课程目标

- 能够使用相关命令查看和配置主机网络信息，如ifconfig/ip addr/route等
- 掌握主机名、DNS和静态IP的配置
- 理解路由表的作用
- 能够使用图形抓包工具wireshark进行数据包的抓取

任务要求

1. 最小化安装Centos6.5和Centos7.5系统
2. 配置好静态IP，主机名，网关和DNS
3. 安装wireshark图形抓包工具

理论知识

一、常见的网络接口

接口	描述	备注
eth0	以太网接口	eth0,eth1,ethN
wlan0	无线接口	
enp3s0	以太网接口	Centos7+
lo	本地回环接口	127.0.0.1(默认), 127.x.x.x
virbr0	桥接接口(虚拟交换机)	
br0	桥接接口(虚拟交换机)	
vnet0	KVM虚拟机网卡接口	

二、查看网络信息命令

```
[root@node1 ~]# ip addr                          //查看IP、掩码、MAC
[root@node1 ~]# ip a
[root@node1 ~]# ip addr show eth0                 //只显示eth0的信息
[root@node1 ~]# ip route                         //查看本机路由表
default via 10.1.1.254 dev eth0                  //默认网关，默认路由
[root@node1 ~]# cat /etc/resolv.conf             //查看DNS
nameserver 8.8.8.8
[root@node1 ~]# hostname                        //查看主机名
node1.itcast.cc


ifconfig命令：
1. 给网卡配置临时子接口
   34  ifconfig
   35  ifconfig -a
```

```
   36  ifconfig eth0:1 192.168.0.1 netmask 255.255.255.0
```
重启网络失效

2. 永久生效需要创建子配置文件

```
   40  cp ifcfg-eth0 ifcfg-eth0:1
   41  vi ifcfg-eth0:1
   [root@node2 network-scripts]# cat ifcfg-eth0:1
DEVICE=eth0:1
TYPE=Ethernet
ONBOOT=yes
NM_CONTROLLED=no
BOOTPROTO=none
IPADDR=192.168.0.1
NETMASK=255.255.255.0
GATEWAY=10.1.1.254
```
重启网络

```
service network restart
```

3. 其他命令

```
ifup eth0
ifdown eth1
ifconfig eth0 down/up
```

三、修改网络信息

1. 配置静态IP

方法1:

```
[root@node1 ~]# setup
```

方法2:

修改网卡配置文件

```
[root@node1 ~]# cat /etc/sysconfig/network-scripts/ifcfg-eth0
DEVICE=eth0
TYPE=Ethernet
ONBOOT=yes
BOOTPROTO=none
IPADDR=10.1.1.1
NETMASK=255.255.255.0
GATEWAY=10.1.1.254

++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
DEVICE=eth0              设备名
TYPE=Ethernet            以太网
BOOTPROTO=none           IP地址获取方式，静态: static,none  动态:dhcp,dynamic
ONBOOT=yes               重启网卡是否激活该网卡
BROADCAST=192.168.2.255    广播地址
HWADDR=00:E0:4C:41:95:DB   MAC地址
NM_CONTROLLED=yes          是否接受NetworkManager管理
IPADDR=192.168.2.253       IP地址
```

```
PREFIX=24                  子网掩码 NETMASK=255.255.255.0
NETWORK=192.168.2.0         网络地址
GATEWAY=192.168.2.254        默认网关
DNS1=202.106.0.20           DNS服务器
DNS2=8.8.8.8                DNS服务器备

+++++++++++++++++动态获取IP(dhcp)+++++++++++++++
DEVICE=eth0
BOOTPROTO=dhcp
ONBOOT=yes
```

2. 修改主机名

```
Centos6:
临时修改:

永久修改:

Centos7:
临时修改:

永久修改:
```

3. 配置DNS

```
[root@node2 ~]# cat /etc/resolv.conf
nameserver DNS服务器
nameserver 114.114.114.114
nameserver 8.8.8.8
nameserver 192.168.159.2
```

4. 关闭防火墙和selinux

```
Centos6.5:
临时关闭:
[root@node2 ~]# service iptables stop
iptables: Setting chains to policy ACCEPT: filter          [  OK  ]
iptables: Flushing firewall rules:                         [  OK  ]
iptables: Unloading modules:                               [  OK  ]
[root@node2 ~]# service iptables status
iptables: Firewall is not running.
[root@node2 ~]#
开机自动关闭:
[root@node2 ~]# chkconfig --list|grep iptables
iptables          0:off 1:off 2:on  3:on  4:on  5:on  6:off
[root@node2 ~]# chkconfig iptables off
```

```
Centos7.5:
[root@centos7 ~]# systemctl status firewalld    //查看防火墙状态
[root@centos7 ~]# systemctl stop firewalld      //临时关闭防火墙
查看防火墙是否开机自动启动：enabled表示自动启动；disabled表示关闭
[root@centos7 ~]# systemctl list-unit-files|grep firewalld
firewalld.service                             enabled
[root@centos7 ~]# systemctl disable firewalld      //永久关闭防火墙，开机不自动启动
Removed symlink /etc/systemd/system/multi-user.target.wants/firewalld.service.
Removed symlink /etc/systemd/system/dbus-org.fedoraproject.FirewallD1.service.
[root@centos7 ~]# systemctl list-unit-files|grep firewalld
firewalld.service                             disabled

[root@centos7 ~]# systemctl enable firewalld    //开机自动启动

关闭selinux：
[root@node2 ~]# getenforce
Enforcing
[root@node2 ~]# setenforce
usage:  setenforce [ Enforcing | Permissive | 1 | 0 ]
[root@node2 ~]# setenforce 0     临时变成警告模式
[root@node2 ~]# getenforce
Permissive
[root@node2 ~]# cat /etc/selinux/config
...
SELINUX=disabled     //关闭selinux，下次开机生效
...
```

5. 其他工具

```
lspci：显示系统中所有PCI总线设备或连接到该总线上的所有设备的工具
//查看当前主机的所有网卡（包括已经驱动了和没有驱动）
[root@misshou ~]# lspci |grep -i eth
00:03.0 Ethernet controller: Red Hat, Inc Virtio network device

//查看物理连接状态（网线是否ok）
[root@misshou ~]# ethtool eth0
Settings for eth0:
   Link detected: yes

[root@node1 ~]# mii-tool eth0
eth0: negotiated 100baseTx-FD, link ok
```

四、抓包工具

1. wireshark工具

```
1. 挂载光盘到虚拟机
```

```
虚拟机—>设置—>CD/DVD—>选择ISO映像文件（系统什么版本就选择什么版本）—>选择启动时连接和连接
2. 修改配置文件
[root@node1 yum.repos.d]# pwd
/etc/yum.repos.d
[root@node1 yum.repos.d]# vim server.repo
[root@node1 yum.repos.d]# cat server.repo
[server]
name=xxxx
baseurl=file:///media/CentOS_6.5_Final/
enable=1
gpgcheck=0

3.清除yum缓存
[root@node1 yum.repos.d]# yum clean all
Loaded plugins: fastestmirror, refresh-packagekit, security
Cleaning repos: server
Cleaning up Everything
Cleaning up list of fastest mirrors
[root@node1 yum.repos.d]# yum makecache
Loaded plugins: fastestmirror, refresh-packagekit, security
Determining fastest mirrors
server                                                   | 4.0 kB     00:00 ...
server/group_gz                                          | 220 kB     00:00 ...
server/filelists_db                                      | 5.8 MB     00:00 ...
server/primary_db                                        | 4.4 MB     00:00 ...
server/other_db                                          | 2.7 MB     00:00 ...
Metadata Cache Created

4. 安装wireshark工具
[root@node1 yum.repos.d]# yum -y install wireshark
```

2. tcpdump工具

```
查看arp缓存 （同一网段主机的MAC地址）
[root@node1 Desktop]# arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.1.1.254               ether   00:50:56:c0:00:01   C                     eth0
删除目标主机的MAC缓存
[root@node1 Desktop]# arp -d 10.1.1.254
[root@node1 Desktop]# arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.1.1.254                       (incomplete)                              eth0

查看主机10.1.1.1收到的和发送的数据包
[root@node1 Desktop]# tcpdump -i eth0 -nn host 10.1.1.1
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
22:33:25.148389 ARP, Request who-has 10.1.1.254 tell 10.1.1.1, length 28
22:33:25.148896 ARP, Reply 10.1.1.254 is-at 00:50:56:c0:00:01, length 46
22:33:30.714605 IP 10.1.1.254 > 10.1.1.1: ICMP echo request, id 1, seq 237, length 40
```

```
22:33:30.714619 IP 10.1.1.1 > 10.1.1.254: ICMP echo reply, id 1, seq 237, length 40
```

-i 指定网络接口，对于多个网络接口有用
-n 显示IP地址，不查主机名。当DNS不起作用时常用到这个参数
-nn 不显示协议和端口名。即显示IP地址和端口

其他用法：

```
man tcpdump
TCP Packets
The general format of a tcp protocol line is:
              src > dst: flags data-seqno ack window urgent options
       Src and dst are the source and destination IP addresses and ports.  Flags are some
combination  of  S
       (SYN),  F  (FIN),  P (PUSH), R (RST), W (ECN CWR) or E (ECN-Echo), or a single '.' (no
flags).
```

1.获取主机10.1.1.1接收或发出的telnet包

```
#tcpdump tcp port 23 and host 10.1.1.1
```

2.对本机的udp协议的123端口进行监听（123是ntp服务端口）

```
# tcpdump udp port 123
```

3.只对hostname的主机的通信数据包进行监视。主机名可以是本地主机，也可以是网络上的任何一台计算机。
下面的命令可以查看主机hostname发送的所有数据：

```
#tcpdump -i eth0 src host hostname
#tcpdump -i eth0 src host 10.1.1.254
```

4.下面的命令可以查看所有送到主机hostname的数据包：

```
#tcpdump -i eth0 dst host hostname
#tcpdump -i eth0 dst host 10.1.1.1
```

5.监视通过指定网关的数据包：

```
#tcpdump -i eth0 gateway Gatewayname
#tcpdump -i eth0 gateway 10.1.1.254
```

6.其他
只需要列出送到80端口的数据包，用dst port;

```
#tcpdump –i eth0 host hostname and dst port 80   //目的端口是80
```

只需要看到返回80端口的数据包，用src port

```
#tcpdump –i eth0 host hostname and src port 80  //源端口是80,一般是提供http的服务的主机
```

如果条件很多的话要在条件之前加and 或 or 或 not

```
#tcpdump -i eth0 host ! 210.161.223.70 and ! 210.161.223.71 and dst port 80
```