网络学员面试常见问题：

1．请你修改一下 LINUX 的视频驱动和声音驱动

答： redhatlinux 中用 sndconfig 来设置声卡，如果没有某个模块，就需要重新编译内核(编译最新发布的 linux 内核)，如果还不行，只好用 ALSA 音效驱动程式. Redhat-config-

2．请你修改一下 LINUX 的启动速度

1.运行级别设为 3 2.chkconfig 从中可以关掉一些不需要的服务，如 sendmail

4．请你说下怎么取消 APACHE 的目录索引

Apache 中第一个目录设置都是在

<Directory>

</Directory>

在他们之间的里面会有一个 options 的选项后面如果有 indexes 选项的话就是说如果在目录下找不到主文件的话就把目录下的内容列出来如 FTP 一样你把那个 indexes 去掉就好了

5．热备份路由(HSRP)的实现方法

答：通过共享一个 IP 地址和 MAC 地址，两个或者多个路由器可以作为一个虚拟路由器，当某个路由器按计划停止工作，或出现预料之外的故障时，其他路由器能够无缝的接替它进行路由选择。这使得 LAN 内的主机能够持续的向同一个 IP 地址和 MAC 地址发送 IP 数据包，路由器的故障切换对主机和其上的会话是透明的。已经开始的 TCP 会话也可以承受故障切换

6．负载(集群)的实现方法

两台计算机和一个磁盘柜是主要的硬件设备，每太计算机上有两块网卡，其中的一快网卡相互连接，来贞听心跳指数，另一块网卡连接公共网络，当一台计算机 DOWN 机以后，另外一台计算机通过心跳指数来判断，然后自己接替另外一台计算机的工作，他们的数据放在公共的磁盘柜里。这样可以使他们提供服务数据的一致性。

7．ACPHE 的实现方法

1. 基本配置

KeepAlive 设置问 on

MaxClient 5000 设置客户端最大清楚数量 5000

ServerAdmin root@aiyh.com 设置管理员的 e-mail

ServerName aiyh.com 设置服务器的 FQDN

DiretcoryIndex index.html index.php index.htm index.cgi 设置服务器默认文档

2. 分割配置任务

在主配置文件中加入以下内容

<Directory "/var/www/html/private">

AllowOverride Options

</Directory>

然后到“/var/www/html/private”目录下建立”.htaccess”文件

在里写上 “Options -Indexes”

重新启动 httpd 服务 # service httpd restart

3. 配置每个用户的 WEB 站点

修改主配置文件 http.conf

加入：

<IfModule mod_userdir.c>

UserDir disable root 禁止 root 用户使用个人站点

Userdir public_html 每个用户 WEB 站点的目录

</IfModule>

去掉：

```
<Directory /home/*/public_html>
    AllowOverride FileInfo AuthConfig Limit Indexes
    Options MultiViews Indexes SymLinksIfOwnerMatch IncludesNoExec
    <Limit GET POST OPTIONS PROPFIND>
        Order allow,deny
        Allow from all
    </Limit>
    <LimitExcept GET POST OPTIONS PROPFIND>
        Order deny,allow
        Deny from all
    </LimitExcept>
</Directory>
```

前面的注释内容

在每个用户的主目录下建立 public_html 站点目录。在站点目录中建立网页

设置用户目录的权限为 744 如果是动态网页根据需求设置权限

4. 认证和授权

在主配置文件中加入以下内容

```
<Directory "/var/www/html/private">          对/var/www/html/private 目录认证
    AllowOverride None                  不使用.htaccess 文件
    AuthType Basic                      认证模式
    AuthName "benet"                    提示信息
    AuthUserFile /var/www/passwd/benet    密码文件存放路径
    require valid-user                  授权给人证口令文件中的所有用户
</Directory>
```

在 /var/www/passwd/下生成密码文件 #htpasswd -c <passwd-file> <user>

#htpasswd -c benet benet

修改密码文件的权限为 apache

#chown apache.apache benet

重新启动 http 服务

8．DNS 的实现方法

DNS 的全称是（Domain name system）有迭代查询和递归查询两种方式

9．防火墙(LINUX)的实现方法

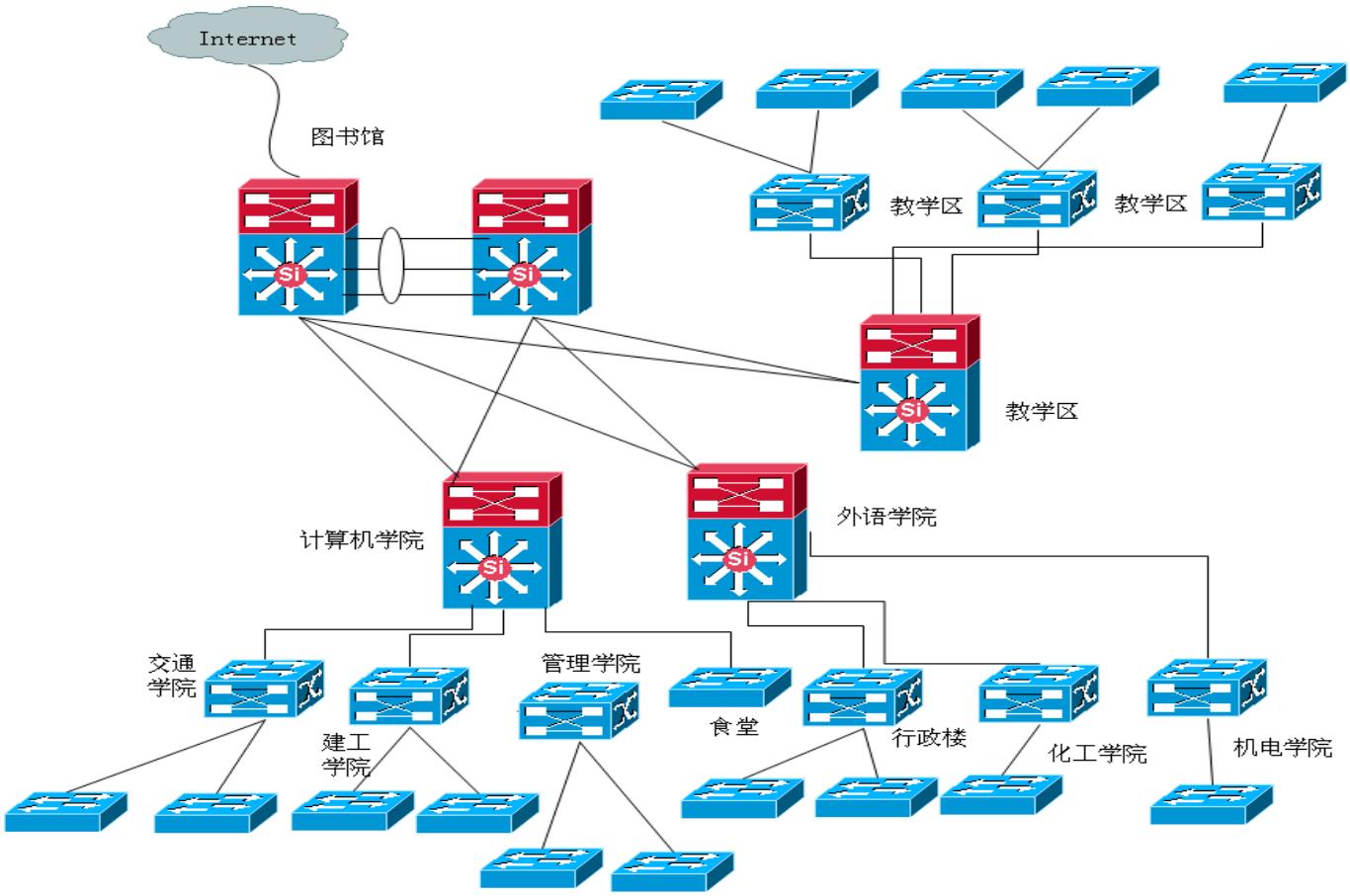
10．WEB 服务器的负载均衡？

在网卡属性上有个负载均衡，然后在两台计算机上写上他们共有的 IP 地址，就可以实现负载均衡了。

11．设计一个校园网络方案（画出拓扑图）

A 用 D-LINK 产品（D-LINK 是猫，单机上网用的； TP-LINK 是路由器，多机上网用的）

B 用 CISCO 产品



A 用 D-LINK 产品

B 用 CISCO 产品

12．设计一个电子政务系统（画出图）写出设计要点

13．写出常用几种网络操作系统的优缺点

答：Linux 是免费的软件，源代码公开，支持多用户，多进程，多线程，实时性较好，功能强大而且稳定，易用性较差。

Windows 对客户端软件和多媒体软件的支持较好，易用性强

14．用你自己熟悉的网络产品设计电子银行管理系统

15．raid0、1、5 的特点和优点。

答：

类型	特点	优点
raid0	两块磁盘、没有冗余	速度快
raid1	偶数块容量相同的磁盘构成	提供冗余
raid5	三块以上容量相同的磁盘构成	容错功能好，速度快

16．SMTP，POP3 端口号。

答：SMTP TCP 25

POP3 TCP 110

17．OSI 七层模型。

答：OSI (Open System Internetwork)

应用层 （application layer）

表示层 （presentation layer）

会话层 （session layer）

传输层 （transport layer）

网络层 （network layer）

数据链路层 （data link layer）

物理层 （physical layer）

18．添加静态路由命令。

答：**ip route** *network netmask next_hop*

19．LINUX 是实时还是分时操作系统。

答：linux 属于**分时**操作系统

20．浏览网页出现乱码什么原因。

21．VLAN 实现的功能

隔离广播域，实现区域划分

22．IP 子网划分问题。

23．能否将 WIN2000P 升级成 WIN2000S？

答：无法将个人版操作系统升级成服务器版。

24．怎样保证 1 个文档的安全性？

答：可以利用 windows 的 NTFS 权限，对存放该文件的文件夹授予自己可读写，其他人拒绝访问的权限。

再利用加密软件（如 PGP），对文档进行对称加密，确保文档的机密性。

25．SAMBA 实现什么功能？

答：samba 可以在 windows 和 linux 系统之间实现文件和打印机的共享。

26．怎样实现 VLAN 间通信？

在三层上启用路由功能就可以了，在 2 层上要做单臂路由，通过路由器实现 VLAN 通信

27．1 个公有 IP 接入路由器，怎样实现局域网上网？

做代理服务器，或者做 NAT 地址转换，把内网的私有 IP 地址转换成公共 IP 地址。
28．路由器中"sh int" 的意思是什么？
答：查看路由器中的所有端口配置信息。
29．Windows 2000 也有了类似上面的（1 中）界面的工具，叫做什么？
答：“netsh”
30．在 Windows 2000 的 cmd shell 下，输入 netsh 显示什么提示符？输入 int ip 显示什么提示符？输入 dump，我们能看到什么内容？
答：在 command line 下依次输入 netsh、int、ip、dump 显示如下内容：
c:\>netsh
netsh>int
netsh interface>ip
netsh interface ip>dump（在此输入 dump 显示一个配置脚本）
可以看到当前系统的网络配置

31．对于 Windows 95 和 Windows 98 的客户机，使用 winipcfg 命令还是 ipconfig 命令？
答：Windows 95 和 Windows 98 的客户机使用 winipcfg 来查看网络配置信息。

32．要给出所有接口的详细配置报告，包括任何已配置的串行端口使用什么命令？
答：在该设备的特权模式下输入 show interface 即可查看到该设备所有接口的详细配置信息。

33．ipconfig /all 命令的作用？
答：可以用于查看所有网络连接的详细信息。

34．使用 Ping 命令的作用？
答：ping 命令主要用于测试网络的连通性。

35．使用 Ping 命令的一般步骤：
答：<1>ping 127.0.0.1 查看 TCP/IP 协议及配置是否正确；
<2>ping <本机 IP 地址> 验证是否正确地添加到网络；
<3>ping <网关 IP 地址> 验证网关是否运行以及能否与本地主机通讯；
<4>ping <远程 IP 地址> 验证能否通过路由器通讯；通则说明正常，不通说明线路可能存在问题
或使用了防火墙。

36．再用 ping 命令时如果用地址成功，但是用名称 Ping 失败，则问题有可能处在什么地方？为什么？
答：问题可能出在主机到名称服务器这段范围内，由于名称服务器（DNS）无法为主机解析域名（不能
将 IP 地址和域名相对应），所以 ping 地址成功，而 ping 名称会失败。

37．如果在任何点上都无法成功地使用 Ping 命令怎么办？
答：

38．说说 ARP 的解析过程。

答：ARP 用于把一个已知的 IP 地址解析成 MAC 地址，以便在 MAC 层通信。为了确定目标的 MAC 地址，首先查找 ARP 缓存表。如果要查找的 MAC 地址不在表中，ARP 会发送一个广播，从而发现目的地的 MAC 地址，并记录到 ARP 缓存表中以便下次查找。

39．说说你知道的防火墙及其应用。
防火墙可以隔离内部网络和外部网络，能限制内部网络的行为，能防止外部网络的攻击，
40．ATM 的禎 格式。

41．输入网址到网页打开数据经过的过程
答：<1>客户端输入网址，请求与服务器的 80 端口建立连接。
<2>服务器收到请求，并响应客户端；
<3>客户端接收到服务器的响应，准备开始接收数据。服务器开始发送数据。
（三次握手）
第 1 次握手：客户端通过将一个含有“同步序列号（SYN）”标志位的数据段发送给服务器请求连接。
第 2 次握手：服务器用一个带有“确认应答（ACK）”和“同步序列号（SYN）”标志位的数据段响应客户端。
第 3 次握手：客户端发送一个数据段确认收到服务器的数据段，并开始传送实际数据。

42．TCP/IP 中各个字母代表的含义
答：Transmission Control Protocol / Internet Protocol

43. 端口镜像是怎么实现的？
配置 Catalyst 交换端口分析器（SPAN）

介绍
交换端口分析器（SPAN）功能有时被称为端口镜像或端口监控，该功能可通过网络分析器（例如交换机探测设备或者其它远程监控（RMON）探测器）选择网络流量进行分析。以前，SPAN 是 Catalyst 交换机族较为基本的功能，但最新推出的 CatOS 有许多增强功能，而且有许多功能是用户现有才开始使用的。本文并不是 SPAN 功能的又一种配置指南，而是立足于介绍已实施的 SPAN 的最新功能。本文将对 SPAN 的一般问题进行回答 ，例如：
SPAN 是什么？我如何对它进行配置？
有什么不同的功能（尤其是同时进行多个 SPAN 话路）？需要何种级别的软件来执行这些功能？
SPAN 是否会影响交换机的性能？
开始配置前
规则
有关详情，请参阅 Cisco 技术提示规则。
SPAN 简要介绍
SPAN 是什么？为什么需要 SPAN？ 在交换机上引入 SPAN 功能，是因为交换机和集线器有着根本的差异。当集线器在某端口上接收到一个数据包时，它将向除接收该数据包端口之外的其它所有端口发送一份数据包的拷贝。当交换机启动时，它将根据所接收的不同数据包的源 MAC 地址开始建立第 2 层转发表。一旦建立该转发表，交换机将把指定了 MAC 地址的业务直接转发至相关端口。

例如，如果您想要截获从主机 A 发送至主机 B 的以太网业务，而两台主机是用集线器相连的，那么只要在该集线器上安装一嗅探器，所有端口均可看见主机 A 和主机 B 之间的业务：

在交换机中，当知道了主机 B 的 MAC 地址之后，从主机 A 到主机 B 的单播业务仅被转发至主机 B 的端口，因此，嗅探器看不见：

在这个配置中，嗅探器将仅截获扩散至所有端口的业务，例如广播业务、具有 CGMP 或者 IGMP 侦听禁止的组播业务以及未知的单播业务。当交换机的 CAM 表中没有目的地的 MAC 时，将发生单播泛滥。它无法理解向何处发送业务，而将数据包大量发送至 VLAN 中的所有端口。
将主机 A 发送的单播数据包人工复制到嗅探器端口需要一些附加功能来实现。

在上面的图表中，与嗅探器相连的端口配置为：对主机 A 发送的每一个数据包拷贝进行接收。该端口被称为 SPAN 端口。下文各节将说明如何对该功能进行精确的调节，使其作用不仅仅限于监控端口。
SPAN 术语
· 入口业务： 进入交换机的业务。
· 出口业务： 离开交换机的业务。
· 源（SPAN）端口： 用 SPAN 功能受监控的端口。
· 目的地（SPAN）端口： 监控源端口的端口，通常连有一个网络分析器。
· 监控端口：在 Catalyst2900xl/3500xl/2950 术语中，监控端口也是目的地 SPAN 端口。
本地 SPAN：● 当被监控端口全部位于同一交换机上作为目的地端口时，SPAN 功能为本地 SPAN 功能。这和下文中的远程 SPAN 形成对比。
远程 SPAN 或者 RSPAN：● 作为目的地端口的某些源端口没有位于同一交换机上。这是一项高级功能，要求有专门的 VLAN 来传送该业务，并由交换机之间的 SPAN 进行监控。并非所有交换机均支持 RSPAN，所以，请检查各自的版本说明或者配置指南，来核实您要进行配置的交换机是否可以使用该功能。
● PSPAN： 指基于端口的 SPAN。用户对交换机指定一个或者数个源端口以及一个目的地端口。
VSPAN:● 指基于 VLAN 的 SPAN。在给定的交换机中，用户可以使用单个命令来选择对属于专门 VLAN 的所有端口进行监控。
ESPAN● ESPAN 指 SPAN 增强版本。该术语在 SPAN 的发展期间数次用于命名新增功能，因此意义并不很明确。在本文中避免使用该术语。
管理源：● 已配置受监控的源端口或者 VLAN 的列表。
操作源：● 受到有效监控的端口列表。这可能和管理源有所不同。例如，在关闭模式下的端口可能在管理源中出现，但它不受到有效监控。

[page]
所用的组件
本文使用 CatOS 5.5 作为 Catalyst 4000、5000 以及 6000 族的参考。在 Catalyst 2900XL/3500XL 族中使用了 Cisco IOS(r)软件版本 12.0（5）XU。虽然本文以后会根据 SPAN 的变化而更新，但有关 SPAN 功能的最新发展情况，请参阅文档的版本说明。
本文中所提供的信息是在从特殊实验室环境下的设备中产生的。本文中所使用的所有设备均以缺省配置启动。如果您是在实际网络中作业，请确保您在使用所有命令之前，已了解这些命令可能产生的影响。.

Catalyst 2900XL/3500XL 交换机上的 SPAN
提供的功能及限制
Catalyst 2900XL/3500XL 中的端口监控功能没有太过扩展，因此比较容易理解。
您可以根据需要创建多个本地 PSPAN 话路。例如，您可以在您选作目的地 SPAN 端口的端口配置创建 PSPAN 话路，只需用 端口监视 <interface> 命令列出您想监控的源端口即可。在 Catalyst 2900XL/3500XL 的术语中，监控端口其实是目的地 SPAN 端口。
· 主要限制在于：与给定话路相关的所有端口（无论源端口还是目的地端口）必须属于同一 VLAN。.
· 如果您没有在端口监控命令中指定任何接口，则作为接口的所有其它属于同一 VLAN 的端口将受到监控。
以下限制，摘自 Catalyst 2900XL/3500XL 的命令参考：
ATM 端口是唯一无法受到监控的端口。然而您还是可以对 ATM 端口进行监控。以下限制适用于具有端口监控能力的各个端口：
· 快速 EthernetChannel 或者千兆 EthernetChannel 端口群中不能有监控端口。
· 因为端口安全性而无法启用监控端口。
· 监控端口不可以是多 VLAN 端口。
· 当端口受到监控时，监控端口必须是同一 VLAN 的成员。对于监控端口以及受到监控的端口，不允许进行 VLAN 成员的改变。
· 监控端口不可以是动态接入端口或者中继端口。但是，静态接入端口可以对中继线上的 VLAN、多 VLAN 或者动态接入端口进行监控。受到监控的 VLAN 与静态接入端口有关联。
· 如果监控器以及受监控端口为受保护端口，端口监控将不起作用。
有关功能冲突的补充信息，请参阅下文的链接：
· 管理交换机——管理配置冲突 -- Catalyst 2900XL/3500XL 系列
请注意，处于监控状态的端口不执行生成树协议（STP），但端口仍然属于其镜像的端口 VLAN。如果端口监控属于某个环路的一部分（例如，当您将其连接至集线器或者网桥，而环接至网络的其它部分时），您可能会以严重的桥接环路状况收尾，因为您不再受到 STP 的保护。请参阅 “为什么我的 SPAN 话路会产生一个桥接环路？”一节， 看一看产生该情况的一个实例。
配置实例
在本例中，创建了两个并行的 SPAN 话路。
· 端口 Fa0/1 将对由端口 Fa0/2 发送、端口 Fa0/5 接收的业务进行监控。它也将对往返于管理接口 VLAN 1 的业务进行监控。
· 端口 Fa0/4 将对端口 Fa0/3 以及 Fa0/6 进行监控。
端口 Fa0/3、Fa0/4 以及 Fa0/6 均在 VLAN 2 中进行配置；其它端口以及管理接口均在默认的 VLAN 1 中进行配置。
网络图

Catalyst 2900XL/3500XL 上的配置样本
Catalyst 2900XL/3500XL 上的配置样本
<snip> ! interface FastEthernet0/1 port monitor FastEthernet0/2 port monitor FastEthernet0/5 port monitor VLAN1 ! interface FastEthernet0/2 ! interface FastEthernet0/3 switchport access vlan 2 ! interface FastEthernet0/4 port monitor FastEthernet0/3 port monitor FastEthernet0/6 switchport access vlan 2 ! interface FastEthernet0/5 ! interface FastEthernet0/6 switchport access vlan 2 ! <snip> ! interface VLAN1 ip address 10.200.8.136 255.255.252.0 no ip directed-broadcast no ip route-cache ! <snip>

配置步骤说明
如果要将端口 Fa0/1 配置为源端口 Fa0/2、Fa0/5 以及管理接口的目的端口，请在配置模式中选择接口 Fa0/1：
● Switch(config)#int fa0/1

Enter the list of ports to be monitored:
● Switch(config-if)#port monitor fastEthernet 0/2
Switch(config-if)#port monitor fastEthernet 0/5

然后，这两个端口接收的或者发送的数据包也会被复制到端口 Fa0/1。使用另一版本的 port monitor 命令对管理接口的监控进行配置：
Switch(config-if)#port monitor VLAN 1●

注：?/B>上文中的命令并不意味着端口 Fa0/1 将监控整个 VLAN 1。VLAN 1 关键字仅指交换机的管理接口。
● 输入以下命令说明在不同 VLAN 中监控某个端口是不可能的：
Switch(config-if)#port monitor fastEthernet● 0/3
FastEthernet0/1 and FastEthernet0/3 are in different vlan
To finish the configuration, configure another session, this time using Fa0/4 as a destination SPAN port:
Switch(config-if)#int fa0/4●
Switch(config-if)#port monitor fastEthernet 0/3
Switch(config-if)#port monitor fastEthernet 0/6
Switch(config-if)#^Z

检查配置情况的最佳方法是发出简单的 show running 命令，或者使用 show port monitor 命令：
Switch#show port monitor●
Monitor Port Port Being Monitored
--- ---
FastEthernet0/1 VLAN1
FastEthernet0/1 FastEthernet0/2
FastEthernet0/1 FastEthernet0/5
FastEthernet0/4 FastEthernet0/3
FastEthernet0/4 FastEthernet0/6
注：?/B>Catalyst 2900XL 以及 3500XL 不支持单一接收方向的 SPAN（Rx SPAN 或者入口 SPAN）或者单一发送方向的 SPAN（Tx SPAN 或者出口 SPAN）。所有配置 SPAN 的受控端口必须既能进行业务接收（Rx）又能进行业务发送（Tx）。

华为

【3026 等交换机镜像】

S2008/S2016/S2026/S2403H/S3026 等交换机支持的都是基于端口的镜像，有两种方法：

方法一

1. 配置镜像（观测）端口 [SwitchA]monitor-port e0/8
2. 配置被镜像端口 [SwitchA]port mirror Ethernet 0/1 to Ethernet 0/2

方法二

1. 可以一次性定义镜像和被镜像端口

[SwitchA]port mirror Ethernet 0/1 to Ethernet 0/2 observing-port Ethernet 0/8

【8016 交换机端口镜像配置】

1. 假设 8016 交换机镜像端口为 E1/0/15，被镜像端口为 E1/0/0，设置端口 1/0/15 为端口镜像的观测端口。

[SwitchA] port monitor ethernet 1/0/15

2. 设置端口 1/0/0 为被镜像端口，对其输入输出数据都进行镜像。

[SwitchA] port mirroring ethernet 1/0/0 both ethernet 1/0/15

也可以通过两个不同的端口，对输入和输出的数据分别镜像

1. 设置 E1/0/15 和 E2/0/0 为镜像（观测）端口

[SwitchA] port monitor ethernet 1/0/15

2. 设置端口 1/0/0 为被镜像端口，分别使用 E1/0/15 和 E2/0/0 对输入和输出数据进行镜像。

[SwitchA] port mirroring gigabitethernet 1/0/0 ingress ethernet 1/0/15
[SwitchA] port mirroring gigabitethernet 1/0/0 egress ethernet 2/0/0

『基于流镜像的数据流程』
基于流镜像的交换机针对某些流进行镜像，每个连接都有两个方向的数据流，对于交换机来说这两个数据流是要分开镜像的。

【3500/3026E/3026F/3050】

〖基于三层流的镜像〗

1. 定义一条扩展访问控制列表

[SwitchA]acl num 101

2. 定义一条规则报文源地址为 1.1.1.1/32 去往所有目的地址

[SwitchA-acl-adv-101]rule 0 permit ip source 1.1.1.1 0 destination any

3. 定义一条规则报文源地址为所有源地址目的地址为 1.1.1.1/32

[SwitchA-acl-adv-101]rule 1 permit ip source any destination 1.1.1.1 0

4. 将符合上述 ACL 规则的报文镜像到 E0/8 端口

[SwitchA]mirrored-to ip-group 101 interface e0/8

〖基于二层流的镜像〗
1. 定义一个 ACL
[SwitchA]acl num 200
2. 定义一个规则从 E0/1 发送至其它所有端口的数据包
[SwitchA]rule 0 permit ingress interface Ethernet0/1 (egress interface any)
3. 定义一个规则从其它所有端口到 E0/1 端口的数据包
[SwitchA]rule 1 permit (ingress interface any) egress interface Ethernet0/1
4. 将符合上述 ACL 的数据包镜像到 E0/8
[SwitchA]mirrored-to link-group 200 interface e0/8

【5516】

支持对入端口流量进行镜像

配置端口 Ethernet 3/0/1 为监测端口，对 Ethernet 3/0/2 端口的入流量镜像。

[SwitchA]mirror Ethernet 3/0/2 ingress-to Ethernet 3/0/1

【6506/6503/6506R】

目前该三款产品只支持对入端口流量进行镜像，虽然有 outbount 参数，但是无法配置。
镜像组名为 1，监测端口为 Ethernet4/0/2，端口 Ethernet4/0/1 的入流量被镜像。
[SwitchA]mirroring-group 1 inbound Ethernet4/0/1 mirrored-to Ethernet4/0/2

44.在BOOT.INI文件中，将TIMEOUT设置为-1，那么（ ）开机。 A.不等待 B.等待1S C.默认

启动　D.延　长1S

The timeout is changed by editing the boot.ini file which is on the boot partition and changing the timeout parameter:

1. Start a command session (Start - Run - Command)
2. Set the attributes on c:\boot.ini to non-read and non-system
   attrib c:\boot.ini -r -s
3. Edit the file and change the timeout to -1
   [boot loaded]
   timeout = -1
4. Save your changes and set the file back to read only and system
   attrib c:\boot.ini +r +s

if you do like this the boot menu will show forever!
应该是永久显示启动菜单（选项中没有此项？）

3.一台电脑上有2快物理硬盘,最多能建立多少个活动分区?
A.2　B.3　C.1　D.8
每块硬盘只能分四个主分区，并且只有一个分区是活动的，它是系统开机读入MBR之后默认访问的分区，从这个分区的引导扇区读入引导该分区操作系统的信息并引导该系统
4.WINDOWS域的具体实现方式?

可以手动安装域名服务 (DNS) 和 DCPromo（创建 DNS 和 Active Directory 的命令行工具），也可以使用“Windows Server 2003 管理服务器”向导进行安装。本节使用手动工具来完成安装。

使用手动工具安装 DNS 和 Active Directory

1. 单击“开始”按钮，单击“运行”，键入“DCPROMO”，然后单击“确定”。
2. 在出现“Active Directory 安装向导”时，单击“下一步”开始安装。
3. 阅读“操作系统兼容性”信息后，单击“下一步”。
4. 选择“新域的域控制器”（默认），然后单击“下一步”。
5. 选择“在新林中的域”（默认），然后单击“下一步”。
6. 对于“DNS 全名”，键入“contoso.com”，然后单击“下一步”。（这表示一个完全限定的名称。）
7. 单击“下一步”，接受将“CONTOSO”作为默认“域 NetBIOS 名”。（NetBIOS 名称提供向下兼容性。）
8. 在“数据库和日志文件文件夹”屏幕上，将 Active Directory“日志文件文件夹”指向“L:\Windows\NTDS”，然后单击“下一步”继续。
9. 保留“共享的系统卷”的默认文件夹位置，然后单击“下一步”。

10. 在“DNS 注册诊断”屏幕上，单击“在这台计算机上安装并配置 DNS 服务器”。单击“下一步”继续。

11. 选择“只与 Windows 2000 或 Windows Server 2003 操作系统兼容的权限”（默认），然后单击“下一步”。

12. 在“还原模式密码”和“确认密码”中，键入密码，然后单击“下一步”继续。

注意：在生产环境中，应使用复杂的目录服务还原密码。

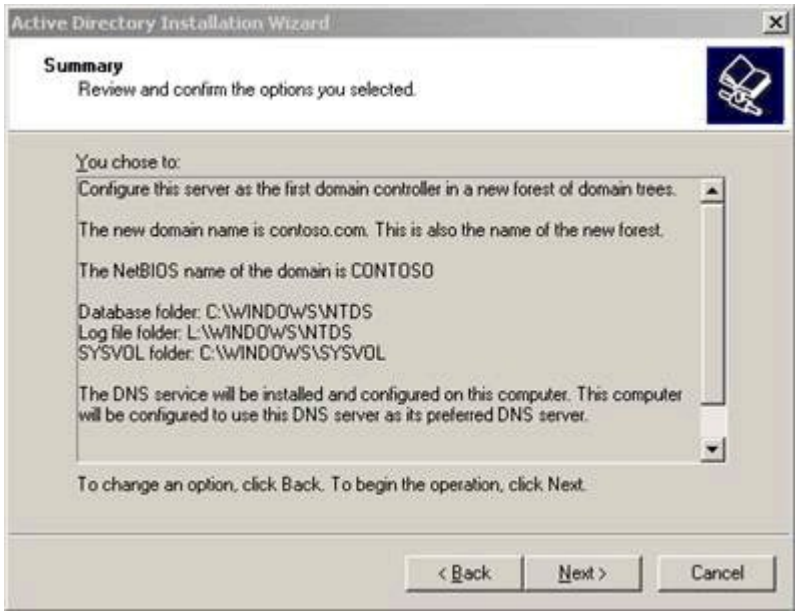


图 3. Active Directory 安装选项摘要

13. 图 3 中显示的是“Active Directory 安装选项摘要”。单击“下一步”开始安装 Active Directory。在出现提示时，请插入 Windows Server 2003 安装 CD。

14. 单击“确定”，对已为 DNS 服务器动态分配了 IP 地址这一提示信息作出确认。

15. 如果有多个网络接口，在“选择连接”下拉列表中选择“10.0.0.0 网络接口”，然后单击“属性”。

16. 在“此连接使用下列项目”部分下面，单击“Internet 协议 (TCP/IP)”，然后单击“属性”。

17. 选择“使用下面的 IP 地址”，然后在“IP 地址”中键入“10.0.0.2”。按两次“Tab”键，然后在“默认网关”中键入“10.0.0.1”。在“首选 DNS 服务器”中键入“127.0.0.1”，然后单击“确定”。单击“关闭”继续。

18. 在“Active Directory 安装向导”完成后，单击“完成”。

19. 单击“立即重新启动”以重新启动计算

5. 国内主要防火墙产品有哪些？各自的性能配置(中新软件公司)

3Com	AboCom(友旺)	ADNS(恒宇视野)	ADTRAN

Amaranten(阿姆瑞特)	**Anton(安盾)**	**Astaro**	**CHECKPOINT**
CISCO(思科)	**D-Link(友讯网络)**	**FORTINET(飞塔)**	**I-SECURITY**
Juniper	**KILL**	**KSMART(金捷)**	**LanGate**
NESCO	**NETGEAR(网件)**	**NUSOFT(新软)**	**OE21(龙兴)**
RESILIENCE	**ShareTech**	**SONICWALL**	**Symantec(赛门铁克)**
VTInfo(网泰)	**WatchGuard**	**Westone(卫士通)**	**ZyXEL(合勤)**
安联	**安氏(iS-One)**	**比威网络**	**东方龙马(OLM)**
东软(Neusoft)	**方正(Founder)**	**华为3Com(华为三康)**	**金浪(KINGNET)**
蓝盾(Bluedon)	**联想(lenovo)**	**诺基亚(NOKIA)**	**清华得实**
清华紫光(thunis)	**清网**	**趋势(TRENDnet)**	**融合网络**
锐捷网络(Ruijie)	**瑞星(RISING)**	**神州盾(SOAR)**	**神州数码**
速通	天融信(TOPSEC)	网新易尚	兴硅谷(SVNET)
兆维	中怡数宽(DWnet)	卓尔	

http://product.it168.com/files/0418search.shtml

热门产品

- 华为3Com Quidway SecPath 100F
- CISCO PIX-515E-R-BUN
- CISCO PIX-525-UR-BUN
- 华为3Com Quidway SecPath 10F
- CISCO PIX-515E-UR-BUN
- CISCO PIX-506E
- CISCO Pix-506E-BUN-K9
- 天融信 NGFW3000-T4
- 神州数码 DCFW-1800E
- CISCO PIX-501
- CISCO PIX-525-R-BUN

- D-Link DFL-100
- CISCO PIX-501-50-BUN-K9
- 华为 3Com Eudemon100
- Juniper NetScreen-25

6. 网络安全防护软件的性能(航安信息科技公司)
金山毒霸2005
1、特别推荐

主动实时升级：
无需用户做任何操作，当有最新的病毒库或者功能出现时，金山毒霸可将此更新自动下载安装。此功能保证您在任何时刻都可以获得与全球同步的最新病毒特征库，防止被新病毒破坏感染，即使面对“冲击波”这样快速传播的病毒，金山毒霸2005也能极大程度的遏制病毒入侵用户计算机！

抢先启动防毒系统：
防毒胜于杀毒，抢先启动的防毒系统可保障在Windows未完全启动时就开始保护用户的计算机系统，早于一切开机自运行的病毒程序，使用户避免“带毒杀毒”的危险。抢先式防毒让您的安全更早一步。

2、经典奉献
主动漏洞修复：
可扫描操作系统及各种应用软件的漏洞，当新的安全漏洞出现时，金山毒霸会下载漏洞信息和补丁，经扫描程序检查后自动帮助用户修补。此功能可确保用户的操作系统随时保持最安全状态，避免利用该漏洞的病毒侵入系统。另外还会扫描系统中存在的诸如简单密码、完全共享文件夹等安全隐患。

跟踪式反间谍：
采用全新的网络程序校验策略。除了传统反黑、拦截木马等功能外，同时对普通应用程序进行跟踪监控。一旦应用程序的大小、内容等属性发生异常变化，系统将特别提醒用户注意，有效防止止木马、间谍软件“冒名顶替”盗取用户数据。

木马防火墙：
通过多种技术，实现对木马进程的查杀。系统中一旦有木马、黑客或间谍程序访问网络，会及时拦截该程序对外的通信访问，然后对内存中的进程进行自动查杀，保护用户网络通信的安全。这对防御盗取用户信息的木马、黑客程序特别有效。
星杀毒软件网络版是一款应用于复杂网络结构的企业级反病毒产品，该产品专门为企业用户量

身定做，使企业轻松构建安全的立体防毒体系。该产品主要适用于企业服务器与客户端，支持WindowsNT/2000/XP、Unix、Linux等多种操作平台，全面满足企业整体反病毒需要。

瑞星杀毒软件网络版创立并实现了“分布处理、集中控制”技术，以系统中心、服务器、客户端、控制台为核心结构，成功地实现了远程自动安装、远程集中控管、远程病毒报警、远程卸载、远程配置、智能升级、全网查杀、日志管理、病毒溯源等功能，它将网络中的所有计算机有机地联系在一起，构筑成协调一致的立体防毒体系。

瑞星杀毒软件网络版采用目前国际上最先进的结构化多层可扩展（SME）技术设计研制的第五代引擎，实现了从预杀式无毒安装、漏洞扫描、特征码判断查杀已知病毒，到利用瑞星专利技术行为判断查杀未知病毒，并通过可疑文件上报系统、嵌入式即时安全信息中心与瑞星中央病毒判别中心构成的信息交互平台，改被动查杀为主动防御，为网络中的个体计算机提供点到点的立体防护
江民杀毒KV2005 9.00.504(2005.1.13)

软件语言：简体中文
授权方式：零售版
软件类别：病毒防治
运行环境：Win9x/WinNT/2000/ME/XP
采用先进的“驱动级编程技术”，能够与操作系统底层技术更紧密结合，具有更好的兼容性，占用系统资源更小。 KV2005突出特点是独创的“系统级深度防护技术”与操作系统互动防毒，彻底改变以往杀毒软件独立于操作系统和防火墙的单一应用模式，开创杀毒软件系统级病毒防护新纪元。据悉，江民对微软的XP SP2安全中心进行了延伸和拓展，在此基础上开发了KV安全中心，不但可以在XP操作系统上应用，WIN98、WIN2000用户同样可以拥有安全中心。同时，KV2005采用了先进的“立体联动防杀技术”，即杀毒软件与防火墙联动防毒、同步升级，对于防范集蠕虫、木马、后门程序等特性于一体的混合型病毒更有效

卡巴斯基(Kaspersky Internet Security) 2006 6.0.9.96 汉化版

软件大小：9005K
软件语言：简体中文
授权方式：免费版
软件类别：病毒防治
运行环境：Win9x/WinNT/2000/ME/XP
软件介绍：

Kaspersky 为任何形式的个体和社团提供了一个广泛的抗病毒解决方案。它提供了所有类型的抗病毒防护：抗病毒扫描仪，监控器，行为阻段和完全检验。它支持几乎是所有的普通操作系统 、e-mail 通路和防火墙。Kaspersky控制所有可能的病毒进入端口，它强大的功能和局部灵活性以及网络管理工具为自动信息搜索、中央安装和病毒防护控制提供最大的便利和最少的时间来建构你的抗病毒分离墙。
这是最新的 Kaspersky 安全套装，包括了反病毒、反黑客、反间谍、反垃圾邮件、前摄防御等全套安全工具，可让你的系统高枕无忧。此版是第一个原型测试版，某些功能尚在开发中，估计

BUG较多，请谨慎使用。
汉化注意事项：
1、请先安装原英文软件。
2、建议汉化前退出 KAV 应用程序，包括系统栏图标！
3、运行汉化包中的汉化补丁，按正确的安装目录进行汉化（汉化会自动查找安装目录）。必要时请重启动电脑。
4、再次启动 Kaspersky 即是中文界面。
5、此次汉化是另加的中文语言包，并保留原英文和俄文的语言。
6、在反黑客的设置中，因原程序原因，规则配置一栏不能汉化，否则在规则描述中原来可修改的值的顺序会被打乱。只有等下一版官方解决了这个问题才行。

Norton2005 安全特警简体中文正式版（含防火墙）

软件语言： 简体中文
软件类型： 国外软件 / 免费版
运行环境： Win9X/Me/WinNT/2000/XP
授权方式： 正式版
软件大小： 174.25MB

有力防护病毒、蠕虫和特洛伊木马程序
诺顿防病毒软件2005包含新的互联网蠕虫防护，保护个人和家庭工作室用户不受迅速传播的新型混合互联网蠕虫的攻击，即使这些病毒可以通过多个入口攻击计算机用户的系统。将蠕虫阻止技术应用到下一层，互联网蠕虫防护可以阻止联网端口以防止诸?quot;震荡
波"，"MyDoom"和"冲击波"威胁的传播，而这些病
毒通常通过传统的防病毒解决方案防护不到的系统漏洞，进行自身传播。

诺顿防病毒软件2005将继续提供可靠的自动服务，无需用户干预，就可以扫描和清除病毒、蠕虫和特洛伊木马程序。诺顿防病毒软件2005还包含间谍软件检测功能，抵御用户计算机上那些被用来恶意泄漏系统安全、监视用户隐私数据或跟踪用户联机行为的程序。

对黑客和隐私窃贼的必要防护
诺顿个人防火墙2005采用了新的机密信息阻止工具，提供增强的隐私控制，因此可以直接保护用户隐私免遭侵害，甚或是最微小的干扰。新特性支持用户不中断地发送机密信息到他们信任的网站；当用户发送个人数据到不可信任的网站时，则发出警告。机密信息阻止技术有助于防止用户成为网页仿冒的牺牲品。网页仿冒是一种欺诈，它引诱互联网用户向有害并具有潜在威胁的网站提供机密的个人信息，从而导致用户身份被窃。

赛门铁克强健的入侵防护技术是诺顿个人防火墙2005的另一个关键配置。它提供重要的附加安全层，可以结合软件的防火墙，从而预先识别潜在的攻击。这一附加防护层支持诺顿个人防火墙2005仔细监测实际互联网流量，以便有效地识别和阻止联网攻击的尝试。这些，是一个基本的没有入侵防护的防火墙所无法做到的。

全面的电子邮件过滤解决方案
由于垃圾邮件持续激增，并日益成为一种安全威胁，赛门铁克最新的增强型诺顿反垃圾邮件

2005将提供更强的过滤能力来解决电子邮件用户最常见的担心。诺顿反垃圾邮件2005将对某些形式的电子邮件欺诈提供更多的保护，它识别在电子邮件消息内的欺诈的URL互联网地址，并过滤这些信息中的欺骗性的、虚假的发送方地址。用户还可以选择过滤色情垃圾邮件，这样，不想要的内容永远不会抵达收件箱。他们也可以使用诺顿反垃圾邮件2005中基于语言的新型过滤器来阻止特定语言的电子邮件信息。

诺顿反垃圾邮件2005将持续发挥作用，在大多数pop3连接中自动拦截和分析电子邮件，并在抵达用户收件箱时识别垃圾邮件。诺顿反垃圾邮件2005将紧密地和最新版本的微软Outlook，Outlook Express、Eudora以及Yahoo! Web email集成在一起，自动创建一个垃圾邮件目录来收集所有检测出的垃圾邮件。诺顿反垃圾邮件2005甚至将在微软Outlook接受Hotmail和MSN邮件时过滤垃圾邮件。这样，用户不仅节省了时间，还可以不受垃圾邮件可能包含的误导信息和不宜内容的干扰。
最完整的多合一安全和隐私保护套件
将诺顿防病毒软件2005、诺顿个人防火墙2005和诺顿反垃圾邮件2005无缝集成到一个软件套件后，诺顿网络安全特警2005将提供完整、自动的保护，可以针对最复杂的互联网威胁提供保护。诺顿网络安全特警2005还包含新的爆发警报，为用户带来附加好处--当威胁级别高的病毒爆发时，用户将自动接收到警报信息。爆发警报将分析用户PC机的安全状态，必要时立刻提供推荐方案强化防护。此外，诺顿网络安全特警2005将通过简单易用的网页内容过滤功能，能够使孩子和家庭不受少儿不宜或色情网站的影响。
安装序列号：BBC2-YGJP-X4B9-PBCM-VH6G-DYKD

天网防火墙个人版是个人电脑使用的网络安全程序，根据管理者设定的安全规则把守网络，提供强大的访问控制、信息过滤等功能，帮你抵挡网络入侵和攻击，防止信息泄露。天网防火墙把网络分为本地网和互联网，可针对来自不同网络的信息，来设置不同的安全方案，适合于任何方式上网的用户。

1)严密的实时监控
　　天网防火墙（个人版）对所有来自外部机器的访问请求进行过滤，发现非授权的访问请求后立即拒绝，随时保护用户系统的信息安全。
2)灵活的安全规则
　　天网防火墙（个人版）设置了一系列安全规则，允许特定主机的相应服务，拒绝其它主机的访问要求。用户还可以根据自己的实际情况，添加、删除、修改安全规则，保护本机安全。
3)应用程序规则设置
　　新版的天网防火墙增加对应用程序数据包进行底层分析拦截功能，它可以控制应用程序发送和接收数据包的类型、通讯端口，并且决定拦截还是通过，这是目前其它很多软件防火墙不具有的功能。
4)详细的访问记录和完善的报警系统
　　天网防火墙（个人版）可显示所有被拦截的访问记录，包括访问的时间、来源、类型、代码等都详细地记录下来，你可以清楚地看到是否有入侵者想连接到你的机器，从而制定更有效的防护规则。与以往的版本相比，天网防火墙（个人版）设置了完善的声音报警系统，当出现异常情况的时候，系统会发出预警信号，从而让用户作好防御措施。

方正熊猫入侵防护个人版(TruPrevent) 2005

文件大小：17.71M
运行平台：Windows9X/ME/NT/2000/XP

方正熊猫入侵防护个人版2005（即TruPrevent）是方正安全公司联手欧洲熊猫软件为2005年推出的一款新品。产品基于“专门针对未知病毒和攻击而设计”的智能识别技术，即是通过采用“行为分析技术”鉴别文件是否具有危险性或攻击性，即使那些诸如冲击波、振荡波之流的未知病毒亦能够有效隔离。该技术改变了传统杀毒软件所使用的“响应式”技术（被动查杀），转而通过对程序行为的主动跟踪和分析，从而判断是否为病毒或攻击并对之相应做出防范措施。该产品面向家庭用户和SOHU用户，是针对个人PC的一款预防性安全解决方案。

朝华·安博士（VirusClean）是朝华软件应用服务有限公司与韩国安博士有限公司联合开发的针对Win 9X/Me/2000 Professional /XP 客户端专用的计算机杀毒软件。与国内外众多杀毒软件相比，VirusClean 不仅提供最快而最强有力的病毒查/杀功能，而且还可以监控、检测并修复互联网上收到的各种数据及文件中的病毒。VirusClean内置了具有国际离领先技术的WARP 防病毒引擎，因此误报率的可能性极少，而且具有出色的文件恢复功能。

所获奖项：计算机世界——获“2003年中国信息安全优秀解决方案”
软件世界——获“2003年中国电子政务十佳防病毒解决方案”
中国计算机报——与“趋势”一起获得“2003年值得信赖防病毒品牌”
中国软件评测中心——以杀毒最快、资源占用最少获最高15颗星的“技术创新

东方卫士2005（完整功能）下载版最先支持WindowsXP推出的SP2服务包，与SP2的安全中心进行了防毒认证，是最先获得微软认证的防毒软件之一。

能够和WindowsXP SP2安全中心状态形成互动，及时提醒防毒软件是否过期。

东方卫士2005（完整功能）下载版不仅延续了“一防、二杀、三恢复”的防毒理念，在防毒功能和特色功能上作了深入改进，真正做到了安全、稳定、易用！

东方卫士2005（完整功能）下载版防毒产品是完整功能版，而且便于下载（5.81MB）。

目前免费使用，免费升级！

冰盾防火墙是全球第一款具备IDS入侵检测功能的专业级抗DDOS防火墙，来自IT技术世界一流的美国硅谷，由华人留学生Mr.Bingle Wang和Mr.Buick Zhang设计开发，采用国际领先的生物基因鉴别技术智能识别各种DDOS攻击和黑客入侵行为，防火墙采用微内核技术实现，工作在系统的最底层，充分发挥CPU的效能，仅耗费少许内存即获得惊人的处理效能。经高强度攻防试验测试表明：在抗DDOS攻击方面，工作于100M网卡冰盾约可抵御每秒25万个SYN包攻击，工作于1000M网卡冰盾约可抵御160万个SYN攻击包；在防黑客入侵方面，冰盾可智能识别Port扫描、Unicode恶意编码、SQL注入攻击、Trojan木马上传、Exploit漏洞利用等2000多种黑客入侵行为并自动阻止。冰盾防火墙的主要防护功能如下：

★ 阻止DOS攻击：TearDrop、Land、Jolt、IGMP Nuker、Boink、Smurf、Bonk、BigPing、OOB等数百种。

★ 抵御DDOS攻击：SYN/ACK Flood、UDPFlood、ICMP Flood、TCP Flood等所有流行的DDOS攻击。

★ 拒绝TCP全连接攻击：自动阻断某一IP对服务器特定端口的大量TCP全连接资源耗尽攻击。
★ 防止脚本攻击：专业防范ASP、PHP、PERL、JSP等脚本程序的洪水式Flood调用导致数据库和WEB崩溃的拒绝服务攻击。
★ 对付DDOS工具：
XDOS、HGOD、SYNKILLER、CC、GZDOS、PKDOS、JDOS、KKDOS、SUPERDDOS、FATBOY、SYNKFW等数十种。
★ 超强Web过滤：过滤URL关键字、Unicode恶意编码、脚本木马、防止木马上传等。
★ 侦测黑客入侵：智能检测Port扫描、SQL注入、密码猜测、Exploit利用等2000多种黑客入侵行为并阻断

全球最畅销的杀毒软件之一，McAfee防毒软件, 除了操作介面更新外,也将该公司的WebScanX功能合在一起,增加了许多新功能! 除了帮你侦测和清除病毒，它还有VShield自动监视系统，会常驻在System Tray，当你从磁盘、网络上、E-mail夹文件中开启文件时便会自动侦测文件的安全性，若文件内含病毒，便会立即警告，并作适当的处理，而且支持鼠标右键的快速选单功能，并可使用密码将个人的设定锁住让别人无法乱改你的设定。

木马分析专家能自动分析、终止可疑进程、窗体类型及木马详细资料(如创建时间,文件大小,分析Config.sys、Autoexec.bat、Winstart.bat、System.ini、Win.ini、注册表Load键值等),并能随时在线升级木马病毒代码特征库,100%查杀各种未知木马。另外，木马分析专家个人防火墙为您的计算机提供全面的保护，有效地监控任何网络连接。通过过滤不安全的服务，防火墙可以极大地提高网络安全，同时减小主机被攻击的风险。使系统具有抵抗外来非法入侵的能力，防止您的计算机和数据遭到破。

2005最新功能有：新增显示与进程及窗体相关的所有详细信息：包括进程ID、优先级、包含的线程数、包含的模块数、进程文件大小、创建时间、访问时间、修改时间、文件的版本信息等。新增(IE/木马)个人防火墙,在线杀毒。最新版加强了对第五代木马的分析与查杀,能完美的查杀各种无进程,捆绑木马。木马分析专家不仅是查杀木马工具,更是一个安全分析审核工具,它提供了十余种安全审核功能,将许多安全审核工作集成于一身,可以帮助您迅速判断本机的安全状况,大大方便您的工作。防火墙新增对第2代反弹型木马的监控。

现在有些木马以系统服务及Dll线程方式伪装插入IE或Explorer等正常进程中，使得这些病毒在正常模式下根本无法完全清除，因为你要杀死它之前必需先杀掉正常进程才行，但在安全模式下Windows只加载系统本身的模块，这时木马病毒也就无处隐藏了，这也是许多杀毒软件建议在安全模式下进行查杀的主要原因。分析以上原理，我们创新出一种无需进入安全模式却有着与它同样或更好效果的【天下无马】查杀模式，该功能主要针对：正常模式下无法清除的已知、未知及杀之过后又来的恶性木马病毒。新增加入防止被木马病毒封杀功能，而且在清除病毒的同时，会自动清理DLL、OCX等木马控件在注册表中的捆绑信息

木马防线2005是安天公司推出的一款面向个人用户的专业级反木马信息安全 产品，也是国内首款通过公安部权威检测的同类软件。该软件的英文版Antiy Ghostbusters于2001年在欧美地区发布，当年就成为全球AntiVirus TOP 50中唯一的上榜中国产品。并在全球木马查杀、反间谍工具排行中遥遥领先，获得多次海内外专业媒体盛誉

7. HTTP、HTTPS、SSL、TELENT的端口号是什么？

http 80
https 443
ssl 端口 443 用于接收 SSL 通信 端口 636 用于 LDAP SSL 连接
tel 23
8.IPTABLES参数代表什么？

Command	-A, --append
Example	iptables -A INPUT ...
Explanation	在所选择的链末添加规则。当源地址或目的地址是以名字而不是 ip 地址的形式出现时若这些名字可以被解析为多个地址，则这条规则会和所有可用的地址结合。
Command	-D, --delete
Example	iptables -D INPUT --dport 80 -j DROP 或 iptables -D INPUT 1
Explanation	从所选链中删除规则。有两种方法指定要删除的规则：一是把规则完完整整地写出来再就是指定规则在所选链中的序号（每条链的规则都各自从 1 被编号）。
Command	-R, --replace
Example	iptables -R INPUT 1 -s 192.168.0.1 -j DROP
Explanation	在所选中的链里指定的行上（每条链的规则都各自从 1 被编号）替换规则。它主要的用处是试验不同的规则。当源地址或目的地址是以名字而不是 ip 地址的形式出现时，若这些名字可以被解析为多个地址，则这条 command 会失败。
Command	-I, --insert
Example	iptables -I INPUT 1 --dport 80 -j ACCEPT
Explanation	根据给出的规则序号向所选链中插入规则。如果序号为 1，规则会被插入链的头部，其实默认序号就是 1。
Command	-L, --list
Example	iptables -L INPUT
Explanation	显示所选链的所有规则。如果没有指定链，则显示指定表中的所有链。如果什么都没有指定，就显示默认表所有的链。精确输出受其它参数影响，如-n 和-v 等参数，下面会介绍。
Command	-F, --flush
Example	iptables -F INPUT
Explanation	清空所选的链。如果没有指定链，则清空指定表中的所有链。如果什么都没有指定，就清空默认表所有的链。当然，也可以一条一条地删，但用这个 command 会快些。
Command	-Z, --zero
Example	iptables -Z INPUT
Explanation	把指定链（如未指定，则认为是所有链）的所有计数器归零。
Command	-N, --new-chain
Example	iptables -N allowed
Explanation	根据用户指定的名字建立新的链。上面的例子建立了一个名为 allowed 的链。注意，所

	用的名字不能和已有的链、target 同名。
Command	-X, --delete-chain
Example	iptables -X allowed
Explanation	删除指定的用户自定义链。这个链必须没有被引用，如果被引用，在删除之前你必须删除或者替换与之有关的规则。如果没有给出参数，这条命令将会删除默认表所有非内建的链。
Command	-P, --policy
Example	iptables -P INPUT DROP
Explanation	为链设置默认的 target（可用的是 DROP 和 ACCEPT，如果还有其它的可用，请告诉我），这个 target 称作策略。所有不符合规则的包都被强制使用这个策略。只有内建的链才可以使用规则。但内建的链和用户自定义链都不能被作为策略使用，也就是说不能象这样使用：iptables -P INPUT allowed（或者是内建的链）。
Command	-E, --rename-chain
Example	iptables -E allowed disallowed
Explanation	对自定义的链进行重命名，原来的名字在前，新名字在后。如上，就是把 allowed 改为 disallowed。这仅仅是改变链的名字，对整个表的结构、工作没有任何影响

10.管理距离和度量值的作用和意义
distance 衡量协议的优先
metric 衡量路径优良

11.路由器和网桥的主要区别是什么？
Router 网络层　ip 的寻址和转发
Bridge 链路层　完成链路层的 mac 地址维护和数据交换

神码最新面试题　8 月 10 日更新
1．小型机　unix、集群、网络基础好
3．TCP/IP 端口号及名称
5．最大的工程拓扑图并加以说明
6．小型机上如何在 WIN2003 环境配集群
7．写硬软件设备及所用过小型机的型号、版本、操作系统
8．Unix 常用命令查询 1 内存使用率，2CPU 使用率，3 硬盘空间 4 网络配置
用 TOP 时时查看内存 CPU 的使用情况　用 do 命令查看磁盘使用空间　用 ifconfig 查看网络配置
9．小型机上运行数据库的关键模型是什么

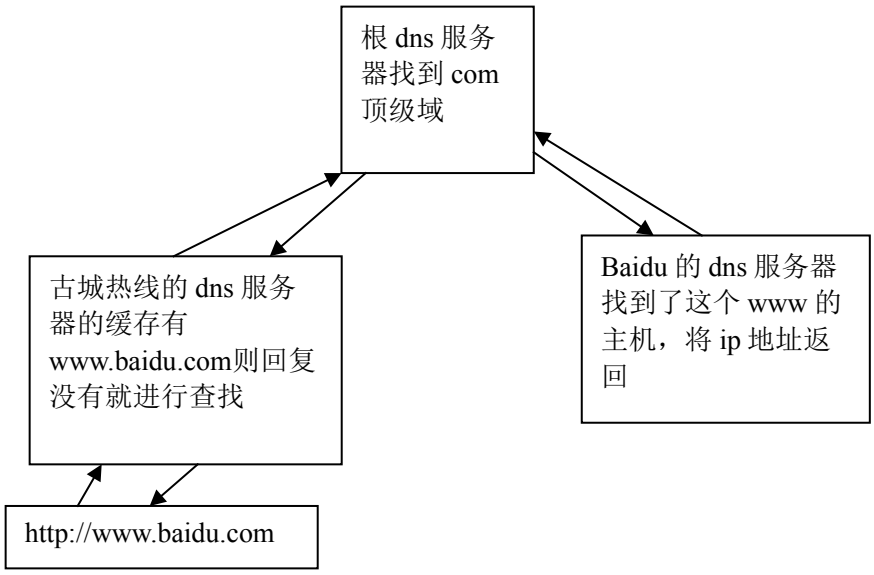
西安启天科技有限公司
一．
1.wondows2000 有两个内置用户分别是　administrator____和__guest_____

2.测试 TCP/IP 协议的网络命令是　　ping_____
3.100BASE-T 分别是 100 代表__100M 带宽__,BASE 代表_基带传输___,T 代表__UTP____
4.组建 LAN 用到的四种线是___铜轴电缆__,_STP____,_光缆____,__UTP_____
5.SQL SERVER 的角色是_ ____,数据库服务器的角色是__ ____
6.组建 LAN 的几种类型__星型__,_环型___,_总线_____
二.
1.安装 wondows2000 的过程和应该注意的问题?
如果是升级安装，注意备份以前的操作系统
2.应用软件的主要作用是什么?
应用软件是专门为某一应用目的而编制的软件，
3.应用软件应该怎样维护?
及时升级，打补丁

富士通试题
1.　网络 7 层协议，TCP/IP 模型

OSI	TCP/IP
应用层	
表示层	应用层
会话层	
传输层	传输层
网络层	网络层
数据链路层	
物理层	网络主机层（网络接口层）

2.　Ping 命令的协议类型　　ICMP（internet 控制消息协议）
3.　DNS 解析的步骤



迭代查询：返回一个能解析该域名的 dns 的地址让主机做“他知道，你去找他吧”
递归查询：返回域名解析的结果，而不是 dns 的地址，也就是“这事我负责到底，你有问题问我好了，我给你解决。”

4. Linux Shell 查找命令
Find 搜索硬盘，查询文件的名称
Whereis 查找文件位置，找某一目录下的文件
Which 查找可执行文件的位置，主要是一些命令存放的位置。
Locate 配合数据库定位文件的位置
5. B 类地址
A 类 1-126 /8 127 是环回地址，指本机
B 类 128-191/16
C 类 192-223/24
6. 区分网络地址和主机地址
主要看他的子网掩码，来判断是主机地址还是网络地址
7. WUS 服务注意事项
配置客户端计算机进行自动更新
指定 Intranet Microsoft 更新服务位置
一个客户端计算机只能同时访问一个更新服务器
当 WSUS 服务器同步后，将根据配置情况获得相应的更新列表。你需要对更新进行批准，以便进行安装或检测；你可以选择一个或多个更新进行批准，如果选择多个更新，那么客户端计算机会一次性进行安装。批准更新的方式有以下五种：
1、 仅检测
2、 安装
3、 拒绝更新
4、 删除
5、 未许可
在自动批准选项中，你可以配置 WSUS 服务器在同步时下载更新程序后自动批准进行检测或者安装。你可以通过更新程序的分类和计算机组来决定自动批准检测或自动批准安装，当两者规则出现冲突时，以自动批准安装的规则为准
8. 网络杀毒步骤
1. 持续扫描，网络进出口的文件。
2. 发现问题主机，主动隔离中毒机，把病毒机统一进行扫毒。
3. 在杀毒之前，备份重要数据文件，以防杀毒完成后文件不能使用。备份时注意病毒的隔离，否则造成杀毒后的机子，又中毒。
安装网络杀毒软件（以诺顿为例）
1 指定服务器，安装服务器
2 安装 sc（安全中心）
3 安装管理单元
4 安装附件（附加安全套件）