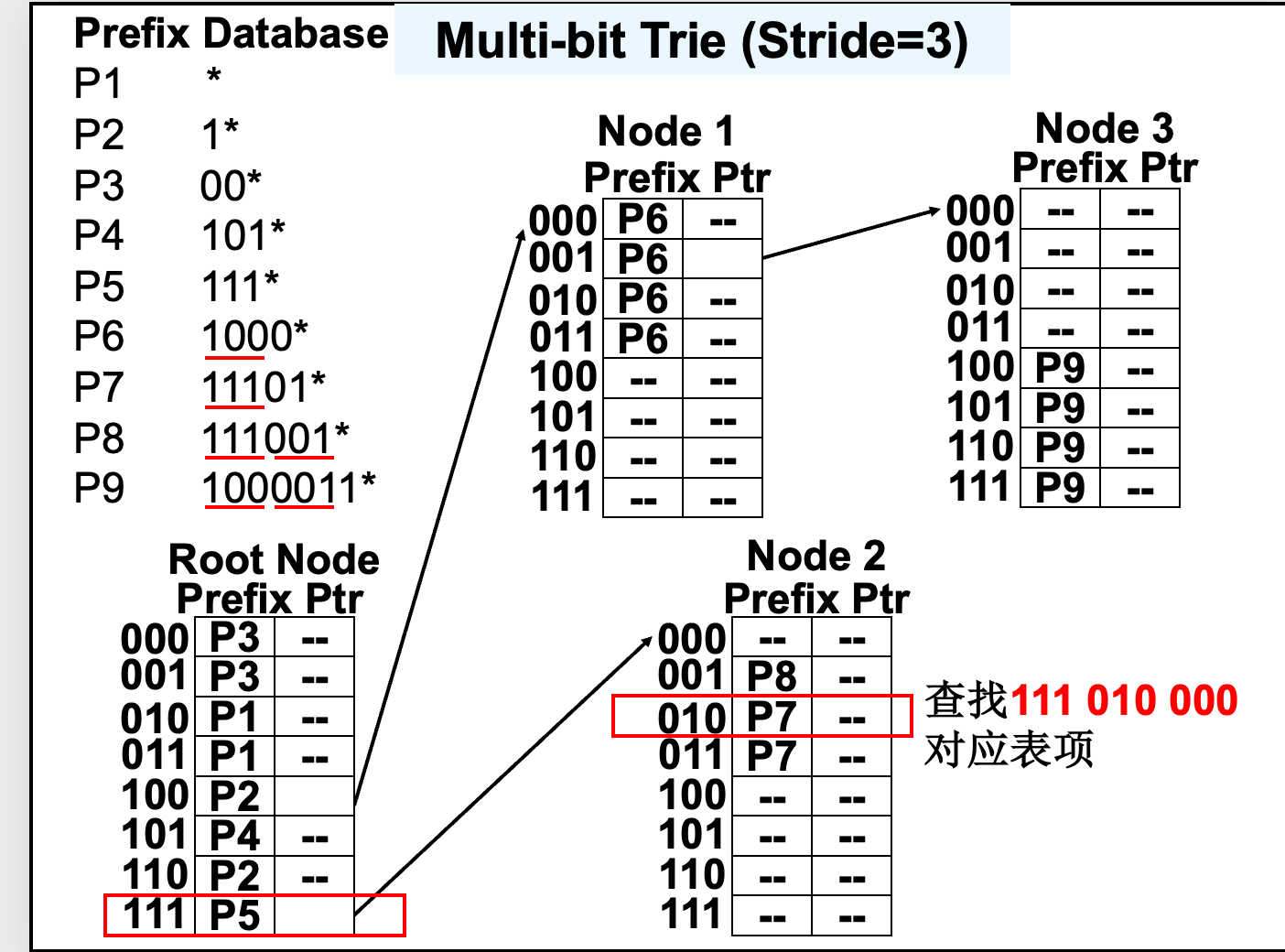
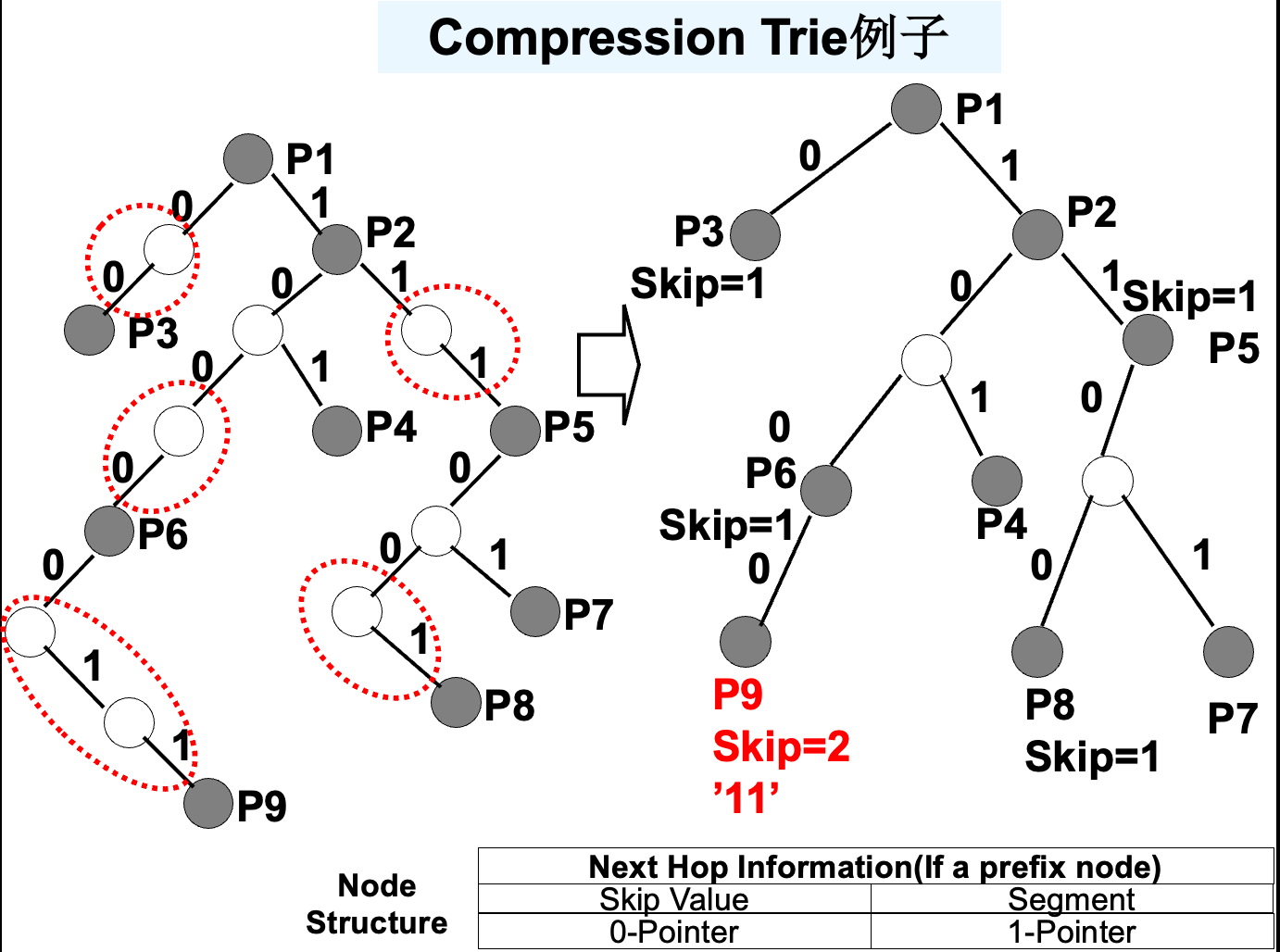
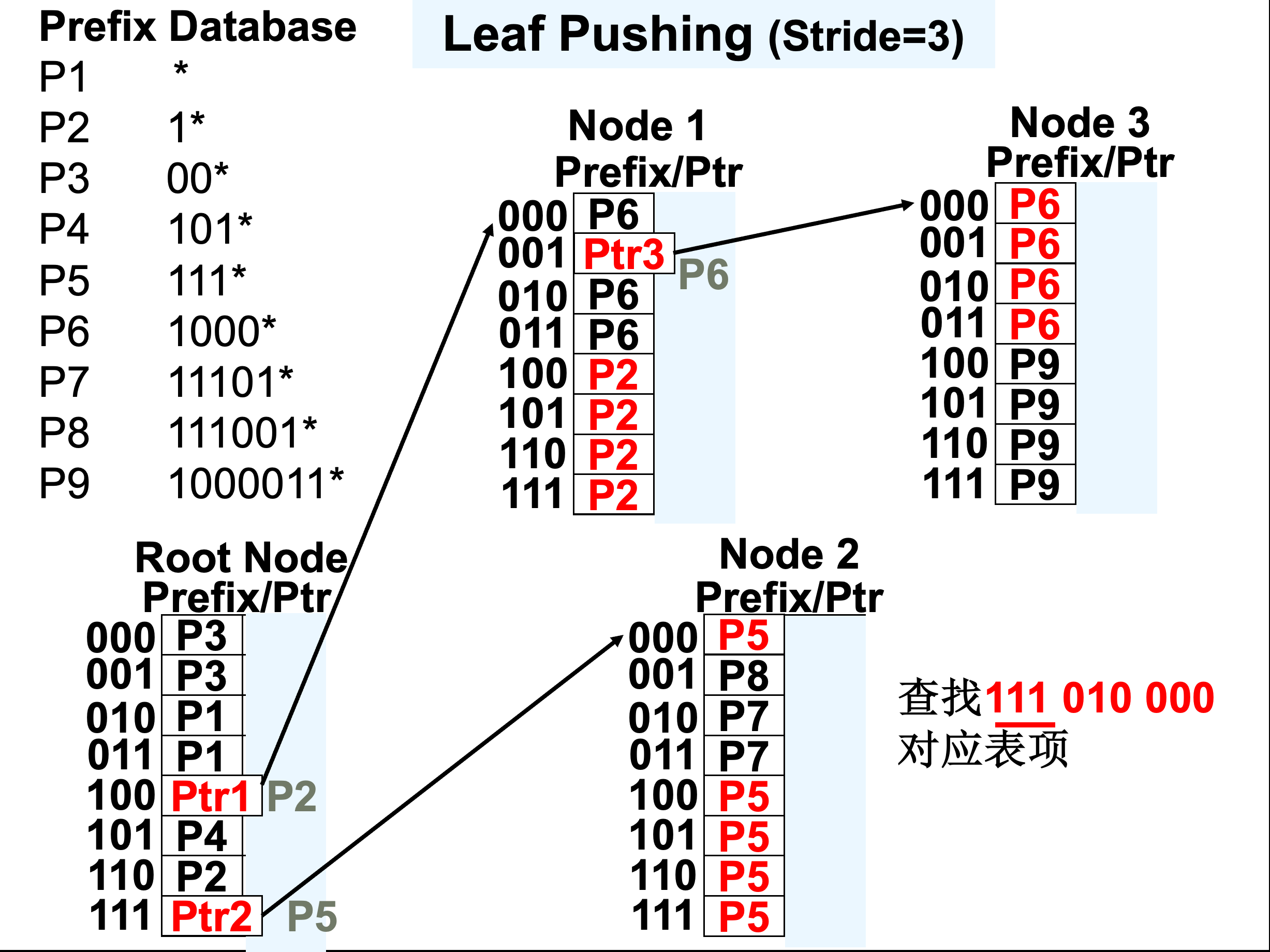
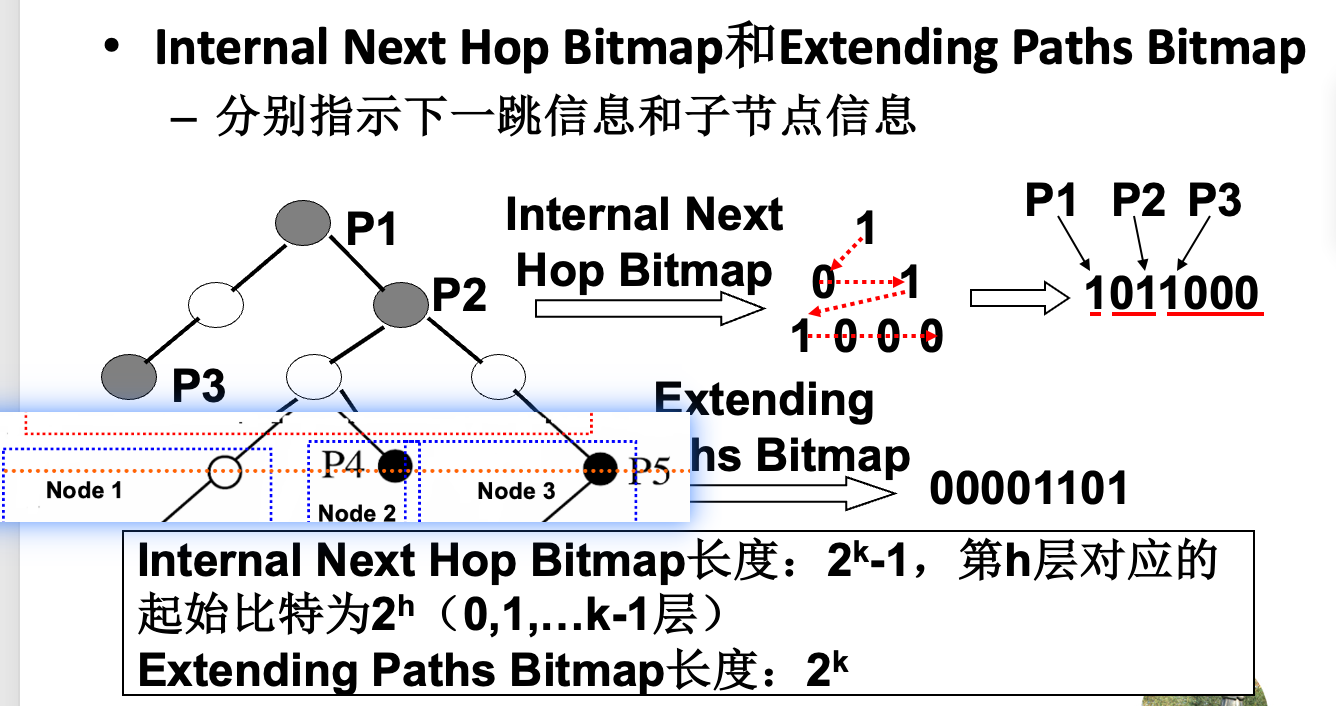
**为什么需要交换？**减少网络中节点之间所需的通信线路增强可扩展性,构建更大规模网络。**虚电路交换与电路交换有哪些相似似之处？为什么说虚电路交换是分组交换而不是电路交换？**虚电路交换与电路交换的相似之处在于它们都是面向连接的通信方式。虚电路交换是分组交换，因为它允许多用户共享物理链路。且通过存储转发机制，数据被分割成独立分组传输，与电路交换的全程链路占用方式明显不同。**电路交换为什么能保证服务质量？分组交换为什么能够提高更高的线路利用率？**电路交换通过交换机在通信双方之间建立一条专用的传输线路，或者占用传输线路的某一个固定的时隙，因而可以保证服务质量。分组交换交换对象是分组，数据以分组的形式进行传输，节点只有在有数据传输时在占有通信线路，多个节点的分组可以共享一条通信线路，因而线路利用率。**电路交换网络能够提供 QoS，虚电路交换网络也能够提供 QoS，这两种网络提供的QoS有什么不同？**电路交换网络提供稳定的比特率和延迟时间，因为一旦通信路径建立，就会被通信双方独占。而虚电路交换网络在通信开始前也会建立一个通信路径，但这个路径是逻辑上的，不是物理上的。虚电路交换网络的比特率和延迟时间取决于多种因素，如网络节点上包队列的长度，应用程序产生数据的比特率，以及使用统计多路复用技术时，共享同一网络资源的其他用户的负荷。**交换机：**网络中执行交换操作的设备，通过一系列交换机得交换操作，在两个通信节点之间建立一条数据传输路径，这条路径由物理或者逻辑上的链路组成。D **交换类型：**交换网络包含：电路交换网络例如传统电话网络，分组交换网络和信息交换网络例如电报网络。分组交换网络又包含数据包交换网络例如 IP 网络和虚电路网络例如 ATM 网络。**电路交换：原理：**电路交换传输线路或者时隙，通过交换机在通信双方之间建立一条专用的传输路径。传输路径建立后，数据像流一样在路径上传输。通信过程有发送端到接收端电路连接建立、数据传输、电路连接拆除。**B 特点:优点：**占用固定得线路资源，保证数据传输得速率、眼熟、可靠性及有效性。**缺点：**线路资源利用率低，没有数据传输时也占用线路或者固定时隙；电路连接建立导致延迟。 (3)为语音传输设计的，支持固定得数据速率。**分组交换：原理：**交换分组：以分组为单位统计复用线路（也称为链路）资源。**统计复用**：只有有数据要传输时才占用线路。分组大小：太小，分组开销大，太大，复用效率低，影响其他分组的发送。两种类型：数据包交换和虚电路交换。**特点：优点：**线路利用率搞，节点只有在有数据要传输时才占用通信线路，因此多个节点得分组可以共享一条通信线路。**缺点：**需要资源管理机制来保证数据传输得速率、延时、可靠性和有序性，增加了复杂性。(3)以分组为单位统计复用线路/链路资源。 (4)分组交换是为数据传输设计的，支持可变的数据速率。**数据报交换：原理：**数据包交换是直接发送分组，比如 IP 网络。**特征：**(1)无连接：直接发送分组，无服务质量保证，(2)健壮性：相同源-目的得分组可能沿不同路径传输，可绕开故障路径。**虚电路交换：原理：**虚电路交换先建立连接，再发送分组，比如 ATM 网络**特征：**(1)面向连接：分组发送前在源和目的之间建立连接。（这个与电路交换不同，连接不是占用固定得线路资源，只是告诉网络得资源需求，在每个交换机上建立“连接状态”；建立得连接路径被称为虚电路） ，具有一定得服务质量保证。 (2)有序性：同一源和目的得分组沿相同得路当**前 Internet 存在的主要问题：(**1)可扩展性 (2)移动性 (3)服务器质量（4）网络安全 (5)能耗。**解决方案和问题1**.DTN：由于连接的间隙性，可能会出现端到端路径不存在的情况。2.SDN:网络缺乏灵活的控制机制，数据面和控制面分离。3.NDN：路由器不知道传输的内容导致冗余传输。通过内容命名。4. MobilityFirst：网络节点身份和位置标识相同（IP地址）GUID - Mapping。**解决现有网络中存在的一些什么问题？但是如果这样做了，又会带来些什么问题？**可以优化网络性能，提高网络安全性，并实现网络和物理世界的融合。但同时，这可能引发隐私问题，增加网络复杂性，并可能增加网络设备的成本。**常用接入网类型，**1.基于ATM架构类：- 传统电信网络- DSL（数字用户线路）- 对称DSL：下行和上行速率相同SHDSL(利用了话音带宽）- 非对称DSL- ADSL ADSL2+:2.基于IEEE 802参考模型的局域网架构类- 新兴IP网络：- 以太网（802.3）、无线局域网（802.11）、甚至包括无线城域网（802.16）3.光纤接入类- 基于ATM：APON、GPON- 基于以太网：EPON。**ATM：为什么选择固定长度（53字节）的信元？**1.构建硬件简单2.交换单元并行处理3.队列行为优化：控制延迟、提高队列处理效率 PPP：在点对点链路上传输多种协议数。PPP over ATM缺乏有效的QoS和组播支持能力- 视频、高质量音频、实时视频会议等服务质量要求高的应用必须选择原始的ATM协议栈。**为什么 Internet 使用IP而不是 ATM？**IP技术发展较早，无连接协议，易于扩展和管理；IP网络开放灵活，设备简单成本低；IP有完整的标准体系，全球互联互通。ATM是一个封闭的网络架构，网络设备相对复杂，成本较高ATM的封闭性、高成本以及专有特性使其更适用于特定高速网络场景。**为什么引入PPPoE**（PPP over Ethernet）的引入是为了解决：1.用户希望通过一个CPE设备接入多台主机，2.以太网却不支持认证和计费等功能，可以把以太网和PPP这两种技术结合起来。**PON：**要解决的关键问题就是如何控制多个ONU/ONT对共享馈线光纤的高效访问。**上行带宽分配、时延、以及数据碰撞等问题**1.多个ONU/ONT采用**TDMA**来避免数据发送冲突。主/从模式：ONU/ONT请求，OLT授权ONU/ONT访问指定时隙。测距（Ranging）：ONU/ONT到OLT的距离为0～20km，传输延迟不同(0~200us)，还有环境变化也会对传输延迟差生影响，通过测距给ONT/ONU插入延迟，确保其到OLT的逻辑距离一样。2. 动态带宽分配(DBA) OLT通过动态分配共享光纤的传输时隙来提高带宽使用率，保证多业务服务质量。**下行：**数据安全性。下行采用广播方式传输，为保证安全性，需要对数据进行加密。**802.11为什么词用CSMA/CA而不是CSMA/CD？**在以太网中，同一网段内任何数据传输数据其它的主机都能侦听到，因而采用的是CSMA/CD。而在无线网中，由于无线信号覆盖范围有限，信道之间的冲突很难让其它设备检测到，因而采用的是（CSMA/CA）。8**02.11 的网络拓扑： 网络构成:(**1)无线站点 STA：配置支持802.11 协议的无线网卡的终端；STA 通过 MAC 层机制来共享同一个无线信道；最简单的 WLAN 仅仅由 STA 组成，他们之间直接通信。(2)无线接入点 AP，基站 BS，数据链路层设备。AP 为 STA 之间的通信提供帧转发功能。**基本 CSMA/CA 原理：**A 两个过程：(1)载波侦听：站点在发送帧之前侦听无线信道是否空闲，如果是，则进入冲突避免阶段，如果当前信道忙，说明现在有其他站点正在传输数据，则延迟发送帧知道侦听到信道空闲。(2)冲突避免：站点在发送帧之前要先等待一个帧间间隔 IFS，并且确保在 IFS 时间内信道空闲，为了防止多个站点在等待 IFS 时间后同时发送而导致冲突，与以太网类似，引入了一个随机退避算法来选择一个退避时间。**D 帧间间隔（IFS）**：控制发送帧之间的等待时间。IFS 越短，帧的优先级越高(1)SIFS:最高优先级，用于 CTS,ACK 等控制帧。(2)PIFS：等于SIFS+1 中等优先级，用于 PCF 操作模式下的帧。(3)DIFS：等于SIFS+2，最低优先级，用于 DCF 操作模式下的数据帧。E退避时间：(1)站点执行随机退避算法来确定退避时间：从 0到竞争窗口 CW之间随机选择一个值 r，则退避时间为 r倍的时槽。(2)竞争窗口 CW 采用与以太网类似的指数退避算法来设置。CW初始化一个最小值 CWmin，当发送方认为发送的帧发生冲突时将CW 加倍增大，直到达到最大值 CWmax。竞争窗口 CW:**开始为 2^k-1,下一次为 2^(k+1)-1。扩展 CSMA/CA 的原理，在什么情况下推荐使用扩展CSMA/CA？**原理：基于RTS/CTS的虚拟信道侦听1.发送方发送RTS帧，其中包含了一个持续时间域，该域的值表明发送方完成帧交换所需要的时间，包括从发送数据帧到接收ACK帧所需要的时间2.收到RTS的站点根据其中的持续时间为自己声明一个虚拟信道，并且该信道正忙，用网络分配向量NAV来表示，在NAV时间内，该站点不会尝试发送帧3.接收方响应CTS帧中也包含一个持续时间域，该域的值足够大，以保证发送方能够完成数据帧交换收到CTS的站点根据其中的持续时间为自己声明一个虚拟信道，并且该信道正忙，在NAV时间内，该站点不会尝试发送帧。使用场景：在高密度的无线网络中，基本CSMA/CA可能由于隐藏节点和冲突较多而效率较低。扩展CSMA/CA减少了冲突的可能性。实时性要求高： 扩展CSMA/CA的帧确认机制有助于提高实时性，减少数据丢失和重传的次数。复杂的网络拓扑： 在存在复杂网络拓扑结构，可能导致信道隐藏节点等问题的情况下，扩展CSMA/CA能够更好地处理这些挑战。在802.11 网络中，站点 A和站点B的 MAC层使用基本的CSMA/CA 机制。**假设数据帧帧间间隔（DIFS）为td，一个时槽（Time Slot）为ts，在两个站点上竞争窗口（CW）初始化为15.在站点 A发送数据的过程中，站点 B 也有数据要发送。假设站点 A 在时刻t0完成数据传输，那么站点 B 最早能在什么时刻开始传输数据？最晚呢？站点B最早能在什么时刻开始传输数据呢？**站点B在站点A完成数据传输后，需要等待一个DIFS的时间，然后进入竞争窗口。在竞争窗口期间，站点B会在0到CW（这里是15）之间选择一个随机数，然后等待相应的时槽数量。因此，站点B最早在时刻t0 + td + 0\*ts开始传输数据（假设站点B选择的随机数为0）。那么，站点B最晚能在什么时刻开始传输数据呢？站点B最晚在时刻t0 + td + 15ts开始传输数据（假设站点B选择的随机数为15）。**与IPv4协议相比，IPv6 协议有哪些变化？为什么会有这些变化？**更大的地址空间,报文结构更精简,更高效的路由基础结构,更好的安全性\原生支持移动性、组播完善和QoS有保证、即插即用（Plug-and-Play）、支持层次化网络结构。这些变化主要是为了应对互联网的快速增长和技术发展的需求，解决IPv4协议在地址空间、安全性、移动性和网络效率等方面的局限性。IPv6的设计旨在支持更大规模的网络，提供更好的性能和安全性，以及更好地适应未来互联网的发展。CIDR 地址块的概念：(1)可变长度的网络前缀取代地址分类中的网络号。(2)具有相同前缀的 IP地址组成 CIDR Block,表示为 A.B.C.D/N，其中 N 为前缀长度。2.**路由中的前缀汇聚**： (1)每个 CIDR Block 分配给一个网络，到该网络的路由通过 CIDR Block前缀来标识。 (2)多个连续的 CIDR Block 所对应的网络如果连接在路由器的同一个端口下面，则在路由器上，到这些网络的路由可以用一个更短前缀来标识，该前缀对应的 CIDR Block 包含这些连续的 CIDR Block。**3.前缀最长匹配规则**：在 CIDR 中，如果路由器上的路由表中有多条表项满足要求，则采用前缀最长匹配规则。**NAT IP地址类型**：全局IP地址用于Internet上的分组转发，要求在Internet范围内唯一；私有IP地址用于指定网络内的分组转发，只要求在指定网内部唯一。**基本NAT：**只使用IP地址信息，需要多个全局的IP地址，一般在NAT设备上维护一个address pool，address pool中地址的数量应该多于有访问外部网络需求的主机的数量。**网络地址和端口转换NAPT：**最常用的一种NAT方式，使用IP地址和TCP/UDP端口号，NAPT操作不仅仅要修改分组的IP头标，还要修改TCP/UDP头标中的端口号，在NAT设备上，虽然内部网络所有的主机共享同一个全局IP地址，但是经过NAT之后不同会话使用的端口号不同。局限性：地址和端口转换将带来比较大的开销，IP地址和端口号可能存在于载荷的任何位置，因此需要软件针对具体的应用做额外的处理，并不是所有的数据都是使用UDP或者TCP来传输，破坏了原有的主机到主机的通信模型。**IPV6 单播地址：链路局部地址、全局地址。1.链路局部地址**：作用范围为链路，在链路范围内分配。(1)前 10 个比特固定位 1111 1110 10，接下来 54 比特的 0，具有形式FE80:/64,(2)最后 64 位为 Interface ID:标识主机上的特定接口。(3)链路局部地址总是自动配置的，只用于链路范围内的数据传输。2．全局地址：(1)前三个比特固定为 001，(2)接下来 45 个位Global Routing Prefix：全局路由前缀，3 个固定比特和 45 比特全局路由前缀组成了 48 比特的站点前缀。(3)接下来 16 比特的 Subnet ID:标识特定的子网，一个站点包含多个子网。(4)最后 64 位为 Interface ID:标识主机上的特定接口。IPv6 组播地**址1.全节点组播地址**：FF02::1(link-local)**2.全路由器组播地址**：FF02::2(link-local)3.被请求节点地址：如果知道这个地址，那么就可以向这个组播组发送，这样缩小了组播的范围。例如: 4037::01:800:200E:8C6C ➡️FF02::1:FF0E:8C6C。**为什么要引入被请求节点地址** 在IPv6中，被请求节点地址（是一种特殊的组播地址，主要用于重复地址检测（DAD）和邻居发现协议（NDP）。这种地址的引入是为了提高网络效率和性能。全节点组播范围太广，没有用到已知的IP地址信息。相比之下被请求节点地址只会发送给特定的一组设备，这些设备的地址在最后24位内与目标地址相同。这样，只有可能是目标接收者的设备才会处理这些请求，大大提高了网络效。**某主机的网络接口 MAC地址为 B8:02:0C:BS:A3:74，给出该接口基于 EUI-64地址生成的链路局部地址，并给出所对应的被请求节点地址《Solicited-node Address）。被请求节点地址的有什么作用？并且举例说明。**基于EUI-64地址生成的链路局部地址（的过程如下：将MAC地址分为两部分，前三个字节和后三个字节，即B8:02:0C和BS:A3:74在这两部分之间插入FFFE，得到B8:02:0C:FF:FE:BS:A3:74。将新的地址的第二个字节的第七位反转，即将B8变为BA，得到BA:02:0C:FF:FE:BS:A3:74。将新的地址转换为十六进制，并添加链路局部前缀FE80::/64，得到链路局部地址FE80::BA02:CFF:FEBS:A374。对应的被请求节点地址是通过将链路局部地址的最后24位添加到FF02::1:FF00:0/104前缀后得到的，即FF02::1:FFBS:A374。被请求节点地址主要用于IPv6的邻居发现协议（NDP）。例如，当一个设备需要找到网络上特定IPv6地址的链路层地址时，它会向对应的被请求节点地址发送邻居请求。只有与被请求节点地址匹配的设备才会响应，这样可以减少不必要的网络流量，提高网络效率。IPV6 邻居发现机制：1.地址解析： A 作用： IP 分组转发过程：（1）根据分组的目的 IP地址查找路由表，得到下一跳节点的 IP 地址（2）根据吓一跳节点的 IP 地址，通过地址解析过程得到其所对应的 MAC 地址。 （3）将分组封装在 MAC 帧中传输，目的 MAC 地址位地址解析得到的MAC 地址。B 过程：（1）通过在节点之间交换邻居请求（NS）和邻居公告(ND)消息来完成。 (2)判断是否需要进行地址解析过程(3)根据需要开始地址解析过程。2.地址重复检测： (1)基于邻居请求（NS） /邻居公告(NA)来实现。(2)节点发送 NS，其中包含要检测的 IPV6 地址。 (3)如果收到相应的 NA，则检测到重复，节点不会使用重复的地址，否则开始使用该 IPV6 地址。3.路由器发现： A 概念： 节点通过路由器发现过程找到本地链路上的路由器集合。B 配置其他网络参数：（1）确定节点地址自动配置方式：是否使用有状态地址自动配置（DHCPV6） （2）为链路定义的网络前缀列表，每个前缀包含 IPV6 网络前缀和有效、推荐生存期。 (3)IPV6头标中 Hop Limit 域的缺省设置。(4)本地链路的 MTU。C 具体过程： (1)被动式： IPV6 路由周期性公告路由器公告 RA 消息：组播发送。同一链路上的 IPV6 主机接收 RA 消息，并且使用其内容来配置或者维护网络参数设置。 （2）主动式：IPv6 主机主动发送路由请求 RS：组播发送。同一链路上的路由器相应 RA:单播或者组播发送。4.被请求节点地址的作用：(1)便于链路寻址，获得 MAC 地址。(2)NS 的目的地址。(3)实现对主机的分组拦截。基于 EUI-64 的 IPV6 地址自动配置过程1.EUI-64 地址：(1)一种新的网络接口地址标准。(2)为网络设备制造商来提供了更多的地址空间。 (3)与 MAC 地址的互相映射。2.自动配置的状态：(1)尝试（Tentative） ：地址正在进行地址重复检测(DAD)过程，不能使用(2)有效(Valid)：地址能够用于发送和接收分组，有效状态包括 Preferred 和 dprecated 状态。首选（Preferred）：DAD 成功，地址有效，能够用于任意的连接或者会话。 弃用(Deprecated):地址有效，除了不能用于新的连接或者会话，其他与 Preferred 状态相同。 (3)无效（Invalid）：地址不能再使用。3.自动配置过程： A 链路局部地址：（1）基于 FE80::/64 和 EUI-64 地址生成的接口标识生成链路局部地址，设置为尝试状态。2)执行地址重复检测(DAD)过程(3)若 DAD 成功，将其设置为有效状态。（4）将链路局部地址的被请求节点地址所对应的组播MAC 加到网络接口的感兴趣 MAC 地址表中。{节点网络接口上的链路局部地址总是在支持 IPV6 的接口初始化时自动配置，不管接口是否连接到网络}。B 全局地址：对于 IPV6 主机，还将继续以下的全局地址自动配置过程： (1)路由器发现过程：主机发送路由器请求（RS）消息，路由器相应路由器公告（RA）消息， RA 中包含网络前缀，缺省路由器、hop limit、MTU 等信息。(2)根据网络前缀信息开始自动配置过程：根据前缀和接口标识自动生成地址，设置为尝试状态，对地址进行 DAD 过程；如果 DAD 成功，设置地址状态为有效状态。根据前缀信息中的 Valid Lifetime 和 Preferred Lifetime域来设置 valid 和 preferred lifetime；将配置地址的被请求节点地址所对应的组播 MAC 加到网络接口的感兴趣 MAC 地址表中。 （3）根据 RA 中包含的其他信息进行缺省路由等网络参数的配置。地址变换：eg.BC:AE:C5:C2:07:21IPv6借口标识生成 1.MAC地址 U/L 位BC（1100) :AE:C5:C2:07:21变成 BE（1110):AE:C5:C2:07:21 2. 第三个和第四个字节之间插入FFFE，变为BE-AE-C5-FF-FE-C2-07-21 3. 写成冒号 16 进制BEAE:C5FF:FEC2:721二、全局 IPv6地2002:1:0:3:BEAE:C5FF:FEC2:721. **七．手动隧道，自动隧道原理及其路由配置。1．手工配置隧道：**（1）对每个 IPV6 分组都事先手工配置它对应的隧道的端点，主要是用于隧道封装所需的 IPV4 地址。 (2)配置到隧道的路由。2.自动配置：本质是建立一个 IPV6 地址到 IPV4 地址间的映射关系。(1)分组中所包含的 IPV6 地址和/或路由的下一跳决定隧道的端点，主要是指用于隧道封装所需的 IPV4 地址。 (2)配置到隧道的路由。ISATAP 两种格式：64-bitUnicastPrefix:0:5EFE:w.x.y.z私有单播 IPv4 地址64-bitUnicastPrefix:200:5EFE:w.x.y.z为公共（全局）单播 IPv4 地址64-bitUnicastPrefix 可以为链路局部、全局和唯一本地前缀。**eg，RI 为ISATAP路由器，为支持 IPv6-in-IPv4 隧道，R1 在网络1中公告IPv6 前缀2002:1:0:1::/64，主机 A的IPV4地址： 160:0:0:2，主机 A 的 ISTAP地址？**全局：2002:1::1:200:5EFE: 160.0.0.2或2002:1:0:1:200:5EFE:160.0.0.2链路局部： FE80::200:5EFE:160.0.0.2. 6to4自动隧道：地址形式：2002：WWXX:YYZZ:Subnet ID:Interface ID。WWXX::YYZZ 表示分配给站点或者主机的全局 IPV4 地址。网络层切换与链路层切换。 1，基本常识： A 切换概念：移动节点从一个接入点到另一个接入点的过程。B 五元组：标识应用会话，结构为<源/目的 IP 地址、协议、源/目的端口号>。 C 切换类型：链路层切换、网络层切换。2.链路层切换：同一个网络中不同的 AP 间的切换时链路层切换，链路层切换不改变 IP 地址，执行链路层操作。因此其不改变五元组，对应用会话无影响。AP:无线接入点。3.网络层切换：不同网络不同 AP 间的切换首先执行链路层切换，再执行网络层切换，进行网络相关参数配置。因此切换过程中移动节点 IP 地址发生变化。问题：通信对端并不知道移动节点地址发生改变；即使通信对端知道了 ADDR2，由于五元组变化，会话也会中断，如何消除影响：（1）应用层：需要应用支持，本质上是重新建立 IP 会话。(2)网络层解决方案：需要增强网络协议，对应用透明。移动 IPV6 如何对上层应用屏蔽移动性。1.基本常识：A 几个关键词：家乡地址 HoA、转交地址 CoA、家乡代理：Home Agent。B 基本过程，移动检测，转交地址配置，绑定注册，分组拦截技术。2.对上层应用屏蔽移动性： A 双向隧道模式：移动节点和通信对端的通信始终使用家乡地址进行通信；移动节点的移动由家乡代理跟踪，对于通信对端来说透明；所有通信必须通过家乡代理转发。B 路由优化模式：通信对端知道移动节点当前的转交地址。PMIPV6 引入的原因及原理：1.基本概念.PMIPV6，代理移动IPV6，基于网络端的本地移动管理。2.引入原因：更加易于部署，更加易于管理、更好的性能。3．原理：A 网络端控制的移动管理：在网络中引入一个功能实体代理移动系欸但执行与家乡代理之间的信令，比如：移动接入网关。 B 本地移动管理：再本地管理域中引入一个类似于家乡代理的功能实体，负责管理域内的移动管理操作，比如：本地移动锚定点。 C 移动管理相关信令运行再移动接入网关和本地移动锚定点之间。**分析移动节点在代理移动 IPv6 域内跨子网移动时的切换延迟。与移动 IPv6 相比，代理移动 TPv6 在哪些方面减少了切换延迟？**代理移动IPv6中，移动节点在域内跨子网移动时的切换延迟主要包括：链路切换延迟、网络层切换延迟。代理移动IPv6在以下方面减少了切换延迟：1.移动节点无需参与移动性管理2. 移动节点无需更改家庭地址。QOS 度量参数：带宽/传输速率、延迟、延迟抖动、丢包率.流：流是从一个源到一个目的的有效分组集合，由特定于具体应用并且具有相同 QOS 需求的分组所组成。一个流和一个应用会话（Session）相对应， IP 网络中通常用五元组来标识一个流。在面向连接的网络中属于同一个流的所有分组将会走相同的路径到达目的地；再无连接的网络中，属于同一个流的分组可能会走不同的路径到达目的地。行为集合：行为结合是在路由器上执行相同 QOS 操作的分组的集合（多个流如果具有相同的 QOS 操作，则在路由器上可以汇聚成一个行为集合）。行为集合有时与类的概念等同，流可以看作是只有 1 个流的行为集合或者类。服务等级协议：用户-网络运营商、网络运营商之间协商的 QOS服务内容；SLA 内容包括服务方式、流量规格、使用费、用户以及网络运营商双方没有履行合同规定时的惩罚条例等；用户有义务保证输入网络的流或者业务保持再 SLA 中约定的水平一下（带宽、突发速率、突发长度等）；网络运行商有义务保证提供的服务不低于 SLA 中的约定的水平。QoS 路由器功能：A 接纳控制：当应用要求 QoS 服务时，判断其要求是否能够得到满足，应该是放在每个网络的入口路由器上。B 流量调节：检查到达的分组是否满足 SLA 中设定的 QoS 水平，如果不满足，实施事先指定的整形操作，包括丢弃、延迟、重标记等。C 流量控制：为了满足 QoS 需求（带宽、丢包率、延迟、延迟抖动等），选择是否向输出链路输出分组以及控制分组的输出顺序（即队列管理和调度），该功能设置在输出端口处。综合服务原理：A 资源预留：(1)正向收集资源状态信息，进行接纳控制 (2)反向进行资源预留，设置资源预留状态B 数据流传输：发送主机发送遵循预留规定的数据流C 流量调节：中间路由器检测数据流是否满足预留规定，如果不满足的话，则： (1)对于保证型服务，采用整形； (2)对于受控负载型服务，将不符合的分组转为尽力服务。D 流量控制：路由器根据指定的服务类型，对每个流进行调度和队列管理，实现指定 QoS（带宽，延迟等）综合服务类型：（保证型是定量服务，二受控负载型和尽力服务为定性服务） ：A 保证型：提供完全保证的服务质量，用于要求低延时的业务，其最大延时和带宽能够得到定量保证。 B 受控负载型：能够提供一种相当于网络节点在低负载情况下的尽力服务，要求低的丢包率，可以接受一定范围内的延迟。 C 尽力服务。区分服务：A 概念：DiffServ,主要是解决综合服务的可扩展性问题。B 原理：预先设置 PHB、数据传输。C 关键词：DSCP(区分服务码点)、PHB(逐条行为，四种)。加速转发型 PHB(EF PHB):提供低丢失率、低延迟和低延时抖动的服务，严格限制 EF 分组到达路由起的速率小于设定的路由器转发 EF 分组的速率（通过在位于网络入口的路由器上限制进入的 EF 分组不超过某一最大速率，从而实现对 EF 分组速率的限制）；EF 由具体的调度算法来实现；推荐 DSCP 为 101110.B 确定转发型 PHB(AF PHB)：比尽力更好的 PHB，为用户提供不同级别的转发保证，定义了四个等级，每个等级定义了 3 个丢弃优先级。IP 分组转发保证取决于多少资源分配给此分组所属的AF等级；此 AF等级当前的符在和拥塞情况，分组的丢弃优先级。综合服务和区分服务的优点:综合服务提供细粒度的以流（Flow）为单位的QoS，并且通过资源预留能够保证端到端的QoS,适用于规模较小的接入网络区分服务通过对流进行聚类（BA），并且在路由器上事先设置分组的处理规则（PHB），具有更好的可扩展性,适用于业务流量大的核心网.**综合服务存在哪些问题？针对这些问题，区分服务有哪些改善？**综合服务时基于流的细粒度分配，带宽、存贮、处理开销随着流的数量的增长而急剧增长，存在可拓展性问题。区分服务以行为集为单位提供QoS，事先在路由器上指定对属于某个行为集合的分组的处理，只在入口路由器上对分组进行分类并且打上标记，进行流量调节。**与综合服务相比，区分服务如何获得更好的可扩展性？这样做的代价是什么？1.**无需保存流状态和信令信息：DiffServ不需要为每个流保存状态信息或进行信令,2.基于类的QoS技术：DiffServ是基于类的QoS技术，它将具有相同特性的若干业务流聚合起来，而不再面向单个业务流.3.在DiffServ模型中，复杂的分类和调节功能主要在网络的边界节点上实现，而核心网络节点主要负责数据包的转发，这降低了网络设备的要求 代价：服务质量可能受限：由于DiffServ无需保存流状态和信令信息，因此在拥挤的链路上，由于缺少端到端的带宽预留，服务保证可能会被削弱。复杂的流量管理：在网络入口处，网络设备需要检查数据包内容，并为数据包进行分类和标记，所有后续的QoS策略都依据数据包中的标记做出，这可能需要复杂的流量管理策略。**为什么说综合服务能够提供端到端的QoS而区分服务不能？,**综合服务模型通过状态监控和资源预留,可以提供端到端的QoS保证;而区分服务模型由于不跟踪每个流的状态,无法提供端到端的QoS保证。一路由器功能与架构。 路由表性能的决定：A 路由查找算法：如何快速的决定输出端口。B 交换结构：如何快速的交换到输出端口IP 路由器功能：A 数据路径功能(1)根据分组目的的 IP 地址查找转发表(2)通过交换结构转发到输出端口(3)输出端口调度和队列管理。 B 控制面管理： (1)系统配置和管理(2)运行路由协议，构建路由表。Binary Trie ： A 数据结构：使用二进制 Trie 来组织转发表。(1)Trie 中的每个节点有两个指针： 0-指针和 1-指针，即每个节点最多由两个子节点。(前缀数据库：转发表中的所有前缀的集合)。C 性能：(1)最差情况下需要由 W 次存储器访问（2）查找复杂度和更新复杂度为 O(W)。（3）存储复杂度为 O(NW)。Leaf Pushing :A 提出背景（先前方法的局限性）：(1)每个节点需要空间来保留指向下一跳信息和子节点的指针。（2）由于使用前缀最长匹配，还有可能存在回溯操作。（3）完全 Trie 方法的存储开销太大。B．定义：分离的前缀 Trie。给那些只有一个叶子节点添加另一个叶子节点，新的叶子节点的信息使用距离其最近的前缀节点。C 性能：Leaf Pushing 可以减少存储开销，因为此时每个节点只需要使用一个指针，要么是指向下一跳信息，要么是指子节点但是 Leaf Pushing 增加更新复杂度。操作：给那些只有一个子节点的节点添加一个叶子节点，新的叶子节点的信息使用距离其最近的前缀节点，这个操作也被称为Leaf Pushing Path Compression：A 原理：(1)Compression:Trie 中只有一个子节点的非前缀节点能够被删除。（2）节点保持 Compression相关信息：skip value,segment skip value:指示路径上有多少个比特被跳过， segment:指示最后一次跳过操作以来具体遗漏的比特串。B性能： (1)路径压缩可以有效的减少稀疏 binary trie的高度。(2)最差情况下采用路径压缩后查询和更新复杂度均为 O(W).Multi-Bit Trie:A 原理：(1)查找时同时检查多个比特，称为查找步长(stride)。（2）如果前缀长度不为步长的整数倍，则对其进行扩充。 (3)步长为 k，则 Trie 中的每个节点的条目数量为2^kB.性能：(1)查找速度提高了 k 倍，查找复杂度为 O(W/k)，更新复 杂度 为 O(W/k+2^k).(2) 存 储 空 间 大 ， 存 储 复 杂 度 为O(N\*2^k\*W/k).（3）Leaf Pushing 优化：节点上的每个条目要么包含一个指针，要么包含下一跳信息;相当于把吓一跳信息Push down 到叶子节点。存储空间减少为 1/2LC Trie： A 概念：全称为 Level Compression Trie:结合Path-Compression 和 multi-bit Trie 的概念来优化 BinaryTrie 结构。B.Path Compression 与 Multi-bit Trie：(1)节点分布稀疏时，Path Compression是压缩 Trie的有效途径。 (2)固定步长 multi-bit 能够提高查找性能，但是当节点分布稀疏时存储冗余大；节点分布越密，存储效率越高，完全 Trie 无冗余。C 构造：(1)如果 Trie 的中间节点包含前缀，则进行 LeafPushing 操作，使得 Trie 中只有叶子节点包含前缀（即为前缀节点）。(2)通过 Path Compression 将 Trie 压缩。(3)当子 Trie的结构为完全子 Trie 时执行 Multi-bit 查找。D，在 LC Trie 中每个节点需要保存：(1)Path Compression 信息（Skip Value, Segment）（2）Multi-bit 查找信息(Stride).路由器吞吐量和加速：A 吞吐量：(1)当所有的输入端口以线速承载百分百的业务的时候，平均汇聚输出速率和平均汇聚输入速率的比率。 (2)如果所有空闲输入-输出端口对都可以传输数据，则可以认为吞吐量是百分百。 B 加速： (1)交换结构的内部转发速率和单个输入端口线速的比值(2)如果加速超过1，则输出端口必须使用缓存(常态)2.内部阻塞和输出端口竞争：降低吞吐量。A 内部阻塞：(1)交换结构内部竞争导致内部阻塞。（2）无阻塞：空闲输入端口和空闲输出端口之间的连接始终可以被建立。(3)可以避免。B 输出端口竞争：(1)多个输入端口请求同一个输出端口导致输出竞争。(2)由 IP 业务的突发性导致(3)不可避免。阻塞和输出端口竞争的区别：阻塞一般是指交换结构内部争用所导致，而输出竞争是发生在交换机的输出端口.阻塞和输出竞争是在空分交换中发生，对于时分交换，业务在时间上进行复用可以避免阻塞。三代交换结构： A 第一代交换技术：共享存储器交换：交换及速 率 受 限 于 共 享 的 存储 器 的 访 问 速 度，通 常 汇 聚 容 量 小 于0.5Gbps。B 第二代交换技术：共享媒介交换。交换机速率受限于共享的总线速率，通常汇聚容量小于 5Gbps。C 第三代交换技术：空分交换。交换机速率受限于交换结构，通常汇聚容量小于50Gbps。输入队列与输出队列：A 输入队列：解决输出竞争.（1）每个输入都设置队列（2）存在着头阻塞问题，降低了交换性能。B 输出队列：解决输出端口竞争（1）每个输出端口都设置队列，（2）加速大于 1（最大为 N）必须使用输出缓存。(3)易于实现基于 QoS 调度。Banyan 交换机：单路径多级交换机。A 结构：(1)基于 2X2 交换单元构建 N 端口 Banyan 交换机。(2)共有 log2 (N)级，每一级都有 N/2 个交换单元，总交叉点数量：Nx=4 X N/2 X log2(N) （3）对于第 k 级，最多由 2^k 个输出可能。**对于采用交换结构的高性能路由器，为什么说输出竞争不可避免？如何缓解输出竞争带来的问题？**多个输入端口请求同一个输出端口导致输出竞争，由IP业务的突发性导致故不可避免。使用输出缓存即输出队列解决输出端口竞争。**对于高性能路由器，交换结构的加速为什么大于1？加速大于1会带来什么问题？**在高性能路由器中，交换结构的加速大于1是为了提高路由器的处理能力。加速大于1也会带来1.计算复杂性增加2.可能引入额外的延迟3.可能引发资源竞争，这可能会导致性能下降。算法图片： **SYN Flood 攻击的实现原理如下**：1.攻击者向目标服务器发送大量伪造的 TCP 连接请求（SYN）。2.服务器为每个连接请求创建一个半开连接，等待客户端发送 ACK 数据包。3.攻击者不发送 ACK数据包，从而使服务器在等待 ACK 数据包的过程中保持半开连接状态。4. 由于服务器在等待 ACK数据包的过程中保持半开连接状态，因此攻击者可以利用这个漏洞来耗尽服务器的资源，从而使其无法处理合法流量。

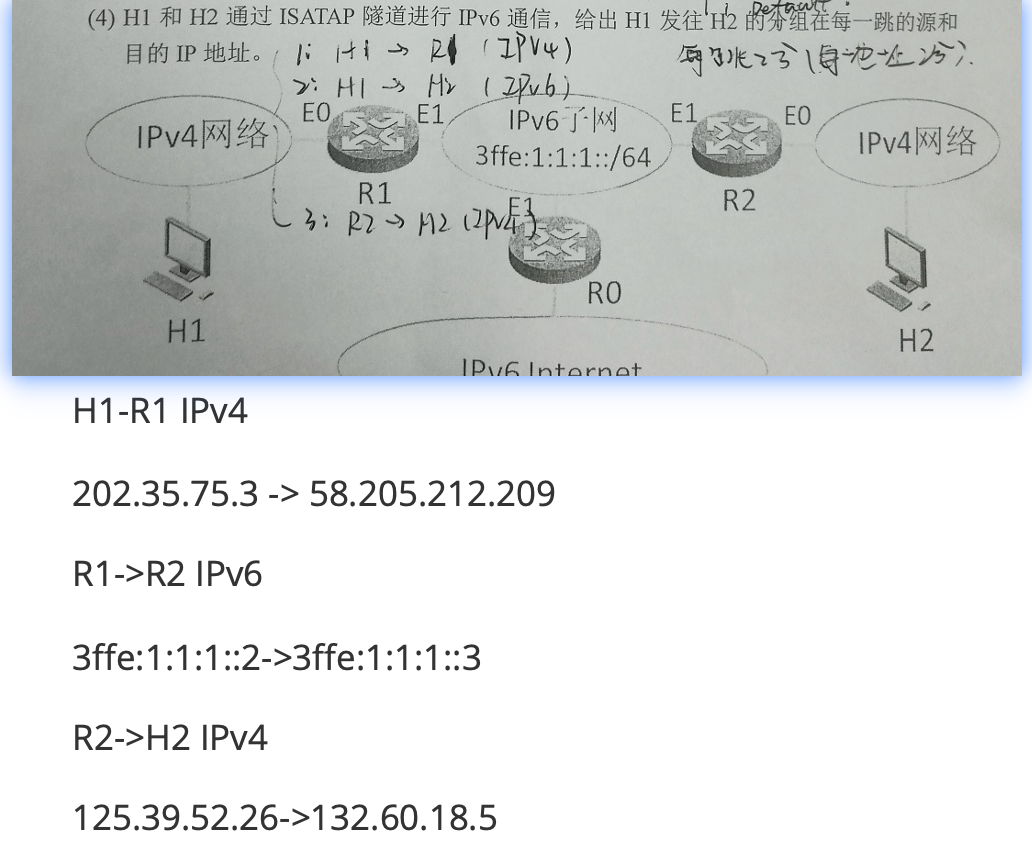


十进制数字转换为十六进制的过程如下：将十进制数字除以16，得到商和余数。记录余数。如果余数在10到15之间，分别用A到F表示。如果商不为0，重复步骤1和2，直到商为0。将记录的余数按照从后往前的顺序排列，就得到了十六进制的表示。将十进制数字238转换为十六进制的过程如下：238除以16得到商14余数14，14在十六进制中表示为E。然后再将商14除以16，得到商0余数14，14在十六进制中表示为E。

在6to4网络中，IPv6地址的前32位是固定的2002，接下来的32位是IPv4地址的16进制表示。因此，路由器R的IPv4地址238.136.16.1对应的16进制表示为EE88:1001。所以，我们可以给子网W1和W2分配的6to4子网前缀如下：子网W1的6to4子网前缀：2002:EE88:1001:1::/64子网W2的6to4子网前缀：2002:EE88:1001:2::/64然后，我们可以给路由器R的E1和E2端口配置IPv6地址如下：路由器R的E1端口IPv6地址：2002:EE88:1001:1::1路由器R的E2端口IPv6地址：2002:EE88:1001:2::1。

路由表写法：一定有一条目的地址为：default(or ::/0)前往子网前缀的话：下一跳为On-Link。A到R是ISATAP的话下一跳要写局部链路地址。路由器1.子网前缀On-Link，2.默认路由3.相连转发路由器。 主机路由：1.子网前缀 ON-link 2.默认路由

在M从子网W1移动到子网W2的过程中，会执行以下操作1重新配置IP地址：M需要在新的子网W2中获取一个有效的IP地址。2更新路由表：路由器需要更新其路由表以反映M的新位置。3通知其他设备：可能需要通知子网W1和W2中的其他设备M的新位置。这些操作可能对M的业务产生以下影响：暂时的服务中断：在M从子网W1移动到子网W2的过程中，可能会有短暂的服务中断。网络性能变化：如果子网W2的网络条件与子网W1不同（例如，带宽、延迟等），则M的网络性能可能会改变。产生这些影响的原因主要是网络配置的变化和网络条件的差异5。重新配置IP地址和更新路由表需要时间，可能导致服务暂时中断。R**1在网络1中公告IPv6前缀2002:1:0:1::/64，主机A配置了IPV4地址160:0:0:2**主机A的ISTAP地址全局：2002:1::1:**200:5EFE:**160.0.0.2链路局部：FE80::**200:5EFE:**160.0.0.2



MTU 是最大传输单元（Maximum Transmission Unit）的缩写，指的是网络层协议所能通过的最大数据包大小。MTU 的值通常与通信接口有关（网络接口卡、串口等）。实验中使用的网络命令：ifconfig ens5`查看网络接口信息。`arp -n` 和 `ip neigh show`：查看 ARP 缓存表或邻居表。`ping -c 1 HostB 的 IPv4 地址`：向 HostB 发送 ICMP 请求。`cat /proc/sys/net/ipv4/ip\_forward` 和 `cat /proc/sys/net/ipv6/conf/all/forwarding`：查看 IP 转发功能的状态。`route -n` 和 `route --inet6`：查看 IP 路由表。nc -l 1958：在 TCP 端口 1958 上监听传入连接。nc S 的IPv4 地址 1958：向 S 主机的 1958 端口发起连接。netstat -aunt：查看当前系统上所有的网络连接和监听端口，以及它们的状态、协议类型、本地地址和远程地址等信息。sudo tcpdump -vxn host HostA 的 IPv6(ens5 scope:link) 地址 and S 的 IPv6(ens5 scope:link）地址 -i ens5：使用 tcpdump 工具来捕获指定主机 HostA 和另一台主机 S 之间通过 ens5 网络接口的 IPv6 通信数据包。ping6 -c 1 S 的 IPv6(ens5 scope:link）地址%ens5：向指定的 IPv6 地址发送一个 ICMPv6 Echo Request 数据包，以测试与目标主机 S 的连通性。sudo tcpdump –vxn host ff02::1 -i ens5：使用 tcpdump 工具来捕获发送到 IPv6 组播地址 ff02::1 的数据包。**sudo ip tunnel add sit1 mode sit remote HostB 的 IPv4 地址 local HostA 的 IPv4 地址 dev ens5：**在 HostA 上创建一个 IPv6 到 IPv4 的隧道，隧道的远程端点是 HostB 的 IPv4 地址，本地端点是 HostA 的 IPv4 地址，数据包通过 ens5 网络接口发送。sudo ip link set sit1 up：将 sit1 隧道接口置为启用状态。**ip link show up**：显示当前已启用的网络接口。sudo ip addr add 3ffe:3216:2101:2106:1234::A/80 dev sit1：将 IPv6 地址 3ffe:3216:2101:2106:1234::A 分配给隧道接口 sit1，前缀长度为 80。ip tunnel show：显示系统中所有隧道接口的信息。sudo tcpdump -vxn -i sit1：使用 tcpdump 工具来捕获在隧道接口 sit1 上传输的网络数据包。ping6 –c 1 3ffe:3216:2101:2106:1234::B：向指定的 IPv6 地址发送一个 ICMP 回显请求数据包，以测试与目标主机的连通性**通过隧道通信与两个 IPv6 主机直接通信的区别是什么：**1.隧道通信的报文中，IPv6 头部包含了源地址和目标地址，以及隧道协议类型。两个 IPv6 主机直接通信的报文中，IPv6 头部只包含了源地址和目标地址。2.隧道通信的报文中，包含了隧道协议头部，用于描述隧道连接的相关信息。两个 IPv6 主机直接通信的报文中，没有隧道协议头部。