G-LAB

G-CNA v2.0课程

讲师：沈老师

广域网技术

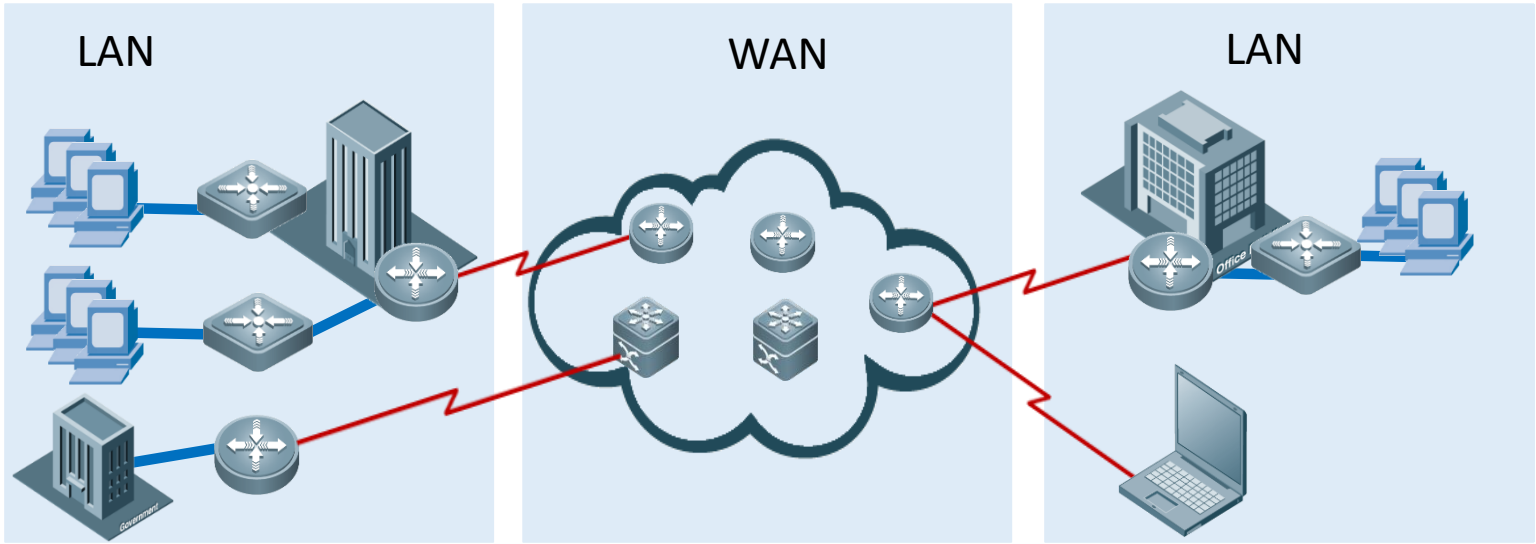
1. 什么是广域网？广域网的物理介质类型?
2. 局域网和广域网的比较?
3. 广域网典型的封装协议HDLC-PPP，比较?
4. PPPOE

前言

- 广域网是连接不同地区局域网或城域网计算机通信的远程网。
- 通常跨接很大的物理范围，所覆盖的范围从几十公里到几千公里，它能连接多个地区、城市和国家，或横跨几个洲并能提供远距离通信，形成国际性的远程网络。
- 随着经济全球化与数字化变革加速，企业规模不断扩大，越来越多的分支机构出现在不同的地域。每个分支的网络被认为一个LAN（Local Area Network，局域网），总部和各分支机构之间通信需要跨越地理位置。因此，企业需要通过WAN（Wide Area Network，广域网）将这些分散在不同地理位置的分支机构连接起来，以便更好地开展业务。
- 广域网技术的发展，伴随着带宽不断的升级：早期出现的X.25只能提供64 kbit/s的带宽，其后DDN（Digital Data Network，数字数据网）和FR（Frame Relay，帧中继）提供的带宽提高到2 Mbit/s，SDH（Synchronous Digital Hierachy，同步数字结构）和ATM（Asynchronous Transfer Mode，异步传输模式）进一步把带宽提升到10 Gbit/s，最后发展到当前以IP为基础的10 Gbit/s甚至更高带宽的广域网络。

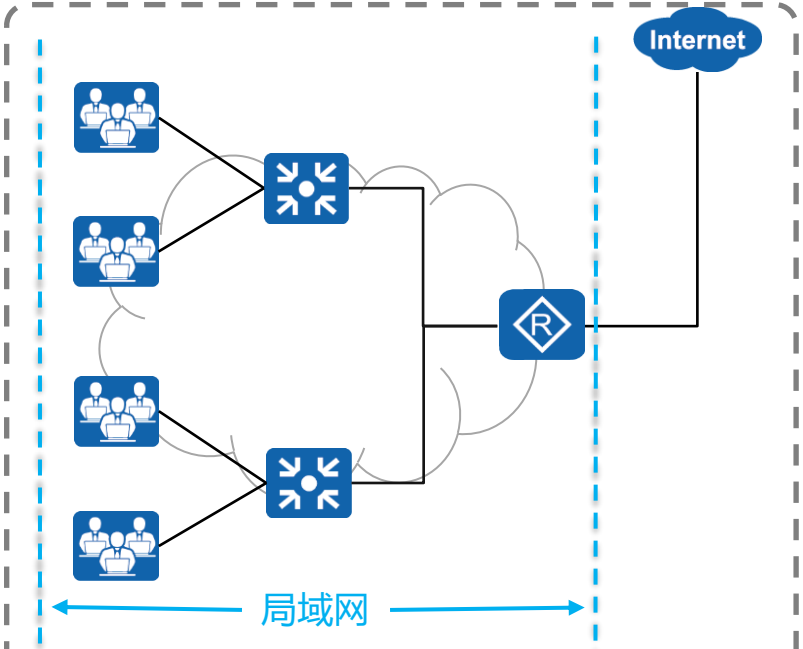
为什么需要WAN？

- 分支机构与总部机构需要跨越运营商实现数据互通
- 出差在外的员工需要通过互联网远程拨入公司，访问公司内网的数据资源
- 广域网并不等同于互联网



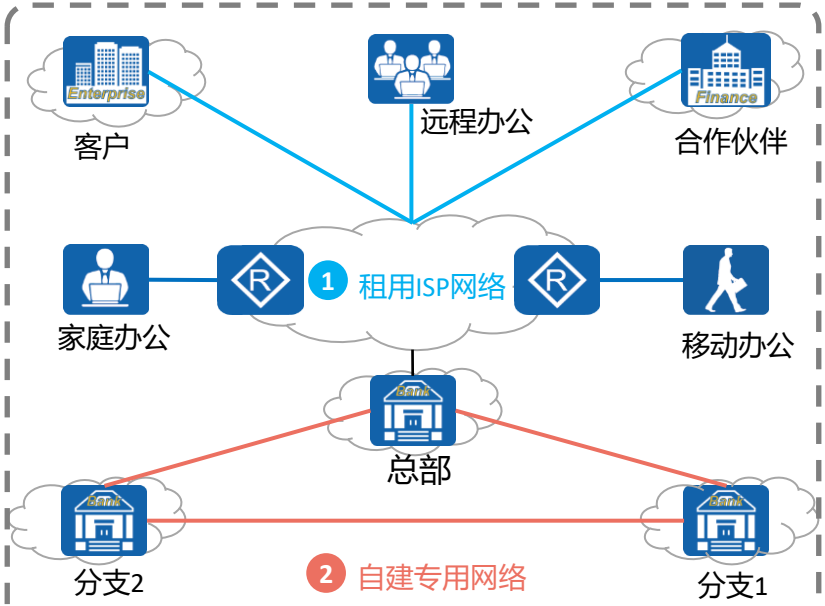
广域网与局域网区别

局域网



- 局域网是一种覆盖地理区域比较小的计算机网络。

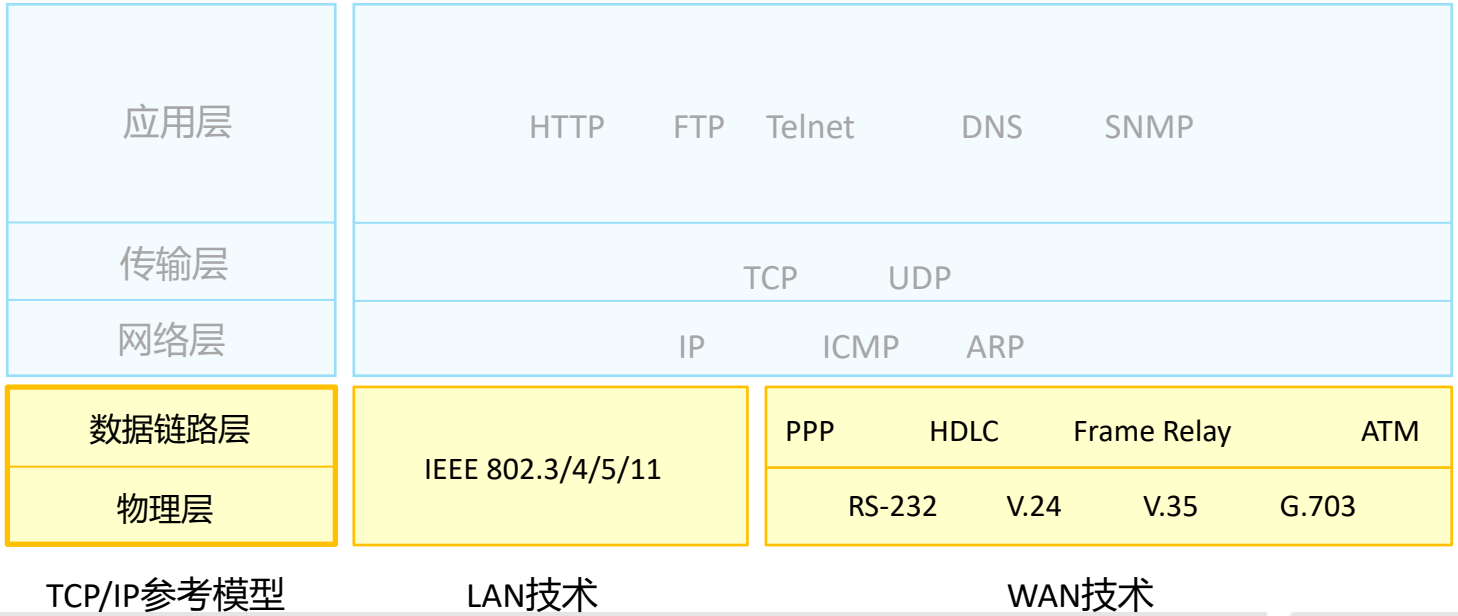
广域网



- 广域网是一种通过租用ISP网络或者自建专用网络来构建的覆盖地理区域比较广的计算机网络。

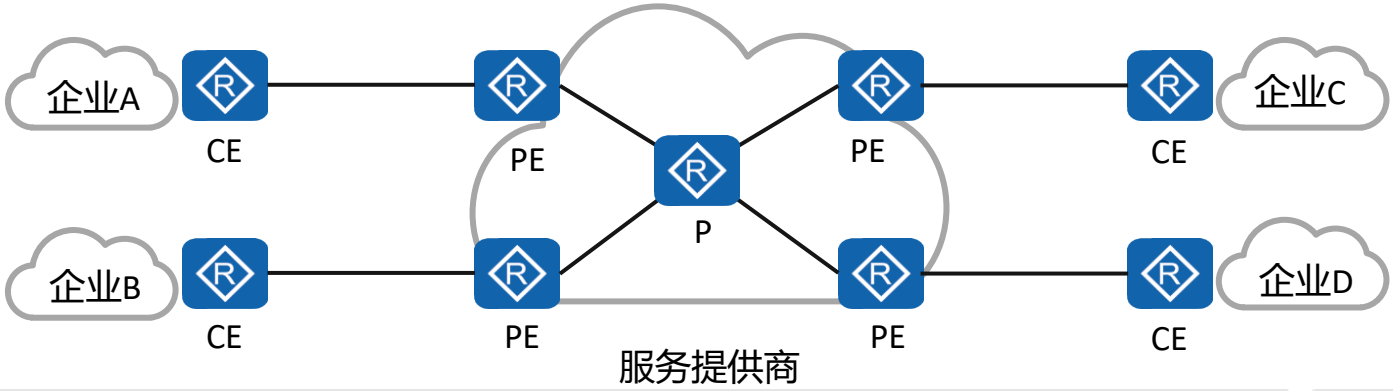
早期广域网技术介绍

- 早期广域网与局域网的区别在于数据链路层和物理层的差异性，在TCP/IP参考模型中，其他各层无差异。



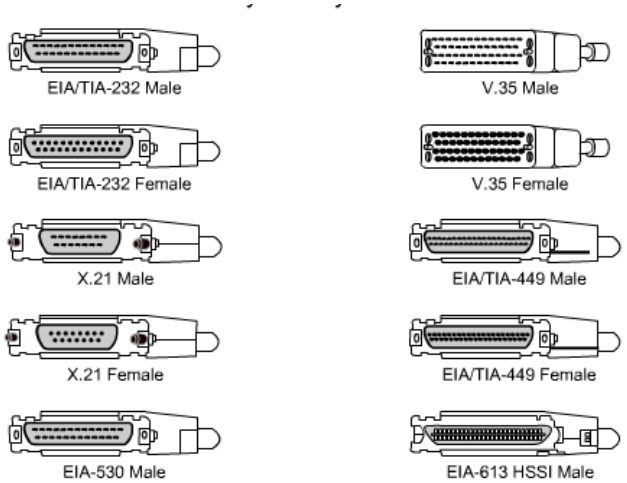
广域网络设备角色介绍

- 广域网络设备基本角色有三种，CE（Customer Edge，用户边缘设备）、PE（Provider Edge，服务提供商边缘设备）和P（Provider，服务提供商设备）。具体定义是：
  - CE：用户端连接服务提供商的边缘设备。CE连接一个或多个PE，实现用户接入。
  - PE：服务提供商连接CE的边缘设备。PE同时连接CE和P设备，是重要的网络节点。
  - P：服务提供商不连接任何CE的设备。



WAN物理层概念

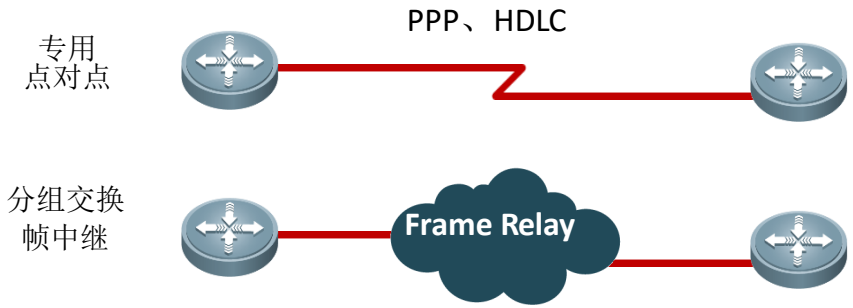
- WAN 物理层协议描述连接WAN 服务所需的电气、机械、操作和功能特性（类似有线局域网的10M、100M、1000M网线）
- WAN 物理层还描述了 DTE 和 DCE 之间的接口
  - DTE：数据终端设备，Data Terminal Equipment
  - DCE：数据通信设备，Data Communicate Equipment



常见的WAN接口连接模块

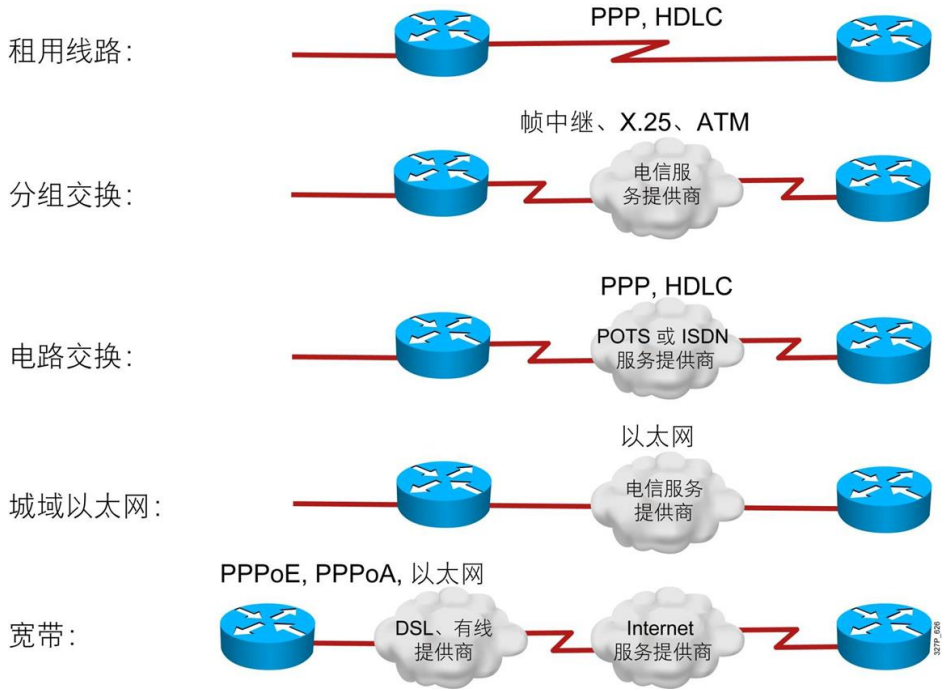
WAN数据链路层概念

- 数据链路层（OSI 第 2 层）协议定义如何封装传向远程位置的数据以及最终数据帧的传输机制（类似以太网中的MAC地址）
  - PPP、HDLC、Frame Relay
  - 帧中继网络现在基本已经淘汰



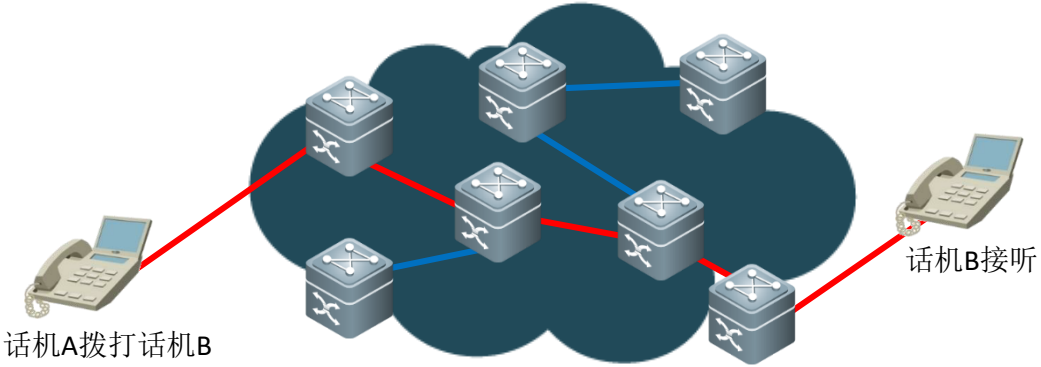
广域网链路类型分类

- 电路交换
- 分组交换
- VPN
- 专线



电路交换

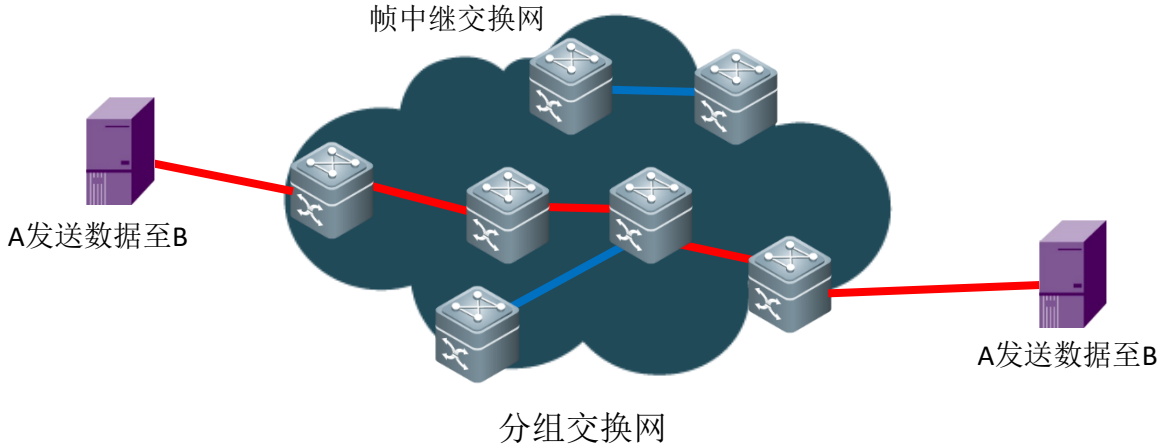
- 在用户通信之前在节点和终端之间建立专用电路（或信道）的网络，常见的比如ISDN，PSTN等
- 传输介质主要是电话线，也可以是光纤
- 由于用户独占分配的固定带宽，因此使用交换电路传输数据的成本通常很高



电路交换

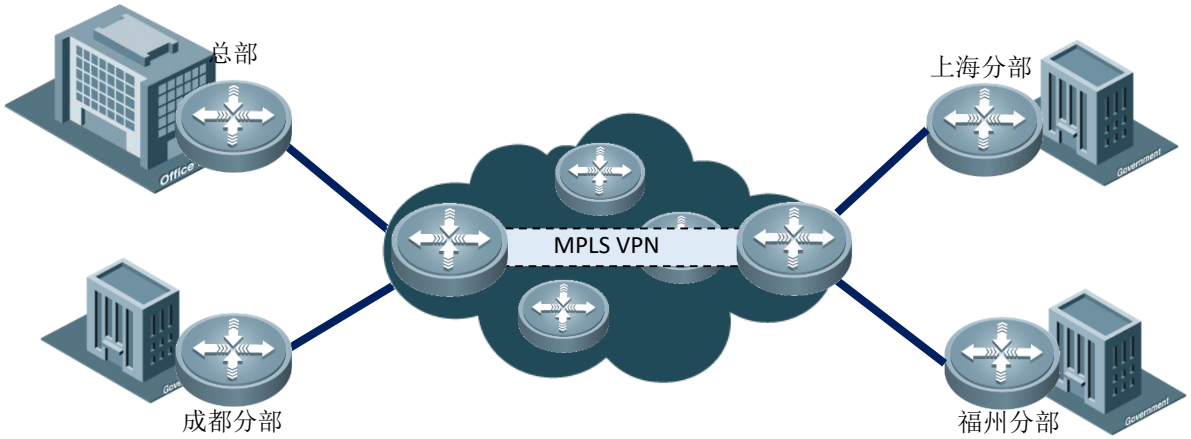
分组交换（包交换）

- 分组交换将流量数据分割成数据包，在共享网络上路由，类似于寄信
- 分为PVC(永久虚电路）和SVC(交换虚电路）：其中PVC为永久建立的虚链路；SVC为按需建立的虚链路
- 常见的分组交换技术包含X.25、帧中继以及ATM



VPN

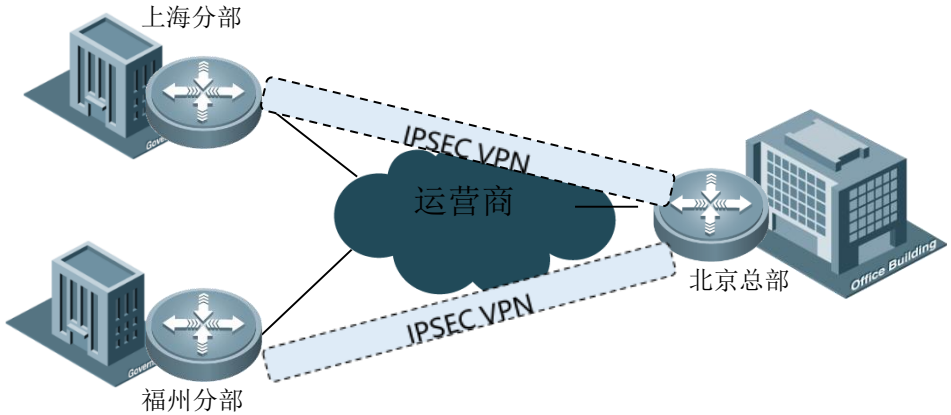
- 运营商管理型VPN：MPLS_VPN
- 由运营商承建并维护



运营商管理型VPN

VPN

- 企业管理型VPN：IPSEC VPN、GRE VPN、L2TP VPN
- 利用运营商网络，由企业内部承建并维护



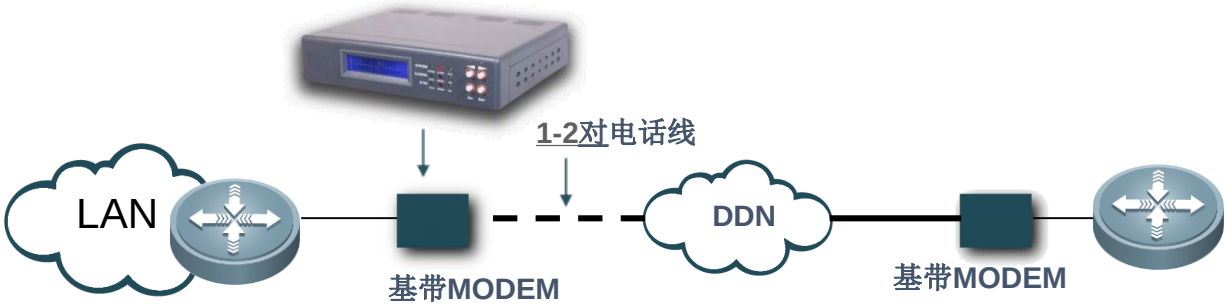
企业管理型VPN

专线

- 由运营商为企业远程节点之间的通信提供的点到点专有线路，用户独占一条速率固定的专用线路，并独享带宽
- 常见的专线技术包含DDN、SDH（如E1、T1、POS、ATM专线）、以太网专线（如MSTP、裸光纤）

专线：DDN线路

- 早期的数据通信使用的是电话交换网络，使用模拟信道传输数据。20 世纪九十年代由当时的邮电部在全国范围内建设了一张专用的数据传输网络——ChinaDDN(china Digital Data Network，中国公用数字数据网)
- 从运营商的DDN业务网中为客户提供的数字信道连接，带宽一般为n*64Kpbs，n 为1-32（即64Kpbs—2.048Mbps）

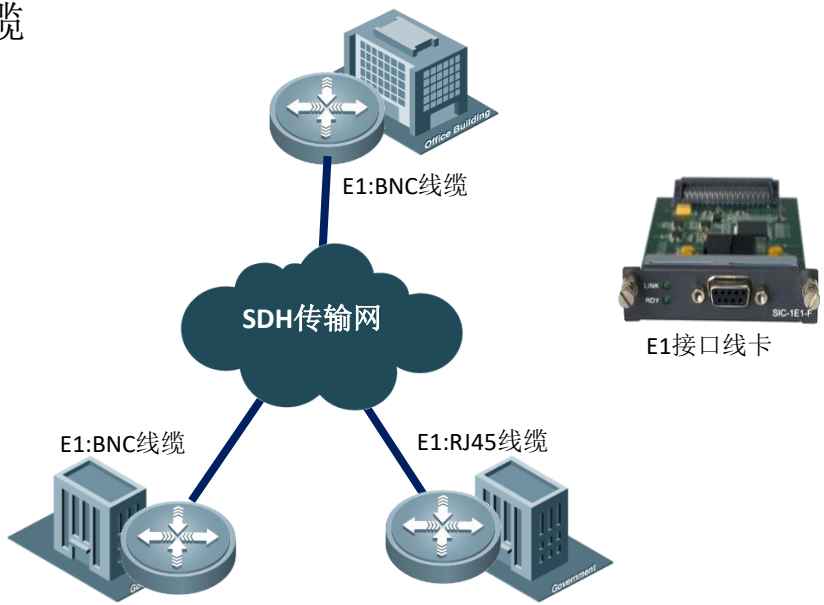


专线：SDH专线

- SDH（Synchronous Digital Hierarchy，同步数字体系）是一种传输技术，将同步复接、线路传输及交换功能融为一体. 速率标准从64K 到10G。
- 常见的SDH 专线包括E1（2.048M）、E3（34.368M）、POS(155M、622M 、2.5G、10G)、CPOS等

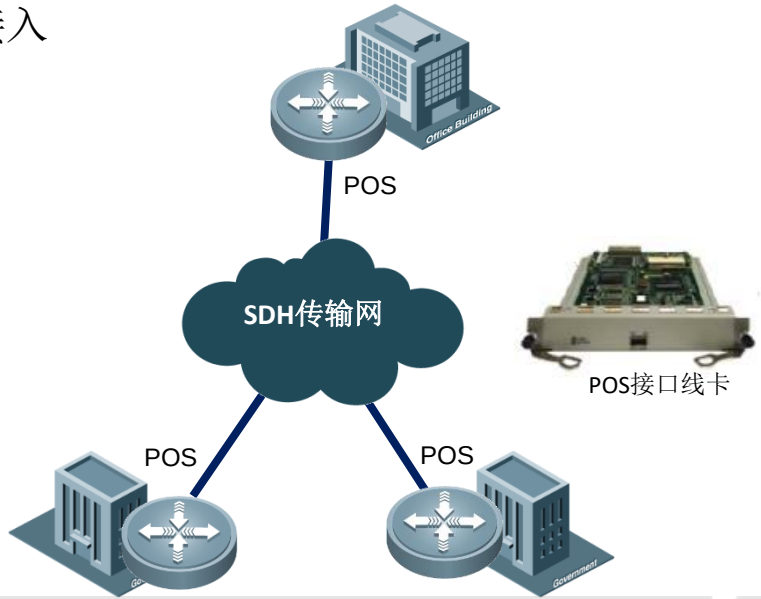
专线：SDH（E1专线）

- E1 是从运营商的SDH/PDH传输网中为客户提供的数字信道连接，速率为2.048Mbps
- 在欧洲和中国等大部分国家使用，主要用于金融、政府行业的分支接入
- 常见接入线缆为V.35、RJ48以及BNC线缆



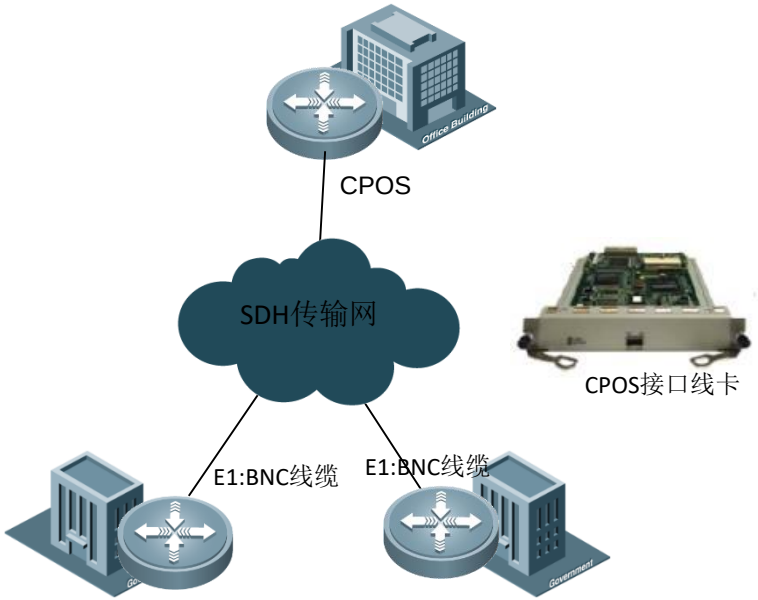
专线：SDH-POS专线

- 从运营商的SDH/PDH 传输网中为客户提供的数字信道连接，标准速率为155M（STM-1，OC3）、622M（STM-4，OC12）、2.5G（STM-16，OC48）、10G（STM-64，OC192）
- 主要用于金融、政府行业汇聚端接入
- 常见接入线缆为光纤



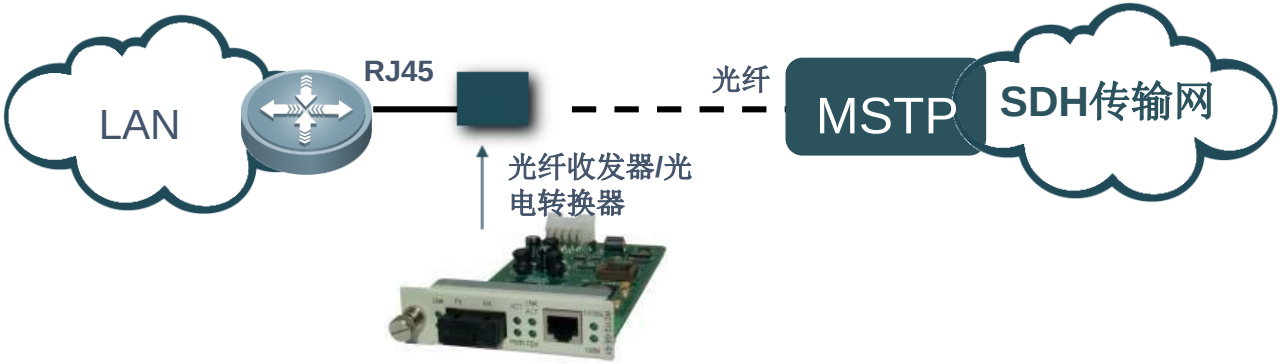
专线：SDH-CPOS专线

- CPOS 接口可以理解为一个多通道的 E1接口
- 可最大支持 63个 E1 线路，或者再细分成 N×64K 时隙的CE1链路
- 主要用于金融、政府行业汇聚端接入
- 常见接入线缆为光纤



专线：SDH-MSTP专线

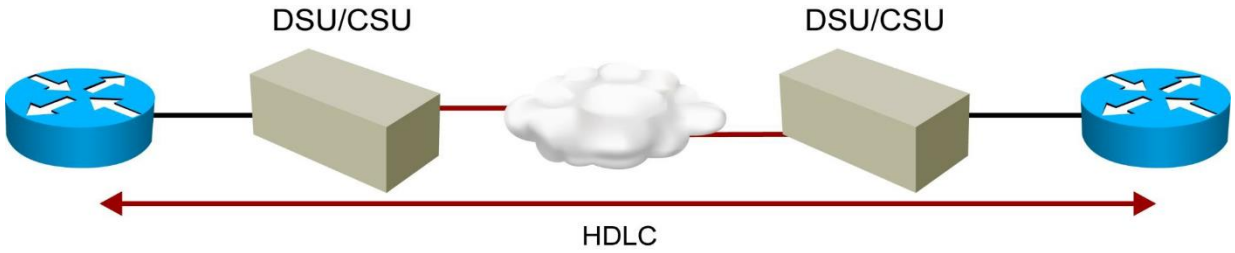
- MSTP从运营商的SDH传输网中为客户提供的数字信道连接，通过SDH传输网边缘的MSTP传输设备连接用户，用户的边界设备只要提供以太网的光口或者电。
- 主要用于金融、政府以及企业端接入
- 常见接入线缆为网线和光纤



HDLC

- HDLC:是在同步数据链路控制封装协议发展而来的数据链路层协议。
- HDLC是CISCO串行线路的缺省封装协议，只允许CISCO专用设备的连接，与其他的供应商的设备不兼容。
- 如果与没有运行CISOC IOS的设备连接应当使用PPP。

HDLC 和 Cisco HDLC



HDLC

标志	地址	控制	数据	FCS	标志

Cisco HDLC

标志	地址	控制	所有权	数据	FCS	标志

301P_483

FCS = 帧校验序列

PPP协议概述

- 点对点协议（Point to Point Protocol，PPP）为在点对点连接上传输多协议数据包提供了一个标准方法。
- PPP 最初设计是为两个对等节点之间的IP 流量传输提供一种封装协议。
  - 通常使用在专线的点对点线路中，不需要使用MAC地址（MAC地址是以太网的内容）
  - PPP与以太网一样工作在OSI模型的数据链路层，使用PPP协议封装数据

PPP协议层次介绍

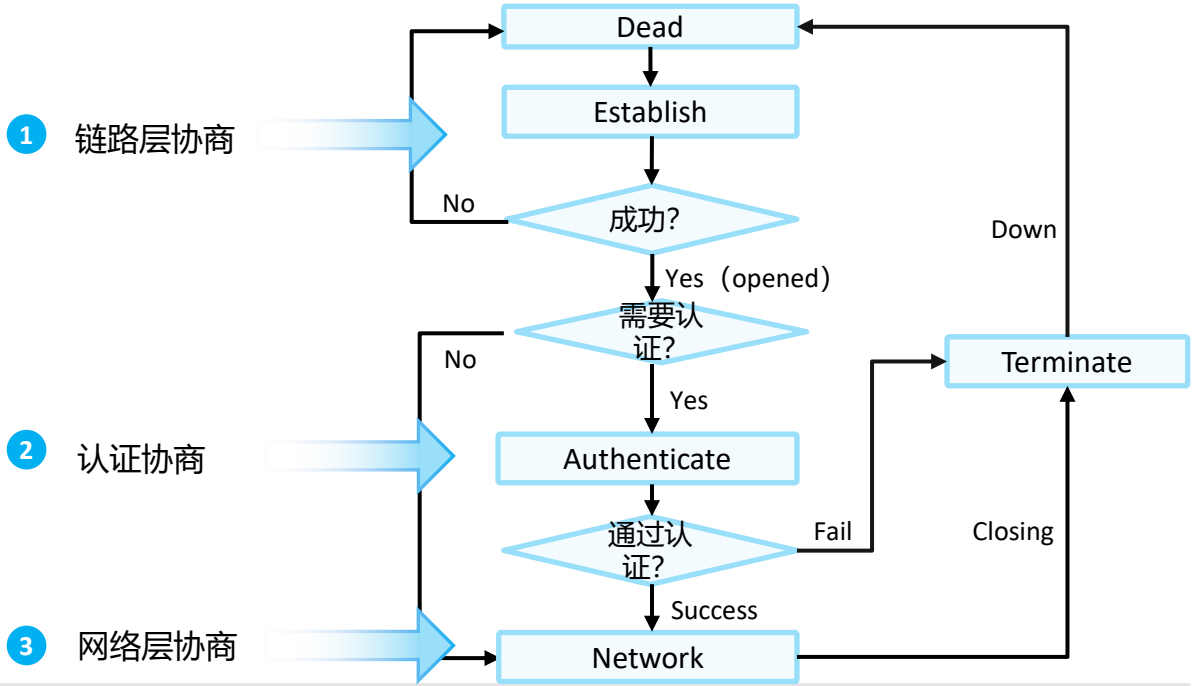
- PPP协议层介绍：
  - PPP协议包含两个子协议：链路层控制协议LCP、网络层控制协议NCP
  - PPP协议的NCP部分上跨到了OSI参考模型的第三层，因此PPP还具有部分网络层的功能

PPP协议工作原理

- PPP链路的建立有三个阶段的协商过程，链路层协商、认证协商（可选）和网络层协商。
  - 链路层协商：通过LCP报文进行链路参数协商，建立链路层连接。
  - 认证协商（可选）：通过链路建立阶段协商的认证方式进行链路认证。
  - 网络层协商：通过NCP协商来选择和配置一个网络层协议并进行网络层参数协商。

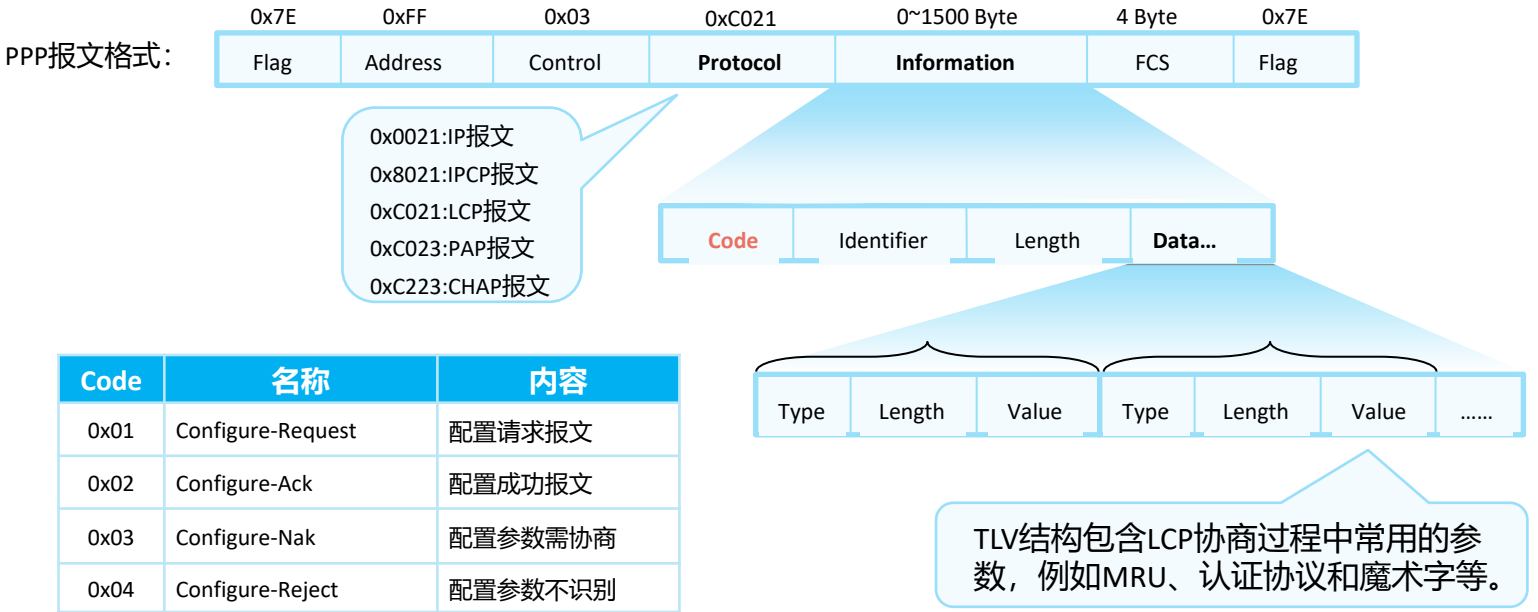
PPP链路接口状态机

- PPP协商由链路两端的接口完成。接口的状态表示了协议的协商阶段。



LCP报文格式

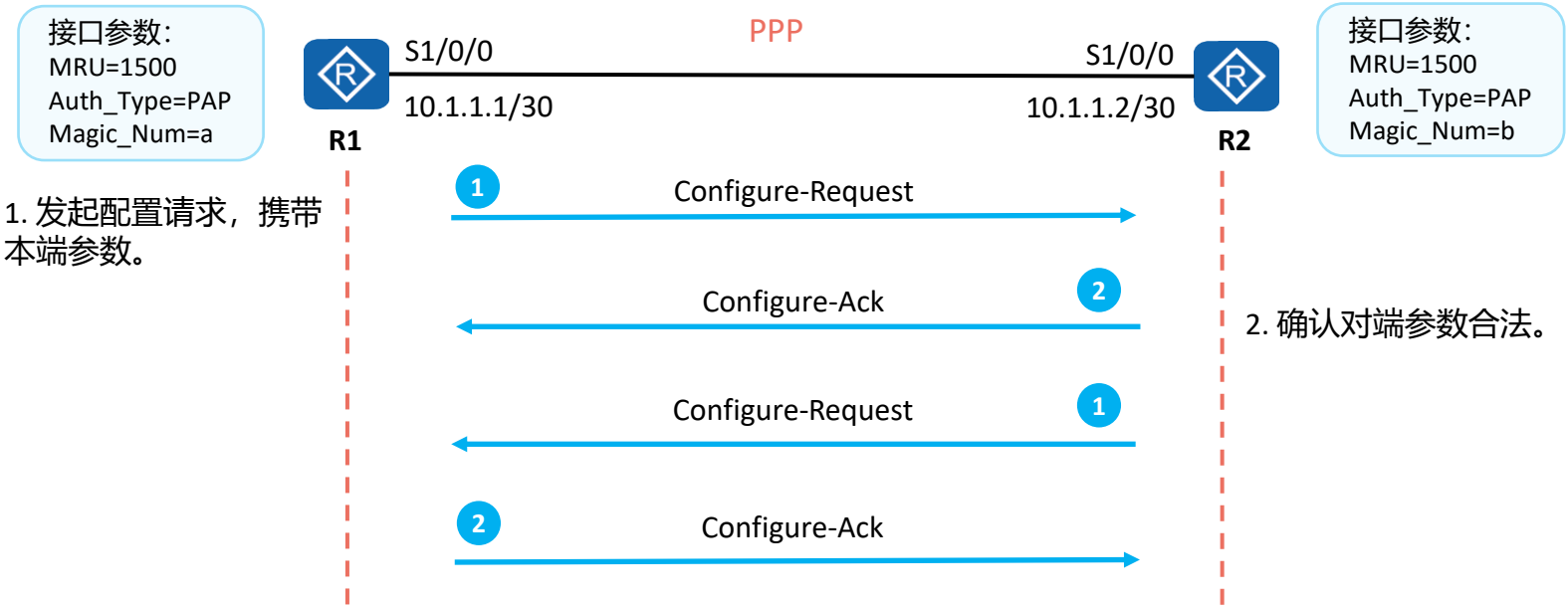
- PPP报文可由Protocol字段标识不同类型的PPP报文。例如，当Protocol字段为0xC021时，代表是LCP报文。此时又由Code字段标识不同类型LCP报文，如下表所示。



Code	名称	内容
0x01	Configure-Request	配置请求报文
0x02	Configure-Ack	配置成功报文
0x03	Configure-Nak	配置参数需协商
0x04	Configure-Reject	配置参数不识别

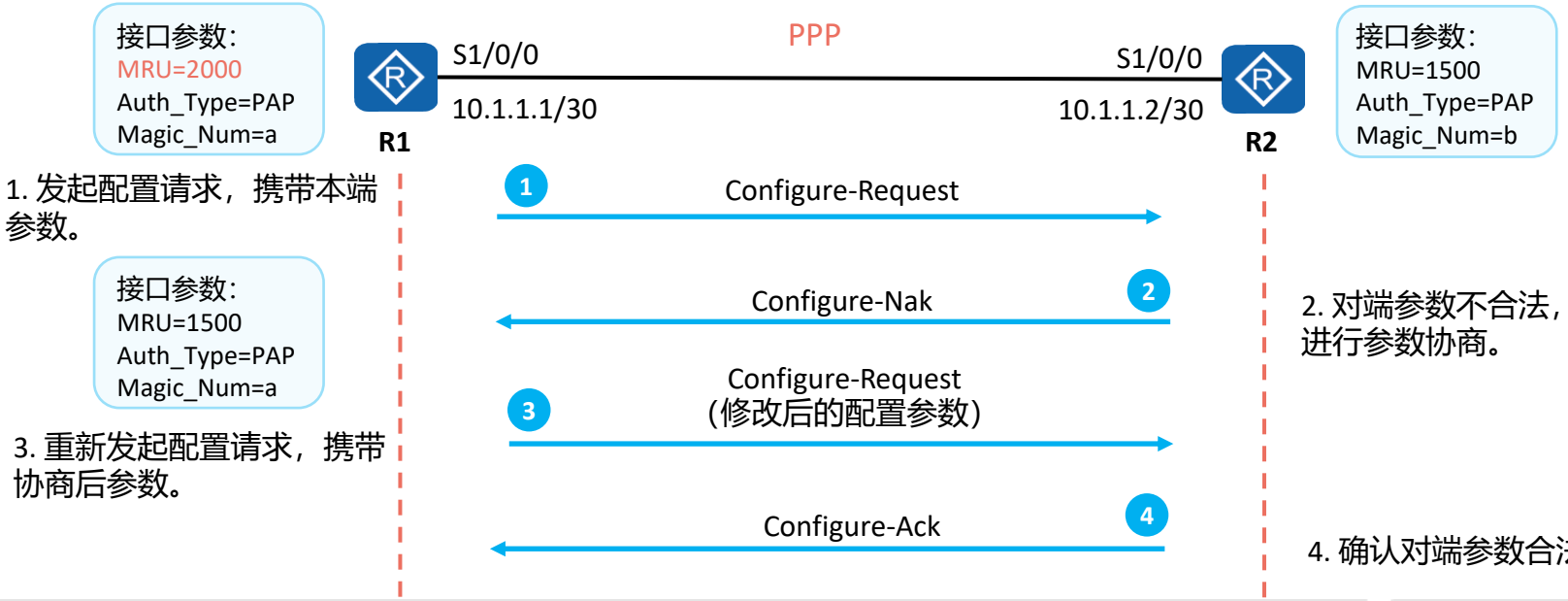
LCP协商过程 – 正常协商

- LCP协商由不同的LCP报文交互完成。协商由任意一方发送Configure-Request报文发起。如果对端接收此报文且参数匹配，则通过回复Configure-Ack响应协商成功。



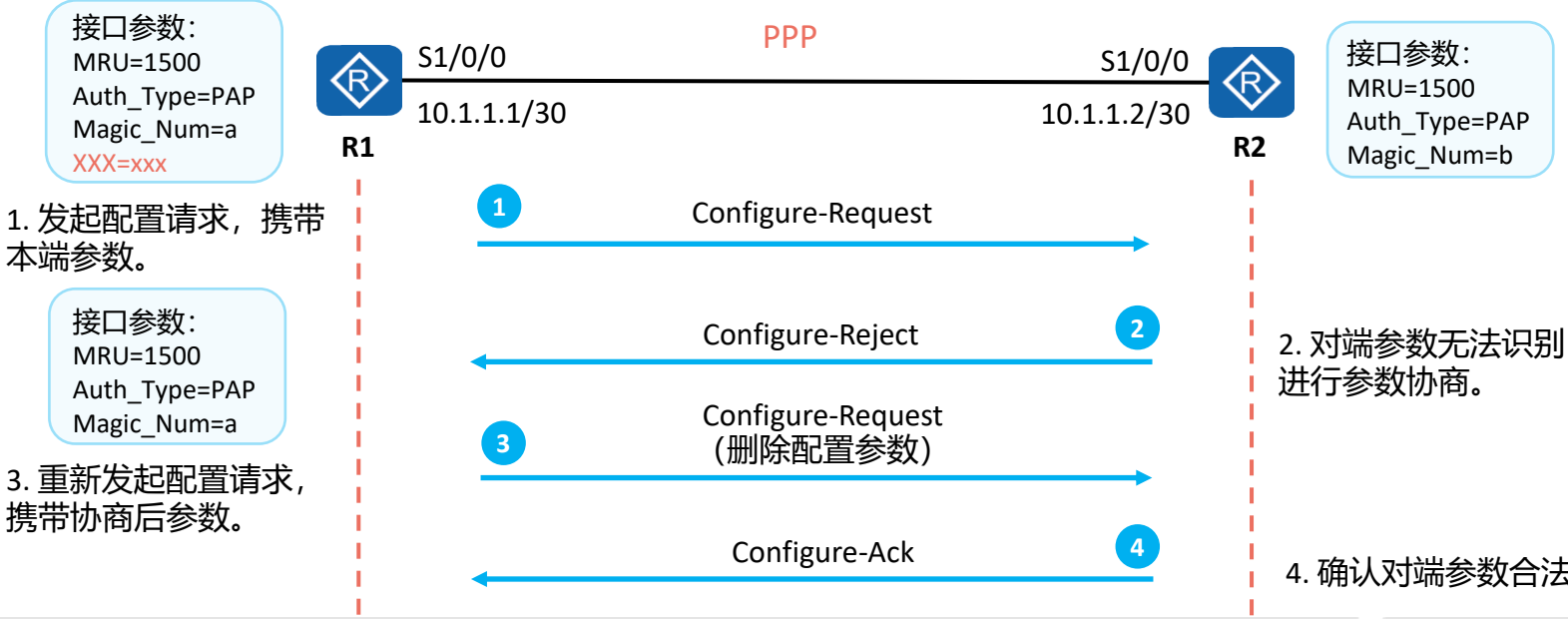
LCP协商过程 - 参数不匹配

- 在LCP报文交互中出现LCP参数不匹配时，接收方回复Configure-Nak响应告知对端修改参数然后重新协商。



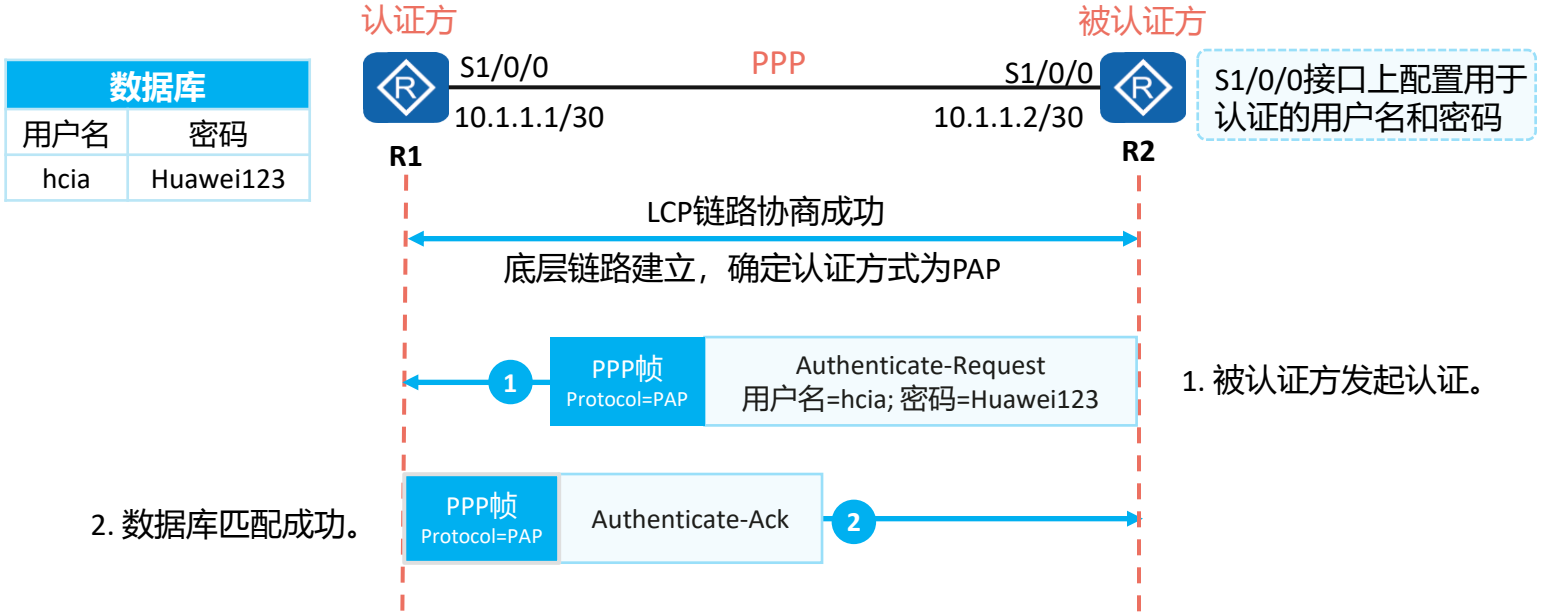
LCP协商过程 – 参数不识别

- 在LCP报文交互中出现LCP参数不识别时，接收方回复Configure-Reject响应告知对端删除不识别的参数然后重新协商。



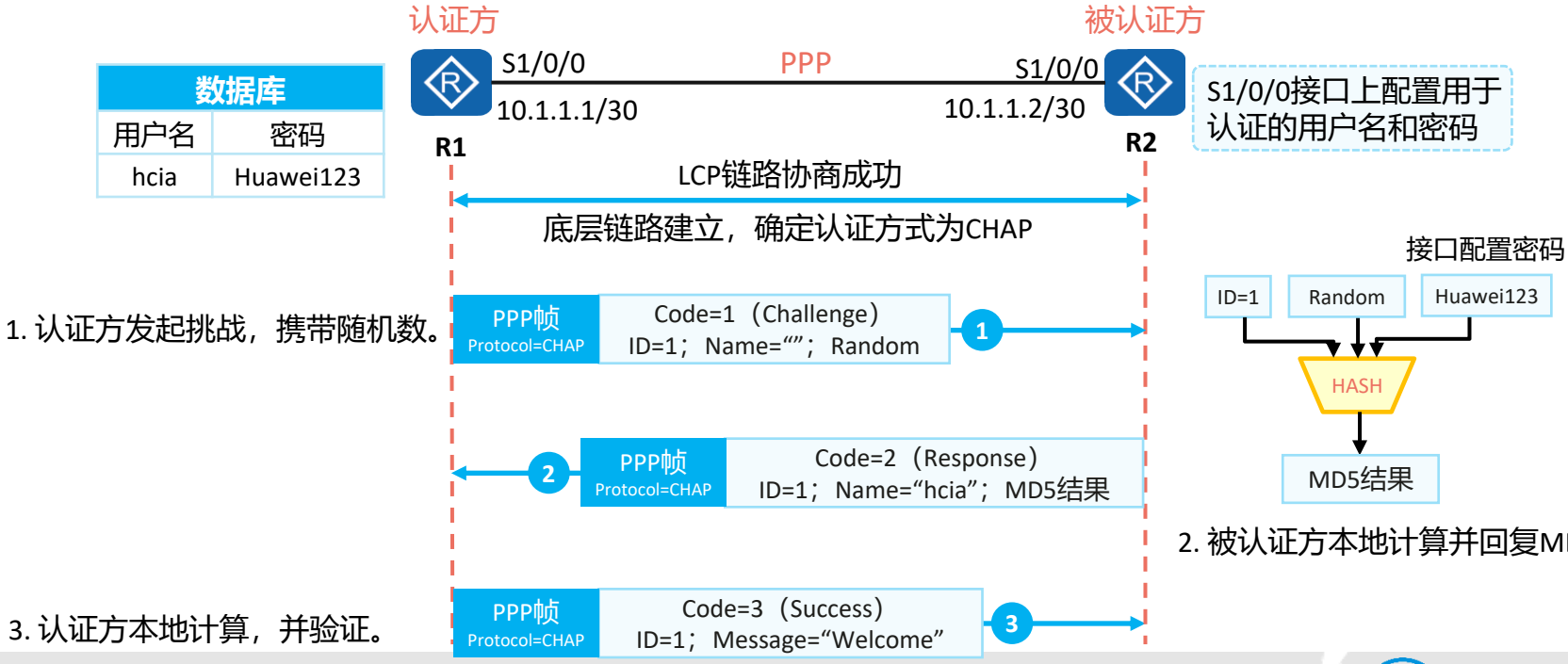
PPP认证模式 - PAP

- 链路协商成功后，进行认证协商（此过程可选）。认证协商有两种模式，PAP和CHAP。
- PAP认证双方有两次握手。协商报文以明文的形式在链路上传输。



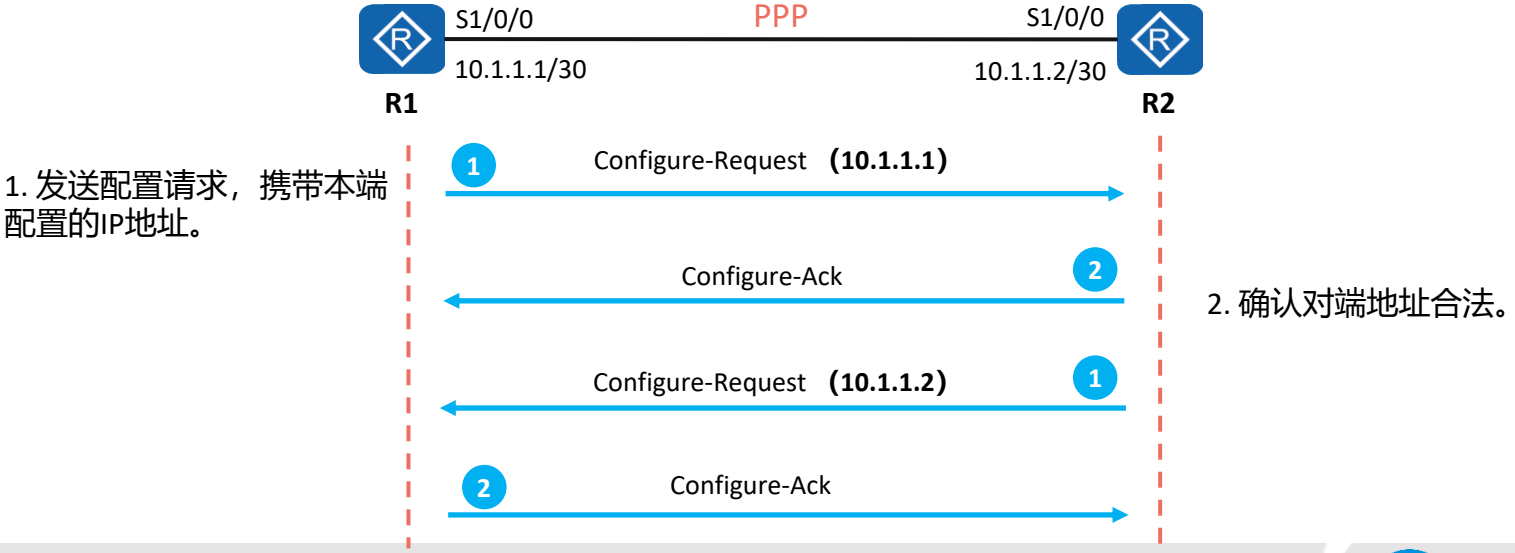
PPP认证模式 - CHAP

- CHAP认证双方有三次握手。协商报文被加密后再在链路上传输。



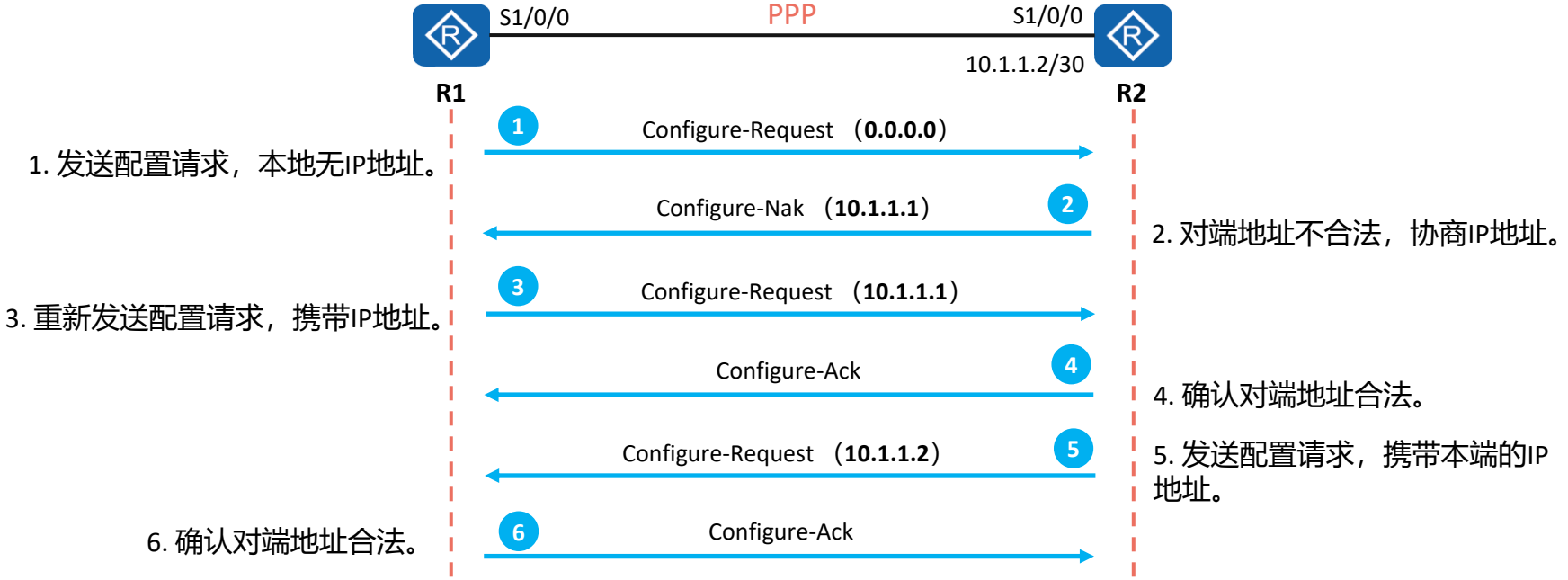
NCP协商 - 静态IP地址协商

- PPP认证协商后，双方进入NCP协商阶段，协商在数据链路上所传输的数据包的格式与类型。以常见的IPCP协议为例，它分为静态IP地址协商和动态IP地址协商。
- 静态IP地址协商需要手动在链路两端配置IP地址。



NCP协商 - 动态IP地址协商

- 动态IP地址协商支持PPP链路一端为对端配置IP地址。



PPP基础配置命令

1. 配置接口封装PPP协议

```
[Huawei-Serial0/0/0] link-protocol ppp
```

在接口视图下，将接口封装协议改为ppp，华为串行接口默认封装协议为ppp。

2. 配置协商超时时间间隔

```
[Huawei-Serial0/0/0] ppp timer negotiate seconds
```

在PPP LCP协商过程中，本端设备会向对端设备发送LCP协商报文，如果在指定协商时间间隔内没有收到对端的应答报文，则重新发送。

PAP认证配置命令

1. 配置验证方以PAP方式认证对端

```
[Huawei-aaa] local-user user-name  password { cipher | irreversible-cipher } password
[Huawei-aaa] local-user user-name service-type ppp
```

```
[Huawei-Serial0/0/0] ppp authentication-mode pap
```

配置验证方以PAP方式认证对端，首先需要通过AAA将被验证方的用户名和密码加入本地用户列表，然后选择认证模式。

2. 配置被验证方以PAP方式被对端认证

```
[Huawei-Serial0/0/0] ppp pap local-user user-name password { cipher | simple } password
```

配置本地被对端以PAP方式验证时，本地发送PAP用户名和口令。

CHAP认证配置命令

1. 配置验证方以CHAP方式认证对端

[Huawei-aaa] **local-user** *user-name* **password { cipher | irreversible-cipher }** *password*
[Huawei-aaa] **local-user** *user-name* **service-type ppp**

[Huawei-Serial0/0/0] **ppp authentication-mode chap**

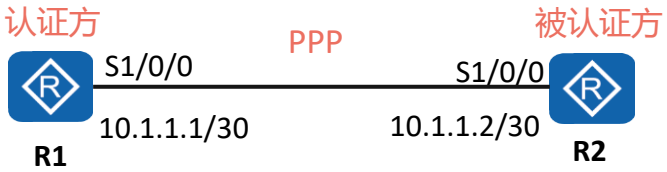
2. 配置被验证方以CHAP方式被对端认证

[Huawei-Serial0/0/0] **ppp chap user** *user-name*

[Huawei-Serial0/0/0] **ppp chap password** { **cipher** | **simple** } *password*

配置本地用户名，配置本地被对端以CHAP方式验证时的口令。

配置举例 - PAP认证



- 实验要求：
  1. 在R1与R2之间的PPP链路上启用PAP认证功能；
  2. 将R1配置为认证方；
  3. 将R2配置为被认证方。

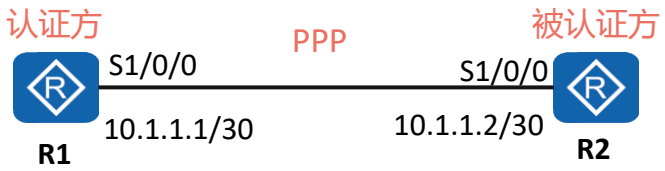
R1的配置如下：

```
[R1]aaa    #添加待认证用户信息
[R1-aaa]local-user huawei password cipher huawei123
[R1-aaa]local-user huawei service-type ppp        #指定认证用户业务类型
[R2]interface Serial 1/0/0
[R1-Serial1/0/0]link-protocol ppp
[R1-Serial1/0/0]ppp authentication-mode pap       #指定认证模式为PAP
[R1-Serial1/0/0]ip address 10.1.1.1 30
```

R2的配置如下：

```
[R2]interface Serial 1/0/0
[R2-Serial1/0/0]link-protocol ppp
[R2-Serial1/0/0]ppp pap local-user huawei password cipher huawei123
                #添加PPP认证的用户信息
[R2-Serial1/0/0]ip address 10.1.1.2 30
```

配置举例 - CHAP认证



- 实验要求：
  1. 在R1与R2之间的PPP链路上启用CHAP认证功能；
  2. 将R1配置为认证方；
  3. 将R2配置为被认证方。

R1的配置如下：

```
[R1]aaa     #添加待认证用户信息
[R1-aaa]local-user huawei password cipher huawei123
[R1-aaa]local-user huawei service-type ppp
#指定认证用户业务类型
[R1]interface Serial 1/0/0
[R1-Serial1/0/0]link-protocol ppp
[R1-Serial1/0/0]ppp authentication-mode chap
#指定认证模式为CHAP
```

R2的配置如下：

```
[R2]interface Serial 1/0/0
[R2-Serial1/0/0]link-protocol ppp
[R2-Serial1/0/0]ppp chap user huawei
[R2-Serial1/0/0]ppp chap password cipher huawei123
#添加PPP认证的用户信息
```

PPP基础命令

- **双方接口封装PPP**

```
Router(config-if)# encapsulation ppp
```

- **认证方配置对端的用户名和密码**

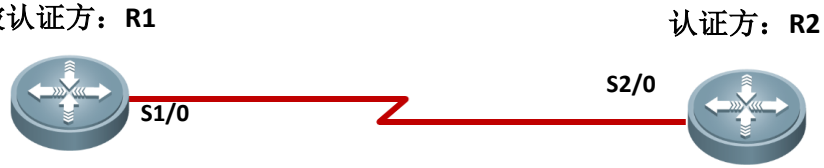
```
Router(config)# username name password password
```

- **认证方配置PPP认证方式（启用PAP或者CHAP认证）**

```
Router(config-if)# ppp authentication {chap | chap pap | pap chap | pap}
```

PPP典型配置案例（PAP单向认证）

ppp authentication pap命令指定本地为验证方，验证方需要配置被验证方的用户名密码列表。




```
interface Serial1/0
 ip address 1.1.1.1 255.255.255.0
 encapsulation ppp

ppp pap sent-username ruijie password 0 ruijie
```

对端配置的用户名　对端配置的密码

对端使用的用户名　对端使用的密码

```
username ruijie password 0 ruijie
interface Serial2/0
encapsulation ppp
 ip address 1.1.1.2 255.255.255.0
ppp authentication pap
```

配置采用PAP认证方式

PPP典型配置案例（PAP单向认证）

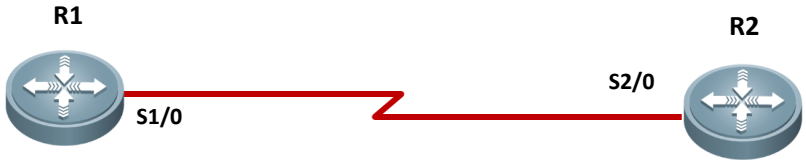
- PAP认证，接口状态验证


```
R1#show interface serial 1/0
Index(dec):35 (hex):23
Serial 1/0 is UP , line protocol is UP
Hardware is Serial
Interface address is: 1.1.1.1/24
  MTU 1500 bytes, BW 2000 Kbit
  Encapsulation protocol is PPP, loopback not set
  Keepalive interval is 10 sec ,retries 10.
  Carrier delay is 2 sec
  Rxload is 1/255, Txload is 1/255
  LCP Open
  Queueing strategy: FIFO
    Output queue 0/40, 0 drops;
    Input queue 0/75, 0 drops
  5 minutes input rate 0 bits/sec, 0 packets/sec
  5 minutes output rate 0 bits/sec, 0 packets/sec
    38021 packets input, 5656110 bytes, 0 no buffer, 0 dropped
    Received 23488 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
    38097packets output, 2135697bytes, 0 underruns , 0 dropped
```

```
R1#show interface serial 2/0
Index(dec):35 (hex):23
Serial 2/0 is UP , line protocol is UP
Hardware is Serial
Interface address is: 1.1.1.2/24
  MTU 1500 bytes, BW 2000 Kbit
  Encapsulation protocol is PPP, loopback not set
  Keepalive interval is 10 sec ,retries 10.
  Carrier delay is 2 sec
  Rxload is 1/255, Txload is 1/255
  LCP Open
  Queueing strategy: FIFO
    Output queue 0/40, 0 drops;
    Input queue 0/75, 0 drops
  5 minutes input rate 0 bits/sec, 0 packets/sec
  5 minutes output rate 0 bits/sec, 0 packets/sec
    38325 packets input, 5655320 bytes, 0 no buffer, 0 dropped
    Received 23358 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
    38235packets output, 2135895bytes, 0 underruns , 0 dropped
```

PPP典型配置案例（PAP双向认证）

- ppp authentication pap命令指定本地为验证方，验证方需要配置被验证方的用户名密码列表。

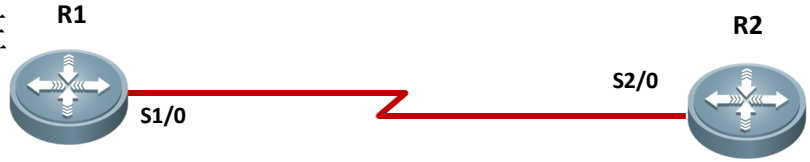



```
username ruijie2 password 0 ruijie2
interface Serial1/0
 ip address 1.1.1.1 255.255.255.0
 encapsulation ppp
ppp authentication pap
ppp pap sent-username ruijie1 password 0 ruijie1
```

```
username ruijie1 password 0 ruijie1
interface Serial2/0
encapsulation ppp
ppp authentication pap
 ip address 1.1.1.2 255.255.255.0
ppp pap sent-username ruijie2 password 0 ruijie2
```

PPP典型配置案例（PAP双向认证）

- 接口状态信息验证

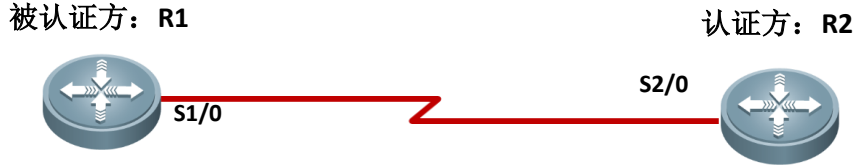



```
R1#show interface serial 1/0
Index(dec):35 (hex):23
Serial 1/0 is UP , line protocol is UP
Hardware is Serial
Interface address is: 1.1.1.1/24
  MTU 1500 bytes, BW 2000 Kbit
  Encapsulation protocol is PPP, loopback not set
  Keepalive interval is 10 sec ,retries 10.
  Carrier delay is 2 sec
  Rxload is 1/255, Txload is 1/255
  LCP Open
  Queueing strategy: FIFO
    Output queue 0/40, 0 drops;
    Input queue 0/75, 0 drops
  5 minutes input rate 0 bits/sec, 0 packets/sec
  5 minutes output rate 0 bits/sec, 0 packets/sec
    38021 packets input, 5656110 bytes, 0 no buffer, 0 dropped
    Received 23488 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
    38097packets output, 2135697bytes, 0 underruns , 0 dropped
```

```
R1#show interface serial 2/0
Index(dec):35 (hex):23
Serial 2/0 is UP , line protocol is UP
Hardware is Serial
Interface address is: 1.1.1.2/24
  MTU 1500 bytes, BW 2000 Kbit
  Encapsulation protocol is PPP, loopback not set
  Keepalive interval is 10 sec ,retries 10.
  Carrier delay is 2 sec
  Rxload is 1/255, Txload is 1/255
  LCP Open
  Queueing strategy: FIFO
    Output queue 0/40, 0 drops;
    Input queue 0/75, 0 drops
  5 minutes input rate 0 bits/sec, 0 packets/sec
  5 minutes output rate 0 bits/sec, 0 packets/sec
    38325 packets input, 5655320 bytes, 0 no buffer, 0 dropped
    Received 23358 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
    38235packets output, 2135895bytes, 0 underruns , 0 dropped
```

PPP典型配置案例（CHAP单向认证）

- ppp authentication chap命令指定本地为验证方，验证方需要配置被验证方的用户名密码列表。

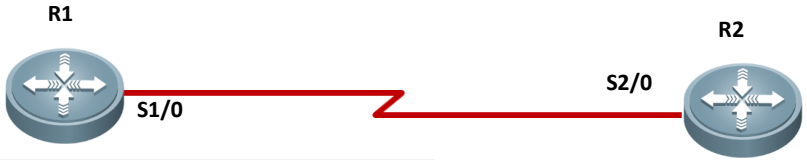



```
interface Serial1/0
 ip address 1.1.1.1 255.255.255.0
 encapsulation ppp
 ppp chap hostname ruijie1
 ppp chap password 0 ruijie1
```

```
username ruijie1 password 0 ruijie1
interface Serial2/0
encapsulation ppp
 ip address 1.1.1.2 255.255.255.0
ppp authentication chap
```

PPP典型配置案例（CHAP单向认证）

- 接口状态信息验证

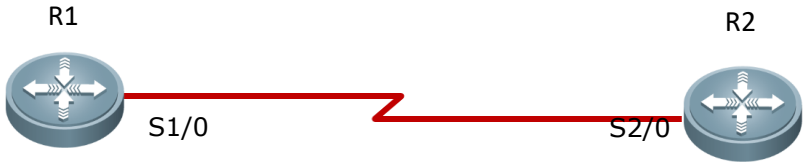



```
R1#show interface serial 1/0
Index(dec):35 (hex):23
Serial 1/0 is UP , line protocol is UP
Hardware is Serial
Interface address is: 1.1.1.1/24
  MTU 1500 bytes, BW 2000 Kbit
  Encapsulation protocol is PPP, loopback not set
  Keepalive interval is 10 sec ,retries 10.
  Carrier delay is 2 sec
  Rxload is 1/255, Txload is 1/255
  LCP Open
  Queueing strategy: FIFO
    Output queue 0/40, 0 drops;
    Input queue 0/75, 0 drops
  5 minutes input rate 0 bits/sec, 0 packets/sec
  5 minutes output rate 0 bits/sec, 0 packets/sec
    38021 packets input, 5656110 bytes, 0 no buffer, 0 dropped
    Received 23488 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
    38097packets output, 2135697bytes, 0 underruns , 0 dropped
```

```
R1#show interface serial 2/0
Index(dec):35 (hex):23
Serial 2/0 is UP , line protocol is UP
Hardware is Serial
Interface address is: 1.1.1.2/24
  MTU 1500 bytes, BW 2000 Kbit
  Encapsulation protocol is PPP, loopback not set
  Keepalive interval is 10 sec ,retries 10.
  Carrier delay is 2 sec
  Rxload is 1/255, Txload is 1/255
  LCP Open
  Queueing strategy: FIFO
    Output queue 0/40, 0 drops;
    Input queue 0/75, 0 drops
  5 minutes input rate 0 bits/sec, 0 packets/sec
  5 minutes output rate 0 bits/sec, 0 packets/sec
    38325 packets input, 5655320 bytes, 0 no buffer, 0 dropped
    Received 23358 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
    38235packets output, 2135895bytes, 0 underruns , 0 dropped
```

PPP典型配置案例（CHAP双向认证）

- ppp authentication chap命令指定本地为验证方，验证方需要配置被验证方的用户名密码列表。

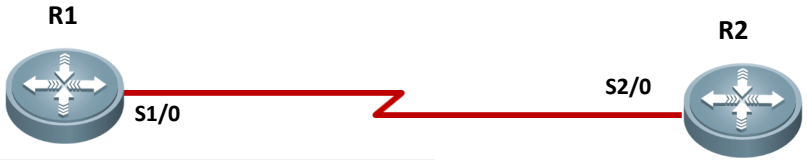



```
username ruijie2 password 0 ruijie2
interface Serial1/0
 ip address 1.1.1.1 255.255.255.0
 encapsulation ppp
 ppp authentication chap
 ppp chap hostname ruijie1
 ppp chap password 0 ruijie1
```

```
username ruijie1 password 0 ruijie1
interface Serial2/0
 ip address 1.1.1.2 255.255.255.0
encapsulation ppp
ppp authentication chap
ppp chap hostname ruijie2
 ppp chap password 0 ruijie2
```

PPP典型配置案例（CHAP双向认证）

- 接口状态信息验证

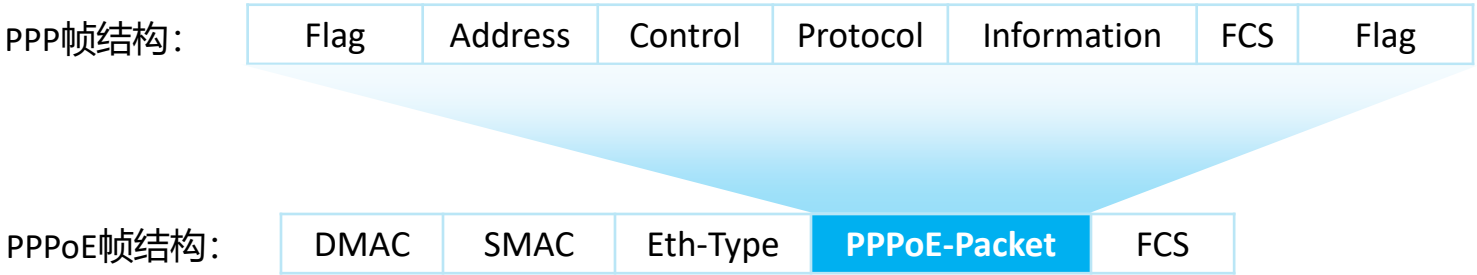



```
R1#show interface serial 1/0
Index(dec):35 (hex):23
Serial 1/0 is UP , line protocol is UP
Hardware is Serial
Interface address is: 1.1.1.1/24
  MTU 1500 bytes, BW 2000 Kbit
  Encapsulation protocol is PPP, loopback not set
  Keepalive interval is 10 sec ,retries 10.
  Carrier delay is 2 sec
  Rxload is 1/255, Txload is 1/255
  LCP Open
  Queueing strategy: FIFO
    Output queue 0/40, 0 drops;
    Input queue 0/75, 0 drops
  5 minutes input rate 0 bits/sec, 0 packets/sec
  5 minutes output rate 0 bits/sec, 0 packets/sec
    38021 packets input, 5656110 bytes, 0 no buffer, 0 dropped
    Received 23488 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
    38097packets output, 2135697bytes, 0 underruns , 0 dropped
```

```
R1#show interface serial 2/0
Index(dec):35 (hex):23
Serial 2/0 is UP , line protocol is UP
Hardware is Serial
Interface address is: 1.1.1.2/24
  MTU 1500 bytes, BW 2000 Kbit
  Encapsulation protocol is PPP, loopback not set
  Keepalive interval is 10 sec ,retries 10.
  Carrier delay is 2 sec
  Rxload is 1/255, Txload is 1/255
  LCP Open
  Queueing strategy: FIFO
    Output queue 0/40, 0 drops;
    Input queue 0/75, 0 drops
  5 minutes input rate 0 bits/sec, 0 packets/sec
  5 minutes output rate 0 bits/sec, 0 packets/sec
    38325 packets input, 5655320 bytes, 0 no buffer, 0 dropped
    Received 23358 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
    38235packets output, 2135895bytes, 0 underruns , 0 dropped
```

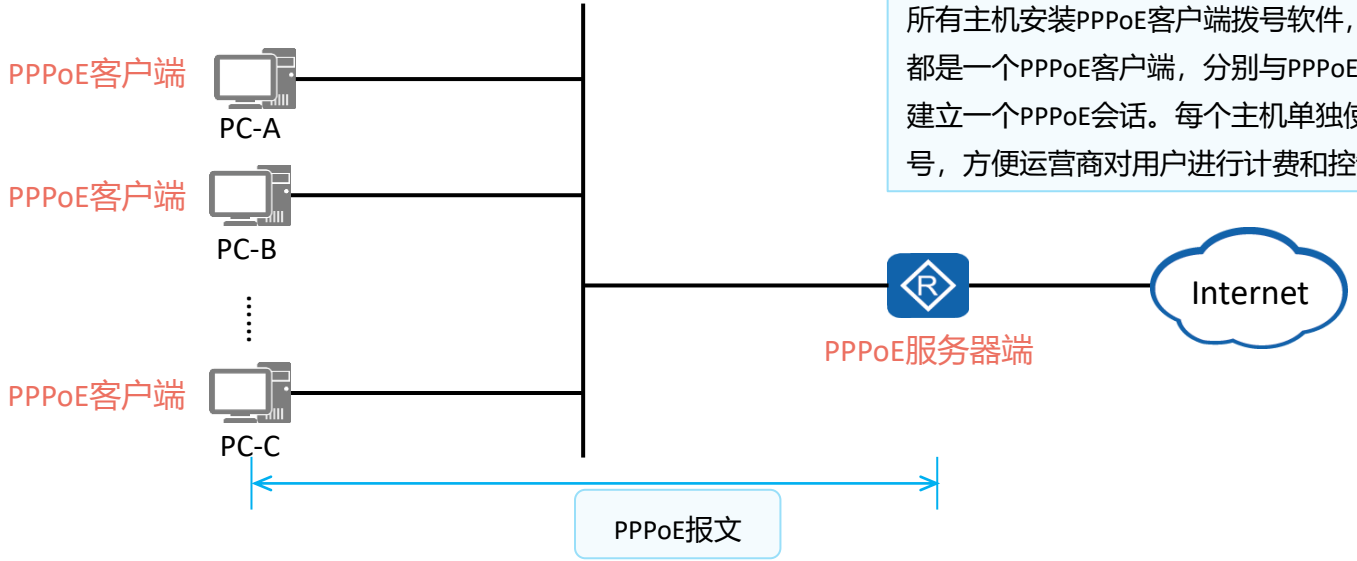
什么是PPPoE

- PPPoE（PPP over Ethernet，以太网承载PPP协议）是一种把PPP帧封装到以太网帧中的链路层协议。PPPoE可以使以太网网络中的多台主机连接到远端的宽带接入服务器。
- PPPoE集中了PPP和Ethernet两个技术的优点。既有以太网的组网灵活优势，又可以利用PPP协议实现认证、计费等功能。



PPPoE应用场景

- PPPoE实现了在以太网上提供点到点的连接。PPPoE客户端与PPPoE服务器端之间建立PPP会话，封装PPP数据报文，为以太网上的主机提供接入服务，实现用户控制和计费，在企业网络与运营商网络中应用广泛。
- PPPoE的常见应用场景有家庭用户拨号上网、企业用户拨号上网等。



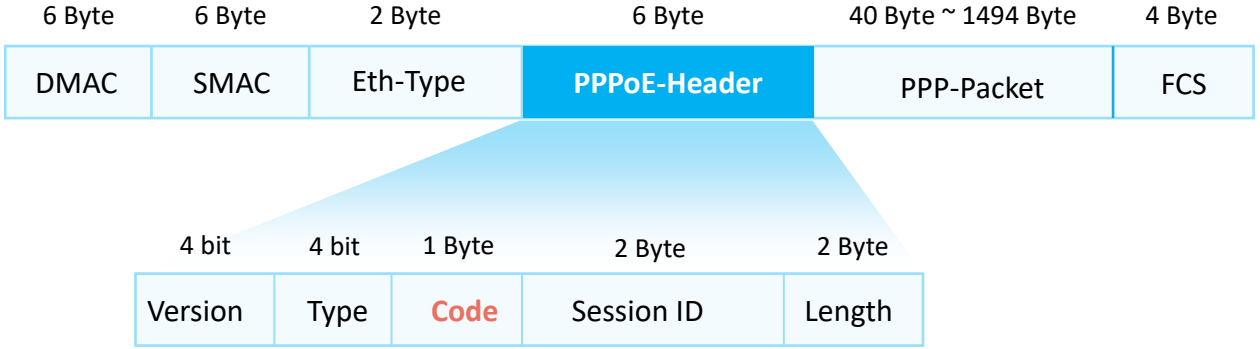
所有主机安装PPPoE客户端拨号软件，每个主机都是一个PPPoE客户端，分别与PPPoE服务器端建立一个PPPoE会话。每个主机单独使用一个账号，方便运营商对用户进行计费和控制。

PPPoE会话建立

- PPPoE的会话建立有三个阶段，PPPoE发现阶段、PPPoE会话阶段和PPPoE终结阶段。

PPPoE报文

- PPPoE会话的建立通过不同的PPPoE报文交互实现。PPPoE报文结构及常见的报文类型如下所示：

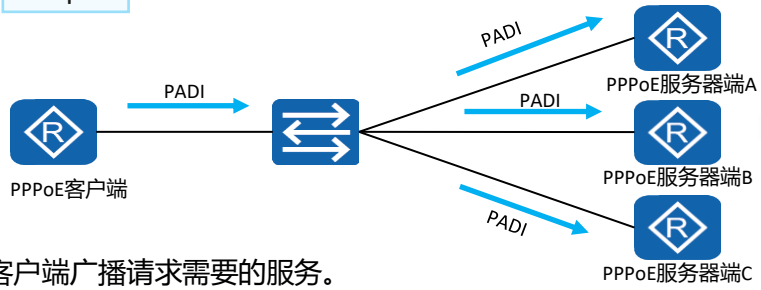


Code	名称	内容
0x09	PADI	PPPoE Active Discovery Initiation，PPPoE激活发现起始报文
0x07	PADO	PPPoE Active Discovery Offer，PPPoE激活发现服务报文
0x19	PADR	PPPoE Active Discovery Request，PPPoE激活发现请求报文
0x65	PADS	PPPoE Active Discovery Session-confirmation，PPPoE激活发现会话确认报文
0xa7	PADT	PPPoE Active Discovery Terminate，PPPoE激活发现终止报文

PPPoE发现阶段

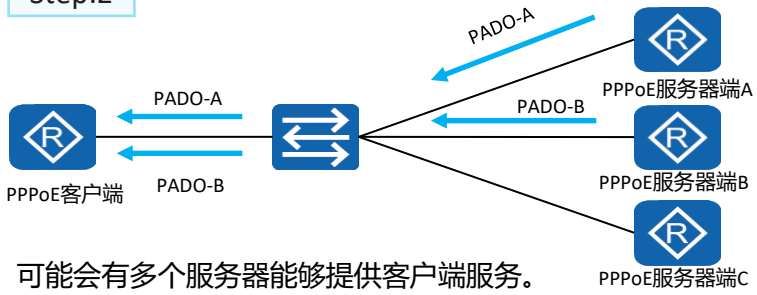
- PPPoE协议发现有四个步骤：客户端发送请求、服务端响应请求、客户端确认响应和建立会话。

Step:1



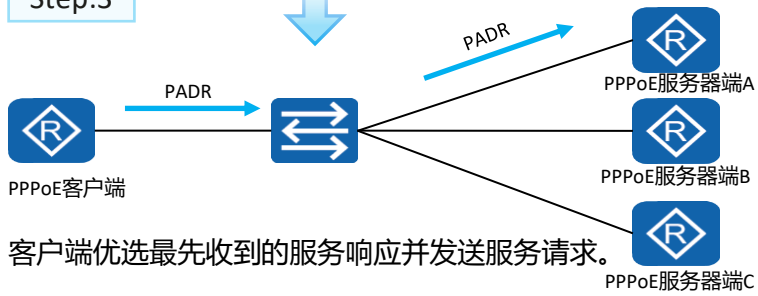
- 客户端广播请求需要的服务。

Step:2



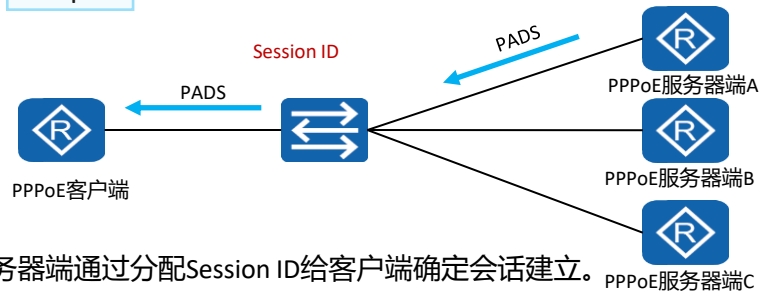
- 可能会有多个服务器能够提供客户端服务。

Step:3



- 客户端优选最先收到的服务响应并发送服务请求。

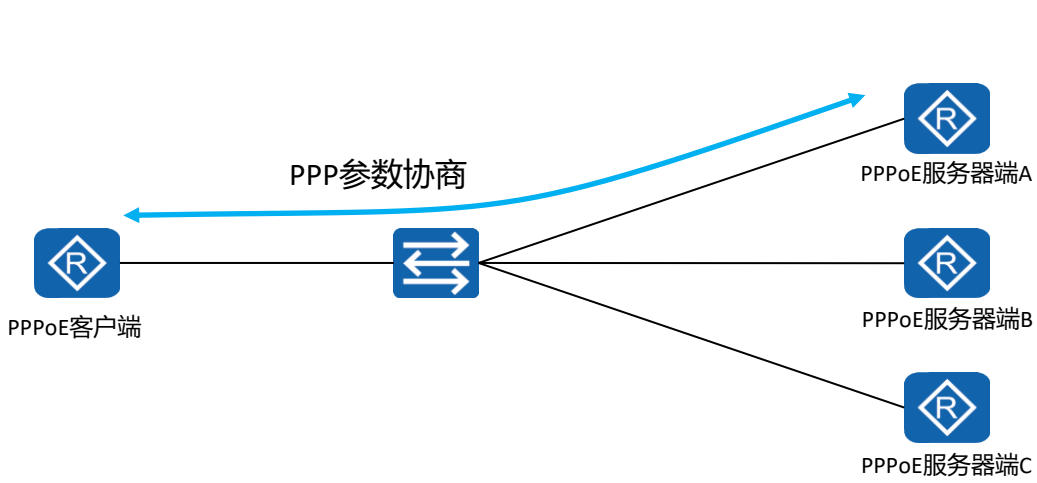
Step:4



- 服务器端通过分配Session ID给客户端确定会话建立。

PPPoE会话阶段

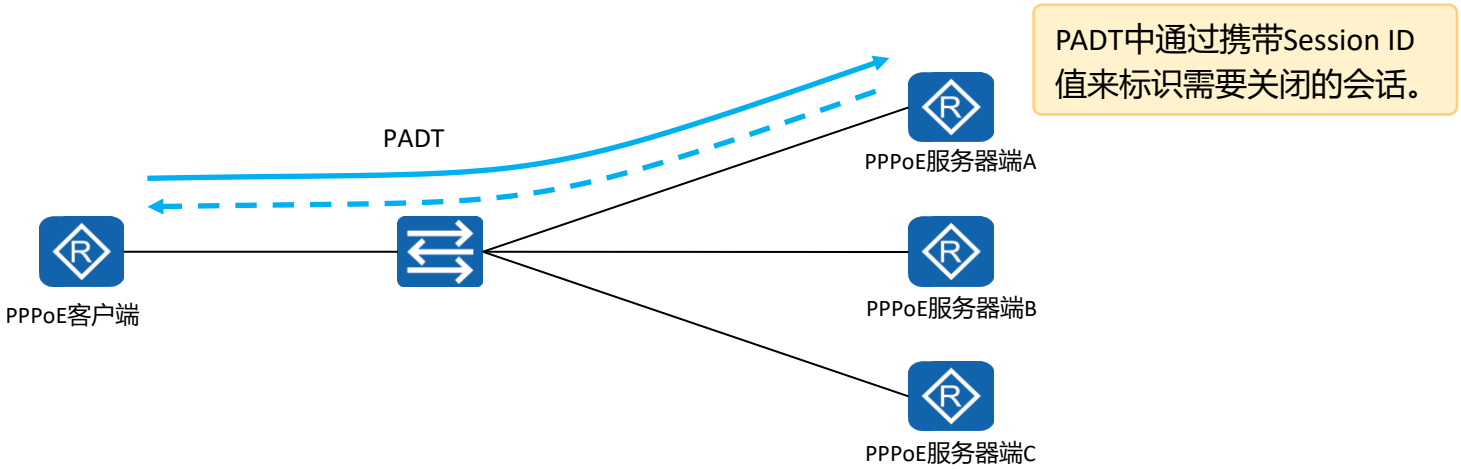
- PPPoE会话阶段会进行PPP协商，分为LCP协商、认证协商、NCP协商三个阶段。



在整个会话阶段，由PPPoE服务器端分配的Session ID值保持不变。

PPPoE会话终结阶段

- 当PPPoE客户端希望关闭连接时，会向PPPoE服务器端发送一个PADT报文，用于关闭连接。
- 同样，如果PPPoE服务器端希望关闭连接时，也会向PPPoE客户端发送一个PADT报文。



PPPoE基础配置

1. 通过拨号规则来配置发起PPPoE会话的条件

```
[Huawei] dialer-rule
```

2. 配置拨号接口用户名，此用户名必须与对端服务器用户名相同

```
[Huawei-Dialer1]dialer user username
```

3. 将接口置于一个拨号访问组

```
[Huawei-Dialer1]dialer-group group-number
```

4. 指定当前拨号接口使用的拨号绑定

```
[Huawei-Dialer1]dialer-bundle number
```

5. 将物理端口与dialer-bundle进行绑定

```
[Huawei-Ethernet0/0/0]pppoe-client dial-bundle-number number
```

配置实例 - PPPoE客户端

- 实验要求：
  1. 将R1设置为PPPoE客户端，R2为PPPoE服务器端；
  2. 在R1上配置PPPoE客户端拨号接口；
  3. 在R1上配置PPPoE客户端拨号接口的认证功能；
  4. R1上的拨号接口获取PPPoE服务器端分配的IP地址；
  5. R1通过拨号接口可以访问服务器端。

1.创建拨号接口并配置被认证方用户名和密码：

```
[R1]dialer-rule
[R1-dialer-rule]dialer-rule 1 ip permit
[R1-dialer-rule]quit
[R1]interface dialer 1
[R1-Dialer1] dialer user enterprise
[R1-Dialer1] dialer-group 1
[R1-Dialer1] dialer bundle 1
[R1-Dialer1] ppp chap user enterprise@huawei
[R1-Dialer1] ppp chap password cipher huawei123
[R1-Dialer1] ip address ppp-negotiate
```

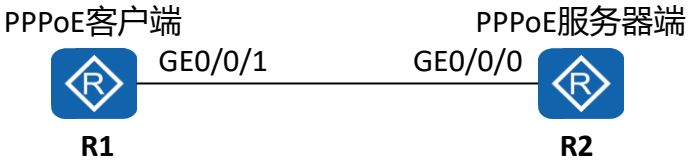
2.将拨号接口绑定出接口：

```
[R1]interface GigabitEthernet 0/0/1
[R1-GigabitEthernet0/0/1]pppoe-client dial-bundle-number 1
[R1-GigabitEthernet0/0/1]quit
```

3.配置本端到达服务器端的缺省路由：

```
[R1]ip route-static 0.0.0.0  0.0.0.0  dialer 1
```

配置实例 - PPPoE服务器端



- 实验要求：
  1. 在PPPoE服务器端上创建为客户端分配IP的地址池；
  2. PPPoE服务器端完成PPPoE客户端认证并分配合法的IP地址。

1.创建地址池与虚拟模板：

```
[R2]ip pool pool1          #创建地址池，指定分配的IP地址和网关
[R2-ip-pool-pool1]network 192.168.1.0 mask 255.255.255.0
[R2-ip-pool-pool1]gateway-list 192.168.1.254
[R2]interface Virtual-Template 1        #创建虚拟模板接口
[R2-Virtual-Template1]ppp authentication-mode chap
[R2-Virtual-Template1]ip address 192.168.1.254 255.255.255.0
[R2-Virtual-Template1]remote address pool pool1
```

2.将物理接口与虚拟模板绑定：

```
[R2]interface GigabitEthernet 0/0/0
[R2-GigabitEthernet0/0/0]pppoe-server bind virtual-template 1
[R2-GigabitEthernet0/0/0]quit
```

3.创建访问用户：

```
[R2]aaa       #添加认证用户信息
[R2-aaa]local-user huawei1 password cipher huawei123
[R2-aaa]local-user huawei1 service-type ppp
```

配置验证

1、查看拨号接口详细信息

```
<R1>display interface Dialer 1
Dialer1 current state: UP
Line protocol current state: UP (spoofing)
Description: HUAWEI, AR Series, Dialer1 Interface
Route Port, The Maximum Transmit Unit is 1500, Hold timer is
10(sec)
Internet Address is negotiated, 192.168.10.254/32
Link layer protocol is PPP
LCP initial
Physical is Dialer
Bound to Dialer1:0:
Dialer1:0 current state : UP
Line protocol current state : UP
Link layer protocol is PPP
LCP opened, IPCP opened
```

2、查看PPPoE-client会话初始状态信息

```
[R1]display pppoe-client session summary
PPPoE Client Session:
ID   Bundle  Dialer  Intf      Client-MAC      Server-MAC    State
0      1       1    GE0/0/1  54899876830c  000000000000  IDLE
```

3、查看PPPoE-client会话建立状态信息

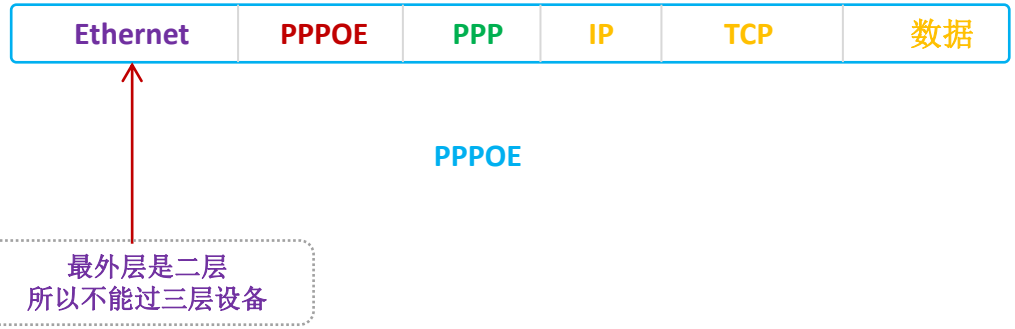
```
[R1]display pppoe-client session summary
PPPoE Client Session:
ID   Bundle  Dialer  Intf      Client-MAC      Server-MAC     State
1      1       1    GE0/0/1  00e0fc0308f6  00e0fc036781   UP
```

PPPOE介绍

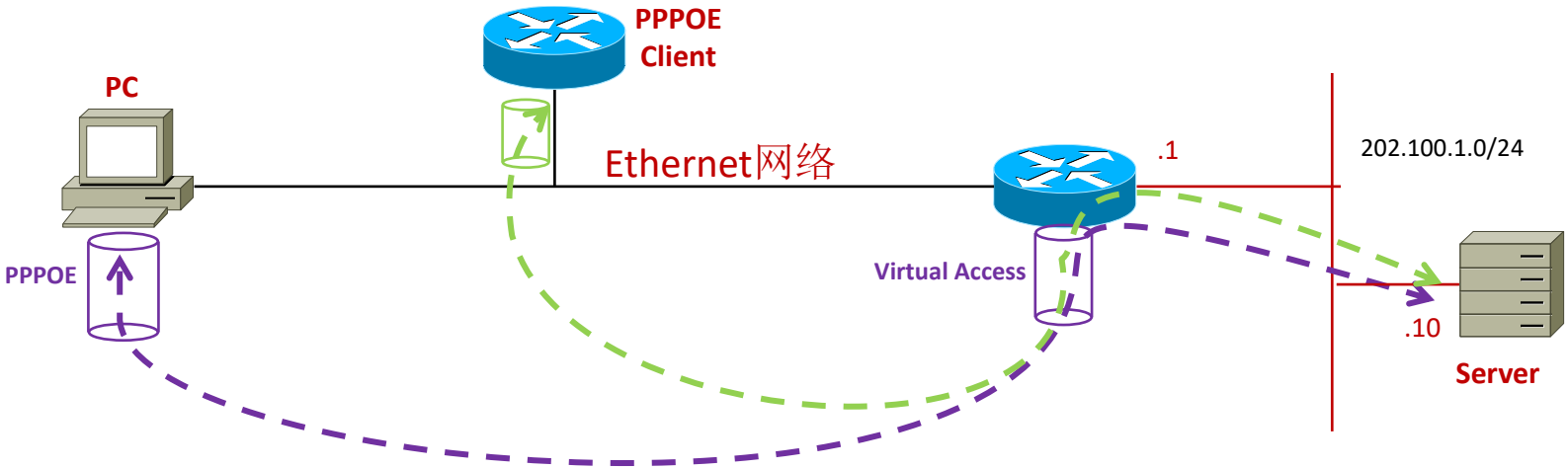
1. PPPOE是一个网络层协议用于把PPP帧封装到以太网帧内。
2. PPPOE被大量运用到电信运营商对用户的认证。
3. **PPPOE会话建立有两个阶段：PPPOED（0X8863）；PPPOES（0X8864）**

注意：ASA支持PPPOE的客户端， ASA不能做PPPOE的Server

PPPOE包结构



PPPOE实验拓扑



ETH Header SIP:MAC DIP:MAC	PPPOE	PPP	IP Header SIP:61.128.1.101 DIP:202.100.1.10	IP Payload

Cisco路由器PPPOE服务器配置

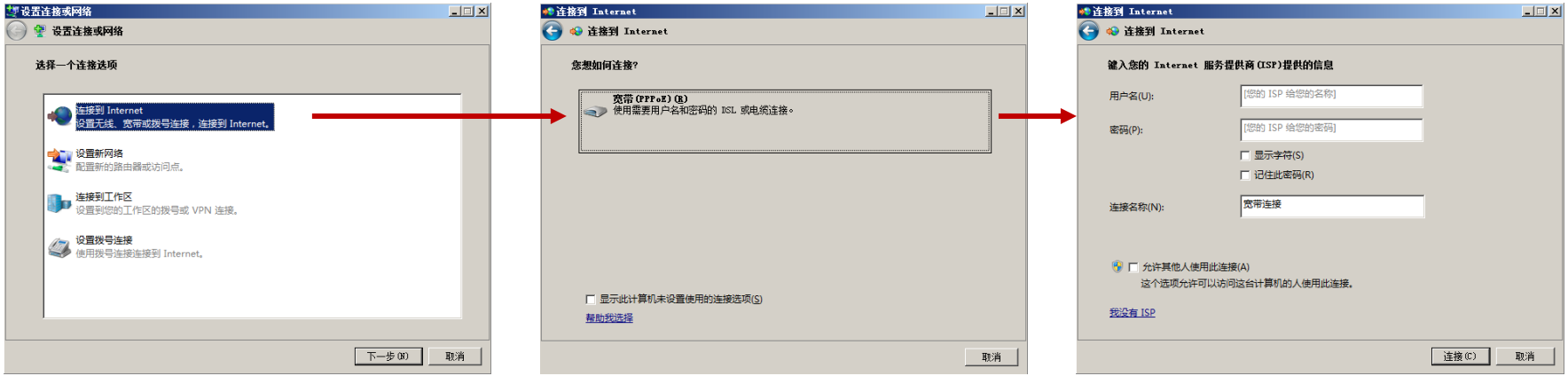
```
interface FastEthernet0/0
 no ip address（无需配置IP地址）
 pppoe enable （激活PPPOE）
!
username pppoeglab password 0 cisco
ip local pool ippool 61.128.1.100 61.128.1.200
!
bba-group pppoe global
 virtual-template 1
!
interface Virtual-Template1
 ip unnumbered Loopback0
 peer default ip address pool ippool
 ppp authentication pap（国内很多运营商的默认策略）
!
Interface Loopback 0
 ip address 202.100.1.10 255.255.255.0
```

Cisco路由器PPPOE-Client配置

PPPOE-Client

```
interface FastEthernet0/0
  no ip address
  pppoe-client dial-pool-number 1（激活PPPOE客户端）
interface Dialer1
  ip address negotiated
  ip mtu 1492（减去PPPOE+PPP的8个字节）
  encapsulation ppp
  dialer pool 1
  ppp ipcp route default （获得地址同时获取默认路由）
  ppp authentication pap callin（Callout不认证对端）
  ppp pap sent-username pppoeglab password 0 cisco
```

PC拨号配置



华为PPP0E配置

PPPoE服务器端的配置:

1)设置全局的用户名和密码用于认证

```
aaa
 local-user glab password cipher Huawei
 local-user glab service-type ppp
```

2）配置地址池，用于分发地址

```
ip pool PPPoE1
 network 202.100.1.0 mask 255.255.255.0
 dns-list 114.114.114.114
```

3）配置虚拟模版和调用模版

```
interface Virtual-Template1
 ppp authentication-mode chap
 remote address pool PPPoE1
 ip address 202.100.1.254 255.255.255.0
```

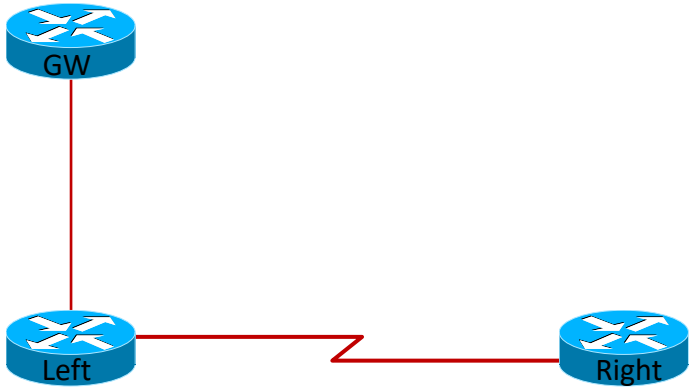
4)接口调用模版

```
interface GigabitEthernet0/0/0
 pppoe-server bind Virtual-Template 1
```

华为PPP0E配置

客户端配置:
[RTA]dialer-rule
[RTA-dialer-rule]dialer-rule 1 ip permit—允许所有IP报文转发
[RTA-dialer-rule]quit
[RTA]interface dialer 1
[RTA-Dialer1]dialer user enterprise---该用户名不用于认证，是标识作用以及和dialer绑定
[RTA-Dialer1]dialer-group 1
[RTA-Dialer1]dialer bundle 1
[RTA-Dialer1]ppp chap user glab
[RTA-Dialer1]ppp chap password cipher Huawei
[RTA-Dialer1]ip address ppp-negotiate
[RTA]interface GigabitEthernet 0/0/1
[RTA-GigabitEthernet0/0/1]pppoe-client dial-bundle-number 1
[RTA-GigabitEthernet0/0/1]quit
[RTA]ip route-static 0.0.0.0 0 dialer 1

课堂实验四



1.在上图中完成PPP封装
2.在上图中完成PPP的PAP验证
3.在上图中完成PPP的CHAP验证
第二个完成后改做第三个，建议做好第一个保存
4.完成Left和GW之间的PPPOE实验

IP地址分类和划分

1. 二八十十六进制之间的换算?
2. IP地址的分类? 什么是网络位? 什么是主机位?
3. 私有地址的作用?
4. 什么是掩码?
5. 可变长子网的概念和划分?

二进制、十进制和十六进制

进制	字符范围	基值
二进制	0 — 1	2
十进制	0 — 9	10
十六进制	0 —9，A — F	16

- 在IP网络中，二进制和十六进制是常用的编码方式。

进制之间转换

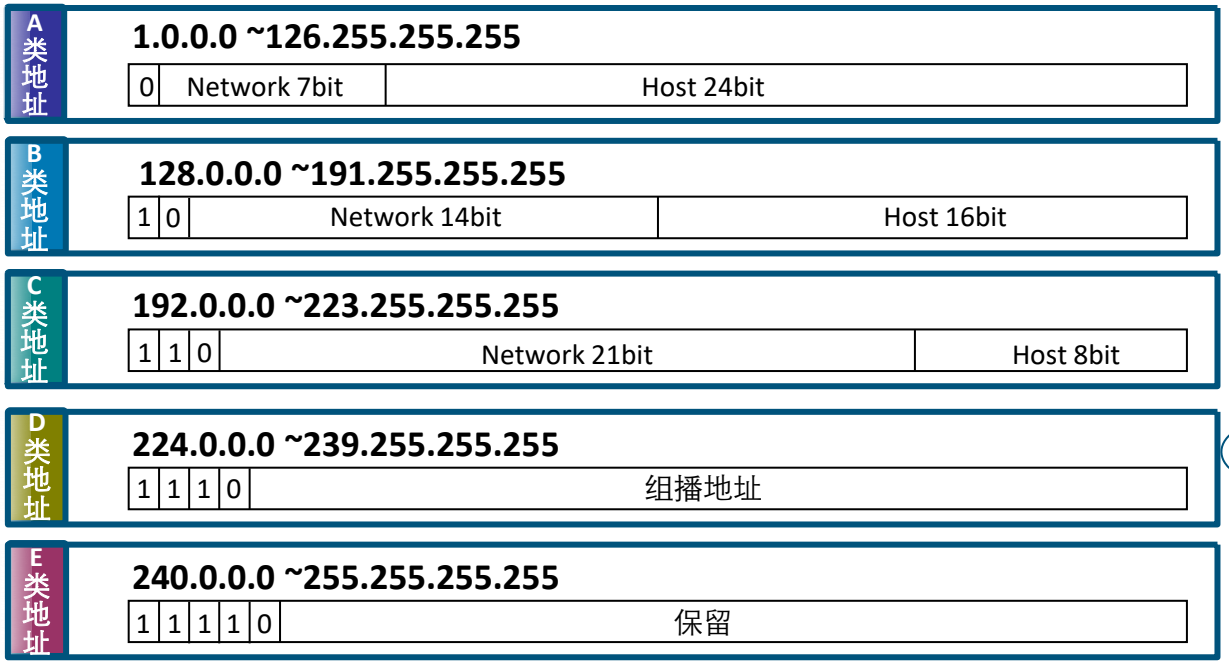
比特位	1	1	1	1	1	1	1	1
乘方	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
数值	128	64	32	16	8	4	2	1

十进制	二进制	十六进制
0	00000000	00
1	00000001	01
2	00000010	02
3	00000011	03
4	00000100	04
5	00000101	05
6	00000110	06
7	00000111	07
8	00001000	08

十进制	二进制	十六进制
9	00001001	09
10	00001010	0A
11	00001011	0B
12	00001100	0C
13	00001101	0D
14	00001110	0E
15	00001111	0F
…	…	…
255	11111111	FF

IP地址分类

IP地址的分类



子网掩码的出现使这种分类的概念弱化

IPv4私有地址

类	私有地址范围
A	10.0.0.0 到 10.255.255.255
B	172.16.0.0 到 172.31.255.255
C	192.168.0.0 到 192.168.255.255

思考：

1. 什么是私有地址?
2. 私有地址的作用是什么?

可变长子网划分实例

实例：
G-LAB 实验室总共7个部门，如下：
销售部16人
技术部25人
生产部60人
财务部6人
采购部12人
没事喝茶部5人
高级认证部17人
要求：从192.168.10.0/24的c类网络划分7个不同的子网给各部门，请分别写出每个部门的网络号、掩码、主机最大个数、网关、广播地址。

可变长子网划分练习一

某分公司通过总公司获得一个IP网络

172.30.88.0/24

需划分出几个子网

部门一：5个人　五年内不扩展

部门二：16个人　五年内可达23人

部门三：31个人，五年内可达63人

再划分出两个特殊的网络，广域网A有5个路由器，广域网B是一个点到点网络

写出所有网络号和掩码的二进制

算出以上网络号，可用地址范围，子网掩码，不得有冲突存在

可变长子网划分练习二

求出以下几个IP地址的网络号、可用主机范围、广播地址及子网掩码十进制格式。

172.16.133.135/27

189.29.213.233/28

10.1.11.0/23

路由技术

1. 路由是什么？为什么需要路由?
2. 路由中唯一的标识是什么?
3. 路由表的组成?
4. 路由协议的分类和介绍
5. 动态路由和静态路由的比较?

路由表组成

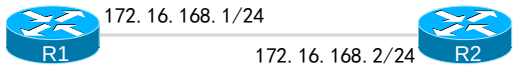
路由表作用：数据转发的语句，控制层

```
11.0.0.0/32 is subnetted, 1 subnets
   11.1.1.1 [110/11] via 12.1.1.1, 00:00:19, Ethernet0/0
12.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
   12.1.1.0/24 is directly connected, Ethernet0/0
   12.1.1.2/32 is directly connected, Ethernet0/0
13.0.0.0/24 is subnetted, 1 subnets
   13.1.1.0 [110/20] via 12.1.1.1, 00:00:19, Ethernet0/0
100.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
   100.1.1.0/24 is directly connected Ethernet0/1
   100.1.1.2/32 is directly connected Ethernet0/1
```

路由表三个重要组成：

目标网段+下一跳+出接口

路由架构数据包通讯原理（一）



简述拓扑中R1 ping 172.16.168.2的通讯过程（R1上处理过程如下）？

1. 无故ARP解析（作用是什么？）
2. 查找路由表
3. ARP请求
4. 收到ARP回复
5. 数据包封装
6. 数据包发送出去

路由架构数据包通讯原理（二）

简述拓扑中R1 ping R3 192.168.1.2的通讯过程？

路由架构数据包通讯原理（三）

简述拓扑中R1 ping R3 192.168.1.2的通讯过程？

形成路由表的方法

1. 静态路由（协议）:Static. IPv6 Static
2. 动态路由协议
   - 内部网关协议（IGP）
     - RIP(v1,v2) RIPng
     - EIGRPv4 EIGRPv6
     - OSPFv2 OSPFv3
     - ISIS
   - 外部网关协议（EGP ）
     - BGP MP-BGP

静态路由 Static

1. 网络管理员手动输入路由器的路由
2. 基于目标网段指定的路由
3. 单向性，回来的数据包需要单独再写一条
4. 优点是稳定，缺点是不适合大型网络，配置繁琐

配置语法

R1(config)#ip route 12.1.1.0 255.255.255.0 100.1.1.1

或者

R1(config)#ip route 12.1.1.0 255.255.255.0 s0/0

讨论：指定出接口和指定下一跳的区别？

默认路由 Static

R1(config)#ip route 0.0.0.0 0.0.0.0 100.1.1.1

- 0.0.0.0 代表任意网段
- 出口路由器一般配置默认路由到运营商ISP

思考：出口路由器接两条运营商的时候，默认路由怎么配置（静态浮动路由）？流量从哪条运营商出去？如何实现负载?

静态路由路由表

```
R1#sh ip route static
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is 12.1.1.2 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 12.1.1.2
      100.0.0.0/24 is subnetted, 1 subnets
S        100.1.1.0 [1/0] via 13.1.1.3
R1#
```

S*：默认路由在路由表的前缀标识

S：静态路由在路由表的前缀标识

课堂实验五

实验需求：

1. R1环回口11.1.1.1模拟PC1
2. R2建立2个环回口模拟Server
   - Server-1:22.1.1.1
   - Server-2:44.1.1.1
3. 要求使用静态路由实现全网互通
   - PC1去往server-1从华为R走
   - PC1去往server-2不从华为R走
   - PC1可以telnet R2环回口172.18.129.100进行登录管理

THANK YOU

Ping 通您的梦想～

腾讯课堂交流群：17942636

ADD：苏州市干将东路666号和基广场401-402；Tel：0512-8188 8288；

课程咨询QQ：2853771087 ； 官网 :www.51glab.com