

试题一（25 分）

小李居住的小区中，有电信提供的宽带 LAN 接入服务。该小区是一个由三幢小高层组成的，整个网络结构如图 1 所示。

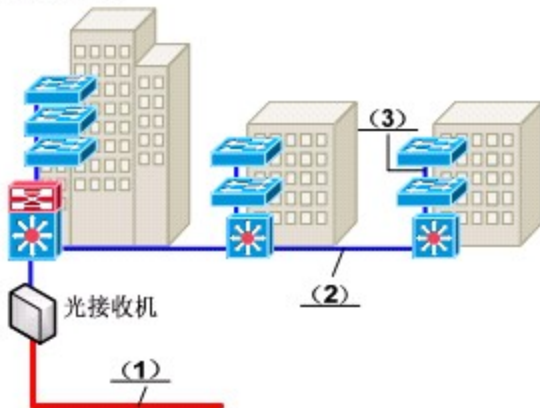


图 1 某小区网络结构示意图

【问题 1】（6 分）

根据图 10 所示的网络结构，可以看出这属于 FTTx 中的哪一种？除了这一种之外，还有哪些类型？

【问题 2】（4 分）

图 1 中位置（1）处应该使用什么传输介质？根据综合布线的标准，位置（2）、（3）分别应属什么子系统？

【问题 3】（2 分）

该小区住户访问 Internet 的理论最高速率，哪个环节将起到决定作用？

【问题 4】（3 分）

应该如何估算楼层级交换机数量，请简要说明。（字数限制为 100 字以内）

试题一参考答案

【问题 1】(8 分)

属于 FTTZ (或光纤到小区, 2 分)

还包括 FTTC (或光纤到路边)、FTTB (或光纤到楼)、FTTF (或光纤到楼层)、FTTH (或光纤到户) 四种。(每列出 1 种得 2 分)

【问题 2】(6 分)

(1) 光纤 (2 分)

(2) 建筑群主干子系统 (2 分)

(3) 干线子系统 (或垂直子系统, 2 分)

【问题 3】(3 分)

接入小区的光纤所提供的速率。(3 分)

【问题 4】(8 分)

交换机的数量估算应该利用公式“信息点 (户数) / 交换机端口数量” (4 分), 而且要考虑双绞线的最大连接距离为 100 米的限制。(4 分)

试题一分析

【问题 1】

随着光纤通信技术的平民化,以及高速以太网的发展,现在许多宽带智能小区就是采用以千兆以太网技术为主干、充分利用光纤通信技术完成接入的。实现高速以太网的宽带技术常用的方式是 FTTx+LAN,即光纤+局域网。根据光纤深入用户的程序,可以分为:

- FTTC (Fiber To The Curb): 光纤到路边;
- FTTZ (Fiber To The Zone): 光纤到小区;
- FTTB (Fiber To The Building): 光纤到楼;
- FTTF (Fiber To The Floor): 光纤到楼层;
- FTTH (Fiber To The Home): 光纤到户。

显然,在图 1 中,光纤是连接到小区,然后利用小区的综合布线系统连接到每一户的,因此属于 FTTZ。

【问题 2】

这个问题所涉及的知识并不复杂,主要是要考生能够正确地临场发挥。

- 位置(1)所指出的传输媒介是连接到“光接收机”,从此不难看出其显然是应该采用光纤。
- 而位置(2)的干线主要是用来连接三座楼的交换机,因此显然属于“建筑群子系统”。
- 位置(3)是连接一座楼中的各楼层交换机的,其线缆是与大楼垂直,显然不难得知其为“垂直子系统”即“干线子系统”。

【问题 3】

这道题考查的是考生对网络访问瓶颈的分析,以及对常见网络结构的理解。由于图 1 所表现的是为一个小区提供宽带上网,即互联网服务,因此光纤的另一端就是连接到 ISP(电信局),实现 Internet 接入。

因此这根光纤就将成为整个小区连接 Internet 的必经之地,不管楼层交换机的速度有多快、小区主干交换机的速度有多快,即使达到千兆到桌面,其最终还是会受到这根光纤速率的限制。因为,实际上整个小区的用户是在共享这个光纤的带宽。

【问题 4】

这道题则是变化了一种形式来考查接入层交换机的选型要点。我们知道，在选择网络层交换机中，首先要评估有多个信息点，就是连接数，在本应用中也就是住户的个数。而由于本小区非商业用户，每层楼的信息点较少，因此会尽可能复用交换机，只要在 100 米距离的限制之内都可以共享。

有了信息点，要多个交换机呢？显然就应该根据交换机的端口密度来决定，如果交换机的端口多，个数就肯定会减少。因此可以得出公式：“信息点数/交换机端口数量”。

试题二 (25 分)

某广域网如图 1 所示，其中路由器 C 位于整个网络的中心区域，因此 WAN 连接最多。其中 CIR 表示帧中继虚电路，路由器 F 到路由器 C 则有两条 PPP 链路。

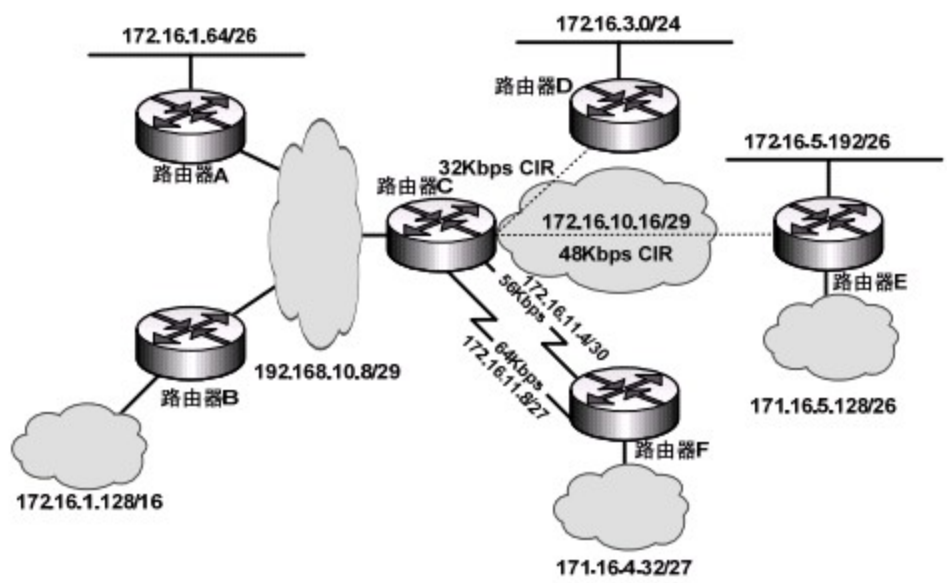


图 1 广域网结构示意图

【问题 1】(10 分)

以下是路由器 C 上的配置片断，请根据题目要求和图 1 的信息，填充 (1) - (5)。

.....

```
interface fddi0
```

```
    ip address 192.168.10.11 255.255.255.248
```

```
interface serial0
```

```
    encapsulation (1)
```

```
    ip address 172.16.10.17 255.255.255.248
```

```
    bandwidth 80
```

```
interface serial1
```

```
    encapsulation ppp
```

```
    ip address 172.16.11.5 255.255.255.252
```

```
    bandwidth (2)
```

```
interface serial2
```

```
    encapsulation ppp
```

```
    ip address 172.16.11.9 255.255.255.0
```

```
    bandwidth (3)
```

```
route (4) 100
```

```
    network 172.16.0.0
```

```
    network 192.168.10.0
```

```
ip route 172.16.1.64 255.255.255.192 172.16.10.9
```

```
ip route 172.16.1.128 255.255.255.192 172.16.10.10
```

```
ip route 172.16.3.0 255.255.255.0 172.16.10.18
```

```
ip route 172.16.4.32 255.255.255.224 (5)
```

```
ip route 172.16.4.32 255.255.255.224 172.16.11.9
```

```
ip route 172.16.5.128 255.255.255.128 172.16.10.19
```

.....

【问题2】(8分)

1. 在问题 1 中的配置信息最后一部分中的 **ip route** 命令的作用是什么？为什么需要这些配置？

2. 在问题 1 中的配置 **bandwidth** 的功能是什么？

【问题3】(7分)

为了解决在问题 2 中遇到的问题，就采用了 **EIGRP** 路由选择协议来代替 **IGRP**。下面就是新的配置片断，请将第 (1) - (3) 的位置上补充相应的配置命令。

.....

```
interface serial2
```

```
    encapsulation ppp
```

```
    ip address 172.16.11.9 255.255.255.0
```

.....

```
    (1)  eigrp 100 172.16.1.0 255.255.255.0 (设置 IP 汇总)
```

```
route (2)
```

```
    network 172.16.0.0
```

```
    (3)                                     (关闭路由自动汇总)
```

```
var 2
```

.....

试题二参考答案

【问题 1】(10 分)

- (1) frame 或者 frame-relay (2 分)
- (2) 56 (2 分)
- (3) 64 (2 分)
- (4) igrp (2 分)
- (5) 172.16.11.5 (2 分)

【问题 2】(8 分)

1. ip route 命令是用来设置静态路由的。(2 分)

由于 IGRP 对 VLSM 的处理不好，因此需要设置静态路由 (2 分)

2. 用来设置该条链路的带宽 (2 分)，从而使 IGRP 在生成路由时可以考虑到带宽。(2 分)

【问题 3】(7 分)

- (1) ip summary-address (2 分)
- (2) eigrp 100 (2 分)
- (3) no auto-summary (3 分)

试题二分析

【问题 1】-【问题 2】

这两个问题主要涉及的是 IGRP 路由协议的配置, 首先我们依次看一下这几个空的含义, 以及应该填入的内容。

- 第(1)空的关键字是 **encap**, 它是用来设置该链路所使用的二层协议。根据该接口配置的 IP 地址是“172.16.10.17”, 可以从图中找出相关的链路是帧中继虚电路, 因此应该填入 “**frame**” 或者 **frame-relay**。
- 第(2)、(3)空的关键字是 **bandwidth**, 这是 IGRP 协议的一个特性, 它是用来指定链路的带宽, 通常单位为 Kbps。因此重要的是根据其 IP 地址来确定其代表的是哪条链路。显然 S1 连接的是 56Kbps 的链路, S2 连接的是 64Kbps 的链路。因此分别应该填入 **56**、**64**。
- 第(4)空则应该输入的是 IGRP 路由选择协议的关键字, 即 **igrp**。

由于 IGRP 对于 VLSM 的支持不太好, 无法对子网进行路由 (network 后的 IP 地址是不带子网掩码的, 因此我们需要用 **ip route** 来指定。配置命令 **ip route** 是用来配置静态路由的, 其格式是: **ip route** 目的地址 目的地址子网掩码 网关。

因此第(5)空, 显然就是要填网关, 我们从图中可以发现, 到 172.16.4.32/27 的网络, 可以通过 S1 和 S2 两个端口到达, 而后一名正是通过 S2 端口的路由, 因此应该填入的是 S1 端口的 IP 地址 172.16.11.5。

【问题 3】

正是因为 IGRP 对 VLSM 的支持存在问题，因此也出现了 EIGRP，它能够有效地解决这个问题。与 IGRP 不同的是，EIGRP 发送的是增量更新，它们不会随便发送消耗带宽，只是在需要的时候才发送。EIGRP 是一个无类路由协议，也就是在路由更新时中包含子网掩码的，因此可以支持 VLSM。在 IGRP 中，一个主网络的所有子网都指定了一个同样的掩码，这就造成了 IP 地址浪费。

不过，在 EIGRP 中对不连续子网的支持不是默认的，当要跨越不同的主网通告一个网络的子网时，EIGRP 会自动将这些子网汇总给主网号，因此每个路由器除了能够到达自己的子网外不能到达其他子网。

因此，我们就需要使用 `no auto-summary` 命令来禁止这个自动汇总，这样就可以支持如图 1 所示的不连续子网，但同时也增大了路由表的大小。

由于我们的所有子网可以在整个网络上路由，EIGRP 提供了手工汇总的命令，这个汇总命令是用于子配置模式的（也就是说针对一个接口有效）：`ip summary-address eigrp AS network mask`（AS 表示自治系统号、network 表示网络号、mask 是子网掩码）。

试题三（25 分）

在某公司的分支机构和总部之间，为了实现网络通信的安全，采用了 L2TP 构建了一个 VPN 网络，其网络结构如图 1 所示。

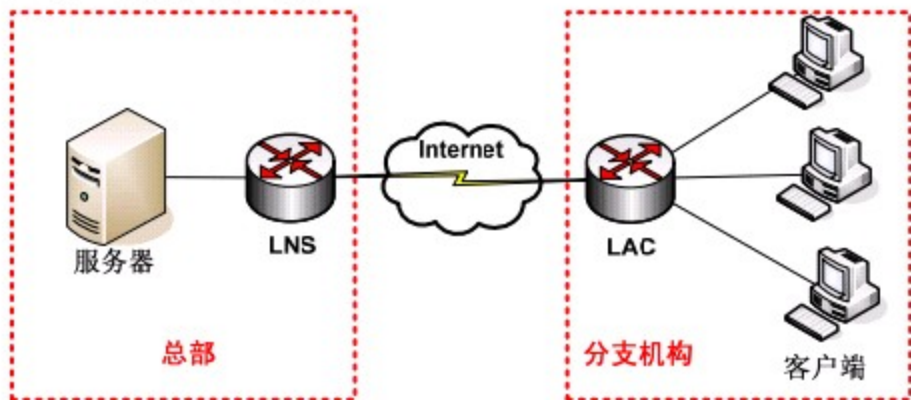


图 1 L2TP VPN 网络结构示意图

【问题 1】（8 分）

在图 1 中的 LNS 和 LAC 分别代表什么？其作用是什么？

【问题2】(8分)

以下是 LAC 上的路由器配置片断，请在 (1) - (3) 处填入相应的配置命令或配置命令的解释。

.....

```
hostname lac01
```

```
pppoe virtual-template 0
```

```
vpdn enable
```

(1)

```
vpdn domain-delimiter suffix @
```

```
interface eth1/0
```

```
    ip address 10.1.1.1/30
```

```
linterface eth5/0
```

```
    pppoe enable
```

```
interface virtual-template0
```

```
    ppp authentication chap default
```

```
    ppp authorization default
```

.....

```
vpdn-group 2
```

(2)

```
request dialin l2tp ip 10.1.1.2 domain abc.com
```

(3)

```
no l2tp tunnel authentication
```

【问题3】(9分)

以下是 LNS 上的路由器配置片断，请在 (4) - (6) 处填入相应的配置命令或配置命令的解释。

```
ip local pool default 192.168.0.2 192.168.0.100
```

(4)

```
interface eth0/0
```

```
    ip address 10.1.1.2/30
```

```
interface virtual-template0
```

```
    ip address 192.168.0.1/24
```

```
    ppp authentication chap default
```

```
    peer default ip address pool default
```

```
dial-peer voice default voip
```

```
voice-class codec default
```

```
voice-class h323 default
```

```
dial-peer voice default pots
```

```
ip route 0.0.0.0/0 10.1.1.1
```

```
.....
```

```
vpdn-group 2
```

```
accept dialin l2tp virtual-template 0 remote lac01
```

```
no l2tp tunnel authentication
```

(5)

(6)

试题三参考答案

【问题 1】（8 分）

LAC 是接入集中器（2 分），用于发起呼叫、接收呼叫和建立隧道。（2 分）

LNS 是 L2TP 网络服务器（2 分），是所有隧道的终端。（2 分）

【问题 2】（8 分）

（1）启用 VPDN。（2 分）

（2）创建 VPDN 组 2。（2 分）

（3）发起 L2TP 通道请求，呼叫 10.1.1.2。（4 分）

【问题 3】（9 分）

（1）vpdn enable（3 分）

（2）接受 L2TP 通道连接请求，并根据 virtual-template 1 创建 virtual-access 接口，并设置通道远端名称为 lac01。（3 分）

（3）关闭 L2TP 的通道验证功能。（3 分）

[查看分析](#)

试题三分析

【问题 1】

L2TP，即第二层通道协议，它是一种使用广泛的隧道技术，用于在 Internet 中建立安全、高优先级的临时通路。L2TP 使用两种报文：用于建立、维护和释放隧道的控制报文；用于包装通过隧道传输的 PPP 帧的数据报文。使用 L2TP 构建的 VPN 主要是由 LAC（接入集中器）和 LNS（L2TP 网络服务器）两个部分构成。其中，LAC 主要是支持客户端的 L2TP，用于发起呼叫、接收呼叫和建立隧道；LNS 是所有隧道的终端。

【问题2】-【问题3】

以下是创建 L2TP VPN 时最常用的几组命令：

■ 创建或删除 VPDN 组

- 命令格式：**[no] vpdn-group *group-number***
- 参数说明：**group-number** 为 VPDN 组号，范围是 1-3000。
- 记忆要点：这是创建 VPN 关键的第一步。“创建组号为 *x* 的 VPDN 组”或“删除组号为 *x* 的 VPDN 组”。

■ 指定接受呼叫时，通道对端的名称及使用的 Virtual-template

- 命令格式：**accept-dialin l2tp virtual-template *vt-num* remote *remote-name***
- 参数说明：**vt-num** 指定用于创建新的虚拟访问接口时所使用的虚拟接口模板。
remote-name 指定发起连接请求的通道对端的名称，大小写区分。
- 记忆要点：这是在 VPN 配置中最关键的一个设置命令。通常在 VPDN 命令执行

后执行。“接受 L2TP 通道连接请求，并根据 Virtual-template 1

创

建 Virtual-access 接口，并设置对端的名称为 *xx*”。

■ 指定隧道本端的名称

- 命令格式：**local name *name* | no local name**
- 命令说明：在创建一个 VPDN 组时，本端名会被初始化为路由器的名称。如果要恢复成默认名称，可以使用 **no** 形式。
- 记忆要点：“指定隧道本端名称为 *name*”。

■ 设置是否允许 LNS 与 Client 间重新协商 LCP（链路控制协议）

- 命令格式：**lcp renegotiation | no lcp renegotiation**
- 命令说明：该命令还可以有一个变化，**lcp renegotiation always**，即一直允许进

行 LCP 协商。

- 记忆要点：“开启 LCP 协商功能”、“关闭 LCP 协商功能”。

- 设置 L2TP 的通道验证功能是否启用
 - 命令格式: `l2tp tunnel authentication | no l2tp tunnel authentication`
 - 命令说明: 在默认情况下是启用的, 这也是更安全的。但如果为了进行网络的连通性测试或者是接收不知名对端发起的连接, 则可以关闭。
 - 记忆要点: “启用 L2TP 通道验证”、“关闭 L2TP 通道验证”。
- 设置 L2TP 的通道密码: `l2tp tunnel password password`
- 设置 L2TP 的通道密码: `l2tp tunnel password password`
 将 L2TP 的通道密码还原为默认值 : `no l2tp tunnel password`
 当创建一个 VPDN 组时, 本端名称与通道密码都将初始化为路由器名称。
- 断开通道连接: `clear vpdn tunnel l2tp remote-name`
- 强制 LNS 与 Client 之间重新进行 CHAP 验证: `force-local-chap`
- 禁止 LNS 与 Client 之间重新进行 CHAP 验证: `no force-local-chap`