CCNA-网络工程师面试题

※什么是三层交换，说说和路由的区别在那里？

三层交换机和路由器都可工作在网络的第三层，根据 ip 地址进行数据包的转发（或交换），原理上没有太大的区别，这两个名词趋向于统一，我们可以认为三层交换机就是一个多端口的路由器。
但是传统的路由器有 3 个特点：基于 CPU 的单步时钟处理机制；能够处理复杂的路由算法和协议；主要用于广域网的低速数据链路
在第三层交换机中，与路由器有关的第三层路由硬件模块也插接在高速背板/总线上，这种方式使得路由模块可以与需要路由的其他模块间高速的交换数据，从而突破了传统的外接路由器接口速率的限制(10Mbit/s---100Mbit/s)。

※对路由知识的掌握情况，对方提出了一个开放式的问题：简单说明一下你所了解的路由协议。

路由可分为静态&动态路由。静态路由由管理员手动维护；动态路由由路由协议自动维护。

路由选择算法的必要步骤：1、向其它路由器传递路由信息；2、接收其它路由器的路由信息；3、根据收到的路由信息计算出到每个目的网络的最优路径，并由此生成路由选择表；4、根据网络拓扑的变化及时的做出反应，调整路由生成新的路由选择表，同时把拓扑变化以路由信息的形式向其它路由器宣告。
两种主要算法：距离向量法（Distance Vector Routing）和链路状态算法（Link-State Routing）。由此可分为距离矢量（如：RIP、IGRP、EIGRP）&链路状态路由协议（如：OSPF、IS-IS）。
路由协议是路由器之间实现路由信息共享的一种机制，它允许路由器之间相互交换和维护各自的路由表。当一台路由器的路由表由于某种原因发生变化时，它需要及时地将这一变化通知与之相连接的其他路由器，以保证数据的正确传递。路由协议不承担网络上终端用户之间的数据传输任务。

※简单说下 OSPF 的操作过程

① 路由器发送 HELLO 报文；②建立邻接关系；③形成链路状态④ SPF 算法算出最优路径⑤形成路由表

※OSPF 路由协议的基本工作原理，DR、BDR 的选举过程，区域的作用及 LSA 的传输情况（注：对方对 OSPF 的相关知识提问较细，应着重掌握）。

特点是：1、收敛速度快；2、支持无类别的路由表查询、VLSM 和超网技术；3、支持等代价的多路负载均衡；4、路由更新传递效率高（区域、组播更新、DR/BDR）；5、根据链路的带宽（cost）进行最优选路。

通过发关 HELLO 报文发现邻居建立邻接关系，通过泛洪 LSA 形成相同链路状态数据库，运用 SPF 算法生成路由表。
DR/BDR 选举：1、DR/BDR 存在->不选举；达到 2-way 状态 Priority 不为 0->选举资格；3、先选 BDR 后 DR；4、利用“优先级”“RouterID”进行判断。
1、通过划分区域可以减少路由器 LSA DB，降低 CPU、内存、与 LSA 泛洪带来的开销。
2、可以将 TOP 变化限定在单个区域，加快收敛。
LSA1、LSA2 只在始发区域传输；LSA3、LSA4 由 ABR 始发，在 OSPF 域内传输；LSA5 由 ASBR 始发在 OSPF 的 AS 内传输；LSA7 只在 NSSA 内传输。

※OSPF 有什么优点？为什么 OSPF 比 RIP 收敛快？

优点：1、收敛速度快；2、支持无类别的路由表查询、VLSM 和超网技术；3、支持等代价的多路负载均衡；4、路由更新传递效率高（区域、组播更新、DR/BDR）；5、根据链路的带宽进行最优选路
采用了区域、组播更新、增量更新、30 分钟重发 LSA

※RIP 版本 1 跟版本 2 的区别？
答：① RIP-V1 是有类路由协议，RIP-V2 是无类路由协议② RIP-V1 广播路由更新，RIP-V2 组播路由更新③ RIP-V2 路由更新所携带的信息要比 RIP-V1 多

※描述 RIP 和 OSPF，它们的区别、特点

RIP 协议是一种传统的路由协议，适合比较小型的网络，但是当前 Internet 网络的迅速发展和急剧膨胀使 RIP 协议无法适应今天的网络。
OSPF 协议则是在 Internet 网络急剧膨胀的时候制定出来的，它克服了 RIP 协议的许多缺陷。
RIP 是距离矢量路由协议；OSPF 是链路状态路由协议。
RIP&OSPF 管理距离分别是：120 和 110
1．RIP 协议一条路由有 15 跳（网关或路由器）的限制，如果一个 RIP 网络路由跨越超过 15 跳（路由器），则它认为网络不可到达，而 OSPF 对跨越路由器的个数没有限制。
2．OSPF 协议支持可变长度子网掩码（VLSM），RIP 则不支持，这使得 RIP 协议对当前 IP 地址的缺乏和可变长度子网掩码的灵活性缺少支持。
3．RIP 协议不是针对网络的实际情况而是定期地广播路由表，这对网络的带宽资源是个极大的浪费，特别对大型的广域网。OSPF 协议的路由广播更新只发生在路由状态变化的时候，采用 IP 多路广播来发送链路状态更新信息，这样对带宽是个节约。
4．RIP 网络是一个平面网络，对网络没有分层。OSPF 在网络中建立起层次概念，在自治域中可以划分网络域，使路由的广播限制在一定的范围内，避免链路中继资源的浪费。
5．OSPF 在路由广播时采用了授权机制，保证了网络安全。
上述两者的差异显示了 OSPF 协议后来居上的特点，其先进性和复杂性使它适应了今天日趋庞大的 Internet 网，并成为主要的互联网路由协议。

※什么是静态路由？什么是动态路由？各自的特点是什么？

静态路由是由管理员在路由器中手动配置的固定路由，路由明确地指定了包到达目的地必须经过的路径，除非网络管理员干预，否则静态路由不会发生变化。静态路由不能对网络的改变作出反应，所以一般说静态路由用于网络规模不大、拓扑结构相对固定的网络。
静态路由特点
1、它允许对路由的行为进行精确的控制；
2、减少了网络流量；
3、是单向的；
4、配置简单。
动态路由是网络中的路由器之间相互通信，传递路由信息，利用收到的路由信息更新路由器表的过程。是基于某种路由协议来实现的。常见的路由协议类型有：距离向量路由协议（如 RIP）和链路状态路由协议（如 OSPF）。路由协议定义了路由器在与其它路由器通信时的一些规则。动态路由协议一般都有路由算法。其路由选择算法的必要步骤
1、向其它路由器传递路由信息；
2、接收其它路由器的路由信息；
3、根据收到的路由信息计算出到每个目的网络的最优路径，并由此生成路由选择表；
4、根据网络拓扑的变化及时的做出反应，调整路由生成新的路由选择表，同时把拓扑变化以路由信息的形式向其它路由器宣告。
动态路由适用于网络规模大、拓扑复杂的网络。
动态路由特点：
1、无需管理员手工维护，减轻了管理员的工作负担。
2、占用了网络带宽。
3、在路由器上运行路由协议，使路由器可以自动根据网络拓朴结构的变化调整路由条目；

※VLAN 和 VPN 有什么区别？分别实现在 OSI 的第几层？

VPN 是一种三层封装加密技术，VLAN 则是一种第二层的标志技术（尽管 ISL 采用封装），尽管用户视图有些相象，但他们不应该是同一层次概念。
VLAN（Virtual Local Area Network）即虚拟局域网，是一种通过将局域网内的设备逻辑地而不是物理地划分成一个个网段从而实现虚拟工作组的新兴技术。
VLAN 在交换机上的实现方法，可以大致划分为 2 大类：基基于端口划分的静态 VLAN；
2、基于 MAC 地址|IP 等划分的动态 VLAN。当前主要是静态 VLAN 的实现。
跨交换机 VLAN 通讯通过在 TRUNK 链路上采用 Dot1Q 或 ISL 封装（标识）技术。
VPN（虚拟专用网）被定义为通过一个公用网络（通常是因特网）建立一个临时的、安全的连接，是一条穿过混乱的公用网络的安全、稳定的隧道。
VPN 使用三个方面的技术保证了通信的安全性：隧道协议、数据加密和身份验证。
■VPN 使用两种隧道协议：点到点隧道协议（PPTP）和第二层隧道协议（L2TP）。

■VPN 采用何种加密技术依赖于 VPN 服务器的类型，因此可以分为两种情况。
对于 PPTP 服务器，将采用 MPPE 加密技术 MPPE 可以支持 40 位密钥的标准加密方案和 128 位密钥的增强加密方案。只有在 MS-CHAP、MS-CHAP v2 或 EAP/TLS 身份验证被协商之后，数据才由 MPPE 进行加密，MPPE 需要这些类型的身份验证生成的公用客户和服务器密钥。
对于 L2TP 服务器，将使用 IPSec 机制对数据进行加密 IPSec 是基于密码学的保护服务和安全协议的套件。IPSec 对使用 L2TP 协议的 VPN 连接提供机器级身份验证和数据加密。在保护密码和数据的 L2TP 连接建立之前，IPSec 在计算机及其远程 VPN 服务器之间进行协商。IPSec 可用的加密包括 56 位密钥的数据加密标准 DES 和 56 位密钥的三倍 DES (3DES)。
■VPN 的身份验证方法
前面已经提到 VPN 的身份验证采用 PPP 的身份验证方法，下面介绍一下 VPN 进行身份验证的几种方法。
CHAP CHAP 通过使用 MD5（一种工业标准的散列方案）来协商一种加密身份验证的安全形式。CHAP 在响应时使用质询-响应机制和单向 MD5 散列。用这种方法，可以向服务器证明客户机知道密码，但不必实际地将密码发送到网络上。
MS-CHAP 同 CHAP 相似，微软开发 MS-CHAP 是为了对远程 Windows 工作站进行身份验证，它在响应时使用质询-响应机制和单向加密。而且 MS-CHAP 不要求使用原文或可逆加密密码。
MS-CHAP v2 MS-CHAP v2 是微软开发的第二版的质询握手身份验证协议，它提供了相互身份验证和更强大的初始数据密钥，而且发送和接收分别使用不同的密钥。如果将 VPN 连接配置为用 MS-CHAP v2 作为唯一的身份验证方法，那么客户端和服务器端都要证明其身份，如果所连接的服务器不提供对自己身份的验证，则连接将被断开。
EAP EAP 的开发是为了适应对使用其他安全设备的远程访问用户进行身份验证的日益增长的需求。通过使用 EAP，可以增加对许多身份验证方案的支持，其中包括令牌卡、一次性密码、使用智能卡的公钥身份验证、证书及其他身份验证。对于 VPN 来说，使用 EAP 可以防止暴力或词典攻击及密码猜测，提供比其他身份验证方法（例如 CHAP）更高的安全性。
在 Windows 系统中，对于采用智能卡进行身份验证，将采用 EAP 验证方法；对于通过密码进行身份验证，将采用 CHAP、MS-CHAP 或 MS-CHAP v2 验证方法。

※关于 VPN

一、VPN（Virtual Private Network）：虚拟专用网络，是一门网络新技术，为我们提供了一种通过公用网络安全地对企业内部专用网络进行远程访问的连接方式。
二、VPN 使用三个方面的技术保证了通信的安全性：隧道协议、身份验证和数据加密。
三、1.隧道技术是 VPN 的基本技术，类似于点对点连接技术，它在公用网建立一条数据通道（隧道），让数据包通过这条隧道传输。隧道是由隧道协议形成的，分为第二、三层隧道协议。第二层隧道协议是先把各种网络协议封装到 PPP 中，再把整个数据包装入隧道协议中。这种双层封装方法形成的数据包靠第二层协议进行传输。第二层隧道协议有 L2F、PPTP、L2TP 等。L2TP 协议是目前 IETF 的标准，由 IETF 融合 PPTP 与 L2F 而形成。

2、第三层隧道协议是把各种网络协议直接装入隧道协议中，形成的数据包依靠第三层协议进行传输。第三层隧道协议有 VTP、IPSec 等。IPSec（IP Security）是由一组 RFC 文档组成，定义了一个系统来提供安全协议选择、安全算法，确定服务所使用密钥等服务，从而在 IP 层提供安全保障。

四、VPN 的身份验证方法：1、PPP 的身份验证方法；2、CHAP：CHAP 通过使用 MD5（一种工业标准的散列方案）来协商一种加密身份验证的安全形式。CHAP 在响应时使用质询-响应机制和单向 MD5 散列。用这种方法，可以向服务器证明客户机知道密码，但不必实际地将密码发送到网络上。3、MS- CHAP：同 CHAP 相似，微软开发 MS-CHAP 是为了对远程 Windows 工作站进行身份验证，它在响应时使用质询-响应机制和单向加密。而且 MS- CHAP 不要求使用原文或可逆加密密码。4、MS-CHAP v2：MS-CHAP v2 是微软开发的第二版的质询握手身份验证协议，它提供了相互身份验证和更强大的初始数据密钥，而且发送和接收分别使用不同的密钥。如果将 VPN 连接配置为用 MS-CHAP v2 作为唯一的身份验证方法，那么客户端和服务器端都要证明其身份，如果所连接的服务器不提供对自己身份的验证，则连接将被断开。5、EAP：EAP 的开发是为了适应对使用其他安全设备的远程访问用户进行身份验证的日益增长的需求。通过使用 EAP，可以增加对许多身份验证方案的支持，其中包括令牌卡、一次性密码、使用智能卡的公钥身份验证、证书及其他身份验证。对于 VPN 来说，使用 EAP 可以防止暴力或词典攻击及密码猜测，提供比其他身份验证方法（例如 CHAP）更高的安全性。 6、在 Windows 系统中，对于采用智能卡进行身份验证，将采用 EAP 验证方法；对于通过密码进行身份验证，将采用 CHAP、MS-CHAP 或 MS- CHAP v2 验证方法。

五、VPN 的加密技术。VPN 采用何种加密技术依赖于 VPN 服务器的类型，因此可以分为两种情况。1、

对于 PPTP 服务器，将采用 MPPE 加密技术 MPPE 可以支持 40 位密钥的标准加密方案和 128 位密钥的增强加密方案。只有在 MS-CHAP、MS- CHAP v2 或 EAP/TLS 身份验证被协商之后，数据才由 MPPE 进行加密，MPPE 需要这些类型的身份验证生成的公用客户和服务器密钥。2、对于 L2TP 服务器，将使用 IPSec 机制对数据进行加密 IPSec 是基于密码学的保护服务和安全协议的套件。IPSec 对使用 L2TP 协议的 VPN 连接提供机器级身份验证和数据加密。在保护密码和数据的 L2TP 连接建立之前，IPSec 在计算机及其远程 VPN 服务器之间进行协商。IPSec 可用的加密包括 56 位密钥的数据加密标准 DES 和 56 位密钥的三倍 DES（3DES）

六、VPN 有三种解决方案，用户可以根据自己的情况进行选择。这三种解决方案分别是：远程访问虚拟网（AccessVPN）、企业内部虚拟网（IntranetVPN）和企业扩展虚拟网（ExtranetVPN），这三种类型的 VPN 分别与传统的远程访问网络、企业内部的 Intranet 以及企业网和相关合作伙伴的企业网所构成的 Extranet 相对应。

※以思科路由器为例,你写下单臂路由的配置命令？

答：router(config)#interface f0/1.1
router(config-if)#encapsulation dotlQ 100
router(config-if)#ip add 192.168.1.1 255.255.255.0
router(config-if)#no shutdown
router(config-if)#interface f0/1.2
router(config-if)#i encapsulation dotlQ 200

router(config-if)#i ip add 192.168.2.1 255.255.255.0
router(config-if)#no shutdown

※STP 协议的主要用途是什么？为什么要用 STP

主要用途：1、STP 通过阻塞冗余链路，来消除桥接网络中可能存在的路径回环；2、当前活动路径发生故障时，STP 激活冗余链路恢复网络连通性。
原因：交换网络存在环路时引起：广播环路（广播风暴）；桥表损坏。

※介绍一下 ACL 和 NAT？NAT 有几种方式？

ACL：1、访问控制列表（ACL）是应用在路由器接口的指令列表（规则），用来告诉路由器哪些数据包可以接收转发，哪些数据包需要拒绝；2、ACL 的工作原理 ：读取第三层及第四层包头中的信息，根据预先定义好的规则对包进行过滤；3、使用 ACL 实现网络控制：实现访问控制列表的核心技术是包过滤；4、ACL 的两种基本类型（标准访问控制列表；扩展访问控制列表）
NAT：改变 IP 包头使目的地址，源地址或两个地址在包头中被不同地址替换。
静态 NAT、动态 NAT、PAT

※STP 的判定过程？
答： STP 判定步骤为：①确定根网桥，使用网桥 ID；②计算到根网桥的最小根路径成本；③确定最小的发送方网桥 ID；④确定最小的端口 ID。
STP 过程为：①选根网桥 ②在每个非根网桥上选择根端口 ③在每个网段上标定一个指定端口

※HSRP 是什么?它是如何工作的？
答：HSRP 是热备份路由协议，思科专有。通过 HSRP，一组路由器可以一起协同工作，来代表一台虚拟路由器，备份组像一台路由器一样工作，一个虚拟 IP 地址和 MAC 地址，从末端主机来看，虚拟主路由器是一台有自己 IP 地址和 MAC 地址的路由器，它不同于实际物理路由器，那么该组中一台路由器失效则另一台路由器接替工作，路由选择照常。

※PPP 协议组成及简述协议协商的基本过程？
一、PPP（Point-to-Point Protocol 点到点协议）是为在同等单元之间传输数据包这样的简单链路设计的链路层协议。设计目的主要是用来通过拨号或专线方式建立点对点连接发送数据，使其成为各种主机、网桥和路由器之间简单连接的一种共通的解决方案。
二、PPP 协议中提供了一整套方案来解决链路建立、维护、拆除、上层协议协商、认证等问题。
三、PPP 协议包含这样几个部分：链路控制协议 LCP（Link Control Protocol）；网络控制协议 NCP（Network Control Protocol）；认证协议，最常用的包括口令验证协议 PAP（Password Authentication Protocol）和挑战握手验证协议 CHAP（Challenge-Handshake Authentication Protocol）。
四、一个典型的链路建立过程分为三个阶段：创建阶段、认证阶段和网络协商阶段。

阶段 1：创建 PPP 链路

LCP 负责创建链路。在这个阶段，将对基本的通讯方式进行选择。链路两端设备通过 LCP 向对方发送配置信息报文（Configure Packets）。一旦一个配置成功信息包（Configure-Ack packet）被发送且被接收，就完成了交换，进入了 LCP 开启状态。

应当注意，在链路创建阶段，只是对验证协议进行选择，用户验证将在第 2 阶段实现。

阶段 2：用户验证

在这个阶段，客户端会将自己的身份发送给远端的接入服务器。该阶段使用一种安全验证方式避免第三方窃取数据或冒充远程客户接管与客户端的连接。在认证完成之前，禁止从认证阶段前进到网络层协议阶段。如果认证失败，认证者应该跃迁到链路终止阶段。

在这一阶段里，只有链路控制协议、认证协议，和链路质量监视协议的 packets 是被允许的。在该阶段里接收到的其他的 packets 必须被静静的丢弃。

最常用的认证协议有口令验证协议（PAP）和挑战握手验证协议（CHAP）。 认证方式介绍在第三部分中介绍。

阶段 3：调用网络层协议

认证阶段完成之后，PPP 将调用在链路创建阶段（阶段 1）选定的各种网络控制协议（NCP）。选定的 NCP 解决 PPP 链路之上的高层协议问题，例如，在该阶段 IP 控制协议（IPCP）可以向拨入用户分配动态地址。

这样，经过三个阶段以后，一条完整的 PPP 链路就建立起来了。

五、认证方式

1）口令验证协议（PAP）

PAP 是一种简单的明文验证方式。NAS（网络接入服务器，Network Access Server）要求用户提供用户名和口令，PAP 以明文方式返回用户信息。很明显，这种验证方式的安全性较差，第三方可以很容易的获取被传送的用户名和口令，并利用这些信息与 NAS 建立连接获取 NAS 提供的所有资源。所以，一旦用户密码被第三方窃取，PAP 无法提供避免受到第三方攻击的保障措施。

2）挑战-握手验证协议（CHAP）

CHAP 是一种加密的验证方式，能够避免建立连接时传送用户的真实密码。NAS 向远程用户发送一个挑战口令（challenge），其中包括会话 ID 和一个任意生成的挑战字串（arbitrary challengestring）。远程客户必须使用 MD5 单向哈希算法（one-way hashing algorithm）返回用户名和加密的挑战口令，会话 ID 以及用户口令，其中用户名以非哈希方式发送。

CHAP 对 PAP 进行了改进，不再直接通过链路发送明文口令，而是使用挑战口令以哈希算法对口令进行加密。因为服务器端存有客户的明文口令，所以服务器可以重复客户端进行的操作，并将结果与用户返回的口令进行对照。CHAP 为每一次验证任意生成一个挑战字串来防止受到再现攻击（replay attack）。在整个连接过程中，CHAP 将不定时的向客户端重复发送挑战口令，从而避免第 3 方冒充远程客户（remote client impersonation）进行攻击。

六、PPP 协议的应用

PPP 协议是目前广域网上应用最广泛的协议之一，它的优点在于简单、具备用户验证

能力、可以解决 IP 分配等。

家庭拨号上网就是通过 PPP 在用户端和运营商的接入服务器之间建立通信链路。目前，宽带接入正在成为取代拨号上网的趋势，在宽带接入技术日新月异的今天，PPP 也衍生出新的应用。典型的应用是在 ADSL（非对称数据用户环线，Asymmetrical Digital Subscriber Loop）接入方式当中，PPP 与其他的协议共同派生出了符合宽带接入要求的新的协议，如 PPPoE（PPP over Ethernet），PPPoA（PPP over ATM）。

利用以太网（Ethernet）资源，在以太网上运行 PPP 来进行用户认证接入的方式称为 PPPoE。PPPoE 即保护了用户方的以太网资源，又完成了 ADSL 的接入要求，是目前 ADSL 接入方式中应用最广泛的技术标准。

同样，在 ATM（异步传输模式，Asynchronous Transfer Mode）网络上运行 PPP 协议来管理用户认证的方式称为 PPPoA。它与 PPPoE 的原理相同，作用相同；不同的是它是在 ATM 网络上，而 PPPoE 是在以太网网络上运行，所以要分别适应 ATM 标准和以太网标准。

PPP 协议的简单完整使它得到了广泛的应用，相信在未来的网络技术发展中，它还可以发挥更大的作用。