(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 113285935 B
(45)授权公告日 2023.01.10

(21)申请号 202110527998.0

(22)申请日 2021.05.14

(65)同一申请的已公布的文献号
申请公布号 CN 113285935 A

(43)申请公布日 2021.08.20

(73)专利权人 山东云海国创云计算装备产业创新中心有限公司
地址 250001 山东省济南市自由贸易试验区济南片区浪潮路1036号浪潮科技园S01楼35层

(72)发明人 袁涛 高李娜 张磊 魏永哲

(74)专利代理机构 北京集佳知识产权代理有限公司 11227
专利代理师 牛亭亭

(51)Int.Cl.
H04L 9/40(2022.01)
H04L 45/60(2022.01)

(56)对比文件
CN 112152932 A,2020.12.29
CN 112152932 A,2020.12.29
CN 104052622 A,2014.09.17
CN 1595877 A,2005.03.16
CN 112152932 A,2020.12.29
WO 2016148812 A1,2016.09.22
US 2018109415 A1,2018.04.19
CN 110620731 A,2019.12.27

审查员 刘金鑫

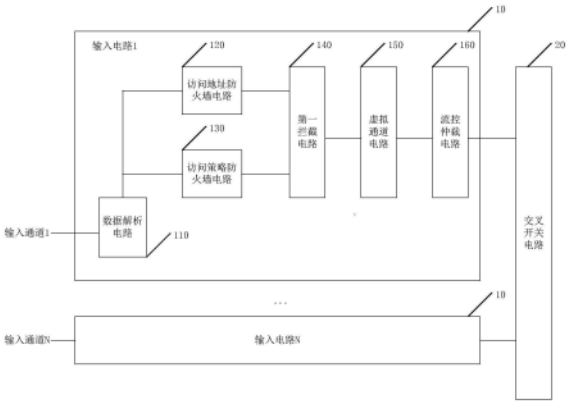
权利要求书3页 说明书15页 附图10页

(54)发明名称

一种通信系统和一种片上网络路由器

(57)摘要

本申请公开了一种片上网络路由器，包括：N个输入电路；交叉开关电路；每个输入电路均包括：数据解析电路，用于从数据头传输微片中解析出传输信息；访问地址防火墙电路，用于判断传输信息是否符合地址访问设定规则，如果否，则输出第一信息；访问策略防火墙电路，用于根据传输信息确定出目的ID并结合传输信息确定出访问关系，判断访问关系是否符合访问关系设定规则，如果否，则输出第二信息；第一拦截电路，用于当接收到第一信息或者第二信息时，拦截数据包，否则将数据包发送至虚拟通道电路；虚拟通道电路；流控仲裁电路。应用本申请的方案，有利于有效地提高片上网络路由器的传输安全性，本申请还提供了一种通信系统，具有相应技术效果。



CN 113285935 B

1.一种片上网络路由器,其特征在于,包括:

分别与N个输入通道连接的N个输入电路;与N个输入电路连接的交叉开关电路;N为正整数,每个所述输入电路均包括:

数据解析电路,用于解析出接收的数据包的各个传输微片的类型,并且从数据头传输微片中解析出传输信息;

访问地址防火墙电路,用于判断所述传输信息是否符合地址访问设定规则,如果否,则输出第一信息;

访问策略防火墙电路,用于根据所述传输信息确定出目的ID并结合所述传输信息确定出访问关系,判断所述访问关系是否符合访问关系设定规则,如果否,则输出第二信息;

第一拦截电路,用于当接收到所述第一信息或者所述第二信息时,拦截所述数据包,当未接收到所述第一信息且未接收到所述第二信息时,将所述数据包发送至虚拟通道电路;

虚拟通道电路,用于进行数据包的缓存管理;

流控仲裁电路,用于进行所述虚拟通道电路的仲裁;

所述交叉开关电路包括:

与N个流控仲裁电路连接的仲裁器,用于根据预设仲裁规则选取出一个流控仲裁电路的输出作为所述仲裁器的当前输出;

与所述仲裁器连接的2X2的行方向交叉开关电路;

与所述仲裁器连接的2X2的列方向交叉开关电路;

与所述仲裁器连接的本地访问输出电路;

还包括:

与所述交叉开关电路连接,用于进行容错重传的容错重传电路;

所述容错重传电路包括分别与所述交叉开关电路的M个输出端连接的M个容错重传单元,M为正整数,每个所述容错重传单元均包括:

与所述交叉开关电路连接的第一缓冲电路,用于接收所述交叉开关电路输出的数据包并且同时向第二缓冲电路以及后级网络输出所述数据包;

重传控制器,用于当接收到所述后级网络反馈的所述数据包传输失败的信息时,控制所述第二缓冲电路重新向所述后级网络输出所述数据包;

所述第二缓冲电路。

2.根据权利要求1所述的片上网络路由器,其特征在于,所述访问地址防火墙电路,具体用于:

获取所述传输信息中的源ID和访问地址,并且判断所述访问地址是否超出对应于所述源ID的设定的地址范围,如果是,则确定访问地址范围错误,如果否,则确定访问地址范围无误;

获取所述传输信息中的源ID和访问类型,并且判断针对所述访问类型的访问地址属性是否符合对应于所述源ID的设定的属性配置规则,如果是,则确定访问地址属性无误,如果否,则确定访问地址属性错误;

当确定出访问地址范围错误或者确定出访问地址属性错误时,确定所述传输信息不符合地址访问设定规则,并且输出第一信息。

3.根据权利要求2所述的片上网络路由器,其特征在于,所述访问策略防火墙电路,具

体用于：

确定出所述传输信息中的访问地址所映射的目的ID；

判断所述源ID与所述目的ID的访问关系是否符合访问关系设定规则，如果否，则输出第二信息。

4.根据权利要求3所述的片上网络路由器，其特征在于，所述虚拟通道电路，包括：

第一多路分解器，用于当所述第一拦截电路未接收到所述第一信息且未接收到所述第二信息时，接收所述第一拦截电路发送的所述数据包，所述传输信息中的访问类型以及访问优先级，并且接收所述访问策略防火墙电路发送的所述源ID和所述目的ID，并且根据所述访问优先级，将接收的数据发送至对应优先级的缓冲电路中；

K个不同优先级的缓冲电路，K为大于1的正整数，每个所述缓冲电路均用于：

当接收到所述第一多路分解器发送的数据时，判断当前已经申请的各个虚拟通道中，是否存在一个虚拟通道的目的ID和访问类型分别与接收到的目的ID和访问类型一致；

如果存在，则优先利用该虚拟通道的私有缓冲存储所述数据包，在该虚拟通道的私有缓冲无空闲位置且该缓冲电路的共享缓冲有空闲位置时，利用该缓冲电路的共享缓冲存储所述数据包；

如果不存在，则申请一个目的ID和访问类型分别与接收到的目的ID和访问类型一致的虚拟通道，并且利用申请的虚拟通道的私有缓冲存储所述数据包。

5.根据权利要求4所述的片上网络路由器，其特征在于，每个所述缓冲电路均还用于：

当任意一个已申请的虚拟通道的闲置时长达到第一阈值时，将该虚拟通道设置为未使能状态。

6.根据权利要求4所述的片上网络路由器，其特征在于，所述流控仲裁电路，具体用于：

按照预设规则轮询K个不同优先级的缓冲电路的各个虚拟通道，确定出各个存在有效访问请求的虚拟通道的权重值，每次轮询一轮之后，将该轮中权重值最大且第一个出现的最大权重值所对应的有效访问请求作为所述流控仲裁电路的输出；

其中，在轮询K个不同优先级的缓冲电路时，高优先级的缓冲电路优先于低优先级的缓冲电路。

7.根据权利要求6所述的片上网络路由器，其特征在于，针对任意一个存在有效访问请求的虚拟通道，根据该有效访问请求的传输信息以及等待时长进行权重值的计算，且等待时长与计算出的权重值正相关。

8.根据权利要求6所述的片上网络路由器，其特征在于，任意一个虚拟通道的权重值为通过以下操作计算出的权重值：

当该虚拟通道存在有效访问请求时，将该虚拟通道对应的3bit的二进制数据中的最高位数据置为1，当该虚拟通道不存在有效访问请求时，将该虚拟通道对应的3bit的二进制数据中的最高位数据置为0；

根据该虚拟通道的有效访问请求的传输信息，确定出该虚拟通道的权重值的3bit的二进制数据中的最低位数据以及中间位数据；

将该虚拟通道对应的3bit的二进制数据的算术值，作为该虚拟通道的权重值；

相应的，所述流控仲裁电路，具体用于：

按照预设规则轮询K个不同优先级的缓冲电路的各个虚拟通道，确定出各个存在有效

访问请求的虚拟通道的权重值，每次轮询一轮之后，基于比较器电路，确定出该轮中权重值最大且第一个出现的最大权重值，并且将该轮中权重值最大且第一个出现的最大权重值所对应的有效访问请求作为所述流控仲裁电路的输出；

其中，在轮询K个不同优先级的缓冲电路时，高优先级的缓冲电路优先于低优先级的缓冲电路。

9.一种通信系统，其特征在于，包括如权利要求1至8任意一项所述的片上网络路由器。

一种通信系统和一种片上网络路由器

技术领域

[0001] 本发明涉及通信技术领域,特别是涉及一种通信系统和一种片上网络路由器。

背景技术

[0002] 随着市场需求和半导体工艺技术的发展,SOC(system-on-chip,片上系统)规模和复杂程度日益增加,为完成复杂功能需求,以NOC(network-on-chip,片上系统通信方法)为代表的将计算与通信分离的全新片上通信方式应运而生。

[0003] 传统的NOC架构中,NOC将PE(Processing Element,处理单元)通过NIU(Network Interface Unit,网络接口单元)连接至片上网络路由器Router,从而互联彼此。目前的NOC主要研究方向涵盖网络拓扑,路由算法,路由结构,低功耗等。其工作流程表现为数据通过NIU从源PE发送到Router并由Router转发到下一个Router继续传输,直至最终目的PE。Router作为NOC架构中的核心,目前的路由方式一般采用虫洞路由方式,相比于存储转发的路由方式,虫洞路由方式基于flit传输,对缓冲数量要求较低。传统的Router一般用于连接5个输入/输出通道,即通常用于连接东、西、南、北和本地PE,即5x5的互联。

[0004] 传统的NOC中的Router架构中,完成输入通道1～N与输出通道1～N的互联,Router中的数据通路中引入虚拟通道,是为了避免队首阻塞,假设目前网络有2组访问,且假设某一个片上网络路由器只有1个物理通道,则如果一组发生阻塞,另一组的传输也会无法进行被阻塞。而如果该片上网络路由器支持2个虚拟通道,则此时第一组可以利用虚拟通道1,第二组可以利用虚拟通道2,这样即使第一组被阻塞,第二组的数据仍可通过虚拟通道2传输,有效避免队首阻塞。

[0005] Router中的控制逻辑包括路由计算、虚拟通道仲裁、交换分配和交叉开关。1、路由计算,路由计算的对象是当前Router中的每个数据包,当数据包中的头flit到达时,根据路由算法将其传至对应的物理通道。2、虚拟通道仲裁,传统的虚拟通道仲裁通常包含2级,第一级对输入的虚拟通道进行仲裁,即对所有请求该输入的虚拟通道的数据包请求进行仲裁,第二级对输出的虚拟通道进行仲裁,虚拟通道仲裁以数据包为单位,当数据头flit到达时进行仲裁。3、交换分配,对所有请求交叉开关的虚拟通道请求进行仲裁,仲裁获胜的filt经过交叉开关传输至输出通道。4、交叉开关,采用的是全互联开关结构,完成N对N的全连接。

[0006] 在传统的Router中,对传输请求不进行安全性检查,例如当源PE请求的目的地址在数据头flit传输过程中,由于串扰导致某一bit产生不期望的变化,从而造成源PE通过Router访问本不属于该PE应访问的地址段,进而可能导致出现不可预期的硬件行为。

[0007] 综上所述,如何有效地提高片上网络路由器的传输安全性,是目前本领域技术人员急需解决的技术问题。

发明内容

[0008] 本发明的目的是提供一种通信系统和一种片上网络路由器,以有效地提高片上网

络路由器的传输安全性。

[0009] 为解决上述技术问题,本发明提供如下技术方案:

[0010] 一种片上网络路由器,包括:

[0011] 分别与N个输入通道连接的N个输入电路;与N个输入电路连接的交叉开关电路;N为正整数,每个所述输入电路均包括:

[0012] 数据解析电路,用于解析出接收的数据包的各个传输微片的类型,并且从数据头传输微片中解析出传输信息;

[0013] 访问地址防火墙电路,用于判断所述传输信息是否符合地址访问设定规则,如果否,则输出第一信息;

[0014] 访问策略防火墙电路,用于根据所述传输信息确定出目的ID并结合所述传输信息确定出访问关系,判断所述访问关系是否符合访问关系设定规则,如果否,则输出第二信息;

[0015] 第一拦截电路,用于当接收到所述第一信息或者所述第二信息时,拦截所述数据包,当未接收到所述第一信息且未接收到所述第二信息时,将所述数据包发送至虚拟通道电路;

[0016] 虚拟通道电路,用于进行数据包的缓存管理;

[0017] 流控仲裁电路,用于进行所述虚拟通道电路的仲裁。

[0018] 优选的,所述访问地址防火墙电路,具体用于:

[0019] 获取所述传输信息中的源ID和访问地址,并且判断所述访问地址是否超出对应于所述源ID的设定的地址范围,如果是,则确定访问地址范围错误,如果否,则确定访问地址范围无误;

[0020] 获取所述传输信息中的源ID和访问类型,并且判断针对所述访问类型的访问地址属性是否符合对应于所述源ID的设定的属性配置规则,如果是,则确定访问地址属性无误,如果否,则确定访问地址属性错误;

[0021] 当确定出访问地址范围错误或者确定出访问地址属性错误时,确定所述传输信息不符合地址访问设定规则,并且输出第一信息。

[0022] 优选的,所述访问策略防火墙电路,具体用于:

[0023] 确定出所述传输信息中的访问地址所映射的目的ID;

[0024] 判断所述源ID与所述目的ID的访问关系是否符合访问关系设定规则,如果否,则输出第二信息。

[0025] 优选的,所述虚拟通道电路,包括:

[0026] 第一多路分解器,用于当所述第一拦截电路未接收到所述第一信息且未接收到所述第二信息时,接收所述第一拦截电路发送的所述数据包,所述传输信息中的访问类型以及访问优先级,并且接收所述访问策略防火墙电路发送的所述源ID和所述目的ID,并且根据所述访问优先级,将接收的数据发送至对应优先级的缓冲电路中;

[0027] K个不同优先级的缓冲电路,K为大于1的正整数,每个所述缓冲电路均用于:

[0028] 当接收到所述第一多路分解器发送的数据时,判断当前已经申请的各个虚拟通道中,是否存在一个虚拟通道的目的ID和访问类型分别与接收到的目的ID和访问类型一致;

[0029] 如果存在,则优先利用该虚拟通道的私有缓冲存储所述数据包,在该虚拟通道的

私有缓冲无空闲位置且该缓冲电路的共享缓冲有空闲位置时，利用该缓冲电路的共享缓冲存储所述数据包；

[0030] 如果不存在，则申请一个目的ID和访问类型分别与接收到的目的ID和访问类型一致的虚拟通道，并且利用申请的虚拟通道的私有缓冲存储所述数据包。

[0031] 优选的，每个所述缓冲电路均还用于：

[0032] 当任意一个已申请的虚拟通道的闲置时长达到第一阈值时，将该虚拟通道设置为未使能状态。

[0033] 优选的，所述流控仲裁电路，具体用于：

[0034] 按照预设规则轮询K个不同优先级的缓冲电路的各个虚拟通道，确定出各个存在有效访问请求的虚拟通道的权重值，每次轮询一轮之后，将该轮中权重值最大且第一个出现的最大权重值所对应的有效访问请求作为所述流控仲裁电路的输出；

[0035] 其中，在轮询K个不同优先级的缓冲电路时，高优先级的缓冲电路优先于低优先级的缓冲电路。

[0036] 优选的，针对任意一个存在有效访问请求的虚拟通道，根据该有效访问请求的传输信息以及等待时长进行权重值的计算，且等待时长与计算出的权重值正相关。

[0037] 优选的，任意一个虚拟通道的权重值为通过以下操作计算出的权重值：

[0038] 当该虚拟通道存在有效访问请求时，将该虚拟通道对应的3bit的二进制数据中的最高位数据置为1，当该虚拟通道不存在有效访问请求时，将该虚拟通道对应的3bit的二进制数据中的最高位数据置为0；

[0039] 根据该虚拟通道的有效访问请求的传输信息，确定出该虚拟通道的权重值的3bit的二进制数据中的最低位数据以及中间位数据；

[0040] 将该虚拟通道对应的3bit的二进制数据的算术值，作为该虚拟通道的权重值；

[0041] 相应的，所述流控仲裁电路，具体用于：

[0042] 按照预设规则轮询K个不同优先级的缓冲电路的各个虚拟通道，确定出各个存在有效访问请求的虚拟通道的权重值，每次轮询一轮之后，基于比较器电路，确定出该轮中权重值最大且第一个出现的最大权重值，并且将该轮中权重值最大且第一个出现的最大权重值所对应的有效访问请求作为所述流控仲裁电路的输出；

[0043] 其中，在轮询K个不同优先级的缓冲电路时，高优先级的缓冲电路优先于低优先级的缓冲电路。

[0044] 优选的，所述交叉开关电路包括：

[0045] 与N个流控仲裁电路连接的仲裁器，用于根据预设仲裁规则选取出一个流控仲裁电路的输出作为所述仲裁器的当前输出；

[0046] 与所述仲裁器连接的2X2的行方向交叉开关电路；

[0047] 与所述仲裁器连接的2X2的列方向交叉开关电路；

[0048] 与所述仲裁器连接的本地访问输出电路。

[0049] 优选的，还包括：

[0050] 与所述交叉开关电路连接，用于进行容错重传的容错重传电路。

[0051] 优选的，所述容错重传电路包括分别与所述交叉开关电路的M个输出端连接的M个容错重传单元，M为正整数，每个所述容错重传单元均包括：

[0052] 与所述交叉开关电路连接的第一缓冲电路，用于接收所述交叉开关电路输出的数据包并且同时向第二缓冲电路以及后级网络输出所述数据包；

[0053] 重传控制器，用于当接收到所述后级网络反馈的所述数据包传输失败的信息时，控制所述第二缓冲电路重新向所述后级网络输出所述数据包；

[0054] 所述第二缓冲电路。

[0055] 一种通信系统，包括上述任意一项所述的片上网络路由器。

[0056] 应用本发明实施例所提供的技术方案，在每个输入电路中均设置了数据解析电路，访问地址防火墙电路，访问策略防火墙电路，以及第一拦截电路。数据解析电路可以解析出接收的数据包的各个传输微片的类型，并且从数据头传输微片中解析出传输信息，访问地址防火墙电路，可以判断传输信息是否符合地址访问设定规则，如果否，则输出第一信息；访问策略防火墙电路可以根据传输信息确定出目的ID并结合传输信息确定出访问关系，判断访问关系是否符合访问关系设定规则，如果否，则输出第二信息。可以看出，当输出了第一信息或者第二信息时，说明当前的访问存在安全隐患，因此第一拦截电路会在接收到第一信息或者第二信息时，拦截当前的数据包，有利于提高传输的安全性，同时避免了无意义的数据传输，有利于避免功耗和带宽的浪费。此外，本申请设置了访问地址防火墙电路，用于判断传输信息是否符合地址访问设定规则，还设置了访问策略防火墙电路用于判断访问关系是否符合访问关系设定规则，有利于实现较为全面的访问安全性的保障。综上，本申请的方案有利于有效地提高片上网络路由器的传输安全性。

附图说明

[0057] 为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0058] 图1为本发明中一种片上网络路由器的结构示意图；

[0059] 图2a为一种具体实施方式中的输入电路的第一部分的结构示意图；

[0060] 图2b为一种具体实施方式中的输入电路的第二部分的结构示意图；

[0061] 图3为一种具体实施方式中的访问地址防火墙电路的结构示意图；

[0062] 图4为一种具体实施方式中的访问策略防火墙电路的功能示意图；

[0063] 图5为传统的Router中的虚拟通道电路的示意图；

[0064] 图6为一种具体实施方式中的交叉开关电路的结构示意图；

[0065] 图7为一种具体实施方式中的虚拟通道的权重值计算以及轮询示意图；

[0066] 图8为一种具体实施方式中的容错重传单元的结构示意图；

[0067] 图9为一种具体实施方式中的容错重传的原理示意图；

[0068] 图10a为传统的片上网络路由器与本申请的一种具体实施方式中的支持动态虚拟通道的片上网络路由器的虚拟通道利用率比较示意图；

[0069] 图10b为传统的片上网络路由器与本申请的一种具体实施方式中的支持动态虚拟通道的平均传输延迟的比较示意图；

[0070] 图10c为传统的片上网络路由器与本申请的一种具体实施方式中的具有容错重传

功能的片上网络路由器的PEF比较示意图。

具体实施方式

[0071] 本发明的核心是提供一种片上网络路由器，有利于有效地提高片上网络路由器的传输安全性。

[0072] 为了使本技术领域的人员更好地理解本发明方案，下面结合附图和具体实施方式对本发明作进一步的详细说明。显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0073] 请参考图1，图1为本发明中一种片上网络路由器的结构示意图，该片上网络路由器可以包括：

[0074] 分别与N个输入通道连接的N个输入电路10；与N个输入电路10连接的交叉开关电路20；N为正整数，每个输入电路10均包括：

[0075] 数据解析电路110，用于解析出接收的数据包的各个传输微片的类型，并且从数据头传输微片中解析出传输信息；

[0076] 访问地址防火墙电路120，用于判断传输信息是否符合地址访问设定规则，如果否，则输出第一信息；

[0077] 访问策略防火墙电路130，用于根据传输信息确定出目的ID并结合传输信息确定出访问关系，判断访问关系是否符合访问关系设定规则，如果否，则输出第二信息；

[0078] 第一拦截电路140，用于当接收到第一信息或者第二信息时，拦截数据包，当未接收到第一信息且未接收到第二信息时，将数据包发送至虚拟通道电路150；

[0079] 虚拟通道电路150，用于进行数据包的缓存管理；

[0080] 流控仲裁电路160，用于进行虚拟通道电路150的仲裁。

[0081] 具体的，片上网络路由器具有N个物理通道，即N个输入通道，N的具体取值可以根据实际需要进行设定和选取，目前的实际应用中通常可以选取为8。当然，后续的实际应用中，随着架构的复杂，即当片上网络路由器的互联结构更为复杂时，N可以根据实际需要设置为其他的数值。

[0082] 针对任意一个数据包，可以通过片上网络路由器的路由计算功能确定出该数据包对应的输入通道，本申请的附图中并未示出实现路由计算功能的具体结构，此外，实现路由计算功能具体采用的规则也可以根据实际需要进行设定，

[0083] 通常是依据数据包的数据头flit中的目标地址进行路由计算，可以采用固定模式，例如方向优先的固定模式，例如，应用到NOC架构中时，源PE0作为片上网络数据传输发起方initiator，访问的片上网络数据接收方target为PE8，路由算法规定向东优先，经过的路径为R0-R1-R2-R5-R8。又如设置为自适应模式，具体可以根据网络传输负载的动态平衡进行路由计算，应用到NOC架构中时，PE0访问P8，根据当前传输负载平衡结果，选择的路由路径为R0-R1-R4-R7-R8。可以理解的是，当路由计算功能设定完毕之后，相同路径的数据包会被置入相同的输入通道中。

[0084] 每个输入通道均有与该输入通道连接的输入电路10。

[0085] 输入电路10中的数据解析电路110可以解析出接收的数据包的各个传输微片的类

型，并且从数据头传输微片中解析出传输信息；

[0086] 数据包通常有3种类型的传输微片：数据头传输微片，数据传输微片以及数据尾传输微片，本申请的后文以及附图中，将传输微片表示为flit。

[0087] 数据解析电路110可以确定出数据包的数据头flit，进而从数据头flit中解析出传输信息，传输信息的具体项目构成可以根据实际需要进行设定，通常至少会包括源ID，访问地址，传输长度，读写访问类型等项目，又如在一种场合中，考虑到后续需要按照优先级的不同进行不同数据包的先后处理，则传输信息的具体项目中还可以设置有优先级信息。

[0088] 例如下表一为一种具体场合中数据解析电路110从数据头flit中解析出的传输信息。

[0089] 表一：

[0090]

源 ID	读写访问类型	指令/数据访问	访问地址	传输长度	存储器属性	可配置的优先级(urgent)

[0091] 数据解析电路110解析数据头flit，得到了传输信息之后，需要将传输信息发送到访问地址防火墙电路120和访问策略防火墙电路130。

[0092] 访问地址防火墙电路120是针对地址访问的有效性进行确定，具体的，可以判断传输信息是否符合地址访问设定规则，如果否，说明地址访问存在问题，便会输出第一信息，反之，如果符合地址访问设定规则，说明地址访问有效，则可以不输出信息，或者可以输出表示地址访问有效的提示信息，具体取决于实际场合中的具体电路设置情况，例如本申请的图2a的实施方式中，访问地址防火墙电路120输出0表示地址访问有效，输出1表示地址访问无效，即访问地址防火墙电路120输出1时，表示的是输出了第一信息，地址访问出现了错误。

[0093] 此外，地址访问设定规则的具体内容也可以根据实际需要进设定和调整。

[0094] 例如在本发明的一种具体实施方式中，访问地址防火墙电路120，具体用于：

[0095] 获取传输信息中的源ID和访问地址，并且判断访问地址是否超出对应于源ID的设定的地址范围，如果是，则确定访问地址范围错误，如果否，则确定访问地址范围无误；

[0096] 获取传输信息中的源ID和访问类型，并且判断针对访问类型的访问地址属性是否符合对应于源ID的设定的属性配置规则，如果是，则确定访问地址属性无误，如果否，则确定访问地址属性错误；

[0097] 当确定出访问地址范围错误或者确定出访问地址属性错误时，确定传输信息不符合地址访问设定规则，并且输出第一信息。

[0098] 可参阅图3，需要说明的是，在图3的实施方式中，设置了4个地址片段解析电路，是考虑到可能存在的访问地址范围较大，可以利用4个地址片段解析电路分别负责一部分，这样相较于设置单个的地址片段解析电路判断访问地址是否超出对应于源ID的设定的地址范围，成本会更低，当然，在其他具体实施方式中，可以选用其他数量的地址片段解析电路，只要能够实现本申请的访问地址防火墙电路120的功能即可，并不影响本申请的实施。

[0099] 例如一种具体场合中，某一个数据包的数据头flit经过解析之后，传输信息中的访问地址需要由地址片段解析电路4负责处理，则不参与负责的地址片段解析电路1至3均会输出0。地址片段解析电路4则判断解析出的访问地址是否超出对应于源ID的设定的地址

范围，即如果判断出大于对应于源ID的设定的地址范围的上限，或者判断出低于对应于源ID的设定的地址范围的下限，便可以确定地址属性错误，既如果不大于上限也不小于下限，则可以确定访问地址属性无误，在图3中用一个或门的输出0表示访问地址范围无误，而如果该或门输出的是1，说明访问地址范围错误。

[0100] 该种实施方式中，除了进行访问地址范围的有效性检测之外，还进行了访问地址属性的有效性检测，从而有利于更加全面地实现访问地址的有效性检测。

[0101] 具体的，通过获取传输信息中的源ID和访问类型，判断针对访问类型的访问地址属性是否符合对应于源ID的设定的属性配置规则。属性配置规则的具体内容可以根据实际需要进行设定和调整，例如下表二为一种具体场合中的属性配置规则协议表。例如，当源ID＝0，读写属性配置为Device Non-bufferable(该属性配置要求写相应信号由最终的目的设备返回读不可预取，写操作不可合并等)，而如果当前的数据头flit中的源ID＝0，但读写属性不是Device Non-bufferable，则可以确定是访问地址属性错误。

[0102] 表二：

[0103]

读属性（ARCACHE[3:0]）	写属性(AWCACHE)	存储器属性
0000	0000	Device Non-Bufferable（Device 属性非缓冲）
0001	0001	Device Bufferable（Device 属性缓冲特性）
0010	0010	Normal Non-cacheable Non-bufferable（普通非 Cache，非缓冲属性）
0011	0011	Normal Non-cacheable Bufferable（普通非 Cache 属性，缓冲属性）
1010	0110	Write-Through No-Allocate（cache 属性，贯穿写属性更新 cache 和外部存储器）

[0104]

1110(0110)	0110	Write-Through Read-Allocate（cache 属性，贯穿写属性更新 cache 和外部存储器读回时数据先读回 cache 后再从 cache 访问访问方）
1010	1110	Write-Through Write-Allocate（与上述类似，参见 AXI 协议）
1110	1110	Write-Through Read and Write-Allocate（与上述类似，参见 AXI 协议）
1011	0111	Write-Back No-Allocate（与上述类似，参见 AXI 协议）
1111(0111)	0111	Write-Back Read-Allocate（与上述类似，参见 AXI 协议）
1011	1111(1011)	Write-Back Write-Allocate（与上述类似，参见 AXI 协议）
1111	1111	Write-Back Read and Write-Allocate

[0105]

		（与上述类似，参见 AXI 协议）

[0106] 访问地址防火墙电路120是针对地址访问的有效性进行确定，访问策略防火墙电

路130则是针对访问策略的有效性进行确定，具体的是针对访问关系的有效性进行确定。访问策略防火墙会判断访问关系是否符合访问关系设定规则，如果不符合，会输出第二信息。反之，如果符合访问关系设定规则，说明访问策略有效，则可以不输出信息，或者输出表示访问策略有效的提示信息，具体取决于实际场合中的具体电路设置情况，例如本申请的图2a的实施方式中，输出0表示访问策略有效，输出1表示访问策略无效，即访问策略防火墙电路130输出1时，表示的是输出了第二信息。

[0107] 访问关系设定规则的具体内容也可以根据实际需要进行设定。

[0108] 在本发明的一种具体实施方式中，访问策略防火墙电路130，具体用于：

[0109] 确定出传输信息中的访问地址所映射的目的ID；

[0110] 判断源ID与目的ID的访问关系是否符合访问关系设定规则，如果否，则输出第二信息。

[0111] 该种实施方式中，通过传输信息中的访问地址确定出其所映射的目的ID，确定了目的ID之后，根据源ID，目的ID以及访问类型，便可以确定源ID与目的ID的访问关系，具体的，可以确定源ID与目的ID的读/写访问关系。例如图4为一种具体场合中的访问策略防火墙电路130的功能示意图，并且示出了一种具体场合中访问关系设定规则中的8×8的源ID与目的ID的写访问关系设定图，可以看出，该种具体实施方式中，不允许源ID对自身进行写访问。

[0112] 当然，其他实施方式中，可以根据实际需要，设定更加复杂的访问关系设定规则。

[0113] 当访问地址防火墙电路120输出第一信息，或者访问策略防火墙电路130输出第二信息时，均说明访问不具备有效性，因此，第一拦截电路140会在接收到第一信息或者第二信息时，拦截数据包。

[0114] 在图2a的实施方式中，当访问地址防火墙电路120输出第一信息，或者访问策略防火墙电路130输出第二信息时，第一拦截电路140中的与访问地址防火墙电路120和访问策略防火墙电路130连接的或门均是输出1，此时，第一拦截电路140中的拦截分解器便会拦截下数据包，即不允许将数据包中的各个flit向后级进行输出，相应的，如果该或门输出的是0，则说明未接收到第一信息且未接收到第二信息时，此时无需拦截，可以将数据包发送至虚拟通道电路150。

[0115] 此外需要说明的是，在图2a的实施方式中，第一拦截电路140中包括了1和或门电路和两个拦截分解器，是考虑到部分实施方式中，除了需要将数据包中的各个flit发送到后级电路，还需要将传输信息发送到后级电路，例如图2a中具体需要将访问类型以及优先级发送到后级电路，因此，设置了2个两个拦截分解器。

[0116] 第一拦截电路140将数据包发送至虚拟通道电路150中，虚拟通道电路150可以进行数据包的缓存管理。

[0117] 本申请考虑到，在传统的虚拟通道电路150中，存在着虚拟通道的利用率较低的问题，可参阅图5，为传统的Router中的虚拟通道电路的示意图，每个输入通道静态分配n个虚拟通道，例如该输入通道对应的PE输出请求的数据包只有数据包2，则在此传输场景下，只利用2个虚拟通道，其余n-2个被静态分配的虚拟通道未被利用。每个虚拟通道中静态分配k个flit缓冲，例如该虚拟通道对应的PE输出的数据包只包含3个flit，具体为一个数据头flit，一个数据flit以及一个数据尾flit，因此k个flit缓冲的利用率只有3/k。

[0118] 由图5可知，传统的虚拟通道/内部缓冲利用率不足，其余未被利用的虚拟通道及内部的flit缓冲的功耗不可忽视，与此同时，如果降低k和n的取值，有可能导致在面对高负载网络传输时，虚拟通道和内部flit缓冲不足的情况，造成传输性能下降。

[0119] 因此，在本发明的一种具体实施方式中，并不是静态配置，而是通过动态配置虚拟通道和flit缓冲，实现功耗的降低，提高虚拟通道和flit缓冲的利用率。

[0120] 可参阅图2b，该种实施方式中，虚拟通道电路150，包括：

[0121] 第一多路分解器150，用于当第一拦截电路140未接收到第一信息且未接收到第二信息时，接收第一拦截电路140发送的数据包，传输信息中的访问类型以及访问优先级，并且接收访问策略防火墙电路130发送的源ID和目的ID，并且根据访问优先级，将接收的数据发送至对应优先级的缓冲电路中；

[0122] K个不同优先级的缓冲电路，K为大于1的正整数，每个缓冲电路均用于：

[0123] 当接收到第一多路分解器150发送的数据时，判断当前已经申请的各个虚拟通道中，是否存在一个虚拟通道的目的ID和访问类型分别与接收到的目的ID和访问类型一致；

[0124] 如果存在，则优先利用该虚拟通道的私有缓冲存储数据包，在该虚拟通道的私有缓冲无空闲位置且该缓冲电路的共享缓冲有空闲位置时，利用该缓冲电路的共享缓冲存储数据包；

[0125] 如果不存在，则申请一个目的ID和访问类型分别与接收到的目的ID和访问类型一致的虚拟通道，并且利用申请的虚拟通道的私有缓冲存储数据包。

[0126] 该种实施方式中，第一多路分解器150接收第一拦截电路140发送的数据包，并且还需要获取传输信息中的访问类型以及访问优先级，并且接收访问策略防火墙电路130发送的源ID和目的ID，之后便可以根据访问优先级，将接收的数据发送至对应优先级的缓冲电路中。当然，在其他实施方式中，第一多路分解器150可以通过第一拦截电路140接收数据包，而传输信息中的访问类型以及访问优先级，以及源ID和目的ID可以通过其他方式获取，例如通过数据解析电路110获取，又如虚拟通道电路150自身设置了用于解析传输信息的装置。当然，本申请的图4的实施方式中，直接从前级电路获取各项所需要的数据，实施时简单方便，利于提高效率。

[0127] K的具体取值可以根据实际需要进行设定和调整，在本申请的图2b的实施方式中，将K设置为2，实施时较为简单，即图2b中具有一个高优先级缓冲电路152和一个低优先级缓冲电路153，当然，在其他实施方式中，K可以有其他的取值。

[0128] 针对每一个缓冲电路，当该缓冲电路当接收到第一多路分解器151发送的数据时，会将相同的目的ID和访问类型的数据包置入同一虚拟通道中，这样的方式设置有利于提高数据传输的效率。虚拟通道以队列的形式组织数据，每个虚拟通道都有该虚拟通道对应的队列。

[0129] 缓冲电路会判断当前已经申请的各个虚拟通道中，是否存在一个虚拟通道的目的ID和访问类型分别与接收到的目的ID和访问类型一致，如果存在，本申请是优先利用该虚拟通道的私有缓冲存储数据包，在该虚拟通道的私有缓冲无空闲位置且该缓冲电路的共享缓冲有空闲位置时，利用该缓冲电路的共享缓冲存储数据包。

[0130] 可以看出，申请的虚拟通道具有其私有缓冲，同时，同一个缓冲电路中的各个虚拟通道都可以利用共享缓冲存储数据包，使得本申请方案的flit缓冲的利用率大幅提高。

[0131] 进一步的，为例降低虚拟通道的功耗，每个缓冲电路均还可以用于：

[0132] 当任意一个已申请的虚拟通道的闲置时长达到第一阈值时，将该虚拟通道设置为未使能状态。从而避免闲置的虚拟通道的功耗浪费。设置虚拟通道为未使能状态，具体可以通过常规动态功耗控制实现，例如通过门控时钟的方式控制未使能能状态的虚拟通道的功耗。

[0133] 此外需要说明的是，每个缓冲电路均需要设置其可申请的虚拟通道数量阈值，例如本申请的图2b的实施方式中，高优先级缓冲电路可以最多使能5个虚拟通道，低优先级缓冲电路可以最多使能3个虚拟通道。可以理解的是，在实际应用中，当缓冲电路接收到第一多路分解器151发送的数据，并且判断出需要申请一个目的ID和访问类型分别与接收到的目的ID和访问类型一致的虚拟通道之后，可以判断是否有剩余虚拟通道可申请，如果没有，则需要等待。

[0134] 同样的，在利用已经申请的虚拟通道存储数据包时，如果该虚拟通道的私有缓冲无空闲位置，且剩余的共享缓冲也没有空闲位置时，同样需要暂停该数据包的缓冲，等待该虚拟通道的私有缓冲或者剩余的共享缓冲存在空闲位置之后，再重新进行该数据包的缓冲。

[0135] 在本发明的一种具体实施方式中，流控仲裁电路160，具体用于：

[0136] 按照预设规则轮询K个不同优先级的缓冲电路的各个虚拟通道，确定出各个存在有效访问请求的虚拟通道的权重值，每次轮询一轮之后，将该轮中权重值最大且第一个出现的最大权重值所对应的有效访问请求作为流控仲裁电路160的输出；

[0137] 其中，在轮询K个不同优先级的缓冲电路时，高优先级的缓冲电路优先于低优先级的缓冲电路。

[0138] 按照预设规则轮询K个不同优先级的缓冲电路的各个虚拟通道，具体顺序可以根据实际需要进行设定，但是，本申请的该种实施方式中，在轮询K个不同优先级的缓冲电路时，设定了高优先级的缓冲电路优先于低优先级的缓冲电路，而且，轮询一轮之后，权重值最大且第一个出现的最大权重值所对应的有效访问请求作为流控仲裁电路160的输出，这样有利于高优先级的缓冲电路优先进行输出。但又不会使得高优先级的缓冲电路完全占据输出，例如低优先级的缓冲电路的权重值非常高时，仍然能够及时地被输出。

[0139] 例如针对图2b的实施方式，将低优先级缓冲电路153的3个虚拟通道编号为0，1，2，将高优先级缓冲电路152的5个虚拟通道编号为3至7，且轮询的虚拟通道顺序为3→4→5→6→7→0→1→2，之后重新回到3，开始下一轮轮询。

[0140] 确定出各个存在有效访问请求的虚拟通道的权重值的具体方式可以根据实际需要进行设定，例如在本发明的一种具体实施方式中，任意一个虚拟通道的权重值为通过以下操作计算出的权重值：

[0141] 当该虚拟通道存在有效访问请求时，将该虚拟通道对应的3bit的二进制数据中的最高位数据置为1，当该虚拟通道不存在有效访问请求时，将该虚拟通道对应的3bit的二进制数据中的最高位数据置为0；

[0142] 根据该虚拟通道的有效访问请求的传输信息，确定出该虚拟通道的权重值的3bit的二进制数据中的最低位数据以及中间位数据；

[0143] 将该虚拟通道对应的3bit的二进制数据的算术值，作为该虚拟通道的权重值；

[0144] 相应的，流控仲裁电路160，具体用于：

[0145] 按照预设规则轮询K个不同优先级的缓冲电路的各个虚拟通道，确定出各个存在有效访问请求的虚拟通道的权重值，每次轮询一轮之后，基于比较器电路，确定出该轮中权重值最大且第一个出现的最大权重值，并且将该轮中权重值最大且第一个出现的最大权重值所对应的有效访问请求作为流控仲裁电路160的输出；

[0146] 其中，在轮询K个不同优先级的缓冲电路时，高优先级的缓冲电路优先于低优先级的缓冲电路。

[0147] 该种实施方式中，给出了一种具体场合中的计算权重值的方案，较为简单方便，便于理解结合图7以及表三进行说明。

[0148] 该种实施方式中，针对任意一个虚拟通道，该虚拟通道是否存在有效访问请求，会决定该虚拟通道对应的3bit的二进制数据中的最高位数据，从而对该虚拟通道的权重值产生决定性影响。

[0149] 例如图7中的虚拟通道4，由于虚拟通道4存在有效访问请求，并且，根据虚拟通道4的有效访问请求的传输信息，确定出本轮中，虚拟通道4的权重值的3bit的二进制数据中的最低位数据以及中间位数据均为1，也即本轮中，虚拟通道4所对应的3bit的二进制数据为111，其算术值为7，7也就是虚拟通道4本轮的权重值。

[0150] 又如，图7中的虚拟通道5不存在有效访问请求，且虚拟通道5的权重值的3bit的二进制数据中的最低位数据以及中间位数据均为0，即本轮中，虚拟通道5所对应的3bit的二进制数据为000，其算术值为0。并且，在实际应用中，当某个虚拟通道不存在有效访问请求时，可以直接将该虚拟通道的本轮权重值置为0。

[0151] 例如具体的轮询的虚拟通道顺序为上文的实施例中的3→4→5→6→7→0→1→2，可以看出，虽然图7中的虚拟通道4和虚拟通道6的权重值均为7，但是，由于该轮中权重值最大且第一个出现的最大权重值来自于虚拟通道4，因此是将虚拟通道4所对应的有效访问请求作为流控仲裁电路160的输出。

[0152] 此外，该种实施方式中，是基于比较器电路确定出各个权重值当中的第一个出现的最大权重值，例如图7的具体场合中，利用了7个具有2个输入端的比较器来构建所需要的比较器电路，在其他场合中，基于虚拟通道数量的不同，可以选取其他形式的比较器电路，只要能够实现本申请的目的即可，即，只要能够确定出该轮中权重值最大且第一个出现的最大权重值即可。

[0153] 该种实施方式中，权重值的3bit的二进制数据中的最低位数据以及中间位数据，是由传输信息决定的，具体的对应规则可以根据实际需要进行设定，例如在表三的实施方式中，按照传输信息中的访问类型的不同，可以确定出不同的访问级别，其中，访问级别最高，则权重值的3bit的二进制数据中的中间位数据以及最低位数据均为1。访问级别次高，则权重值的3bit的二进制数据中的中间位数据为1且最低位数据为0。访问级别普通，则权重值的3bit的二进制数据中的中间位数据为0且最低位数据为1。访问级别低，则权重值的3bit的二进制数据中的中间位数据为0且最低位数据为0。

[0154] 表三：

[0155]

编号	访问级别	对应组	对应访问类型定义
0	最高	最高级别组	紧急(数据头 flit 中对应 urgent=1) 中断 低延时需求的控制信号 短数据包(数据头 flit 中 length 小于等于 128 比特)
1	次高	次高级别组	实时或流数据，如视频
2	普通	普通级别组	存储器/寄存器读写访问
3	低	低级组	数据块（一般大于 4096 字节）

[0156] 在本发明的一种具体实施方式中，针对任意一个存在有效访问请求的虚拟通道，根据该有效访问请求的传输信息以及等待时长进行权重值的计算，且等待时长与计算出的权重值正相关。

[0157] 该种实施方式中，权重值还会受到等待时长的影响，可以避免高优先级的访问长久仲裁获胜，使得低优先级无法得到服务的情况。例如一种场合中，按照前述实施方式得到各个虚拟通道各自对应的3bit的二进制数据的算术值之后，并不是直接作为各个虚拟通道的权重值，而是需要再与变量T叠加，叠加之后的结果再作为各个虚拟通道的权重值。而变量T则是一个受到该虚拟通道的有效访问请求的等待时长影响的数值，当然，二者应当是正相关关系，使得等待时长越长，越能够被优先处理。

[0158] 当然，在其他具体实施方式中，还可以设置更多影响权重值的参数，例如可以包括寄存器静态配置等参数。并且可以设置更为复杂的计算权重值的算法。

[0159] 在本发明的一种具体实施方式中，可参阅图6，交叉开关电路20包括：

[0160] 与N个流控仲裁电路160连接的仲裁器，用于根据预设仲裁规则选取出一个流控仲裁电路160的输出作为仲裁器的当前输出；

[0161] 与仲裁器连接的2X2的行方向交叉开关电路；

[0162] 与仲裁器连接的2X2的列方向交叉开关电路；

[0163] 与仲裁器连接的本地访问输出电路。

[0164] 本申请考虑到，在传统的方案中的交叉开关的网络复杂程度为$O(N^2)$，N通常为8，并且随着规模的扩大，芯片后端实现时的布线难度不断增加。

[0165] 本申请的该种实施方式中，交叉开关电路20中的行方向交叉开关电路和列方向交叉开关电路的网络复杂程度均为2X2，有利于降低后端的布线难度。

[0166] 仲裁器采用的仲裁规则可以有多种，例如可以简单设置为按照顺序轮询的方式，又如可以设定为根据访问flit中标识的优先级访问的方式，在实际应用中，考虑到前级的流控仲裁电路160已经是按照优先级进行数据包的选取，仲裁器此时可以设定为按照顺序轮询即可。

[0167] 通过行方向交叉开关电路，列方向交叉开关电路以及与仲裁器连接的本地访问输出电路，使得经过交叉开关电路20之后，按照目的地址的不同，具有5个输出方向。当然，在实际应用中，当互联结构更为复杂，即Router具有更多的输出方向时，可以相适应地调整交叉开关电路20的具体结构。

[0168] 在本发明的一种具体实施方式中，还可以包括，与交叉开关电路20连接，用于进行容错重传的容错重传电路。

[0169] 由于设置了容错重传电路，使得本申请的片上网络路由器可以应对串扰，耦合噪声引起的传输错误，容错重传电路的具体设计可以有多种，例如可以设计为数据包进入网络传输时，同时会输入至容错重传电路中，如果下游回复传输失败，则可以从容错重传电路的缓冲中读取数据包以尝试一次或者多次重传，直到传输成功或者达到上限，此外，容错重传电路还可以支持以例如中断的方式，上报错误或记录，从而使得在内部网络传输错误表中可以进行后续的查询。

[0170] 在本发明的一种具体实施方式中，容错重传电路可以包括分别与交叉开关电路20的M个输出端连接的M个容错重传单元，M为正整数，每个容错重传单元20均包括：

[0171] 与交叉开关电路20连接的第一缓冲电路801，用于接收交叉开关电路输出的数据包并且同时向第二缓冲电路802以及后级网络输出数据包；

[0172] 重传控制器803，用于当接收到后级网络反馈的数据包传输失败的信息时，控制第二缓冲电路802重新向后级网络输出数据包；

[0173] 第二缓冲电路802。

[0174] 具体的，可参阅图8，图8示出的是与交叉开关电路20的某一个输出端连接的容错重传单元，该容错重传单元的第一缓冲电路801可以接收并缓存交叉开关电路输出的数据包，例如图9的一种具体场合中，第一缓冲电路801具体选取为FIFO缓冲，在第0时刻，FIFO缓冲中有2个数据包，分别为数据包1:H1，D1，D2，T1。以及数据包2:H2，D3，D4，T2。H表明为Header flit，D表明为data flit，T表明为Tail flit。

[0175] 在第1时刻，FIFO缓冲将H1向后级网络传输，同时，还会向第二缓冲电路802输出H1。此时后级网络向重传控制器803回复NACK，表明传输失败，H1丢弃。

[0176] 在第2时刻，FIFO缓冲将D1向后级网络传输，同时，还会向第二缓冲电路802输出D1。此时后级网络向重传控制器803回复NACK，表明传输失败，D1丢弃。

[0177] 在第3时刻，FIFO缓冲将D2向后级网络传输，同时，还会向第二缓冲电路802输出D2。此时后级网络向重传控制器803回复NACK，表明传输失败，D2丢弃。

[0178] 在第4时刻，FIFO缓冲将T1向后级网络传输，同时，还会向第二缓冲电路802输出T1。此时后级网络向重传控制器803回复NACK，表明传输失败，T1丢弃。

[0179] 在第5时刻，由于之前的数据包传输失败，即数据包1传输失败，因此，重传控制器803会控制第二缓冲电路802重新向后级网络输出数据包1。此外，如前文的描述，在实际应用中，可以尝试一次或者多次重传，直到传输成功或者达到上限，此外，容错重传电路还可以支持以例如中断的方式，上报错误或记录，从而使得在内部网络传输错误表中可以进行后续的查询。

[0180] 图10a为传统的片上网络路由器与本申请的一种具体实施方式中的支持动态虚拟通道的片上网络路由器的虚拟通道利用率比较示意图，图10b为传统的片上网络路由器与本申请的一种具体实施方式中的支持动态虚拟通道的平均传输延迟的比较示意图，可以看出，本申请支持动态虚拟通道的方案虚拟通道利用率高，平均传输延迟低。

[0181] 图10c为传统的片上网络路由器与本申请的一种具体实施方式中的具有容错重传功能的片上网络路由器的PEF比较示意图，可以看出，本申请的方案错误数低，PEF低。PEF是

性能功耗容错度(Performance,Energy and Fault-tolerance),是反映性能,功耗以及容错度三者之间关系的度量。PEF(平均延迟×数据包传输功耗)/数据包传输完成率。

[0182] 相应于上面的片上网络路由器的实施例,本发明实施例还提供了一种通信系统,可以包括上述任意实施例中的片上网络路由器,可与上文相互对应参照,此处不再重复说明。

[0183] 应用本发明实施例所提供的技术方案,在每个输入电路10中均设置了数据解析电路110,访问地址防火墙电路120,访问策略防火墙电路130,以及第一拦截电路140。数据解析电路110可以解析出接收的数据包的各个传输微片的类型,并且从数据头传输微片中解析出传输信息,访问地址防火墙电路120,可以判断传输信息是否符合地址访问设定规则,如果否,则输出第一信息;访问策略防火墙电路130可以根据传输信息确定出目的ID并结合传输信息确定出访问关系,判断访问关系是否符合访问关系设定规则,如果否,则输出第二信息。可以看出,当输出了第一信息或者第二信息时,说明当前的访问存在安全隐患,因此第一拦截电路140会在接收到第一信息或者第二信息时,拦截当前的数据包,有利于提高传输的安全性,同时避免了无意义的数据传输,有利于避免功耗和带宽的浪费。此外,本申请设置了访问地址防火墙电路120,用于判断传输信息是否符合地址访问设定规则,还设置了访问策略防火墙电路130用于判断访问关系是否符合访问关系设定规则,有利于实现较为全面的访问安全性的保障。综上所述,本申请的方案有利于有效地提高片上网络路由器的传输安全性。

[0184] 还需要说明的是,在本文中,诸如第一和第二等之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来,而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。而且,术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含,从而使得包括一系列要素的过程、方法、物品或者设备不仅包括那些要素,而且还包括没有明确列出的其他要素,或者是还包括为这种过程、方法、物品或者设备所固有的要素。在没有更多限制的情况下,由语句“包括一个……”限定的要素,并不排除在包括所述要素的过程、方法、物品或者设备中还存在另外的相同要素。

[0185] 专业人员还可以进一步意识到,结合本文中所公开的实施例描述的各示例的单元及算法步骤,能够以电子硬件、计算机软件或者二者的结合来实现,为了清楚地说明硬件和软件的可互换性,在上述说明中已经按照功能一般性地描述了各示例的组成及步骤。这些功能究竟以硬件还是软件方式来执行,取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能,但是这种实现不应认为超出本发明的范围。

[0186] 本文中应用了具体个例对本发明的原理及实施方式进行了阐述,以上实施例的说明只是用于帮助理解本发明的技术方案及其核心思想。应当指出,对于本技术领域的普通技术人员来说,在不脱离本发明原理的前提下,还可以对本发明进行若干改进和修饰,这些改进和修饰也落入本发明权利要求的保护范围。

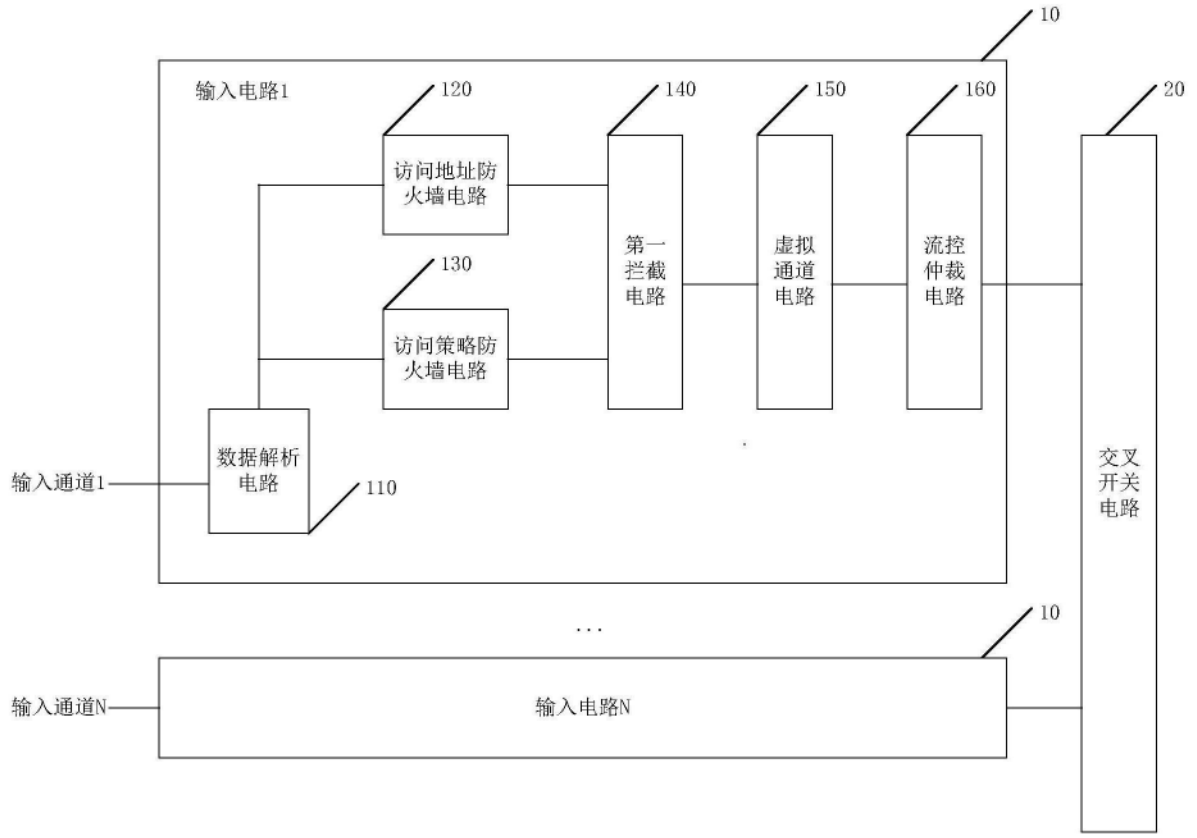

10
输入电路1
120
140
150
160
20
访问地址防火墙电路
130
访问策略防火墙电路
第一拦截电路
虚拟通道电路
流控仲裁电路
交叉开关电路
数据解析电路
110
输入通道1
...
10
输入通道N
输入电路N

图1

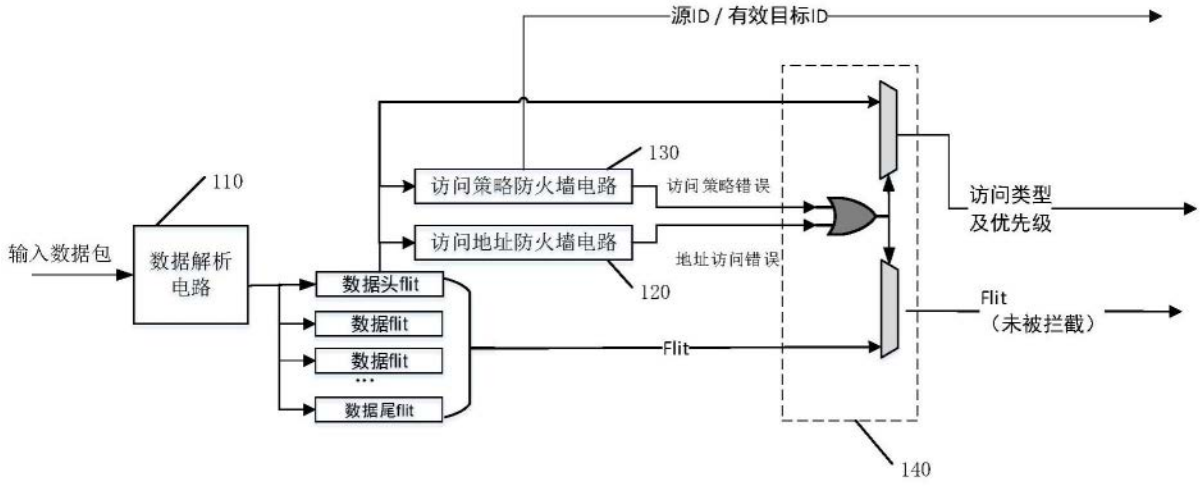

源ID / 有效目标ID
130
访问策略防火墙电路
访问策略错误
访问类型及优先级
110
输入数据包
数据解析电路
访问地址防火墙电路
地址访问错误
120
数据头flit
数据flit
数据flit
...
数据尾flit
Flit
Flit（未被拦截）
140

图2a

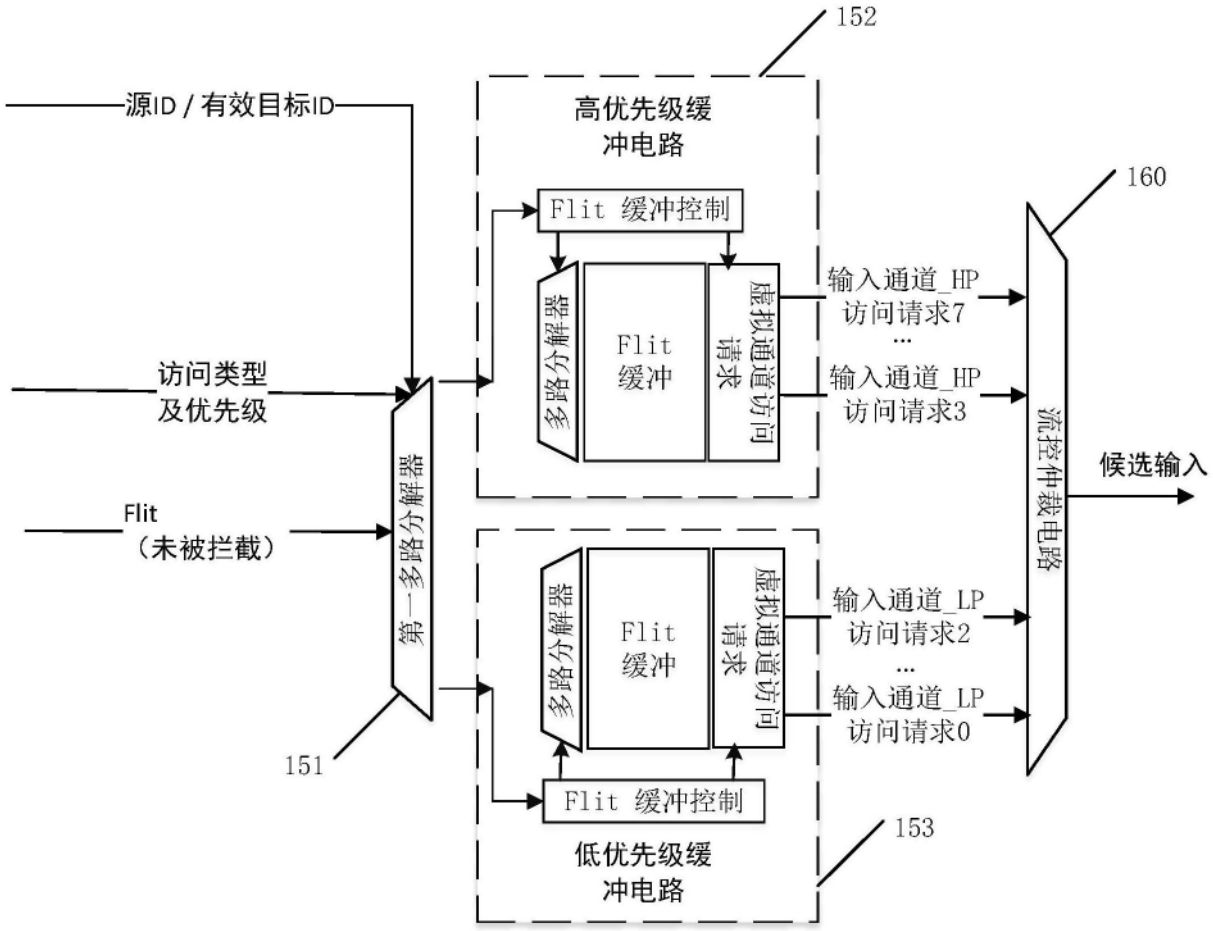

152
源ID / 有效目标ID
高优先级缓冲电路
Flit 缓冲控制
多路分解器
Flit 缓冲
虚拟通道访问请求
输入通道_HP 访问请求7
...
输入通道_HP 访问请求3
160
访问类型及优先级
Flit（未被拦截）
第一多路分解器
流控仲裁电路
候选输入
多路分解器
Flit 缓冲
虚拟通道访问请求
输入通道_LP 访问请求2
...
输入通道_LP 访问请求0
151
Flit 缓冲控制
153
低优先级缓冲电路

图2b

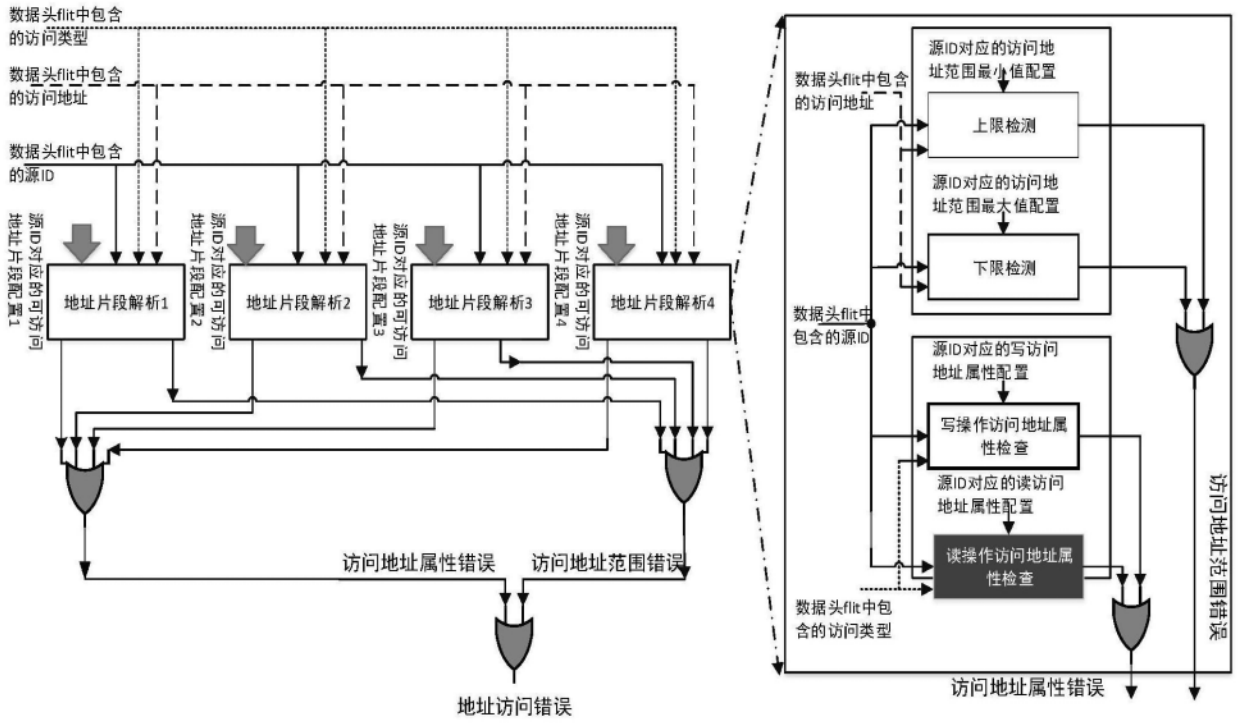

数据头flit中包含的访问类型
数据头flit中包含的访问地址
数据头flit中包含的源ID
源ID对应的可访问地址片段配置1
源ID对应的可访问地址片段配置2
源ID对应的可访问地址片段配置3
源ID对应的可访问地址片段配置4
地址片段解析1
地址片段解析2
地址片段解析3
地址片段解析4
访问地址属性错误
访问地址范围错误
地址访问错误
源ID对应的访问地址范围最小值配置
上限检测
源ID对应的访问地址范围最大值配置
下限检测
源ID对应的写访问地址属性配置
写操作访问地址属性检查
源ID对应的读访问地址属性配置
读操作访问地址属性检查
数据头flit中包含的访问地址
数据头flit中包含的源ID
数据头flit中包含的访问类型
访问地址范围错误
访问地址属性错误

图3

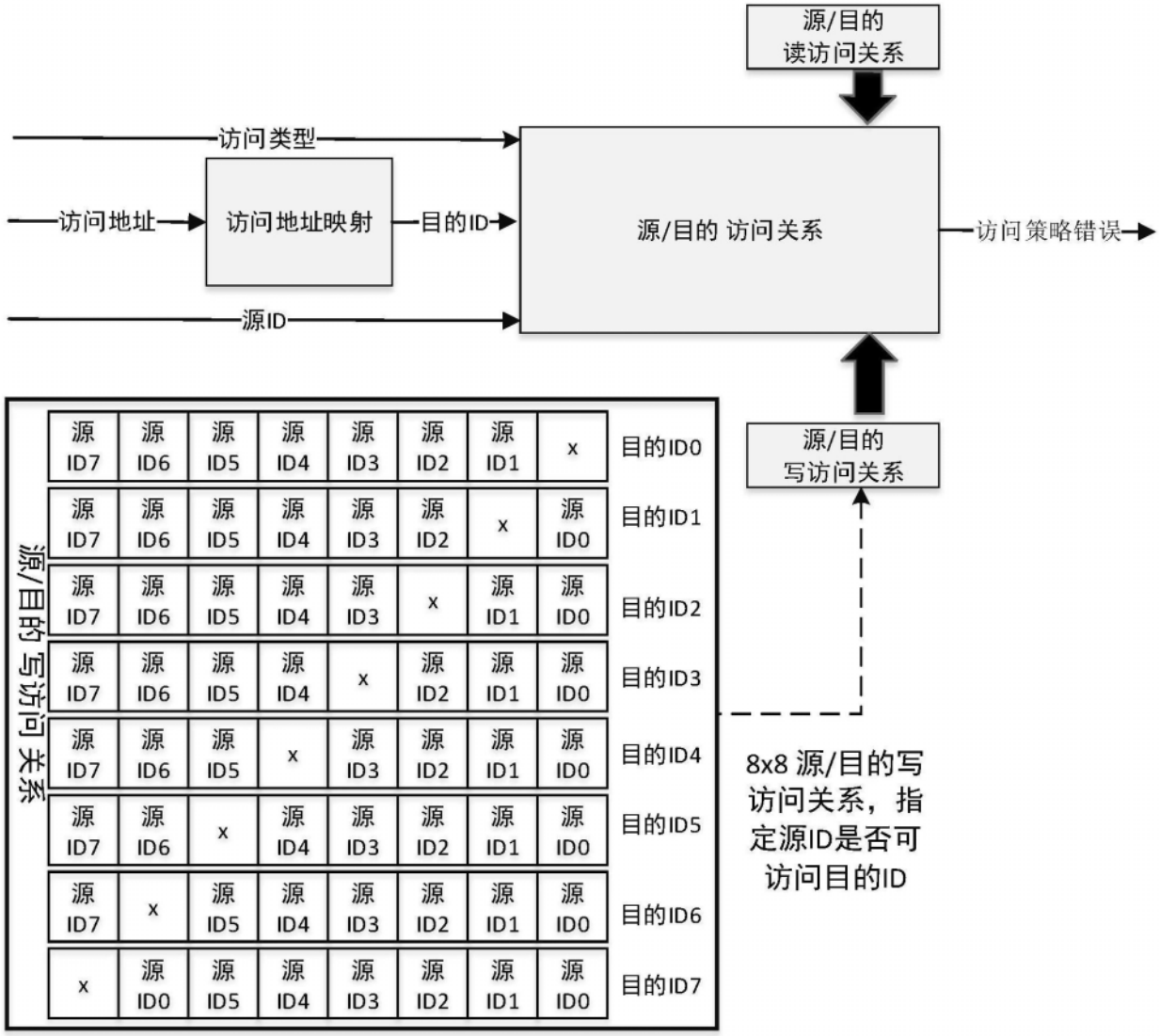

源/目的
读访问关系
访问类型
访问地址
访问地址映射
目的ID
源/目的 访问关系
访问策略错误
源ID
源/目的
写访问关系
源/目的 写访问 关系
源ID7 源ID6 源ID5 源ID4 源ID3 源ID2 源ID1 x 目的ID0
源ID7 源ID6 源ID5 源ID4 源ID3 源ID2 x 源ID0 目的ID1
源ID7 源ID6 源ID5 源ID4 源ID3 x 源ID1 源ID0 目的ID2
源ID7 源ID6 源ID5 源ID4 x 源ID2 源ID1 源ID0 目的ID3
源ID7 源ID6 源ID5 x 源ID3 源ID2 源ID1 源ID0 目的ID4
源ID7 源ID6 x 源ID4 源ID3 源ID2 源ID1 源ID0 目的ID5
源ID7 x 源ID5 源ID4 源ID3 源ID2 源ID1 源ID0 目的ID6
x 源ID0 源ID5 源ID4 源ID3 源ID2 源ID1 源ID0 目的ID7
8x8 源/目的写
访问关系，指
定源ID是否可
访问目的ID

图4

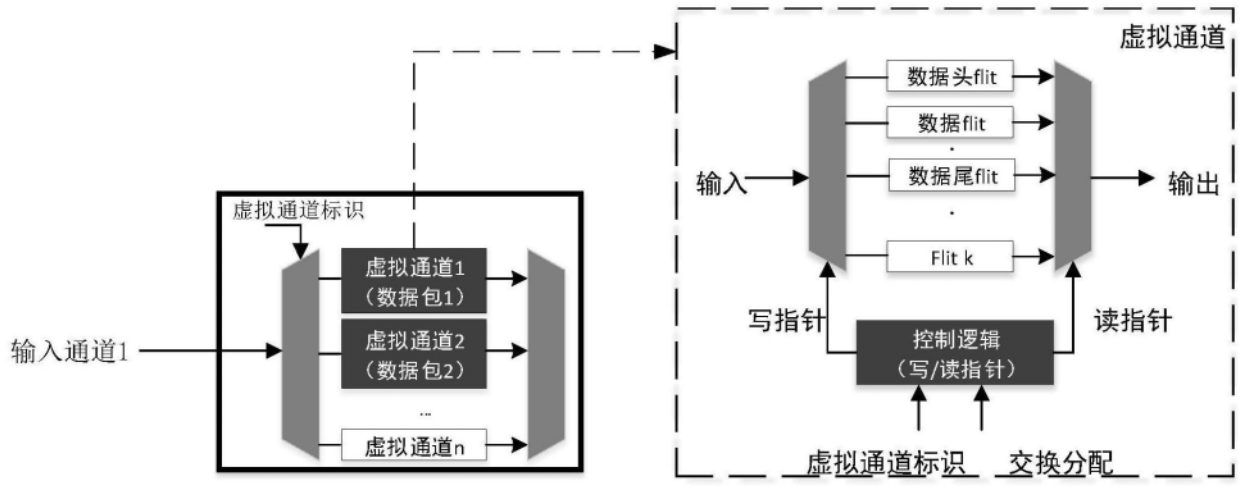

虚拟通道
数据头flit
数据flit
数据尾flit
Flit k
输入
输出
写指针
读指针
控制逻辑
（写/读指针）
虚拟通道标识
交换分配
虚拟通道标识
虚拟通道1
（数据包1）
虚拟通道2
（数据包2）
虚拟通道n
输入通道1

图5

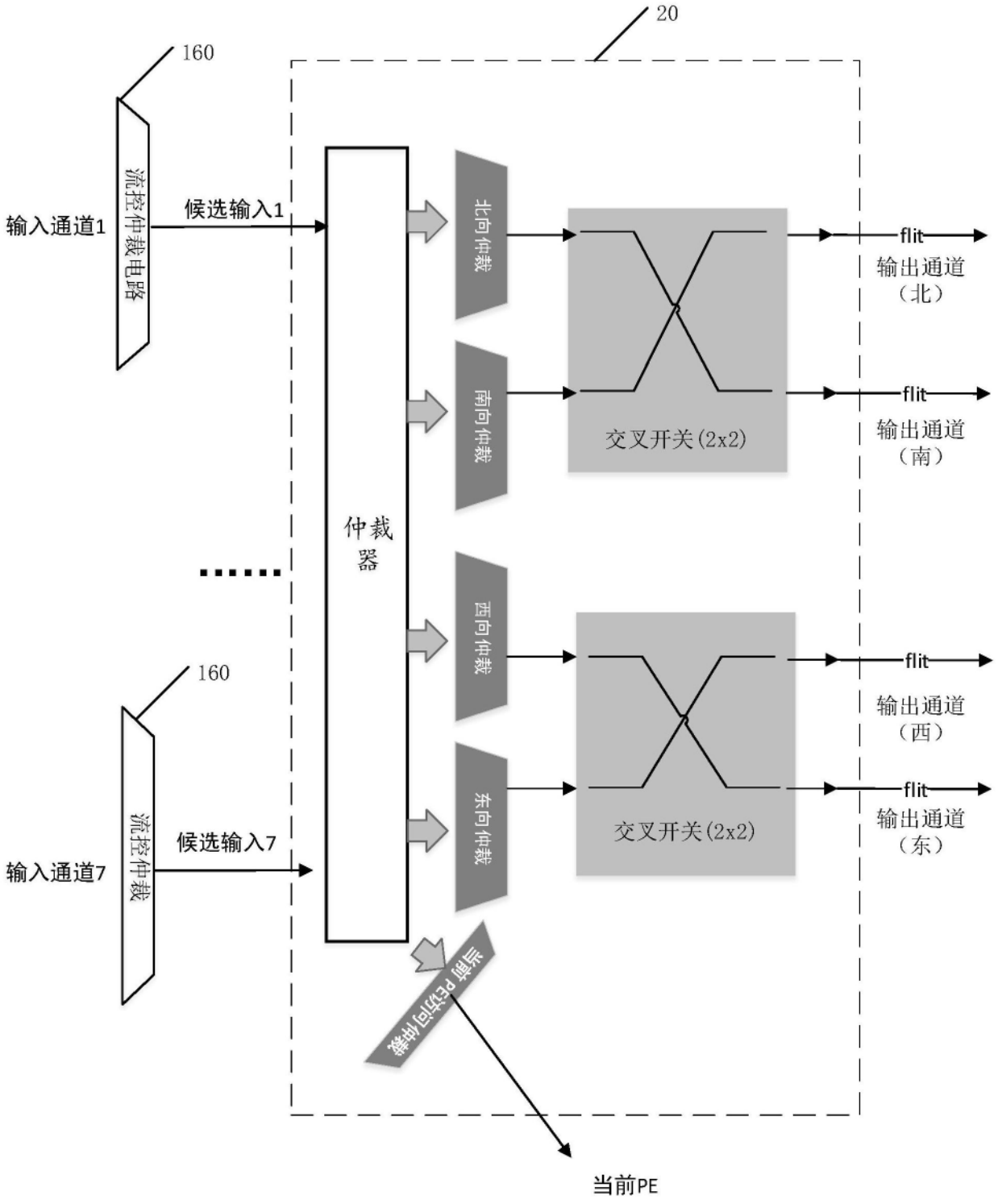

20
160
流控仲裁电路
输入通道1
候选输入1
仲裁器
北向仲裁
南向仲裁
西向仲裁
东向仲裁
交叉开关(2x2)
交叉开关(2x2)
flit
输出通道（北）
flit
输出通道（南）
flit
输出通道（西）
flit
输出通道（东）
160
流控仲裁
输入通道7
候选输入7
当前PE向仲裁
当前PE

图6

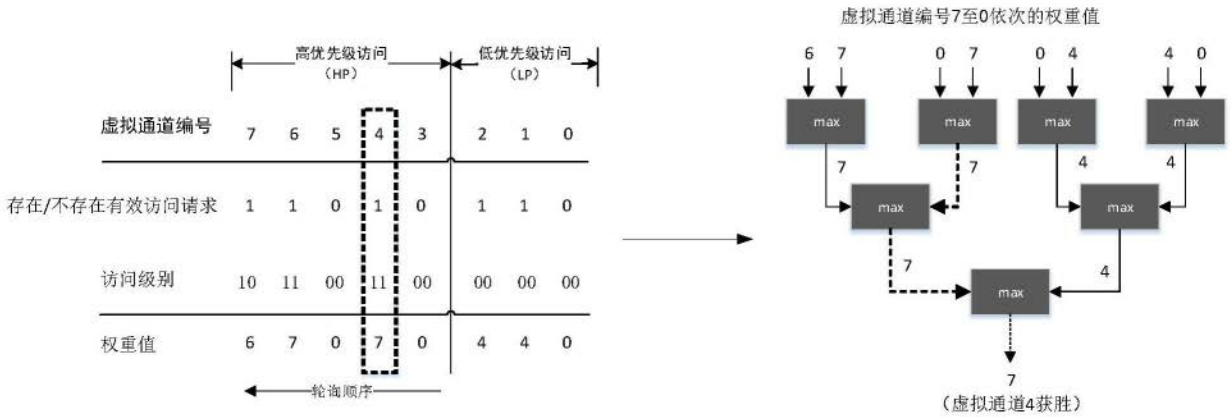

高优先级访问
（HP）
低优先级访问
（LP）
虚拟通道编号
7 6 5 4 3 2 1 0
存在/不存在有效访问请求
1 1 0 1 0 1 1 0
访问级别
10 11 00 11 00 00 00 00
权重值
6 7 0 7 0 4 4 0
轮询顺序
虚拟通道编号7至0依次的权重值
max
（虚拟通道4获胜）

图7

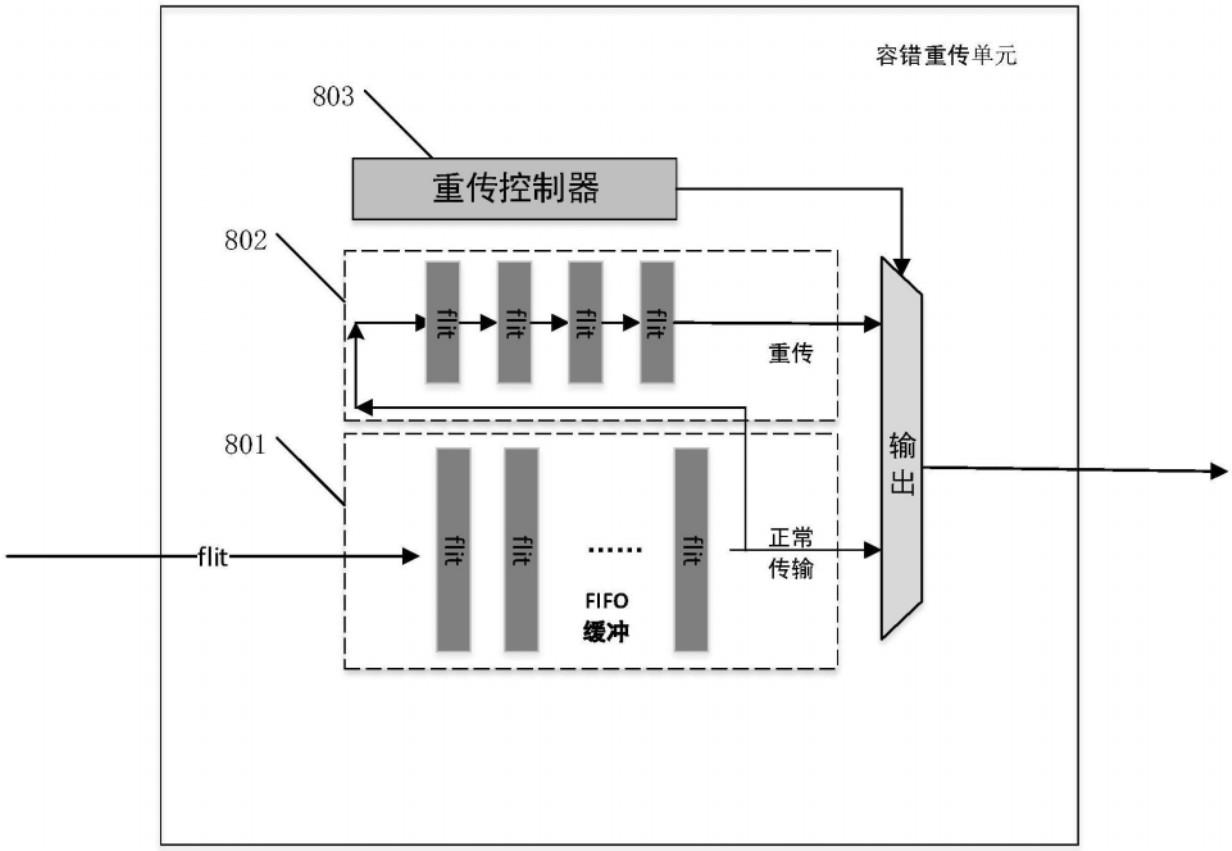

容错重传单元
803
重传控制器
802
flit
重传
801
输出
flit
正常
传输
FIFO
缓冲

图8

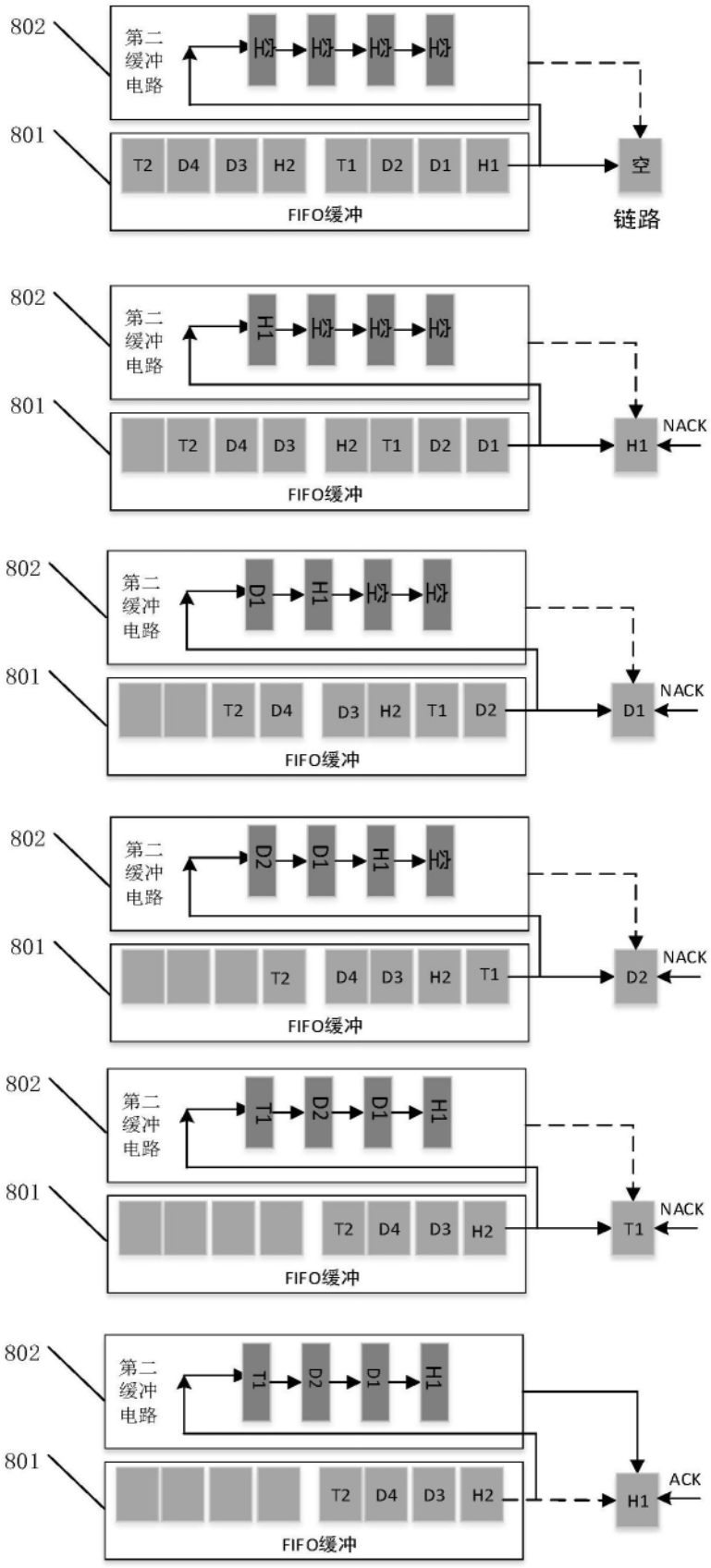

802
第二缓冲电路
H4
H3
H2
H1
801
T2
D4
D3
H2
T1
D2
D1
H1
空
FIFO缓冲
链路
802
第二缓冲电路
H1
H4
H3
H2
801
T2
D4
D3
H2
T1
D2
D1
H1
NACK
FIFO缓冲
802
第二缓冲电路
D1
H1
H4
H3
801
T2
D4
D3
H2
T1
D2
D1
NACK
FIFO缓冲
802
第二缓冲电路
D2
D1
H1
H4
801
T2
D4
D3
H2
T1
D2
NACK
FIFO缓冲
802
第二缓冲电路
T1
D2
D1
H1
801
T2
D4
D3
H2
T1
NACK
FIFO缓冲
802
第二缓冲电路
T1
D2
D1
H1
801
T2
D4
D3
H2
H1
ACK
FIFO缓冲

图9

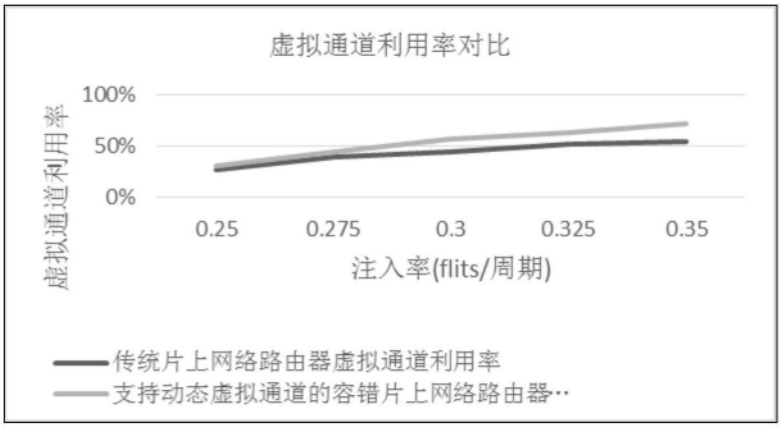

虚拟通道利用率对比
虚拟通道利用率
100%
50%
0%
0.25
0.275
0.3
0.325
0.35
注入率(flits/周期)
传统片上网络路由器虚拟通道利用率
支持动态虚拟通道的容错片上网络路由器…

图10a

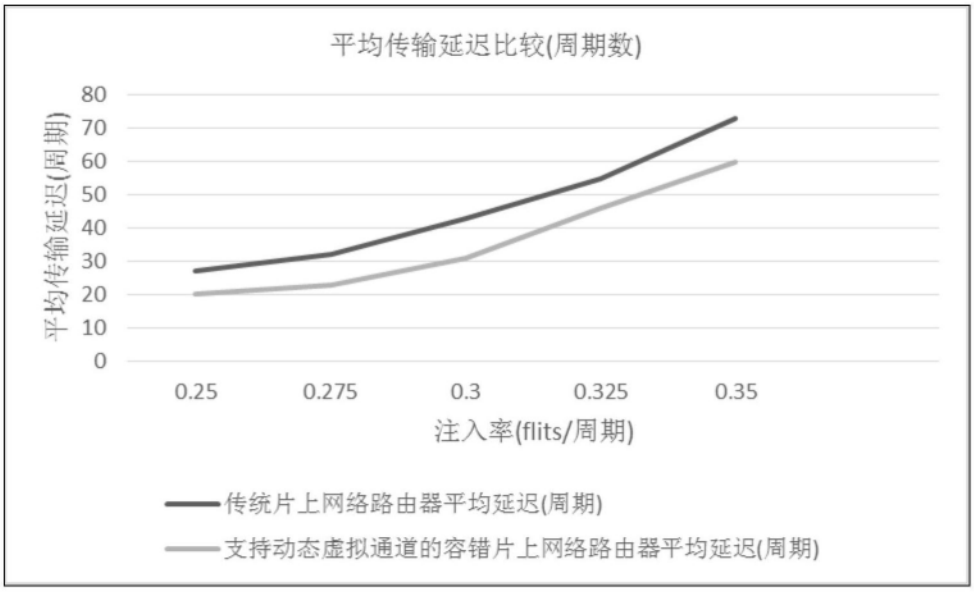

平均传输延迟比较(周期数)
平均传输延迟(周期)
80
70
60
50
40
30
20
10
0
0.25
0.275
0.3
0.325
0.35
注入率(flits/周期)
传统片上网络路由器平均延迟(周期)
支持动态虚拟通道的容错片上网络路由器平均延迟(周期)

图10b

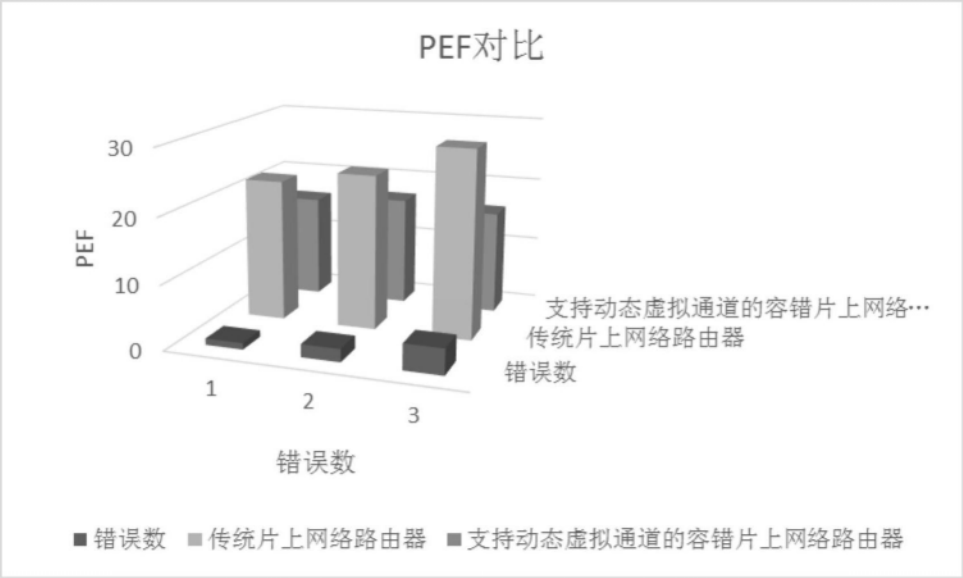

PEF对比
30
20
10
0
PEF
1
2
3
错误数
支持动态虚拟通道的容错片上网络…
传统片上网络路由器
错误数
错误数
传统片上网络路由器
支持动态虚拟通道的容错片上网络路由器

图10c