

第十一节-多播、VPN、NAT、MPLS 和 SDN

一、课程目标

理解多播、VPN、NAT、MPLS 和 SDN 相关概念和协议。

二、课程内容

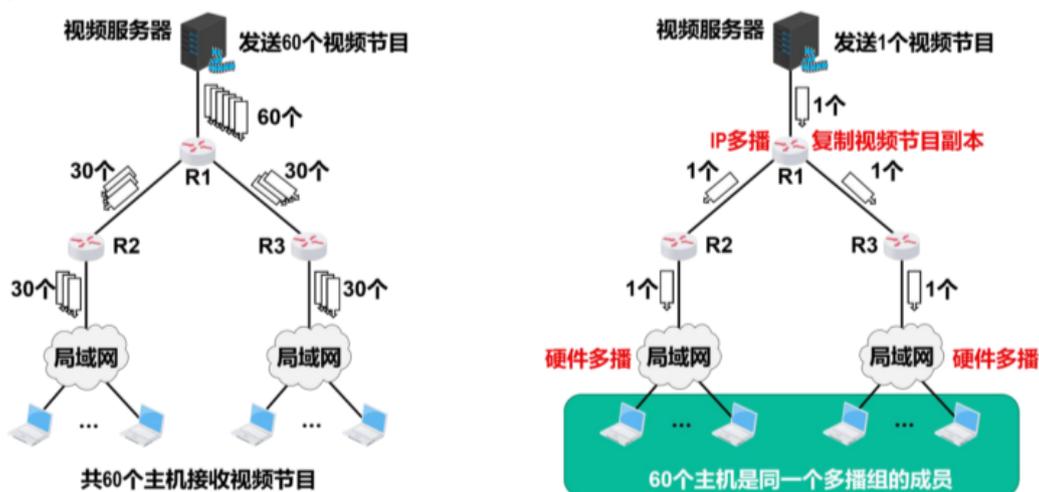
1、IP 多播

(1) 相关概念

单播：用于发送数据包到单个目的地，且每发送一份单播报文都使用一个单播 IP 地址作为目的地址。是一种点对点传输方式。

广播：是指发送数据包到同一广播域或子网内的所有设备的一种数据传输方式，是一种点对多点传输方式。

多播 (Multicast, 也称为组播)：是一种实现“点对多点”通信的技术，与传统单播“点对点”通信相比，多播可以极大地节省网络资源。在因特网上进行的多播，称为 IP 多播。IP 多播包括局域网内的硬件多播、因特网上的多播两种类型。



(2) 多播技术优点

提高数据传送效率，减少主干网拥塞风险，显著减少网络资源消耗。

(3) 在局域网上进行硬件多播

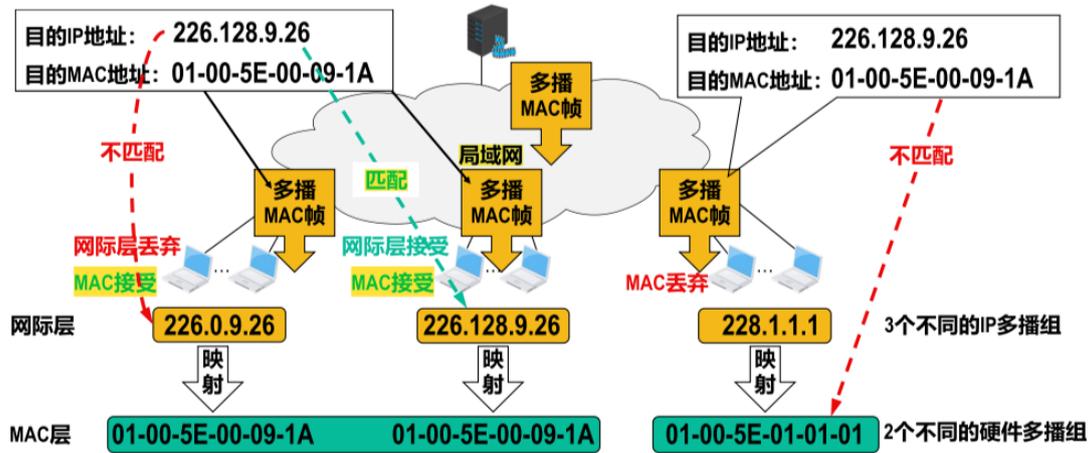
基本原理：使用特殊的映射规则将把 IPv4 多播地址映射成多播 MAC 地址（即可将 IP 多播数据报封装在局域网的 MAC 帧中），这样可利用硬件多播来实现局域网内的 IP 多播。

补充：

用于多播的 MAC 地址为 01-00-5E-00-00-00 到 01-00-5E-7F-FF-FF，共有 2^{23} 个。

用于多播的 IP 地址（D 类，前 4 比特固定为 1110，后 28 比特是组播组地址标识 ID），共有 2^{28} 个。

因此，IP 多播地址与多播 MAC 地址的映射关系并不是唯一的。因此收到 IP 多播数据报的主机还要在网际层利用软件进行过滤，把不是主机要接收的 IP 多播数据报丢弃。



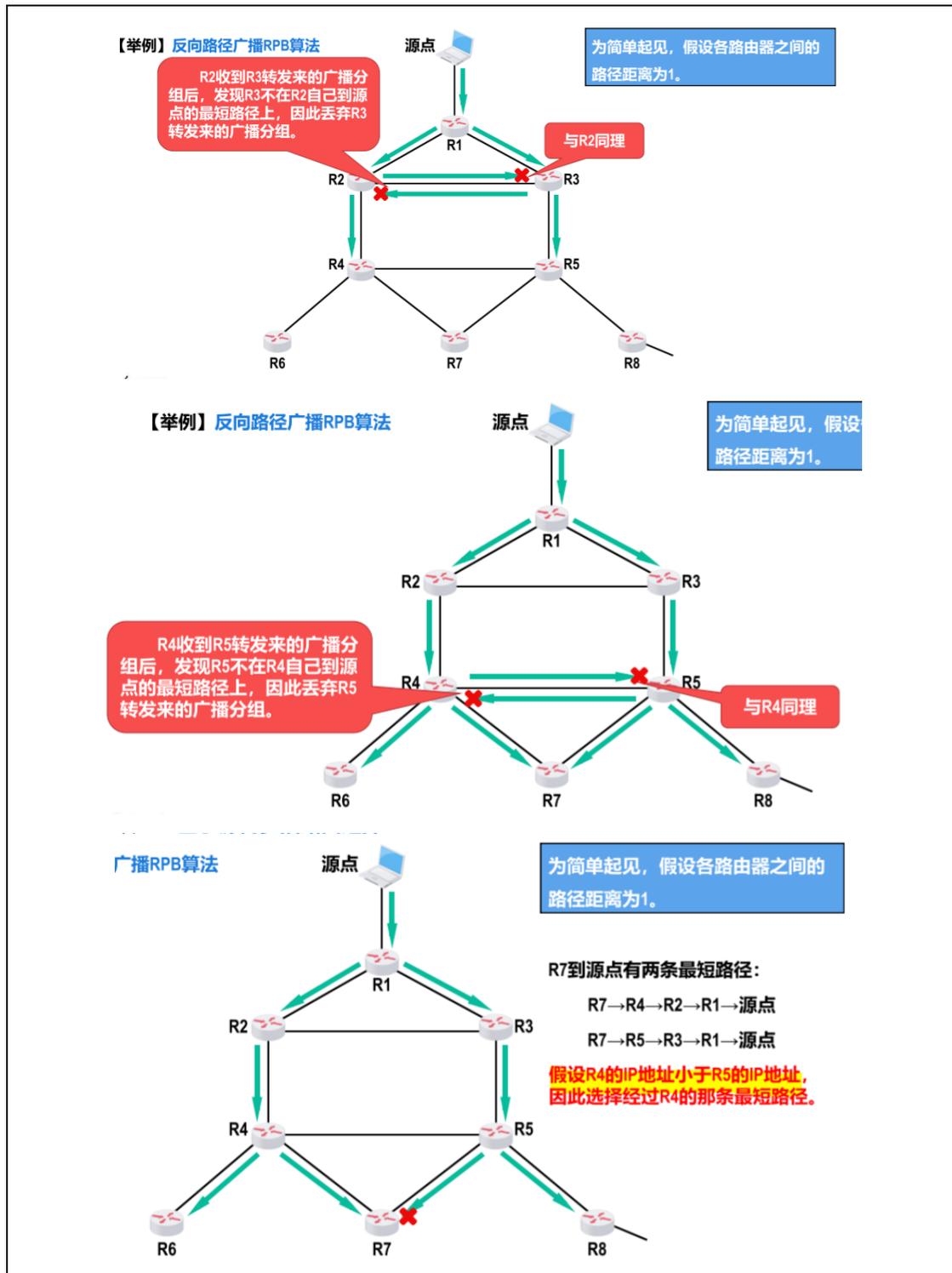
(4) 在因特网上进行 IP 多播需要的两种协议：**网际组管理协议 IGMP** 与 **多播路由选择协议**

- **网际组管理协议的功能：**使本地局域网上的多播路由器知道本局域网上是否有主机加入或退出了某个多播组。
- **多播路由选择协议的功能：**在多播路由器之间为每个多播组建立多播转发树。构建多播转发树的两种方法包括基于源树 (Source-Base Tree) 多播路由选择和组共享树 (Group-Shared Tree) 多播路由选择。
 - ◇ **基于源树多播路由选择：**最典型算法是反向路径多播 (Reverse Path Multicasting, RPM) 算法，并使用洪泛 (Flooding) 法建立广播转发树，利用剪枝 (Pruning) 算法剪除广播转发树中的下游非成员路由器。
 - ◇ **组共享树多播路由选择：**采用基于核心的分布式生成树算法来建立共享树，在每个多播组中指定一个核心 (core) 路由器，以该路由器为根，建立一棵连接多播组的所有成员路由器的生成树，作为多播转发树。

反向路径多播 (Reverse Path Multicasting, RPM) 算法：
 每个路由器在收到一个广播分组后，首先检查是否从源点经最短路径传送来的。
 若是，本路由器将该广播分组广播到其他接口。
 若不是，丢弃该广播分组。

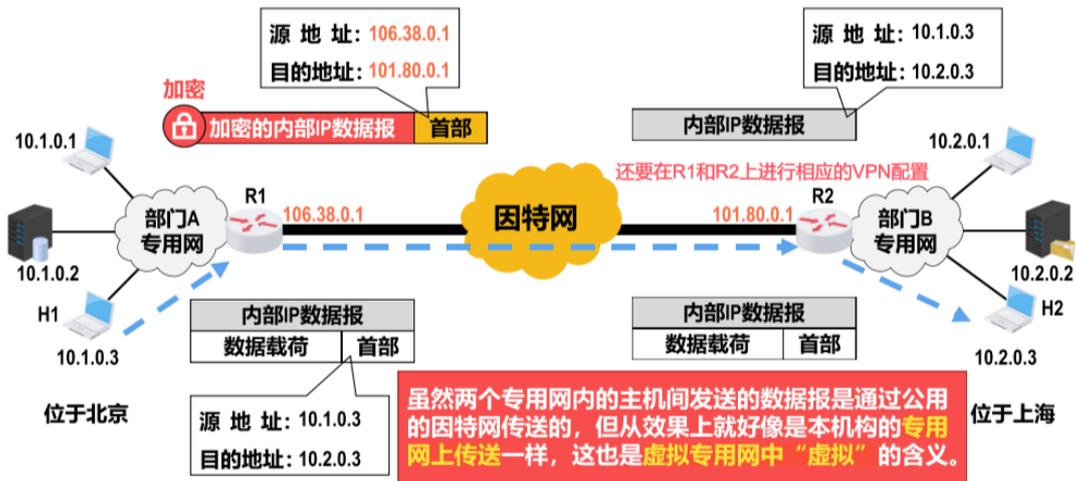
相关原则：
 (1) 若存在多条最短路径，则只保留邻居路由器 IP 地址最小的路径。
 (2) 反向路径含义是在计算最短路径时把源点当作终点。

举例：



(4) 因特网的多播路由选择协议建议方案包括距离向量多播路由选择协议 DVMRP、开放最短路径优先的多播扩展 MOSPF 等，但 **IP 多播都没有大规模应用。应用层多播成为实际方案。**

2、虚拟专用网 VPN：通过公有网络（如互联网）建立安全、可靠的专用网络，又称 **IP 隧道技术**。



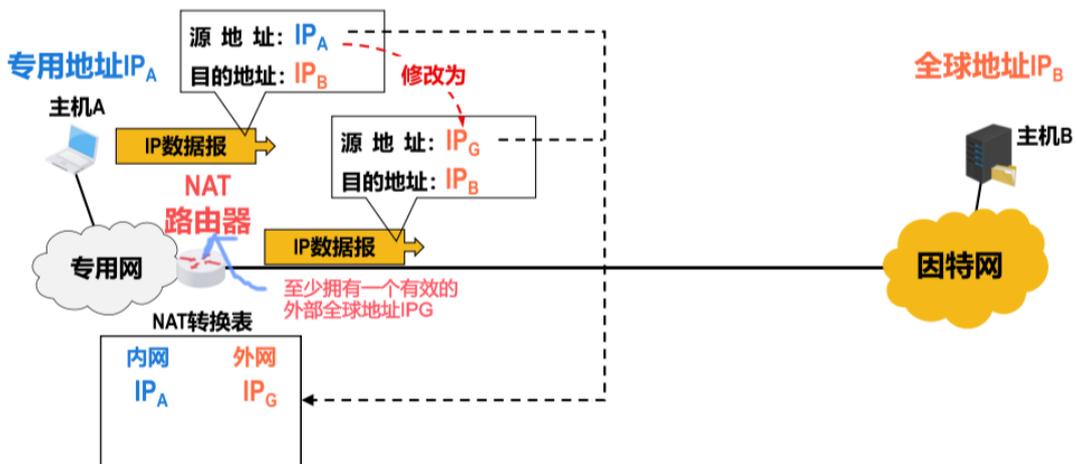
(1) 专用地址: 只能用于一个机构的内部通信,而不能用于和互联网上的主机通信。在互联网中的所有路由器,对目的地地址是专用地址的数据报一律不进行转发。

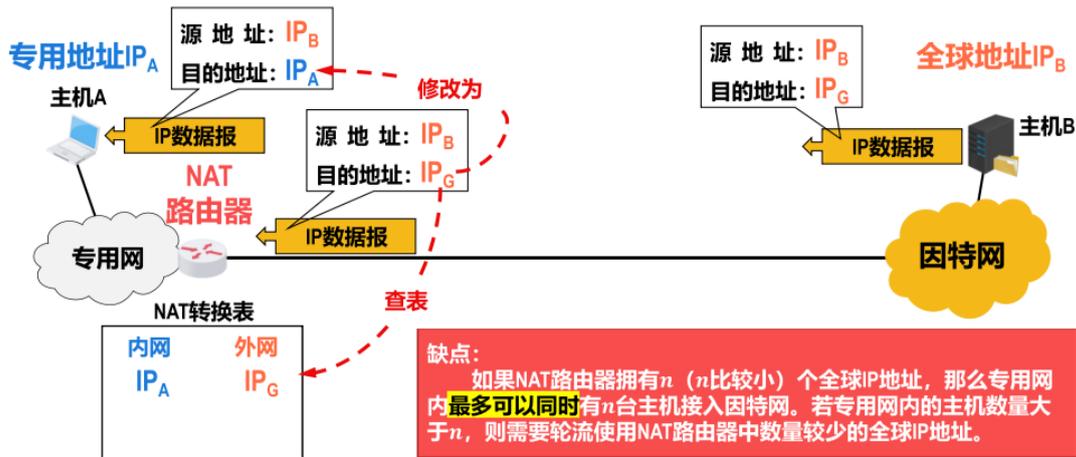
- 10.0.0.0 到 10.255.255.255 (或记为 10.0.0.0/8, 又称为 24 位块)
- 172.16.0.0 到 172.31.255.255 (或记为 172.16.0.0/12, 又称为 20 位块)
- 192.168.0.0 到 192.168.255.25 (或记为 192.168.0.0/16, 又称为 16 位块)

3、网络地址转换 NAT: 使大量使用内部专用地址的专用网络用户共享少量外部全球地址来访问因特网上的主机和资源,缓解 IPv4 地址空间即将耗尽的问题。

(1) 网络地址与端口号转换方法 (NAPT): 对源端口号重新动态分配,将 NAT 转换和运输层端口号结合使用,进一步提高 NAT 效率。

(2) NAT (NAPT) 缺点总结: 对网络应用并不完全透明;通信必须有专用网先发起,外网主机不能首先发起通信(需要 NAT 穿透技术解决)。



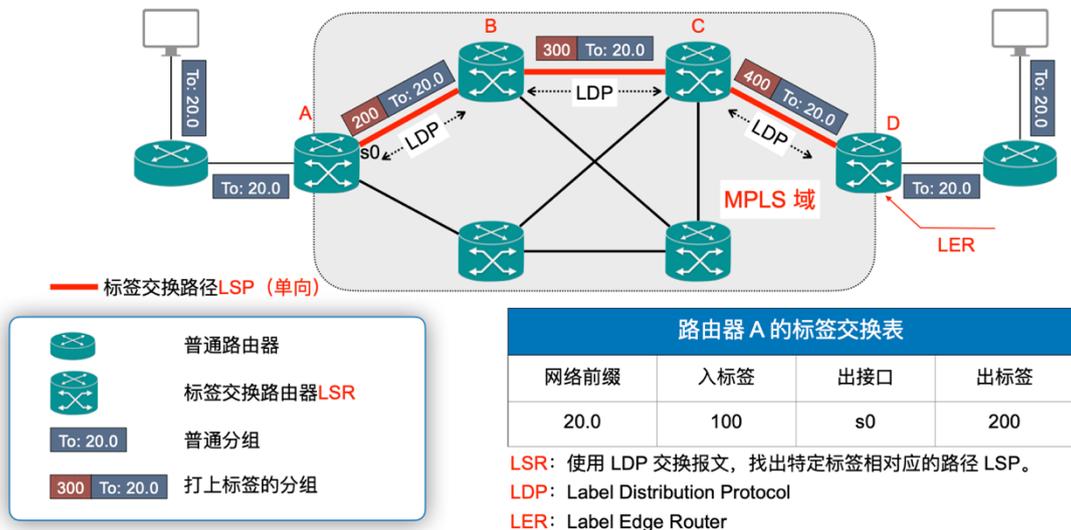


4、多协议标记交换 MPLS

(1) 基本原理:

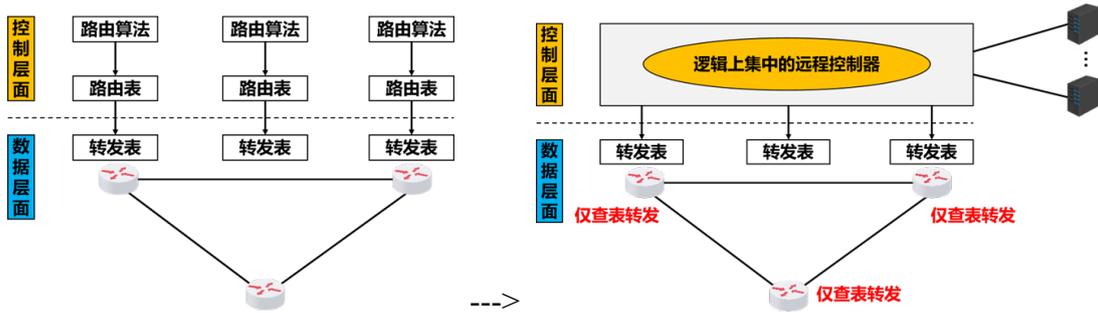
在传统的 IP 网络中，分组每到达一个路由器，都必须查找路由表，并按照“最长前缀匹配”的原则找到下一跳的 IP 地址。当网络很大时，查找含有大量项目的路由表要花费很多的时间。在出现突发性的通信量时，往往还会使缓存溢出，这就会引起分组丢失、传输时延增大和服务质量下降。

MPLS 在 MPLS 域的入口处，给每一个 IP 数据报打上固定长度“标记”，然后对打上标记的 IP 数据报用硬件进行转发，这就使得 IP 数据报转发的过程大大地加快了。采用硬件技术对打上标记的 IP 数据报进行转发就称为标记交换。“交换”也表示在转发时不再上升到第三层查找转发表，而是根据标记在第二层（链路层）用硬件进行转发。MPLS 可使用多种链路层协议，如 PPP、以太网、ATM 以及帧中继等。



5、软件定义网络 SDN

(1) 基本原理: 斯坦福大学的 Nick McKeown 教授于 2009 年提出的一种新型网络体系结构，谷歌于 2010~2012 年间建立的数据中心网络 B4 是 SDN 最成功的应用案例。其核心思想是把网络的控制层面和数据层面分离，而让控制层面利用软件来控制数据层面设备，数据平面执行匹配转发。



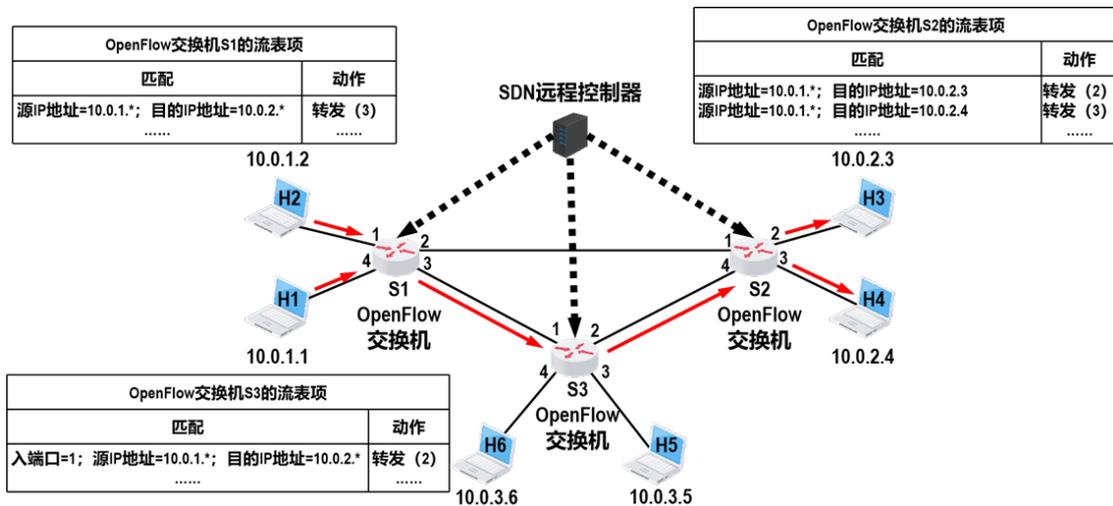
(2) 在 SDN 中取代传统路由器中转发表的是流表 (Flow Table)

OpenFlow1.0版本的流表		
首部字段值	计数器	动作
首部字段值	计数器	动作
...
首部字段值	计数器	动作

首部字段值字段包含11个项目涉及三个层次的首部

入端口	源 MAC地址	目的 MAC地址	类型	ID	优先级	源 IP地址	目的 IP地址	协议	服务类型	源 端口	目的 端口
	以太网			VLAN		IP			TCP/UDP		
数据链路层						网际层			运输层		

(3) 简单转发案例



三、重点习题

P202: 全部