2020北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE

优势互补促进产业协同

国货当自强

杨庆华
山石网科高级副总裁 首席技术专家

国货当自强

“国货当自强”的口号，至少在灾难深重的抗日战争前后，中国民族工业就喊了出来。一些爱国人士和民族企业家发出“实业救国”的呐喊，“提倡国货”等口号一时间传遍大江南北，冯玉祥、宋则久甚至开办了专卖国货的商场。

但那时中国民族工业毕竟刚起步，加之国力孱弱，国货并不具备与“洋货”全面竞争的条件。

为什么需要国产化

国产化需求背景

- **安全需求：**棱镜门事件，网络监听，CPU等硬件后门问题日益突出。
- **政策要求：**网络安全即国家安全，国家及行业政策要求产品国产化，如军工，保密行业强制执行。
- **芯片受控：**中兴事件，华为禁售的反思，芯片大多数是国外进口，产品的生产、研发完全被国外公司控制。

网络安全上升到国家高度

- 2014年2月27日网信领导小组第一次会议：习近平指出，**没有网络安全就没有国家安全。**
- 2016年4月19日网信座谈会：互联网核心技术是最大的“命门”，核心技术受制于人是我们最大的隐患。
- 2018年4月网信工作会议：自主创新推进网络强国建设，**核心技术是国之重器。**

实体名单

- 《美国出口管制条例》（Export Administration Regulations，“**EAR**”）
- 十大一般性禁止行为，几个维度：出口管制分类编码（ECCN）；目的地（Commerce Country Chart）；最终用户（Entity List）；最终用途（核武器、生化武器、火箭系统、军事等）；行为（资金支持、货运代理，等）。
-

一	向已列入名单的国家出口和再出口受控物项
二	在国外出口和再出口含有美国管制物项的外国制造品，其含量超过最低量
三	在国外出口和再出口利用美国技术和软件直接生产的外国制造品
四	从事被否决令禁止的行为
五	向被禁止最终用户或用于被禁止最终用途的出口和再出口
六	向禁运目的地出口或再出口
七	支持扩散活动（美国人员扩散活动）
八	通过特定国家转运或正在转运
九	违反任何许可证或许可证例外的命令、条款或条件
十	明知正在违反或即将违反规定的情况下继续进行交易

Entity List

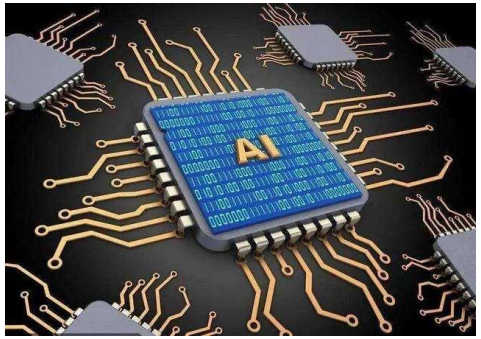
- 在出口管制方面，美国已经形成一套由商务部、能源部和国务院组成的清单管理制度，该制度也是美国实施出口管制最重要的执法工具之一。美国商务部主管出口管制的机构是产业安全局

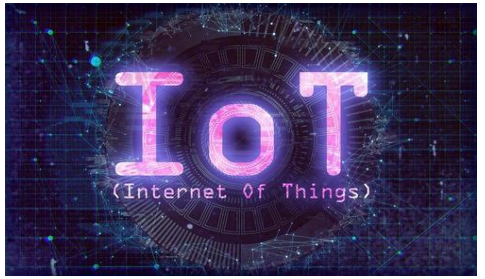
清单 类别	被拒绝清单(Denied Persons List)	实体清单(Entity List)	未经核实清单(UVL)	特别指定国民名单（SDN List）
管理机构	BIS	BIS	BIS	美国财政部海外资产管理办公室（OFAC）
被列入原因	违反任何EAR, IEEPA[5],ISA[6], AECA[7]中的管制规定[8]	存在BIS认定的严重违反美国国家安全和/或外交政策利益的活动[9]	BIS无法完成相应的最终用途审核以确认该类实体的善意使用	被列入SDN List可能有多种原因，包括但不限于支持恐怖活动、麻醉品贩卖等原因；以及因违反美国的制裁法律而被制裁
列入后果	不得以任何方式直接或间接，参与涉及从美国出口或将从美国出口受EAR约束的任何商品、软件或技术的任何交易或受EAR约束的任何其他活动（包括ECCN物项以及EAR99物项）等	对其设置特定的许可证要求，绝大多数为“推定拒绝”（Denial of presumption）	不再适用许可证例外；需要事先在AES申报；对不需要许可证的物项也需要事先获得所有交易方的最终用途和最终用户申明（UVL Statement）	包括一级制裁和次级制裁两种结果。一级制裁是美国由于直接具有管辖权而实施的制裁，直接限制或禁止美国人(定义广泛)与SDN List上实体的业务活动。次级制裁则是指非美国人与SDN实体进行交易在特定情形下被美国政府实施制裁

应用强国缺乏安全精品

中国是网络应用大国

但网络强国?





安全问题 关系到国家安危

2013年6月，斯诺登将美国国家安全局关于PRISM监听项目的秘密文档披露给了《卫报》和《华盛顿邮报》，随即遭美国政府通缉，事发时人在香港，随后飞往俄罗斯。
2013年6月21日，斯诺登通过《卫报》再次曝光英国"颞颥"秘密情报监视项目。

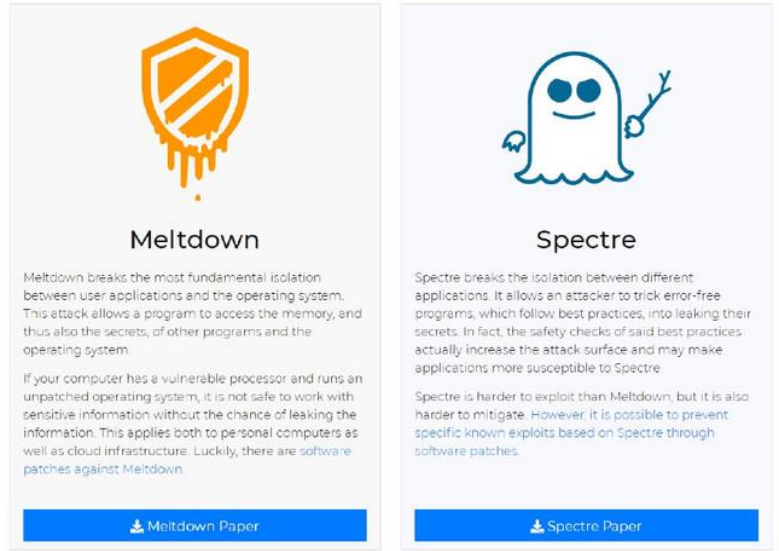
棱镜计划(PRISM)是一项由美国国家安全局(NSA)自2007年小布什时期起开始实施的绝密电子监听计划，该计划的正式名号为"US-984XN"。英国《卫报》和美国《华盛顿邮报》2013年6月6日报道，美国国家安全局(NSA)和联邦调查局(FBI)于2007年启动了一个代号为"棱镜"的秘密监控项目，直接进入美国网际网络公司的中心服务器里挖掘数据、收集情报，包括微软、雅虎、谷歌、苹果等在内的9家国际网络巨头皆参与其中。

斯诺登向德国《明镜》周刊提供的文件表明:美国针对中国进行大规模网络进攻，并把中国领导人和华为公司列为目标。攻击的目标还包括商务部、外交部、银行和电信公司等。
美国国家安全局对部分中国企业进行攻击和监听。例如为了追踪中国军方，美国国家安全局入侵了中国两家大型移动通信网络公司。因为担心华为在其设备中植入后门，美国国家安全局攻击并监听了华为公司网络，获得了客户资料、内部培训文件、内部电子邮件、甚至还有个别产品源代码。
美国国家安全局还对中国顶尖高等学府清华大学的主干网络发起大规模的黑客攻击。其中2013年1月的一次攻击中，至少63部电脑和服务器被黑。中国六大骨干网之一的"中国教育和科研计算机网"就设在清华大学，清华的主干网络被黑，意味着数百万中国公民的网络数据可能失窃。

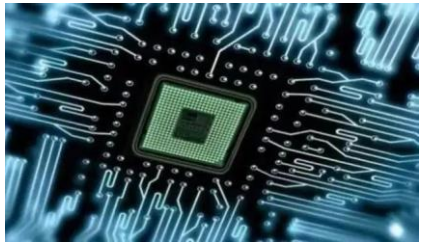
安全问题 关系到国家安危

全球最大计算机芯片制造商英特尔(Intel)的产品，2017年1月3日被爆出在安全漏洞，处理器内核内存的数据可能遭黑客窃取，令用户的密码等敏感数据外泄
除了inter确认波及到ARM和AMD（目前使用的手机CPU架构基本上全部是ARM，苹果/高通/华为等所使用的CPU全部都是基于ARM架构上做了自己的优化和改进），也就是说，近二十年来生产的几乎一切手机、电脑、云计算产品都在风险之列。
安全人员将两个新的漏洞命名为Meltdown（熔断）和Spectre（幽灵）。

Meltdown（熔断）允许低权限、用户级别的应用程序“越界”访问系统级的内存，从而造成数据泄露。
Spectre（幽灵）则可以骗过安全检查程序，使得应用程序访问内存的任意位置。
目前，Meltdown已经被Linux、macOS修复，谷歌也号称修复（应该是安卓），至于Windows，解释如下:
不过，Spectre由于复杂度更高、极为顽固，暂时还无解，修复正在进行中。
除了给消费者带来麻烦外，有许多云服务使用Intel的服务器，它们也会受到影响，亚马逊、微软、谷歌已经行动起来，给云服务打补丁，按计划中断服务，防止攻击者窃取数据，攻击者可能会在相同的共享云服务器上窃取其它数据。



认识差距 承认差距

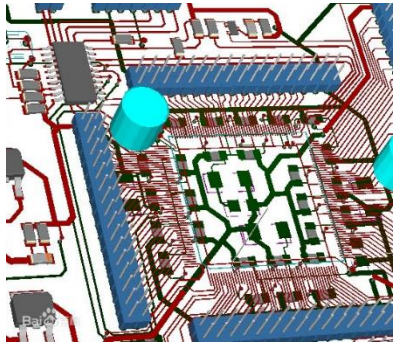


芯片

光刻机

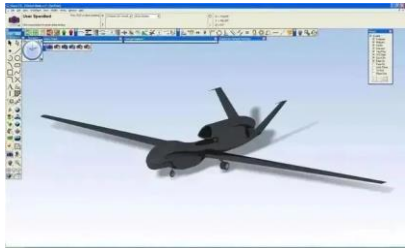
操作系统

光刻胶

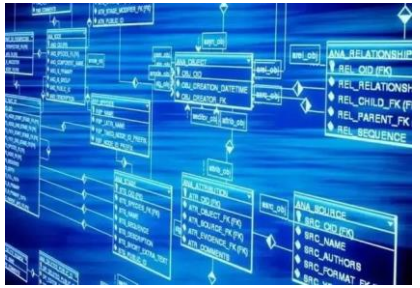


电子设计自动化EDA

高端电容电阻



设计软件



数据库管理系统

性能不足

边界安全产品的性能无法和路由交换设备相比，是否会成为网络的瓶颈?

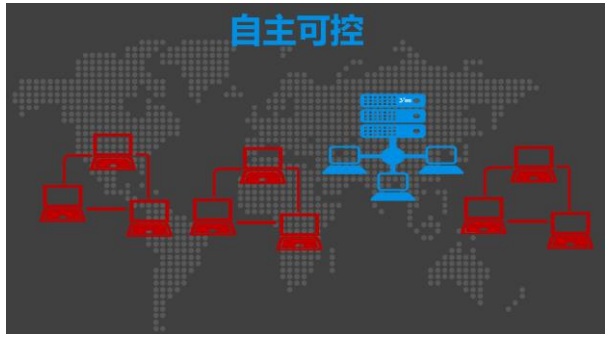
性能要求越来越高，刚买的设备几年就过时了?

私有云环境下，如何做到流量可视以及保障东西向流量的安全?

海量的数据访问，如何满足监管的需求溯源问题的用户?

边界安全产品是否会成为故障点，可靠性如何保障?

企业网络的应用层安全如何保障?



边界安全产品如何响应国家国产化的号召?

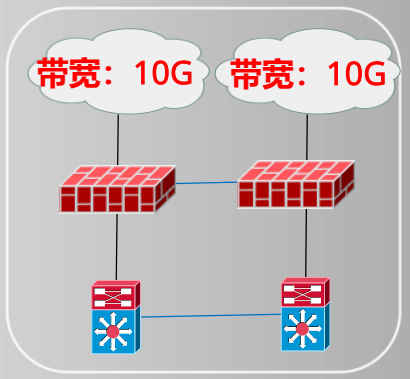
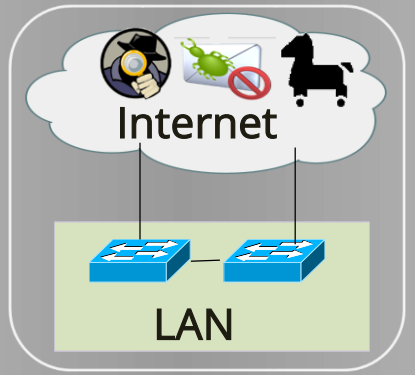
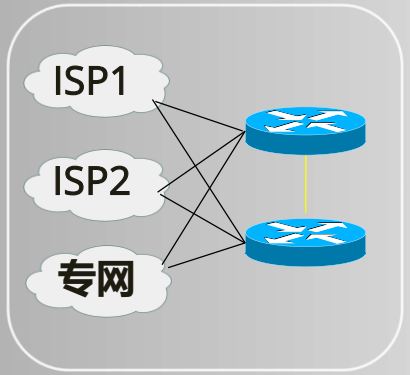
供应链不安全

国产化需求背景

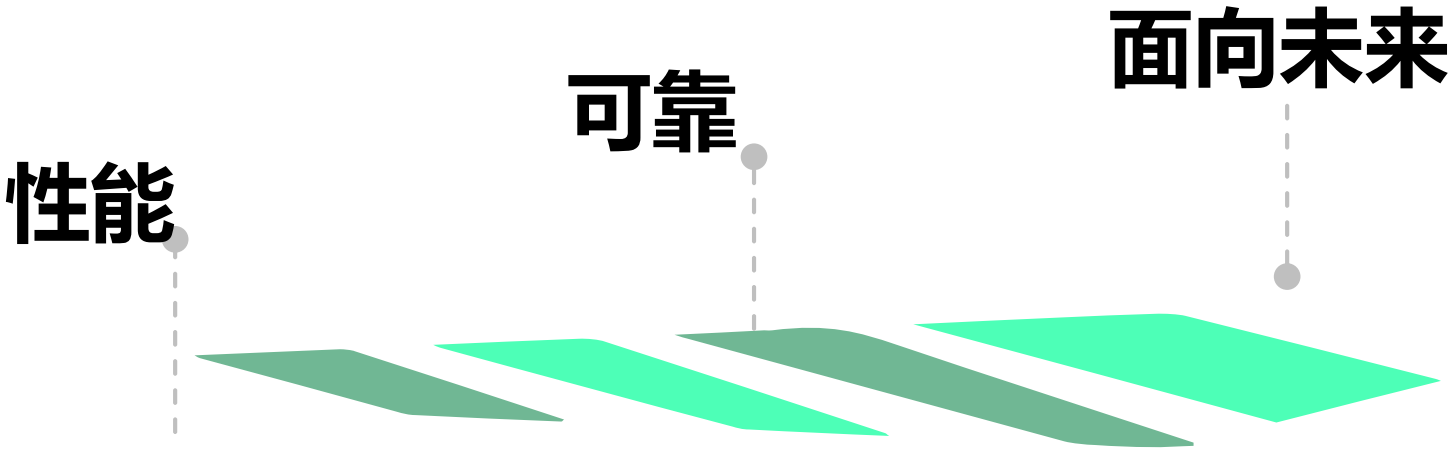
- **安全需求：**棱镜门事件，网络监听，CPU等硬件后门问题日益突出。
- **政策要求：**网络安全即国家安全，国家及行业政策要求产品国产化，如军工，电力行业强制执行。
- **芯片受控：**中兴禁售令事件的反思，芯片大多数都是国外进口，产品的生产、研发完全被国外公司控制。

最核心的CPU始终未摆脱对国外技术的依赖，从CPU指令集、CPU内核、制造三个维度来看，依赖程度逐一提高，制造方面的核心技术装备基本掌握在国外公司手中。

设备综合防护效果差

下一代互联网	高带宽、大流量	网络威胁泛滥	多运营商出口	各类日志审计
				
如何防御 IPv6 时代安全威胁?	如何保障同时开启多种安全功能下的数据转发性能?	如何有效抵御各类应用层网络攻击?	如何有效利用带宽资源?	如何对越权操作和泄密行为进行监管?

我们需要什么样的产品



网络安全国产化 势在必行

“实践反复告诉我们

关键核心技术是要不来、买不来、讨不来的。”

即使能要来买来讨来，关键核心技术依然是
理解不了的，也消化不了的

研发更高性能设备


○整机吞吐能力
○应用层吞吐能力
○新建连接能力
○硬件加解密能力
○并发连接能力
○入侵检测防御能力
基于自主创新技术，国内厂商需加大研发力度，缩小与世界一流产品的差距。

采用国产关键元器件提升供应链安全

保障供应链安全需依靠自身研发设计，全面掌握产品核心技术，实现信息系统从硬件到软件的自主研发、生产、升级、维护的全程可控。

作为整机厂商应采用国家认可的基础软硬件厂商的元器件及软件产品，如：

- 核心芯片：兆芯、龙芯、申威、飞腾等
- 操作系统：中标麒麟、天津麒麟、中科方德等

提升综合防护能力

1. ○ 平滑过渡IPv6，并保持原有的性能、功能
2. ○ 采用高性能或多处理器满足同时开启多功能后的高性能
3. ○ 防护未知威胁、异常行为、0-Day漏洞攻击等新型攻击

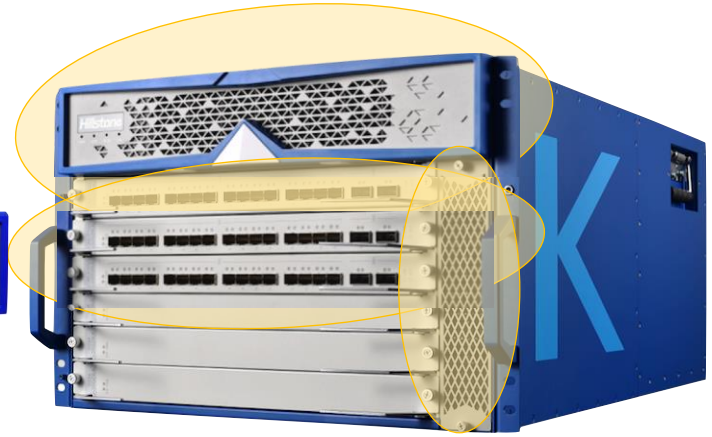
4. ○ 日志审计满足合规要求
5. ○ 硬件级冗余、扩展架构设计提升可靠、稳定性

K9180 打造国产芯片高性能安全平台“芯”高度

- 吞吐量300Gbps，并发连接数1**亿**
- 关键元器件**国产化**，**自主知识产权**操作系统
- **全分布式架构**，机框式扩展设计，整机最大支持高达20**颗国产**CPU协同工作。
- 硬件**设计**、**生产**全流程国产化
- 硬件全冗余的**电信级**99.999%**高可靠**

硬件自主设计研发保障更高可靠性

前后通风符合新一代数据中心
散热设计要求



N+M冗余电源，降额设计
保证至少50%余量的电源高可靠

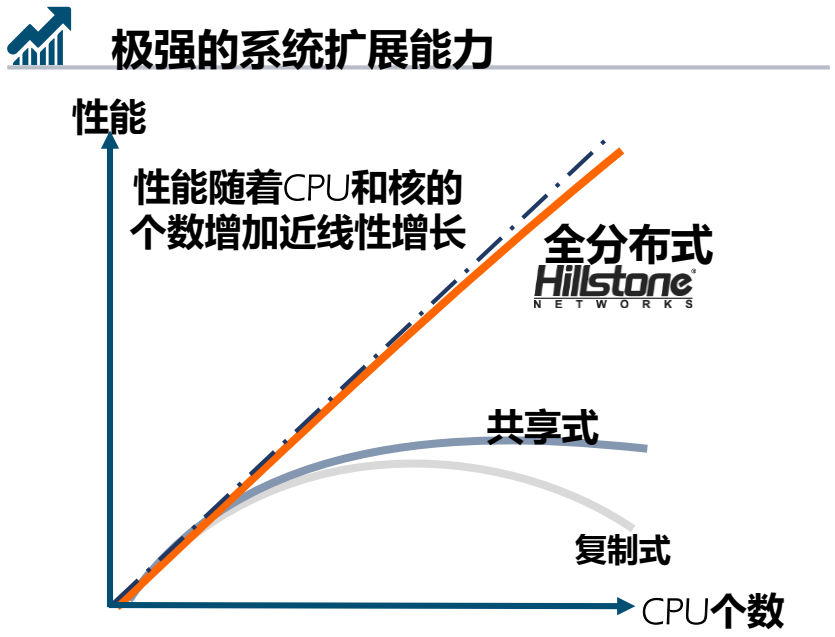
所有板卡、电源支持热插拔和在线更
换，交换板主控板冗余

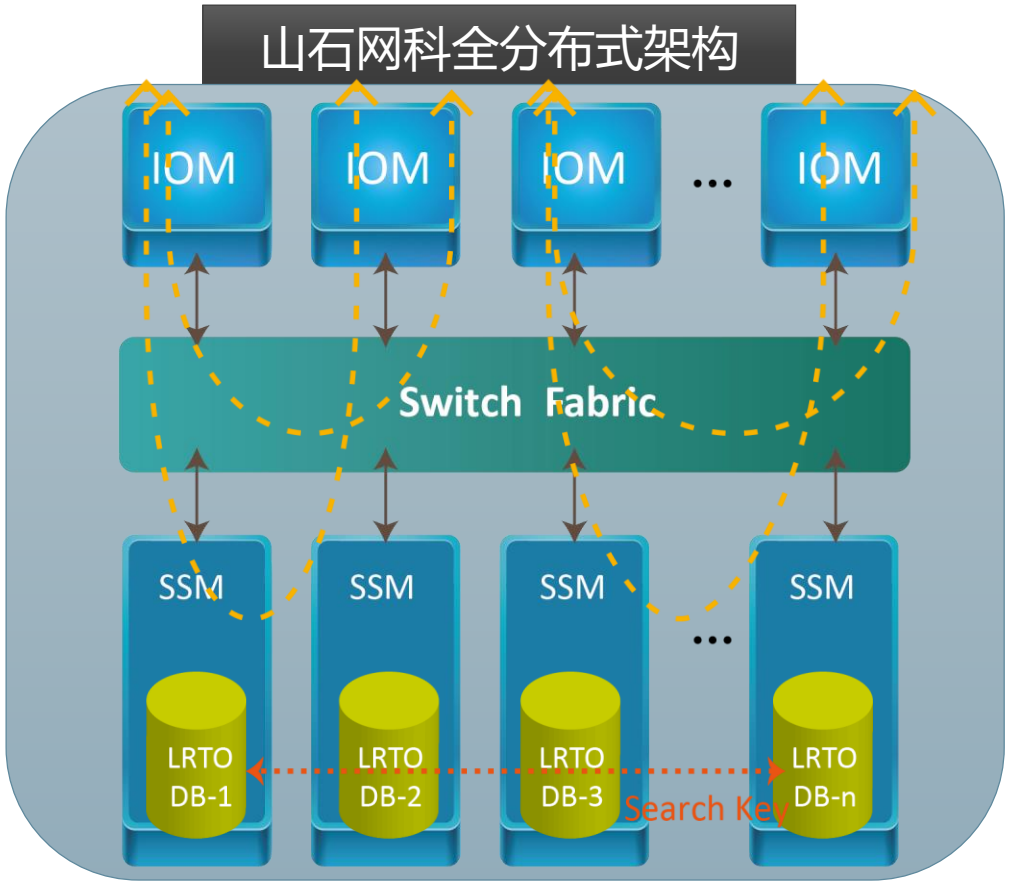
模块化、可扩展的机箱结构设计，
提供高速率、高密度网络接口，
更利于设计冗余网络

冗余风扇盘，每个风扇盘10
个长效风扇,支持在线更换

硬核科技1：多处理器全分布式并行构架

单系统支持20个8核通用处理器





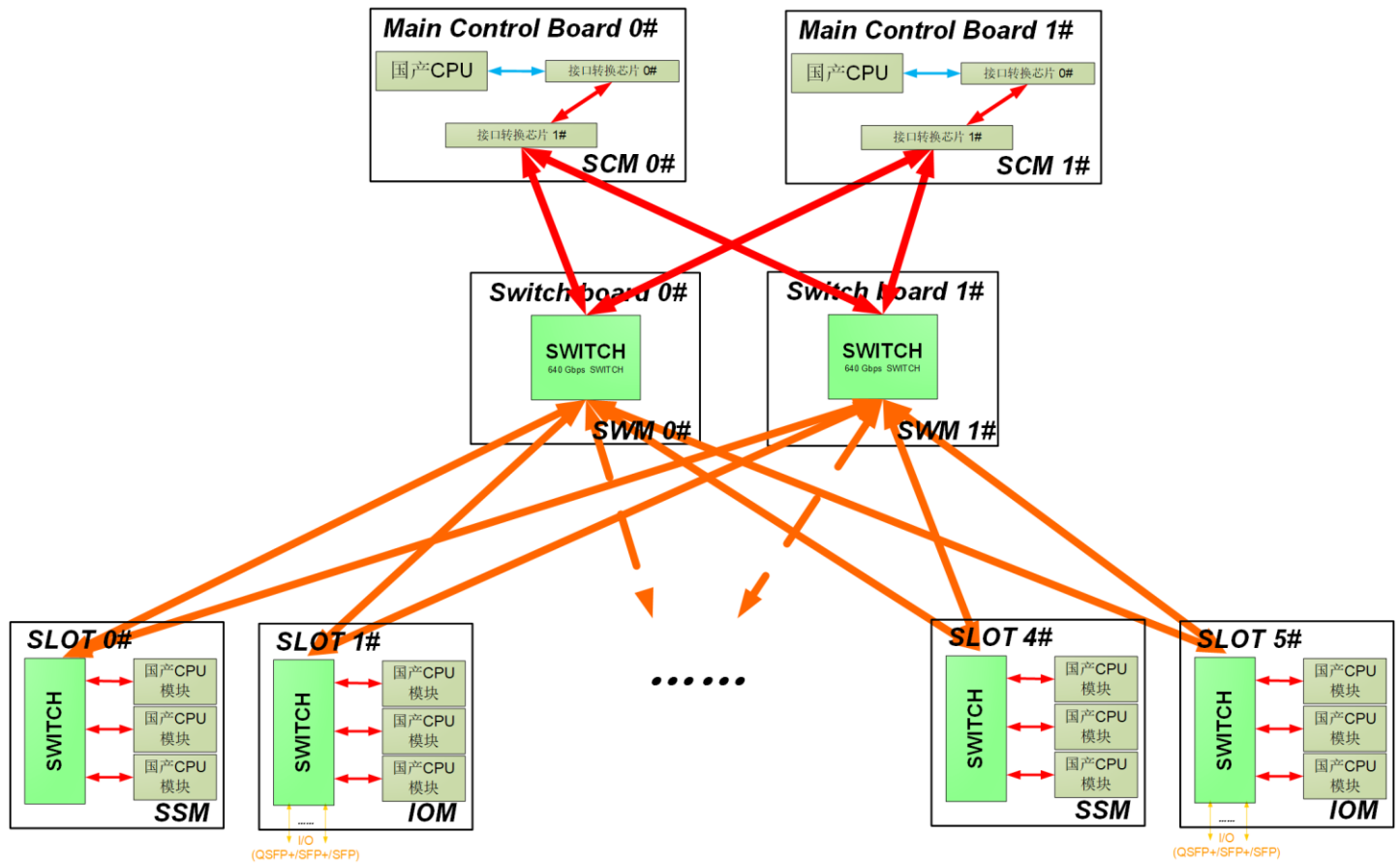
硬核科技2：分布式全交换架构

冗余交换

硬件、软件支持热插拔

整机交换容量1.28Tbps

可扩展为2.56Tbps



呼吁

少些浮夸 多些务实
少些口号 多些行动

把精力放在解决卡脖子问题上，不要放在怎么限制友商上
用合作的心态解决安全问题，而不要想怎么独占市场

优势互补促进产业协同

2020北京网络安全大会

2020 BEIJING CYBER SECURITY CONFERENCE

THANKS

全球网络安全 倾听北京声音