

第 7 篇 广域网接入和互连

第 29 章 配置 HDLC

第 30 章 配置 PPP

第 31 章 配置 3G

第 32 章 配置 WLAN

第29章 配置 HDLC

HDLC (High Level Data Link Control, 高级数据链路控制) 协议是由 IBM 的 SDLC (Synchronous Data Link Control, 同步数据链路控制) 协议演变而来。ANSI 和 ISO 均采纳并发展了 SDLC, 并分别提出了自己的标准。ANSI 提出了 ADCCP (Advanced Data Communication Control Procedure, 高级通讯控制过程), 而 ISO 提出了 HDLC。本章将讲解 HDLC 协议的基本原理以及基础配置。

29.1 本章目标

课程目标

○ 学习完本课程, 您应该能够:

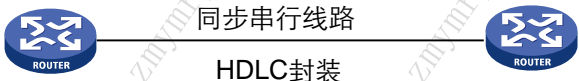
- 描述HDLC协议的基本特点
- 掌握HDLC协议的基本配置



www.h3c.com

29.2 HDLC概述

HDLC概述



同步串行线路
HDLC封装

- 面向比特
- 透明传输
- 标准HDLC不支持多协议

www.h3c.com

HDLC (High-level Data Link Control, 高级数据链路控制) 是一种面向比特的链路层协议, 其最大特点是对任何一种比特流, 均可以实现透明的传输。

在 HDLC 中, 只要载荷数据流中不存在同标志字段 F 相同的数据, 就不至于引起帧边界的错误判断。万一出现同边界标志字段 F 相同的数据, 即数据流中出现连续六个 1 的情况, 可以用零比特填充法解决。

在标准 HDLC 协议格式中没有包含标识所承载的上层协议信息的字段, 所以在采用标准 HDLC 协议的单一链路上只能承载单一的网络层协议。

29.3 HDLC的帧格式



在 HDLC 中，数据和控制报文均以帧的标准格式传送。总体上，HDLC 有三种不同类型的帧：信息帧（I 帧）、监控帧（S 帧）和无编号帧（U 帧），这三种类型不同的 HDLC 帧在 HDLC 协议中发挥着不同的作用。其中：

- 信息帧用于传送用户数据，通常简称为 I 帧；
- 监控帧用于差错控制和流量控制，通常称为 S 帧；
- 无编号帧也称为 U 帧，用于提供对链路的建立、拆除以及多种控制功能。

而 HDLC 的帧格式由标志、地址、控制、信息和帧校验序列等字段组成：

- 标志字段 F：标志一个 HDLC 帧的开始和结束，所有的帧必须以 F 开头，并以 F 结束；
- 地址字段 A：用于标识接收或发送 HDLC 帧的地址；
- 控制字段 C：用来实现 HDLC 协议的各种控制信息，并标识是否是数据；
- 信息字段 I：可以是任意的二进制比特串，是链路层的有效载荷（用户数据）；
- 帧检验序列字段 FCS：可以使用 16 位 CRC，对两个标志字段之间的整个帧的内容进行校验。

29.4 HDLC链路状态检测



HDLC 具有简单的探测链路及对端状态的功能。在链路物理层就绪后，HDLC 设备以轮询时间间隔为周期，向链路上发送 Keepalive 消息，探测对方设备是否存在。如果在 5 个周期内无法收到对方发出的 Keepalive 消息，HDLC 设备就认为链路不可用，则链路层状态变为 Down。


同一链路两端设备的轮询时间间隔应设为相同的值，否则会导致链路不可用。

缺省情况下，接口的 HDLC 轮询时间间隔为 10 秒。如果将两端的轮询时间间隔都设为 0，则禁止链路状态检测功能。

29.5 HDLC协议特点

HDLC协议特点

- 对于任何一种比特流都可透明传输
- 较高的数据链路传输效率
- 所有的帧都有**FCS**，传输可靠性高
- 用统一的帧格式来实现传输
- 不支持验证，缺乏足够的安全性
- 协议不支持**IP**地址协商
- 用于点到点的同步链路



紫光集团 H3C
核心企业 数字化转型方案领导者

www.h3c.com


HDLC 具有以下主要特点：

- 协议不依赖于任何一种字符编码集，对于任何一种比特流都可透明传输；
- 全双工通讯，有较高的数据链路传输效率；
- 所有的帧（包括响应帧）都有 **FCS**，对信息帧进行顺序编号，可防止漏收重收，传输可靠性高；
- 采用统一的帧格式来实现数据、命令、响应的传输，容易实现；
- 不支持验证，缺乏足够的安全性；
- 协议不支持 **IP** 地址协商；

用于点到点的同步链路，例如同步模式下的串行接口和 **POS** 接口等。

29.6 HDLC配置

HDLC配置



紫光集团 H3C
核心企业 数字化转型领导者

- 设置接口链路层协议为HDLC

[Router-Serial1/0] link-protocol hdlc

- 设置HDLC的Keepalive轮询时间间隔

[Router-Serial1/0] timer-hold seconds

www.h3c.com

要在路由器上配置 HDLC 协议，首先应进入相应串口的接口视图，然后用 **link-protocol hdlc** 命令将 HDLC 配置为链路层协议即可。配置时应注意的是，链路两端的设备都需要配置为 HDLC，否则无法通信。

要设置 HDLC 协议轮询时间间隔，应进入相应串口的接口视图，然后用 **timer-hold seconds** 命令配置时间间隔，单位为秒。默认情况下，接口的 HDLC 协议轮询时间间隔为 10 秒，取值范围为 0~32767 秒。

注意：

路由器串口的默认链路层协议为 PPP。

29.7 本章总结

本章总结

- HDLC协议概念
- HDLC协议帧格式
- HDLC协议状态轮询
- HDLC协议特点
- HDLC协议使用限制
- HDLC协议配置

www.h3c.com

第30章 配置 PPP

多样的广域网线路类型需要更强大、功能更完善的链路层协议支持，例如适应多变的链路类型，并提供一定的安全特性等。PPP 协议是提供在点到点链路上传递、封装网络层数据包的一种数据链路层协议。由于支持同异步线路，能够提供验证，并且易于扩展，PPP 获得了广泛的应用。

30.1 本章目标

课程目标

● 学习完本课程，您应该能够：

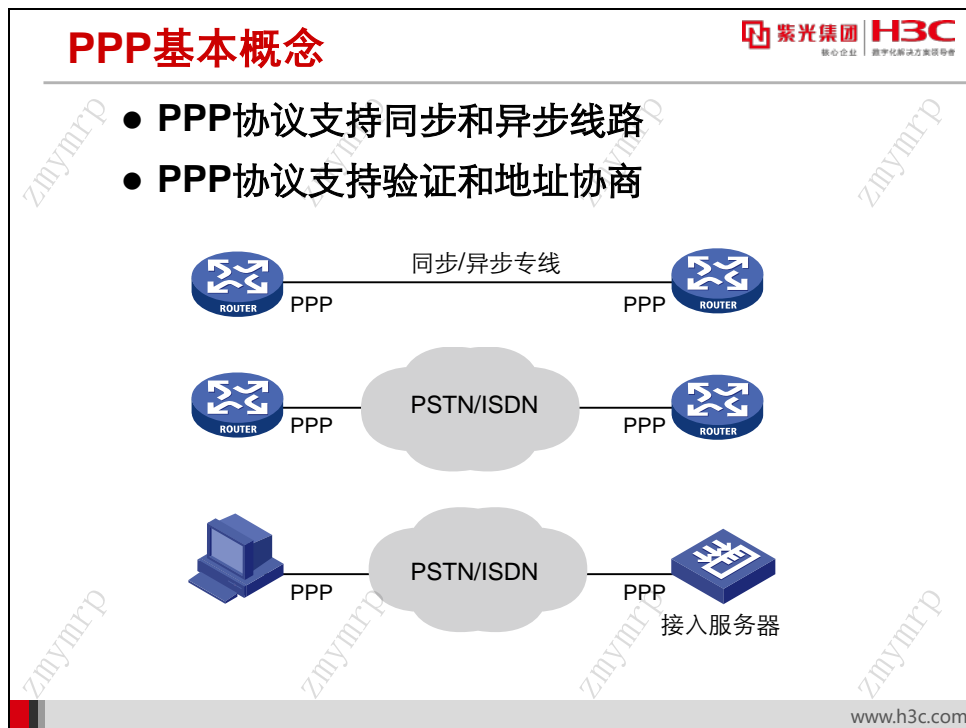
- 掌握PPP协议的原理和特点
- 掌握PPP协议的协商过程
- 掌握PPP协议两种验证方式
- 掌握PPP协议的配置
- 掌握PPP MP的实现及配置
- 熟悉PPP协议的维护命令及方法



www.h3c.com

30.2 PPP 协议概述

30.2.1 PPP 基本概念



PPP (Point-To-Point Protocol, 点到点协议) 是在 SLIP (Serial Line IP, 串行线 IP 协议) 的基础上发展起来的。SLIP 协议只支持异步传输方式, 无协商过程, 尤其是不能协商诸如双方 IP 地址等网络层属性, 因此逐步被 PPP 协议所替代。

作为一种提供在点到点链路上传输、封装网络层数据包的数据链路层协议, PPP 处于 TCP/IP 协议栈的网络接口层, OSI 参考模型的数据链路层, 主要被设计用于在支持全双工的同异步链路上进行点到点之间的数据传输。


PPP 可以用于多种链路类型, 包括:

- 同步和异步专线;
- 异步拨号链路, 如 PSTN 拨号连接;
- 同步拨号链路, 如 ISDN 拨号连接。

30.2.2 PPP 的特点

PPP的特点

- 可以工作在同异步方式下
- 能够控制数据链路的建立
- 支持验证，更加安全
- 可同时支持多种网络层协议
- 可以对网络层地址进行协商，能够远程分配 IP 地址
- 无重传机制，网络开销小



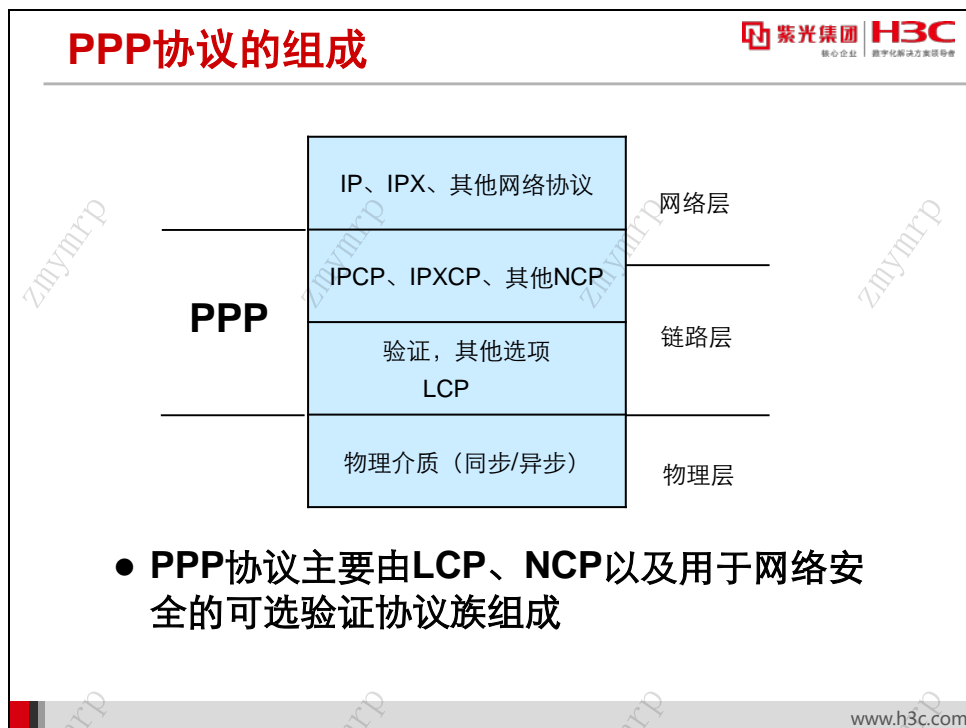
紫光集团 H3C
核心企业 数字化转型方案领导者

www.h3c.com

作为目前使用最广泛的广域网协议，PPP 具有如下特点：

- PPP 是面向字符的，在点到点串行链路上使用字符填充技术，既支持同步链路又支持异步链路；
- PPP 通过 LCP（Link Control Protocol，链路控制协议）部件能够有效控制数据链路的建立；
- PPP 支持验证协议族 PAP（Password Authentication Protocol）和 CHAP（Challenge-Handshake Authentication Protocol），更好地保证了网络的安全性；
- PPP 支持各种 NCP（Network Control Protocol，网络控制协议），可以同时支持多种网络层协议。典型的 NCP 包括支持 IP 的 IPCP 和支持 IPX 的 IPXCP 等；
- PPP 可以对网络层的地址进行协商，支持 IP 地址的远程分配，能满足拨号线路的需求；
- PPP 无重传机制，网络开销小。

30.2.3 PPP 协议的组成



PPP 并非单一的协议，而是由一系列协议构成的协议族。上图展示了 PPP 协议的分层结构。

在物理层，PPP 能使用同步介质（如 ISDN 或同步 DDN 专线），也能使用异步介质（如基于 Modem 拨号的 PSTN）。

另外 PPP 通过链路控制协议族（Link Control Protocol，LCP）在链路管理方面提供了丰富的服务，这些服务以 LCP 协商选项的形式提供；通过网络控制协议族（Network Control Protocol，NCP）提供对多种网络层协议的支持；通过 PPP 扩展协议族提供对 PPP 扩展特性的支持，例如 PPP 以验证协议 PAP（Password Authentication Protocol）和 CHAP（Challenge-Handshake Authentication Protocol）实现安全验证的功能。

PPP 的主要组成及其作用如下：

- **链路控制协议（Link Control Protocol，LCP）**：主要用于管理 PPP 数据链路，包括建立、拆除和监控数据链路等；
- **网络控制协议（Network Control Protocol，NCP）**：主要用于协商所承载的网络层协议的类型及其属性，协商在该数据链路上所传输的数据包的格式与类型，配置网络层协议等；
- **验证协议 PAP（Password Authentication Protocol）和 CHAP（Challenge-Handshake Authentication Protocol）**：主要用来验证 PPP 对端设备的身份合法性，在一定程度上保证链路的安全性。

在上层，PPP 通过多种 NCP 提供对多种网络层协议的支持。每一种网络层协议都有一种对应的 NCP 为其提供服务，因此 PPP 具有强大的扩展性和适应性。

30.3 PPP协议会话

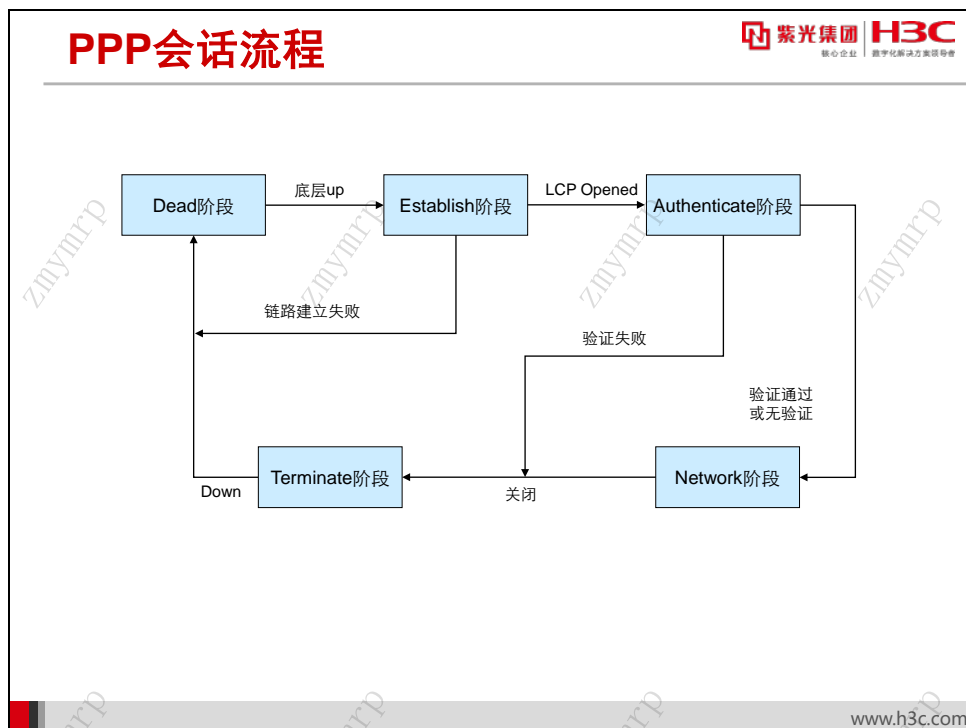
30.3.1 PPP 会话建立的过程



一个完整的 PPP 会话建立大体需要如下三步：

- **链路建立阶段：**在这个阶段，运行 PPP 的设备会发送 LCP 报文来检测链路的可用情况，如果链路可用则会成功建立链路，否则链路建立失败；
- **验证阶段（可选）：**链路成功建立后，根据 PPP 帧中的验证选项来决定是否验证。如果需要验证，则开始 PAP 或者 CHAP 验证，验证成功后进入网络协商阶段；
- **网络层协商阶段：**在这一阶段，运行 PPP 的双方发送 NCP 报文来选择并配置网络层协议，双方会协商彼此使用的网络层协议（例如是 IP 还是 IPX），同时也会选择对应的网络层地址（如 IP 地址或 IPX 地址）。如果协商通过则 PPP 链路建立成功。

30.3.2 PPP 会话流程

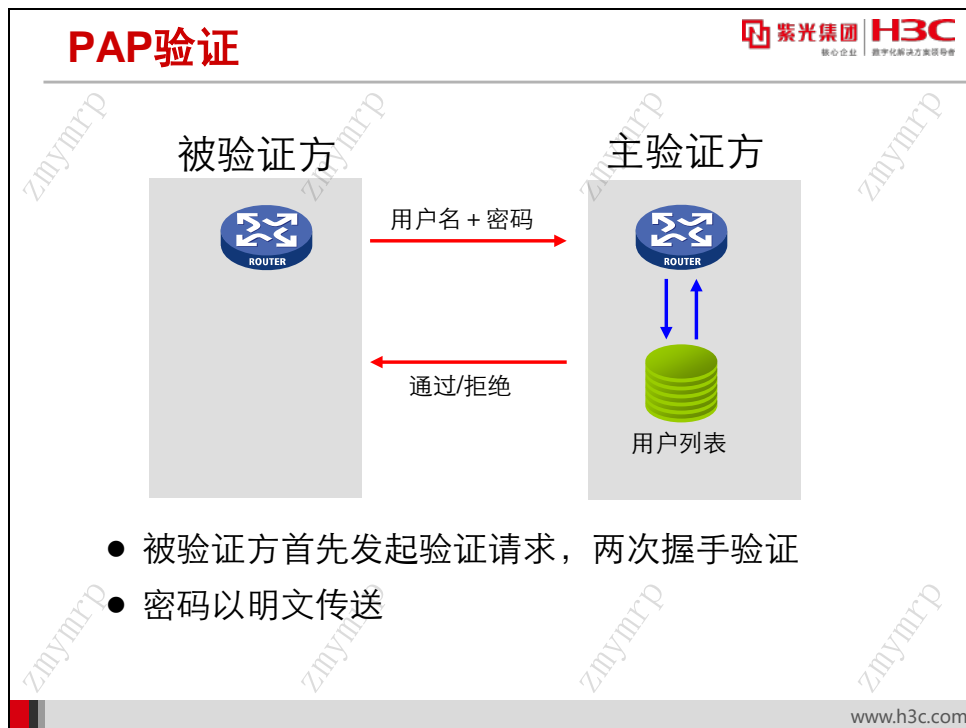


详细的 PPP 会话建立流程如下：

- 当物理层不可用时，PPP 链路处于 dead 阶段，链路必须从这个阶段开始和结束；
- 当物理层可用时进入 Establish 阶段。PPP 链路在 Establish 阶段进行 LCP 协商，协商的内容包括是否采用链路捆绑、使用何种验证方式、最大传输单元等。协商成功后 LCP 进入 Opened 状态，表示底层链路已经建立；
- 如果配置了验证，则进入 Authenticate 阶段，开始 CHAP 或 PAP 验证；
- 如果验证失败则进入 Terminate 阶段，拆除链路，LCP 状态转为 Down；如果验证成功则进入 Network 阶段，由 NCP 协商网络层协议参数，此时 LCP 状态仍为 Opened，而 NCP 状态从 Initial 转到 Request；
- NCP 协商支持 IPCP 协商，IPCP 协商主要包括双方的 IP 地址。通过 NCP 协商来选择和配置一个网络层协议。只有相应的网络层协议协商成功后，该网络层协议才可以通过这条 PPP 链路发送报文；
- PPP 链路将一直保持通信，直至有明确的 LCP 或 NCP 帧来关闭这条链路，或发生了某些外部事件（例如线路被切断）。

30.4 PPP 验证

30.4.1 PAP 验证



PAP（Password Authentication Protocol）验证为两次握手验证，验证的过程如下：

- 被验证方以明文发送用户名和密码到主验证方；
- 主验证方核实用户名和密码。如果此用户合法且密码正确，则会给对端发送 **ACK** 消息，通告对端验证通过，允许进入下一阶段协商；如果用户名或密码不正确，则发送 **NAK** 消息，通告对端验证失败。

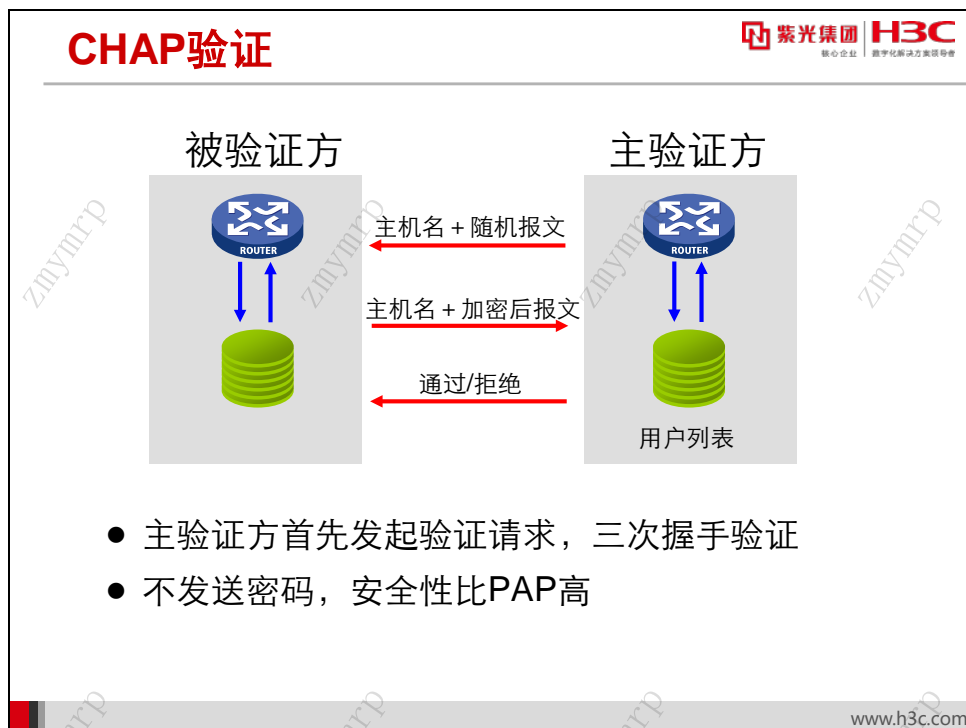
为了确认用户名和密码的正确性，主验证方要么检索本机预先配置的用户列表，要么采用类似 **RADIUS** 的远程验证协议向网络上的验证服务器查询用户名密码信息。

PAP 验证失败后并不会直接将链路关闭。只有当验证失败次数达到一定值时，链路才会被关闭，这样可以防止因误传、线路干扰等因素造成不必要的 **LCP** 重新协商。

PAP 验证可以在一方进行，即由一方验证另一方的身份，也可以进行双向身份验证。双向验证可以理解成两个独立的单向验证过程，即要求通信双方都要通过对方的验证程序，否则无法建立二者之间的链路。

在 **PAP** 验证中，用户名和密码在网络上以明文的方式传递。如果在传输过程中被监听，监听者可以获知用户名和密码，并利用其通过验证，从而可能对网络安全造成威胁。因此，**PAP** 适用于对网络安全要求相对较低的环境。

30.4.2 CHAP 验证



CHAP（Challenge-Handshake Authentication Protocol）验证为三次握手验证，验证过程如下：


- **Challenge:** 主验证方主动发起验证请求，主验证方向被验证方发送一个随机产生的数值，并同时将从本端的用户名一起发送给被验证方；
- **Response:** 被验证方接收到主验证方的验证请求后，检查本地密码。如果本端接口上配置了默认的 CHAP 密码，则被验证方选用此密码；如果没有配置默认的 CHAP 密码，则被验证方根据此报文中主验证方的用户名在本端的用户表中查找该用户对应的密码，并选用找到的密码。随后，被验证方利用 MD5 算法对报文 ID、密码和随机数生成一个摘要，并将此摘要和自己的用户名发回主验证方；
- **Acknowledge or Not Acknowledge:** 主验证方用 MD5 算法对报文 ID、本地保存的被验证方密码和原随机数生成一个摘要，并与收到的摘要值进行比较。如果相同则向被验证方发送 Acknowledge 消息声明验证通过；如果不同则验证不通过，向被验证方发送 Not Acknowledge。

CHAP 单向验证是指一端作为主验证方，另一端作为被验证方。双向验证是单向验证的简单叠加，即两端都是既作为主验证方又作为被验证方。

30.4.3 PAP 与 CHAP 的对比

PPP验证对比

- PAP是两次握手，CHAP是三次握手
- PAP密码以明文方式在链路上发送，缺乏安全性
- CHAP只在网络上传输用户名，而并不传输用户密码
- PAP和CHAP都支持双向身份验证



核心企业 | 数字化转型方案领导者

www.h3c.com

PPP 支持的两种验证方式 PAP 和 CHAP 区别如下：


- PAP 通过两次握手的方式完成验证，而 CHAP 通过三次握手验证远端节点；
- PAP 密码以明文方式在链路上发送，并且当 PPP 链路建立后，被验证方会不停地在链路上反复发送用户名和密码，直到身份验证过程结束，所以不能防止攻击；
- CHAP 只在网络上传输用户名，而并不传输用户密码，因此它的安全性要比 PAP 高。

PAP 和 CHAP 都支持双向身份验证。但由于 CHAP 的安全性优于 PAP，其应用更加广泛。

30.5 配置PPP

30.5.1 PPP 基本配置

PPP基本配置



紫光集团 H3C
核心企业 数字化转型解决方案领导者

- 设置接口报文的封装PPP


```
[H3C-Serial1/0] link-protocol ppp
```
- 设置验证类型


```
[H3C-Serial1/0] ppp authentication-mode { pap | chap }
```
- 设置用户名、密码、服务类型


```
[H3C] local-user user-name class network
[H3C-luser-network-name] password simple
password
[H3C-luser-network-name] service-type ppp
```

www.h3c.com

要在路由器接口上封装 PPP 协议，在接口视图下使用 **link-protocol ppp** 命令。默认情况下，路由器串口链路层协议为 PPP。配置时同样应注意，通信双方的接口都要使用 PPP，否则通信无法进行。

要设置验证类型，选择 PAP 验证或是 CHAP 验证，则在接口视图下配置：

```
[H3C-Serial1/0] ppp authentication-mode { chap | pap }
```

要设置用户名、密码、服务类型等，须在全局视图下配置：

```
[H3C] local-user user-name class network
[H3C-luser-network-name] password { cipher | simple } password
[H3C-luser-network-name] service-type ppp
```

其中若使用 **cipher** 关键字，则表示用户需要直接以密文的方式设置密码；若使用 **simple** 关键字，则表示用户要以明文的方式设置密码，但是在配置文件中仍只显示哈希后的结果。


注意：

配置 **ppp authentication-mode { chap | pap }** 而不加 **domain** 关键字时，默认使用的 **domain** 是系统默认的域 **system**，验证方式是本地验证，地址分配必须使用该域下配置的地址池（通过

display domain 命令可以查看该域的配置)。如果该命令加了 domain, 则必须在对应的 domain 中配置地址池。

30.5.2 配置 PPP PAP 验证

配置PAP验证



- 主验证方：配置用户列表以及验证方式

```
[H3C] local-user user-name class network
[H3C-luser-network-name] password simple
password
[H3C-luser-network-name] service-type ppp
[H3C-Serial1/0] ppp authentication-mode { pap |
chap }
```

- 被验证方：配置PAP用户名

```
[H3C-Serial1/0] ppp pap local-user username
password { cipher | simple } password
```

www.h3c.com

PAP 验证双方分为主验证方和被验证方。在主验证方路由器上配置 PPP PAP 的步骤如下：

第 1 步：设置本地验证对端的方式为 PAP，在接口视图下配置：

```
[H3C-Serial1/0] ppp authentication-mode pap
```

第 2 步：将对端用户名和密码加入本地用户列表并设置服务类型，在全局视图下配置：

```
[H3C] local-user user-name class network
```

```
[H3C-luser-network-name] password { cipher | simple } password
```

```
[H3C-luser-network-name] service-type ppp
```


在被验证方路由器上配置 PPP PAP，须在接口视图下，配置 PAP 验证时被验证方发送的 PAP 用户名和密码：

```
[H3C-Serial1/0] ppp pap local-user username password { cipher | simple }
password
```

被验证方将用户名和密码送给主验证方，主验证方查找本地用户列表，检查被验证方送来的用户名和密码是否完全正确，并根据验证结果确认连接建立或拒绝连接。

30.5.3 配置 PPP CHAP 验证

配置CHAP验证

 紫光集团 | H3C
核心企业 | 数字化转型方案领导者

主验证方配置

- 配置本地验证对端方式为CHAP

```
[H3C-Serial1/0] ppp authentication-mode chap
```

- 配置本地名称

```
[H3C-Serial1/0] ppp chap user username
```

- 将对端用户名和密码加入本地用户列

```
[H3C] local-user user-name class network
[H3C-luser-network-name] password simple password
[H3C-luser-network-name] service-type ppp
```

被验证方配置

- 配置本地名称和密码

```
[H3C-Serial1/0] ppp chap user username
[H3C-Serial1/0] ppp chap password { cipher | simple } password
```

www.h3c.com

CHAP 验证双方同样分为主验证方和被验证方，主验证方首先发起验证。在主验证方路由器上配置 PPP CHAP 的步骤如下：

第 1 步：在接口视图下，配置本地验证对端的方式为 CHAP：

```
[H3C-Serial1/0] ppp authentication-mode chap
```

第 2 步：在接口视图下，配置本地用户名称，用户名是发送到对端设备进行 CHAP 验证时使用的用户名：

```
[H3C-Serial1/0] ppp chap user username
```

第 3 步：将对端用户名和密码加入本地用户列表设置验证类型，在全局视图下配置：

```
[H3C] local-user user-name class network
[H3C-luser-network-name] password { cipher | simple } password
[H3C-luser-network-name] service-type ppp
```

在被验证方路由器上配置 PPP CHAP 的步骤如下：

第 1 步：在接口视图下配置本地名称，用户名是发送到对端设备进行 CHAP 验证时使用的用户名：

```
[H3C-Serial1/0] ppp chap user username
```

第 2 步：配置本地用户密码信息，有两种配置方式。一种方式是在全局视图下向本地用户列表添加用户名和密码：

```
[H3C] local-user user-name class network
```

```
[H3C-luser-network-name] password { cipher | simple } password
```

```
[H3C-luser-network-name] service-type ppp
```

另一种方式是在接口视图下配置默认的 CHAP 密码，这样接口在进行 CHAP 验证时就会使用此密码：

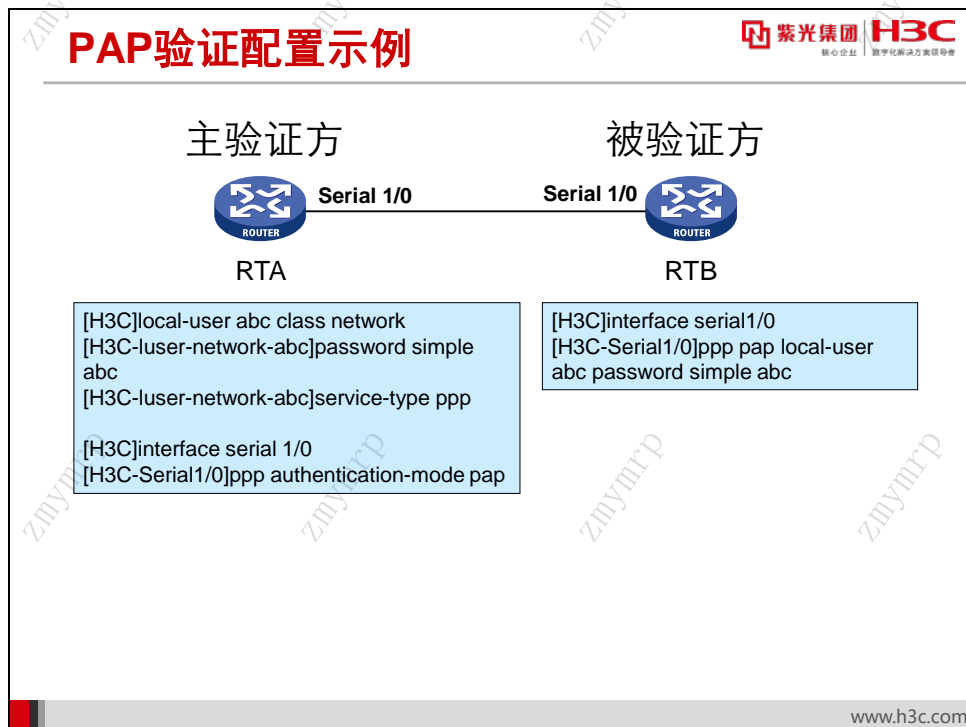
```
[H3C-Serial1/0] ppp chap password { cipher | simple } password
```

注意：

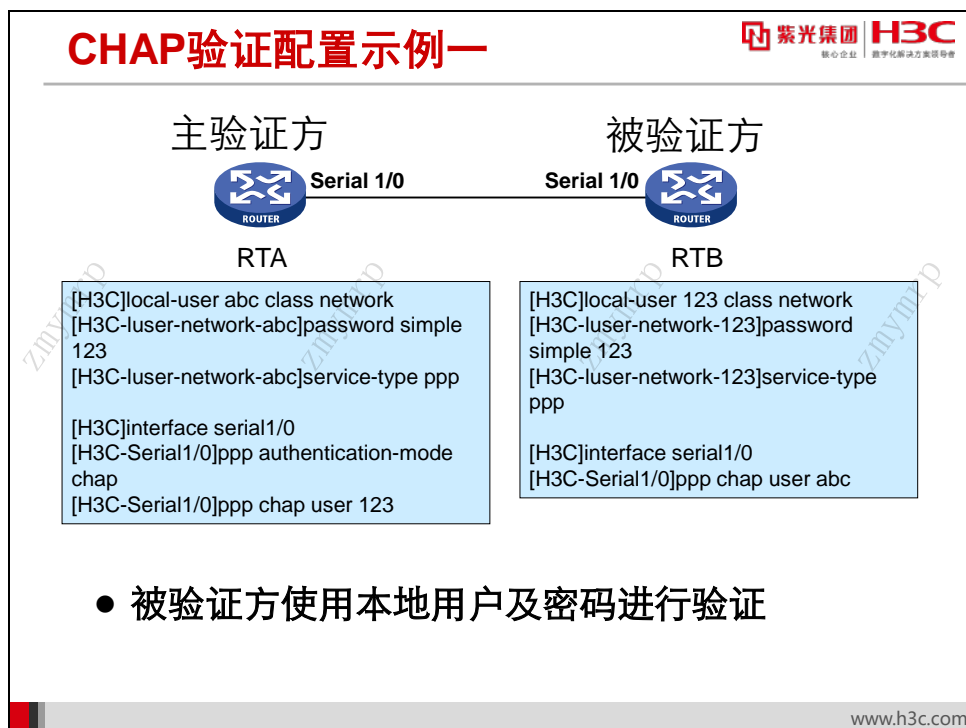
配置 CHAP 验证时，被验证方发送的 *username* 应与主验证方用户列表中的 *username* 相同，而且对应的 *password* 要一致。

当配置被验证方使用默认 CHAP 密码时，在主验证方可以不配置第 2 步。

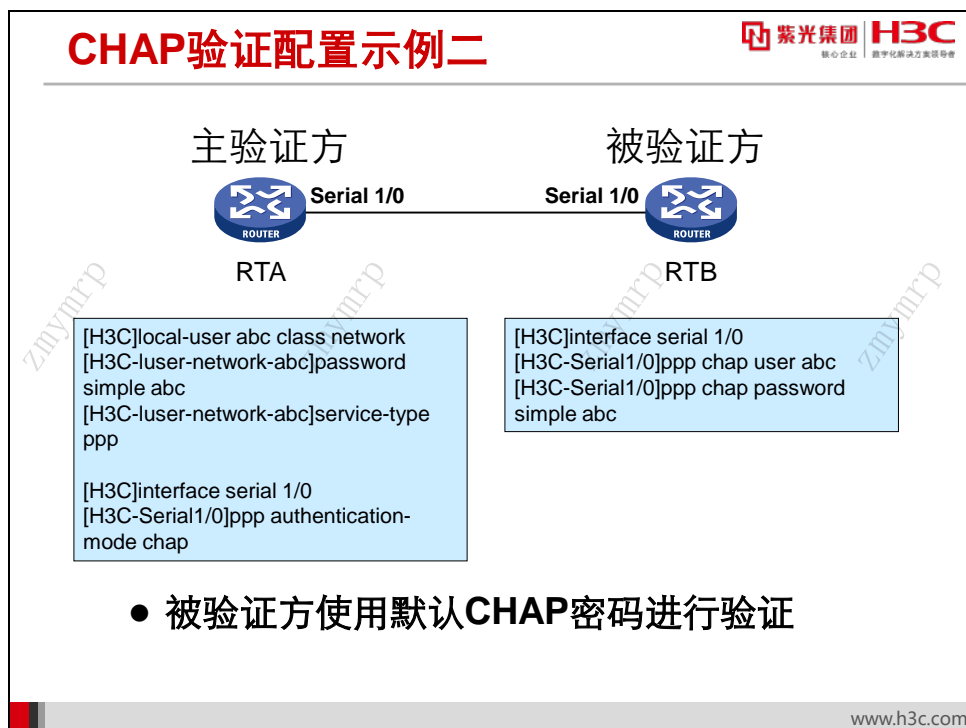
30.5.4 PPP 配置示例



在本例中，RTB 使用用户名 *abc* 密码 *abc* 向 RTA 请求验证。由于双方使用了默认封装 PPP，所以不需要再配置接口的链路协议。



在本例中，RTA 和 RTB 均在接口上配置了 **ppp chap user** 命令，并都配置了本地用户名和密码。其中 RTA 接口上配置的用户名与 RTB 的本地用户名相同，而 RTB 接口上配置的用户名与 RTA 的本地用户名相同，并且双方密码一致。

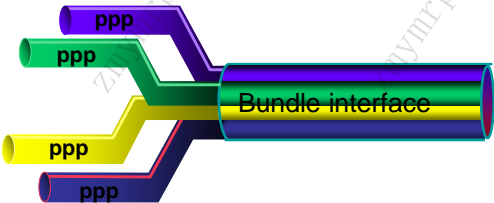


在本例中，RTB 在接口上配置了用户名 abc 和默认 CHAP 密码 abc，此用户名与 RTA 本地用户 abc 名称相同，而此密码与 RTA 本地用户 abc 的密码相同。

30.6 PPP MP

30.6.1 PPP MP 简介

PPP MP简介



- **MP (Multilink PPP)** 将多个PPP链路捆绑后当作一条链路使用
- **MP**可以实现增加带宽、负载分担、链路备份以及降低报文时延的目的

www.h3c.com

PPP 允许将多个链路绑定在一起，形成一个捆绑（Bundle），当作一个逻辑链路（MP 链路）使用。这种技术称为 MP（Multilink PPP，多链路 PPP）。MP 的作用主要有：


- 提供更高的带宽：当一条链路带宽无法满足需要时，可以用多个 PPP 链路捆绑提供更高的带宽；
- 结合 DCC（Dial Control Center，拨号控制中心）实现动态增加或减小带宽：可以在当前使用的链接带宽不足时再自动接通一条链路，而带宽足够时挂断另一条链路；
- 实现多条链路的负载分担：PPP 可以向捆绑在一起的多条链路上平均分配载荷数据；
- 多条链路互为备份：同一 MP 捆绑中的某条链路中断时，整个 MP 捆绑链路仍然可以正常工作；
- 利用分片可以降低报文传输延迟：MP 可以将报文分片并分配在多个链路上，这样在发送较大的分组时可以降低其传输延迟。

MP 能在任何支持 PPP 封装的接口下工作，包括串口、ISDN 的 BRI/PRI 接口等，也包括 PPPoX（PPPoE、PPPoA、PPPoFR 等）这类虚拟接口。配置 MP 时建议尽量将同一类的接口捆绑使用，而不要将不同类的接口捆绑使用。

30.6.2 PPP MP 实现方式

PPP MP实现方式

- 一种是通过配置虚拟模板接口（Virtual-Template, VT）来实现MP
 - 可利用用户名确定捆绑
 - 一个VT接口可派生多个捆绑
- 一种是利用MP-Group接口实现MP
 - Mp-Group是MP专用接口，一个MP-group只能对应一个绑定



核心企业 数字化转型方案领导者

www.h3c.com


MP 的实现主要有两种方式，一种是通过配置虚拟模板接口（Virtual-Template, VT）实现，一种是利用 MP-Group 接口实现。这两种配置方式的区别主要是：

- 虚拟模板接口方式可以与验证相结合，可以根据对端的用户名找到指定的虚拟模板接口，从而利用模板上的配置，创建相应的捆绑，以对应一条 MP 链路。而 MP-Group 则只能在物理接口下配置验证；
- 由一个虚拟模板接口还可以派生出若干个捆绑，每个捆绑对应一条 MP 链路。这样一来，从网络层看来，这若干条 MP 链路会形成一个点对多点的网络拓扑。从这个意义上讲，虚拟模板接口比 MP-Group 接口更加灵活；
- 为区分虚拟模板接口派生出的多个捆绑，需要指定捆绑方式。系统在虚拟模板接口视图下提供了命令 **ppp mp binding-mode** 来指定绑定方式，绑定方式有 **authentication**、**both**、**descriptor** 三种，默认是 **both**。**authentication** 是根据验证用户名捆绑，**descriptor** 是根据终端描述符捆绑（终端标识符是用来唯一标识一台设备的标志，LCP 协商时，会协商出这个选项值），**both** 是要同时参考这两个值捆绑；
- MP-group 接口是 MP 的专用接口，一个 MP-group 只能对应一个绑定。MP-group 不能利用对端的用户名来指定捆绑，也不能派生多个捆绑。但正因为它的简单，导致了这种方式的配置简单，容易理解。

通常情况下推荐以 MP-group 方式配置 MP。

30.6.3 用虚模板方式配置 PPP MP

虚拟模板方式配置 PPP MP



- 创建虚拟模板接口

[H3C] interface virtual-template *number*
- 将物理接口或用户名与虚拟模板接口关联
 - 将物理接口与虚拟模板接口关联

[H3C-Serial1/0] ppp mp virtual-template *number*
 - 将用户名与虚拟模板接口关联

[H3C] ppp mp user *username* bind virtual-template *number*

[H3C-Virtual-Template1] ppp mp binding-mode authentication

[H3C-Serial1/0] ppp mp

www.h3c.com

采用虚拟模板接口配置 MP 时，又可以细分为两种情况：

- 将物理接口与虚拟模板接口直接关联：通过命令 **ppp mp virtual-template** 直接将链路绑定到指定的虚拟模板接口上，这时可以配置验证也可以不配置验证。如果不配置验证，系统将通过对端的终端描述符捆绑出 MP 链路；如果配置了验证，系统将通过用户名和/或对端的终端描述符捆绑出 MP 链路；
- 将用户名与虚拟模板接口关联：根据验证通过后的用户名查找相关联的虚拟模板接口，然后根据用户名和对端终端描述符捆绑出 MP 链路。这种方式需在要绑定的接口下配置 **ppp mp** 及双向验证（CHAP 或 PAP），否则链路协商不通。

在虚拟模板接口下指定捆绑方式时，可以使用用户名、终端标识符或两者同时使用。用户名是指 PPP 链路进行 PAP 或 CHAP 验证时所接收到的对端用户名；终端标识符是指进行 LCP 协商时所接收到的对端终端标识符。系统可以根据接口接收到的用户名或终端标识符来进行 MP 捆绑，以此来区分虚模板接口下的多个 MP 捆绑（对应多条 MP 链路）。

注意：

ppp mp 和 **ppp mp virtual-template** 命令互斥，同一个接口只能配置其中一种方式。

对于需要绑在一起的接口，必须采用同样的配置方式。

实际使用中也可以配置单向验证，即一端直接将物理接口绑定到虚拟模板接口，另一端则通过用户名查找虚拟模板接口。

30.6.4 用 MP-Group 方式配置 PPP MP

MP-Group方式配置PPP MP

 紫光集团  H3C
核心企业 数字化转型方案领导者

- 创建MP-Group接口

```
[H3C] interface Mp-group mp-number
```

- 加入MP-Group组

```
[H3C-Serial1/0] ppp mp Mp-group mp-number
```

www.h3c.com

MP-group 的配置比较简单。首先创建 MP-Group 接口，在全局视图下配置：

```
[H3C] interface Mp-group mp-number
```

然后，将物理接口加入指定的 MP-Group，使接口工作在 MP 方式，在接口视图下配置：

```
[H3C-Serial1/0] ppp mp Mp-group mp-number
```

以上两项配置没有严格的顺序要求，可以先创建 MP-Group 接口，也可以先配置将物理接口加入 MP-Group。

注意：

加入 MP-Group 的接口必须是物理接口，Tunnel 接口等逻辑接口不支持该命令。
如果需要为 MP 配置验证，须在实际物理接口下配置。

30.6.5 PPP MP 配置示例

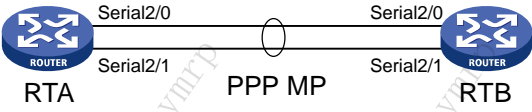
PPP MP配置示例一



 紫光集团 H3C

核心企业 数字化转型方案领导者

- 将物理接口与虚拟模板接口关联



```


[RTA]interface virtual-template 1
[RTA-Virtual-Template1]ip address 1.1.1.1 24
[RTA]interface serial 2/0
[RTA-Serial2/0]ppp mp virtual-template 1
[RTA]interface serial 2/1
[RTA-Serial2/0]ppp mp virtual-template 1

[RTB]interface virtual-template 1
[RTB-Virtual-Template1]ip address 1.1.1.2 24
[RTB]interface serial 2/0
[RTB-Serial2/0]ppp mp virtual-template 1
[RTB]interface serial 2/1
[RTB-Serial2/0]ppp mp virtual-template 1
  
```

www.h3c.com

在本例中，两个物理接口 S2/0 和 S2/1 被直接绑定到 virtual-template 接口上，并形成 MP 捆绑。

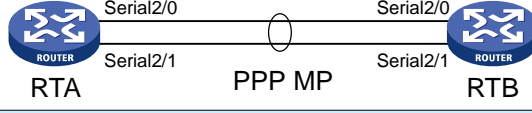
PPP MP配置示例二



 紫光集团 H3C

核心企业 数字化转型方案领导者

- 将用户名与虚拟模板接口关联



```

[RTA]local-user rtb class network
[RTA-luser-network-rtb]password simple rtb
[RTA-luser-network-rtb]service-type ppp
[RTA]ppp mp user rtb bind virtual-template 1
[RTA]interface virtual-template 1
[RTA-Virtual-Template1]ip address 1.1.1.1 24
[RTA-Virtual-Template1]ppp mp binding-mode authentication
[RTA]interface serial 2/0
[RTA-Serial2/0]link-protocol ppp
[RTA-Serial2/0]ppp authentication-mode pap domain system
[RTA-Serial2/0]ppp pap local-user rta password simple rta
[RTA-Serial2/0]ppp mp
[RTA]interface serial 2/1
.....

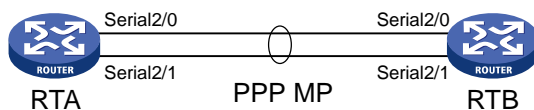
[RTA]domain system
[RTA-isp-system]authentication ppp local
[RTA-isp-system]quit
  
```

www.h3c.com

PPP MP配置示例二（续）

紫光集团 H3C
核心企业 数字化转型方案领导者

● 将用户名与虚拟模板接口关联



```
[RTB]local-user rta class network
[RTB-luser-network-rta]password simple rta
[RTB-luser-network-rta]service-type ppp
[RTB]ppp mp user rta bind virtual-template 1
[RTB]interface virtual-template 1
[RTB-Virtual-Template1]ip address 1.1.1.2 24
[RTB-Virtual-Template1]ppp mp binding-mode authentication
[RTB]interface serial 2/0
[RTB-Serial2/0]link-protocol ppp
[RTB-Serial2/0]ppp authentication-mode pap domain system
[RTB-Serial2/0]ppp pap local-user rtb password simple rtb
[RTB-Serial2/0]ppp mp
[RTB]interface serial 2/1
.....

[RTB]domain system
[RTB-isp-system]authentication ppp local
[RTB-isp-system]quit
```

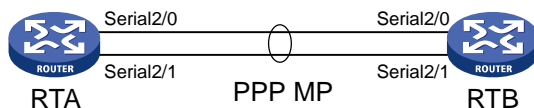
www.h3c.com

在本例中，RTA 和 RTB 双方均采用用户名来识别物理链路是否属于 MP 链路，并据此形成 MP 捆绑。

PPP MP配置示例三

紫光集团 H3C
核心企业 数字化转型方案领导者

● MP-Group方式配置



```
[RTA]interface mp-group 1
[RTA-MP-group1]ip address 1.1.1.1 24
[RTA]interface Serial2/0
[RTA-Serial2/0]ppp mp mp-group 1
[RTA]interface Serial2/1
[RTA-Serial2/1]ppp mp mp-group 1
```


```
[RTB]interface mp-group 1
[RTB-MP-group1]ip address 1.1.1.2 24
[RTB]interface Serial2/0
[RTB-Serial2/0]ppp mp mp-group 1
[RTB]interface Serial2/1
[RTB-Serial2/1]ppp mp mp-group 1
```

www.h3c.com

在本例中，两个物理接口 S2/0 和 S2/1 被直接绑定到 mp-group 接口上，并形成 MP 捆绑。

30.7 PPP协议显示与调试

PPP显示与调试



紫光集团 H3C
核心企业 数字化转型方案领导者

- 显示接口的PPP配置和运行状态
`[H3C] display interface interface-name`
- 查看已创建的MP-Group接口的状态信息
`[H3C] display interface Mp-group [mp-number]`
- 显示指定MP接口的接口信息和统计信息
`[H3C] display ppp mp [interface interface-type interface-number]`
- 显示PPP验证的本地用户
`[H3C] display users`
- 查看PPP的调试信息
`<H3C> debugging ppp all [interface interface-type interface-number]`

www.h3c.com

上图列出了常用的 PPP 的显示与调试命令,其中使用最频繁的命令为 **display interface**,用来显示接口的 PPP 配置和运行状态。

用display interface命令显示接口信息

紫光集团 H3C
核心企业 数字化转型方案领导者

```
[H3C]display interface Serial 5/0
Serial5/0
Current state: UP
Line protocol state: UP
Description: Serial5/0 Interface
Bandwidth: 64kbps
Maximum Transmit Unit: 1500
Hold timer: 10 seconds
Internet Address is 1.1.1.1/24 Primary
Link layer protocol: PPP
LCP: opened, IPCP: opened
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
Last clearing of counters: Never
Physical layer: synchronous, Virtual baudrate: 64000 bps
Last 300 seconds input rate: 0.00 bytes/sec, 0 bits/sec, 0.00 packets/sec
Last 300 seconds output rate: 0.00 bytes/sec, 0 bits/sec, 0.00 packets/sec
Input:
  24 packets, 678 bytes
  0 broadcasts, 0 multicasts
  0 errors, 0 runts, 0 giants
  0 CRC, 0 align errors, 0 overruns
  0 aborts, 0 no buffers, 0 frame errors
Output:
  24 packets, 678 bytes
  0 errors, 0 underruns, 0 collisions
  0 deferred
DCD: UP, DTR: UP, DSR: UP, RTS: UP, CTS: UP
```

物理接口UP
PPP协议UP

LCP和IPCP状态
为opened

← Current state: UP

← Line protocol state: UP

← LCP: opened, IPCP: opened

www.h3c.com

通过 **display interface** 命令可以显示具体接口信息。当接口物理状态和协议状态都为 UP 时候，可以看到 LCP 状态为 opened，IPCP 状态也为 opened，说明 PPP 工作正常。

用debugging ppp all命令调试PPP

紫光集团 H3C
核心企业 数字化转型方案领导者

```
<H3C>debugging ppp all
*Oct 20 12:55:03:685 2013 H3C PPP/7/EXTERNAL_EVENT_0:
PPP External Event:
  Serial5/0: PPP daemon receive PPP_IFMSG_UP event!
%Oct 20 12:55:03:686 2013 H3C IFNET/3/PHY_UPDOWN: Physical state on the interface Serial5/0 changed to up.
*Oct 20 12:55:03:685 2013 H3C PPP/7/EXTERNAL_EVENT_0:
PPP External Event:
  Serial5/0: PPP daemon enter lcp establish flow!
*Oct 20 12:55:03:685 2013 H3C PPP/7/FSM_EVENT_0:
PPP Event:
  Serial5/0 LCP Open Event
  State initial
*Oct 20 12:55:03:686 2013 H3C PPP/7/FSM_STATE_0:
PPP State Change:
  Serial5/0 LCP: initial --> starting
*Oct 20 12:55:03:686 2013 H3C PPP/7/FSM_EVENT_0:
PPP Event:
  Serial5/0 LCP Lower Up Event
  State starting
*Oct 20 12:55:03:687 2013 H3C PPP/7/FSM_STATE_0:
PPP State Change:
  Serial5/0 LCP: starting --> reqsent
*Oct 20 12:55:03:687 2013 H3C PPP/7/FSM_PACKET_0:
PPP Packet:
  Serial5/0 Output LCP(c021) Packet, PktLen 14
  Current State reqsent, code ConfReq(01), id 3, len 10
  MagicNumber(5), len 6, val 40 06 90 7c
*Oct 20 12:55:04:641 2013 H3C PPP/7/EXTERNAL_EVENT:
PPP External Event:
  Serial5/0 deliver packet to user space success
```

www.h3c.com

通过 **debugging ppp all** 命令可以开启整个 PPP 链路建立过程中的所有调试信息。上图只列出了部分调试信息供参考。其中 **PPP event** 和 **PPP state change** 显示了 PPP 链路建立过程中的所有事件和状态的改变。

30.8 本章总结

本章总结

- PPP协议概念
- PPP协议特点及组成
- PPP协议会话建立流程
- PPP协议两种验证方式对比
- PPP MP的概念以及实现
- PPP协议配置和调试

第31章 配置 3G

随着无线通信网的快速发展，3G 已经成为了人们日常生活中最常使用的通信技术之一。3G 系统采用了智能信号处理技术，不仅能够支持更高速率的移动多媒体业务，还能提供更高的频谱效率和服务质量，实现了语音业务为主的多媒体数据通信，具有更强的多媒体业务服务能力和极大的通信容量。

31.1 本章目标

课程目标

● 学习完本课程，您应该能够：

- 掌握3G的概念
- 掌握3G的标准
- 了解3G的接入方式
- 掌握3G的配置
- 熟悉3G的维护命令




www.h3c.com

31.2 3G技术概述

31.2.1 3G 基本概念

3G基本概念



紫光集团 H3C
核心企业 数字化转型解决方案领导者

- **3G最早是在1985年提出，于1996年正式更名为IMT-2000**
- **3G移动通信技术标准中，国际上目前最具代表性的有三种：WCDMA、TD-SCDMA、CDMA2000**


www.h3c.com

3G（3rd Generation，第三代移动通信技术）最早是由国际电信联盟（ITU）在 1985 年提出，考虑到该系统将于 2000 年左右进入商用市场，工作的频段在 2000MHz，且最高业务速率为 2000Kbps，故于 1996 年正式更名为 IMT-2000。

IMT-2000 目前共有四种技术标准：WCDMA、TD-SCDMA、CDMA2000、WiMAX。前三种技术标准是基于蜂窝移动通信系统，WiMAX 是基于无线宽带接入系统。

3G技术特点

- 全球统一频段
- 全球统一制式
- 全球无缝漫游能力
- 高频谱效率
- 支持移动多媒体业务



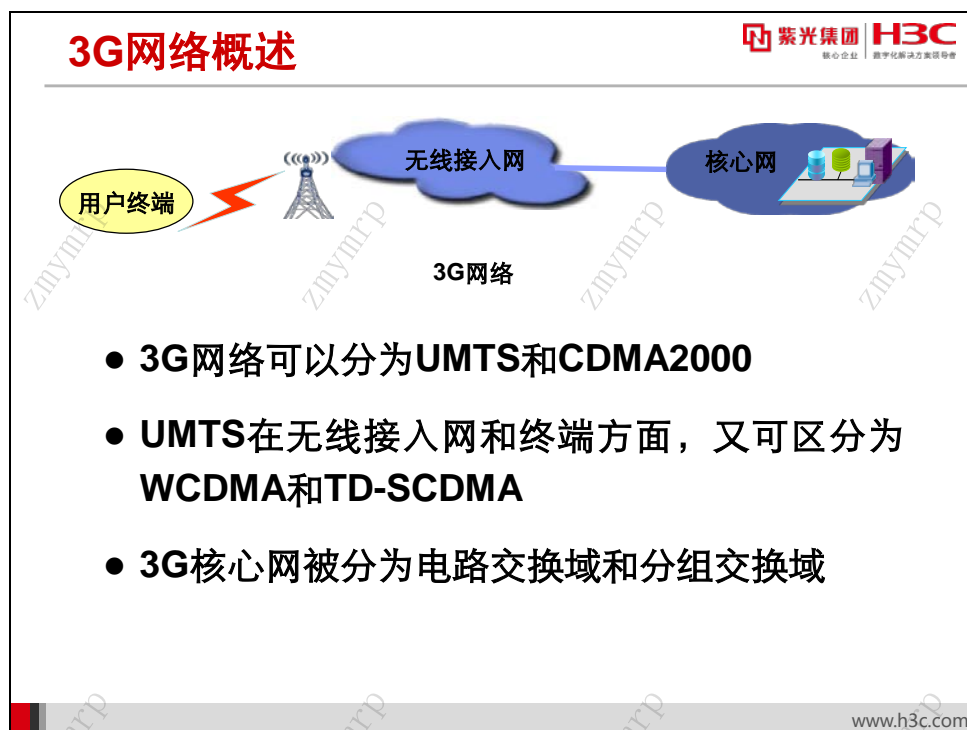
紫光集团 H3C
核心企业 数字化转型集团领导者

www.h3c.com

3G 技术特征为全球统一频段、全球统一制式、全球无缝漫游能力、高频谱效率、支持移动多媒体业务：

- 全球统一频段：欧洲、中日韩和绝大多数国家目前规划的频段和 ITU 基本一致，与 2G 相比，频段的统一向前迈进了一大步；
- 全球统一制式：虽然 ITU 通过了 5 个标准，并未完全统一。但是国际上主流的 FDD 标准只有 WCDMA 和 CDMA2000，以及中国的 TDD 标准 TD-SCDMA，相较于 2G 技术有了明显的统一趋势；
- 全球无缝漫游能力：全球技术标准的趋同，使得无缝漫游能力也得到了进一步的发展；
- 高频谱效率：相较于 2G 技术，各个 3G 标准的频谱效率均有了数倍的提升；
- 支持移动多媒体业务：3G 能够提供个性化的多媒体业务，其数据速率也有了很大幅度的提高。

31.2.2 3G 网络概述



除 WiMAX 外，3G 网络可以分为 UMTS 和 CDMA2000，UMTS 在无线接入网和终端方面又可以区分为 WCDMA 和 TD-SCDMA。

3G 的核心网被分为电路交换域和分组交换域。电路交换域的成员包括移动服务中心、归属位置寄存器以及网关，它们在 UMTS 和 CDMA2000 标准中是相同的。而分组交换域的成员在这两种标准中是不同的。

31.3 3G标准

31.3.1 3G 技术标准

3G技术标准			紫光集团 H3C 核心企业 数字化转型方案领导者
3G标准	标准描述	中国ISP	
WCDMA	由标准化组织3GPP所制定	中国联通	
CDMA-2000	由美国高通北美公司为主导提出，摩托罗拉、Lucent和韩国三星都有参与	中国电信	
TD-SCDMA	该标准是由中国大陆独自制定的3G标准	中国移动	

目前主流的 3G 技术标准主要分为以下三种：

- **WCDMA**：宽频分码多重存取，由标准化组织 3GPP 所制定。其支持者主要是以 GSM 系统为主的欧洲厂商。这套系统能够架设在现有的 GSM 网络上，对于系统提供商而言可以较轻易地过渡，由于 GSM 技术在世界数字移动电话领域所占的比例已经超过 70%，因此 WCDMA 具有先天的市场优势；
- **CDMA-2000**：由美国高通北美公司为主导提出，摩托罗拉、Lucent 和后来加入的韩国三星都有参与，韩国现在成为该标准的主导者。这套系统可以从原有的 CDMA1x 结构直接升级到 3G，建设成本低廉。目前使用 CDMA 的地区只有日、韩和北美，所以 CDMA2000 的支持者不如 WCDMA 多。不过 CDMA2000 的研发技术却是目前各标准中进度最快的；
- **TD-SCDMA**：该标准是由中国大陆独自制定的 3G 标准。该标准将智能无线、同步 CDMA 和软件无线电等当今国际领先技术融于其中。另外，由于中国国内庞大的市场，该标准受到各大主要电信设备厂商的重视，全球一半以上的设备厂商都宣布可以支持 TD-SCDMA 标准。

31.3.2 3G 频段划分

3G频段划分		
<div><div>紫光集团</div><div>H3C</div><div>核心企业 数字化转型方案领导者</div></div>		
说明项	2G	3G
中国移动	GSM/GPRS/EDGE 890~908 MHz（下行），935~953MHz（上行）	TD-SCDMA/HSDPA/HSUPA（TDD）： • 核心频段：1880~1900MHz（A频段） 2010~2025MHz（B频段） • 补充频率：2300~2400MHz（C频段）
中国联通	GSM/GPRS 909~915 MHz（下行），954~960 MHz（上行）	WCDMA/HSDPA/HSUPA（FDD）： • 核心频段：1920~1980MHz（上行）， 2110~2170MHz（下行） • 补充频率：1755~1785MHz（上行）， 1850~1880MHz（下行）
中国电信	CDMA1X 核心频段：825~835MHz（上行）， 870~880MHz（下行）	CDMA2000 EVDO（FDD）： • 核心频段：825~835MHz（上行）， 870~880MHz（下行） • 补充频率：885~915MHz（上行）， 930~960MHz（下行）

www.h3c.com

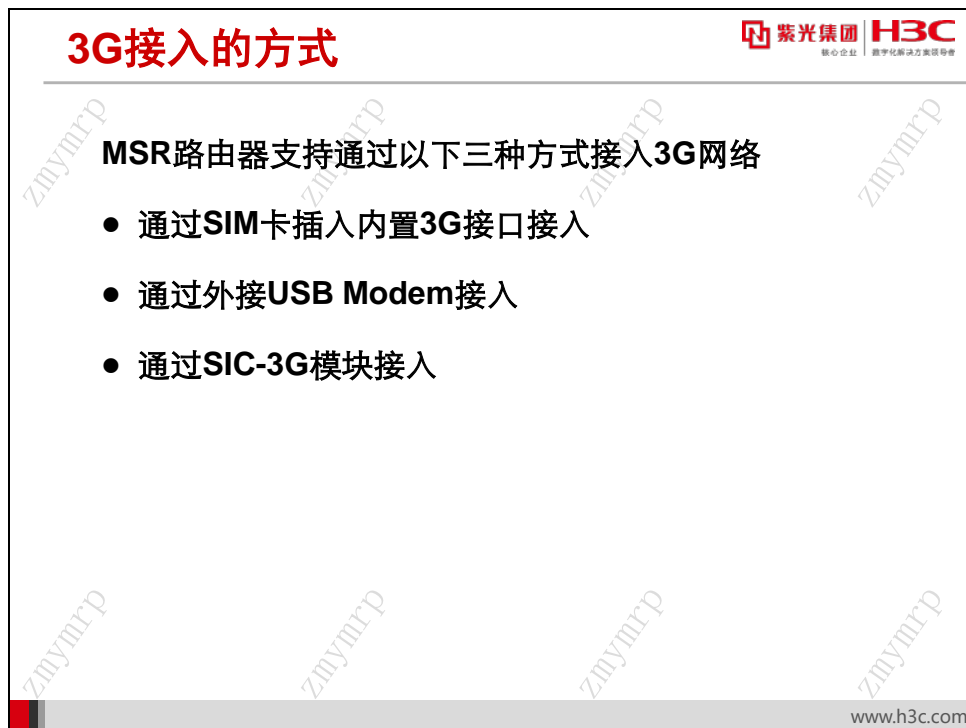
中国移动采用的 TDD（时分双工）技术，其上行和下行的通信使用同一频率信道的不同时间隙，用时间来分离接收和传送信道。

中国联通的 FDD 技术是频分双工，在分离的两个对称频率信道上，系统进行接收和发送。

中国电信获得的 3G 频段是 1920-1935MHz，但实际上电信 3G 重用了 CDMA1X 频段，暂未使用分配的频段。

31.4 3G接入方式

31.4.1 3G 接入方式



路由器的 3G 无线通信方案是指设备通过外接方式，提供上行 3G 无线通信或作为有线通信链路的备份或补充的一种通信应用方式。

MSR 路由器支持三种 3G 接入方式，用户可以通过插入 SIM 卡、外接 USB Modem 或插入 SIC-3G 模块来完成 3G 拨号功能。如 MSR 930-GU 系列路由器内置了 3G Modem，插入联通 SIM 卡即可进行 3G 拨号。

这种无线通信方案的主要特点和优势是：

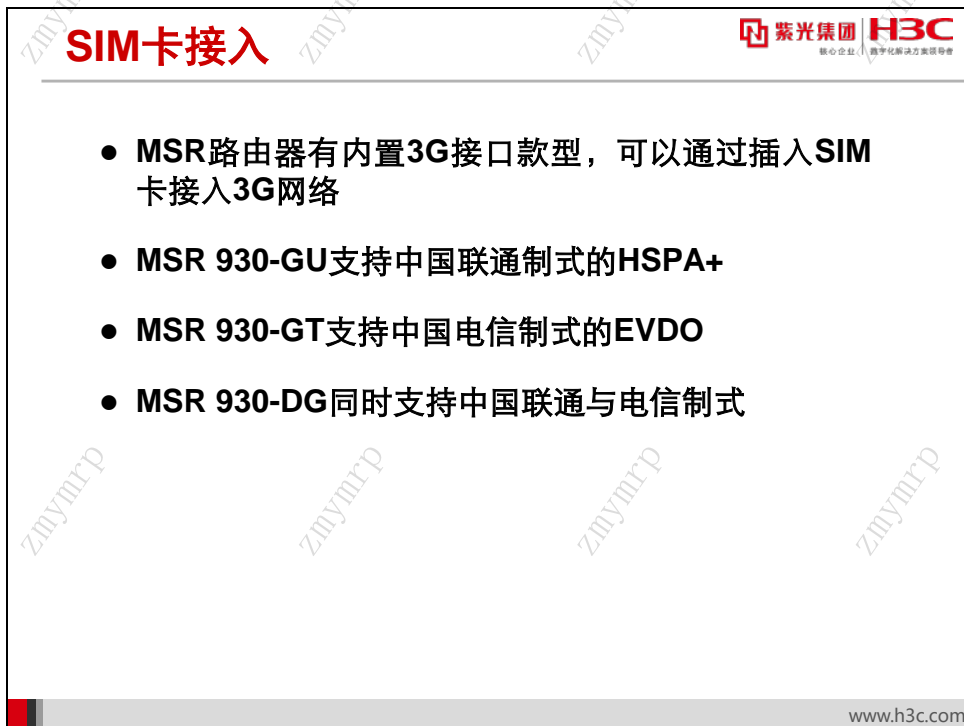
- 3G 无线通信的带宽得到了大幅提升，可用性大大增强，为其普及和推广应用创造了有利条件；
- 3G 无线通信很好地满足了不方便获取有线链路资源或需要移动通信的应用场景的通信需求，增强了路由器或网关设备的通信适应能力；
- 3G 无线通信覆盖的网络是一个公网环境，利用路由器或网关设备强大的网络安全和数据加密功能，完全可以解除无线通信应用的安全隐患；
- 3G 无线通信接口在路由器和网关上封装出来的是标准 IP 接口，与其它有线接口没有任何功能和业务上的差异，这就保证了 3G 无线通信的功能完善性。

注意：

对于没有 SIC 插槽的 MSR 路由器无法支持 3G 无线模块。

2 个 USB 接口的 MSR 路由器，仅在 0 端口支持 USB 3G Modem。

31.4.2 SIM 卡接入



SIM卡接入

- **MSR路由器有内置3G接口款型，可以通过插入SIM卡接入3G网络**
- **MSR 930-GU支持中国联通制式的HSPA+**
- **MSR 930-GT支持中国电信制式的EVDO**
- **MSR 930-DG同时支持中国联通与电信制式**

www.h3c.com

MSR 930 路由器有多个款型支持内置 3G 接口，可以通过插入 SIM 卡来接入 3G 网络。

其中的 MSR 930-GU 内置的 3G 接口支持中国联通制式的 HSPA+。G 表示 3G，U 是指 Unicom（联通），GU 就标明这是支持联通 3G 的 MSR 930 款型。

MSR 930-GT 也类似，内置了一个支持中国电信 EVDO 制式的 3G 接口，T 是指 Telecommunication（电信），GT 标明这款设备支持电信 3G。

MSR 930-DG 内置了两个 SIM 卡槽，同时支持联通和电信的 3G 接入，其中 D 是指 Double，DG 标明这是一款支持双 3G 的设备，两条 3G 链路可以作为主备链路存在。

31.4.3 USB Modem 接入



MSR 路由器的 USB 接口可以插入 USB 3G Modem，以此实现 3G 拨号功能。

USB 3G Modem 可以外接到设备的 USB 接口上。Modem 插入后，待系统启动会自动生成 Cellular0/0 接口，可以将该接口作为路由器的 WAN 接口使用。在 USB 3G Modem 的使用中，如果需要热拔出 USB 3G Modem，需要先 shutdown USB 3G Modem 对应的 Cellular0/0 接口。

由于目前 Modem 的实现标准不统一，因此导致不同标准的 Modem 需要对应开发不同的 USB 驱动接口，随着版本更新将支持更多类型 3G Modem，具体以版本说明书更新为准。

31.4.4 SIC-3G 模块接入

SIC-3G模块接入

```
graph LR; MSR[MSR主机] --- GE1[GE]; MSR --- GE2[GE]; GE1 --- CPU[CPU]; GE2 --- CPU; CPU --- USB[USB]; CPU --- Modem[Modem]; USB -.-> Internet((Internet));
```

● **MSR路由器可以插入SIC-3G单板，使路由器接入3G网络**

单板显示名称	制式	中国运营商
SIC-3G-HSPA	WCDMA	中国联通
SIC-3G-TD	TD-SCDMA	中国移动
SIC-3G-CDMA	CDMA2000	中国电信

紫光集团 H3C

核心企业 数字化转型方案领导者

www.h3c.com


MSR 路由器还支持通过配置 SIC-3G 模块来实现 3G 接入的功能。

具体模块的选配，要根据不同的运营商来区分。

31.5 配置3G

31.5.1 3G 基本配置

3G基本配置



紫光集团 H3C
核心企业 数字化转型方案领导者

- 配置接口报文封装ppp

[H3C-Cellular-number] link-protocol PPP
- 配置接口工作在协议模式

[H3C-Cellular-number] async mode protocol
- 配置chap认证时的用户名密码

[H3C-Cellular-number] ppp chap user *username*
[H3C-Cellular-number] ppp chap password simple *password*

www.h3c.com

配置 3G 接入的 cellular 接口时，要求封装为 PPP 协议。

在接口视图下配置：

[H3C-Cellular-number] link-protocol ppp

配置接口工作在协议模式，需在接口视图下配置：

[H3C-Cellular-number] async mode protocol

若运营商处需要对接入用户进行 chap 认证，要在接口视图下分别配置用户名和密码：

[H3C-Cellular-number] ppp chap user *username*

[H3C-Cellular-number] ppp chap password simple *password*

3G基本配置



- 配置pap认证时的用户名密码

```
[H3C-Cellular-number] ppp pap local-user
username password simple password
```

- 配置本端接口接收PPP协商产生的由对端分配的地址

```
[H3C-Cellular-number] ip address ppp-negotiate
```

- 配置使能轮询DCC

```
[H3C-Cellular-number] dialer enable-circular
```

www.h3c.com

若运营商对接入用户进行 pap 认证，要在接口视图下配置用户名和密码：

```
[H3C-Cellular-number] ppp pap local-user username password simple
password
```

在进行 3G 拨号时，本端的地址通常根据运营商的分配来确定。本端接口根据 PPP 协商，使用对端分配的地址的命令为：

```
[H3C-Cellular-number] ip address ppp-negotiate
```

设备在进行 3G 拨号时，必须要在接口下使能轮询 DCC 功能：

```
[H3C-Cellular-number] dialer enable-circular
```

3G 基本配置



- 配置拨号访问组及拨号访问控制条件

```
[H3C] dialer-rule group-number { protocol-name
{ deny | permit } | acl { acl-number | name acl-
name } }
```

- 将接口加入拨号访问组

```
[H3C-Cellular-number] dialer-group group-number
```

- 配置允许 Modem 呼入和呼出

```
[H3C-ui-tty12] modem both
```

www.h3c.com

设备拨号时，要设置拨号访问组的拨号控制列表，以此来控制拨号访问组的 DCC 呼叫发生条件：

```
[H3C] dialer-rule group-number { protocol-name { deny | permit } | acl
{ acl-number | name acl-name } }
```

之后将接口加入到拨号访问组中：

```
[H3C-Cellular-number] dialer-group group-number
```

先使用 display user-interface 命令，查看 cellular 接口对应的 TTY 号，然后进入相应的视图下，配置 Modem 的呼入/呼出功能。当 cellular 接口对应 TTY 12 时，配置如下：

```
[H3C-ui-tty12] modem both
```

3G基本配置



● 配置参数描述模板APN

```
[H3C-Cellular-number] profile create profile-number  
{ dynamic | static apn } authentication-mode  
authentication [ user username ] [ password  
password ]
```

- 对于WCDMA和TD-SCDMA必须配置APN，该命令被下发到Modem中，配置无法查看
- 对于更换了网络或第一次使用的Modem，必须配置

www.h3c.com

对于联通和移动的 3G 接入用户来说，必须要进行 APN 的配置。

配置参数描述模板 APN 的命令为：

```
[H3C-Cellular-number] profile create profile-number { dynamic | static apn }  
authentication-mode authentication [ user username ] [ password password ]
```

由于该命令被直接写入到 Modem 硬件中，因此无法在设备的配置文件中保存或查看。

31.5.2 3G 配置示例

3G配置示例

1

```
[H3C]interface Cellular0/0
[H3C-Cellular0/0]ip address ppp-negotiate
[H3C-Cellular0/0]nat outbound
[H3C]ip route-static 0.0.0.0 0.0.0.0 Cellular0/0
```

2

```
[H3C-Cellular0/0]async mode protocol
[H3C-Cellular0/0]link-protocol ppp
[H3C-Cellular0/0]ppp chap user card
[H3C-Cellular0/0]ppp chap password simple card
[H3C-Cellular0/0]ppp pap local-user card password simple card
```

认证方式由运营商提供
电信默认为card/card

3

```
[H3C]dialer-rule 1 ip permit
[H3C-Cellular0/0]dialer enable-circular
[H3C-Cellular0/0]dialer-group 1
[H3C-Cellular0/0]dialer timer idle 60
[H3C-Cellular0/0]dialer number #777
```

拨号串
联通移动为*99#
电信为#777

www.h3c.com

上图是一个典型的 3G 拨号配置案例。在本例中，拨号口为 Cellular0/0，地址由运营商分配获得。在设备上配置一条默认路由，从拨号口转发报文。

在配置 3G 拨号时，需要配置链路协议为 PPP，且 cellular 接口工作在协议模式。具体的用户认证方式由运营商确定，在使用时需要咨询运营商。电信默认的用户名密码为 card/card，配置方式见示例。

第三部分主要配置了拨号规则。要先创建拨号访问组，配置访问组的拨号控制列表，定义触发拨号的流量，并将其与接口 Cellular0/0 相关联。示例中配置链路空闲时间为 60 秒，即在 60 秒内若没有感兴趣报文在链路上传送，则 DCC 自动挂断该链路。设备默认的链路空闲时间为 120 秒，若配置为 0 则表示在链路建立后，永不挂断。最后是要配置拨号串，联通和移动的拨号串为*99#，电信为#777。

3G配置示例（续）

```
[H3C]display user-interface
```

Idx	Type	Tx/Rx	Modem	Privi	Auth	Int
12	TTY 12	9600	-	0	N	Cellular0/0
80	AUX 0	9600	-	3	N	-
81	VTY 0		-	0	P	-
82	VTY 1		-	0	P	-
83	VTY 2		-	0	P	-
84	VTY 3		-	0	P	-
85	VTY 4		-	0	P	-

← 查看Cellular接口对应的TTY，此处为TTY 12


```
[H3C]user-interface tty 12
[H3C-ui-tty12]modem both
```

www.h3c.com

通过查看用户接口，确定 3G 拨号口 Cellular0/0 对应的 TTY 号，之后在该对应的用户接口下配置 Modem 允许呼入和呼出。

31.6 3G 的显示与调试

3G 的显示与调试



紫光集团 H3C
核心企业 数字化转型方案领导者

- 显示 3G Modem 的呼叫连接信息

```
<H3C> display cellular interface-number all
```

- 清除指定接口的统计信息

```
<H3C> reset counters interface [ cellular [ interface-number ] ]
```


- 查看 3G 拨号过程的调试信息

```
<H3C> debugging ppp all
```

www.h3c.com

这是几个常用的 3G 显示与调试的命令，其中使用最频繁的命令为 **display cellular interface-number all**，用来显示 3G 模块当前的详细状态信息。

3G状态信息



紫光集团 H3C
核心企业 数字化转型方案领导者

```

<H3C>display cellular 0/0 all
Modem State:
Hardware Information
=====
Model = E176G
Modem Firmware Version = 11.124.05.04.112
Hardware Version = CD25TCPV
International Mobile Subscriber Identity (IMSI) = 460016004345081
International Mobile Equipment Identity (IMEI) = 357267023325644
Factory Serial Number (FSN) = GB5TAA1981305641
Modem Status = Online
Profile Information
=====
Profile 1 = ACTIVE
-----
PDP Type = IPv4, Header Compression = OFF
Data Compression = OFF
Access Point Name (APN) = 3gnet
Packet Session Status = Active
* - Default profile

```

← 3G Modem处于
上电状态

← 3G Modem的PDP设置状
态为已经配置参数模板

← APN接入点名称

www.h3c.com

通过 **display cellular 0/0 all** 命令可以显示接口的详细信息。

Model 字段描述当前 Modem 的型号，实例中的 Modem 为 **E176G**。在设备的使用中，需要关注 **Modem Status** 项，必须该项为“Online”时 3G 拨号功能才可以正常使用。若该项为“Offline”则说明设备的 3G Modem 处于下电或省电状态，3G 拨号功能不可用。

如果用户要接入联通（WCDMA）或移动（TD-SCDMA）的 3G 网络，则首先要配置 APN。APN 会通过 Profile 配置直接下发到 Modem 中，无法在命令行查看当前配置看到该信息。

USB Modem 一般可保存 16 个 Profile，MSR 路由器只能配置和管理其中的第一个。

紫光集团H3C
核心企业 数字化转型决策领导者

3G状态信息（续）

Network Information
=====

Current Service Status = Service available
Current Service = Combined
Packet Service = Attached
Packet Session Status = Active
Current Roaming Status = Home
Network Selection Mode = Manual
Network Connection Mode = Auto
Current Network Connection = HSDPA and HSUPA
Mobile Country Code (MCC) = 460
Mobile Network Code (MNC) = 01
Location Area Code (LAC) = 248
Cell ID = 20021
Downstream Bandwidth = 7200000 bps
Radio Information
=====

Current Band = ANY
Current RSSI = -70 dBm
Modem Security Information
=====

PIN Verification = Disabled
PIN Status = Ready
Number of Retries remaining = 3
SIM Status = OK

3G Modem的服务
状态为服务有效

当前接入的网络

当前信号质量, -70dBm
(-110dBm~-51dBm)

SIM卡状态正常

www.h3c.com

设备上显示的 3G Modem 的服务状态主要有以下几种：“Service available”表示当前有可用的服务；“Emergency”表示服务受限；“No service”表示无服务；“Low power”表示省电模式。设备在正常使用过程中，显示的服务状态应该为 Service available。


网络连接状态显示当前接入的网络类型，若该项为“No Service”或是“Unknown”则为异常状态。上述示例中显示设备当前接入了 HSDPA 和 HSUPA 网络。

信号强度 RSSI 描述当前接入网络的信号状态。实例中当前信号为-70dBm，属于较好的状态。正常使用中，要求信号在-110dBm~-51dBm 的范围内，通常在信号大于-75dBm 时用户体验较好。

SIM 卡状态由 SIM Status 项来描述，只有该项显示为“OK”时，设备的 3G 拨号功能才可以正常使用。“Network Reject”表示当前 SIM 卡被拒绝接入网络，需要找运营商确认具体的问题原因；“Not Insert”则说明未插入 SIM 卡，接口也无法进行正常的拨号。

- 590 -

31.7 本章总结



本章总结

- 3G概述
- 3G标准
- 3G接入方式介绍
- 3G的配置方法
- 3G的显示与调试

www.h3c.com

第32章 配置 WLAN

随着宽带业务的不断发展，人们对于移动宽带业务的需求也越来越大。WLAN（Wireless Local Area Network，无线局域网）作为一种低成本解决方案，在各行各业逐渐受到人们的重视。无线局域网络具有无需布线，安装快捷，维护简单等特点。它可以在有线网络难以部署的情况下发挥巨大作用。本章将介绍无线局域网的基础知识。

32.1 本章目标

课程目标

○ 学习完本课程，您应该能够：

- 了解WLAN的优势与技术标准
- 熟悉WLAN网络的构成
- 掌握无线控制器和FIT AP组网的特点
- 掌握WLAN的基本配置方法



www.h3c.com

32.2 WLAN的优势与技术标准

32.2.1 WLAN 的优势

无线让网络使用更自由

凡是自由空间均可连接网络，不受限于线缆和端口位置。



办公大楼 候机大厅

渡假山庄 商务酒店

www.h3c.com

WLAN（Wireless Local Area Network，无线局域网）指应用无线通信技术将计算机设备互连起来，以无线信道作传输媒介的计算机局域网。

无线局域网本质的特点是不再使用通信电缆将计算机与网络连接起来，而通过无线的方式连接，从而使网络的构建和终端的移动更加灵活。常见的无线局域网产品主要包括无线接入点、无线路由器、无线网关、无线网桥、无线网卡等等。

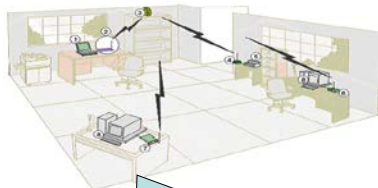
和传统有线以太网相比，WLAN 的优势在于其终端可移动性、网络硬件高可靠性、快速建设与低成本。

WLAN 允许用户在其覆盖范围内的任意地点访问网络数据。用户在使用笔记本电脑、PDA 或数据采集设备等移动终端时能自由地变换位置，这极大方便了因工作需要而不断移动的人员，如教师、护理人员、司机、餐厅服务员等。在一些特殊地理环境架设网络时，如矿山、港口、地下作业场所等，WLAN 无需布线的优势也显而易见。

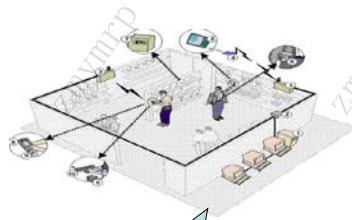
无线让网络建设更经济

紫光集团 H3C
核心企业 数字化转型决策者

- 终端与交换设备之间省去布线，有效降低布线成本。
- 适用于特殊地理环境下的网络架设，如隧道、港口码头、高速公路。



终端与设备之间不方便通过线缆连接



地理环境不适合布设有线网络

www.h3c.com

有线网络中的硬件问题之一是线缆故障。在有线网中，线缆和接头故障常常导致网络连接中断。连接器损坏、线缆断开或接线口因多次使用老化失效等都会干扰正常的网络使用。无线网络技术从根本上避免了由于线缆故障造成的网络瘫痪问题。

无线局域网的工程建设可以节省大量为终端接入而准备的线缆；同时由于减少线缆的布放而大大加快了建设速度，降低了布线费用。在工程建设完毕后，用于网络设备维护和线路租用的费用也会相应减少。在扩充网络容量时，相比传统有线网络，无线局域网也有巨大的成本优势。

32.2.2 WLAN 的协议标准

802.11 协议标准				
	802.11	802.11b	802.11a	802.11g
标准发布时间	July 1997	Sept 1999	Sept 1999	June 2003
合法频宽	83.5MHz	83.5MHz	325MHz	83.5MHz
频率范围	2.400-2.483GHz	2.400-2.483GHz	5.150-5.350GHz 5.725-5.850GHz	2.400-2.483GHz
非重叠信道	3	3	12	3
调制传输技术	BPSK/QPSK FHSS	CCK DSSS	64QAM OFDM	CCK/64QAM OFDM
物理发送速率 (Mbps)	1, 2	1,2,5.5, 11	6, 9, 12, 18, 24, 36, 48, 54	6, 9, 12, 18, 24, 36, 48, 54
理论上的最大UDP吞吐量 (1500 Byte)	1.7 Mbps	7.1 Mbps	30.9 Mbps	30.9 Mbps
理论上的TCP/IP吞吐量 (1500 Byte)	1.6 Mbps	5.9 Mbps	24.2 Mbps	24.2 Mbps
兼容性	N/A	与11g产品可互通	与11b/g不能互通	与11b产品可互通

IEEE 802.11 标准于 1997 年 6 月 26 日制定完成，1997 年 11 月 26 日正式发布。802.11 规范了无线局域网的媒体访问控制层和物理层。IEEE 802.11 使得各种不同厂商的无线产品得以互连。

1999 年 9 月，802.11 标准得到了进一步的完善和修订，并成为 IEEE/ANSI 和 ISO/IEC 的一个联合标准。这次修订增加了两项新内容：

- IEEE 802.11a: 它扩充了标准的物理层，规定该层使用 5.8GHz 的 ISM 频段 (Industrial Scientific Medical Band, 工业、科学、医疗频段)。该标准采用 OFDM (Orthogonal Frequency Division Multiplexing, 正交频分复用) 调制数据，传输速率范围为 6~54Mbps。这样的速率既能满足室内的应用，也能满足室外的应用；
- IEEE 802.11b: 它是 IEEE 802.11 标准的另一个扩充，规定采用 2.4GHz 的 ISM 频带，采用补偿码键控 (CCK) 调制方法。

2003 年 6 月，IEEE 通过了第三种改进的无线局域网接入标准 802.11g。其载波的频率为 2.4GHz (跟 802.11b 相同)，理论传送速度为 54Mbps，净传输速度约为 24.7Mbps (跟 802.11a 相同)。且 802.11g 的设备与 802.11b 兼容。802.11g 是为了提高更高的传输速率而制定的标准，它采用 2.4GHz 频段，使用 CCK 技术与 802.11b 后向兼容，同时它又通过采用 OFDM 技术支持高达 54Mbps 的数据流。


802.11b 是所有 WLAN 标准演进的基石，未来许多的系统都需要与 802.11b 兼容，802.11a 是一个非全球性的标准，与 802.11b 不兼容，但其可提供几倍于 802.11b/g 的高速信道。如 802.11b/g 提供 3 个非重叠信道，而 802.11a 则可达 8~12 个非重叠信道。在 802.11g 和 802.11a

之间存在与 WiFi 兼容性上的差距,为此出现了一种桥接此差距的双频技术——双模(dual band) 802.11a+g (b),它较好地融合了 802.11a/g 技术,工作在 2.4GHz 和 5GHz 两个频段,遵循 802.11b/g/a 等标准。




2004 年 1 月,IEEE 宣布组成一个新的工作组——802.11n。802.11n 的理论传输速度可达 600Mbps,比 802.11b 快 50 倍,而比 802.11g 快 10 倍。虽然 802.11n 的标准制定还处于草案阶段,但毫无疑问 802.11n 将成为 WLAN 今后的技术发展方向。

32.2.3 WLAN 的相关组织和标准

其他WLAN相关组织和标准



- Wi-Fi联盟
 - 成立于1999年的Wi-Fi联盟是一个非盈利国际协会,旨在认证基于IEEE 802.11规格的无线局域网产品的互操作性和推动wireless新标准的制定
 - 目前已知的相关标准
 - WPA: 802.11i的子集,支持802.1x认证以及TKIP加密算法
 - WPA2: 802.11i
 - WMM: 802.11e的子集,支持EDCA方式
- CAPWAP
 - IETF目前有关于无线交换机和FIT AP间控制和管理标准化的工作组
 - 比较重要的标准
 - Architecture Taxonomy for CAPWAP (RFC 4118)
 - LWAPP (最新的草案更名为CAPWAP specification)
- WAPI
 - 中国无线网络产品国标中安全机制的标准,包括无线局域网鉴别(WAI)和保密基础结构(WPI)两部分。

www.h3c.com

在 WLAN 的发展过程中,很多标准化组织参与制定了大量的 WLAN 协议和技术标准。本节将介绍在 WLAN 发展过程中几个起到关键作用的组织与标准。

美国电气和电子工程师协会(Institute of Electrical and Electronics Engineers, IEEE)是一个国际性的电子技术与信息科学工程师的协会。IEEE 802.11 工作组制定了 WLAN 的介质访问控制协议 CSMA/CA 及其物理层技术规范。

2.4GHz 的 ISM 频段为世界上绝大多数国家通用,因此得到了最为广泛的应用。1999 年工业界成立了 WiFi 联盟,致力解决符合 802.11 标准的产品的生产和设备兼容性问题。作为 WLAN 领域内技术的引领者,WiFi 联盟为全世界的 WLAN 产品提供测试认证。

WAPI(Wireless LAN Authentication and Privacy Infrastructure,无线局域网鉴别和保密基础结构)是 WLAN 的一种安全协议,同时也是中国无线局域网安全强制性标准。WAPI 包括无线局域网鉴别(WAI)和保密基础结构(WPI)两部分。与 IEEE 主导完成的公认存在严重

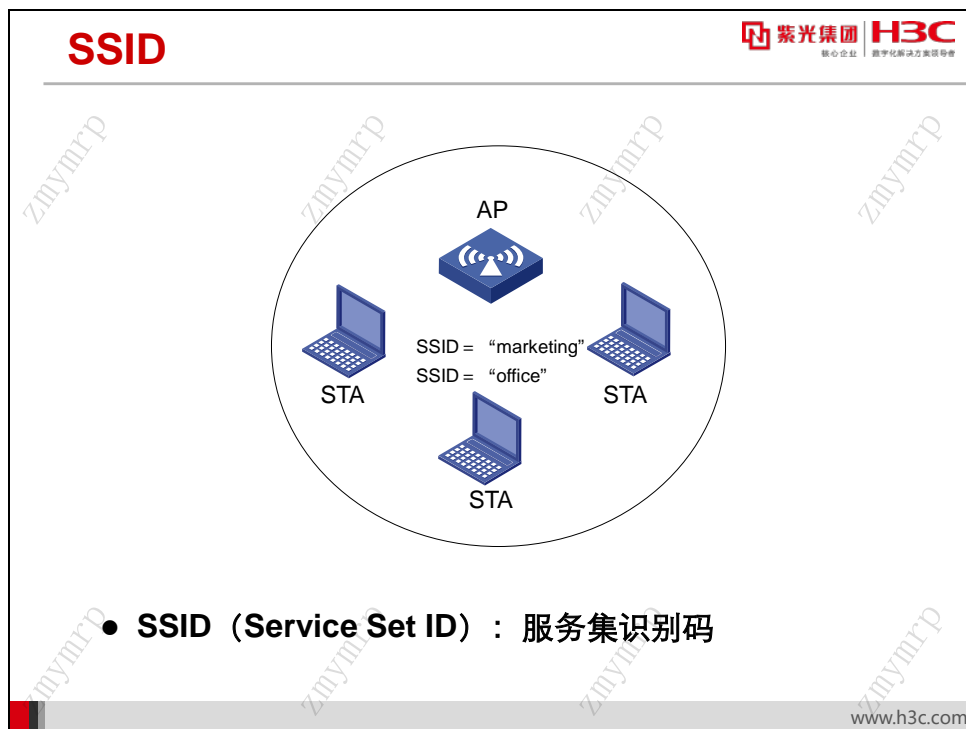
安全缺陷的 802.11i 标准相比，WAPI 具有明显的安全和技术优势，迄今未被发现有安全技术漏洞。

802.11n 有两个提议在互相竞争中——WWiSE (World Wide Spectrum Efficiency) 与 TGn Sync。前者由以 Broadcom 为首的一些厂商支持，后者主要由 Intel 与 Philips 所支持。

正是由于上述组织对相关产业的推动，以及 WLAN 标准的不断完善，才形成了现在 WLAN 技术蓬勃发展的局面。在享受科技创新的同时，不应忘记这些为 WLAN 技术做出贡献的标准化组织。

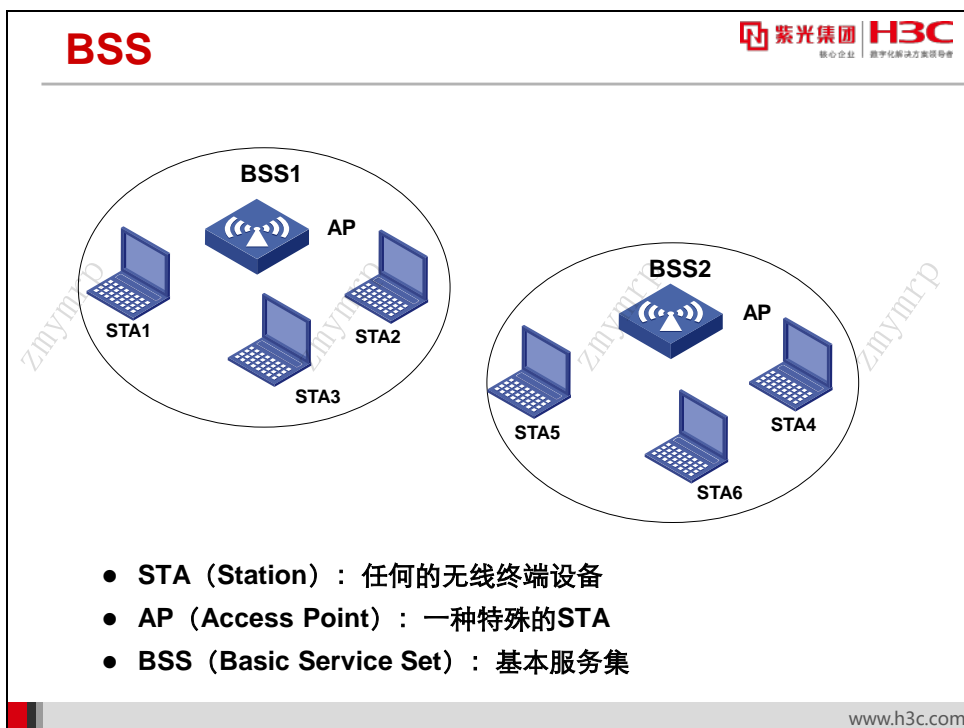
32.3 WLAN网络的构成

32.3.1 WLAN 网络的基本拓扑

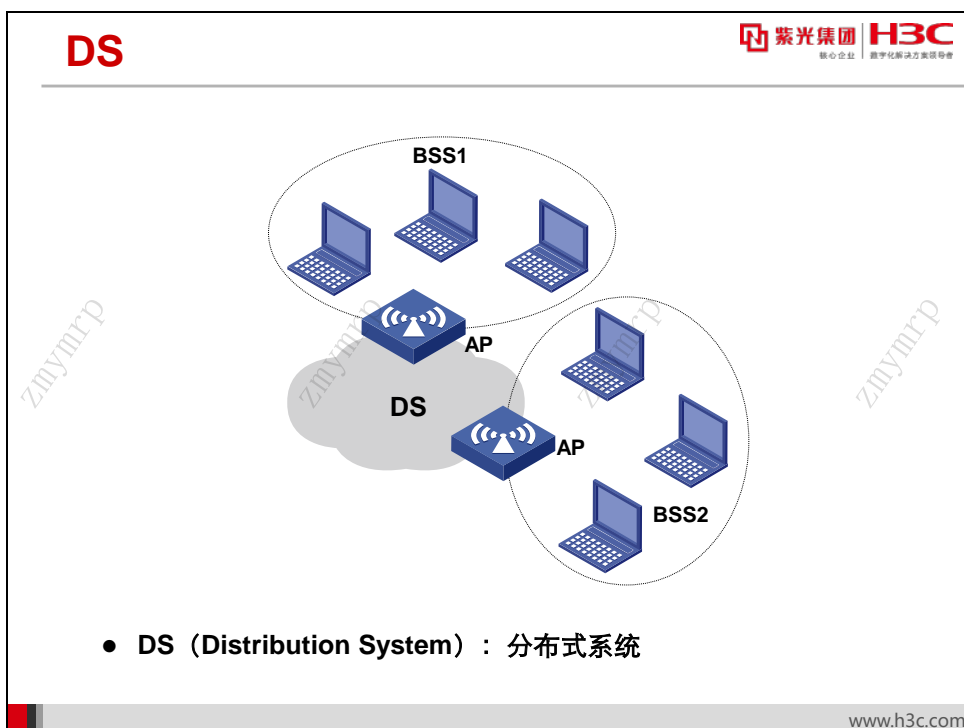


与以太网一样，WLAN 的网络拓扑也是由各种基本元素构建而成的。802.11 协议定义了两种结构模式。一种是 **infrastructure**（基础设施）模式，它由基本服务集、扩展服务集、服务集识别码和分布系统（DS，Distribution System）构成，这就囊括了这种模式中最典型的几个 WLAN 网络基本元素。

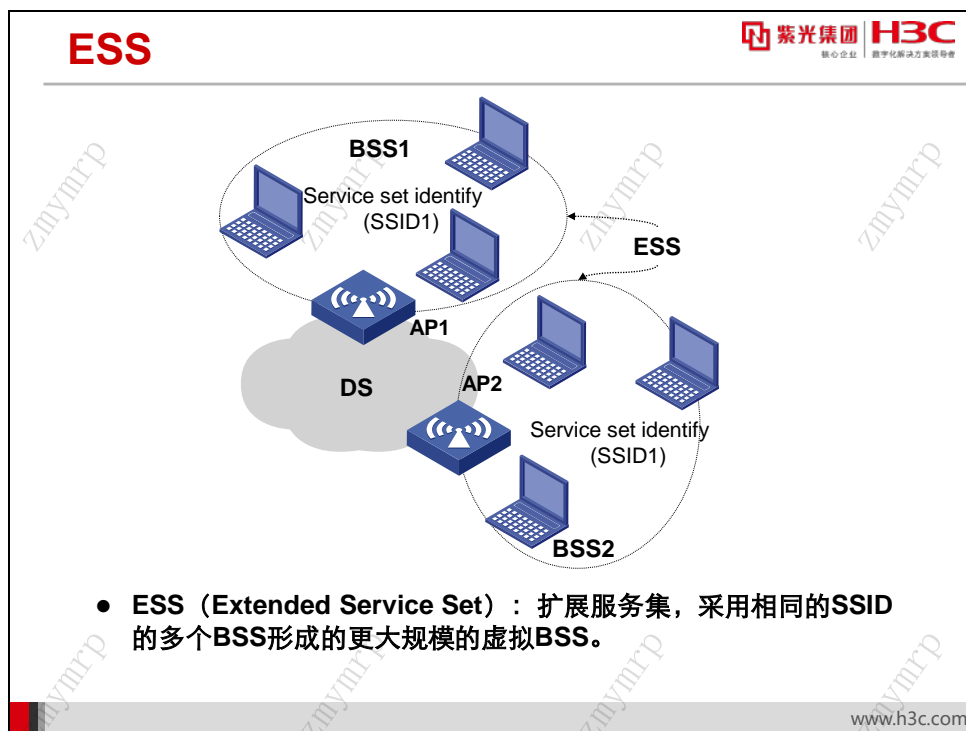
SSID (Service Set Identifier, 服务集识别码)：用来区分不同的网络，无线网卡设置了不同的 SSID 就可以进入不同网络，SSID 通常由 AP 广播出来，通过操作系统自带的扫描功能可以查看当前区域内的 SSID。



BSS (Basic Service Set, 基本服务集)：使用相同服务识别码 (SSID) 的一个单一访问点以及一个无线设备群组，组成一个基本服务组，其必须使用相同的 SSID。使用不同 SSID 的设备彼此之间不能进行通信。

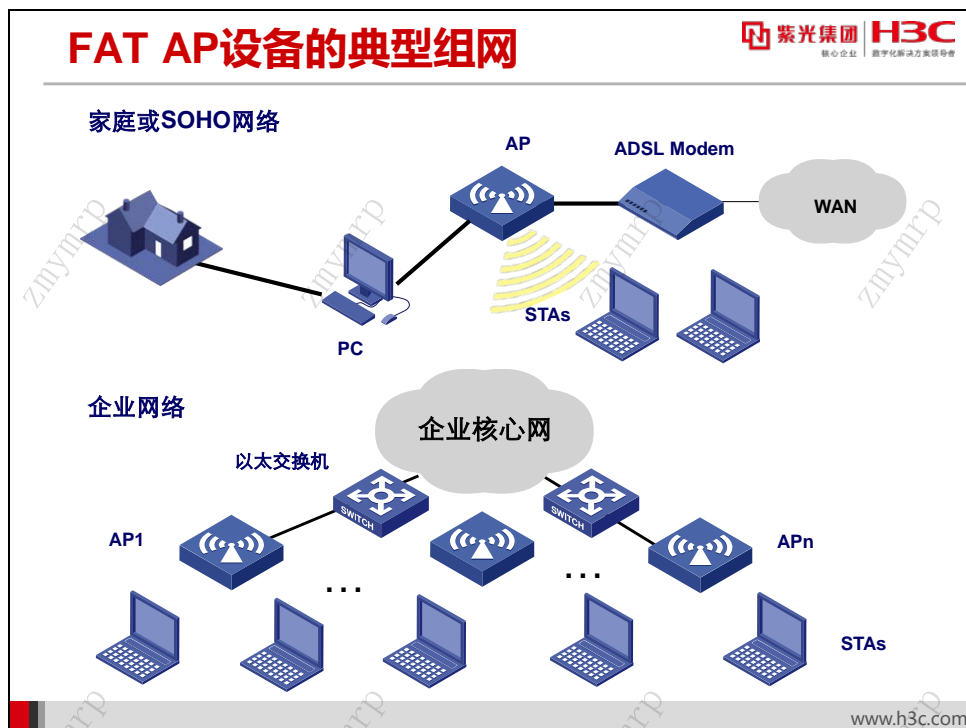


DS（Distribution System 分布系统）：连接 BSS 的组件称为分布系统。DS 的物理实现取决于不同的应用环境，可以包含局域网交换机（LAN Switch），也可以包含其它物理设备。



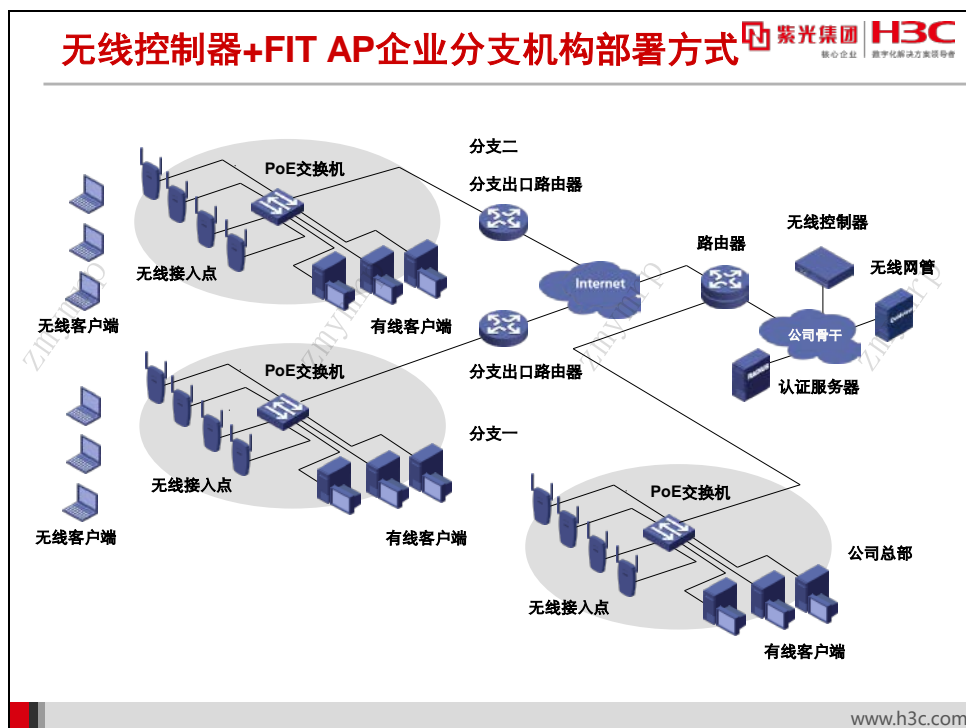
ESS（Extended Service Set，扩展服务集）：使用相同服务识别码（SSID）的多个访问点以及一个无线设备群组，组成一个扩展服务组。同一个 ESS 内的不同访问点可以使用不同的信道。实际上，为了减少干扰，要尽量使相近的访问点之间使用不同的信道。当无线设备在 ESS 所覆盖的区域内进行实体移动时，它们将自动切换到干扰最小、连接效果最好的访问点。这就是漫游功能。

32.3.2 WLAN 设备的典型组网



在本节将介绍两种典型的 WLAN 设备组网模型——小型无线网络和大型分布式无线网络，通过两种方式的比较来掌握 WLAN 设备在小型网络 and 大型网络组网时的异同。

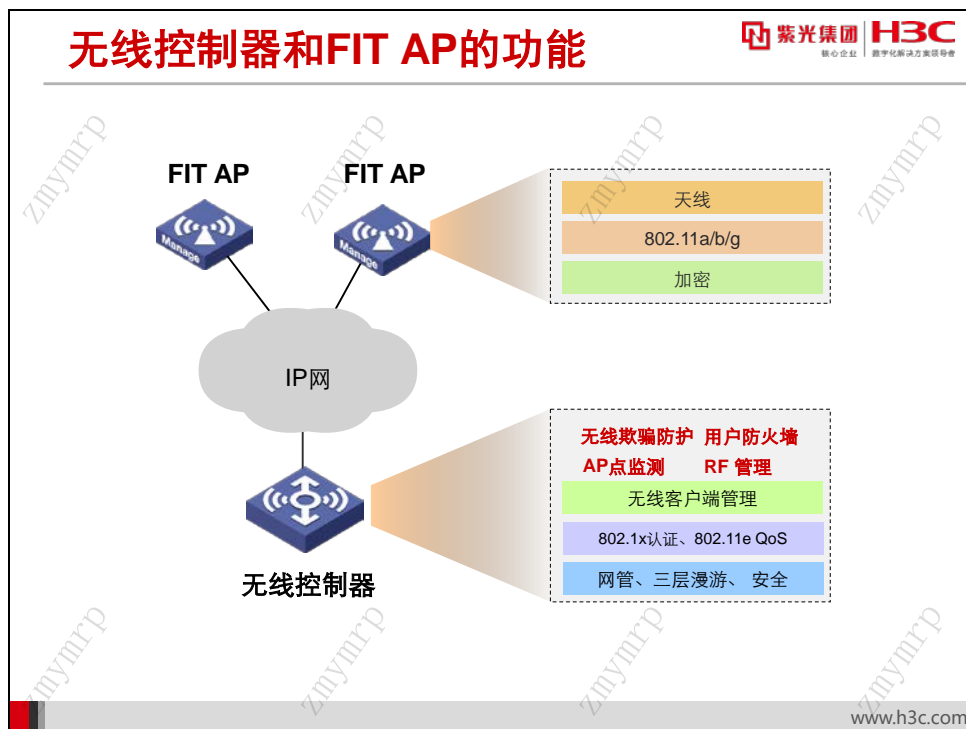
上图是一个典型的小型无线网络，采用了最基本的无线接入设备 AP（Access Point，访问接入点）。AP 在图中的作用仅仅是提供无线信号发射，网络信号通过有线网络传送到 AP，AP 将电信号转换成为无线电信号发送出来，形成无线网的覆盖。根据不同的功率，AP 可实现不同范围的网络覆盖。通常 SOHO 类无线 AP 的功能简单，相当于无线 Hub，在空旷区域的覆盖距离为 100 米以内。



当要部署企业或运营级 WLAN 网络时，简单的 AP 接入方式无法满足客户的需求，WLAN 设备的统一部署、运营和维护成为了大型网络的关键要素。此时就需要在大型网络中部署 AC（Access Control，无线接入控制器），AC 的作用是负责无线网络的接入控制、转发、统计、AP 的配置监控、漫游管理、AP 的网管代理和安全控制等。AC 的出现给中大型 WLAN 网络的维护带来了很大的便利性，AP 在部署、升级、配置上不再需要用户的频繁干预，把网络维护者从繁重的配置操作中解放出来。这种配置方式已经成为大型 WLAN 网络部署和维护的主流方式。

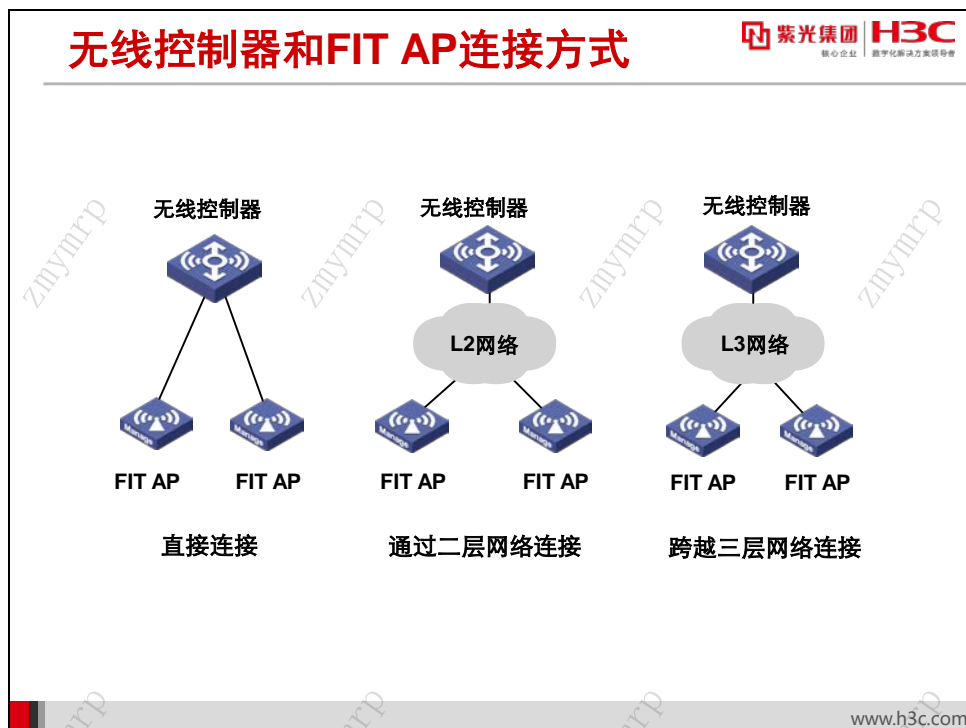
32.4 FIT AP的组网特点

32.4.1 无线控制器和 FIT AP 的功能



在无线控制器+FIT AP 方案中，由无线控制器和 FIT AP 配合在一起提供传统 AP 的功能，无线控制器集中处理所有的安全、控制和管理功能，FIT AP 只提供可靠的、高性能的射频功能。无线控制器+FIT AP 方案除具有易于管理等特点外，还能支持快速漫游、QoS、无线网络安全防护、网络故障自愈等高级功能。

32.4.2 无线控制器和 FIT AP 的连接方式




无线控制器和 FIT AP 支持三种连接方式：直连方式、通过二层网络连接和跨越三层网络连接。

- 直连模式：此连接方式最为简单，只需将 FIT AP 与无线控制器连接即可，但通常受到无线控制器端口数量限制，直连 AP 的数量有限，故一般不会采用此连接方式；
- 二层网络连接方式：可通过 L2 交换机扩展端口数量，实现较多数量的 FIT AP 与无线控制器之间实现二层连接，但必须保证无线控制器与 FIT AP 间为二层网络结构；
- 三层网络连接方式：此连接方式不仅可实现大量 AP 的连接，而且可实现无线控制器与 FIT AP 间跨越三层网络的连接，只要 FIT AP 与无线控制器间三层路由可达即可，但需要 DHCP Server 和 DNS Server 等设备的配合。

由于无线控制器与 FIT AP 之间支持以上三种连接方式，所以无线控制器和 FIT AP 间的连接基本上不受网络结构的限制，可以在任何现有的二层或三层网络中部署无线控制器+FIT AP 的无线解决方案。

32.4.3 无线控制器和 FIT AP 系统的构成特点

无线控制器和FIT AP系统构成特点



紫光集团 H3C
核心企业 数字化转型方案领导者

- 由无线控制器和FIT AP在有线网的基础上构成
- FIT AP零配置
- FIT AP和无线客户端由无线控制器集中管理
- FIT AP和无线控制器之间的流量被私有协议加密
- 可以在任何现有的二层或三层网络中部署

www.h3c.com

无线控制器+FIT AP 系统必须由无线控制器和 FIT AP 在有线网的基础上构成的。

FIT AP 为零配置，硬件主要由 CPU+内存+RF 构成，配置和软件都要从无线控制器上下载。所有 AP 和无线客户端的管理都在无线控制器上完成。

FIT AP 和无线控制器之间的流量被私有协议加密；无线客户端的 MAC 只出现在无线控制器端口，而不会出现在 AP 的端口。

可以在任何现有的二层或三层 LAN 拓扑上部署 H3C 的通用无线解决方案，而无需重新配置主干或硬件。无线控制器以及 FIT AP 可以位于网络中的任何位置。

而由于 FIT AP 为零配置启动，需要从无线控制器下载配置和软件，所以 FIT AP 通过一定的注册流程来保证在复杂的网络环境中找到无线控制器的位置，才可和无线控制器完成数据交互。

32.5 WLAN的配置方式

32.5.1 Web 页面管理



H3C 的无线 AP 可以通过两种方式登录配置：一种是 Web 页面方式，另外一种方式和交换机、路由器一样通过命令行模式登录管理。这里以 WA2210-AG 为例，熟悉 AP 设备的 Web 管理页面与命令行配置管理界面。

当计算机终端与 AP 建立无线连接后，在 IE 页面下输入 AP 的管理 IP 地址，就能够进入 AP 的 Web 登录页面。


输入正确的用户名、密码、随机验证码并选择语言之后，即可进入 AP 的管理页面。



在管理页面中，能看到设备的 CPU 占用率、内存占用率及设备版本和端口信息等基本内容。也可以通过 Web 界面对 AP 进行简单的配置和操作。对于初次接触设备的用户来说，Web 页面简单易懂，是入门学习的好帮手。

32.5.2 命令行管理

命令行配置

 紫光集团 H3C
核心企业 数字化转型方案领导者

- 将当前的Access端口加入到指定的VLAN中

```
[H3C-WLAN-ESS1] port access vlan vlan-id
```
- 创建服务模板并进入服务模板视图

```
[H3C] wlan service-template service-template-number  
{ clear | crypto | wapi }
```
- 设置当前服务模板的SSID

```
[H3C-wlan-st-1] ssid ssid-name
```
- 配置802.11规定的认证方式

```
[H3C-wlan-st-1] authentication-method { open-system |  
shared-key }
```

www.h3c.com

当要对 AP 进行详细配置的时候，命令行界面能够帮助我们解决复杂的配置需求。

在配置无线时，首先需要将 access 端口加入到指定的 vlan 当中。在缺省情况下，所有的 access 端口都属于 vlan 1。

其次要创建服务模板。在服务模板创建时，可以配置当前服务模板的类型为明文方式、密文方式或是 WAPI 方式，不同的配置确定了无线客户端与 AP 关联后发送数据的方式。需要注意，服务模板创建之后将不能修改其类型。

之后在服务模板视图下设置当前服务模板的 SSID，SSID 的名称应该尽量具有唯一性，便于用户识别想要接入的无线网络。

802.11 规定的认证方式有开放式认证和共享密钥认证两种，用户可以根据需要选配其中任一种，或是同时启用两种认证方式。缺省情况下，系统启用的是开放式认证方式。

命令行配置



- 将指定的无线接口绑定到服务模板

```
[H3C-wlan-st-1] bind wlan-ess interface-index
```

- 开启服务模板

```
[H3C-wlan-st-1] service-template enable
```

- 创建并进入 AP 管理模板视图

```
[H3C] wlan ap ap-name [ model model-name [ id ap-id ] ]
```

www.h3c.com

服务模板创建好之后，需要将 WLAN-ESS 接口绑定到服务模板。最后要开启服务模板，缺省情况下服务模板处于关闭状态。

在无线控制器上统一对 AP 进行管理时，需要进入到 AP 管理模板视图中。在创建 AP 管理模板时，必须定义 AP 的型号名称。

命令行配置



- 配置AP的序列号

```
[H3C-wlan-ap-ap1] serial-id [ text | auto ]
```

- 将服务模板映射到指定的射频

```
[H3C-wlan-ap-ap1-radio-1] service-template service-  
template-number [ vlan-id vlan-id | vlan-pool vlan-pool-  
name ] [ nas-port-id nas-port-id | nas-id nas-id ] [ ssid-hide ]
```

- 开启AP的射频

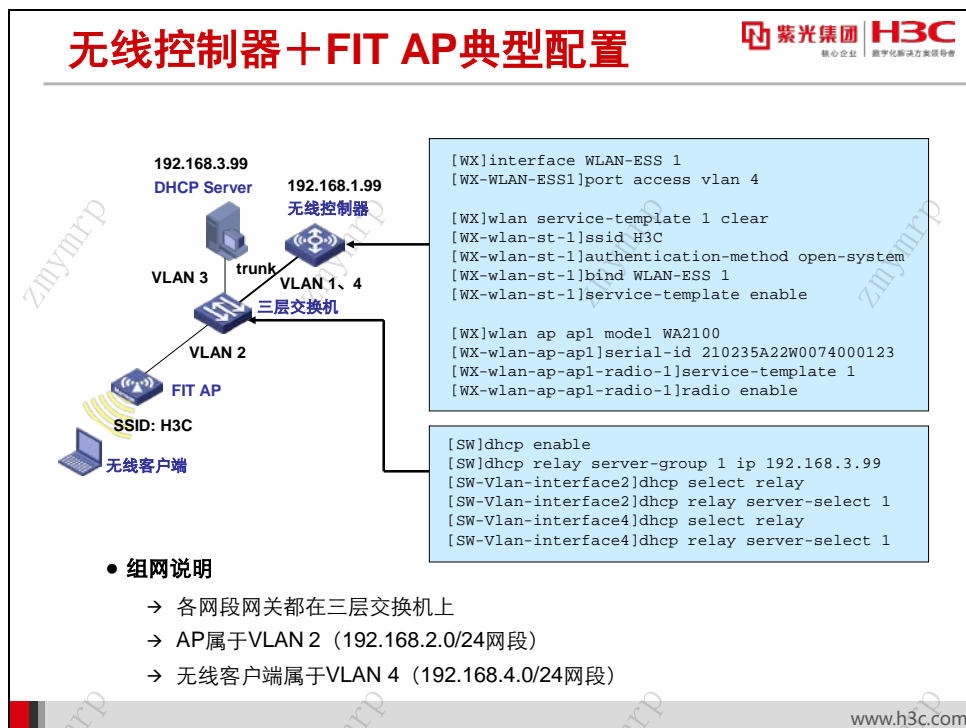
```
[H3C-wlan-ap-ap1-radio-1] radio enable
```

www.h3c.com

在 AP 模板视图下，需要配置 AP 的序列号，序列号是每个 AP 的唯一标识。

指定 AP 的序列号之后，会进入到射频视图中。在射频视图下，需要开启 AP 的射频，并将服务模板映射到指定的射频。

32.5.3 无线控制器+FIT AP 组网典型配置



在无线控制器+FIT AP 的网络中，主要对无线控制器和三层交换机进行相关配置。

三层交换机的主要配置包括：

第1步：创建需要的 VLAN（VLAN1、2、3、4），并配置对应的 VLAN 接口地址。

```

[SW]vlan 2
[SW]vlan 3
[SW]vlan 4
[SW]interface vlan 1
[SW-Vlan-interface1]ip address 192.168.1.254 255.255.255.0
[SW]interface vlan 2
[SW-Vlan-interface2]ip address 192.168.2.254 255.255.255.0
[SW]interface vlan 3
[SW-Vlan-interface3]ip address 192.168.3.254 255.255.255.0
[SW]interface vlan 4
[SW-Vlan-interface4]ip address 192.168.4.254 255.255.255.0
  
```

第2步：在 FIT AP 和无线客户端所在的 VLAN 接口上启用 DHCP relay 功能。

```

[SW]dhcp enable
[SW]dhcp relay server-group 1 ip 192.168.3.99
[SW-Vlan-interface2]dhcp select relay
[SW-Vlan-interface2]dhcp relay server-select 1
[SW-Vlan-interface4]dhcp select relay
[SW-Vlan-interface4]dhcp relay server-select 1
  
```

说明：

本例中，FIT AP 与 DHCP Server 不在同一网段，所以需要在 FIT AP 的网关上启用 DHCP relay 功能，以保证 FIT AP 可以动态获取 IP 地址；同时无线客户端也要动态获取 IP 地址，所以同样需要在无线客户端的网关上启用 DHCP relay 功能。

无线控制器的主要配置：

第1步：创建无线接口，并指定该接口属于 VLAN 4。（默认情况下，新建的无线接口属于 VLAN 1）

```
[WX]interface WLAN-ESS 1
[WX-WLAN-ESS1]port access vlan 4
```

第2步：创建需要无线服务模板，配置 SSID 名称为“H3C”，绑定无线接口。

```
[WX]wlan service-template 1 clear
[WX-wlan-st-1]ssid H3C
[WX-wlan-st-1]authentication-method open-system
[WX-wlan-st-1]bind WLAN-ESS 1
[WX-wlan-st-1]service-template enable
```

第3步：根据 FIT AP 的具体型号和序列号添加 AP，并在 AP 的射频卡 radio 上绑定服务模板。

```
[WX]wlan ap ap1 model WA2100
[WX-wlan-ap-ap1]serial-id 210235A22W0074000123
[WX-wlan-ap-ap1]radio 1 type dot11g
[WX-wlan-ap-ap1-radio-1]service-template 1
[WX-wlan-ap-ap1-radio-1]radio enable
```

32.6 本章总结

本章总结

- WLAN的优势与标准
- WLAN网络的构成
- FIT AP的组网特点
- WLAN的配置方式

www.h3c.com