址、目地MAC地址及目的IP地址；

将所提取源MAC地址作为封装数据包的目的MAC地址，将所提取目的MAC地址作为封装数据包的源MAC地址，将所提取目的IP地址作为封装数据包的源IP地址，将封装数据包的目的IP地址设为所述数据包还原设备的IP地址，UDP目的端口使用指定的所述网络还源设备

监听使用的端口，并将原始数据包装载于所述封装数据包的净荷中，而构造形成所述封装数据包。

12.一种网络数据包还原方法，其特征在于，包括：

通过第二网络接收来自数据包捕获设备的封装有捕获自第一网络或第二网络的原始数据包的封装数据包；

还原所述封装数据包以得到原始数据包并发送到网络分析平台。

13.一种计算机存储介质，其特征在于，存储有计算机程序，所述计算机程序运行时执行如权利要求8至11中任一项所述的数据包捕获方法，或执行如权利要求12所述的网络数据包还原方法。

数据包捕获设备及方法、还原设备及方法、系统和介质

技术领域

[0001] 本发明涉及网络技术领域，尤其涉及数据包捕获设备及方法、还原设备及方法、系统和介质。

背景技术

[0002] 随着互联网的普及，上网的信息量越大越大，因此各种网络安全，网络流量分析，网络审计等平台(以下统称为网络分析平台)被大规模部署应用。这些平台实现的必不可少的一个手段就是对网络数据包捕获，捕获网络数据包的通用方法就是对网络数据镜像。

[0003] 传统镜像数据包设备都是在网络本地部署，网络析平台与网络镜像设备连接也是在部署在本地。如果网络比较分散，网络分析平台部署数量也会随之增加，另外每个网络分析平台的数据都是比较独立的，很难做到关联分析，以致于网络分析的数据准确度不高。

发明内容

[0004] 鉴于以上所述现有技术的缺点，本发明的目的在于提供数据包捕获设备及方法、还原设备及方法、系统和介质，解决现有技术中网络分析平台部署数量大、分散的问题。

[0005] 为实现上述目标及其他相关目标，本发明提供一种数据包捕获设备，包括：第一网络接口，通信连接第一网络；第二网络接口，通信连接第二网络，并用于通过所述第二网络通信连接数据包还原设备通信；数据处理电路，通信连接所述第一网络接口及第二网络接口，用于对从所述第一网络接口和/或第二网络接口捕获的原始网络数据包复制，且按预定格式封装所复制的原始网络数据包为封装数据包，并通过所述第二网络接口传送所述封装数据包至所述数据包还原设备，以供其还原为原始网络数据包。

[0006] 于本发明的一实施例中，所述的数据包捕获设备还包括：线路切换单元，通信连接所述第一网络接口、第二网络接口及数据处理电路，用于切换第一网络接口与第二网络接口连通、或第一网络接口及第二网络接口同数据处理电路连通。

[0007] 于本发明的一实施例中，所述线路切换单元包括控制端，用于在接收到表示所述数据包捕获设备处于正常工作状态的第一类型信号时，控制第一网络接口及第二网络接口同数据处理电路连通；或者，在接收到表示所述数据包捕获设备处于故障状态的第二类型信号时，控制第一网络接口与第二网络接口连通。

[0008] 于本发明的一实施例中，所述第一网络及第二网络为互联网络；所述从所述第一网络接口和/或第二网络接口得到的原始网络数据包复制，且按预定格式封装所复制的原始网络数据包为封装数据包，包括：若所述原始数据包接收自第一网络接口，则从对其复制得到的复制数据包中提取源MAC地址、目地MAC地址及源IP地址；将所提取源MAC地址作为封装数据包的源MAC地址，将所提取目的MAC地址作为封装数据包的目的MAC地址，将所提取源IP地址作为封装数据包的源IP地址，将封装数据包的目的IP地址设为所述数据包还原设备的IP地址，将封装数据包的UDP目的端口设为指定的所述网络还源设备监听使用的端口，并将原始数据包装载于所述封装数据包的净荷中，而构造形成所述封装数据包。

[0009] 于本发明的一实施例中，所述第一网络及第二网络为互联网络；所述从所述第一网络接口和/或第二网络接口得到的原始网络数据包复制，且按预定格式封装所复制的原始网络数据包为封装数据包，包括：若所述原始数据包接收自第二网络接口，则从对其复制得到的复制数据包中提取源MAC地址、目地MAC地址及目的IP地址；将所提取源MAC地址作为封装数据包的目的MAC地址，将所提取目的MAC地址作为封装数据包的源MAC地址，将所提取目的IP地址作为封装数据包的源IP地址，将封装数据包的目的IP地址设为所述数据包还原设备的IP地址，UDP目的端口使用指定的所述网络还源设备监听使用的端口，并将原始数据包装载于所述封装数据包的净荷中，而构造形成所述封装数据包。

[0010] 于本发明的一实施例中，所述第一网络接口通信连接所述第一网络出口的网关设备。

[0011] 为实现上述目标及其他相关目标，本发明提供一种数据包还原设备，通信连接第二网络并通过所述第二网络通信连接于数据包捕获设备，且通信连接于网络分析平台；所述数据包捕获设备还通信连接第一网络，所述数据包还原设备包括：第一网络接口，通信连接所述数据包捕获设备，以得到其发来的封装有捕获自第一网络或第二网络的原始数据包的封装数据包；第二网络接口，通信连接所述网络分析平台；数据处理电路，通信连接所述第一网络接口及第二网络接口，用于还原所述封装数据包以得到原始数据包，并通过所述第二网络接口发送到所述网络分析平台。

[0012] 为实现上述目标及其他相关目标，本发明提供一种网络分析系统，包括：所述的数据包捕获设备；每个数据包捕获设备通信连接于至少一第一网络并连接于一第二网络，用于生成所述封装数据包并通过所述第二网络发送；所述的数据包还原设备，通过第二网络通信连接所述一或多个数据包捕获设备，用于接收所述封装数据包并还原得到原始数据包，并对外发送；网络分析平台，通信连接于所述数据包还原设备，用于接收所述还原得到的原始数据包以并据以进行网络分析。

[0013] 为实现上述目标及其他相关目标，本发明提供一种数据包捕获方法，包括：对从连接于第一网络的第一网络接口和/或连接于第二网络的第二网络接口捕获的原始网络数据包复制，且按预定格式封装所复制的原始网络数据包为封装数据包；其中，所述第二网络接口通过所述第二网络通信连接数据包还原设备通信；通过所述第二网络接口传送所述封装数据包至至数据包还原设备，以供其还原为原始网络数据包。

[0014] 于本发明的一实施例中，所述对从连接于第一网络的第一网络接口和/或连接于第二网络的第二网络接口捕获的原始网络数据包复制，且按预定格式封装所复制的原始网络数据包为封装数据包，包括：若所述原始数据包接收自第一网络接口，则从对其复制得到的复制数据包中提取源MAC地址、目地MAC地址及源IP地址；将所提取源MAC地址作为封装数据包的源MAC地址，将所提取目的MAC地址作为封装数据包的目的MAC地址，将所提取源IP地址作为封装数据包的源IP地址，将封装数据包的目的IP地址设为所述数据包还原设备的IP地址，将封装数据包的UDP目的端口设为指定的所述网络还源设备监听使用的端口，并将原始数据包装载于所述封装数据包的净荷中，而构造形成所述封装数据包。

[0015] 于本发明的一实施例中，所述第一网络及第二网络为互联网络；对从连接于第一网络的第一网络接口和/或连接于第二网络的第二网络接口捕获的原始网络数据包复制，且按预定格式封装所复制的原始网络数据包为封装数据包，包括：若所述原始数据包接收

自第二网络接口，则从对其复制得到的复制数据包中提取源MAC地址、目地MAC地址及目的IP地址；将所提取源MAC地址作为封装数据包的目的MAC地址，将所提取目的MAC地址作为封装数据包的源MAC地址，将所提取目的IP地址作为封装数据包的源IP地址，将封装数据包的目的IP地址设为所述数据包还原设备的IP地址，UDP目的端口使用指定的所述网络还源设备监听使用的端口，并将原始数据包装载于所述封装数据包的净荷中，而构造形成所述封装数据包。

[0016] 为实现上述目标及其他相关目标，本发明提供一种网络数据包还原方法，包括：通过第二网络接收来自数据包捕获设备的封装有捕获自第一网络或第二网络的原始数据包的封装数据包；还原所述封装数据包以得到原始数据包并发送到网络分析平台。

[0017] 为实现上述目标及其他相关目标，本发明提供一种计算机存储介质，存储有计算机程序，所述计算机程序运行时执行所述的数据包捕获方法，或执行所述的网络数据包还原方法。

[0018] 如上所述，本发明的数据包捕获设备及方法、还原设备及方法、系统和介质，所述数据包捕获设备，包括：第一网络接口，通信连接第一网络；第二网络接口，通信连接第二网络，并用于通过所述第二网络通信连接数据包还原设备通信；数据处理电路，通信连接所述第一网络接口及第二网络接口，用于对从所述第一网络接口和/或第二网络接口捕获的原始网络数据包复制，且按预定格式封装所复制的原始网络数据包为封装数据包，并通过所述第二网络接口传送所述封装数据包至所述数据包还原设备，以供其还原为原始网络数据包；本发明实现利用轻量级数据包捕获设备将数据包发送远端集中分析处理，解决现有技术的问题。

附图说明

[0019] 图1显示为本发明实施例中网络分析系统的结构示意图。

[0020] 图2A显示为本发明一实施例中数据包捕获设备的结构示意图。

[0021] 图2B显示为本发明又一实施例中数据包捕获设备的结构示意图。

[0022] 图3显示为本发明实施例中数据包还原设备的结构示意图。

[0023] 图4显示为本发明实施例中一种封装数据包的结构示意图。

[0024] 图5显示为本发明实施例中另一种封装数据包的结构示意图。

[0025] 图6显示为本发明实施例中数据包捕获方法的流程示意图。

[0026] 图7显示为本发明实施例中数据包还原方法的流程示意图。

[0027] 图8显示为本发明实施例中处理装置的结构示意图。

具体实施方式

[0028] 以下通过特定的具体实例说明本发明的实施方式，本领域技术人员可由本说明书所揭露的内容轻易地了解本发明的其他优点与功效。本发明还可以通过另外不同的具体实施方式加以实施或应用，本说明书中的各项细节也可以基于不同观点与应用，在没有背离本发明的精神下进行各种修饰或改变。需说明的是，在不冲突的情况下，本申请中的实施例及实施例中的特征可以相互组合。

[0029] 本发明的技术方案应用于网络技术领域，所述网络可以是互联网，可分为局域网

(Local Area Network,LAN)、广域网(Wide Area Network,WAN)和城域网(Metropolitan Area Network,MAN)等。

[0030] 如图1所示,展示本发明实施例中网络分析系统的结构示意图。

[0031] 如图所示,所述网络分析系统应用于具有第一网络101及第二网络102的环境中,所述第一网络101和第二网络102可以是基于TCP/IP协议的互联网络。

[0032] 所述网络分析系统包括:数据包捕获设备103、数据包还原设备104及网络分析平台105。

[0033] 所述数据包捕获设备103通信连接所述第一网络101及第二网络102,其可用于捕获来自第一网络101及第二网络102的原始数据包,镜像复制该原始数据包得到复制的原始数据包,将原始数据包按其原先路径继续转发,将复制的原始数据包按预定格式封装为封装数据包后,通过第二网络102发送到数据还原设备。

[0034] 具体的,所述数据包捕获设备103可以通过通信连接于第一网络101出口的网关设备来接入第一网络101,所述网关设备例如为交换机或路由器等。

[0035] 所述数据还原设备,用于对接收到的封装数据包加以还原得到原始数据包,发送给所述网络分析平台105进行分析。

[0036] 在本发明的一或多个实施例中,所述数据包捕获设备103可以有多个,每个数据包捕获设备103对应监控一第一网络101,且通过第二网络102集中发送到所述数据包还原设备104并进一步集中到所述网络分析平台105进行分析。

[0037] 由此,本发明可以实现通过集中部署少量的网络分析平台105,每个网络分析平台105可以一对多地对所需监控的多个网络进行远程监控及集中分析,有效提升效率。

[0038] 在实际场景的一或多个实施例中,本发明的该网络分析系统可以应用于网络安全监控领域,举例来说,公安系统的网络取证,传统的取证方式都是如背景技术所述将网络取证平台部署在本地网络,由于取证的隐蔽密性以及网络取证平台的数据的保密性,在本地部署有可能会造成取证暴露以及数据的泄密隐患。

[0039] 而采用本发明的网络分析系统的方案,网络分析平台105作为网络取证平台可以在远程部署,而本地的数据包捕获设备103是不存放数据的,由此可以保证取证数据安全;并且,如上分析所述,本发明的该网络分析系统应用于公安系统的网络取证可以减少网络取证平台的部署,且实现多点取证,且对多点取证数据集中进行关联分析。

[0040] 在实际场景的一或多个实施例中,本发明的该网络分析系统还可以应用于机构总部(例如企、事业单位等)对其分支机构的上网行为监管,对企业上网流量的分析等。

[0041] 如图2A所示,展示本发明实施例中所述数据包捕获设备200的结构示意图。本实施例中的数据包捕获设备200可以用于实现图1实施例中的数据包捕获设备200。

[0042] 所述数据包捕获设备200,包括:第一网络接口201、第二网络接口202及数据处理电路203。

[0043] 所述第一网络接口201,通信连接第一网络。于本发明的一实施例中,所述第一网络接口201通信连接于第一网络出口的网关设备来接入第一网络,所述网关设备例如为交换机或路由器等。

[0044] 所述第二网络接口202,通信连接第二网络,并用于通过所述第二网络通信连接数据包还原设备通信。

[0045] 所述数据处理电路203，通信连接所述第一网络接口201及第二网络接口202，用于对从所述第一网络接口201和/或第二网络接口202捕获的原始网络数据包复制，且按预定格式封装所复制的原始网络数据包为封装数据包，并通过所述第二网络接口202传送所述封装数据包至所述数据包还原设备，以供其还原为原始网络数据包。

[0046] 于本发明的一实施例中，如图2B所示，可选的，数据包捕获设备200a还包括：线路切换单元204，通信连接所述第一网络接口201、第二网络接口202及数据处理电路203，用于切换第一网络接口201与第二网络接口202连通、或第一网络接口201及第二网络接口202同数据处理电路203连通。

[0047] 于本发明的一实施例中，所述线路切换单元204包括控制端，用于在接收到表示所述数据包捕获设备200处于正常工作状态的第一类型信号时，控制第一网络接口201及第二网络接口202同数据处理电路203连通；或者，在接收到表示所述数据包捕获设备200处于故障状态的第二类型信号时，控制第一网络接口201与第二网络接口202连通。

[0048] 具体的，所述线路切换单元204用于在所述数据包捕获设备200能正常工作时，令第一网络接口201及第二网络接口202与数据处理电路203通信，所述数据处理电路203能执行上述接收原始数据包、镜像复制原始数据包、封装数据包并发送网络还原设备等功能，例如将从第一网络接口201接收的原始数据包通过第二网络接口202转发，并复制该原始数据包进行封装得到封装数据包，再将封装数据包通过该第二网络接口202发送到数据包还原设备，或者，也可以从第二网络接口202接收来自第二网络侧的原始数据包，并通过第一网络接口201转发到第一网络侧的通信设备；而当所述数据包捕获设备200出现故障时，所述线路切换单元204则切换至令第一网络接口201与第二网络接口202直接连通，不会影响原始数据包的传送。

[0049] 于本发明的一实施例中，所述第一网络及第二网络为互联网络，遵循TCP/IP协议。

[0050] 于本发明的一实施例中，所述封装数据包可以是基于UDP协议所定义的UDP格式的数据包。

[0051] 按所述数据包捕获设备200或200a来讲，有两种传送数据包的方式，一种是从第一网络接口201把数据包传送到第二网络接口202，另一种是从第二网络接口202把数据包传送到第一网络接口201，也就是分别对应上行、下行中的一者及另外一者；因此，所述数据包捕获设备200或200a的封装方式按原始数据包来自第一网络接口201或第二网络接口202而不同。

[0052] 所述数据处理电路203，若发现所接收到的原始数据包接收自第一网络接口201，则从对其复制得到的复制数据包中提取源MAC地址、目地MAC地址及源IP地址；将所提取源MAC地址作为封装数据包的源MAC地址，将所提取目的MAC地址作为封装数据包的目的MAC地址，将所提取源IP地址作为封装数据包的源IP地址，将封装数据包的目的IP地址设为所述数据包还原设备的IP地址，将封装数据包的UDP目的端口设为指定的所述网络还源设备监听使用的端口，并将原始数据包装载于所述封装数据包的净荷中，而构造形成所述封装数据包。

[0053] 如图3所示，展示了根据来自第一网络接口的原始数据包得到的封装数据包的结构。

[0054] 在图中所展示的原始数据包的结构中，A字段存储原始数据包的目的MAC地址，B字

段存储原始数据包的源MAC地址，C字段存储原始数据包的目的IP地址，D字段存储原始数据包的源IP地址，E存储原始数据包的IP净荷数据。

[0055] 而在封装数据包1中，F字段存储封装数据包的新目的MAC地址(即原始数据包的目的MAC地址)，G字段存储封装数据包的新源MAC地址(即原始数据包的源MAC地址)，H字段存储封装数据包的新目的IP地址(即数据包还原设备的IP地址)，I字段存储封装数据包的新源IP地址(即原始数据包的源IP地址)，J字段存储封装数据包的新目的UDP端口号(即为指定的所述网络还源设备监听使用的端口)，K字段存储封装数据包的新源UDP端口号。

[0056] 另外，所述数据处理电路，若所述原始数据包接收自第二网络接口，则从对其复制得到的复制数据包中提取源MAC地址、目地MAC地址及目的IP地址；将所提取源MAC地址作为封装数据包的目的MAC地址，将所提取目的MAC地址作为封装数据包的源MAC地址，将所提取目的IP地址作为封装数据包的源IP地址，将封装数据包的目的IP地址设为所述数据包还原设备的IP地址，UDP目的端口使用指定的所述网络还源设备监听使用的端口，并将原始数据包装载于所述封装数据包的净荷(例如UDP净荷)中，而构造形成所述封装数据包。

[0057] 如图4所示，展示了根据来自第二网络接口的原始数据包得到的封装数据包的结构。

[0058] 在图中所展示的原始数据包的结构中，A字段存储原始数据包的目的MAC地址，B字段存储原始数据包的源MAC地址，C字段存储原始数据包的目的IP地址，D字段存储原始数据包的源IP地址，E存储原始数据包的IP净荷数据。

[0059] 而在封装数据包2中，F1字段存储封装数据包的新目的MAC地址(即原始数据包的源MAC地址)，G字段存储封装数据包的新源MAC地址(即原始数据包的目的MAC地址)，H1字段存储封装数据包的新目的IP地址(即数据包还原设备的IP地址)，I1字段存储封装数据包的新源IP地址(即原始数据包的目的IP地址)，J1字段存储封装数据包的新目的UDP端口号(即为指定的所述网络还源设备监听使用的端口)，K1字段存储封装数据包的新源UDP端口号。

[0060] 从上述可知，所述数据包捕获设备200或200a是复制原始数据并借用原始数据包中的IP地址和MAC地址并封装数据包传到远端，数据包捕获设备200或200a本身不需要配置IP地址，它是复制且不会改变原始数据包的传输路径，基本上可以做到即插即用，零配置，特别符合网络监控隐蔽性的特点。

[0061] 并且，本发明的数据包捕获设备200或200a可以有多个，分别对应不同的第一网络，因此，不会受到网络限制。

[0062] 如图5所示，展示本发明实施例中的数据包还原设备500的结构示意图。本实施例中的数据包还原设备500可用于实现图1实施例中的数据包还原设备500。

[0063] 所述数据包还原设备500包括：第一网络接口501、第二网络接口502及数据处理电路503。

[0064] 所述第一网络接口501，通信连接所述数据包捕获设备，以得到其发来的封装有捕获自第一网络或第二网络的原始数据包的封装数据包。即例如图3或图4结构的封装数据包。

[0065] 所述第二网络接口502，通信连接网络分析平台。

[0066] 所述数据处理电路503，通信连接所述第一网络接口501及第二网络接口502，用于还原所述封装数据包以得到原始数据包，并通过所述第二网络接口502发送到所述网络分

析平台。

[0067] 于本发明的一实施例中，所述还原即去除图3或图4结构的封装数据包的封装，而从净荷中提取出原始数据包，发送给所述网络分析平台进行分析。

[0068] 如图6所示，展示本发明提供的数据包捕获方法的流程示意图。所述数据包捕获方法可以应用于前述实施例中的数据包捕获设备。

[0069] 所述数据包捕获方法包括：

[0070] 步骤S601：对从连接于第一网络的第一网络接口和/或连接于第二网络的第二网络接口捕获的原始网络数据包复制，且按预定格式封装所复制的原始网络数据包为封装数据包；其中，所述第二网络接口通过所述第二网络通信连接数据包还原设备通信；

[0071] 步骤S602：通过所述第二网络接口传送所述封装数据包至至数据包还原设备，以供其还原为原始网络数据包。

[0072] 于本发明的一实施例中，所述对从连接于第一网络的第一网络接口和/或连接于第二网络的第二网络接口捕获的原始网络数据包复制，且按预定格式封装所复制的原始网络数据包为封装数据包，包括：若所述原始数据包接收自第一网络接口，则从对其复制得到的复制数据包中提取源MAC地址、目地MAC地址及源IP地址；将所提取源MAC地址作为封装数据包的源MAC地址，将所提取目的MAC地址作为封装数据包的目的MAC地址，将所提取源IP地址作为封装数据包的源IP地址，将封装数据包的目的IP地址设为所述数据包还原设备的IP地址，将封装数据包的UDP目的端口设为指定的所述网络还源设备监听使用的端口，并将原始数据包装载于所述封装数据包的净荷中，而构造形成所述封装数据包。

[0073] 于本发明的一实施例中，所述第一网络及第二网络为互联网络；对从连接于第一网络的第一网络接口和/或连接于第二网络的第二网络接口捕获的原始网络数据包复制，且按预定格式封装所复制的原始网络数据包为封装数据包，包括：若所述原始数据包接收自第二网络接口，则从对其复制得到的复制数据包中提取源MAC地址、目地MAC地址及目的IP地址；将所提取源MAC地址作为封装数据包的目的MAC地址，将所提取目的MAC地址作为封装数据包的源MAC地址，将所提取目的IP地址作为封装数据包的源IP地址，将封装数据包的目的IP地址设为所述数据包还原设备的IP地址，UDP目的端口使用指定的所述网络还源设备监听使用的端口，并将原始数据包装载于所述封装数据包的净荷中，而构造形成所述封装数据包。

[0074] 如图7所示，展示本发明实施例中的网络数据包还原方法的流程示意图。所述方法可以应用于前述实施例中的网络数据包还原设备。

[0075] 所述方法包括：

[0076] 步骤S701：通过第二网络接收来自数据包捕获设备的封装有捕获自第一网络或第二网络的原始数据包的封装数据包；

[0077] 步骤S702：还原所述封装数据包以得到原始数据包并发送到网络分析平台。

[0078] 于本发明的一实施例中，所述还原即去除图3或图4结构的封装数据包的封装，而从净荷中提取出原始数据包，发送给所述网络分析平台进行分析

[0079] 如图8所示，展示本发明实施例中的一种处理装置，所述处理装置可应用于所述的数据包捕获设备或数据包还原设备，例如用作为所述数据包捕获设备或数据包还原设备中的数据处理电路。

[0080] 所述处理装置包括:处理器801及存储器802,所述存储器802存储有软件程序,所述处理器801运行该软件程序以实现所对应的功能。

[0081] 所述处理器801可以是通用处理器,包括中央处理器(CentralProcessingUnit,简称CPU)、网络处理器(NetworkProcessor,简称NP)等;还可以是数字信号处理器801(DigitalSignalProcessing,简称DSP)、专用集成电路(ApplicationSpecificIntegratedCircuit,简称ASIC)、现场可编程门阵列(Field-ProgrammableGateArray,简称FPGA)或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件。

[0082] 所述存储器802可能包含随机存取存储器(RandomAccessMemory,简称RAM),也可能还包括非易失性存储器(non-volatilememory),例如至少一个磁盘存储器。

[0083] 在本发明的一或多个实施例中,本发明还能提供一种计算机存储介质,其可用于存储运行时执行如图6实施例中的数据包捕获方法的计算机程序,或存储运行时执行如图7实施例中的网络数据包还原方法的计算机程序。所述计算机存储介质包括所有形式的非易失性存储器、介质和存储器设备,包括例如:半导体存储器设备,例如EPROM、EEPROM和闪存设备;磁盘,例如内部硬盘或可移动盘;磁光盘;以及CD-ROM和DVD-ROM盘。

[0084] 综上所述,本发明的数据包捕获设备及方法、还原设备及方法、系统和介质,所述数据包捕获设备,包括:第一网络接口,通信连接第一网络;第二网络接口,通信连接第二网络,并用于通过所述第二网络通信连接数据包还原设备通信;数据处理电路,通信连接所述第一网络接口及第二网络接口,用于对从所述第一网络接口和/或第二网络接口捕获的原始网络数据包复制,且按预定格式封装所复制的原始网络数据包为封装数据包,并通过所述第二网络接口传送所述封装数据包至所述数据包还原设备,以供其还原为原始网络数据包;本发明实现利用轻量级数据包捕获设备将数据包发送远端集中分析处理,解决现有技术的问题。

[0085] 上述实施例仅例示性说明本发明的原理及其功效,而非用于限制本发明。任何熟悉此技术的人士皆可在不违背本发明的精神及范畴下,对上述实施例进行修饰或改变。因此,举凡所属技术领域中具有通常知识者在未脱离本发明所揭示的精神与技术思想下所完成的一切等效修饰或改变,仍应由本发明的权利要求所涵盖。

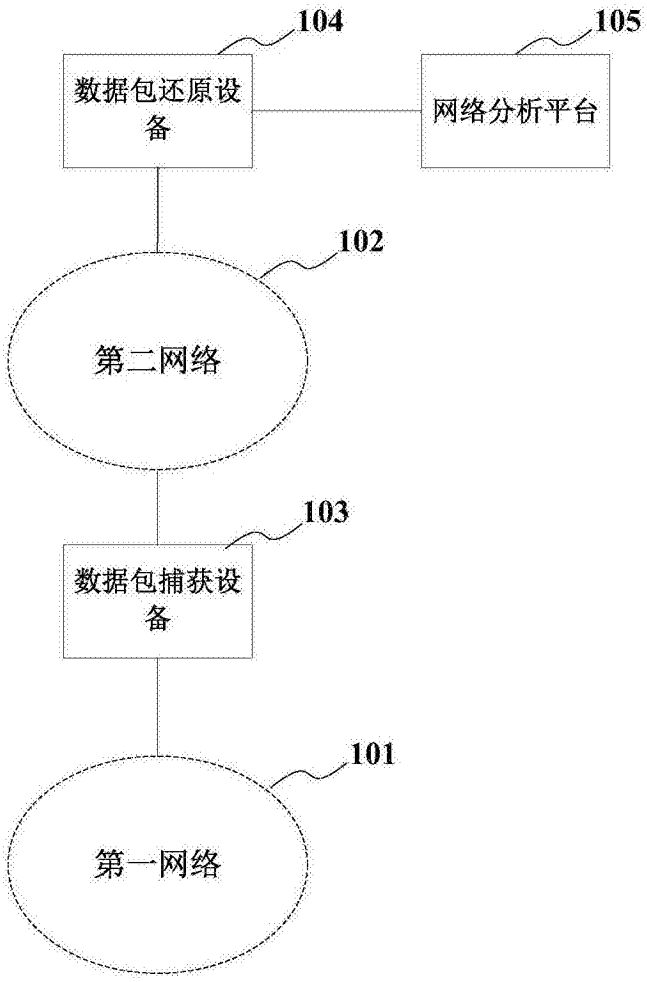

104
105
数据包还原设备
网络分析平台
102
第二网络
103
数据包捕获设备
101
第一网络

图1

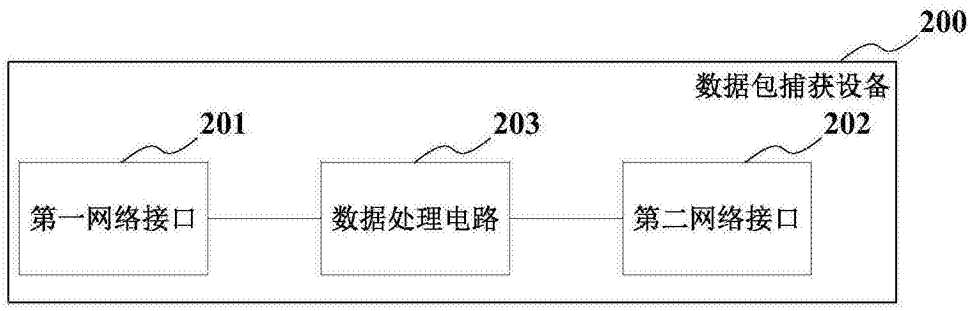

200
数据包捕获设备
201
203
202
第一网络接口
数据处理电路
第二网络接口

图2A

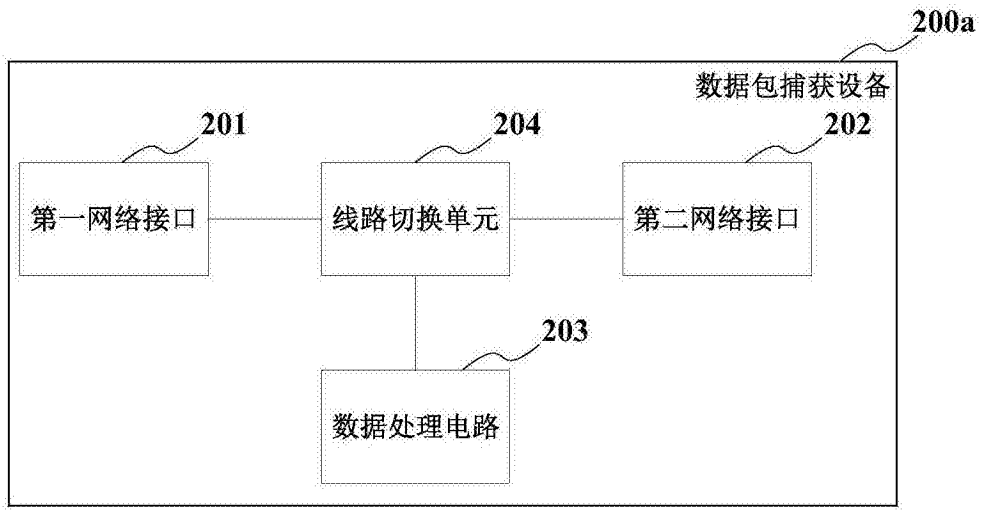

200a
数据包捕获设备
201
204
202
第一网络接口
线路切换单元
第二网络接口
203
数据处理电路

图2B

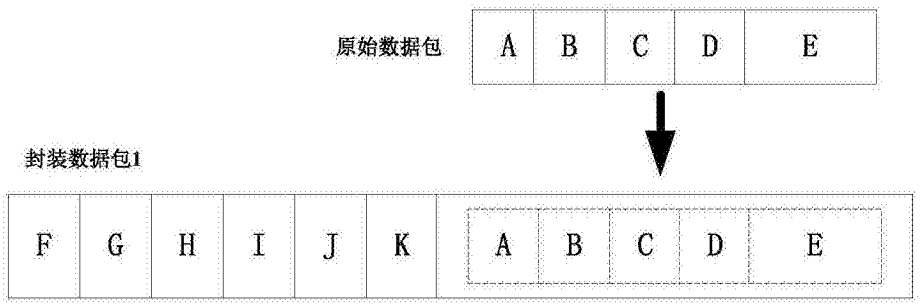

原始数据包
A
B
C
D
E
封装数据包1
F
G
H
I
J
K
A
B
C
D
E

图3

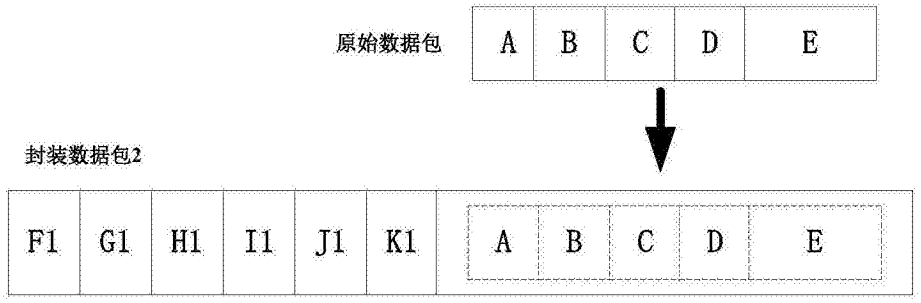

原始数据包
A
B
C
D
E
封装数据包2
F1
G1
H1
I1
J1
K1
A
B
C
D
E

图4

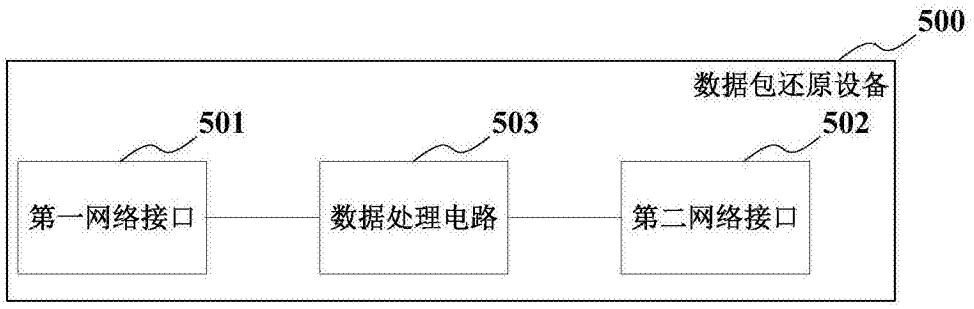

500
数据包还原设备
501
503
502
第一网络接口
数据处理电路
第二网络接口

图5

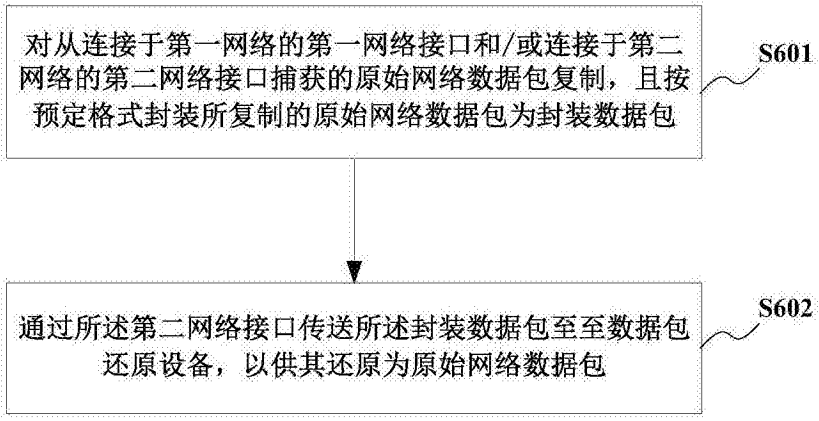

对从连接于第一网络的第一网络接口和/或连接于第二网络的第二网络接口捕获的原始网络数据包复制，且按预定格式封装所复制的原始网络数据包为封装数据包
S601
通过所述第二网络接口传送所述封装数据包至至数据包还原设备，以供其还原为原始网络数据包
S602

图6

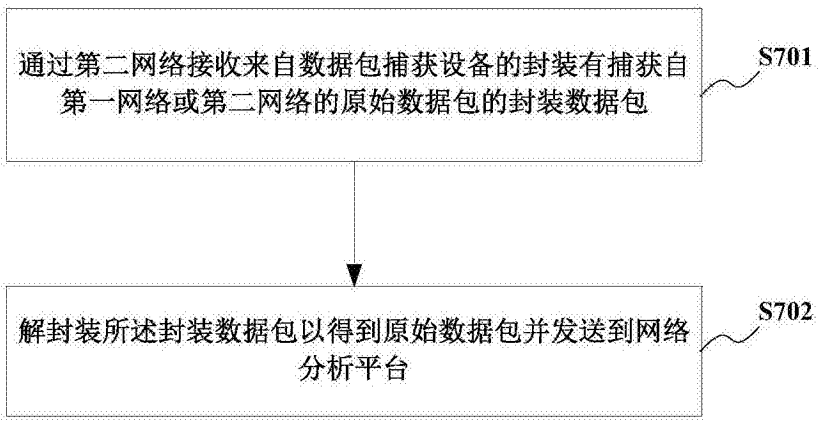

通过第二网络接收来自数据包捕获设备的封装有捕获自第一网络或第二网络的原始数据包的封装数据包
S701
解封装所述封装数据包以得到原始数据包并发送到网络分析平台
S702

图7

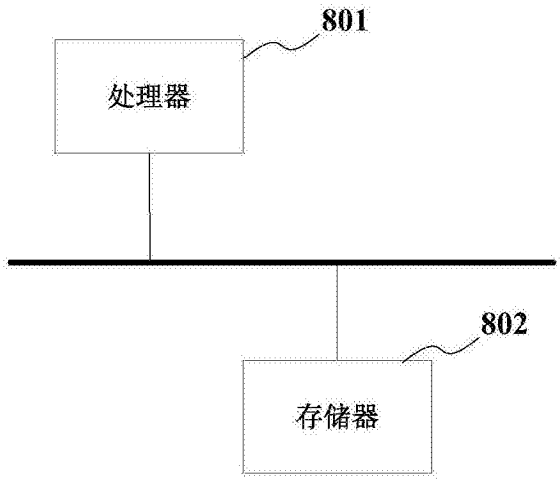


图8