网络技术与信息安全

第3讲：接入互联网

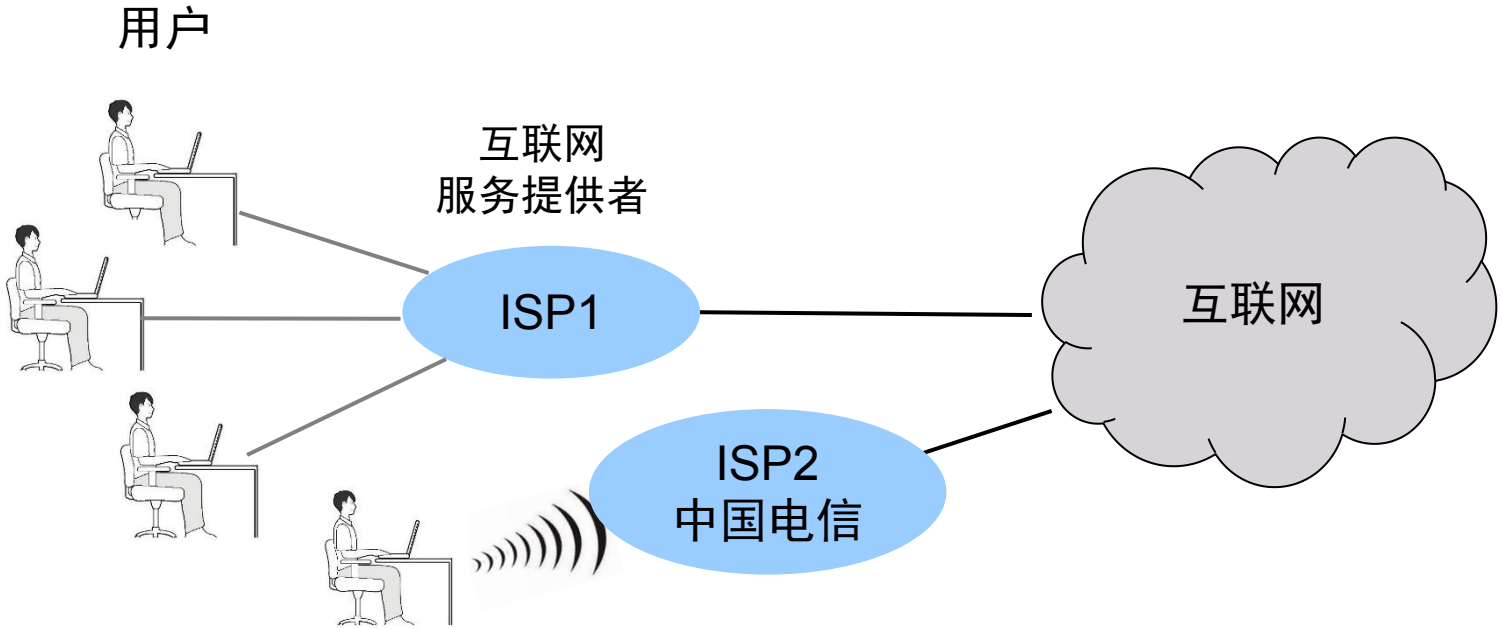
河南中医药大学信息技术学院
许成刚

一、基本概念

1. 基本概念

Internet接入的概念

- Internet接入是通过特定的信息采集与共享的传输通道，利用某种传输技术完成用户与IP广域网的高带宽、高速度的物理连接。
- 家庭或单位用户要接入Internet，可通过某种通信线路连接到ISP（Internet服务提供商），由ISP提供Internet的入网连接和信息服务。



用户通过ISP接入互联网

（有线接入或无线接入）

➢ 接入方式汇总

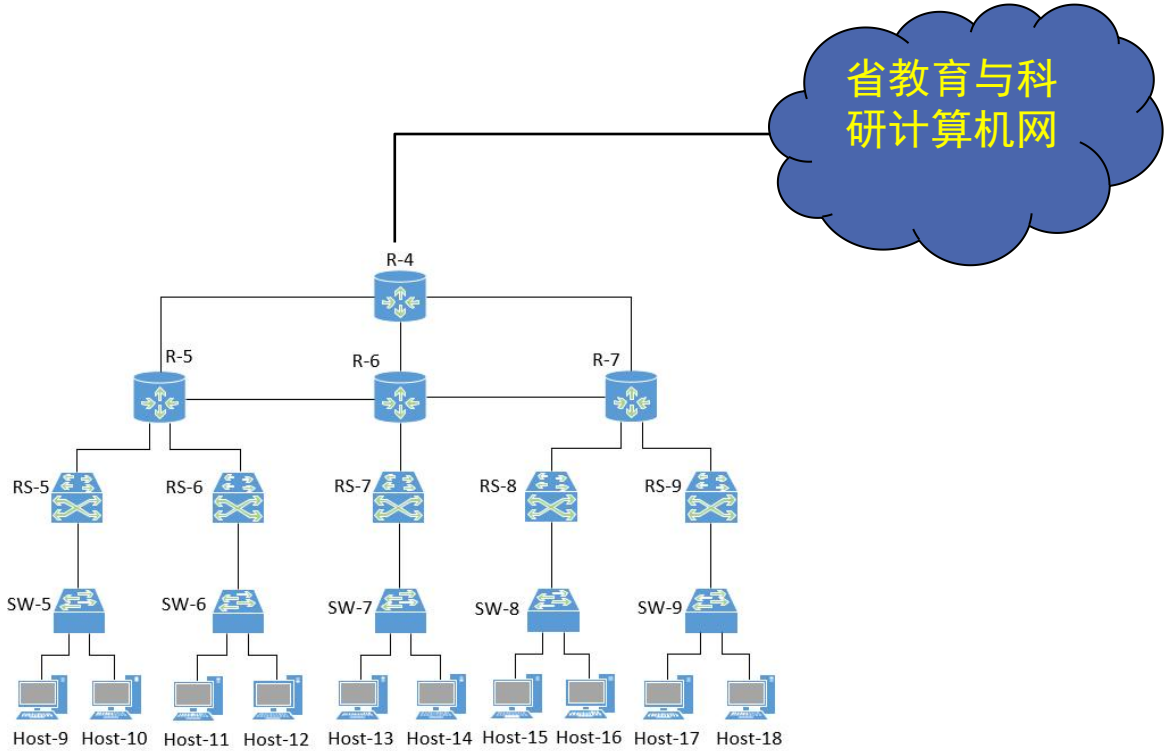
- 网络接入
  - 园区网接入
    - RIP/OSPF/BGP：与上级网络互联
    - NAT：接入到ISP
  - 个人用户接入
    - ADSL（电话线+Modem）
    - ADSL（EPON，光纤+光Modem+波分，单条光纤）
    - 无线网络（WLAN，4G，5G）
  - 案例分析
    - 案例1：家庭局域网接入ISP
    - 案例2：实验中心局域网接入校园网
    - 案例3：园区网双链路NAT接入互联网

二、园区网接入

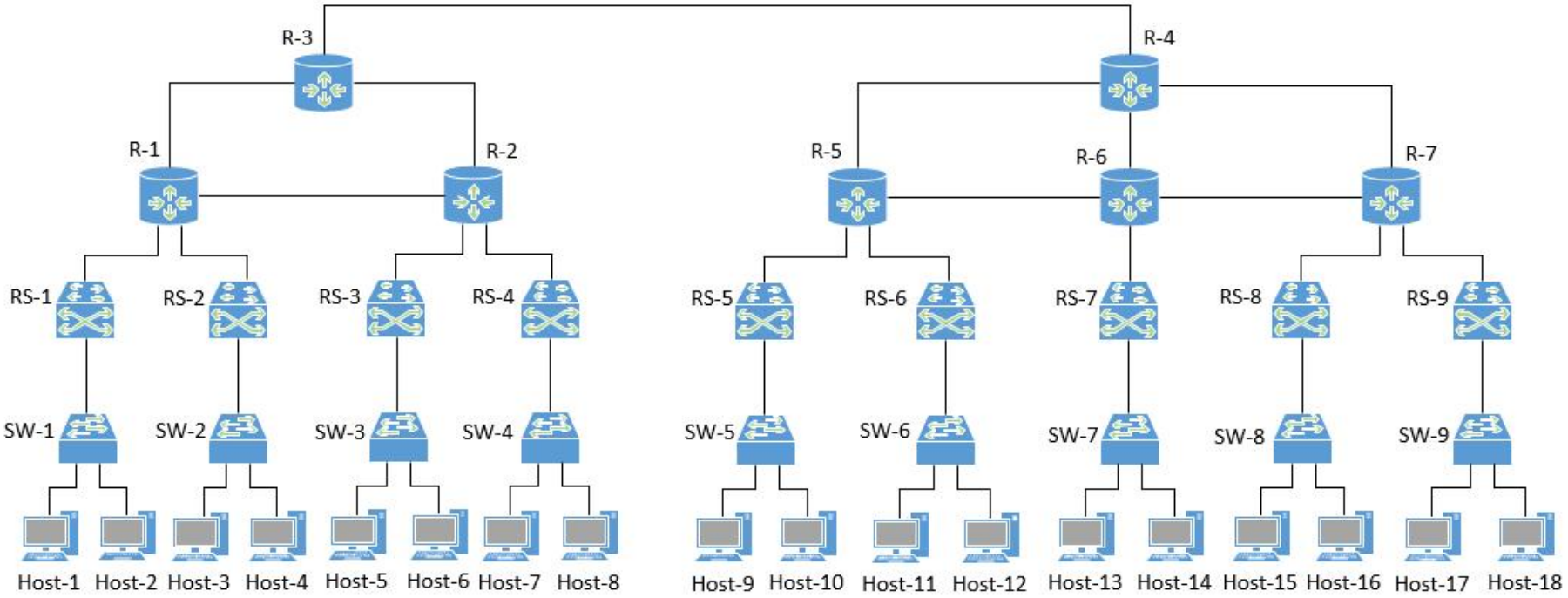
（路由接入）

接入方式 —— 园区网接入

- 举例：河南中医药大学接入省教科网



接入方式 —— 园区网接入 — OSPF/BGP方式接入



举例：河南中医药大学接入省教科网

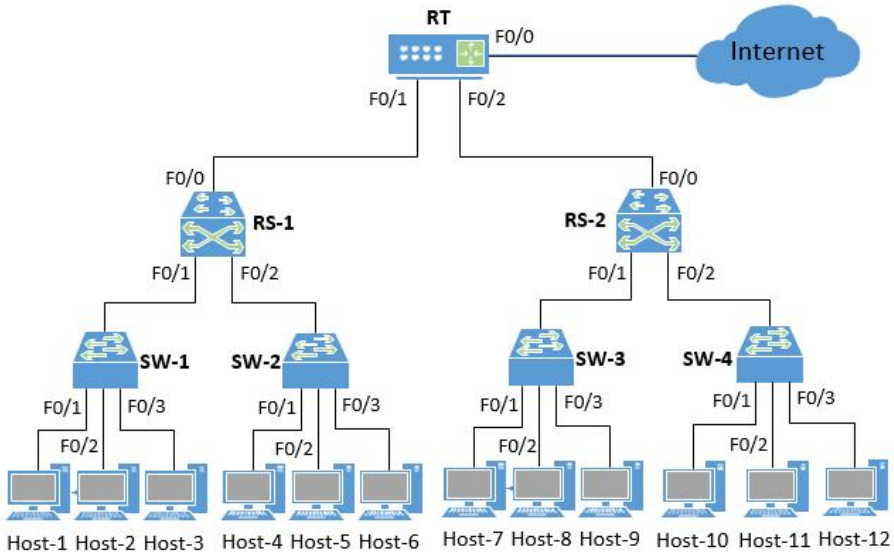
三、园区网接入

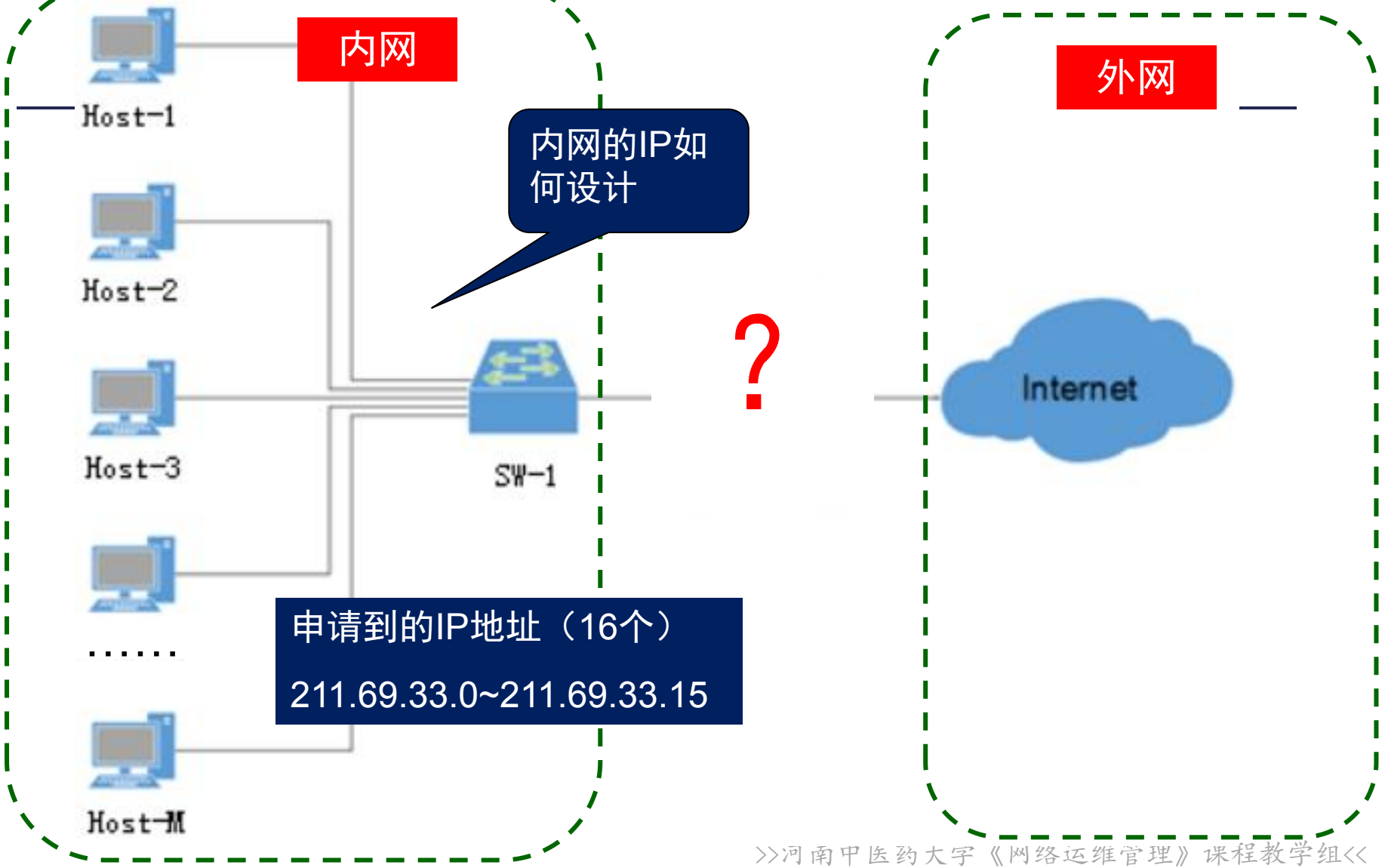
（NAT接入）

接入方式—— 企业网（以太网）NAT接入互联网

举例：

- 当一个企业网分配到的IP地址很少时（例如，某单位购买了联通的数字链路，联通为其提供了一个包含16个IP地址的地址块），如何实现内部局域网（多台计算机）接入互联网？




内网
外网
Host-1
Host-2
Host-3
Host-M
SW-1
内网的IP如何设计
?
Internet
申请到的IP地址（16个）
211.69.33.0~211.69.33.15

接入方式—— 企业网（以太网）NAT接入互联网

- 做法：
  - 内部网使用私有IP地址，通过网络地址转换（NAT），接入互联网。

接入方式—— 企业网（以太网）NAT接入互联网

回忆：私有地址

- 在可供分配的主机IP地址资源中，还可以分为公有IP地址和私有IP地址两类。
- 共有IP地址是连接到公用网络的主机使用的，必须是唯一的，需要统一管理和分配，通常从Internet服务提供者（ISP）处获得。
- 私有IP地址被保留给使用TCP/IP协议的内部网络使用的。
  - 内部网络由于不与外部网络互连，因而网络管理者可以使用任意的IP地址，只要内部相互之间IP不重复即可。之所以保留专门的私有IP地址供其使用，其目的是为了避免以后接入公网时引起地址混乱。

接入方式—— 企业网（以太网）NAT接入互联网

- 回忆：私有地址

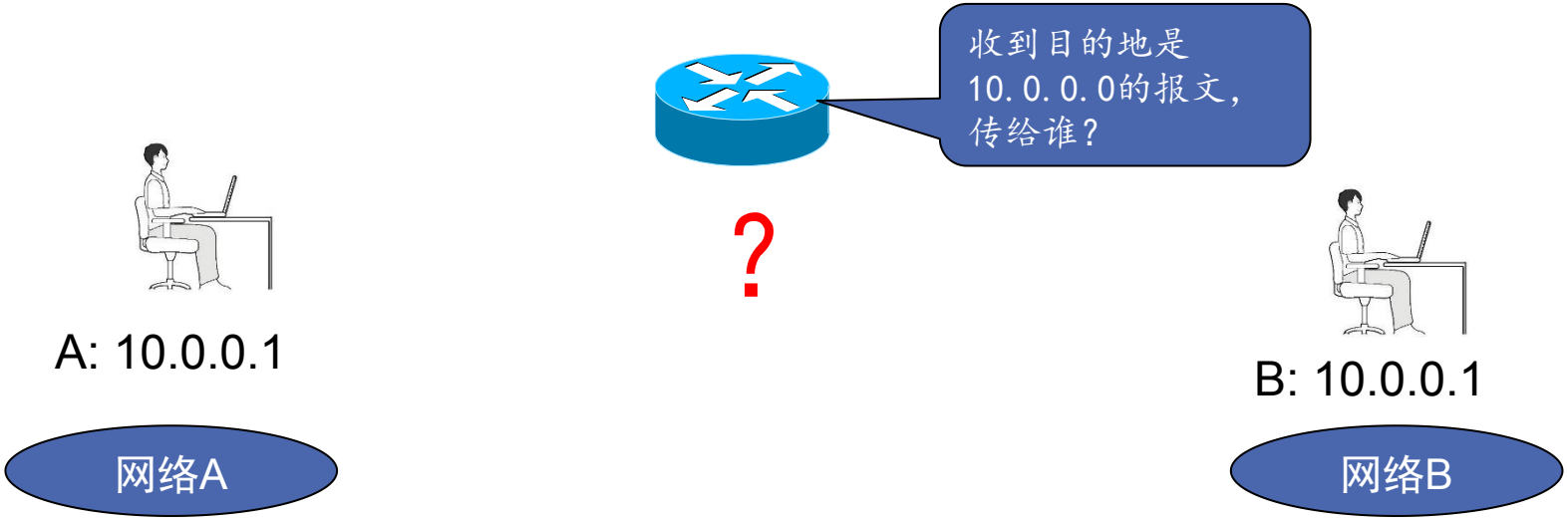
A、B、C三类地址中均有部分地址被用作私有地址。

地址类型	私有地址范围	网络个数
A类	10.0.0.0 ~10.255.255.255	1个A
B类	172.16.0.0 ~ 172.31.255.255	16个B
C类	192.168.0.0 ~ 192.168.255.255	256个C

接入方式—— 企业网（以太网）NAT接入互联网

回忆：私有地址

- 根据规定，所有以私有地址为目标地址的数据包，都不能被路由到Internet上。（防止在Internet上出现IP地址冲突）

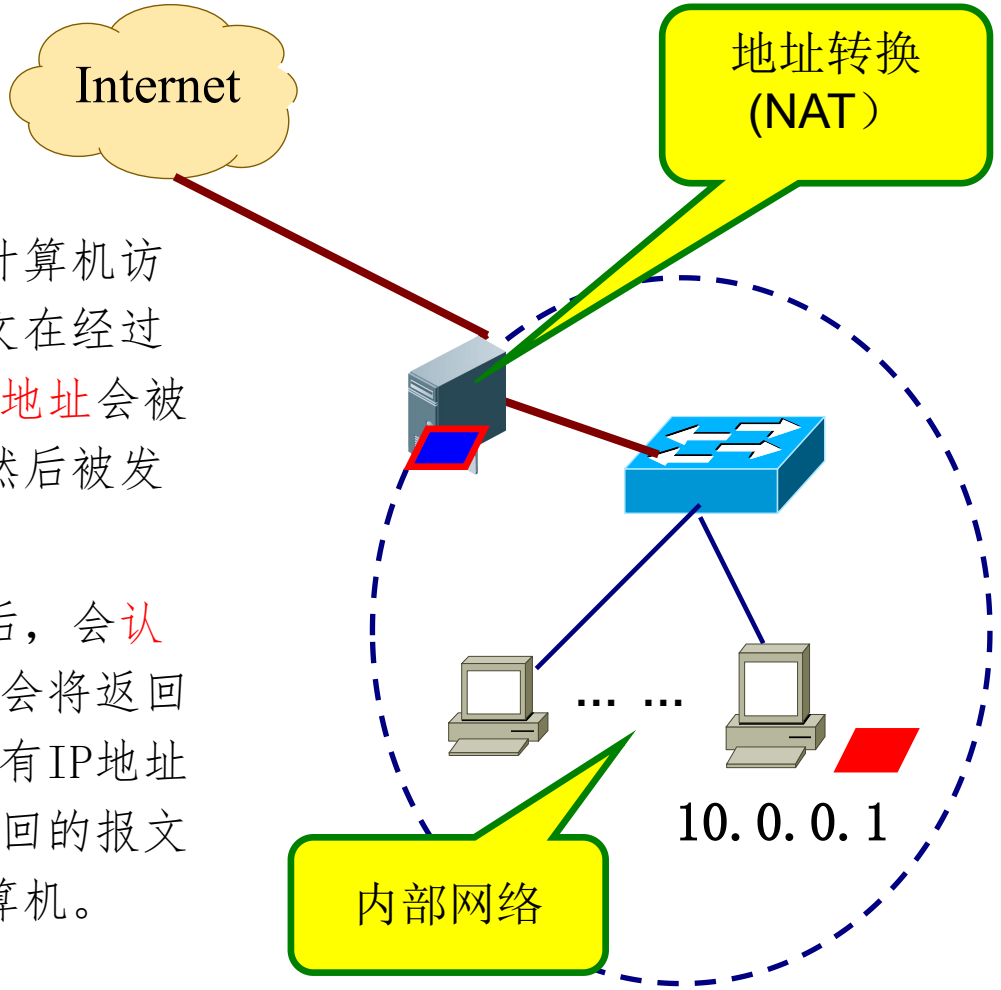


接入方式—— 企业网（以太网）NAT接入互联网

使用NAT

- 使用私有IP地址的内部网络在接入Internet（或外部网络）时，要使用网络地址转换（NAT），将私有地址转换成公有地址，然后才能访问Internet。

- 当内部网中使用私有地址的计算机访问Internet时，所发出的报文在经过NAT设备时，报文首部的源IP地址会被转换成指定的公有IP地址，然后被发送到互联网上。
- 互联网的目的用户收到报文后，会认为该报文来自NAT设备，因此会将返回报文发送给NAT设备上指定公有IP地址接口。然后，NAT设备再将返回的报文转发给内部网中的相应的计算机。

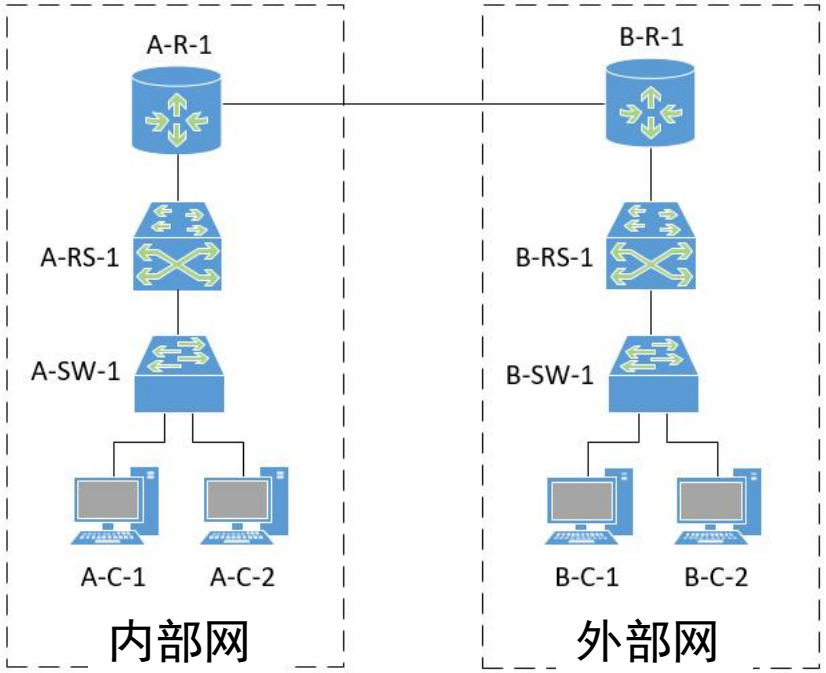


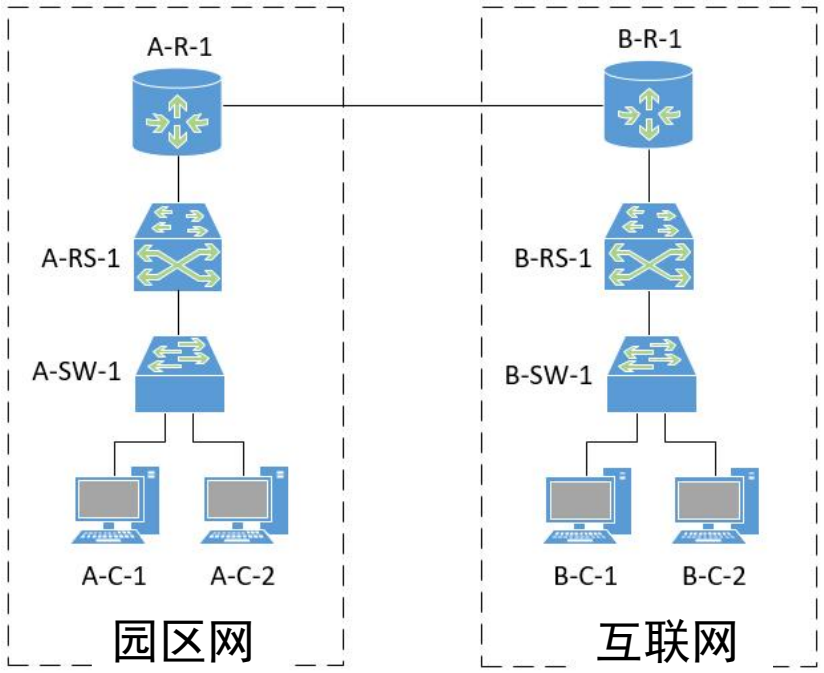
接入方式—— 企业网（以太网）NAT接入互联网

网络地址转换（NAT）

- 网络地址转换（Network Address Translation，NAT），也称IP地址伪装技术（IP Masquerading）。
- 最初设计NAT的目的是允许将私有IP地址映射到公网上（合法的因特网IP地址），以缓解IP地址短缺的问题。
- NAT带来的安全性：通过NAT，不仅可以解决IP的问题，而且可以防止互联网用户掌握内部网络结构，因此从一定程度上降低了内部网络被攻击的可能性，提高了私有网络的安全性。因此，企业网（园区网）通常在内部采用私有IP，通过NAT接入互联网。

特别强调：NAT的功能是进行地址转换，**并不是**只能用于私有地址向公有地址的转换，即并不是只能用于私有网络接入互联网的场合。

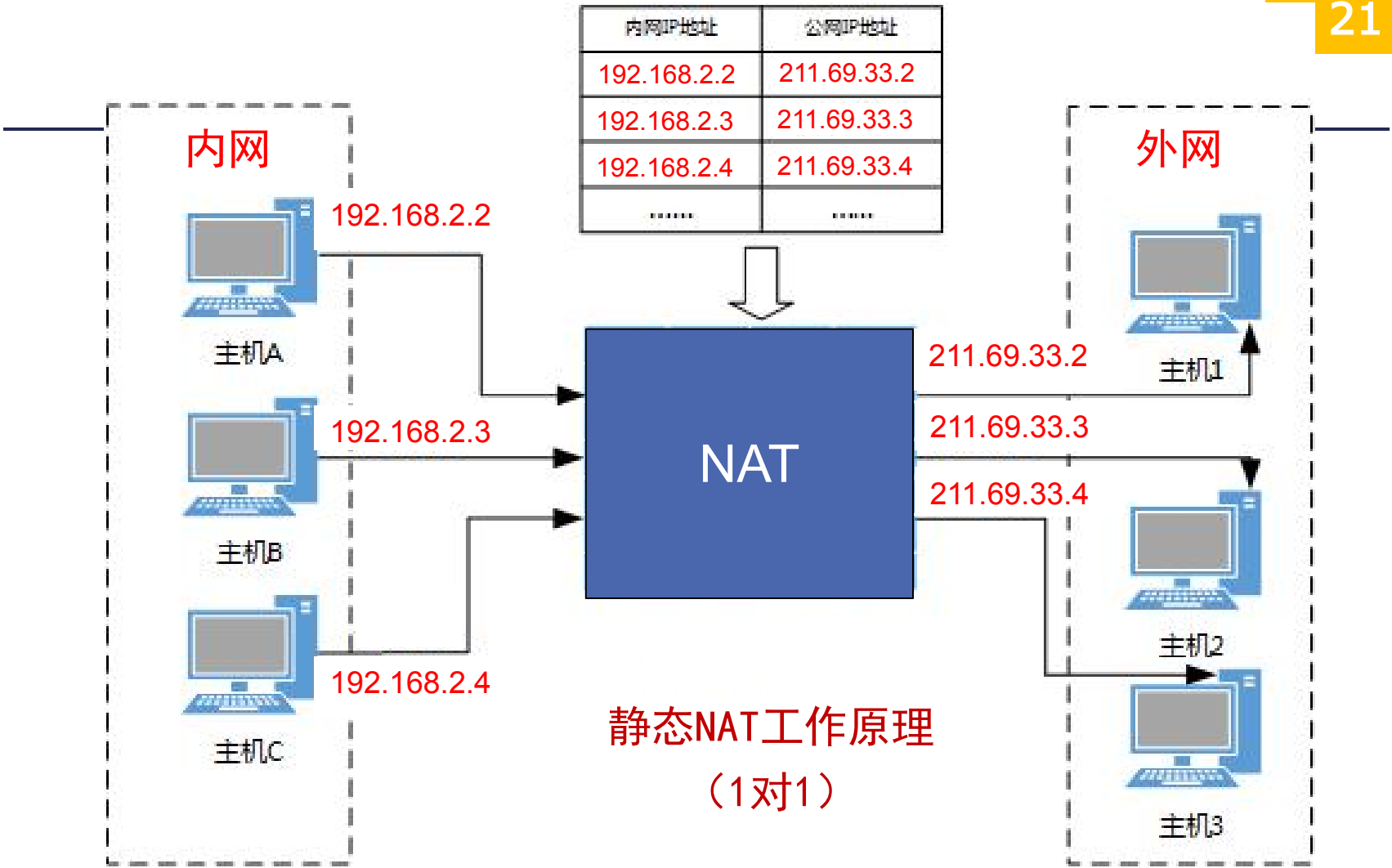




接入方式—— 企业网（以太网）NAT接入互联网

- NAT的实现方式有三种

1、静态转换:是指内部本地地址一对一转换成内部全局地址，相当内部本地的每一台PC都绑定了一个全局地址。一般用于在内网中对外提供服务的服务器。

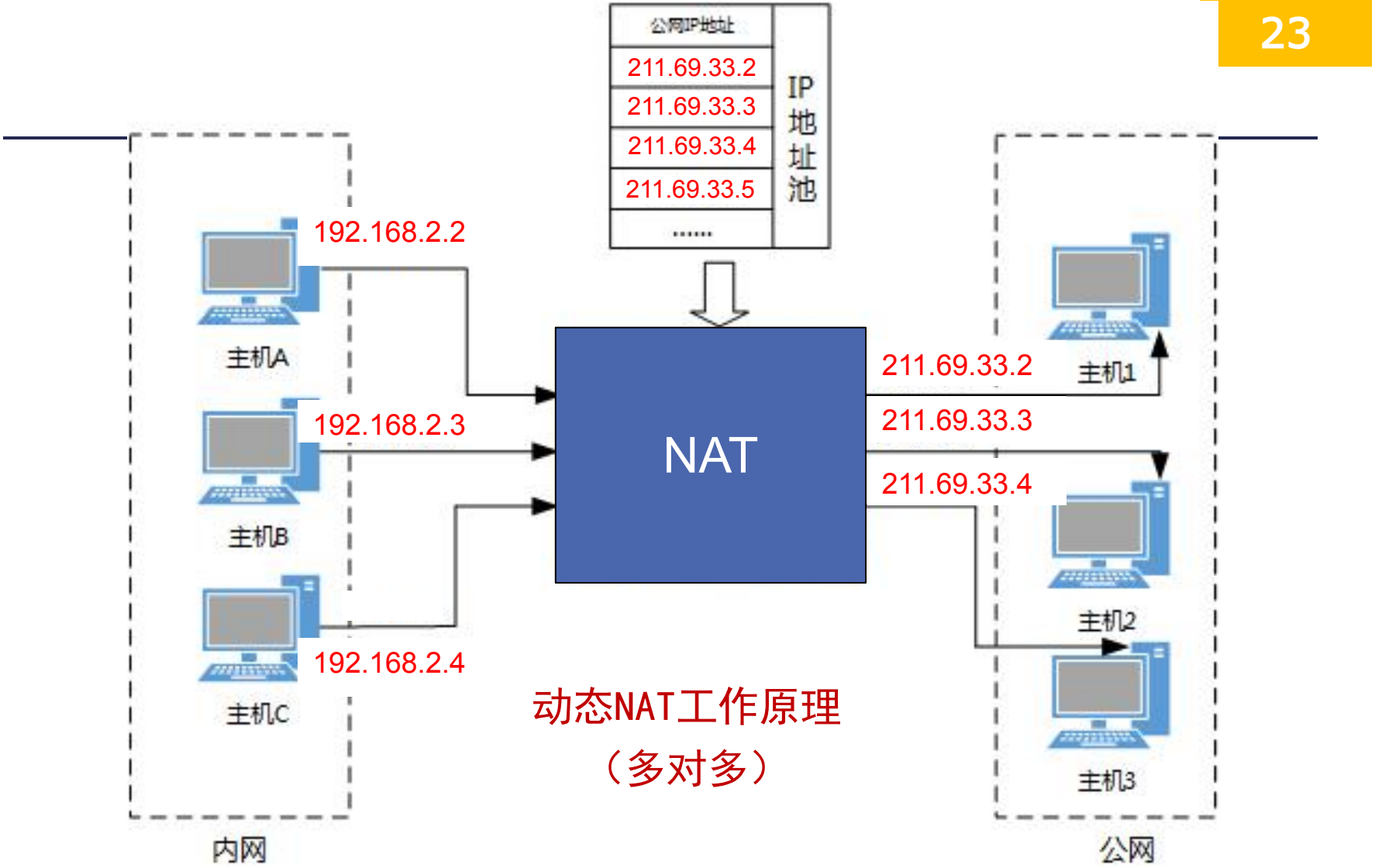

内网IP地址
公网IP地址
192.168.2.2
211.69.33.2
192.168.2.3
211.69.33.3
192.168.2.4
211.69.33.4
.....
.....
内网
外网
192.168.2.2
主机A
192.168.2.3
主机B
192.168.2.4
主机C
NAT
211.69.33.2
211.69.33.3
211.69.33.4
主机1
主机2
主机3
静态NAT工作原理
（1对1）

接入方式—— 企业网（以太网）NAT接入互联网

NAT的实现方式有三种

2、动态转换:是指将内部网络的私有IP地址转换为公用IP地址时，IP地址是不确定的，是随机的，所有被授权访问上Internet的私有IP地址可随机转换为任何指定的合法IP地址。也就是说，只要指定哪些内部地址可以进行转换，以及用哪些合法地址作为外部地址时，就可以进行动态转换。

- 当ISP提供的合法IP地址略少于网络内部的计算机数量时，可以采用动态转换的方式。

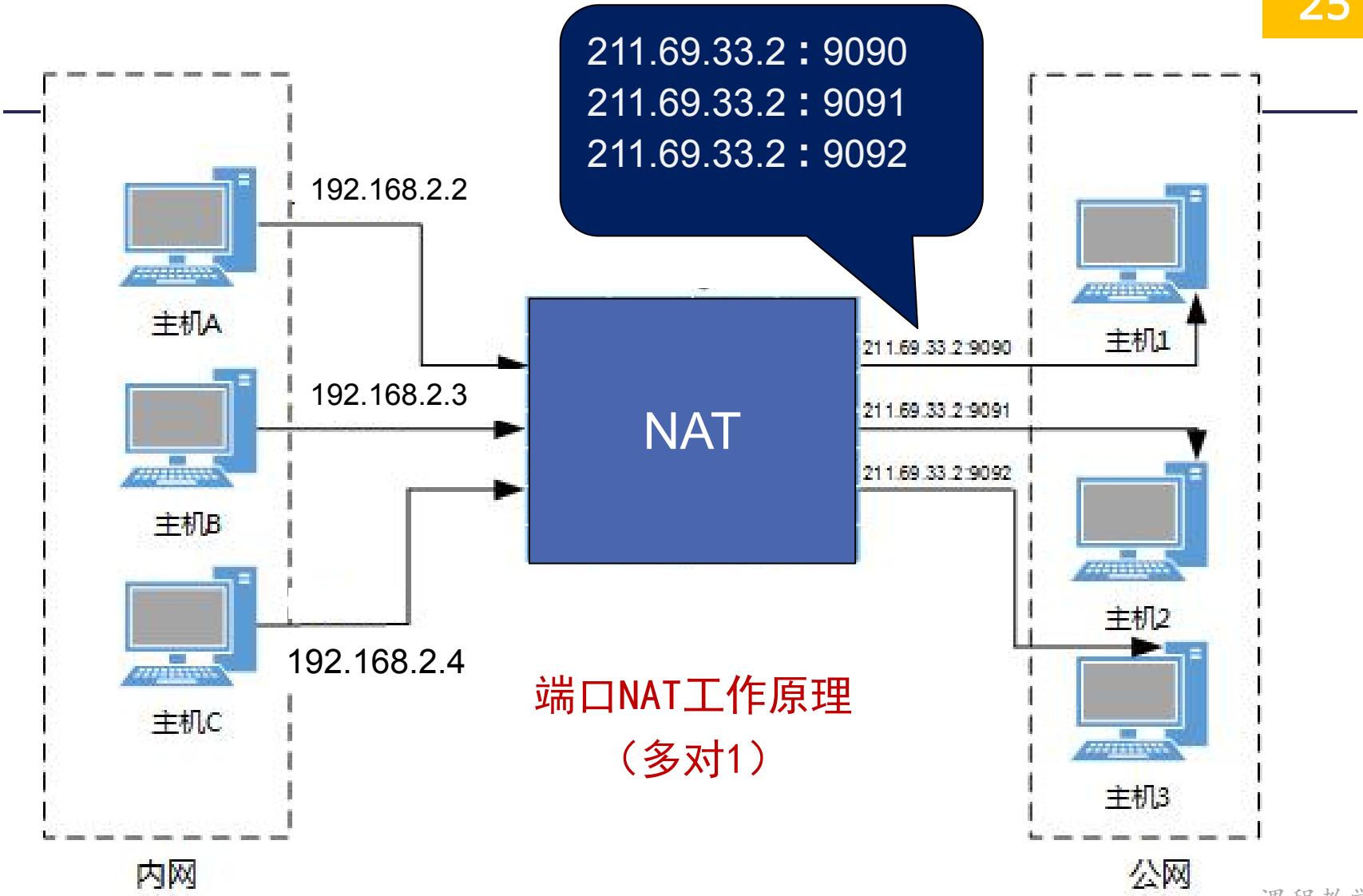

公网IP地址
211.69.33.2
211.69.33.3
211.69.33.4
211.69.33.5
.....
IP地址池
192.168.2.2
192.168.2.3
192.168.2.4
主机A
主机B
主机C
内网
NAT
211.69.33.2
211.69.33.3
211.69.33.4
主机1
主机2
主机3
公网
动态NAT工作原理
（多对多）

接入方式—— 企业网（以太网）NAT接入互联网

- NAT的实现方式有三种

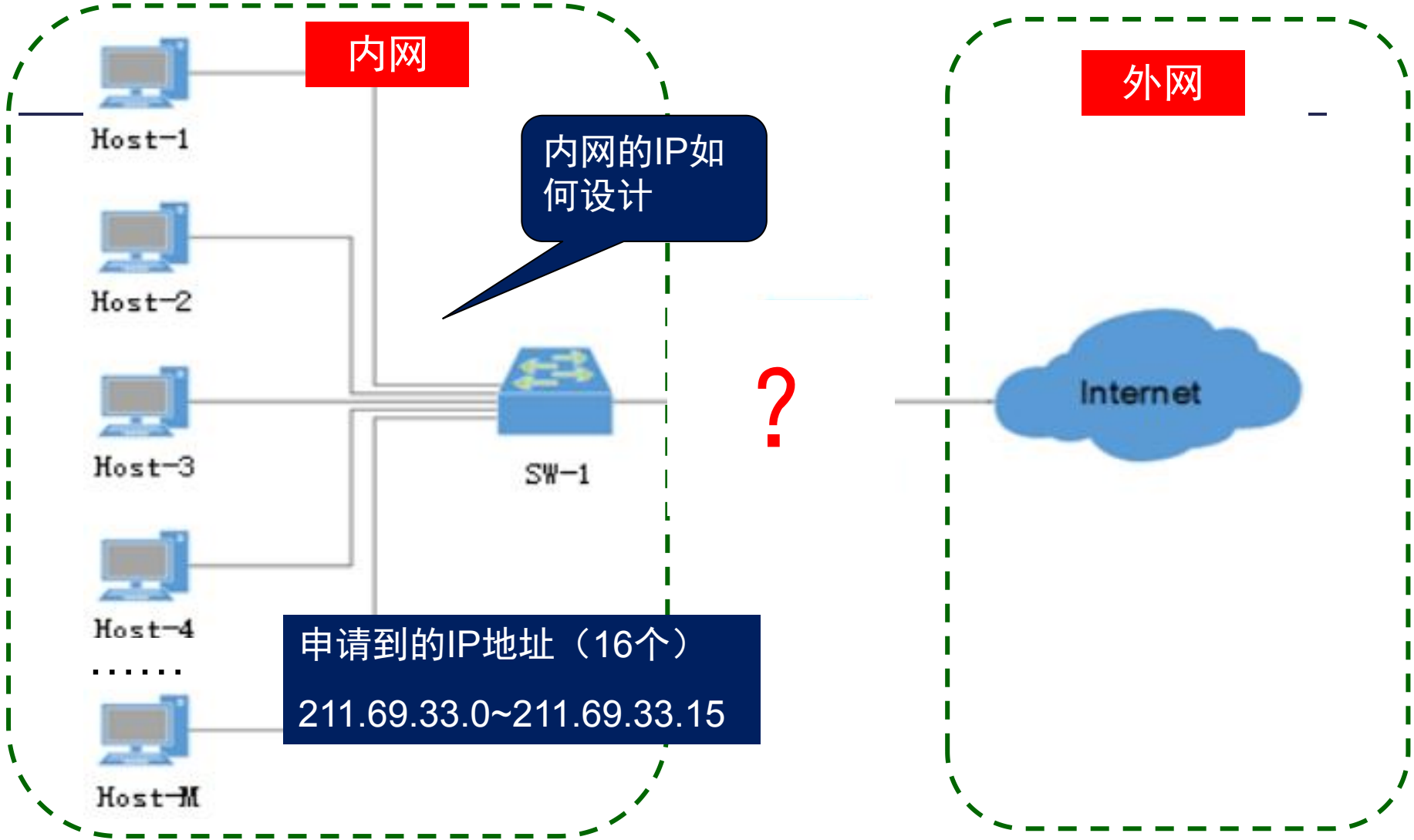
3、网络地址端口转换（Network Address Por Translation）

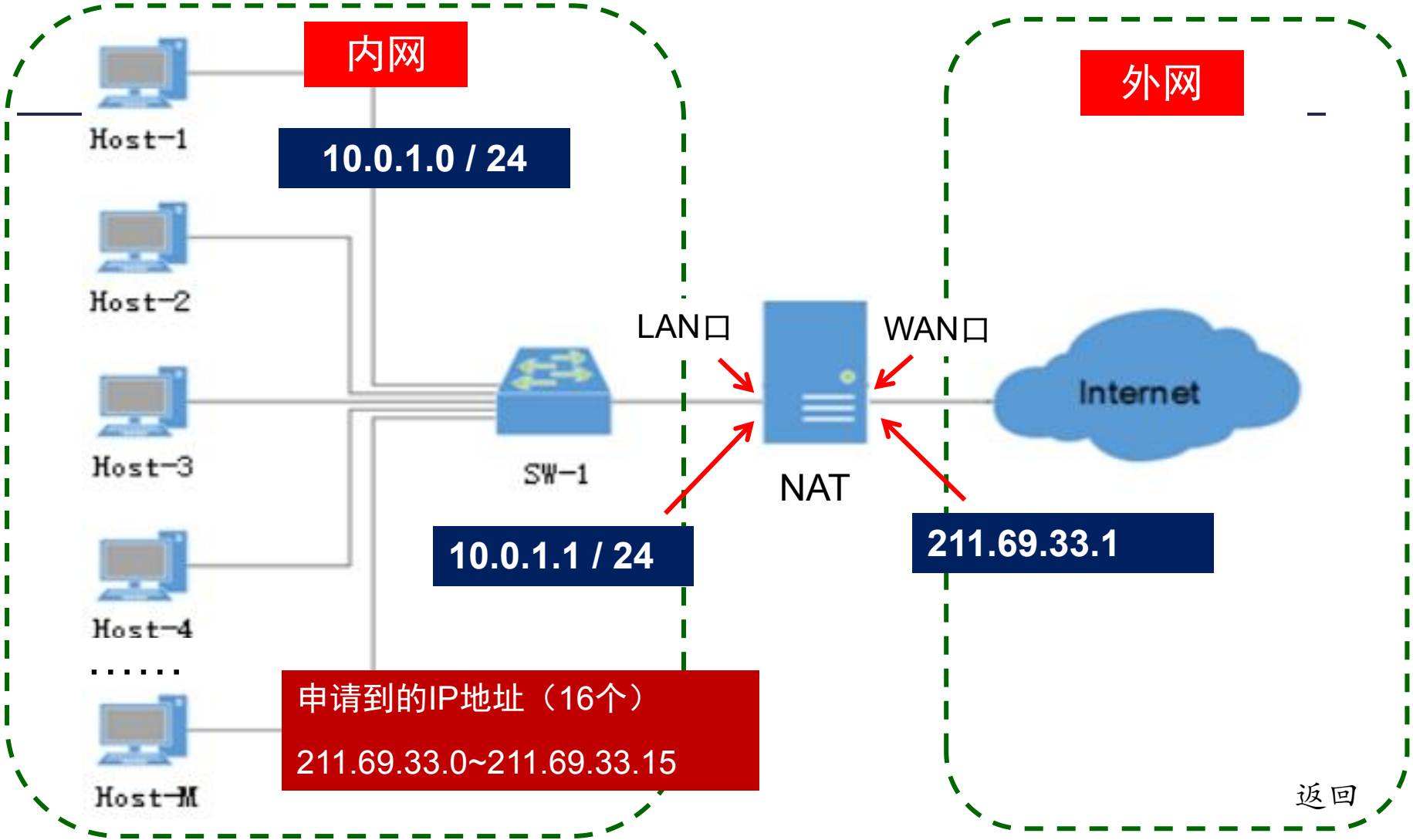
- 通过NAPT，可以将一个中小型网络的内部连接隐藏在外部网络中的一个合法的IP地址后面（即将多个内部地址映射为一个合法公网地址），同时在该地址上加上一个由NAT设备选定的TCP端口号（即以不同的协议端口号与不同的内部地址相对应），也被称为“多对一”的NAT。
- NAPT可以最大限度地节约IP地址资源，同时，又可隐藏网络内部的所有主机，有效避免来自Internet的攻击。因此，网络中应用最多的就是端口多路复用方式。。



端口NAT工作原理

（多对1）


内网
外网
Host-1
Host-2
Host-3
Host-4
.....
Host-M
SW-1
内网的IP如何设计
?
Internet
申请到的IP地址（16个）
211.69.33.0~211.69.33.15


内网
外网
Host-1
Host-2
Host-3
Host-4
.....
Host-M
10.0.1.0 / 24
SW-1
LAN口
WAN口
NAT
Internet
10.0.1.1 / 24
211.69.33.1
申请到的IP地址（16个）
211.69.33.0~211.69.33.15
返回

四、用户接入

（ADSL方式接入）

4. 接入方式 —— ADSL

ADSL

- ADSL（Asymmetric Digital Subscribe Line，不对称数字用户线路）使用普通电话线作为传输介质。
- ADSL的优点在于它可以将数据通信与普通电话共存于一条电话线上，上网和打电话，可以同时进行而又互不影响。

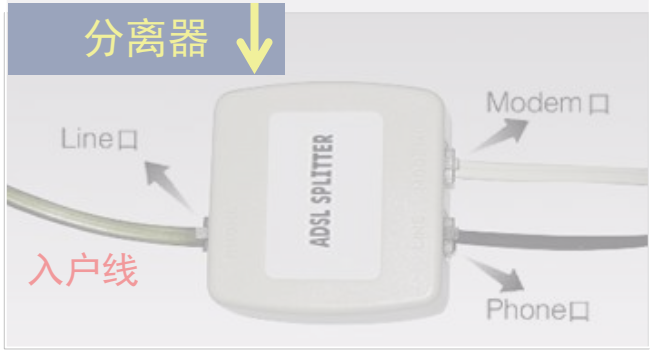
4. 接入方式 —— ADSL

ADSL

- ADSL采用频分复用技术把普通的电话线分成了电话、上行和下行3个相对独立的信道，使用40KHz以上频率传输数据，40KHz以下用来传输语音，避免了相互之间的干扰。
- 不对称数字用户线路：ADSL是一种上行和下行速率不对称的技术，其下行速率（可以达到1.5Mb/s~8Mb/s）要远远高于上行速率（一般为512b/s～1Mb/s）。

ADSL接入中用到的设备

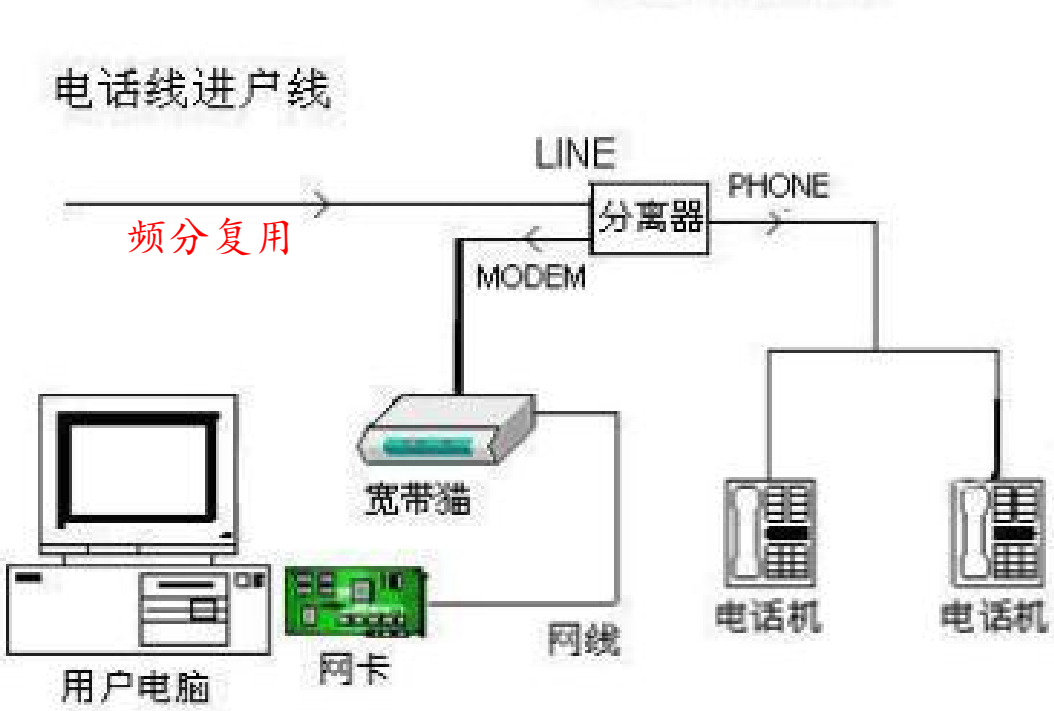
调制解调器（modem）



所谓调制，就是把数字信号转换成电话线上传输的模拟信号；解调，即把模拟信号转换成数字信号。合称调制解调器。

调制解调器，是调制器和解调器的缩写，一种计算机硬件，它能把计算机的数字信号翻译成可沿普通电话线传送的模拟信号，而这些模拟信号又可被线路另一端的另一个调制解调器接收，并译成计算机可懂的语言。这一简单过程完成了两台计算机间的通信。

ADSL接入拓扑



LINE口接电话进线

PHONE口接电话机

MODEM口接宽带猫

上网和打电话同时进行而又互不影响。

五、EPON接入方式

5. 接入方式 —— EPON

PON技术

- PON（Passive Optical Network，无源光纤网络），与传统的有源光纤接入技术相比其有效消除了局端与用户端之间的有源设备，使得网络设备更加容易维护，而且应用可靠性更高、成本更低。

5. 接入方式 —— EPON

EPON

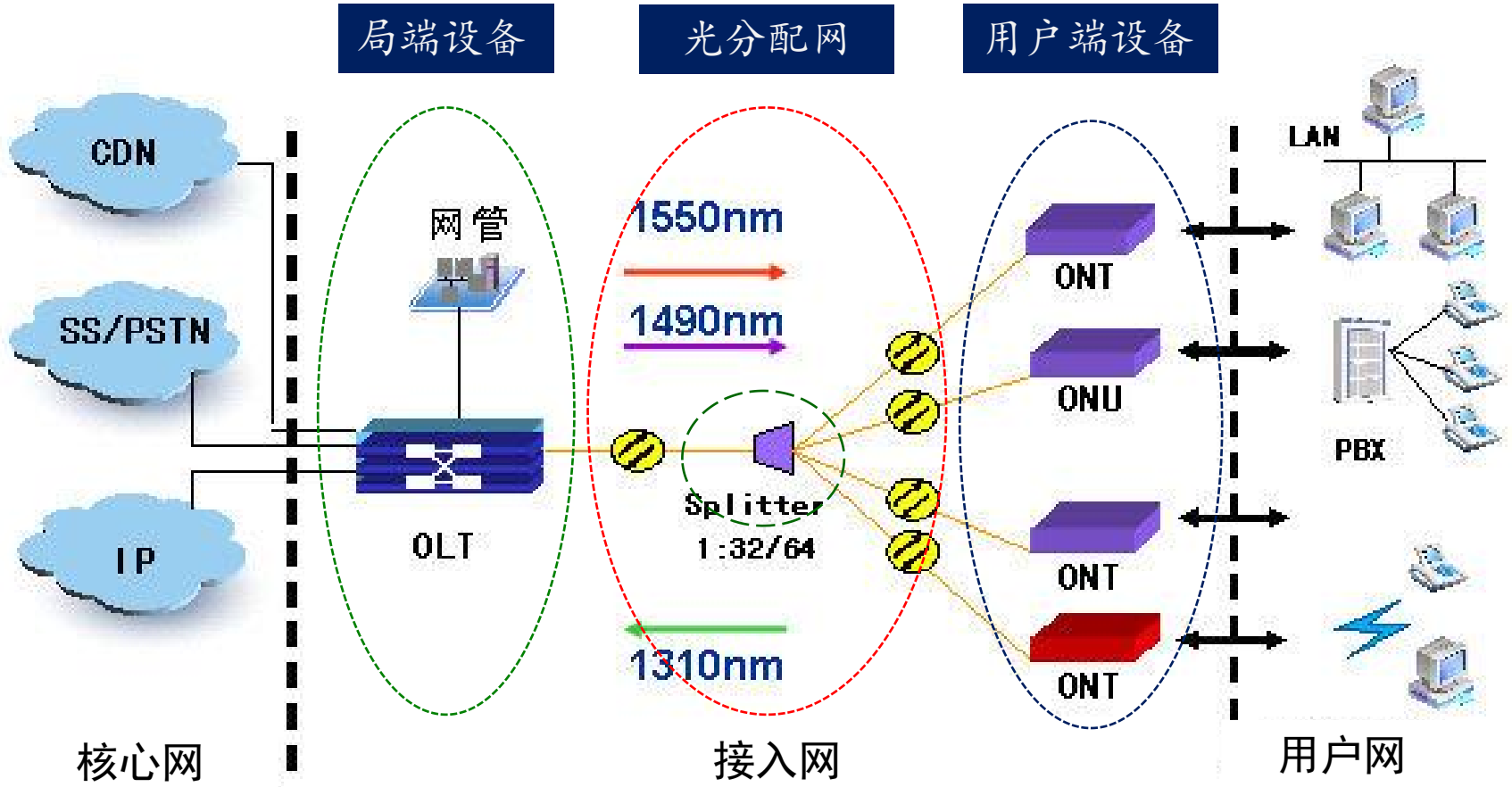
- EPON（Ethernet Passive Optical Network，以太网无源光网络），顾名思义，是基于以太网的PON技术。
- EPON将以太网和PON技术结合，在物理层采用PON技术，通过使用光纤以及光无源器件等实现了物理层传输；在数据链路层使用以太网协议，利用PON的拓扑结构实现以太网接入。

5. 接入方式 —— EPON

EPON的结构

- EPON系统由局端设备OLT（光线路终端）、用户端设备ONU（光网络单元）以及光分配网ODN（光分配网）组成。
- ODN由无源的光缆、光分/合路器等组成。
- OLT与ONU之间仅有光纤、光分路器等光无源器件，无需租用机房、无需配备电源、无需有源设备的维护人员，因此可节省建设和运营维护成本；

EPON的接入拓扑图


局端设备
光分配网
用户端设备
CDN
SS/PSTN
IP
网管
OLT
1550nm
1490nm
1310nm
Splitter
1:32/64
ONT
ONU
ONT
ONT
LAN
PBX
核心网
接入网
用户网

5. 接入方式 —— EPON

- EPON中使用的分光器

诺可信 全新插片式PLC分光器1分8光纤分路器1比8电信级二级分光入户 插片式1分8SC/UPC

京东价 ¥45.00 降价通知　　累计评价 40+

促　销　满减　满199.00减5.00，满299.00减9.00，满399.00减12.00

配送至　北京朝阳区三环以内　有货　店铺单笔订单不满269元，收运费10元

由 诺可信旗舰店 从 广东深圳市 发货，并提供售后服务。

选择颜色　插片式1分8SC/UPC　插片式1分16SC/UPC　插片式1分4SC/UPC　插片式1分2SC/UPC

白条分期　30天免息　¥15.23×3期　¥7.73×6期　¥3.98×12期　¥2.1×24期

5. 接入方式 —— EPON

- EPON中使用的分光器


中国电信
CHINA TELECOM
PLC 光分路器

六、无线局域网接入

无线局域网的组成

DS：分布式系统，负责将帧传送到目的地

AP：接入点，管理员在安装配置AP时，需要为该AP配置至少一个服务集标识符（又叫网络标识符）SSID和一个信道。


瘦AP
无线移动终端通过AP接入园区网，进而接入互联网
PC
PC
MT
MT
AP
AP
AP
AP
Internet
PoE交换机
网关路由器
无线控制器

返回

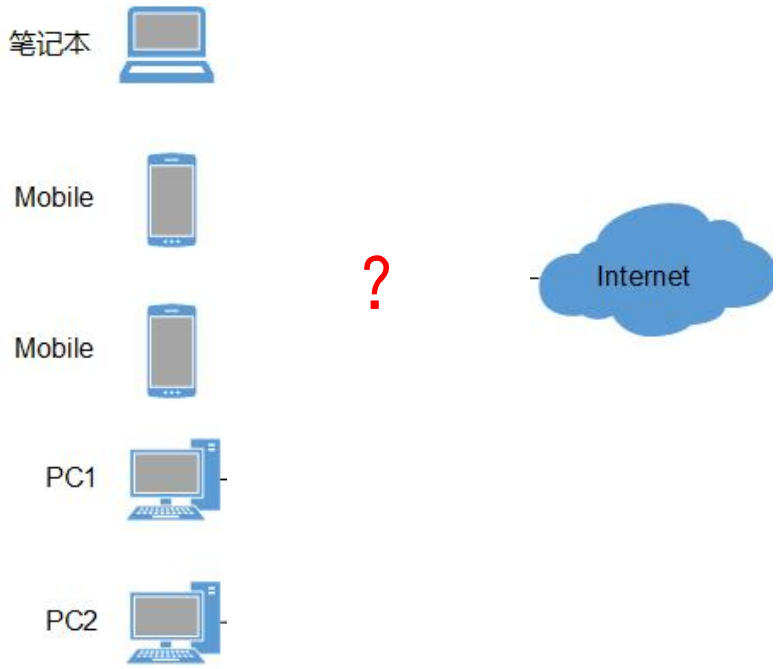
七、案例讨论

应用案例

- 案例1：家庭局域网接入互联网（ISP）的方法

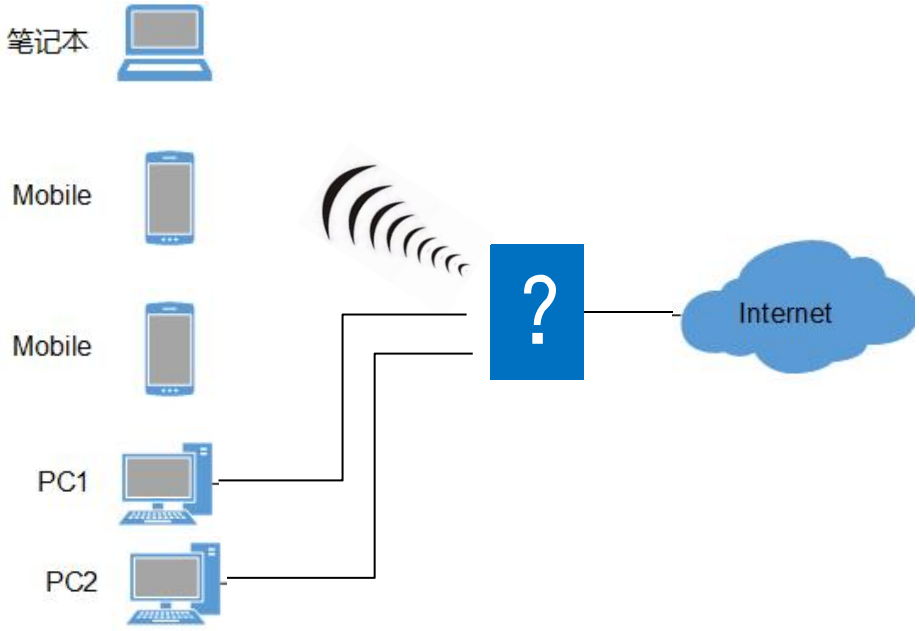
家庭局域网接入互联网的方法

- 需求：
  - 某家庭需要接入网络的设备有2台PC、1台笔记本、2部智能手机。



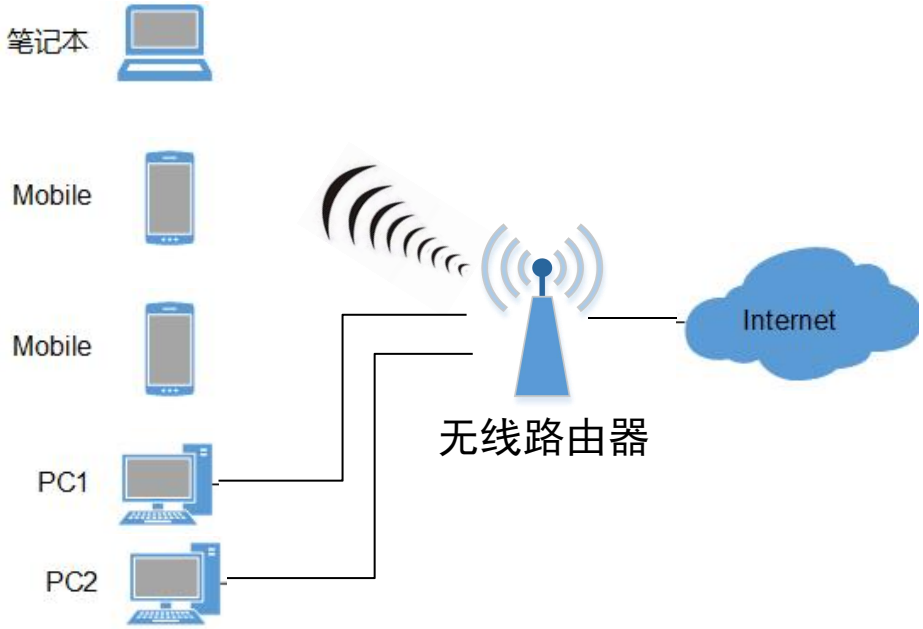
家庭局域网接入互联网的方法

- 分析：
  - 手机（或笔记本）上网，使用无线方式；
  - PC上网使用有线方式；
  - IP地址动态分配；



家庭局域网接入互联网的方法

- 实施：
  - 选择设备
    - 无线路由器




入户光纤
光猫
网线
WAN
LAN
电脑
ISP提供的用户端设备
接无线路由器的
WAN接口
接无线路由器的
LAN接口

家庭局域网接入互联网的方法

无线路由器的基本功能

- 无线终端的接入
  - 手机等移动终端可以接入无线路由器，并通过无线路由器上网。

家庭局域网接入互联网的方法

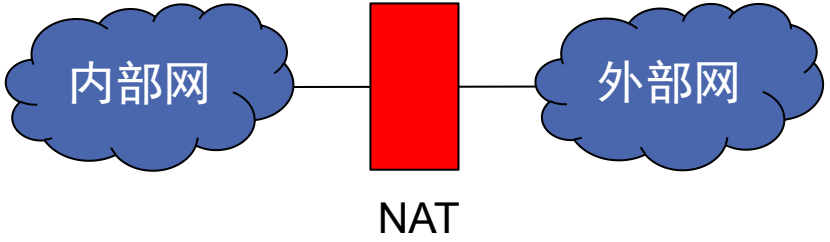
无线路由器的基本功能

- 提供DHCP服务
  - 自动为接入无线路由器的设备提供IP地址

家庭局域网接入互联网的方法

无线路由器的基本功能

- 提供NAT功能
  - 将家庭内部的私有IP地址（多个）转换成所接入的ISP分配的IP地址（1个）。



家庭局域网接入互联网的方法

- 无线路由器的基本功能
  - 接入控制（安全）功能
    - 限制哪些设备能接入无线路由器（即上网），哪些设备不能接入。

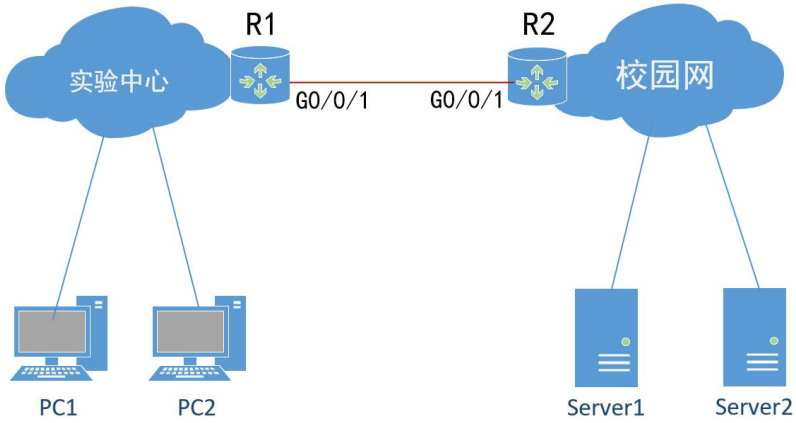
应用案例

- 案例2：实验中心局域网NAT接入校园网

案例2：实验中心局域网接入校园网

建设背景

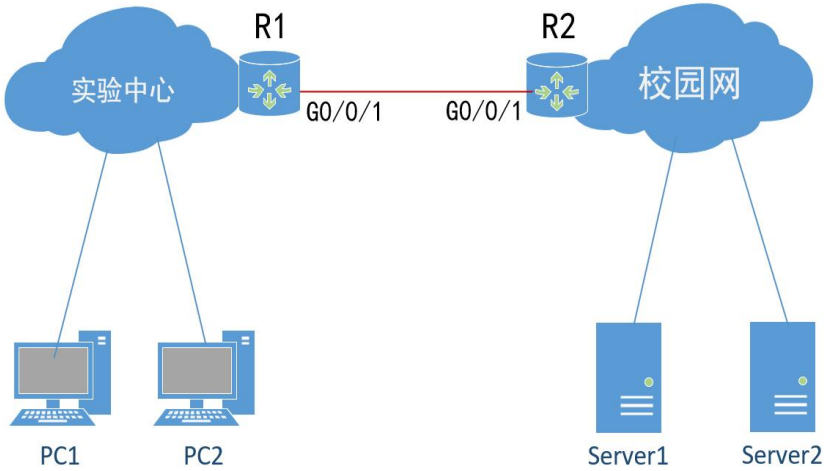
- 信息技术学院实验教学中心包含有若干个实验室（约500台计算机），并建设有覆盖全中心的局域网，使用的是192.168.*.*的IP地址。现要将实验教学中心的局域网接入到校园网中。经过与校园网管理中心沟通，获取到以下信息：
  - 实验教学中心局域网的边界路由器R1的GE0/0/1接口，通过一根光纤接入到校园网中心机房的路由器R2的GE0/0/1接口；
  - 校园网管理中心**分配**给实验教学中心的IP地址块是172.16.1.0/30，默认网关地址是172.16.1.1。
  - 初步形成实验教学中心局域网接入校园网的拓扑，如右图。



案例2：实验中心局域网接入校园网

分析

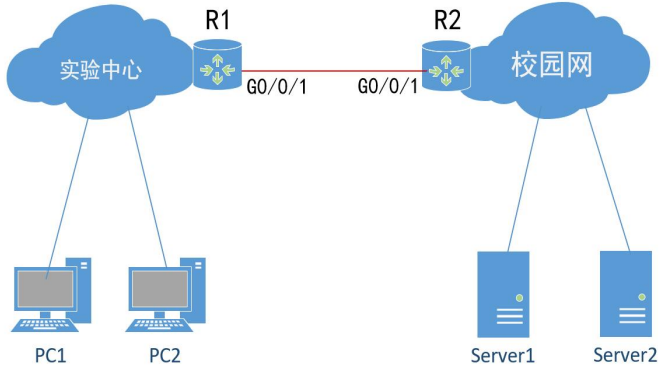
- （1）实验教学中心的局域网要接入校园网，就必须遵守校园网的IP地址分配和管理规定，即实验教学中心局域网必须使用校园网IP地址管理机构所分配的IP地址，才能接入校园网并正常通信。



案例2：实验中心局域网接入校园网

分析

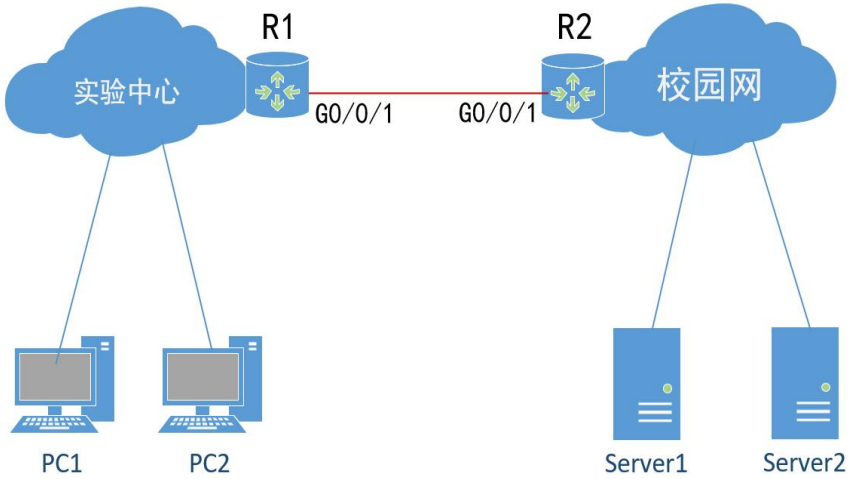
- （2）实验教学中心局域网原来使用的IP地址192.168.*.*，是不能直接接入校园网的，否则无法正常通信（即使使用光纤将R1和R2连接起来）。
  - 校园网中的路由器，是否转发目的IP地址是192.168.*.*的报文？
  - 假如校园网内部也有使用192.168.*.*的网段，会出现什么问题？



案例2：实验中心局域网接入校园网

分析

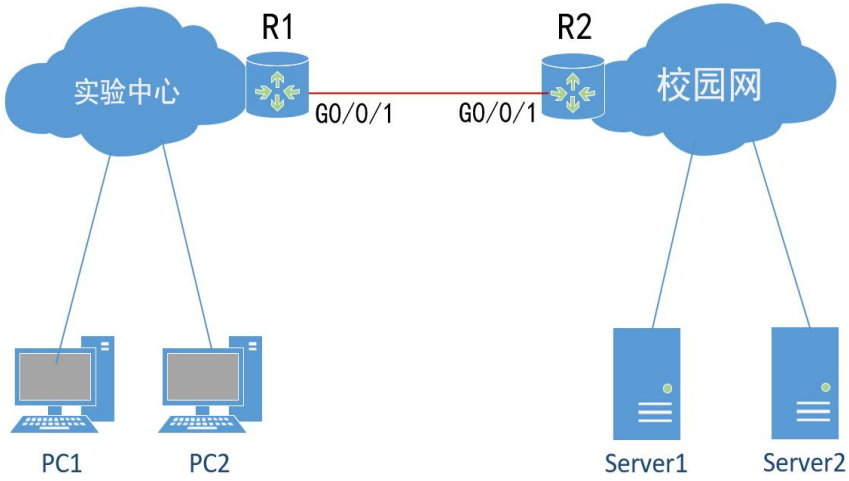
- （3）对于校园网中路由设备，当它们收到目的IP地址是172.16.1.0/30的报文，该如何转发？



案例2：实验中心局域网接入校园网

确定接入方式—— NAT

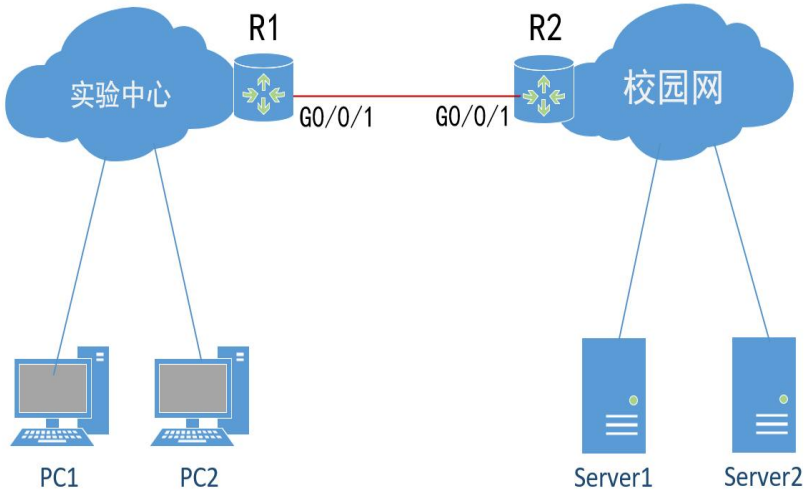
- 鉴于校园网管理机构分配给实验中心局域网的IP地址数量太少，因此决定采用NAT方式接入校园网。
- 思考：采用哪种NAT方式？
  - 一对一（静态NAT）
  - 多对多（动态NAT）
  - 多对一（NAPT，端口多路复用）



案例2：实验中心局域网接入校园网

配置过程讨论（2）

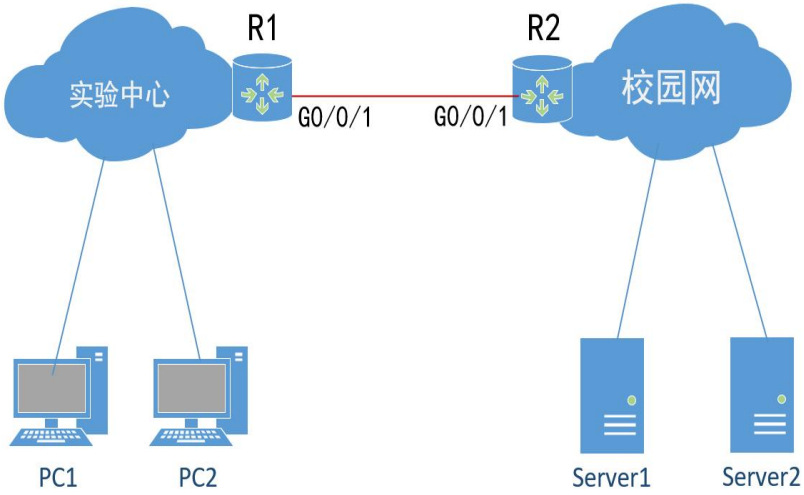
- 校园网分配的IP地址块172.16.1.0/30中，包含几个地址？实验中心管理员能够用来进行网络接口配置的IP地址是什么？
- 根据NAT的功能，可知当局域网内部的主机访问校园网的报文从局域网发出时，其源IP地址应该变为校园网所分配的地址，那么，要把该地址配置在局域网的什么位置？
- 配置NAT的具体命令，可参见相应设备的产品文档。



案例2：实验中心局域网接入校园网

配置过程讨论（3）

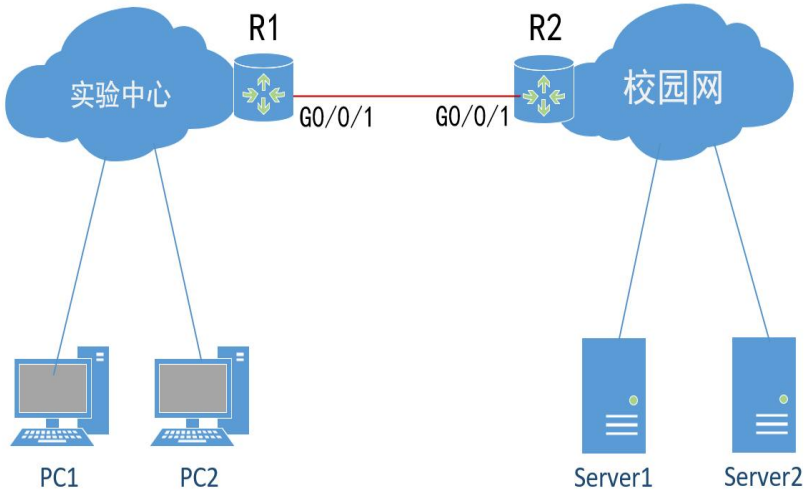
- 校园网给出的默认网关是172.16.1.1。此处的“默认网关”如何理解？
- 该默认网关应该配置在哪里？
- R2(G0/0/1)



案例2：实验中心局域网接入校园网

配置过程讨论（4）

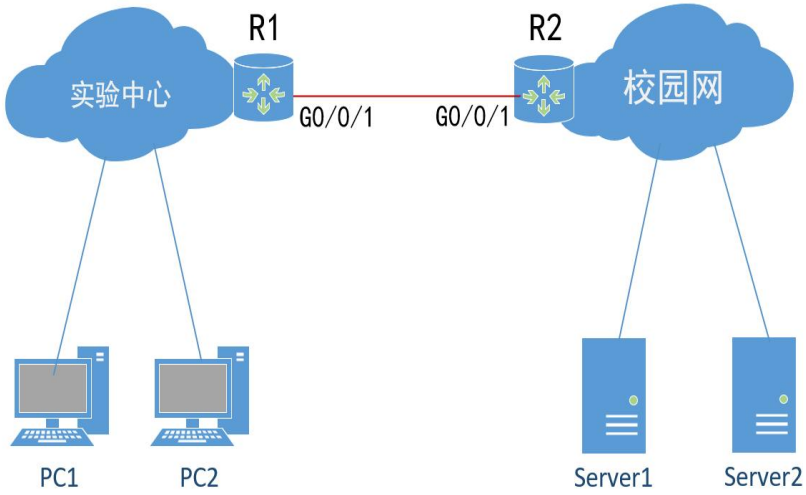
- 校园网中的路由设备是否需要知道到达实验教学中心局域网内部IP地址网段（即192.A.B.*）的路由信息？也就是说，是否需要通过配置，使得校园网中的路由设备，其路由表中有目的网络是192.A.B.*的路由记录信息？
- 当PC1访问Server1的报文到达Server1后，如何返回？即校园网中的路由设备如何转发返回报文？



案例2：实验中心局域网接入校园网

配置过程讨论（5）

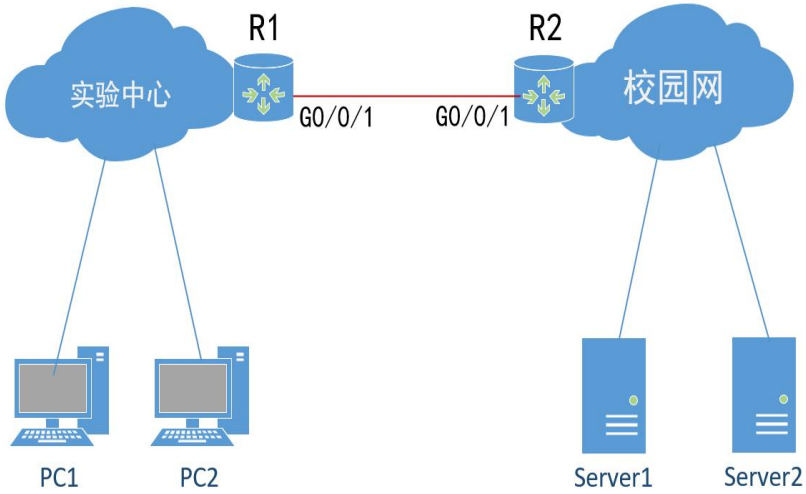
- 在配置实验中心局域网内部的路由设备时，如何配置目的网络是实验中心局域网内部子网（例如某个实验室的网络）的路由？
- 又如何配置目的网络是“校园网”的路由？注意，此处的“校园网”只是一个笼统的叫法，校园网中可能包含多个具体的网络。



案例2：实验中心局域网接入校园网

配置过程讨论（6）

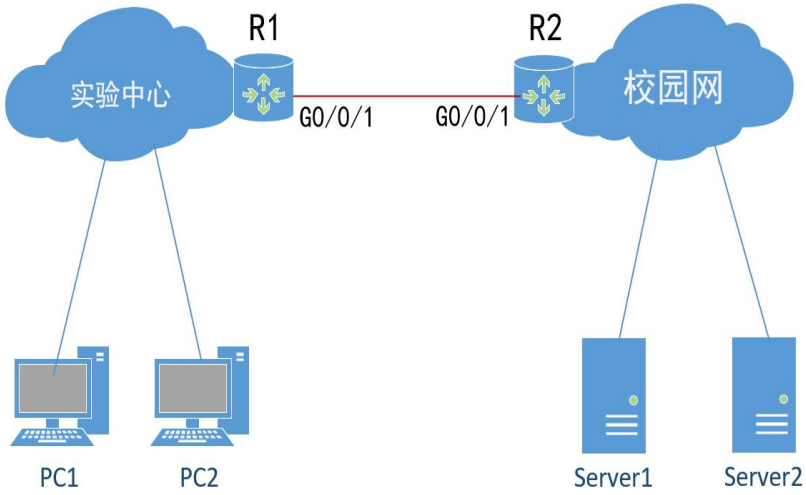
- 实验中心的局域网，是否可以使用静态路由？谈谈你的配置思路。
- 如果使用OSPF动态路由协议呢？谈谈你的配置思路。



案例2：实验中心局域网接入校园网

配置过程讨论（7）

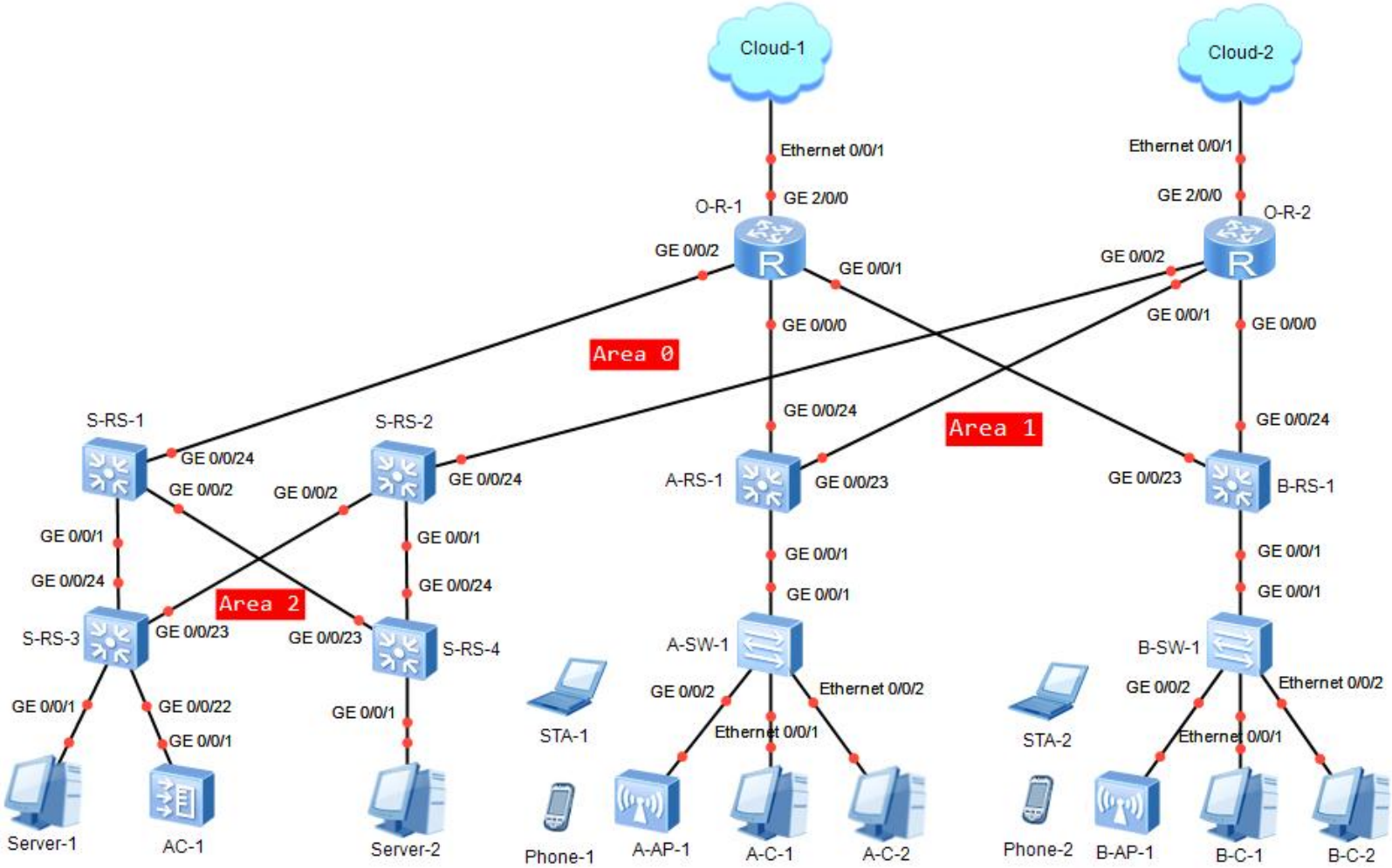
- 如果在右图中的路由器R1上配置OSPF，那么在宣告R1的直连网段时，是否宣告其G0/0/1接口所在的网段？
- 同样，如果在路由器R2上配置OSPF，那么在宣告R2的直连网段时，是否宣告其G0/0/1接口所在的网段？



返回

应用案例

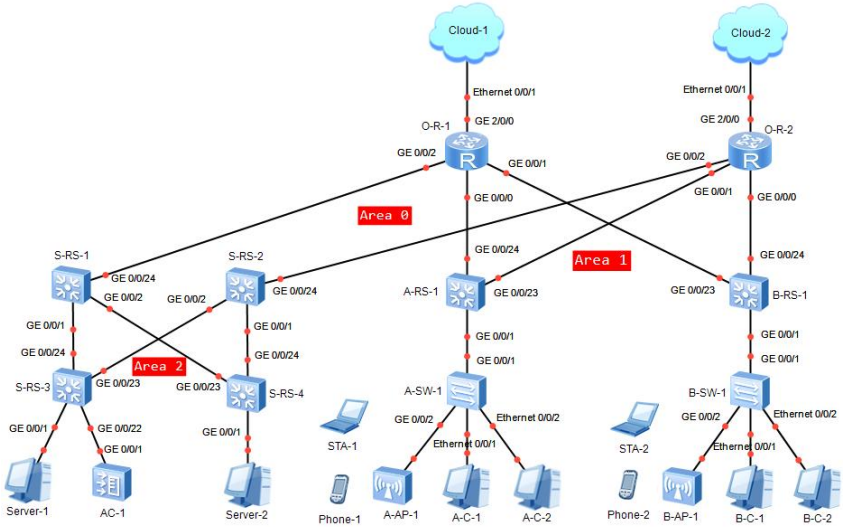
- 案例3：园区网双链路NAT接入互联网


Cloud-1
Cloud-2
Ethernet 0/0/1
GE 2/0/0
O-R-1
GE 0/0/2
GE 0/0/1
GE 0/0/0
Area 0
Area 1
Area 2
S-RS-1
S-RS-2
GE 0/0/24
GE 0/0/2
GE 0/0/1
GE 0/0/23
A-RS-1
B-RS-1
S-RS-3
S-RS-4
A-SW-1
B-SW-1
GE 0/0/22
Ethernet 0/0/2
Server-1
AC-1
Server-2
STA-1
STA-2
Phone-1
Phone-2
A-AP-1
A-C-1
A-C-2
B-AP-1
B-C-1
B-C-2

案例3：园区网双链路NAT接入互联网

配置过程讨论（1）

- 假设在eNSP中仿真实现该案例，根据上网环境的不同，园区网边界路由器的出口地址和默认网关地址（即下一跳地址）如何确定？
- 1. 家里面，部署了无线路由器；
- 2. 寝室里，有线网络接口；
- 3. 实验室里



案例3：园区网双链路NAT接入互联网

配置过程讨论（2）

- 教材P73 【提醒】

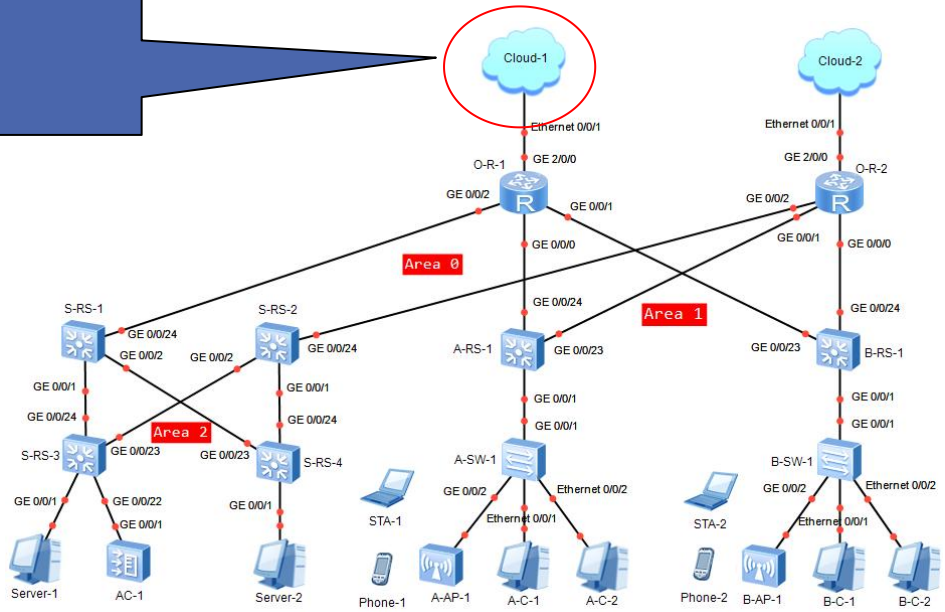
1. 本任务中，必须保证读者的计算机（即本地实体主机）能够正常访问互联网；

2. 通过eNSP的云设备（Cloud）绑定本地实体主机的网卡时，要绑定有线网卡，若绑定无线网卡可能无法访问互联网。

提醒：可以用仿真网络代替互联网（见下页）

案例3：园区网双链路NAT接入互联网

用仿真网络代替互联网



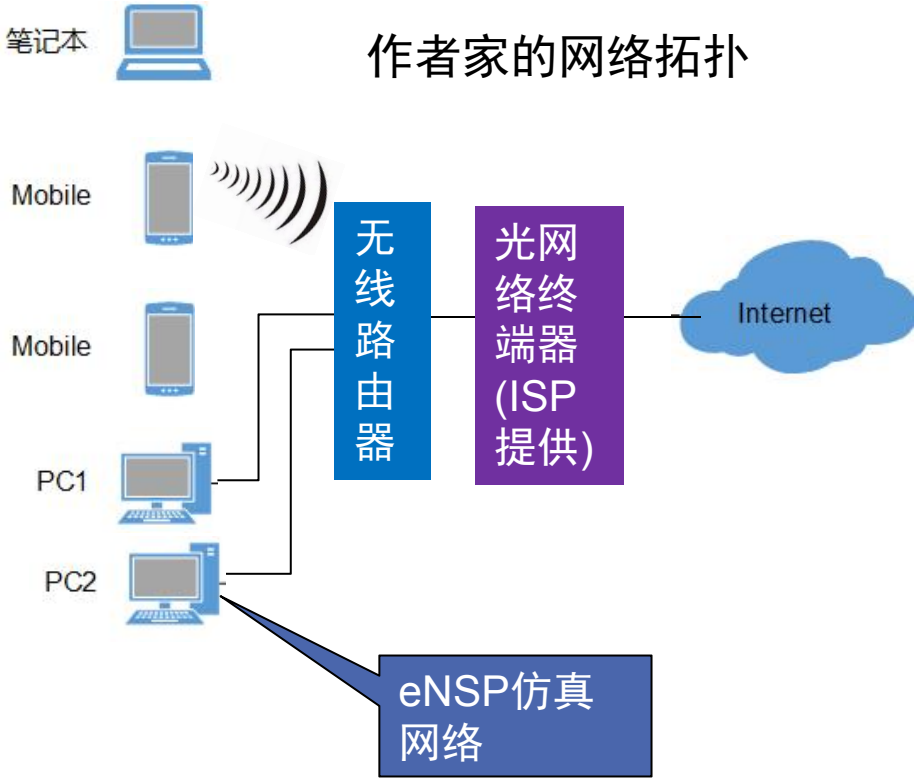
案例3：园区网双链路NAT接入互联网

配置过程讨论（2）

- 教材P74 【提醒1】

1. 此处作者的计算机首先通过网线接入一台无线路由器，然后接入互联网。192.168.31.0 /24（私有IP地址）是作者的计算机接入互联网时所使用的IP地址段，这与作者所用的无线路由器有关，无线路由器自身也有NAT功能；

2. 读者在配置A-R-1的互联网接口IP地址，要使用与本地实体主机在同一网段的IP地址，或者根据实际网络环境而定。

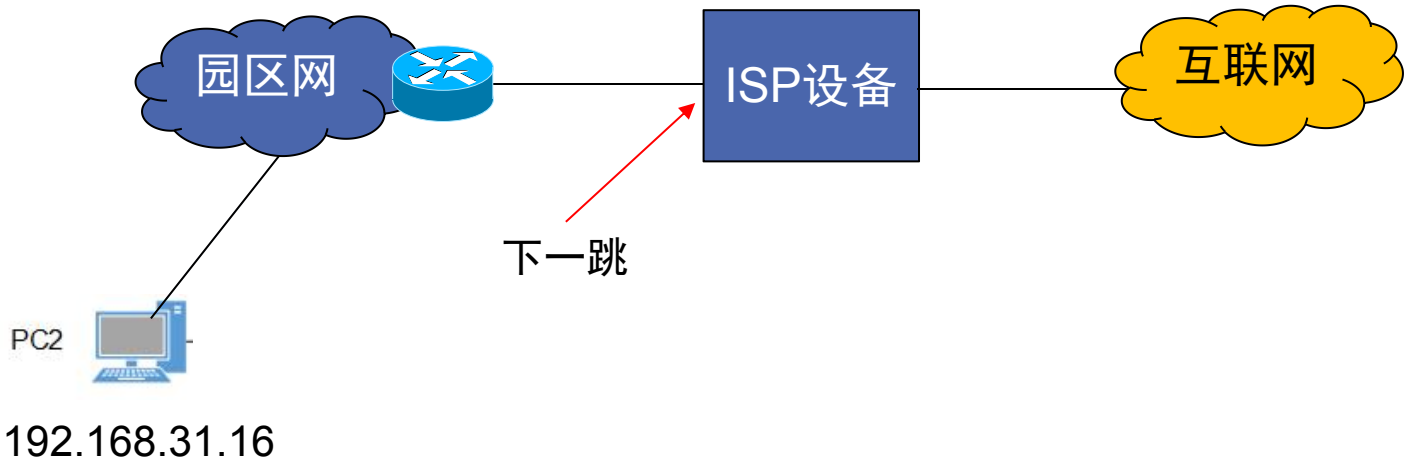



ISP提供的用户端设备
无线路由器

配置过程讨论（2）

- 教材P74 【提醒2】

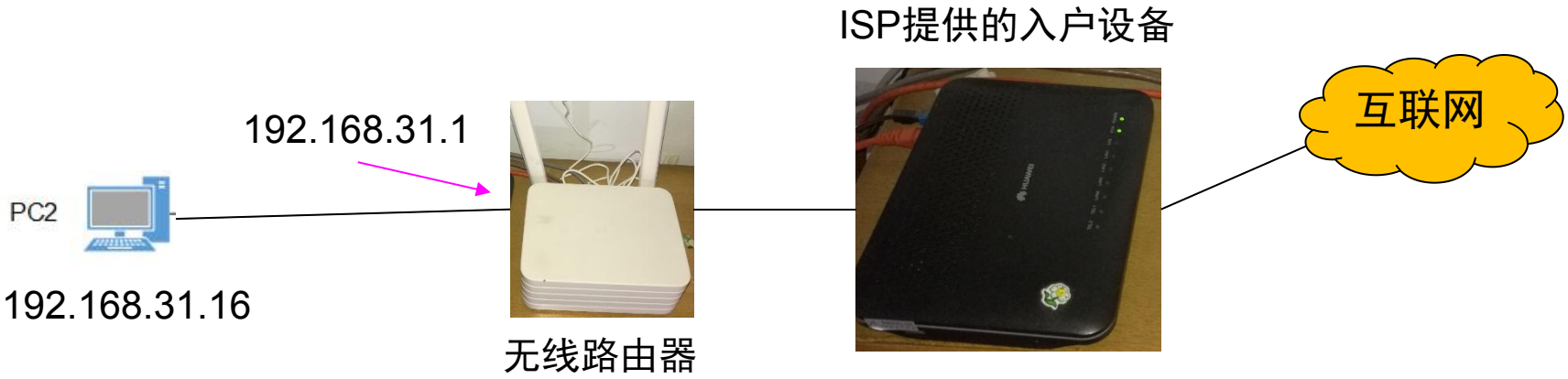
1. 在实际应用中，园区网边界路由器所配置的默认路由中，其下一跳地址通常由所接入的互联网运营商提供，该地址通常是公有IP地址；



配置过程讨论（2）

- 教材P74 【提醒2】

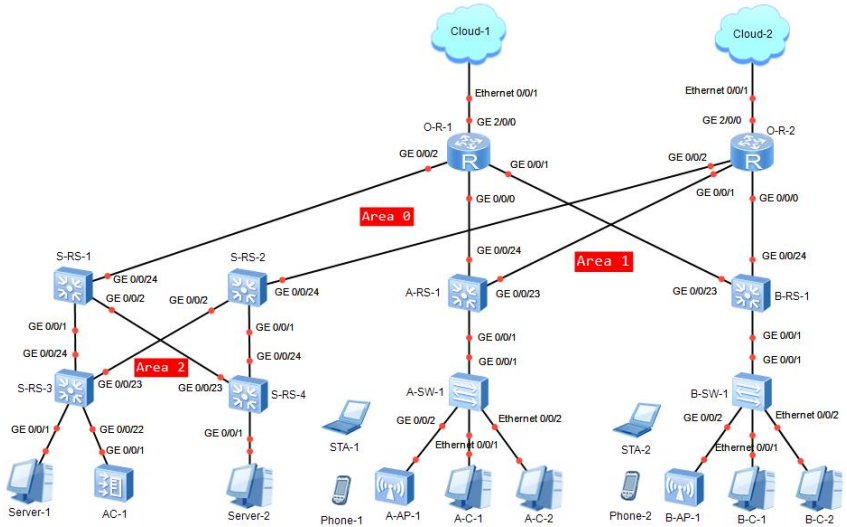
2. 此处边界路由器的默认路由中，下一跳地址是作者计算机的默认网关192.168.31.1（私有IP地址），这与作者所用的无线路由器有关。读者在配置下一跳地址时，可使用自己计算机（实体主机）的默认网关地址，或者根据实际网络环境而定。



案例3：园区网双链路NAT接入互联网

配置过程讨论（2）

- 假设在eNSP中仿真实现该案例，园区网边界路由器O-R-1和O-R-2的出接口IP地址是配置成相同网段的地址，还是不同网段的地址？

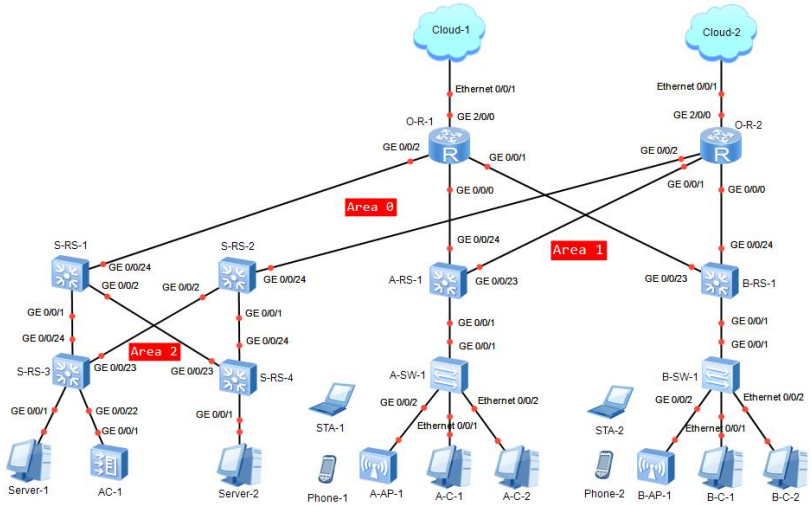


配置过程讨论（3）

- 教材P81 【提醒】

1. 在实际应用中，园区网的两个出口链路通常分别接入不同的电信运营商，因此两台边界路由器的互联网接口IP地址应该属于不同的网段（由所接入的电信运营商提供）；

2. 由于作者计算机所在网络环境的限制，此处将A-R-1和B-R-1的互联网接口IP地址设置为同一网段，即192.168.31.0/24，仅用来验证NAT接入互联网以及出口链路的冗余效果。读者在具体实践时，要根据自己所处的网络环境来确定两个边界路由器互联网接口的IP地址。

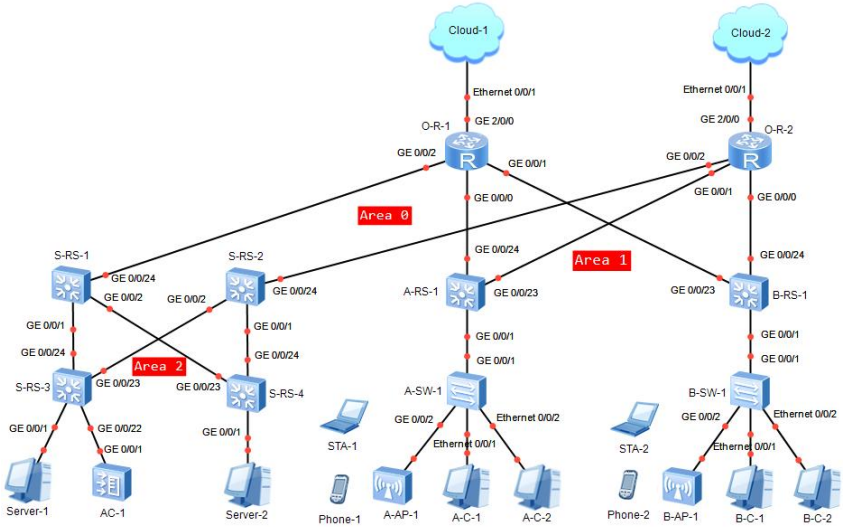


案例3：园区网双链路NAT接入互联网

配置过程讨论（3）

- 园区网能否全网使用静态路由？

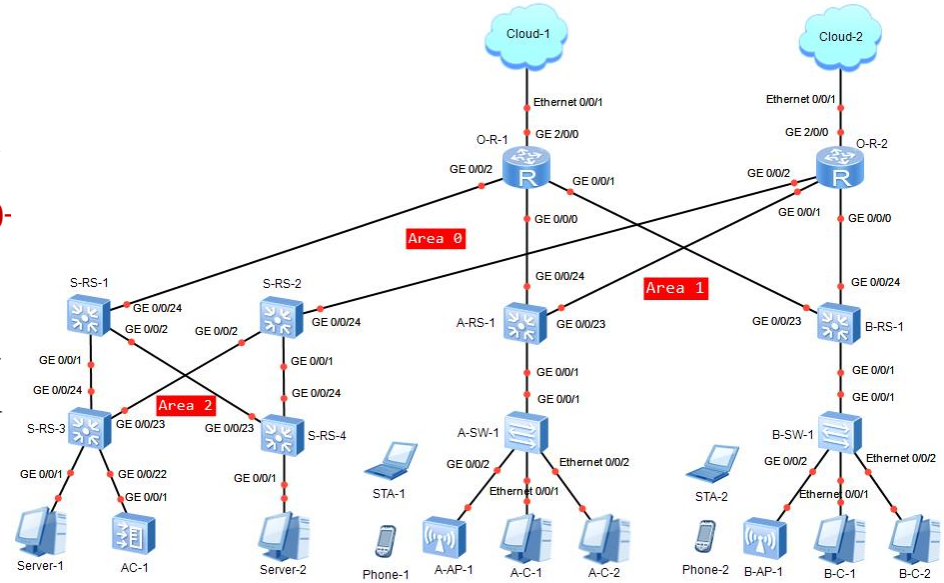
提示：如何表示互联网上的目的地？



案例3：园区网双链路NAT接入互联网

配置过程讨论（4）

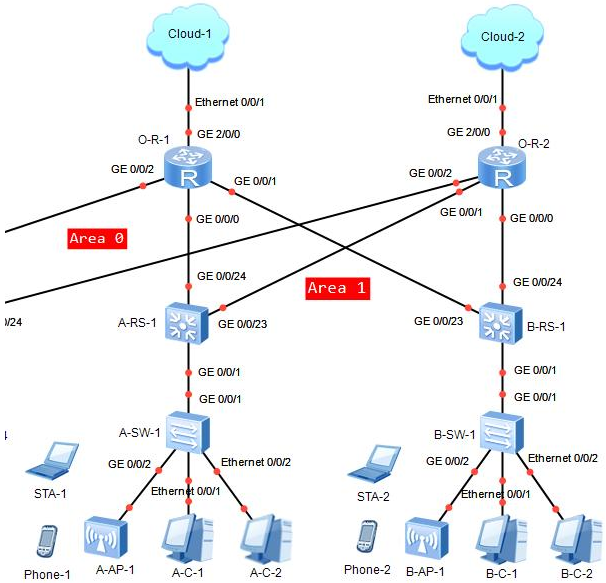
- 假设园区网使用了OSPF
- 从园区网内部主机发出的、访问互联网的报文，如何被转发到边界路由器O-R-1或O-R-2，进而被发送出去？举例说明。
  - 思考：仅仅依靠OSPF可以吗？如果在园区网内部的路由设备上配置缺省路由又会存在什么问题？



案例3：园区网双链路NAT接入互联网

配置过程讨论（5）

- default-route-advertise命令用来将缺省路由通告到普通OSPF区域中，这样OSPF区域中的其他路由器也会学习到该默认路由，并自动修改下一跳地址。例如，如果已经在O-R-1上配置了一条默认路由，则通过执行default-route-advertise命令，可以让该默认路由信息传递到A-RS-1和B-RS-1，并且下一跳地址变为O-R-1。示例：




```
[A-R-1]ospf 1
//在ospf 1中引入默认路由，并发布到整个OSPF区域，注意添加always参数。
[A-R-1-ospf-1]default-route-advertise always
```

案例3：园区网双链路NAT接入互联网

配置过程讨论（6）

- 下图显示了此时三层交换机A-RS-1的路由表，其第1条记录中的O_ASE表示本记录是通过OSPF引入的外部路由协议的路由信息，注意其下一跳地址为10.0.0.1（即O-R-1的GE0/0/1接口），表示其他所有报文都转发至10.0.0.1，并且该路由信息是动态的；

A-RS-1

```
<A-RS-1>display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 9        Routes : 9

Destination/Mask    Proto   Pre  Cost      Flags NextHop

        0.0.0.0/0   O_ASE   150  1           D   10.0.0.1
       10.0.0.0/30  Direct  0    0           D   10.0.0.2
       10.0.0.2/32  Direct  0    0           D   127.0.0.1
      127.0.0.0/8   Direct  0    0           D   127.0.0.1
      127.0.0.1/32  Direct  0    0           D   127.0.0.1
   192.168.64.0/24  Direct  0    0           D   192.168.64.254
 192.168.64.254/32  Direct  0    0           D   127.0.0.1
   192.168.65.0/24  Direct  0    0           D   192.168.65.254
```

Thanks.