



Lab 2 路由器的基本管理



温州大学
WENZHOU UNIVERSITY

实验目的

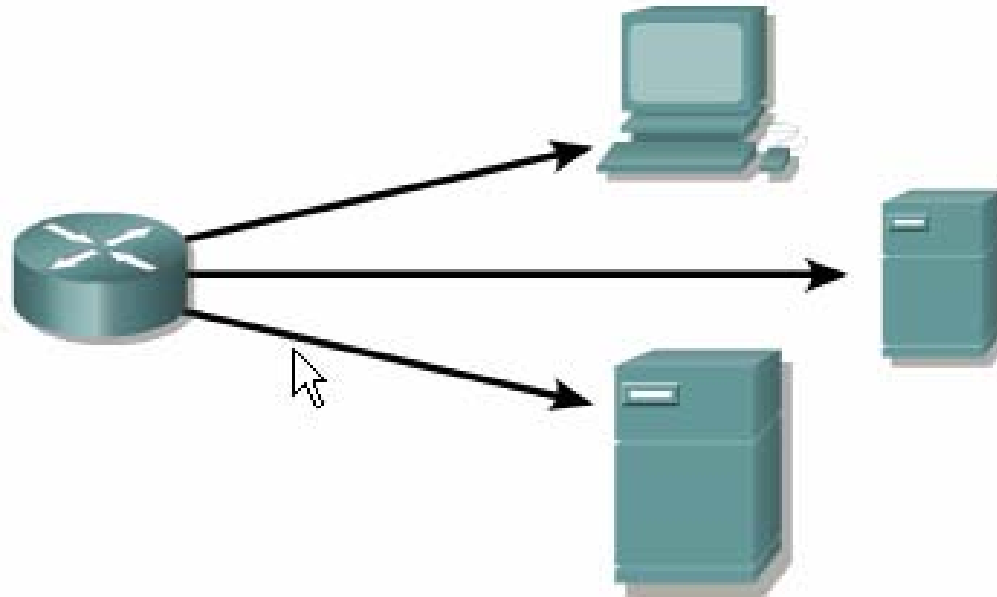
1. 理解**TFTP**服务的特点与作用与配置
2. 掌握**TFTP**服务的配置
3. 掌握使用**TFTP**上传进行**IOS**备份的方法
4. 掌握使用**TFTP**下载进行**IOS**恢复/更新的方法
5. 掌握使用**TFTP**进行配置文件的备份与恢复的方法
6. 掌握路由器密码恢复的基本方法

实验内容1

通过**TFTP**进行**IOS**备份、恢复/更新

(注：实验室中进行)

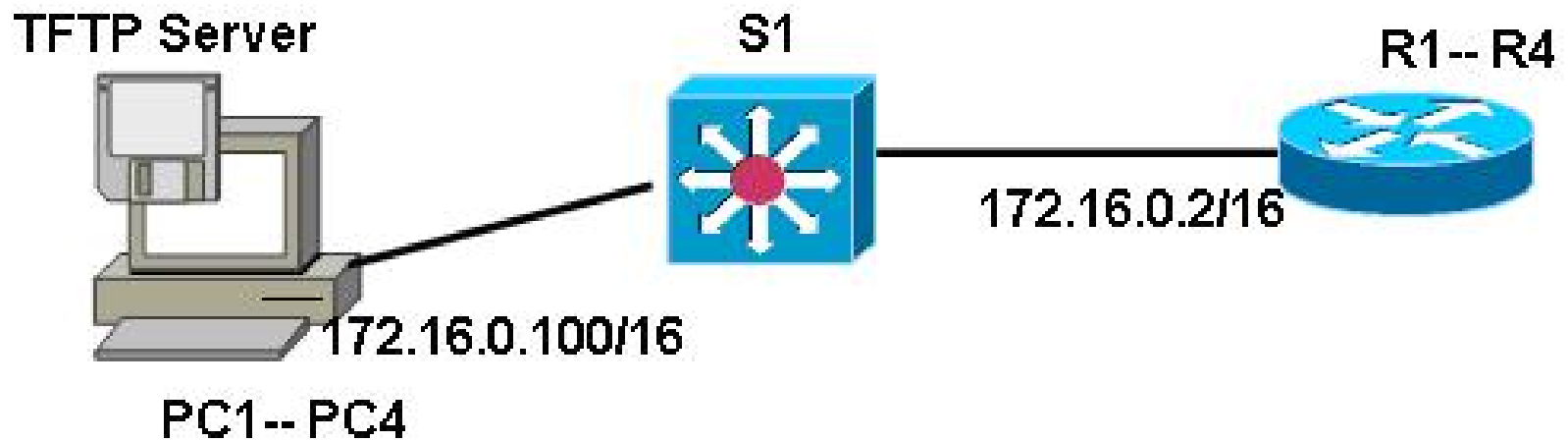
知识要点1: IOS备份与恢复方式



Save configuration files to a:

- TFTP Server
- Network Server
- Disk in a safe place

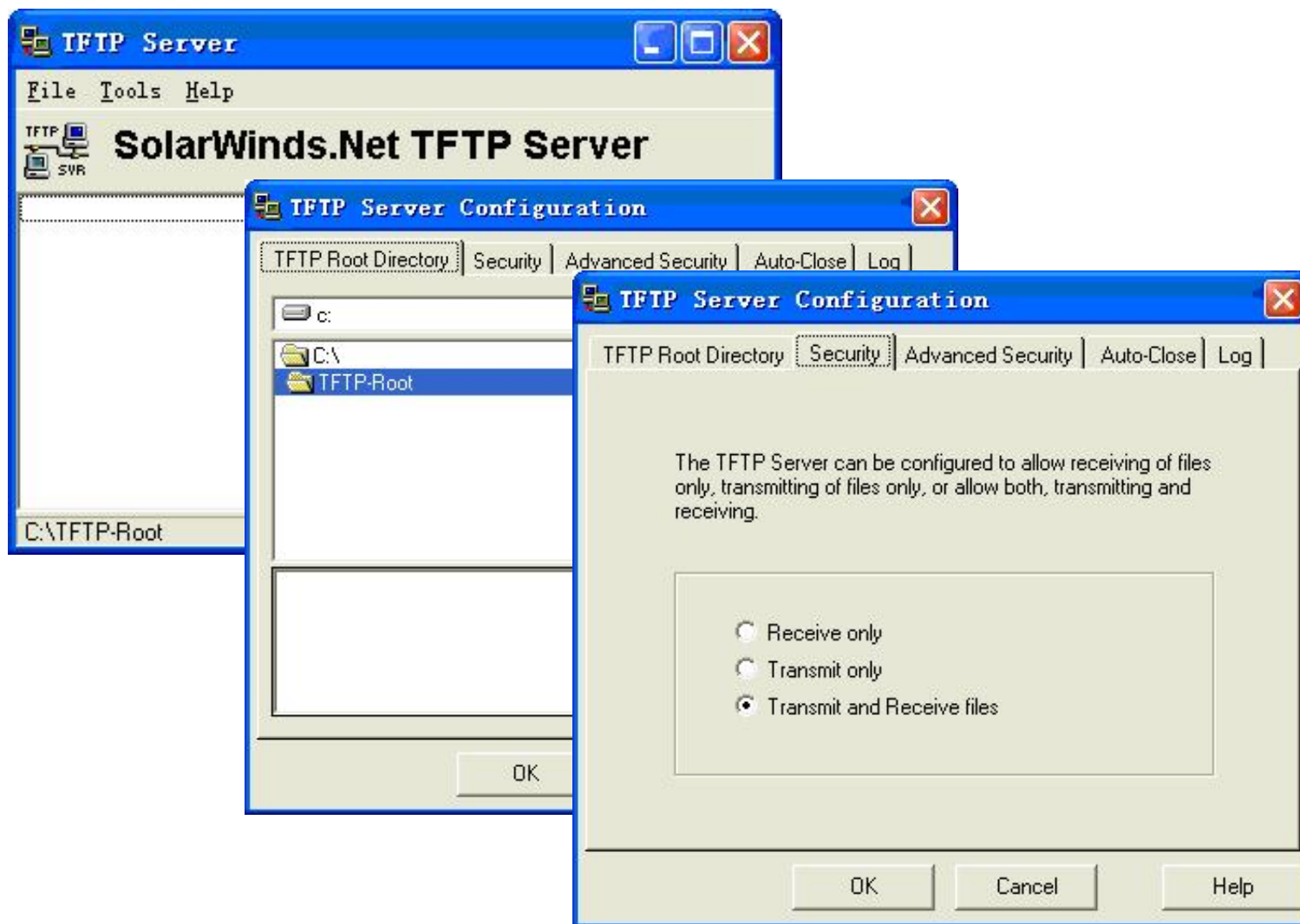
物理连接



TFTP Server软件的安装、准备

1. 从<http://solarwinds.net>上免费下载**SolarWinds TFTP Server**软件；
2. 下载后安装；
3. 运行该软件。

TFTP Server软件的安装、准备（续）



保证路由器和计算机间的IP可达

```
R2(config)#int g0/0
```

```
R2(config-if)#no shutdown
```

```
R2(config-if)#ip address 172.16.0.2 255.255.0.0
```

```
R2(config-if)#exit
```

//以上在路由器的以太网接口配置IP地址，并启用接口

```
R2#ping 172.16.0.100
```

Type escape sequence to abort.

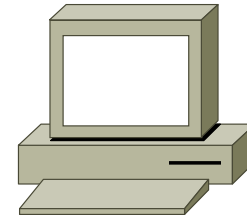
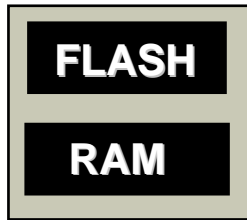
Sending 5, 100-byte ICMP Echos to 172.16.0.100, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms

//测试从R2到PC（TFTP服务器）的IP可达

确定TFTP服务器有足够的空间



TFTP
Server

```
Router# show flash
System flash directory:
File Length Name/status
  1  5848552 c2600-i-mz.122-8.T1.bin
[5848616 bytes used, 10928600 available, 16777216 total]
16384K bytes of processor board System flash (Read/Write)
```

```
Router# ping tftp_address
...
!!!!
```

```
(On the TFTP server, for example, a UNIX host)
dir c2600-i-mz.122-8.T1.bin
```


备份IOS到TFTP服务器的相关注释

R2#show flash:

CompactFlash directory:

File Length Name/status

1 41205996 c2800nm-adventerprisek9-mz.124-11.T1.bin

[41206060 bytes used, 23019216 available, 64225276 total]

62720K bytes of ATA CompactFlash (Read/Write)

//先查看flash中的IOS大小，文件名等

R2#copy flash:c2800nm-adventerprisek9-mz.124-11.T1.bin tftp:

//把IOS备份到TFTP服务器上

Address or name of remote host []? 172.16.0.100

//回答TFTP服务器的IP地址

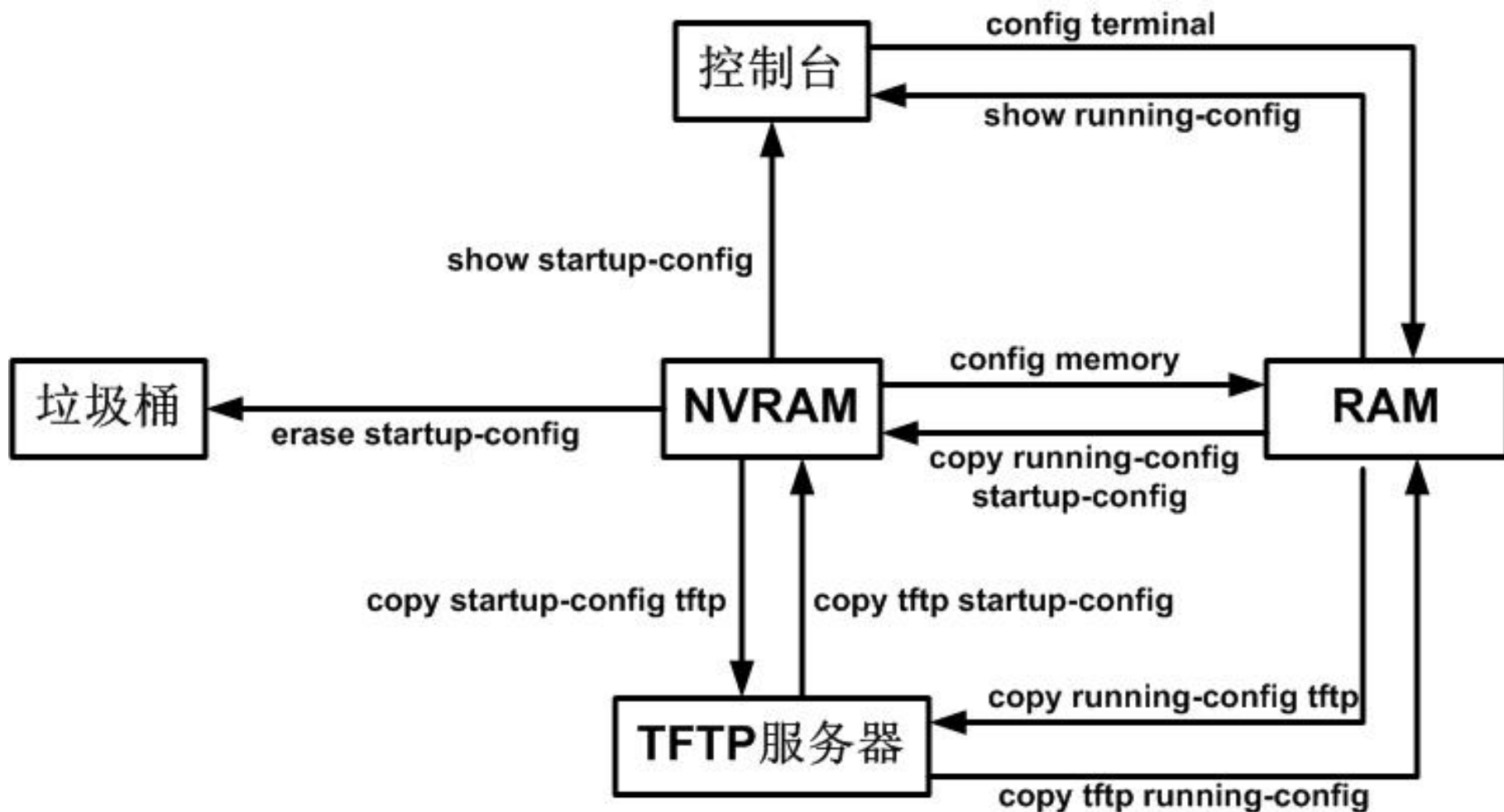
Destination filename [c2800nm-adventerprisek9-mz.124-11.T1.bin]?

//回答文件名。默认时和源文件名是一样的，不建议修改文件名，因为IOS文件名包含了IOS的版本、特征等信息

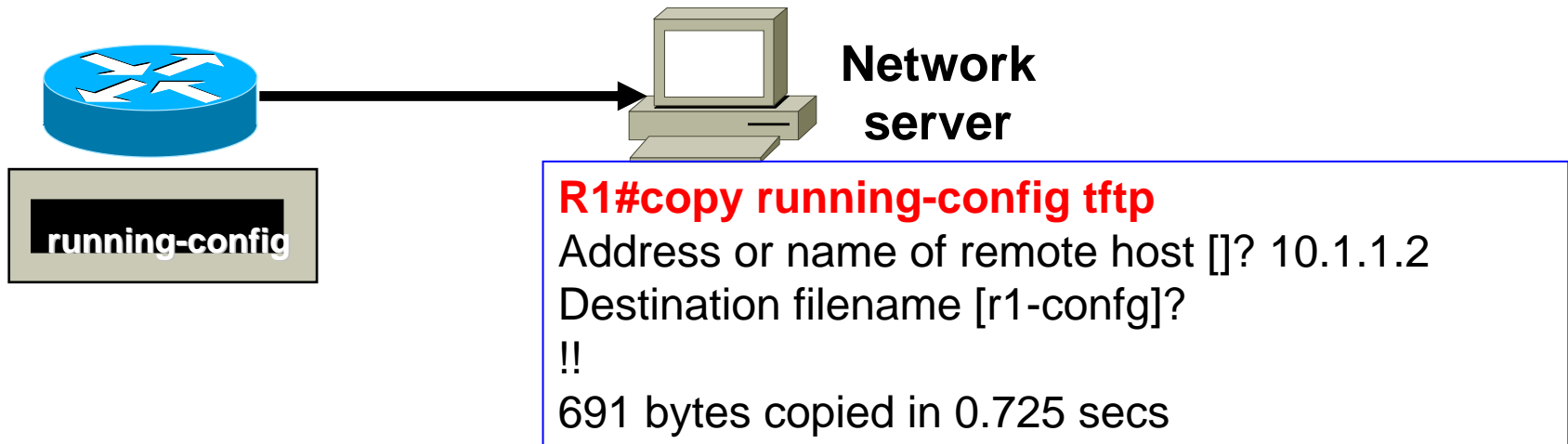
!! (此处省略)

//备份成功后可以在c:\tftp-root目录下找到该文件。

知识要点2：配置文件的流动



备份配置文件到TFTP服务器



R2#copy running-config tftp:

//把内存中的配置文件备份到TFTP服务器上

Address or name of remote host []? 172.16.0.100

//回答TFTP服务器的IP地址

Destination filename [r2-config]?

//回答文件名，默认时为“路由器名-config”

!!

1381 bytes copied in 0.452 secs (3055 bytes/sec)

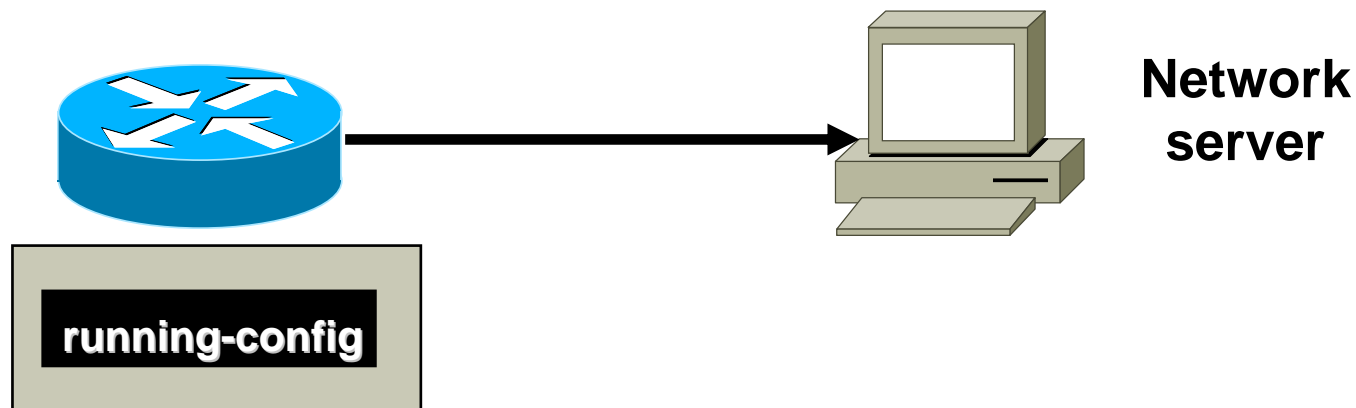
//备份成功，共1381字节，可以在c:\tftp-root目录下找到该文件，是一个纯文本的文件。可以用写字板打开，而用记事本打开则格式会出现问题

通过捕获文本的方式进行配置文件的备份

: 采用“复制、粘贴”备份配置文件

1. 可以简单地在终端窗口中，执行“**show running-config**”命令显示当前的配置，在终端窗口中复制全部配置，粘贴到某文本文件中。
2. 如果是在**Windows**自带的超级终端窗口中复制、粘贴配置，会有“**---more---**”等字样，要记得删除这些字符。

从TFTP下载配置文件



```
R1#copy tftp running-config
```

```
Address or name of remote host []? 10.1.1.2
```

```
Source filename []? r1-config
```

```
Destination filename [running-config]?
```

```
Accessing tftp://10.1.1.2/r1-config...
```

```
Loading r1-config from 10.1.1.2 (via FastEthernet0/0): !
```

```
[OK - 691/1024 bytes]
```

```
691 bytes copied in 0.854 secs
```


实验内容2

路由器的密码恢复

(注：在实验室中进行)

配置寄存器 (config-register) 组成

寄存器组成：4位16进制
表示：0xABCD

15 14 13 12



A

11 10 9 8



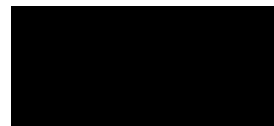
B

7 6 5 4



C

3 2 1 0



D

实例

2

1

0

2

D: 启动域

C: 使得系统软件忽略NVRAM中的内容，关键位为“6”

- 该位值为 0，当路由器启动后会从NVRAM里面的配置文件调到RAM里运行
- 该位值为 1，路由器启动后会忽略NVRAM的配置

A: 关键位为“13”，网络启动次数：

值为1 ——5次， 值为0——无数次

Console口

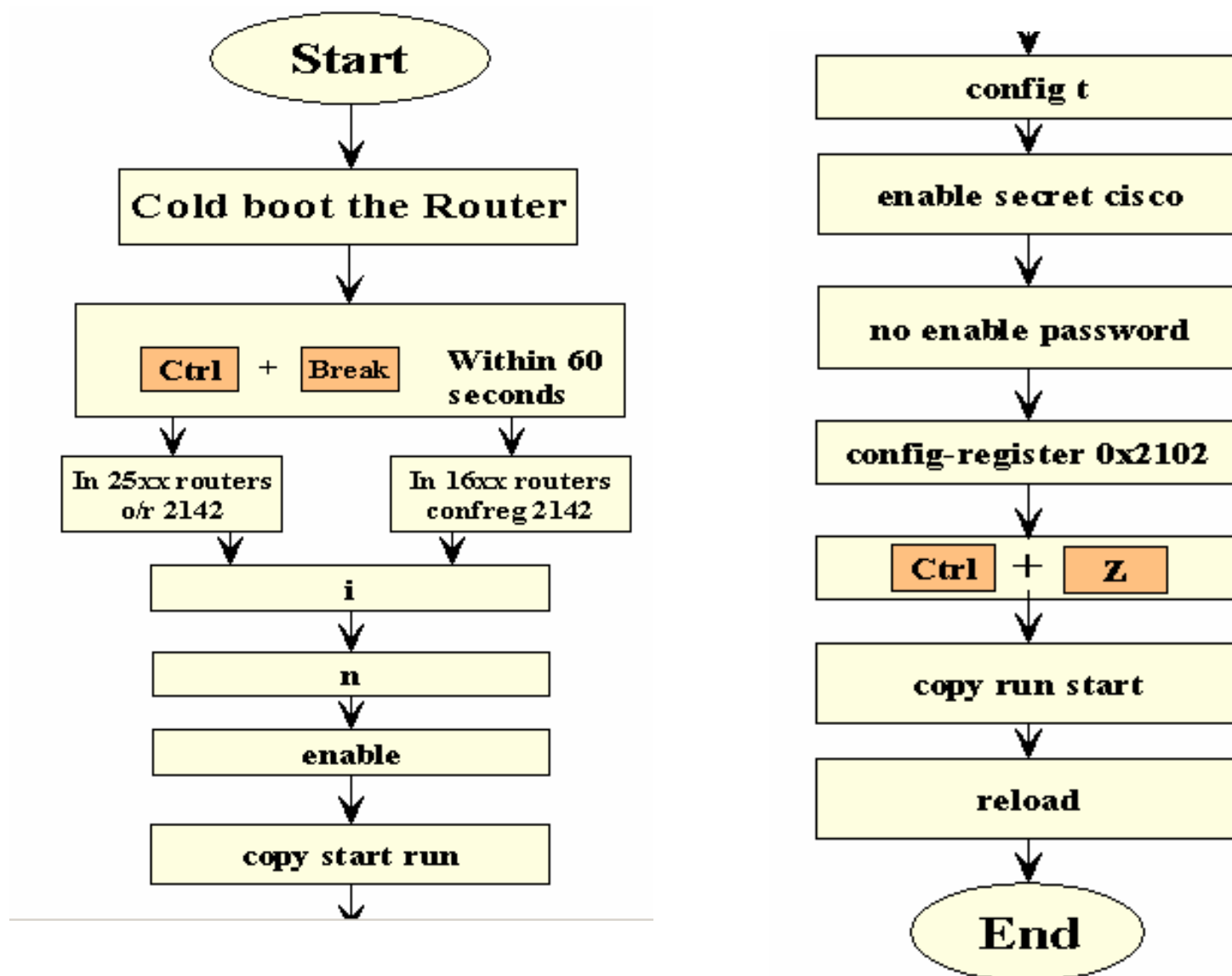
速率设定表

12	11	速率
0	0	9600
0	1	4800
1	0	1200
1	1	2400

配置寄存器启动域

配置寄存器的值（16 进制）	描述
0	使用 ROM 模式
1	自动从 ROM 中启动
2-F	从 FLASH 或 TFTP 服务器启动

路由器密码破解步骤



实验步骤2： 关闭路由器电源并重新开机

1. 关闭路由器电源并重新开机，当控制台出现启动过程，赶快按【**Ctrl+Break**】键中断路由器的启动过程，进入rommon模式
2. **rommon 1>confreg 0x2142**
 - //改变配置寄存器的值为**0x2142**，这会使得路由器开机时不读取**NVRAM**中的配置文件。
3. **rommon 2 > i**
 - //重启路由器。路由器重启后会直接进入**setup**配置模式，用【**Ctrl+C**】或者回答“n”，退出**setup**模式。

实验步骤3: 修改密码

```
Router>enable
```

```
Router#copy startup-config running-config
```

```
Destination filename [running-config]?
```

```
661 bytes copied in 0.625 secs
```

//把配置文件从**NVRAM**中拷贝到**RAM**中，在此基础上修改密码。

```
R2#configure terminal
```

```
R2(config)#enable password cisco
```

//以上把密码改为自己的密码，如果还配置别的密码则一起把它们修改了。

实验步骤4: 恢复寄存器值

R2(config)#config-register 0x2102

//以上把寄存器的值恢复为正常值0x2102

R2(config)#exit

R2#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]

R2#reload

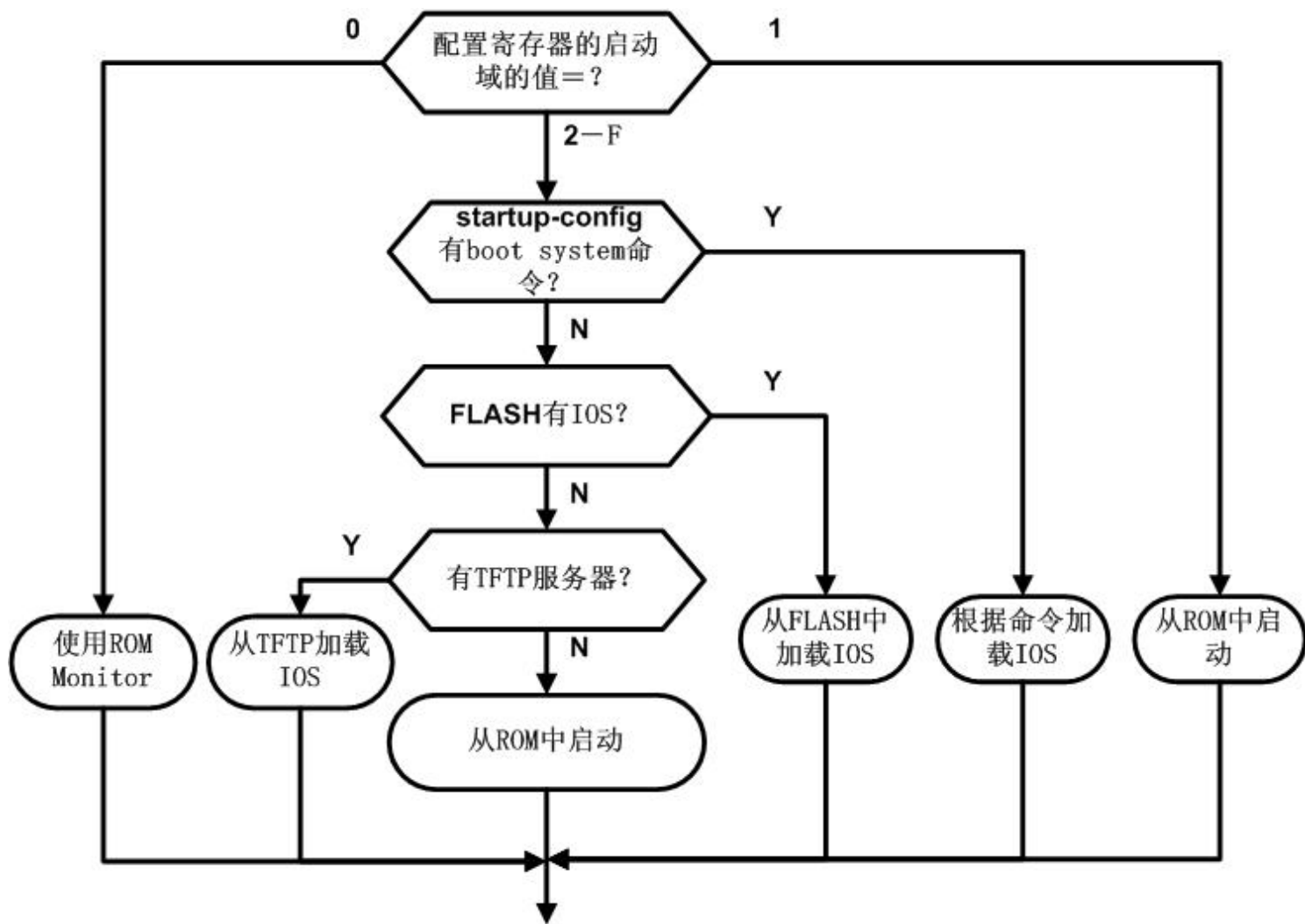
//把路由器的各个接口一一打开，保存配置，重启路由器，检查路由器是否正常

实验内容3

路由器的IOS恢复

(注：在实验室中进行，选做)

知识要点：路由器查找IOS的详细流程



实验环境准备：故意删除flash中的IOS

R2#show flash:

CompactFlash directory:

File Length Name/status

1 41205996 c2800nm-adventerprisek9-mz.124-11.T1.bin

[41206060 bytes used, 23019216 available, 64225276 total]

62720K bytes of ATA CompactFlash (Read/Write)

//显示flash中的IOS

R2#delete flash:c2800nm-adventerprisek9-mz.124-11.T1.bin

Delete filename [c2800nm-adventerprisek9-mz.124-11.T1.bin]?

Delete flash:c2800nm-adventerprisek9-mz.124-11.T1.bin?

[confirm]

//以上是删除flash的IOS，模拟FLASH中的IOS丢失或者IOS升级失败

恢复IOS步骤1——设置变量

1. 请确认**IOS**已经放在**c:\TFTP-Root**目录下。路由器丢失了**IOS**后，开机将自动进入**rommon**模式。
2. **rommon 2 > IP_ADDRESS=172.16.0.2**
3. **rommon 3 > IP_SUBNET_MASK=255.255.0.0**
4. **rommon 4 > DEFAULT_GATEWAY=172.16.0.100**
5. **rommon 5 > TFTP_SERVER=172.16.0.100**
6. **rommon 6 > TFTP_FILE=c2800nm-adventerprisek9-mz.124-11.T1.bin**
 - **//要恢复IOS，需要配置一些变量的值，主要是路由器的IP地址、掩码等。DEFAULT_GATEWAY胡乱地指向TFTP服务器。请注意变量名的大小写。**

恢复IOS步骤2——下载IOS

```
rommon 8 > tftpdnld
```

```
//开始从tftp恢复IOS
```

```
    IP_ADDRESS: 172.16.0.2
    IP_SUBNET_MASK: 255.255.0.0
    DEFAULT_GATEWAY: 172.16.0.100
    TFTP_SERVER: 172.16.0.100
    TFTP_FILE: c2800nm-adventerprisek9-mz.124-11.T1.bin
    TFTP_VERBOSE: Progress
    TFTP_RETRY_COUNT: 18
    TFTP_TIMEOUT: 7200
    TFTP_CHECKSUM: Yes
    TFTP_MACADDR: 00:19:55:66:63:20
    GE_PORT: Gigabit Ethernet 0
    GE_SPEED_MODE: Auto
```

```
Invoke this command for disaster recovery only.
```

```
WARNING: all existing data in all partitions on flash will be lost!
```

```
Do you wish to continue? y/n: [n]: y
```

```
//回答“y”开始从tftp服务器上恢复IOS，根据IOS的大小，通常需要十几分钟
```

恢复IOS步骤13 ——重启路由器

Receiving c2800nm-adventerprisek9-mz.124-11.T1.bin
from 172.16.0.100

!!

（此处省略）

!!

File reception completed.

Validating checksum.

Copying file c2800nm-adventerprisek9-mz.124-11.T1.bin
to flash.

Eee
e

//从tftp服务器接收了IOS后，会进行校验。

rommon 9 > i

//重启路由器