

基础知识

OSI模型

OSI模型用于定义并理解数据从一台计算机转移到另一台计算机，为了完成不同计算机或网络或架构之间的成功通信，国际标准化组织提出了OSI七层模型，该模型(从上到下)包括了应用层、表示层、会话层、传输层、网络层、数据链路层、物理层。

TCP/IP协议

- OSI 参考模型太过于复杂，功能重叠，没有商业化运作，设计时间久，所以只作为理论模型
- 随着阿帕网（因特网的前身）的发展，TCP/IP 协议逐渐成为工业界实际上的事实模型

IPv4

- IP协议是TCP/IP体系中的网络层协议，计算机之间利用IP地址进行身份确认和通信
- 设计IP的目的是提高网络的可扩展性，用于分割顶层网络应用和底层网络技术之间的耦合关系，以利于两者的独立发展
- IP协议又分IPv4、IPv5、IPv6，本教程的网络全部基于IPv4，符合中国大陆的基本国情。
- IPv4地址格式，这里我们只需要知道点分十进制，他把32位的二进制分成4段，每段8位，段与段之间用“.”分隔，并采用十进制来表示，其中每段的取值范围是十进制的0~255，如：`192.168.10.1`

网络分类

- A类地址
 - 由1个字节的网络地址和3个字节的主机地址，网络地址的最高位必须是 0
 - A类IP地址范围：1.0.0.1-126.255.255.254
 - A类IP地址中的私有地址：**10.0.0.1-10.255.255.254**
- B类地址
 - 由2个字节的网络地址和2个字节的主机地址，网络地址的最高位必须是 10
 - B类IP地址范围：128.0.0.1-191.255.255.254
 - B类IP地址中的私有地址：**172.16.0.0-172.31.255.254**
- C类地址
 - 由3个字节的网络地址和1个字节的主机地址，网络地址的最高位必须是 110
 - C类IP地址范围：192.0.0.1-223.255.255.254
 - C类IP地址中的私有地址：**192.168.0.1-192.168.255.255**

局域网

局域网指有限区域（如办公室或楼层）内的多台计算机通过传输介质互连，所组成的封闭网络。

现实中的情况是，在一定空间内通过同一个路由器、一台或多台交换机连接的多台设备就在一个局域网内，不需要过多深入的研究。

NAT

Network Address Translation，网络地址转换协议

随着接入Internet的计算机数量的不断猛增，IP地址资源也就愈加显得捉襟见肘，少量的IP地址根本无法满足网络用户的需求，于是也就产生了NAT技术。

基于RFC 1918规范，为私有网络预留出了三个IP地址块，即上述A、B、C三类地址中的私有地址，这三个范围内的地址不会在因特网上被分配，因此可以不必向ISP或注册中心申请而在公司或企业内部自由使用。

NAT技术原理在此不详细阐述，只需要知道NAT是利用这三个私有地址段，将局域网内的IP地址转换为公网IP地址，所以**局域网内主机的IP地址，一定是上述的三个私有地址段内，其中以B类和C类的私有地址段最为常见。**

连通性

根据IP地址和子网掩码进行与运算，如果结果相同，则在一个局域网内，此时使用[ping命令](#)：`ping 远程主机ip地址`，测试是否能联通。

通常来说大家只需要看IP地址前三个数字是否相同，就可以判断是否在一个局域网内，因为一般子网掩码是255.255.255.0

网络工具

通用

ping

测试远程主机是否能联通：`ping IP地址`，出现回复则说明能联通，在同一个网络内

```
C:\Users\Administrator>ping 192.168.26.136

正在 Ping 192.168.26.136 具有 32 字节的数据:
来自 192.168.26.136 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.26.136 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.26.136 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.26.136 的回复: 字节=32 时间<1ms TTL=64

192.168.26.136 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms, 最长 = 0ms, 平均 = 0ms
```

Linux

net-tools

ifconfig

- 查看已启用的网卡信息: `ifconfig`
 - 其中非回环网络即主机的网络, inet为IPv4地址

```
diklios@diklios-virtual-machine-mint:~$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:93:a5:3e brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.26.139/24 brd 192.168.26.255 scope global dynamic noprefixroute ens33
        valid_lft 1217sec preferred_lft 1217sec
    inet6 fe80::23ae:849:8a8b:5be0/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

route

- 查看路由表: `route -n`

netstat

- 查看 TCP 端口占用: `sudo netstat -tlnp | grep 端口号`
- 查看 UDP 端口占用: `sudo netstat -ulnp | grep 端口号`

iproute2

iproute2 是 linux 下管理控制 TCP/IP 网络和流量控制的新一代工具包, 旨在替代老派的工具链 net-tools, 即大家比较熟悉的 ifconfig, arp, route, netstat 等命令。

ip address

- ip address命令是在Linux系统中配置IP地址的一个命令, 它是ifconfig命令的现代替代品
- 查看本地网络: `ip address`

- 与ifconfig相同，查看inet即可知道本机IP地址

```
diklios@diklios-virtual-machine-mint:~$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:93:a5:3e brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.26.139/24 brd 192.168.26.255 scope global dynamic noprefixroute ens33
        valid_lft 1183sec preferred_lft 1183sec
    inet6 fe80::23ae:849:8a8b:5be0/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

firewall-cmd

- 查询指定端口是否已开启: `firewall-cmd --query-port=端口号/tcp`
 - yes表示开启
 - no表示未开启
- 列出全部生效的防火墙配置: `firewall-cmd --list-all`
- 添加指定需要开放的TCP端口: `firewall-cmd --add-port=端口号/tcp --permanent`
- 执行防火墙命令重载: `firewall-cmd --reload`
- 关闭端口: `firewall-cmd --remove-port=端口号/tcp --permanent`

iptables

Windows

ipconfig

打开 cmd 或者 powershell，输入 ipconfig 并回车运行，查看以太网适配器，只需要查看IPv4地址，即可得到主机的IP地址

```
以太网适配器 Ethernet0:

    连接特定的 DNS 后缀 . . . . . : localdomain
    本地链接 IPv6 地址. . . . . : fe80::78c1:7fb9:df19:d0e7%12
    IPv4 地址 . . . . . : 192.168.26.136
    子网掩码 . . . . . : 255.255.255.0
    默认网关. . . . . : 192.168.26.2
```

route

Windows下查看和操作路由表的命令，虽然与Linux系统中的route是相同作用，但是语法并不相同

- 语法: `ROUTE [-f] [-p] [-4|-6] command [destination] [MASK netmask] [gateway] [METRIC metric] [IF interface]`

- 查看路由表: `route print`
- 查看ipv4 路由表: `route print -4`

netstat

- 查看 TCP 占用端口: `netstat -anp tcp`
- 查看 UDP 占用端口: `netstat -anp udp`

操作路由表

todo: 待补充

双网卡

多网段通信
