第一章：

1. 网络测量有哪些分类方式？请分别按照测量方式、测量节点、测量协议、测量内容进行划分。

按照测量方式：主动测量、被动测量；

按照测量节点：单点测量、多点测量；

按照测量协议：基于BGP的测量、基于SNMP的测量；

按照测量内容：拓扑测量、性能测量、流量测量。

2. 网络测量的测量内容主要包括哪三类，这三者分别有哪些常见的指标？

性能、流量、拓扑。

性能类指标：时延、带宽、丢包；

流量类指标：IP吞吐量、流量大小和分布、流持续时间、峰值流量信息、网络总流量；

拓扑类指标：拓扑结构中心性、相似性、鲁棒性。

3. 网络测量的主要方法有哪些？各自有什么特点？

被动测量：特点：不注入新的流量、非侵扰性、隐蔽性好、面对海量流量时难度大、采用抽样检测技术；

主动测量：特点：主动发送探测包到目标网络、目的性针对性强、会占用网络资源导致测量结果可能有偏差；

协同测量：测量方式上主被动结合（灵活结合两种测量方式优缺点）、测量设备上协同（包括任务调度、配置同步、资源分配、结果合并）

4. 你认为网络测量能够在哪些方面支持互联网的发展，同时又面临什么样的挑战？

对互联网发展的支持：

1.网络测量得到的数据能够帮助分析存在的恶意行为，从而抵御、减少网络攻击，提高网络安全性；

2.能够帮助互联网公司了解用户对服务的反应，改进服务质量以保证良好用户体验；

3.帮助网管、运维等更好地了解网络性能并快速定位问题，从而提高网络的可用性和可靠性。

面临的挑战：

1.测量过程涉及到用户个人信息，需要谨慎处理隐私相关问题；

2.网络规模、地址空间不断增大，进行测量所需要的成本越来越高，如何保证较高的效率；

3.需要进一步规范化管理，制定统一的标准和协议，减少、杜绝非法恶意行为出现。

---

第二章：

1. Libpcap可以实现什么功能？利用Libpcap被动报文获取的原理是什么？

Libpcap提供的接口函数主要实现了数据包采集、构造、发送等有关的功能。

Libpcap在内核中创建一个用于接收数据的缓冲区，当有数据包从网络传输到达时（需要开启混杂模式来监听网络中的所有数据包，并可以设置过滤规则决定捕获哪些包），内核会将包复制到缓冲区中，Libpcap再对其进行解析处理，传给应用程序。

2. 随着信息技术和互联网技术的飞速发展，网络IP流量不断呈现“更多、更快“的特征，针对高速流量的报文获取有哪些解决方案，试举例说明。

基于硬件的捕获方法：DPDK（通过重载网卡驱动和和零拷贝技术，节省CPU中断、内存拷贝时间）、ASIC（专用芯片）、FPGA；

基于抽样的方法：分组抽样（包括系统抽样、简单随机抽样、分层随机抽样）、流抽样；

其他技术：PF\_RING（新型套接字技术，提高读写性能）、Netmap（高速网络I/O架构，基于零拷贝思想，节省CPU资源）

3. 有哪些主动报文构造方法？他们的特点是什么？

Libnet库提供了两种方式：原始套接字接口和链路层接口。

原始套接字接口较为简单，在网络层及以上构造数据包，不需要构造链路层以太网头；

链路层接口较为复杂，在数据链路层构造数据包，不经过网络层直接发送至网络，功能更为强大。

4. 你认为未来的网络测量的发展趋势是什么？

1.高速、大规模的：随着网络流量的不断增长，未来的网络测量将面对海量的数据处理和分析，需要更加高效的算法和技术来应对这一挑战；

2.多样性的：应用场景越来越多元化，日后也许会有更多的协议、设备被提出应用到不同的网络环境中，所以未来的网络测量将需支持多种测量方法和技术，以适应不同的网络场景和测量需求；

3.进一步提高可靠性和安全性：网络测量数据可能会被攻击者利用进行恶意攻击，因此需要在测量过程中采取一系列安全措施来保护数据的机密性和完整性。

---

第三章：

1. （多选）以下哪些情况下可判定NetFlow流终止（CD）

A.收到TCP标志SYN和ACK

B.收到任意数据包特定时间后

C.流记录创建经过特定时间后

D.流缓存已满

2. 简述NetFlow和sFlow这两种流量测量技术，比较它们的不同之处。

1.架构：NetFlow是由CISCO公司开发的一种流量测量技术，基于采样的方式捕获流量数据并进行分析；sFlow是一种可扩展的网络架构，能够定期从交换机和路由器中生成样本数据进行分析。

2.部署方式：NetFlow不需要增加新的网络设备，软件形式部署在路由器交换机等设备上，一定程度影响设备本身性能；sFlow基于硬件芯片实现，不会给网络设备带来较大压力，适用于大规模的数据检测。

3.准确性：NetFlow直接部署在网络设备上，所以获得的实际流量准确性更高；而sFlow无法对实际流量做到精确还原。

---

第四章：

1. 对流量进行随机抽样时，以下哪些对伪随机数发生器和测量哈希函数的描述是正确的？（B）

A. 伪随机数发生器的安全隐患相对较少

B. 伪随机数发生器对算力要求较低

C. 测量哈希函数可使用密码学哈希函数替代

D. 测量哈希函数无需考虑个体内部特征之间的依赖性

2. 仅仅利用被抽中的SYN报文来估计原始TCP流的数量，这可能会导致估计值的误差偏（大）

3. 在哈希函数的选择上，需要保障安全性，不考虑运行性能时，通常选择（C）；当算力不足，且对随机性要求不高时，通常选择（A）；当需要对输入输出的概率特性有较为精准的分析，且追求一定速率时，通常选择（B）。A. 启发性哈希函数 B. 数学哈希函数 C. 密码学哈希函数

---

第五章：

1. 在网络测量中，数据流的定义和分类有哪些？请简要描述每种分类的特点。

通信领域中的数据流：指通信传输过程中，所对应信息的“数字编码信号序列”，是高速到达的输入数据，强调通信和计算基础设施较难传输、计算和存储；

网络数据流：指一个时间区间内顺序到达的报文序列，一个源和目的由报文头的一个或多个字段构成，在IP网中，流可以定义为对一个呼叫或连接的人为逻辑对应；也可以某时间段内通过一个观测点且具有共同性质的报文集合。

2. 基于数据流的定义和分类，你认为除了基于协议、应用和大小的分类外，还可以有哪些其他的分类方法？请结合实际网络应用场景给出至少两个例子。

1.按照数据流中所包含的主要内容分类，比如纯文本类型、图片、音频、视频类型。在不同的应用场景中流的主要内容也有所不同，比如视频会议，传输的主要为音视频类型；社交软件中多为文本和少量图片视频类型；

2.按照流的方向，将其分为入流和出流，比如在网络的安全管理上，需要检测进入网络的流的安全性，在涉及保密性的网络中要关注出流是否携带保密信息。

3. 假设一个大型购物中心的无线网络出现了拥塞现象，导致用户访问速度明显降低。请思考使用数据流分析的方法解决该场景下的问题，简要阐述分析思路和可能遇到的挑战。

思路：

1.监测该网络内的数据流量的来源去向、无线设备连接情况和网络拓扑结构，分析是否存在接入点布局不合理的情况；

2.分析流量数据特征，判断哪些数据流占用了较多的带宽、哪些设备发送了大量数据；

3.根据以上分析找到性能瓶颈，采取措施，比如：调整无线接入点设备布局，在用户密集的区域增加布设密度；对较为占用带宽、数据量大、影响性能的流进行限速，保证大部分用户的体验。

挑战：

1.大型购物中心网络规模较大、接入设备多、带宽大、数据量大，需要更高效的分析工具和专业人员完成；

2.难以选择合适的改进措施，保证服务质量同时还需要兼顾控制成本；随意对用户进行限速可能反而使用户体验更差。

4. Bloom Filter是一种空间有效的数据结构，用于检测一个元素是否在集合中。关于Bloom Filter，以下哪个选项是正确的？（C）

A. Bloom Filter可以精确地检测一个元素是否在集合中，不会出现误报和漏报

B. Bloom Filter可以精确地检测一个元素是否在集合中，只会出现误报，不会出现漏报

C. Bloom Filter不能精确地检测一个元素是否在集合中，可能出现误报，但不会出现漏报

D. Bloom Filter不能精确地检测一个元素是否在集合中，可能出现误报和漏报

---

第六章：

1. 请简要阐述在网络测量领域中对应用流量分析的目的

应用流量分析可以为网络管理提供决策依据，保障网络关键业务的服务质量和安全。

服务质量：考虑网络服务的数据包丢失、传输延迟和抖动，将来自不同应用的流量对应到不同的服务优先级；

异常检测：网络异常行为通常表现为网络中通过流量的异常，异常检测的核心问题是如何实现正常行为的描述；

用户行为分析：加密协议的使用使跟踪恶意行为更困难，因此用户行为识别成为跟踪恶意行为的一种方法。

2. 在进行Web流量分析时，HTTP和HTTPS流量的主要区别是什么，二者测量方法有何差异？

主要区别：

1.HTTP采用明文形式传输数据，无加密处理，信息容易被窃听、拦截篡改；HTTPS基于TLS/SSL协议，传输前将数据加密处理，采用加密的SSL连接防止信息在传输过程中被窃听篡改；

2.端口号不同：HTTP默认端口为80，HTTPS则是443；

3.HTTP的连接很简单，是无状态的；HTTPS协议是由SSL+HTTP协议构建的可进行加密传输、身份认证的网络协议，比http协议安全。

从测量上，HTTP流量使用普通的流量分析工具即可，如Wireshark、Tcpdump，而HTTPS流量涉及到加密所以在捕获后需要对其解密才能完成分析。

3. 在网络游戏中，实时性和交互性至关重要。假如你是一位大型FPS（第一人称射击）游戏的网络架构师，请根据TCP和UDP在网络游戏中的应用，思考如何选择或结合这两种传输协议以实现更好的游戏体验，简要阐述你的方案。

首先分析两种协议的特点：TCP协议具有可靠连接、确保数据完整、按顺序传输的特点，但由于需要进行确认和重传等，网络延迟增加，影响实时性；UDP协议具有传输速度快、延迟低的特点，但是由于没有确认、重传机制，所以数据传输过程中会出现丢包、错乱等问题，会影响数据准确性。

对于FPS游戏而言，玩家的操作（包括位移、射击等）和状态更注重实时性以给玩家更精准的反馈，保障游戏体验；而像地图、音乐、其他玩家身份信息等内容只需要提前加载好即可，不要求实时更新。

所有使用UDP协议来传输实时性较高的关键数据，如玩家位置、动作、伤害、状态等；TCP协议用于传输不注重实时性的数据，如对局信息、排行榜、玩家信息等。二者结合进行优化，兼顾服务质量与传输效率，提供更好的游戏体验。