信息安全工程

同济大学计算机系 钟计东
个人邮箱：zhongjidong@tongji.edu.cn

本课件存放在以下邮箱：
邮箱：tongji_zhong@163.com
密码：tongji_cs

虚拟机简介

虚拟机

- 虚拟机建立过程
  - 安装VMvare10(或其他更高版本) / VMware Fusion (MAC)：
  - 新建虚拟机（建立一台虚拟的计算机）：可以选择稍后建立操作系统（一般此时只是建立一个空白的硬盘）。
  - 安装操作系统
  - 安装WMWareTools（可以改善虚拟机的显示）

虚拟机

- 虚拟机通常和真实机器一致，具有以下可以配置设备：
  - BIOS/EFI启动
  - 处理器（支持多个处理器）
  - 硬盘（IDE/SATA/SCSI/NVMe接口设备等）
  - 光驱
  - 网络接口
  - 声卡

硬盘

- 虚拟机的硬盘通常用一个文件或多个文件表示
  - 文件名后缀为VMDK
  - 可以用DISKGENIUS创建或打开、分区和格式化
    - Diskgenius/磁盘/打开虚拟磁盘文件
  - 一个虚拟机可以有多个硬盘
    - 虚拟机设置/硬盘/添加
  - 一个虚拟机可以有4个IDE接口硬盘

硬盘

- 主机分区或者U盘可以映射为虚拟硬盘
  - 编辑虚拟机设置/硬件/添加/硬盘IDE/使用物理磁盘（如果使用U盘，可能需要重新启动VMWare)
- 硬盘启动顺序可以通过BIOS设置
  - 虚拟机/电源/启动时进入BIOS

操作系统安装

操作系统安装

- 操作系统通常有ISO安装版和GHOST版
  - ISO安装比较简单
  - GHOST版安装稍显复杂（但是安装迅速）
- 操作系统安装大致步骤：
  - 硬盘分区 （ISO版可能自动分区）
  - 可能需要BIOS/EFI启动顺序设置
  - 操作系统安装

ISO安装

- ISO安装版（通过CD/DVD安装）：
  - 如果有安装光盘，选择使用物理驱动器
  - 或者使用ISO映像文件
  - 勾选启动时连接

分区

- 使用DISKGenuis或者其他磁盘工具分区
  - 用DISKGENIUS打开虚拟机中代表硬盘的VMDK文件
  - 建立分区
  - 格式化分区

实验：Ghost版安装XP

- 安装GHOST版WINXP（GHO后缀文件存在于ISO光盘中）：
  - 硬盘分区（如分成两个分区）
  - 将GHOST版的ISO文件载入光驱
  - 电源/开机时进入BIOS，设置光盘启动优先
  - 安装XP
  - 重启再次设置BIOS，设置硬盘优先启动
  - 启动后会安装驱动程序。

实验：安装操作系统

- 安装如下操作系统：
  - windows xp
  - windows server 2003

创建虚拟机

创建虚拟机

- 创建虚拟机有几种方式：
  - 新建
  - 克隆
  - 虚拟化主机

克隆虚拟机（快速创建虚拟机）

- 克隆一个已有的虚拟机:
  - 完全克隆： 复制和黏贴，相当于复制一个新的虚拟硬盘
  - 链接克隆：克隆一个已有的虚拟机，和母机共享虚拟磁盘
  - 注：克隆时一定要注意将网卡的MAC地址重新产生，以防两者一样。

虚拟机与主机数据共享

实验：虚拟机（与主机文件共享）

- 虚拟机与主机之间文件共享可以有多种方式
  - （推荐）安装VMWARE TOOLS后直接COPY-PASTE
  - 用ImDisk挂载到主机里
  - 安装VMWARE TOOLS后编辑虚拟机设置/选项/共享，映射为网络驱动器
  - 用DISKGENIUS打开VMDK文件，直接读取和写入
  - 通过CD/DVD，主机文件可以制作成ISO格式载入CD/DVD
  - 通过U盘（虚拟机/可移动设备）

虚拟机快照

实验：虚拟机（快照）

- 快照表示存储某个时段的虚拟机状态。注意：选择独立磁盘不受快照影响，无法拍摄虚拟机运行时快照
  - 关机
  - 拍摄快照1
  - 开启虚拟机
  - 增加一个新文件
  - 拍摄快照2
  - 恢复快照1（立刻关机，再开机后新增的文件消失）
  - 关机
  - 恢复快照2（自动开机，新增的文件重新出现）

虚拟网络配置

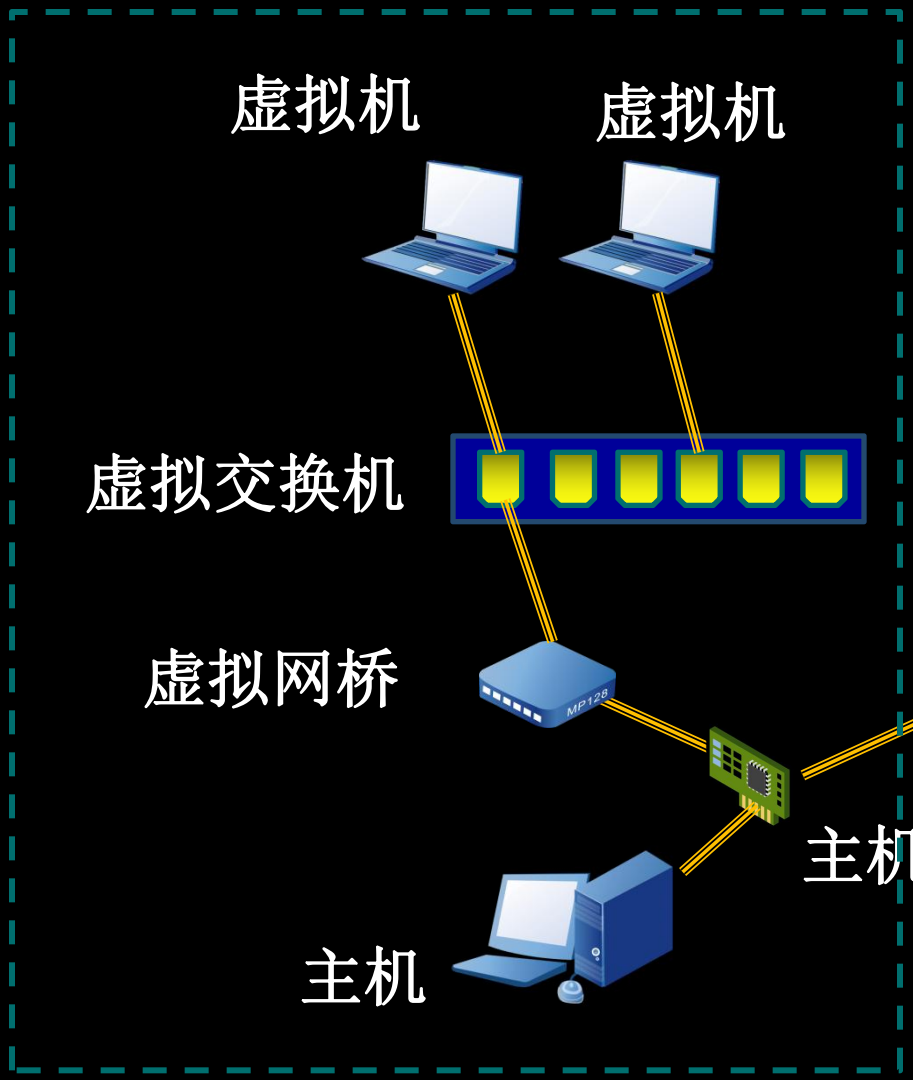
网段

- VMWare支持多个网段
  - 每个网段相当于一个广播型的以太网络(Ethernet)
  - WMWare预设了多个网段（名称为VMNet0, VMNet1....)
    - 虚拟网络设置/添加网络
  - 用户可以自定义更多网段
    - 虚拟机设置/网络适配器/LAN网段

网段连接模式

- VM网段设置有几种模式
  - 桥接模式（bridged）
  - NAT（Network AddressTranslation）模式
  - host-only
  - LAN模式
- 区别主要在于和外部网络的连接方式，桥接模式和NAT模式可以访问外部网络，而后两种不能
- LAN访问不提供DHCP服务，提供更多网段

桥接模式

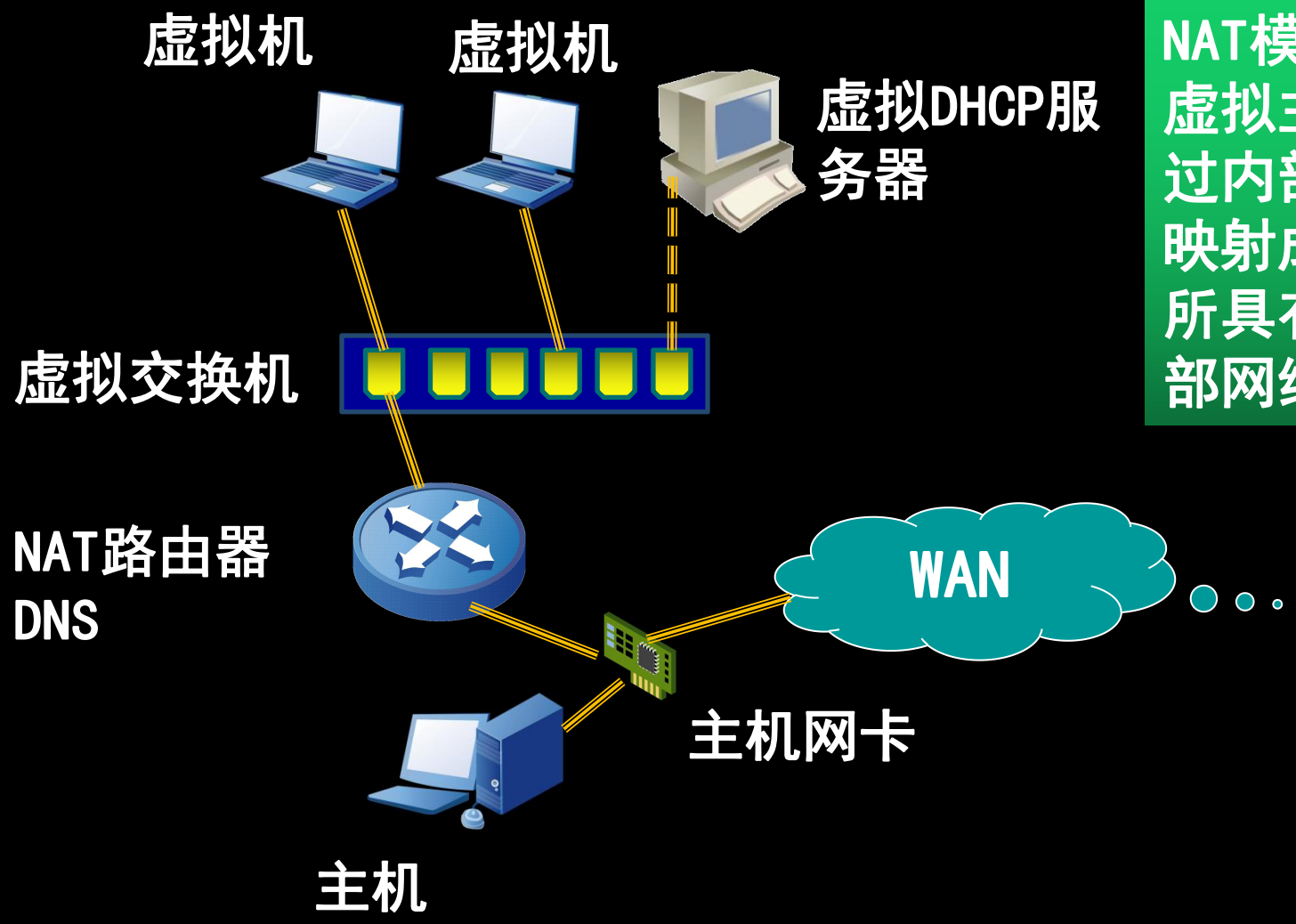


桥接模式:
将主机和虚拟机放在主机所在的物理网络，虚拟机需要独立的IP地址

实验：桥接模式

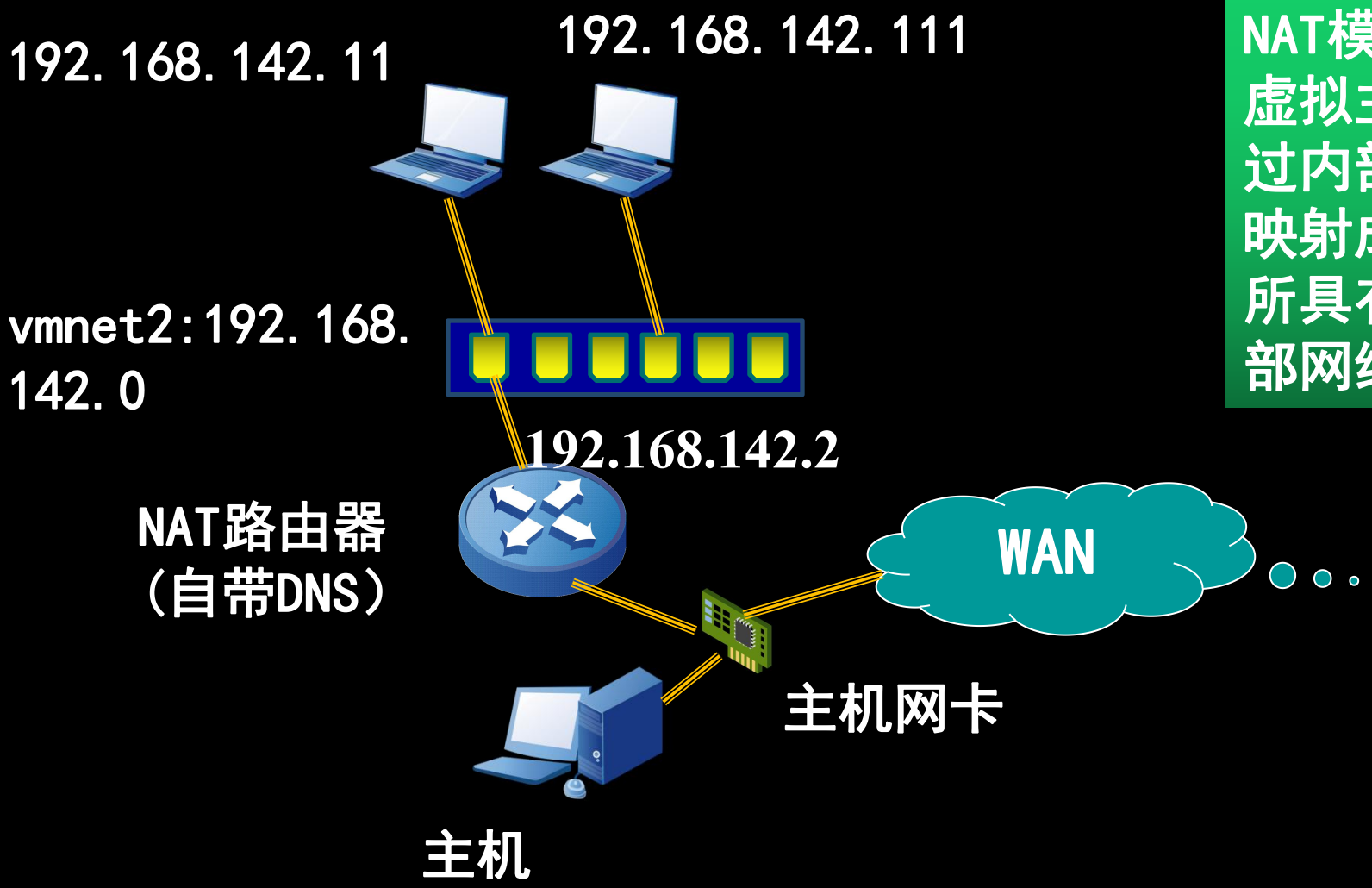
- 实验：将某个虚拟网段设置为桥接模式
  - 虚拟网络编辑器/选择一个网段（如wmnet0)/设置为桥接模式/桥接到一个可以访问外部网络的网口
  - 虚拟机设置/网络适配器/自定义（选择wmnet0)
  - 开启两台虚拟机
  - 查看虚拟机和主机是否和主机有同样的网段、有同样的网关和DNS

NAT模式



NAT模式：虚拟主机通过内部地址映射成主机所具有的外部网络地址

实验：NAT模式



NAT模式：虚拟主机通过内部地址映射成主机所具有的外部网络地址

实验：NAT模式

- 实验：将虚拟网段设置为NAT 模式
  - VM设置：编辑/虚拟网络编辑器/添加网络vmnet2（WMFUSION在偏好设置中有一个+号可以用来添加网络）
  - NAT模式[设置：网关IP：192.168.142.2], [子网IP:192.168.142.0], [子网掩码：255.255.255.0]](WMFusion中为偏好设置）
  - 去掉DHCP（表示不使用DHCP服务器）
  - 去掉将主机适配器添加到此网络，表示主机不连接在142网段

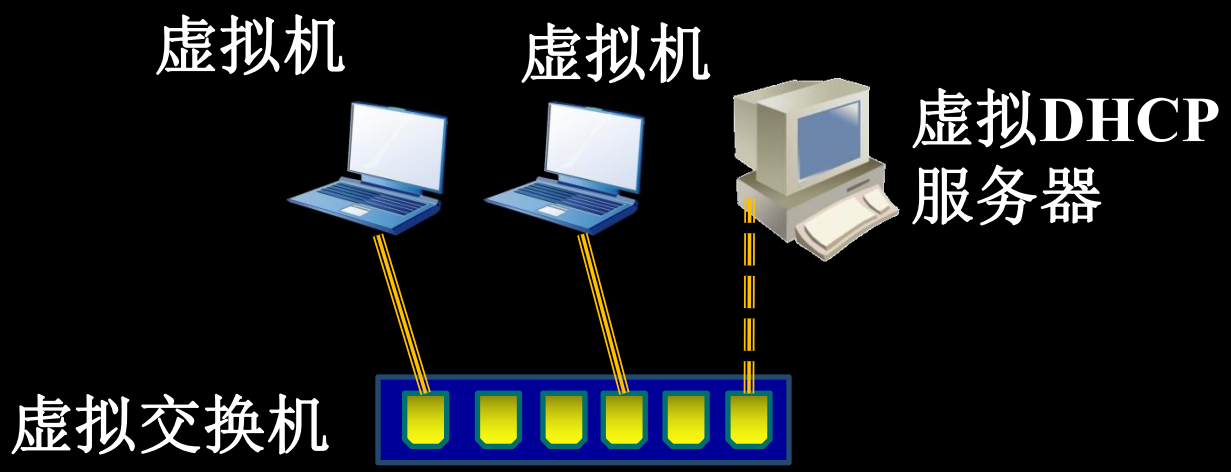
实验：NAT 模式

- 每台虚拟机设置：
  - 网络适配器：选择vmnet2
  - 开启虚拟机：修改网络连接的属性，设置相应的IP地址，网关地址和DNS地址
  - 一台虚拟机：IP:192.168.142.11, gateway:192.168.142.2, DNS:192.168.142.2
  - 另一台虚拟机：IP:192.168.142.111, gateway:192.168.142.2, DNS:192.168.142.2

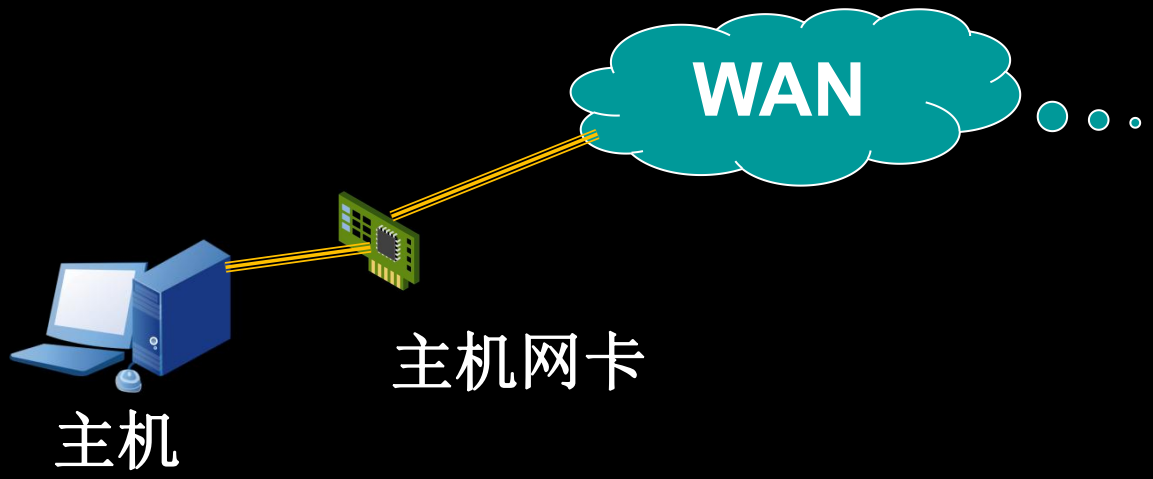
实验：NAT 模式

- 确认虚拟机之间可以连通：
  - 虚拟机之间可以PING通
  - 可以PING网关
  - 可以连接外部网络

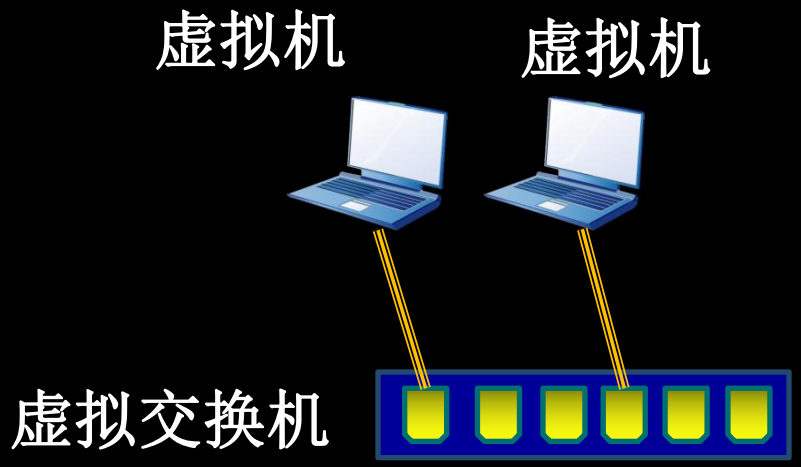
Host-Only



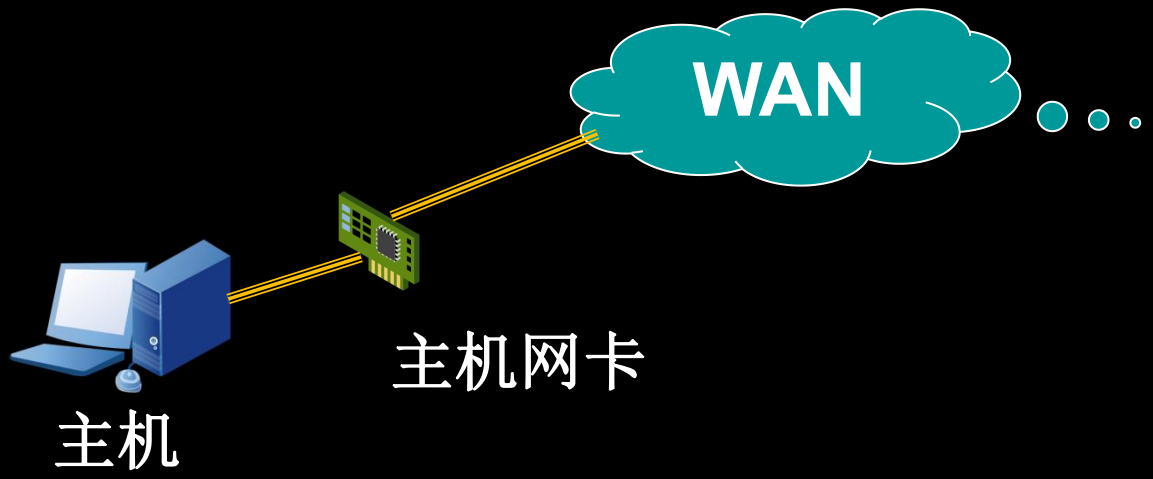
仅主机模式：主机无法访问外部网络



LAN模式



LAN模式：无法访问外部网络



构建虚拟机服务器

实验：虚拟机（开启网络服务）

- windows server 2003 开启WEB, FTP服务器
  - 点击开始—控制面板—添加或删除程序
  - 单击 添加或删除windows组件
  - 勾选应用程序服务器，点击详细信息
  - 勾选internet 信息服务（iis），点击详细信息
  - 勾选万维网服务，FTP服务，点击确定
  - 继续完成后续工作

实验：虚拟机（Http）

- 配置WEB服务器
  - 点击开始—管理工具—internet信息服务（IIS）管理器
  - 点开Internet信息服务下的"+",点开网站，右击默认网站，单击属性
  - 单击网站，在IP地址对应的下拉文本框中点击192.168.142.111（即本机IP地址）
  - 点击文档，勾选启用默认文档，点选其他的文档，单击删除；在文本框中仅仅留下index.htm文档；单击确定

实验：虚拟机（HTTP）

- 双击我的电脑，浏览到web服务器的主目录，空白区域右击，点击新建—文本文档
- 打开新建的文本文档，输入文本内容，并将文件保存为index.htm.
- 双击internet explorer，在地址栏输入http://192.168.142.111,按下enter
- 从结果可看出能正常显示web服务器网站主页。
- 打开另一台虚拟机，双击internet explorer，在地址栏输入http://192.168.142.111,按下enter

实验：虚拟机（FTP）

- 配置FTP服务器
  - 参考WEB的配置
  - 打开新建的文本文档，输入文本内容，并将文件保存在FTP服务器的根目录下
  - 双击internet explorer，在地址栏输入ftp://192.168.142.111，按下enter
  - 下载新建的文本文档

Wireshark

实验：混杂模式

- 目的：熟悉WireShark配置的混杂模式
- 设置：Interface设置中Promiscuous Mode为混杂模式，捕获所有能接收的数据包，不管其目的是否为本机。A，B，C三台主机位于同一网段
  - C: 开启WireShark混杂模式，开始捕获
  - A: Ping B
  - C：查看是否能看到A ping B的数据包

实验：Wireshark

- 目的：熟悉WireShark配置的混杂模式
  - C：WireShark去掉Promiscuous Mode，开始捕获。
  - A: ping B
  - C：Wireshark查看是否可以看到A PING B的数据包

实验：显示过滤器

- 目的：熟悉WireShark的显示过滤器
- 设置：只显示ICMP报文
  - wireshark: Filter: icmp / Apply
  - wireshark查看是否只有icmp报文
- 设置：只显示ICMP Echo Request和Echo reply报文
  - wireshark: Filter: icmp.type == 8 or icmp.type == 0

实验：显示过滤器

- 目的：熟悉WireShark的显示过滤器
- 设置：显示从某个以太网地址MAC-A发出的报文
  - wireshark: Filter: eth.src == MAC-A
- 设置：只显示某个IP-A地址来往的报文
  - wireshark: Filter: ip.addr == IP-A

路由器安装

实验：安装路由器

- 目的：在虚拟机中安装路由器，组成一个简单的网络
- 选择软路由RouterOS软件（MikroTik RouterOS是一种路由操作系统，是基于Linux核心开发，兼容x86 PC的路由软件,并通过该软件将标准的PC电脑变成专业路由器）
- RouterOS非常小巧，GHOST版安装也非常方便（GHOST进行硬盘拷贝local/disk/from image）

实验：安装路由器

- 虚拟机（路由器）安装两张网卡（相当于处于两个网段）VMNet2(192.168.142.100/24)和VMNet0(192.168.140.100/24)[Wmnet0主机模式]
- 登陆帐号：admin，无密码
- 通过winbox对路由器进行设置，使得其能访问外部网络（增加路由，如果主机能够访问外网）

注意事项：MAC地址

- 网上也提供了ROS的更高版本（6.0以上），但只是虚拟机版，虚拟机版直接打开使用就可以了，但要特备注意：
  - ROS内部设置的MAC地址可能和虚拟机提供的MAC地址不一致，因此需要重置：
  - ROS网卡地址可用如下命令查看
    - interface/ethernet/print
  - 如果不一致，利用ROS命令重置ROS内MAC地址
    - interface/ethernet/reset-mac-address

注意事项：MAC地址

- 如果无法重置，利用ROS命令设置ROS内MAC地址
  - interface/ethernet/set

实验：路由器管理方式

- RouterOS支持多种方式访问路由器
  - 命令行格式
  - WINBOX远程管理：
  - Web访问

实验：命令行管理方式

- 命令行格式：TAB键可以查看有什么命令
  - 登录后直接在命令行按TAB就可以查找所有主菜单命令
  - 输入INTERFACE（显示路由器安装了几个网口）
  - 按TAB键就可以查找INTERFACE下的子菜单

实验：命令行设置IP地址

- 目的：设置路由器网卡(Interface)IP地址
- 设置：RouterOS直接设置
  - 打开路由器（虚拟机），登陆
  - 输入interface
  - 输入print，查看接口名（接口顺序和虚拟机里的网卡添加顺序有关）
  - 输入/，回到根目录
  - 输入ip
  - 输入address

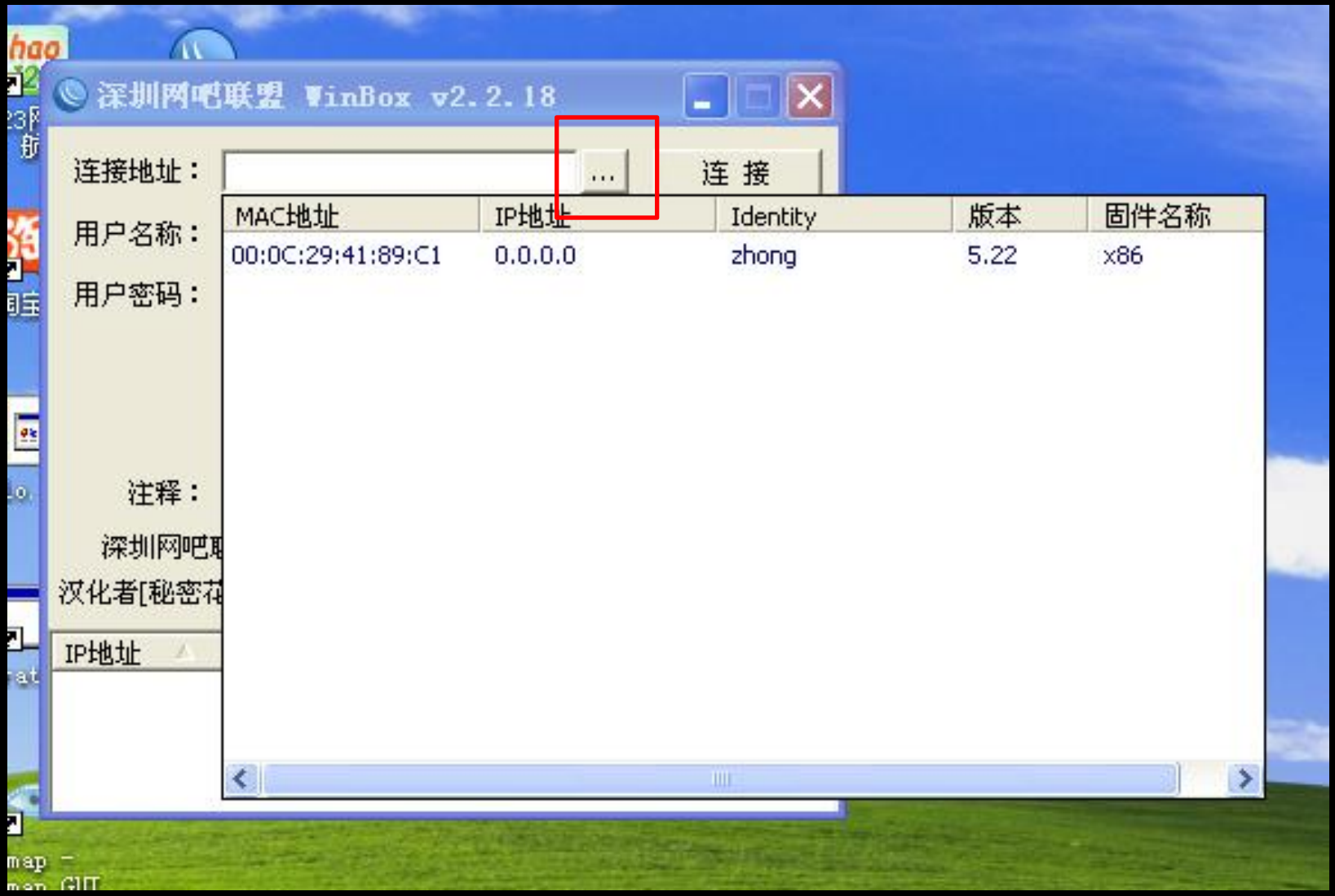
实验：命令行设置IP地址

- 输入add
- Address: 192.168.142.100/24
- Interface: ether1 [前面显示的接口名称]
- 输入print，显示IP配置情况

实验：WinBox设置路由器

- 目的：设置路由器网卡(Interface)IP地址
- 设置：WinBox客户端设置
  - 打开路由器（虚拟机）
  - 打开另一台虚拟机（该虚拟机和路由器相应的网卡处于同一网段，比如同处于WMNet2），打开winbox，登陆（见图，WinBox自动寻找相应的路由器的MAC地址）
  - IP/Addresses/+（选择图标为加号的按钮）
  - Address: 192.168.142.100/24
  - Interface: ether1

实验：WinBox设置路由器



添加路由

- 路由表：RouterOS支持多张路由表，每张路由表有相应的路由标志(routing mark)表示，没有标志的为main（默认）路由表
  - 路由表可以由路由协议获得或者用户构建
  - 每一张路由表都有多条路由(route)组成

路由表项

Route	
Routing Mark	
Destination Address	
Gateway	
Type	unicast/blackhole/prohibit/unreachable
scope	主要用于NEXTHOP查找
target scope	主要用于NEXTHOP查找
pre-src	IP address used for packets generated by this router but not for forwarded packets.

Route

- **Destination Address:** 目的地址，路由决策过程通常匹配最精确的目的地址。
  - 例：路由表中有两条路由：
    - 目标地址：**192.168.134.0/24** 网关：**192.168.138.99**
    - 目标地址：**192.168.134.11/32** 网关：**192.168.140.99**
    - 如果有一个数据包它的目的IP是**192.168.134.11**，那么路由器会选择第二条路由。

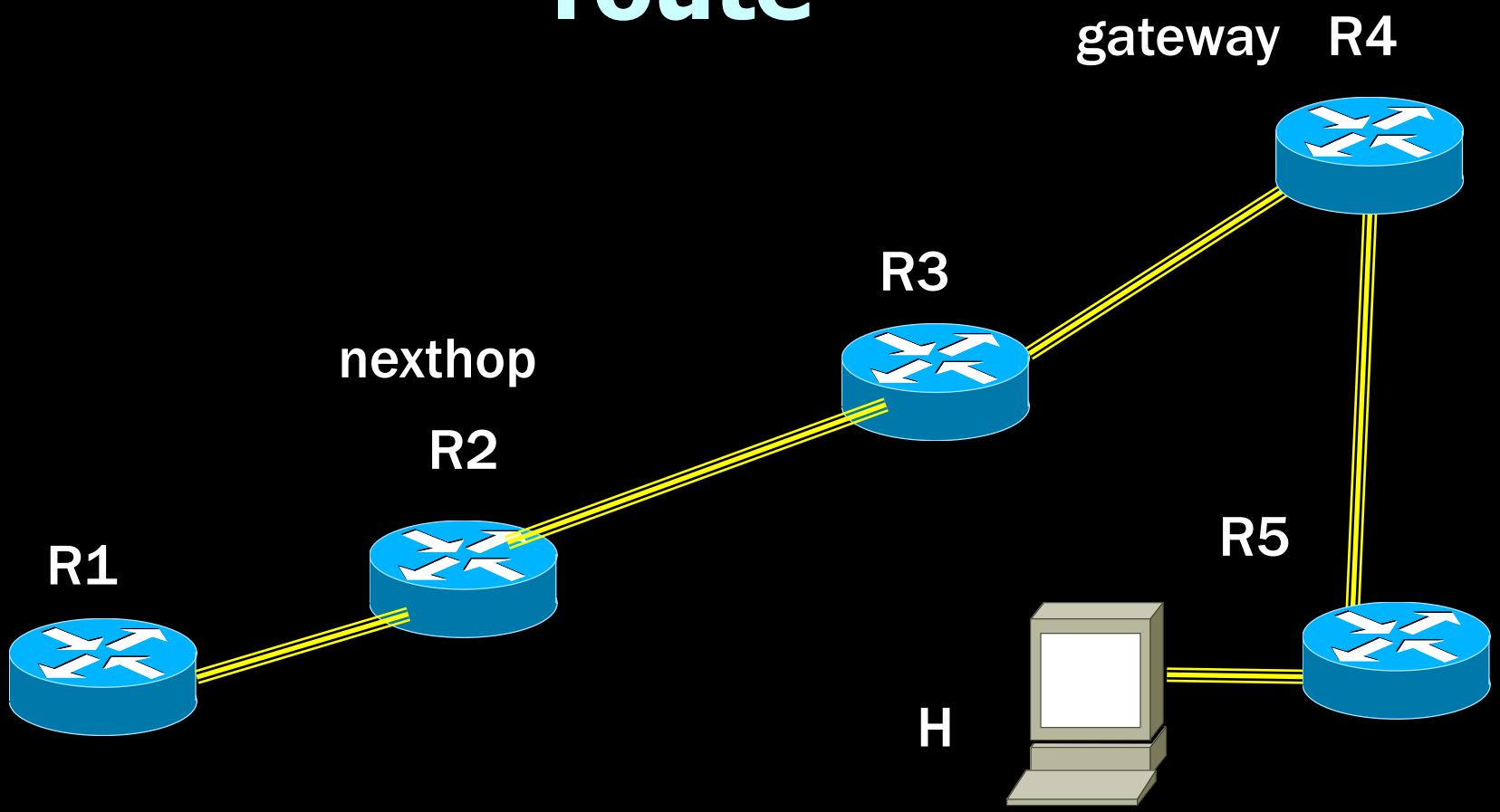
Route

- Gateway: 去往目标地址的网关IP，网关可以离开路由器有几跳距离，不一定非直接可以到达。因此Gateway需要通过Nexthop Lookup来找到最近的Nexthop，这个过程形成了一个Nexthop表
  - Gateway如果为Interface，不需要Nexthop lookup；否则需要Nexthop lookup.

Route

- 如果你设置的Gateway不是可以直接到达，那么需要Nexthop递归查找到能够直接到达的路由器，为了能进行递归查找，scope和target-scope必须设置合理，所以为了方便起见，最好设置成可以直接到达的路由器

route



R1去往H的路由网关可以设置为R4（下一跳确是R2），此时需要Nexthop查找到能够直接到达的路由器（一定要设置target-scope合理范围）

实验：添加路由

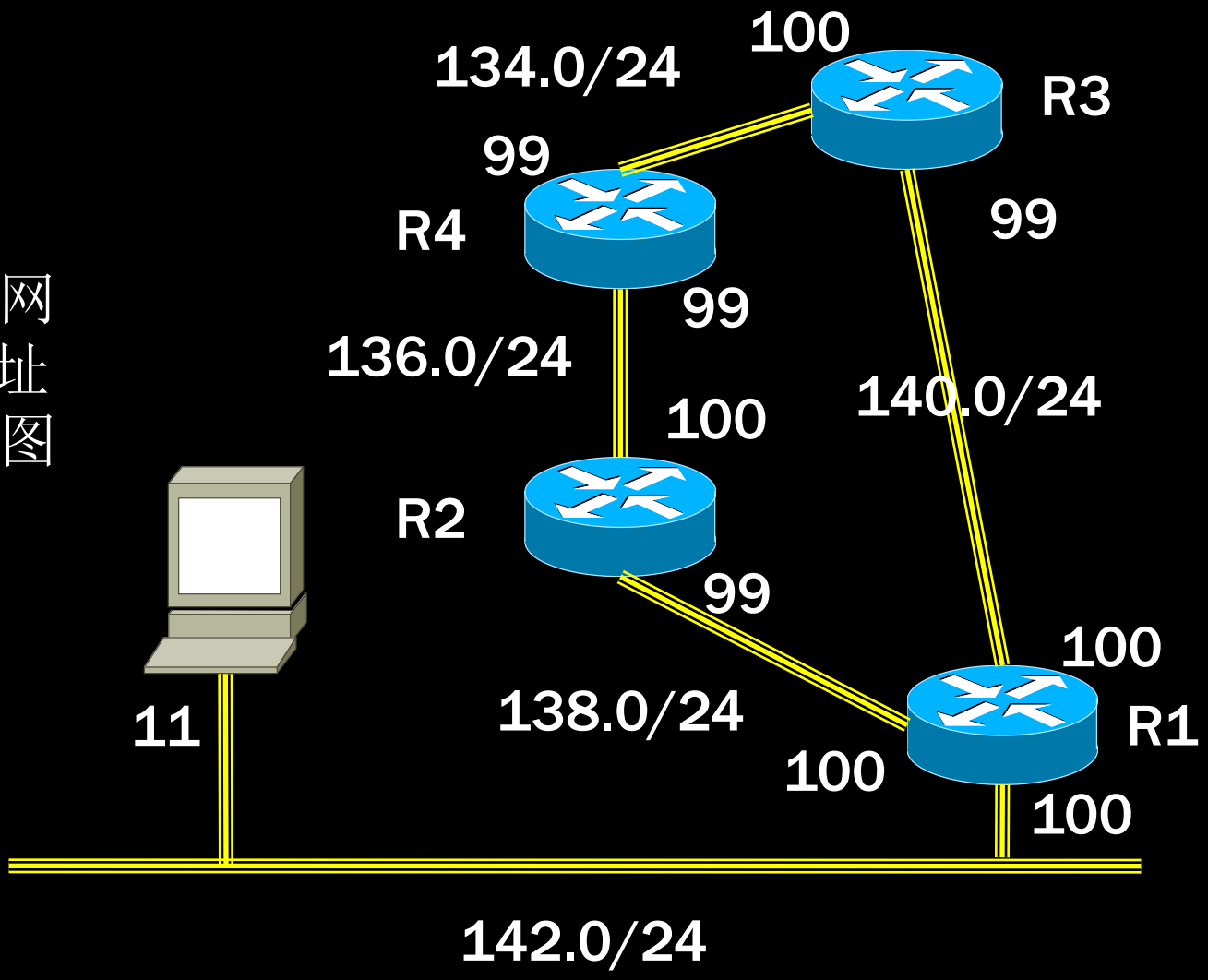
- 可以使用WINBOX
- 命令行方式：
  - ip route
  - add dst-adress 192.168.134.0/24 gateway 192.168.140.99

构建一个简单网络

实验：构建一个简单网络

成绩

注：建立网络时IP地址必须按照图中所示



实验：构建一个简单网络

成绩

- 连线旁边标注的是网络号（省略了192.168前缀），路由器接口旁标注的是接口网址（省略了网络号），构建网络时需注意：
  - 虚拟机拷贝时候很可能网卡的MAC地址也会拷贝（特别是MAC上的WMFUSION），因此可能需要重新产生MAC地址。
  - 编辑网络时，要将默认的添加网络适配器到主机去掉；默认开启DHCP也去掉。

实验：构建一个简单网络

成绩

- 要求：
  - 保证各个设备之间都能互相联通（PING），从各个网段都能访问Web、FTP服务器，并要求能访问外部网络
  - 如果192.168.142.0网络是NAT模式，那么要保证每台路由器和主机都能访问外网，该如何配制路由器？(R1配置NAT或者R1相应接口开启ARP代理）
    - R1配置NAT： IP/Firewall/NAT/General: chain:srcnat, out interface: 往外走的接口, action:masquerade

实验：构建一个简单网络

- 如果192.168.142.0网络是桥接模式，那么要保证每台路由器和主机都能访问外网，该如何配置路由器？假设路由器R1进行拨号连接。

实验：构建一个简单网络

- 如果可以拨号上网，可以在路由器R1上建立一个PPPOE client.
  - R1: (winbox:PPP/Interface/add PPPoE client), General： Interfaces: ether1(外网接口）dial out: 选择Use peer dns(使用ISP服务商提供的DNS），Add default route（相当于增加一个默认网关）
  - R1: IP/DNS/Allow Remote Requests（可供局域网内机器作为DNS服务器）, 查看IP/Routes
  - R1： IP/Firewall/NAT/General: chain:srcnat, out interface: PPPoE接口, action:masquerade

实验：构建一个简单网络

- 如果是使用web认证（网页中输入用户名和密码），比如校园无线网络
  - 主机连接无线热点
  - R1: IP/DHCH client/选择连接外网的接口(ether1)/其他默认/马上就会获得IP地址等信息(status)
  - R1: IP/DNS/Allow Remote Requests（可供局域网内机器作为DNS服务器），查看IP/Routes
  - R1：IP/Firewall/NAT/General: chain:srcnat, out interface: ether1, action:masquerade

实验：构建一个简单网络

- 打开一台虚拟机,IP:192.168.140.11 网关:192.168.140.100, DNS:192.168.140.100;打开浏览器进行Web认证

常见问题

问题：无法PING通

- 可能的常见原因如下：
  - 防火墙原因：无法PING XP， 只要去安全中心关闭防火墙即可
  - VMWare的MAC地址和虚拟机内部MAC地址不一致
    - 设置/网络适配器/高级/MAC地址
    - routeros: interface/ethernet/print
    - 查看两者是否一致
    - 如果不一致使用reset-mac-address重置MAC地址或者用set命令设置MAC地址

问题：无法PING通

- 网卡没有设置IP地址或者地址设置不正确
- 路由器有多张网卡，但设置的IP地址和相应网卡的对应关系搞错
- 没有设置路由
  - 每一个路由器都要有一张去往需要目的地的路由表
  - 网关通常为能够直接到达的下一个路由器：什么叫直接可以到达？
- 默认路由（0.0.0.0/0）：所有不能匹配的目的地址都能匹配此路由
- 通往外网的一台隐形的路由器：192.168.142.2

分析办法

- PING过程通常由请求和响应两个部分
  - 请求是从PING发送者到接收者的过程
  - 应答是从接收者回应发送者的过程
  - 可以在接收者所在的网段开设一台XP，打开其中wireshark，查看是否能够捕获到PING REQUEST来决定目的网络是否能够接收到请求