网络运维

- 要保证网络各项功能正常运行，需要对网络进行日常维护和故障处理，日常维护是预防性的有计划的维护工作，而故障处理则是基于事件触发的维护工作。
- 良好的日常维护习惯能帮助网络工程师及时发现隐患，做到防患于未然。当设备出现异常或故障时，网络工程师需要及时准确地收集设备运行过程中发生的事件。日常维护和故障处理都离不开网络相关的信息收集。
- 本课程介绍日常维护的注意事项、信息收集常用的工具。

网络维护概述

- 网络的生命周期大致包括了网络规划与设计、网络实施、网络维护及优化等阶段。网络维护可以分为两类：日常维护和故障排除。
- 日常维护是为了预防问题发生，尽量减少突发的故障。从故障排除工作中找到的问题原因，可为日常维护工作提供参考。
- 网络维护不仅仅是技术问题，而且也是管理问题。日常维护对操作人员的技术要求不高，但对操作的规范性要求比较高。通过日常维护可以得出网络在正常情况下的各种参数，例如网络设备的版本、网络带宽、网络安全等，从而为故障排除工作打下良好的基础。

- 维护又有“运维”、“运营”、“操作与维护”等不同的叫法，但表达的是同一个概念。
- 网络规划是一个项目的起点，完善细致的规划工作将为后续的项目具体工作打下坚实的基础。具体的工作内容如下：
- 在项目规划阶段需要调查掌握项目的背景。为项目实施提供良好的外部条件，保证项目的顺利推进。

- 在项目规划阶段需要明确网络项目的实施工作范围。
- 需要根据项目目标，工程范围，工作内容等各方面的内容制订项目的预算。
- 在项目规划阶段需要明确网络设计的指导思想，为后续的网络设计提供指导和依据。
- 网络设计阶段负责把网络规划阶段获得的客户需求运用技术手段予以规范化体现。网络设计过程中，设计的网络方案需要把握以下要点：
- 高性能：需要与经济性取得平衡。网络的性能常用可用带宽，延迟，抖动，误码率，利用效率等进行描述。
- 经济性：首先需要遵从客户的预算，在预算范围内提供匹配的解决方案。
- 可靠性：使用平均故障间隔时间 MTBF（Mean Time Between Failures）和平均修复时间 MTTR（Mean Time to Repair）这两个技术指标来评价系统的可靠性。
- MTBF 是指一个系统无故障运行的平均时间，通常以小时为单位。MTBF 越多，可靠性也就越高。
- MTTR 是指一个系统从故障发生到恢复所需的平均时间。
- 扩展性：指网络适应未来发展的能力。
- 安全性：网络设计中需要考虑安全性，以提高网络的持续服务能力，防止承载信息的泄密。
- 可管理性：网络管理包括设备管理，配置管理，故障管理，计费管理等多个方面。
- 网络实施是工程师交付项目的具体操作环节。
- 故障排除的流程将在下个章节中详细介绍。

日常维护 - 内容和方法

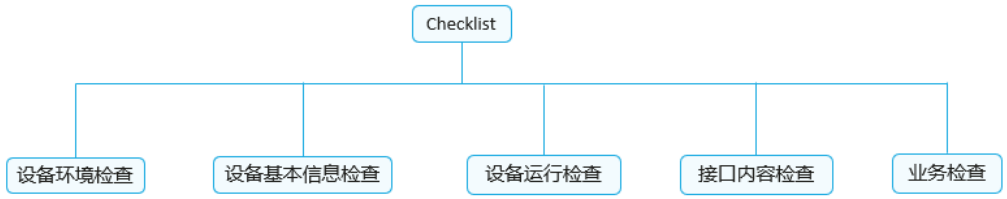
- 日常维护分为设备环境维护和设备软硬件维护两大部分。
- 设备运行环境：
- 硬件运行环境是指设备运行的机房、供电、散热等外部

环境，这是设备运行的基础条件。

- 对于设备环境的维护，工作人员需要亲临现场，甚至借助一些专业工具进行观察、测量。
- 设备软硬件运行情况：
- 设备软硬件运行情况与设备运行的具体业务密切相关。华为数通设备使用了通用的 VRP 平台，网络工程师应该掌握 VRP 平台的常用维护命令。
- 对于设备软硬件的维护，工作人员可以现场操作，也可以远程操作，主要通过设备的 display 命令实现。
- 日常维护可以使用以下两种方法：
- 现场观测 ：观察设备硬件运行环境。
- 远程操作：了解设备软硬件运行情况。

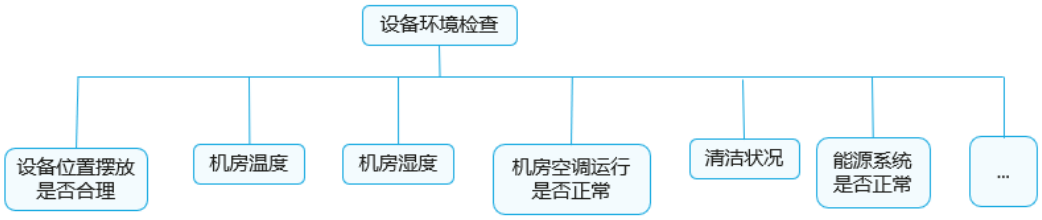
日常维护 - Checklist

日常维护工作是有计划的例行工作，因此，针对各项操作整理一份操作清单（Checklist）是十分必要的。不同网络设备的Checklist可以参考相应的产品文档。日常维护检查的项目也可由客户自定义。



Checklist - 设备环境检查 (1)

- 设备运行环境正常是保证设备正常运行的前提。
- 然而实际工作的时候，当有故障发生，并不会第一时间检查设备环境，因为设备环境相比较其他的因素来说，更加的稳定和不容易发生故障。



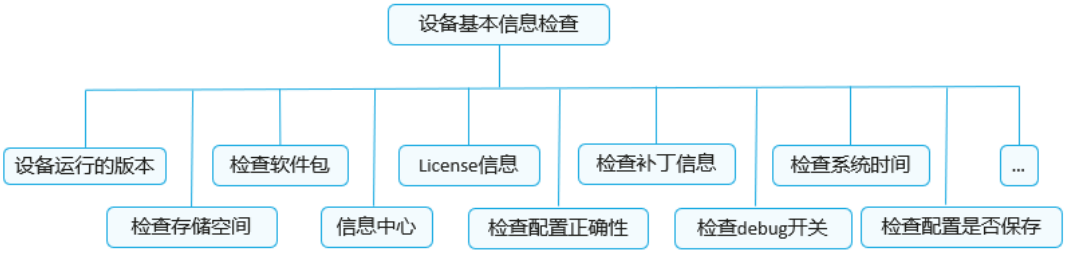
Checklist - 设备环境检查 (2)

检查项	方法/工具	评估标准和说明
设备摆放位置	观察	设备应放在通风、干燥的环境中，且放置位置牢固、平整。设备周围不得有杂物堆积。
机房温度状况	观察/温度计	通常要求机房长期工作环境温度：0℃~45℃；短期工作环境温度：-5℃~55℃。
机房湿度状况	观察/湿度计	通常机房的长期工作环境相对湿度应在5%RH~85%RH之间，不结露；短期工作环境相对湿度应在0%RH~95%RH之间，不结露。
机房内空调运行是否正常	观察/空调	空调可持续稳定运行，使机房的温度和湿度保持在设备规定范围内。
清洁状况	观察	所有项目都应干净整洁无明显尘土附着。注意防尘网的清洁状况，及时清洗或更换，以免影响机柜门及风扇框的通风、散热。
散热情况	观察	设备正常工作时，要求保持风扇正常运转（清理风扇期间除外），擅自关闭风扇会引起设备温度升高，并可能损坏单板。不要在设备子架上通风口处放置杂物，还应定期清理风扇的防尘网。
线缆布放	观察	电源线与业务线缆分开布放。电源线布放整齐、有序。业务线缆布放整齐、有序。 线缆标签清晰、准确，符合规范。
接地方式及接地电阻是否符合要求	观察	一般要求机房的工作地、保护地、建筑防雷地分开设置，因机房条件限制，可采用联合接地。尤其对于户外使用的设备，设备接地非常重要，如果未接地容易造成雷击损坏。
供电系统是否正常	观察/电压表	要求供电系统运行稳定。直流额定电压范围为-48V DC~-60V。交流额定电压范围为100V~240V。
...	...	...

- 设备运行环境正常是保证设备正常运行的前提。
- 温度和湿度对设备正常运行有重大影响，标准的机房都应该配备温度计和湿度计，并且应每天安排人员例行检查和记录。
- 机房的清洁和整齐也影响着设备的正常运行。
- 清洁问题影响设备的散热。
- 整齐主要是指设备、线缆的布放。按照规范的安装部署要求，设备和线缆都需要规范布放。但是在网络运行过程中，时常会有临时的调整，比如临时跳线测试。这些活动积累一段时间后，机房就会变乱。设备环境检查就是发现这些问题并及时纠正。
- 另一方面，非标准的机房更要注意设备环境检查，比如楼层的设备间，需要特别注意清洁和散热问题。
- 以上各种参数不同设备可能有所差异，以各自产品文档为准。

Checklist - 设备基本信息检查(1)

设备基本信息检查包括软件版本检查、License检查、设备存储空间等信息。



Checklist - 设备基本信息检查(2)

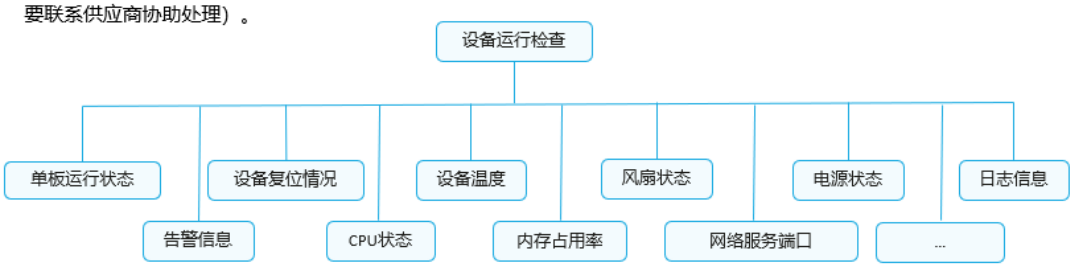
检查项	检查方法	评估标准
设备运行的版本	display version	单板PCB版本号、软件版本号与要求相符。
检查软件包	display startup	检查下述系统文件名是否正确： 当前启动大包名；下次启动大包名；备份大包名；配置、许可文件、补丁、当前启动文件名和下次启动文件名。
License信息	display license display license state	查看GTL License文件名、版本及配置项是否符合要求，确认是否需要升级。 “Master board license state”项为“Normal”。“Master board license state”项为“Demo”或“Trial”时，确认License在有效期内。
检查补丁信息	display patch-information	补丁文件必须与实际要求一致，建议加载华为公司发布的该产品版本对应的最新的补丁文件。 补丁必须已经生效，即补丁的总数量和正在运行的补丁数量一致。
检查系统时间	display clock	系统时间需要与网络管理服务器的时间保持一致（误差不超过5分钟）。
检查Flash/SD卡/CF卡空间	dir flash、dir slave#cfcard	Flash/SD卡/CF卡里的文件都必须是有用的，否则请在用户视图下执行delete/unreserved命令删除。
信息中心	display info-center	“Information Center”项为“enabled”。
检查配置正确性	display current-configuration	通过查看当前生效的配置参数，验证设备配置是否正确。
检查debug开关	display debugging	设备正常运行时debug开关应该全部关闭。
检查配置是否保存	compare configuration	当前的配置和下次启动的配置文件内容一致。
...	...	...

- 关于设备运行的软件版本：
- 设备运行版本在项目建设时就应确认，正常情况下版本信息不会变化。在检查过程中若发现版本信息有变化，应重点关注。这种情况通常是由于不规范的管理造成的。
- 如果是新添加的设备，可能采用不同的软件版本；也有可能由于其他原因升级或降级了部分设备。特别是在网络规模较大的场景下，网络中同一款设备可能运行不同版本的软件。这时就需要重点关注不同版本是否能够满足同样的网络功能需求。
- 关于启动信息：

- 设备上可能存在多个版本或多个配置文件，这种情况下冒然变更启动信息的会对网络的正常运行造成较大的风险。设备一旦重启（比如供电故障），则可能影响整个网络的运行。
- 关于 License 信息：
- 不同设备的 License 规则可能不同，需要区别对待。某些设备的 License 是有期限的，需要重点关注。
- 关于存储空间：
- 尽管大部分设备提供了数十 G 甚至数百 G 的存储空间，但是由于设备运行过程中会不断生成一些文件，如日志文件等。在某些异常情况下，如设备遭受攻击或设备信息频繁变更时，日志文件会急剧增加，如果这种现象持续存在，就可能会导致设备的存储空间耗尽、关键信息丢失。

Checklist - 设备运行状态检查(1)

- 在进行设备运行状态检查时，重点关注设备硬件的运行状态，如板卡、电源、风扇、温度、CPU、内存等。一般设备上都设置了告警灯，通常硬件故障都会导致告警灯亮（具体状态因产品而异）。因此，也可以通过现场观察发现设备运行异常状态。
- 对于板卡、电源、风扇等部件的运行状态，应遵照厂商的相关指导进行判断，有必要时联系厂商进行指导。如果确认为硬件故障，可以联系供应商处理（由于不同项目、不同设备的维保方案不同，有的硬件故障可直接联系厂商更换，有的则需要联系供应商协助处理）。



Checklist - 设备运行状态检查(2)

检查项	检查方法	评估标准
单板运行状态	display device	重点关注单板在位信息及状态信息是否正常。 单板“Online”为“Present”；单板“Power”为“PowerOn”；单板“Register”为“Registered”； 单板“Alarm”为“Normal”。
设备复位情况	display reset-reason、display reboot-info	通过查看复位信息（包括复位时间、复位原因），确认无非正常复位。
设备温度	display temperature、display environment	各模块当前的温度应该在上下限之间。
风扇状态	display fan	Present项为YES表示正常。
电源状态	display power	State项为Supply表示正常。
FTP网络服务端口	display ftp-server	不使用的FTP网络服务端口要关闭。
告警信息	display alarm all	无告警信息。如果有告警，需要记录，对于严重以上告警需并立即分析并处理。
CPU状态	display cpu-usage	各模块的CPU占用率正常。如果CPU占用率如果超过80%，建议重点关注。
内存占用率	display memory-usage	内存占用情况正常，如果“Memory Using Percentage Is”超过60%时需要关注。
日志信息	display logbuffer、display trapbuffer	不存在异常信息。
主用板/备用板的备份状态	display switchover state	主备板同时存在时，要同时有主备板的显示状态信息。倒换完成，设备开始正常工作后，主用板需要显示为“realtime or routine backup”表示正常。
…	…	…

Checklist - 设备接口内容检查

- 网络设备通过接口来交换数据报文。因此，接口的信息非常重要。接口状态异常会影响到网络的功能。
- 接口如果出现大量错包，并且在短时间内不断增加，通常是由于链路（包括物理接口）的问题造成的。

检查项	检查方法	评估标准
接口错包	display interface	业务运行时，要检查接口有无错包，包括CRC错包等。
接口协商模式	display interface	接口协商模式正确，两边接口要一致，不能有半双工模式。
接口配置	display current-configuration interface	接口的配置项合理，如接口双工模式、协商模式、速率、环回配置等。
接口状态	display interface brief	接口的Up/Down状态满足规划要求。接口的收发流量是否过大？（长期超过70%）
PoE供电	display poe power-state interface interface-type interface-number	PoE供电状态正常，“Port power ON/OFF”为“ON”的接口，其“Port power status”为“Delivering-power”。
…	…	…

Checklist - 业务运行状态检查

业务运行状态主要是指网络协议的运行状态。

检查项	检查方法	评估标准
MAC地址表信息	display mac-address	MAC地址表信息正确
VLAN信息	display vlan	查看所有VLAN的基本信息
路由表信息	display ip routing-table	具有默认路由或者其他精确路由，便于故障时候可以远程定位 对于处于一个网络中同一层次的设备，如果运行相同的路由协议，各设备上的路由条目应该相差不大（因为静态路由的配置差异，路由条目上可能存在一定差异）
OSPF邻居状态 IS-IS邻居状态 BGP邻居状态	display ospf peer display isis peer display bgp peer	OSPF邻居状态：邻居状态“State”为“Full”或者”2-Way” IS-IS邻居状态：邻居状态“State”为“Up” BGP邻居状态：邻居状态“State”为“Established”
VRRP状态	display vrrp display vrrp statistics	备份组中的设备的VRRP状态“State”不能同时为“Master”
MSTP状态	display stp brief	指定端口和根端口的“STP State”为“FORWARDING”
…	…	…

日常维护 - 软件与配置的备份

- 备份的目的是为了在极端情况下恢复网络功能。备份的实质是把对应的文件传输到备份服务器上，因此方法有很多。通常将设备作为 FTP 或 TFTP 客户端，通过命令行将相应的文件传输到服务器上。
- 对于配置文件的备份，建议每周例行进行；同时在设备的配置有变更之前，应进行配置文件的备份。
- 软件与配置（包括 License 文件）都需要备份。备份的目的是为了在极端情况下恢复网络功能。
- 当设备因硬件故障无法启动，或更换同型号的设备后，如果没有备份的配置文件，业务将很难快速恢复。
- 软件版本也有必要备份，但同一个产品、同一个版本只需要备份一次即可；也可以从厂商官网获取对应的版本文件保存到本地。
- License 文件是一类特殊的文件，它针对具体的产品进行了设置，一旦意外丢失（如误删除），则需要经过厂商的流程重新申请，通常这个流程需要提供一些证明材料（如合同号，设备 SN 等），因此申请周期也会比较长。如果有备份的 License 文件则可以快速地恢复到设备上。

信息中心简介

- 信息中心是设备的信息枢纽。设备产生的Log、Trap和Debug信息统一发往信息中心，通过信息中心的统一管理和控制，实现信息的灵活输出。
- 通过配置信息中心，对设备产生的信息按照信息类型、严重级别等进行分类或筛选，用户可以灵活地控制信息输出到不同的输出方向（例如，控制台、用户终端、日志主机等）。这样，用户或网络管理员可以从不同的方向收集设备产生的信息，方便监控设备运行状态和定位故障。

信息类型	内容描述
Log信息	Log信息主要记录用户操作、系统故障、系统安全等信息： 用户日志：记录用户操作和系统运行信息。 安全日志：记录包含账号管理、协议、防攻击和状态等内容的信息。 诊断日志：记录协助进行问题定位的信息。
Trap信息	Trap信息是系统检测到故障而产生的通知，主要记录故障等系统状态信息。 这类信息不同于Log信息，其最大特点是需要及时通知、提醒管理用户和对时间敏感。
Debug信息	Debug信息是系统对设备内部运行的信息的输出，主要用于跟踪设备内部运行的状态。 只有在设备上打开相应模块的调试开关，设备才能产生Debug信息。

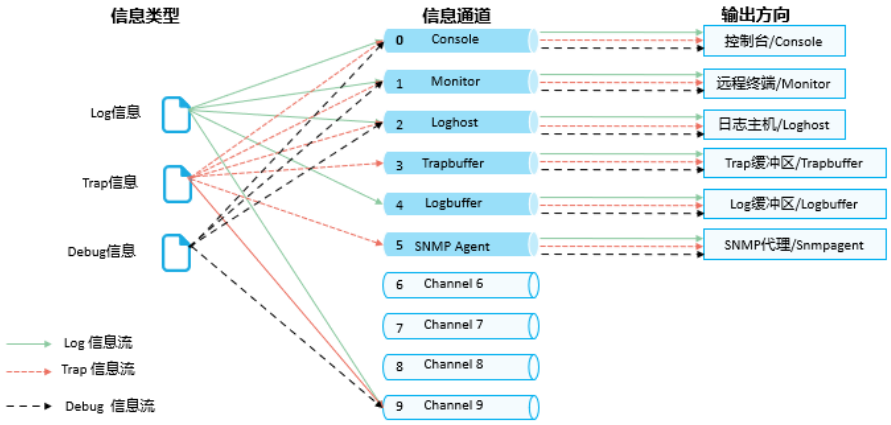
信息的分级

- 设备产生信息比较多时，用户较难分辨哪些是设备正常运转的信息，哪些是出现故障需要处理的信息。对信息进行分级，用户可以根据信息的级别进行粗略判断，及时采取措施，屏蔽无需处理的信息。
- 根据信息的严重等级或紧急程度，信息分为8个等级，信息越严重，其严重等级阈值越小。

显示值	严重等级	描述
0	Emergencies	设备致命的异常，系统已经无法恢复正常，必须重启设备。
1	Alert	设备重大的异常，需要立即采取措施。如设备内存占用率达到极限等。
2	Critical	设备的异常，需要采取措施进行处理或原因分析。如设备内存占用率低于下限阈值和BFD探测出设备不可达等。
3	Error	错误的操作或设备的异常流程，不会影响后续业务，但是需要关注并分析原因。如用户的错误指令、用户密码错误和检测出错误协议报文等。
4	Warning	设备运转的异常点，可能引起业务故障，需要引起注意。如用户关闭路由进程、BFD探测的一次报文丢失和检测出错误协议报文等。
5	Notification	设备正常运转的关键操作信息。如端口shutdown、邻居发现和协议状态机的正常跳转等。
6	Informational	设备正常运转的一般性操作信息。如用户使用display命令等。
7	Debugging	设备正常运转的一般性信息，用户无需关注。

信息的输出

设备产生的信息可以向远程终端、控制台、Log缓冲区、日志文件、SNMP代理等方向输出信息。为了便于各个方向信息的输出控制，信息中心定义了10条信息通道，通道之间独立输出，互不影响。



- 用户可以根据自己的需要配置信息的输出规则，控制不同类别、不同等级的信息从不同的信息通道输出到不同的输出方向。
- 远程终端，即通过 VTY 登录设备的方式，可以接收 Log 信息、Trap 信息、Debug 信息，方便远程维护。

信息的过滤

- 为了使信息的输出控制更加灵活，信息中心提供了信息过滤的功能。设备正常运行后，各模块在业务处理时都会上报信息。当用户希望过滤某些不需要关注的业务模块/级别的信息时，可以配置信息在信息通道中的过滤功能。
- 信息中心通过信息过滤表实现信息在通道中的过滤。信息过滤表是根据信息分类、分级、来源对输出到各个方向的信息进行过滤的。
- 信息过滤表记录的内容如下所示：
- 信息模块号
- Log 信息输出开关状态

- Log 信息输出过滤级别
- Trap 信息输出开关状态
- Trap 信息输出过滤级别
- Debug 信息输出开关状态
- Debug 信息输出过滤级别

信息的输出格式

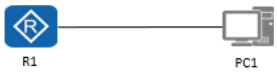
- Log信息的输出格式

<Int_16>	TimeStamp	TimeZone	HostName	%%	dd	ModuleName/	Severity/	Brief	(1)	[DDD]	:Description
1	2	3	4	5	6	7	8	9	10	11	12
前导符	时间戳	时区	主机名	华为标识	版本号	模块名	日志级别	信息摘要	日志标识	流水号	详细信息

- Trap信息的输出格式

#	TimeStamp	TimeZone	HostName	ModuleName/	Severity/	Brief	:Description
1	2	3	4	5	6	7	8
信息类型	时间戳	时区	主机名	模块名	告警级别	信息摘要	详细信息

信息中心的应用场景

向日志主机输出Log信息	向网管输出Trap信息	向控制台输出Debug信息
		
信息中心将指定级别的Log信息输出到日志主机中，维护人员通过查询日志信息，了解设备的运行情况。	信息中心向网管中心发送Trap信息，网管通过接收到的Trap信息，监控设备的运行状态。	信息中心向控制台发送Debug信息，维护人员通过Debug信息来了解设备的运行情况。

信息中心命令简介(1)

1. 使能信息中心功能。

   [HUAWEI] **info-center enable**

   缺省情况下，信息中心功能处于使能状态。

2. 为指定编号的信息通道命名。

   [HUAWEI] **info-center channel** *channel-number* **name** *channel-name*

3. 配置对指定的Log或Trap信息进行过滤的功能。

   [HUAWEI] **info-center filter-id** { *id* | **bymodule-alias** *modname alias* } [**bytime** *interval* | **bynumber** *number*]

   bymodule-alias，指定需要过滤的Log或Trap信息对应的模块名称。

4. 使能Log信息向Log缓冲区的发送功能。

   [HUAWEI] **info-center logbuffer**

   缺省情况下，Log信息向Log缓冲区的发送功能处于使能状态。

- 配置向日志主机输出信息。
- [HUAWEI] info-center loghost ip-address { source-ip source-ip-address } | transport { udp | tcp ssl-policy policy-name }]

信息中心命令简介(2)

1. 配置信息输出时所使用的信息通道。

   [HUAWEI] **info-center** { **console** | **logbuffer** | **logfile** | **monitor** | **snmp** | **trapbuffer** } **channel** { *channel-number* | *channel-name* }

2. 使能终端显示信息中心发送信息的功能。

   [HUAWEI] **terminal monitor**

   缺省情况下，控制台显示功能处于使能状态，用户终端显示功能处于未使能状态。

3. 使能终端显示Debug信息功能。

   [HUAWEI] **terminal debugging**

   缺省情况下，终端显示Debug信息功能处于未使能状态。

4. 使能终端显示Log信息功能。

   [HUAWEI] **terminal logging**

   缺省情况下，终端显示Log信息功能处于使能状态。

信息中心命令简介(3)

1. 查看Log缓冲区记录的信息。

   [HUAWEI] **display logbuffer** [**size** *size* | **slot** *slot-id* | **module** *module-name* | **security** | **level** { *severity* | *level* }]

2. 查看日志文件信息。

   [HUAWEI] **display logfile** *file-name* [*offset* | **hex**]

3. 查看信息中心Trap缓冲区记录的信息。

   [HUAWEI] **display trapbuffer**

4. 查看设备允许发送的调试信息。

   [HUAWEI] **display debugging**

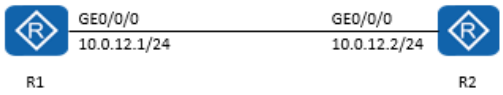
5. 查看信息中心输出方向的配置信息。

   [HUAWEI] **display info-center**

信息中心配置举例

R1和R2的GE0/0/0接口开启OSPF协议。通过Console端口登录R1，在R1设备上观察以下内容：

- Trap信息
- Log信息
- Debug信息




```
<R1> terminal monitor    //缺省情况下，控制台显示功能处于使能状态。
<R1> terminal logging    //缺省情况下，终端显示Log信息功能处于使能状态。
<R1> terminal debugging //缺省情况下，终端显示Debug信息功能处于未使能状态。
<R1> terminal trapping   //缺省情况下，终端显示Trap信息功能处于使能状态。
<R1> system-view
[R1] info-center enable  //缺省情况下，信息中心功能处于使能状态。
```

信息中心配置验证 – 信息通道

```
<R1> display channel
channel number: 0, channel name: console
MODU_ID   NAME      ENABLE  LOG_LEVEL     ENABLE  TRAP_LEVEL  ENABLE  DEBUG_LEVEL
ffff0000  default   Y       warning       Y       debugging   Y       debugging
channel number: 2, channel name: loghost
MODU_ID   NAME      ENABLE  LOG_LEVEL     ENABLE  TRAP_LEVEL  ENABLE  DEBUG_LEVEL
ffff0000  default   Y       informational Y       debugging   N       debugging
channel number: 3, channel name: trapbuffer
MODU_ID   NAME      ENABLE  LOG_LEVEL     ENABLE  TRAP_LEVEL  ENABLE  DEBUG_LEVEL
ffff0000  default   N       informational Y       debugging   N       debugging
channel number: 4, channel name: logbuffer
MODU_ID   NAME      ENABLE  LOG_LEVEL     ENABLE  TRAP_LEVEL  ENABLE  DEBUG_LEVEL
ffff0000  default   Y       warning       N       debugging   N       debugging
...       ...       ...     ...
```

R1设备存在4个通道分别是Console、Loghost、Trapbuffer、Logbuffer

根据信息的严重等级或紧急程度，信息分为8个等级，信息越严重，其严重等级阈值越小。

缺省情况下：

- Warning为第4级，设备运转的异常点，可能引起业务故障，需要引起注意。如用户关闭路由进程、BFD探测的一次报文丢失和检测出错误协议报文等。
- Debugging为第7级，设备正常运转的一般性信息，用户无需关注。

信息中心配置验证 - Trap

查看信息中心Trap缓冲区记录的信息。

```
<R1> display trapbuffer
Trapping buffer configuration and contents: enabled
Allowed max buffer size: 1024
Actual buffer size: 256
Channel number: 3, Channel name: trapbuffer
Dropped messages: 0
Overwritten messages: 0
Current messages: 1
#Jun 23 2020 08:38:51-08:00 R1 LLDP/4/ADDCHGTRAP:OID: [OID] Local management add
ress is changed. (LocManIPAddr=[IPADDR])
```

缺省情况下，Trap信息从缺省的3号信息通道输出。

信息中心配置验证 - Log

```
<R1> display log cli all
---------------------------------------------------------------------------
No.  UserName                Domain        IP-Address
 35                          --            Serial
Time: 2020-06-23 09:34:35-08:00
Cmd:  quit
---------------------------------------------------------------------------
No.  UserName                Domain        IP-Address
 34                          --            Serial
Time: 2020-06-23 09:34:33-08:00
Cmd:  ip address 10.0.12.1 24
---------------------------------------------------------------------------
No.  UserName                Domain        IP-Address
 33                          --            Serial
Time: 2020-06-23 09:34:29-08:00
Cmd:  interface gi 0/0/0
---------------------------------------------------------------------------
No.  UserName                Domain        IP-Address
 32                          --            Serial
Time: 2020-06-23 09:34:26-08:00
Cmd:  system-view
```

查看用户输入的所有命令。如上图所示，完成了R1的GE0/0/0接口IP地址配置。

```
<R1>
Jun 23 2020 10:09:57-08:00 R1 %%01OSPF/4/NBR_CHANGE_E(I)[0]:Neighbor changes event: neighbor status changed. (ProcessId=256,NeighborAddress=10.0.12.2, NeighborEvent=HelloReceived, NeighborPreviousState=Down, NeighborCurrentState=Init)
<R1>
Jun 23 2020 10:09:57-08:00 R1 %%01OSPF/4/NBR_CHANGE_E(I)[1]:Neighbor changes event: neighbor status changed. (ProcessId=256,NeighborAddress=10.0.12.2, NeighborEvent=2WayReceived, NeighborPreviousState=Init, NeighborCurrentState=2Way)
.....
<R1>
Jun 23 2020 10:09:57-08:00 R1 %%01OSPF/4/NBR_CHANGE_E(I)[5]:Neighbor changes event: neighbor status changed. (ProcessId=256,NeighborAddress=10.0.12.2, NeighborEvent=LoadingDone, NeighborPreviousState=Loading, NeighborCurrentState=Full)
```

R1的OSPF邻居状态变化以Log报文格式自动在Console界面输出。

信息中心配置验证 - Debug

```
<R1> debugging ospf packet
<R1>
Jun 23 2020 10:14:21.631.1-08:00 R1 RM/6/RMDEBUG:
 FileID: 0xd0178024 Line: 2236 Level: 0x20
 OSPF 1: RECV Packet. Interface: GigabitEthernet0/0/0
<R1>
<R1>Jun 23 2020 10:14:21.631.2-08:00 R1 RM/6/RMDEBUG:  Source Address: 10.0.12.2
<R1>Jun  23 2020 10:14:21.631.3-08:00 R1 RM/6/RMDEBUG:  Destination Address: 224.0.0.5
<R1>Jun  23 2020 10:14:21.631.4-08:00 R1 RM/6/RMDEBUG:  Ver# 2, Type: 1 (Hello)
<R1>Jun  23 2020 10:14:21.631.5-08:00 R1 RM/6/RMDEBUG:  Length: 48, Router: 10.0.2.2
<R1>Jun  23 2020 10:14:21.631.6-08:00 R1 RM/6/RMDEBUG:  Area: 0.0.0.0, Chksum: ae94
<R1>Jun  23 2020 10:14:21.631.7-08:00 R1 RM/6/RMDEBUG:  AuType: 00
<R1>Jun  23 2020 10:14:21.631.8-08:00 R1 RM/6/RMDEBUG:  Key(ascii): ********
<R1>Jun  23 2020 10:14:21.631.9-08:00 R1 RM/6/RMDEBUG:  Net Mask: 255.255.255.0
<R1>Jun  23 2020 10:14:21.631.10-08:00 R1 RM/6/RMDEBUG:  Hello Int: 10, Option: _E_
<R1>Jun  23 2020 10:14:21.631.11-08:00 R1 RM/6/RMDEBUG:  Rtr Priority: 1, Dead Int: 40
<R1>Jun  23 2020 10:14:21.631.12-08:00 R1 RM/6/RMDEBUG:  DR: 10.0.12.2
<R1>Jun  23 2020 10:14:21.631.13-08:00 R1 RM/6/RMDEBUG:  BDR: 10.0.12.1
<R1>Jun  23 2020 10:14:21.631.14-08:00 R1 RM/6/RMDEBUG:  # Attached Neighbors: 1
<R1>Jun 23 2020 10:14:21.631.15-08:00 R1 RM/6/RMDEBUG:   Neighbor: 10.0.12.1
```

R1从GE0/0/0接口收到了R2发送的HELLO报文，从中可以看到R2的接口IP地址，HELLO报文发送间隔、Router ID等信息。

注意：设备开启Debug功能可能会影响设备正常运行，请谨慎使用。

- 为了方便展示，本页展示的 Debug 信息做了调整。
- R1 从 GE0/0/0 接口发送的 HELLO 报文如下：

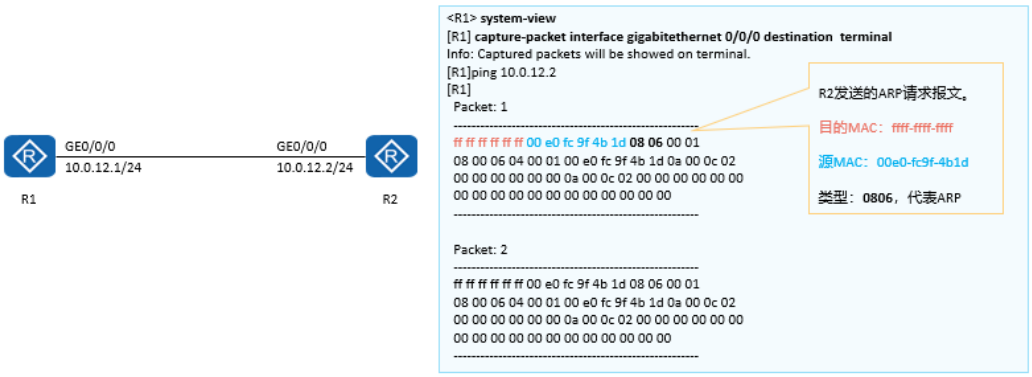
<R1>

Jun 23 2020 10:14:21.751.1-08:00 R1 RM/6/RMDEBUG:
 FileID: 0xd0178025 Line: 559 Level: 0x20
 OSPF 1: SEND Packet. Interface:
GigabitEthernet0/0/0

<R1>Jun 23 2020 10:14:21.751.2-08:00 R1
RM/6/RMDEBUG: Source Address: 10.0.12.1
<R1>Jun 23 2020 10:14:21.751.3-08:00 R1
RM/6/RMDEBUG: Destination Address: 224.0.0.5
<R1>Jun 23 2020 10:14:21.751.4-08:00 R1
RM/6/RMDEBUG: Ver# 2, Type: 1 (Hello)
<R1>Jun 23 2020 10:14:21.751.5-08:00 R1
RM/6/RMDEBUG: Length: 48, Router: 10.0.12.1
<R1>Jun 23 2020 10:14:21.751.6-08:00 R1
RM/6/RMDEBUG: Area: 0.0.0.0, Chksum: ae94
<R1>Jun 23 2020 10:14:21.751.7-08:00 R1
RM/6/RMDEBUG: AuType: 00
<R1>Jun 23 2020 10:14:21.751.8-08:00 R1
RM/6/RMDEBUG: Key(ascii): * * * * * * * *
<R1>Jun 23 2020 10:14:21.751.9-08:00 R1
RM/6/RMDEBUG: Net Mask: 255.255.255.0
<R1>Jun 23 2020 10:14:21.751.10-08:00 R1
RM/6/RMDEBUG: Hello Int: 10, Option: _E_
<R1>Jun 23 2020 10:14:21.751.11-08:00 R1
RM/6/RMDEBUG: Rtr Priority: 1, Dead Int: 40
<R1>Jun 23 2020 10:14:21.751.12-08:00 R1
RM/6/RMDEBUG: DR: 10.0.12.2
<R1>Jun 23 2020 10:14:21.751.13-08:00 R1
RM/6/RMDEBUG: BDR: 10.0.12.1
<R1>Jun 23 2020 10:14:21.751.14-08:00 R1
RM/6/RMDEBUG: # Attached Neighbors: 1
<R1>Jun 23 2020 10:14:21.751.15-08:00 R1
RM/6/RMDEBUG: Neighbor: 10.0.2.2
<R1>Jun 23 2020 10:14:21.751.16-08:00 R1
RM/6/RMDEBUG:

报文捕获

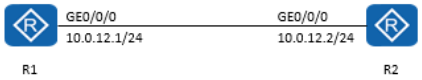
当设备的业务流量出现异常，比如流量状态与流量模型不符时，可以使用报文捕获功能，抓取业务报文进行分析，以便及时处理非法报文，保证网络数据的正常传输。



- 某个时刻只能有一个捕获报文实例，即前一次捕获报文流程没有结束，不能启动下一次捕获报文。
- 捕获的报文有速率限制，如果有突发流量，超过捕获报文的速率限制，可能会存在丢包现象。
- **capture-packet** 命令用来在设备捕获符合设置规则的业务报文，并上送到终端显示，或保存到本地。
- **capture-packet interface** *interface-type interface-number* [**acl** *acl-number*] **destination** { **terminal** | **file** *file-name* } * [**car cir** *car-value* | **time-out** *time* | **packet-num** *number* | **packet-len** { *length* | **total-packet** }] *
- **terminal** ：将捕获的报文发送到终端显示。
- **file** *file-name*：将捕获的报文保存在指定的文件里，

LLDP应用举例

- 链路层发现协议（LLDP，Link Layer Discovery Protocol）是IEEE 802.1ab中定义的链路层拓扑发现协议，它能够准确定位诸如哪些设备附带有哪些接口，以及哪些接口与其他设备相互连接等信息，并能够显示客户端、交换机、路由器、应用服务器和网络服务器之间的路径。
- 在实际组网中可以通过LLDP协议获取设备的物理连接信息。



在R1和R2设备上开启LLDP功能。

```
<R1> system-view
[R1] lldp enable
```

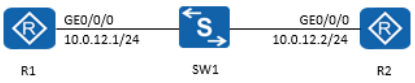
```
<R2> system-view
[R2] lldp enable
```

```
<R1> display lldp neighbor
GigabitEthernet0/0/0 has 1 neighbors:

Neighbor index          1
Chassis type            macAddress
Chassis ID              00e0-fc9f-4b1d
Port ID type            interfaceName
Port ID                 GigabitEthernet0/0/0
Port description        HUAWEI, AR Series, GigabitEthernet0/0/0 Interface
System name             R2
System description      Huawei AR2220 Huawei Versatile Routing Platform Software  VRP (R
                        software,Version 5.130 (AR2220 V200R003C00) Copyright (C) 2011-
                        2012 Huawei Technologies Co., Ltd

Management address type ipV4
Management address      10.0.12.2
Expired time            109s
```

从以上可以看出R1的GE0/0/0接口连接到了R2的GE0/0/0接口，且R2为AR2220系列路由器，接口的IP地址为10.0.12.2。

流量统计

流量可以帮助用户了解应用流策略后流量通过和被丢弃的情况，由此分析和判断流策略的应用是否合理，也有助于进行相关的故障诊断与排查。




```
1. 配置ACL规则
[R2] acl 2000
[R2-acl-basic-2000] rule permit source 10.0.12.1 0
[R2-acl-basic-2000] quit
2. 配置流分类
[R2] traffic classifier c1
[R2-classifier-c1] if-match acl 2000
[R2-classifier-c1] quit
3. 配置流行为
[R2] traffic behavior b1
[R2-behavior-b1] statistic enable
[R2-behavior-b1] quit
```

```
4. 创建流策略
[R2] traffic policy p1
[R2-trafficpolicy-p1] classifier c1 behavior b1
[R2-trafficpolicy-p1] quit
5. 在接口上应用流策略
[R2] interface GigabitEthernet 0/0/0
[R2-GigabitEthernet0/0/0] traffic-policy p1 inbound
[R2-GigabitEthernet0/0/0] quit
```

```
R2]display traffic policy statistics interface GigabitEthernet 0/0/0 inbound
 Interface: GigabitEthernet0/0/0
 Traffic policy inbound: test
 Rule number: 1
 Current status: OK!
 Item                Sum(Packets/Bytes)        Rate(pps/bps)
 ------------------------------------------------------------------------------
 Matched             0/0                       0/0
 Passed              0/0                       0/0
 Dropped             0/0                       0/0
 Filter              0/0                       0/0
 CAR                 0/0                       0/0
 Queue Matched       0/0                       0/0
```

从以上结果得知R2并未收到ICMP报文。据此信息可去排除是否物理链路故障，或者SW1的VLAN配置是否产生故障。

思考题：

- （多选题）关于网络维护的作用，以下的说法正确的有哪些？
- 日常维护是一种预防性的工作。
- 通过日常维护可以得出网络基线，从而为故障排除工作打下良好的基础。
- 日常维护对操作人员的技术要求很高，但对操作的规范性要求不高。

- 网络的维护不仅仅是技术问题，而且也是管理问题。
- （判断题）通过报文捕获采集的各种报文只能在设备命令行界面直接显示，而无法以文件形式保存。
- （判断题）R1 和 R2 两台设备直连，如果 R1 和 R2 的接口 IP 地址不在同一网络，则通过 LLDP 无法获取到对方设备的 Hostname。

参考答案：

- ABD
- 错
- 错
-