西安电子科技大学 XIDIAN UNIVERSITY
计算机科学与技术学院 School of Computer Science and Technology
国家示范性软件学院 National Pilot School of Software Engineering

计算机安全导论

第6章
网络安全 I

主讲人：张志为

二〇二四年秋季学期

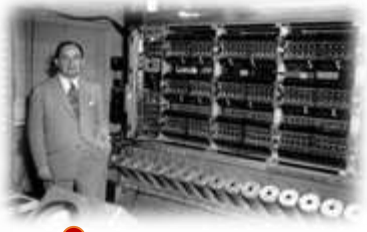
计算机的发展历程

查尔斯·巴贝奇研制了首台计算原型机 — 差分机，并设计分析仪

图灵从理论上证明计算机的存在性-图灵机模型

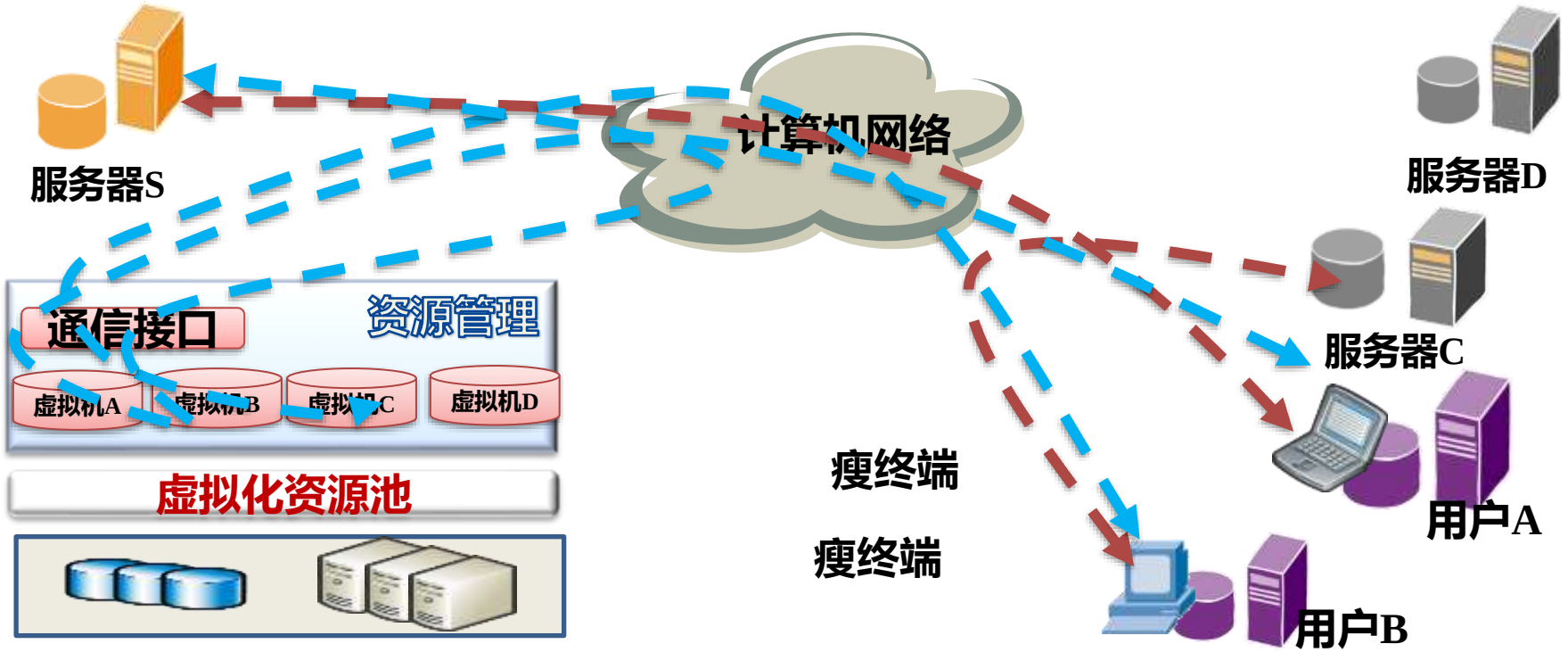
世界上第一台现代电子计算机ENIAC

冯·诺依曼提出存储程序原理，即冯·诺依曼体系结构

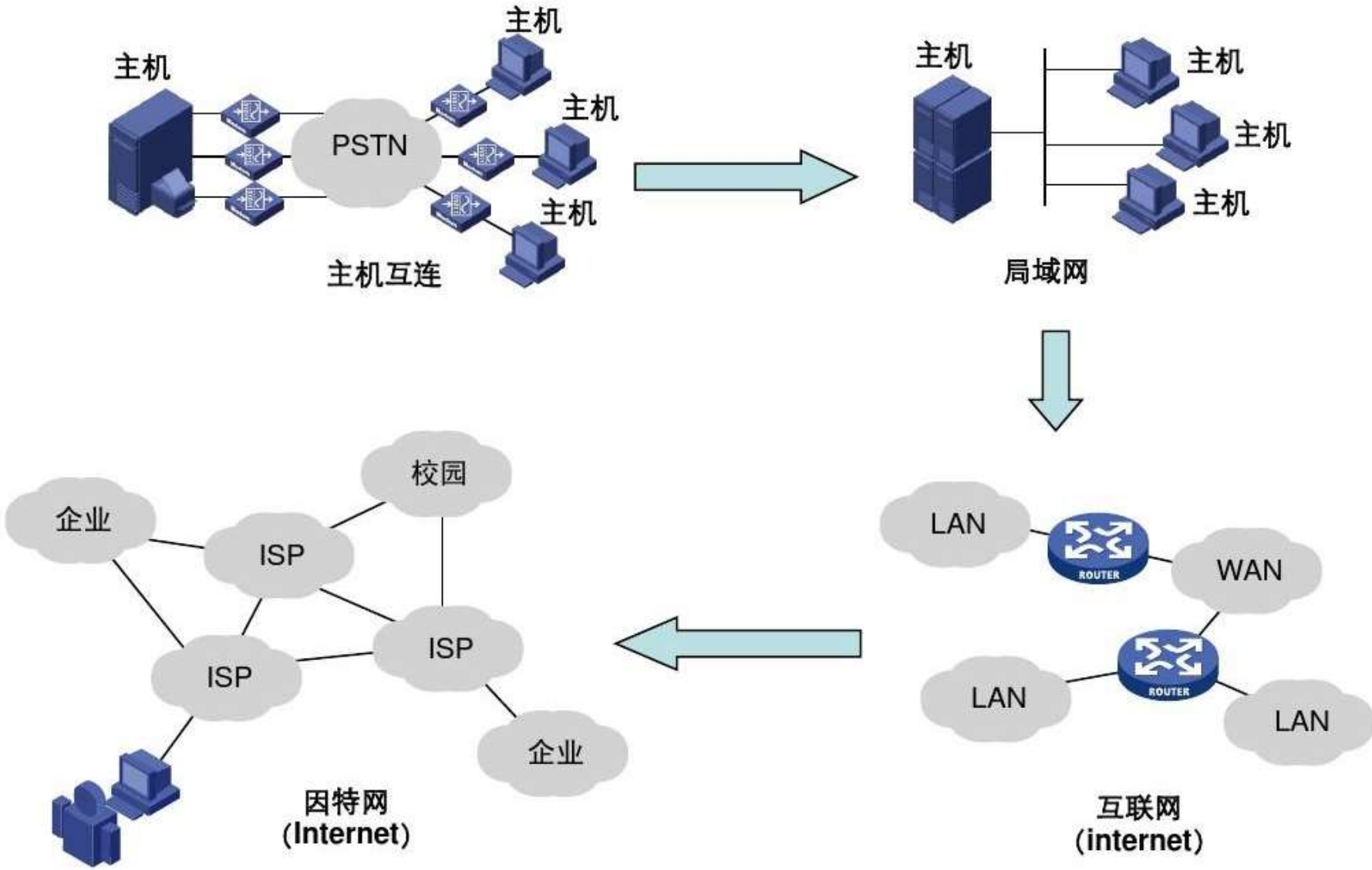


19世纪 — 1936年 — 1946年

大型机 → **桌面PC** → **移动PC** → **云计算** → **边缘计算**



计算机网络

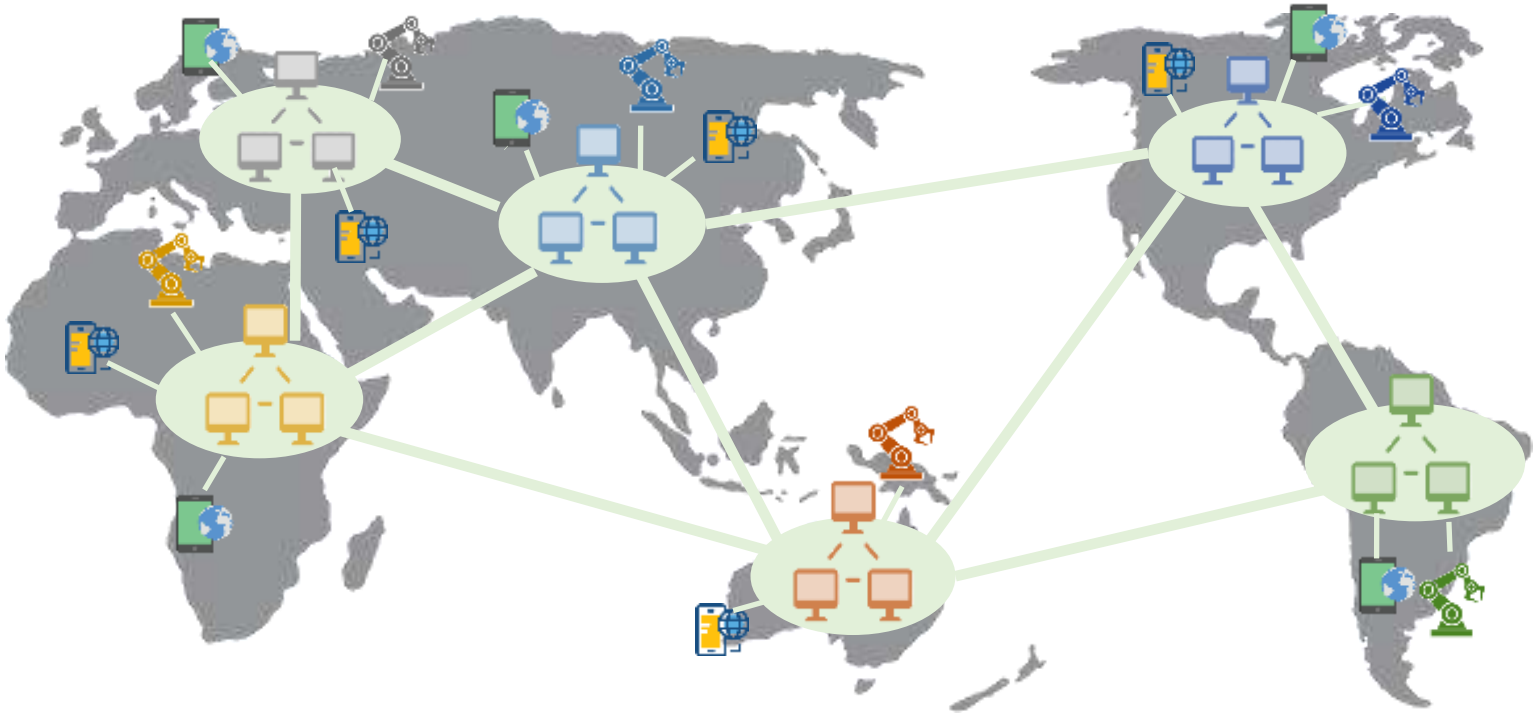

主机
主机
主机
主机
PSTN
主机互连
主机
主机
主机
局域网
LAN
ROUTER
WAN
ROUTER
LAN
LAN
互联网
(internet)
校园
企业
ISP
ISP
ISP
企业
因特网
(Internet)

互联网的演进历程

传统互联网
- 门户网站
- 搜索引擎
- 电子邮件

移动互联网
- 社交网络
- 自媒体
- 移动支付

工业互联网
- 智慧工厂
- 智能制造
- 智慧物流

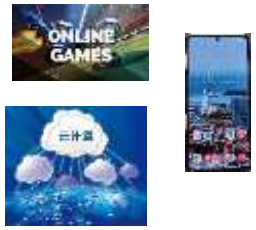


卫星互联网

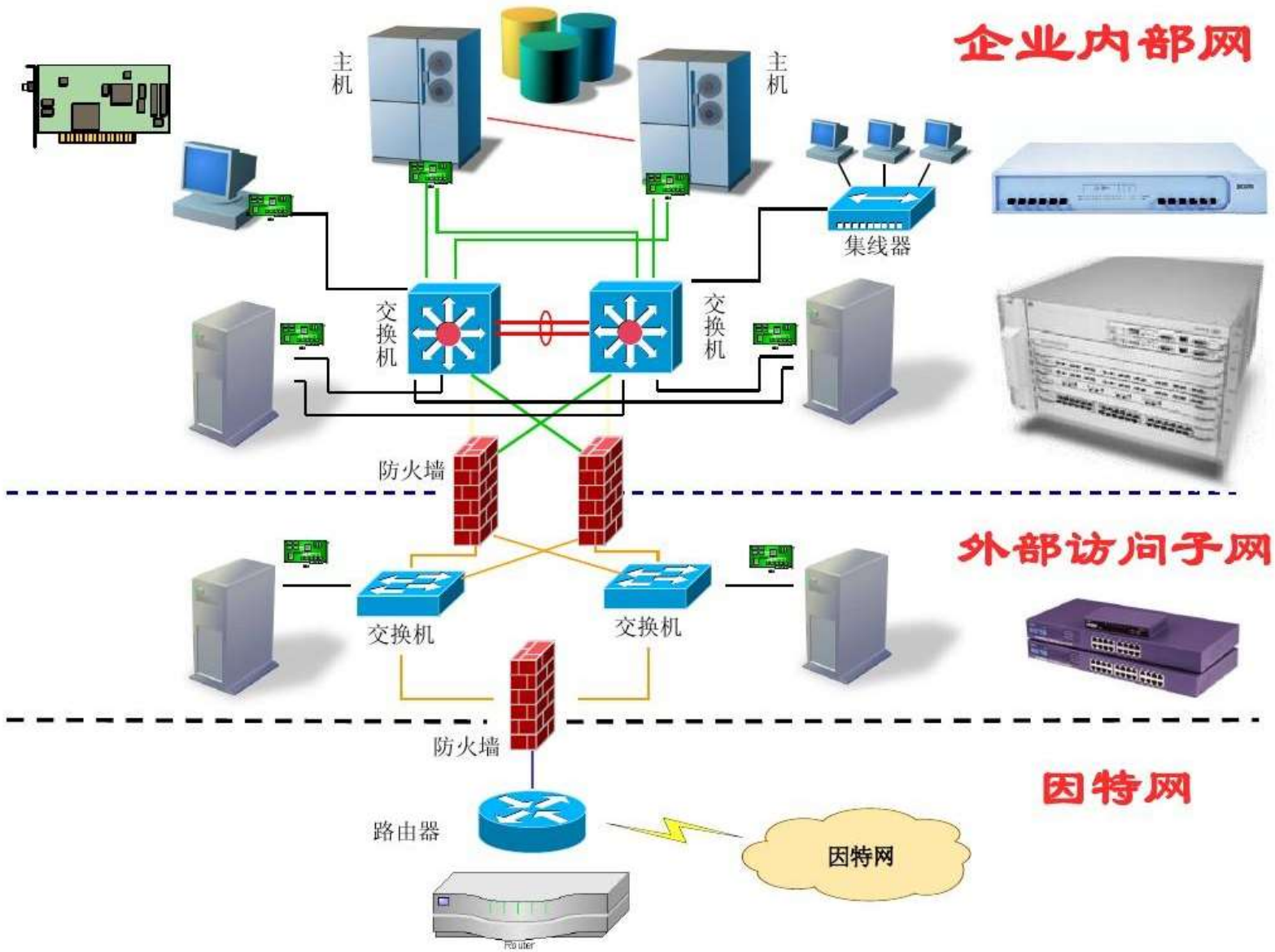
移动通信的演进历程

1980	1990	2000	2010	2020	2030
1G	2G	3G	4G	5G	6G
模拟电话	数字电话	数据服务	移动宽带	移动物联	泛在智联
TACS AMPS NMT FDMA	GSM IS-95 IS-136 PDC	WCDMA TD-SC CDMA WiMAX	LTE OFDMA	3GPP MmWave	THz LC AI RIS
2.4Kbps	64Kbps	2Mbps	100Mbps	20Gbps	1Tbps

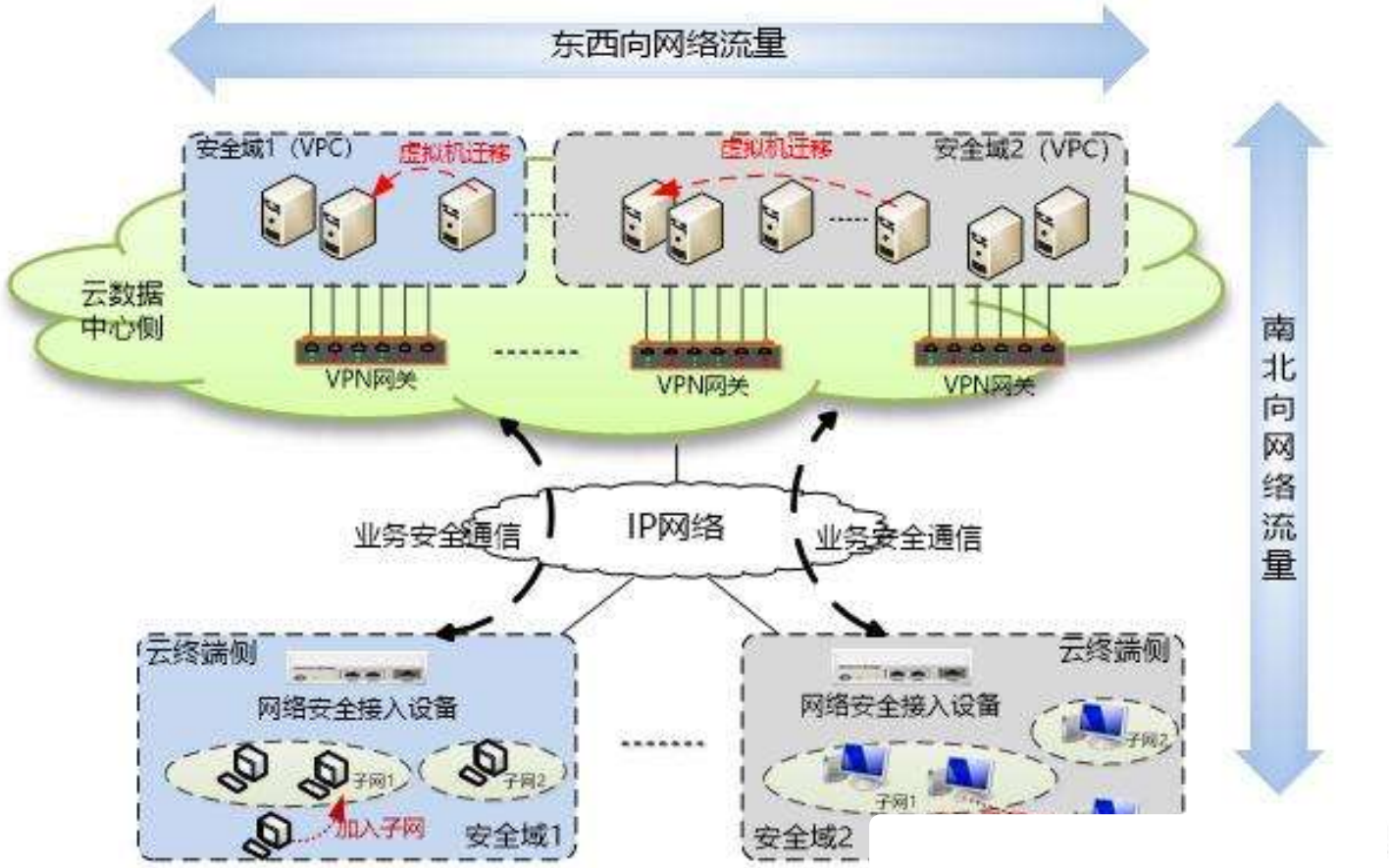
空天地无缝立体的万物智联时代

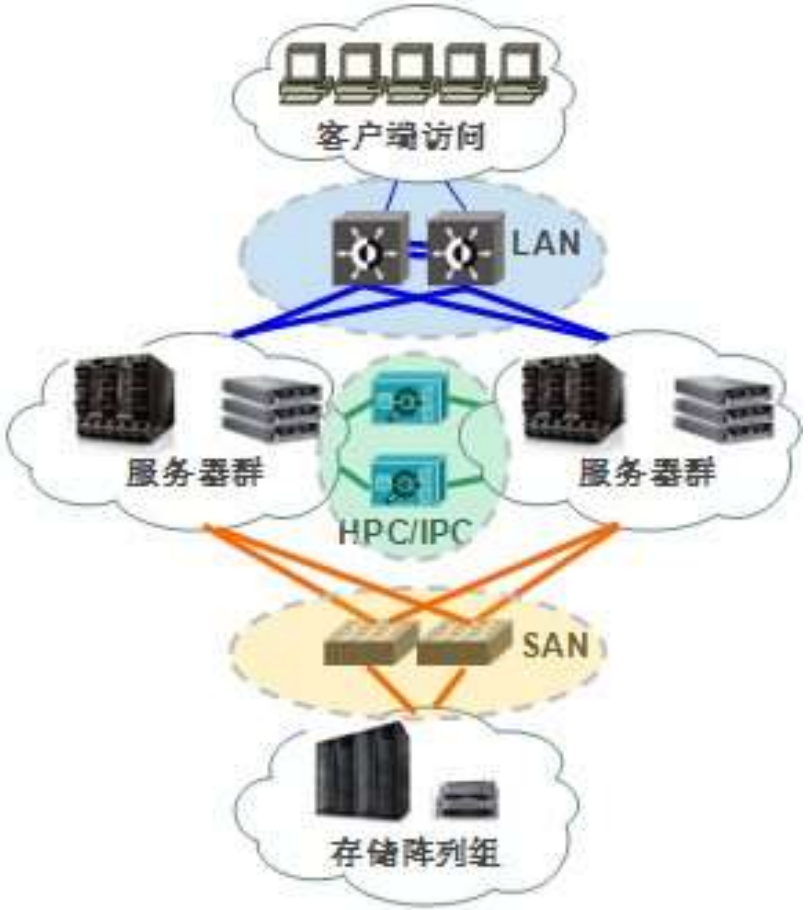


计算机网络常见设备

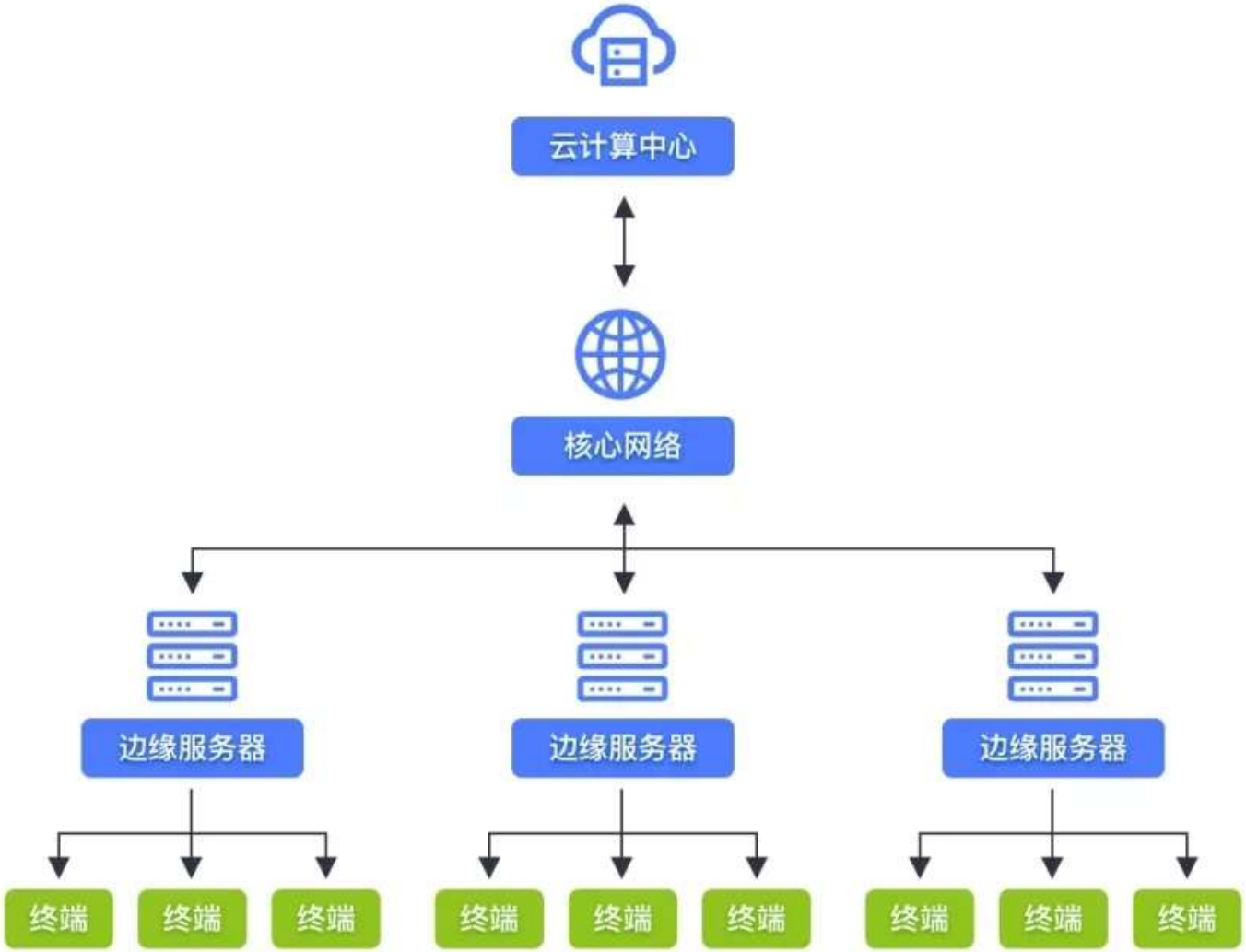


云计算网络架构


东西向网络流量
安全域1（VPC）
虚拟机迁移
虚拟机迁移
安全域2（VPC）
云数据
中心侧
VPN网关
VPN网关
VPN网关
业务安全通信
IP网络
业务安全通信
南北向网络流量
云终端侧
网络安全接入设备
子网1
子网2
加入子网
安全域1
云终端侧
网络安全接入设备
子网2
子网1
安全域2

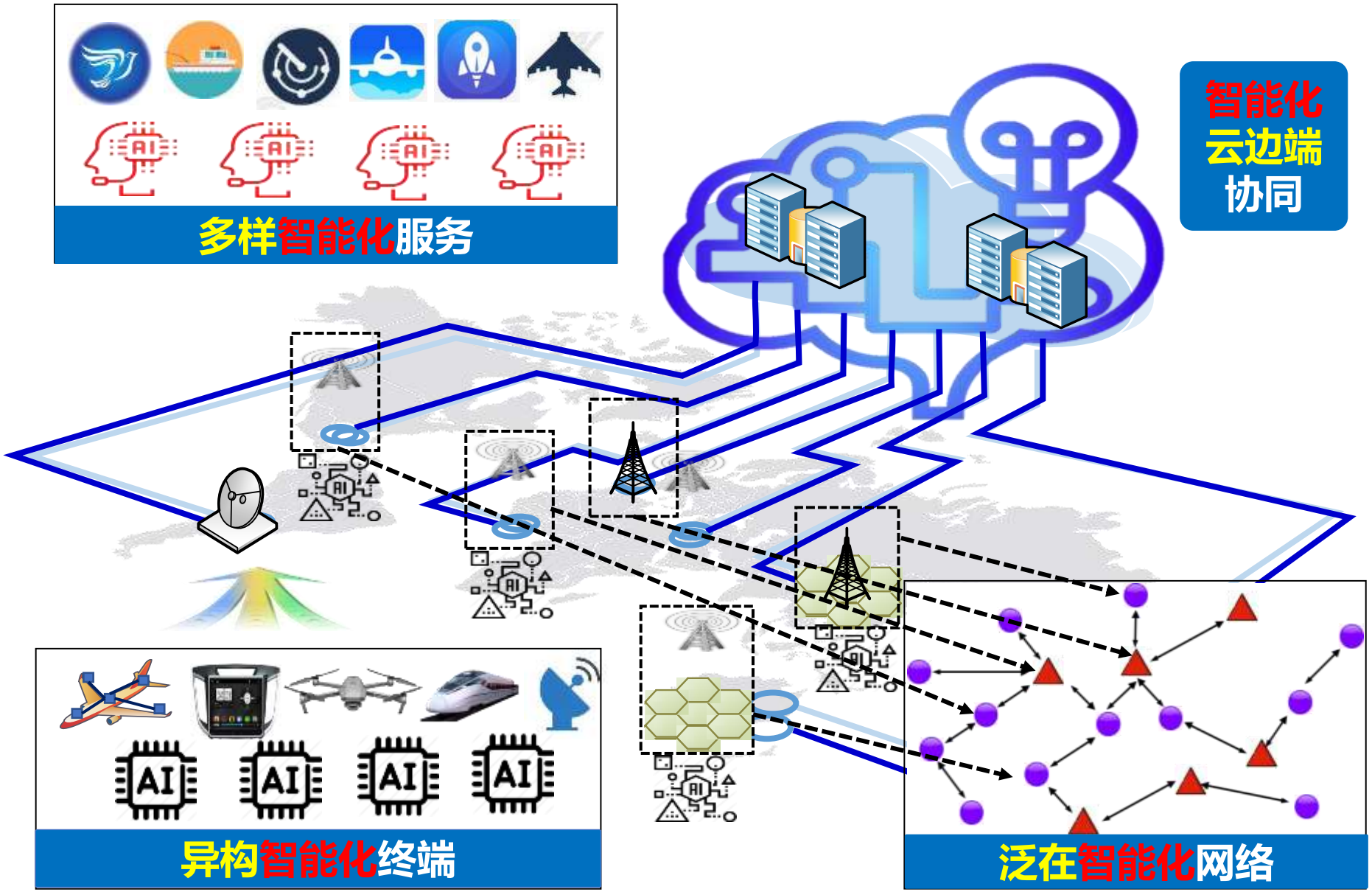

客户端访问
LAN
服务器群
HPC/IPC
服务器群
SAN
存储阵列组

边缘计算基本网络架构



网络信息系统现状与演化趋势

网络信息系统现状与演化趋势



协议三要素

- 语法
- 语义
- 同步

提纲

PART 1 网络安全基本概念

PART 2 链路层及其安全

PART 3 网络层及其安全

PART 4 传输层及其安全

PART 5 拒绝服务DoS攻击

提纲

PART 1 网络安全基本概念

PART 2 链路层及其安全

PART 3 网络层及其安全

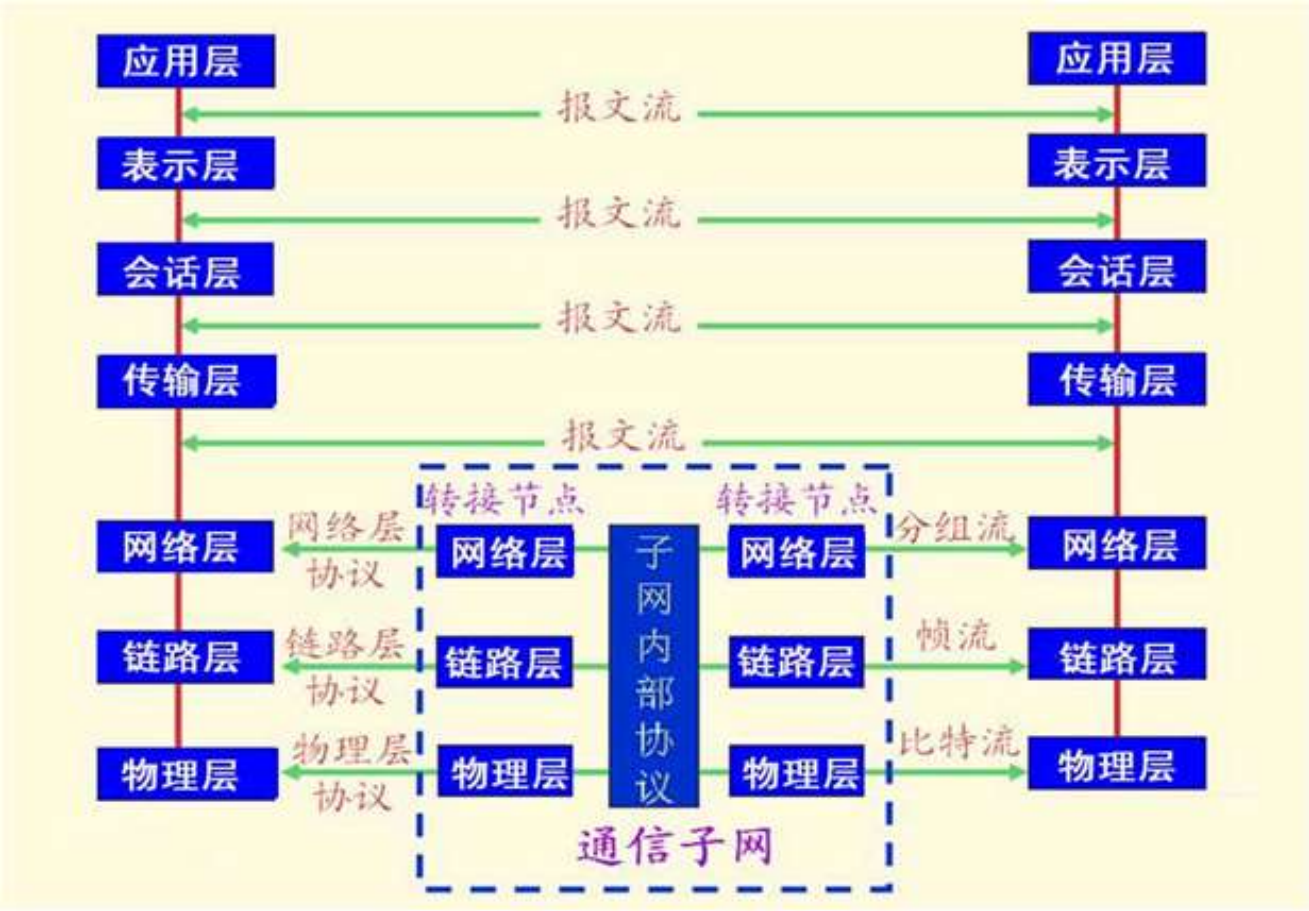
PART 4 传输层及其安全

PART 5 拒绝服务DoS攻击

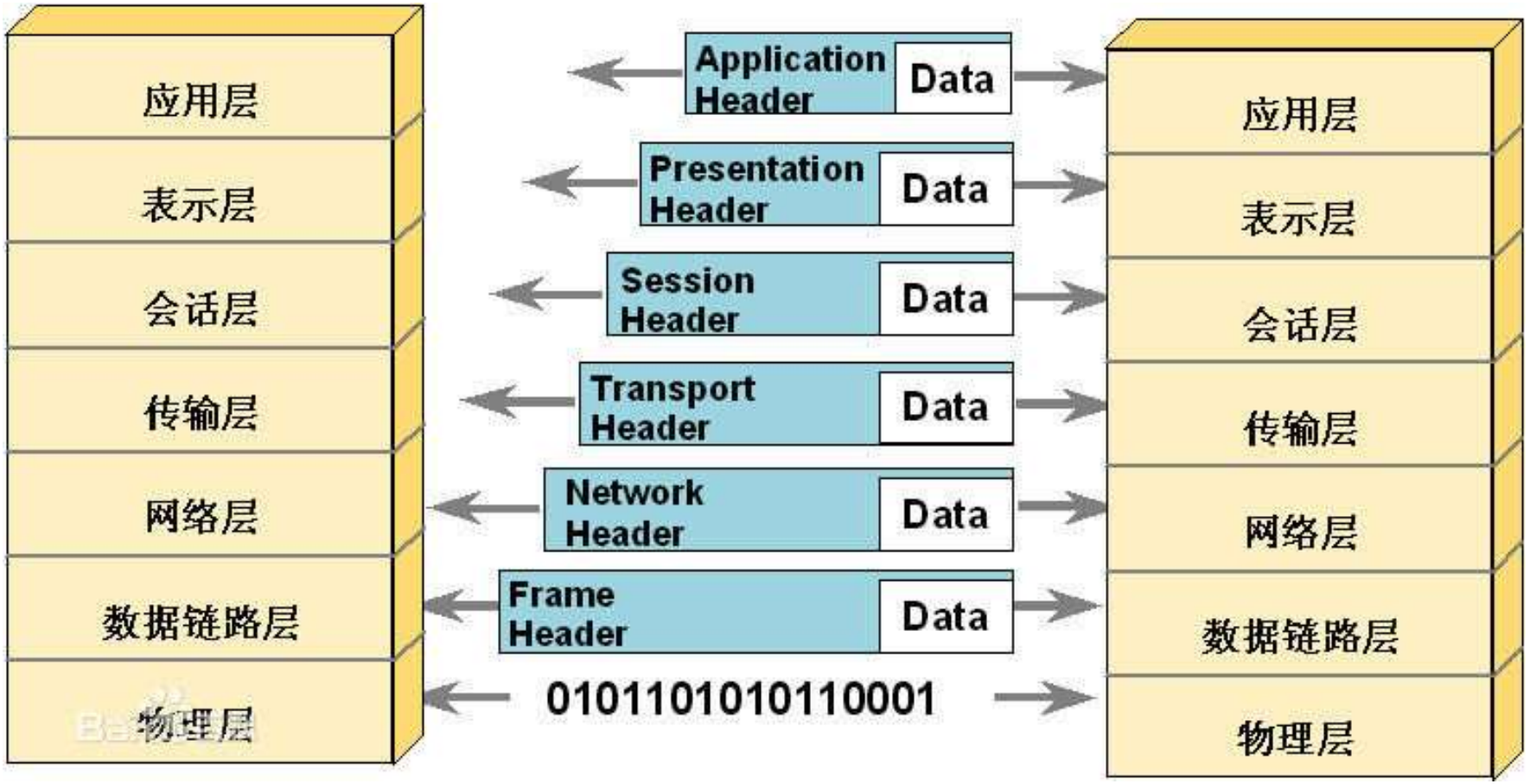
OSI七层网络协议

OSI: Open System Interconnection

OSI七层网络模型

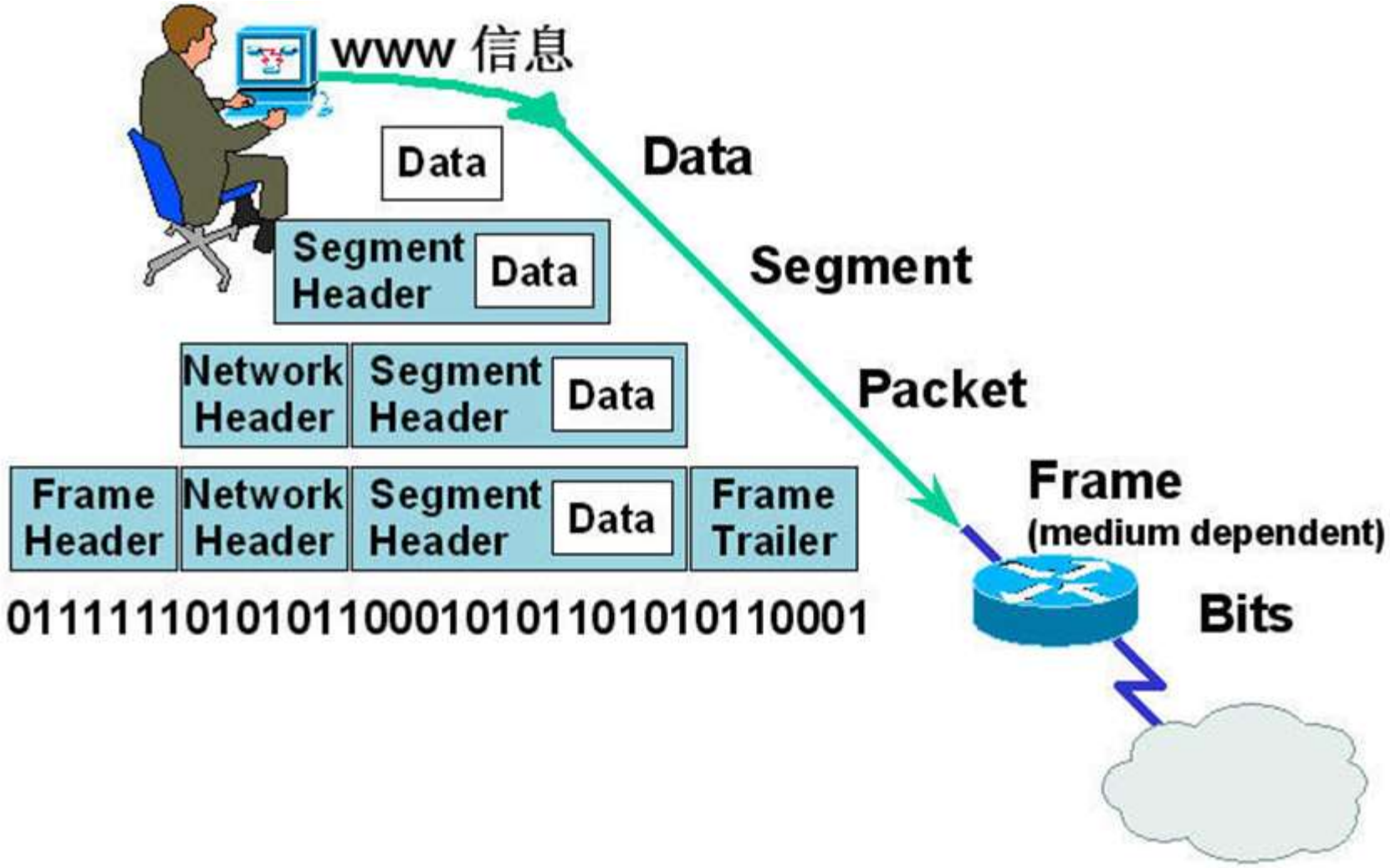


OSI七层网络协议



OSI七层网络模型数据封装

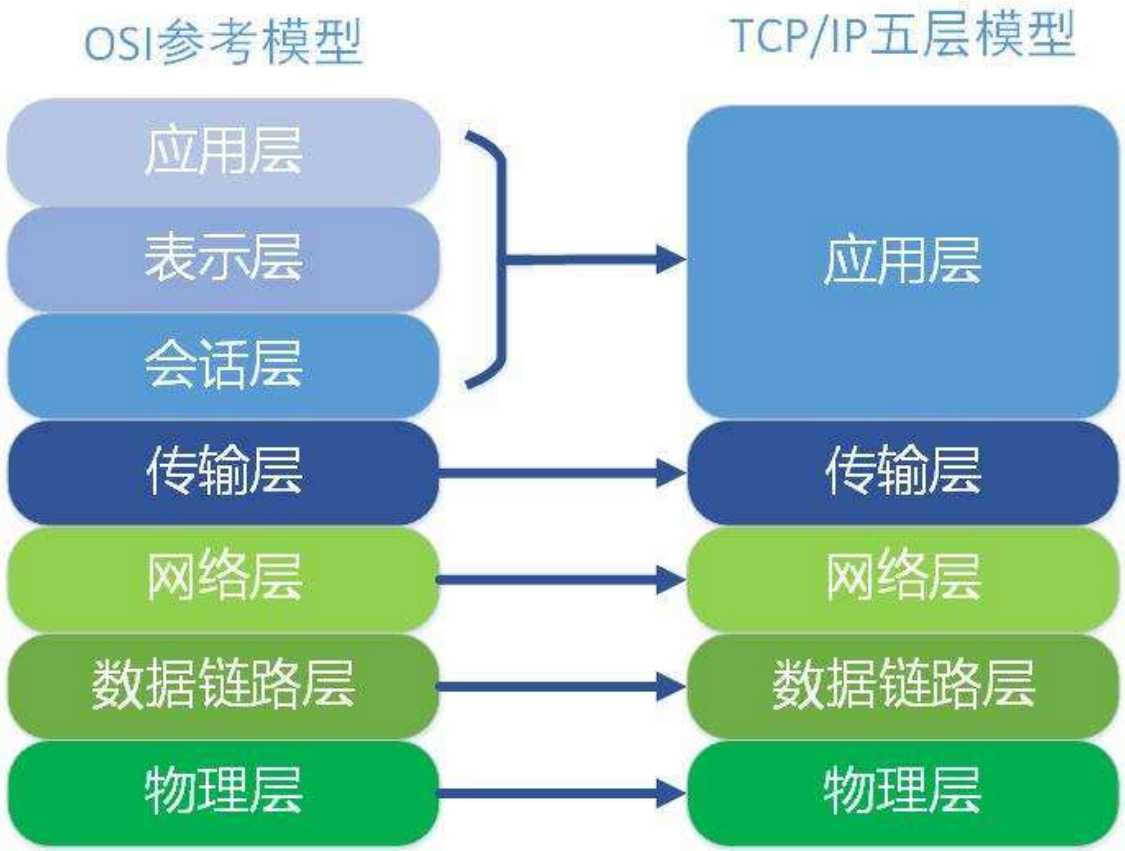
OSI七层网络协议

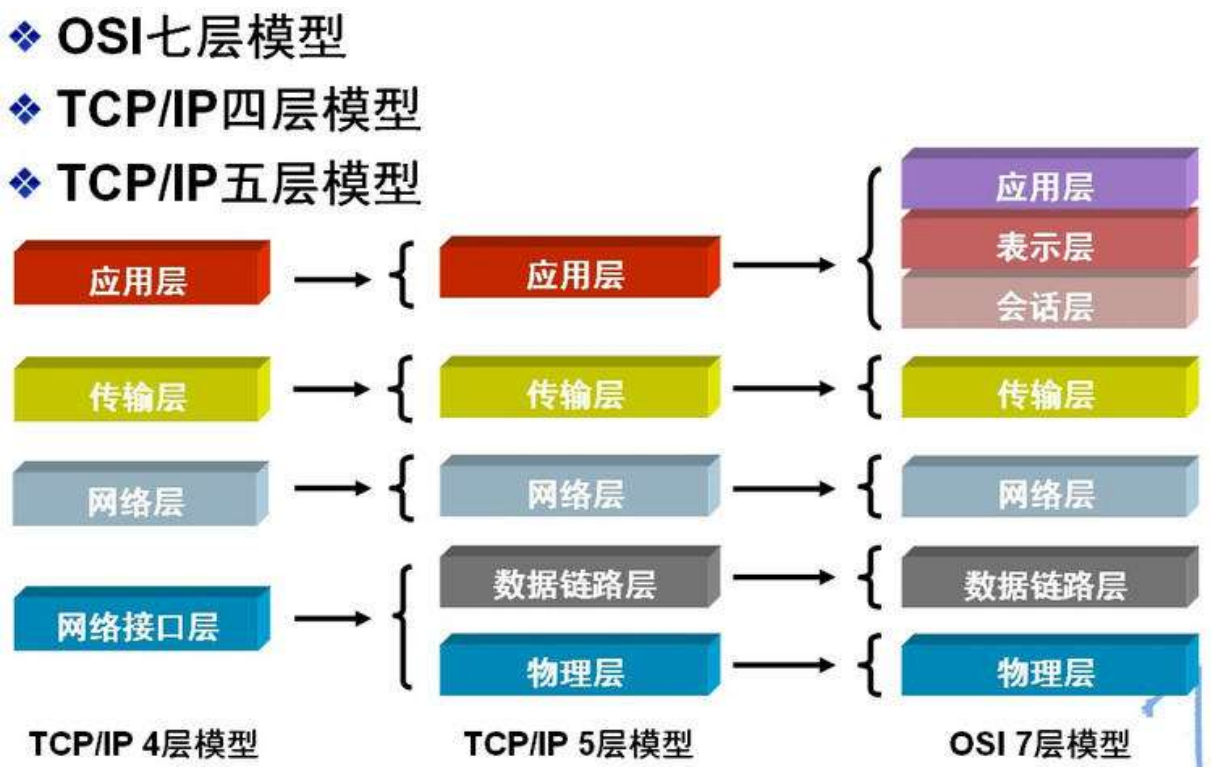


OSI七层网络模型数据封装

TCP/IP协议

TCP/IP协议五层模型：应用层、传输层、网络层、数据链路层、物理层





- **物理层(Physical layer)**
  - 规定通信设备的机械的、电气的、功能的和过程的特性，用以建立、维护和拆除物理链路连接。
  - 在这一层，数据的单位称为比特（bit）。
  - 属于物理层定义的典型规范包括：EIA/TIA RS-232、EIA/TIA RS-449、V.35、RJ-45
  - 提供在网络节点间传输比特的功能，主要处理传输介质相关细节，为链路层提供节点间的比特传输服务。

- **链路层(Link layer)**
  - 在物理层提供比特流服务的基础上，建立相邻结点之间的数据链路，通过差错控制提供数据帧（Frame）在信道上无差错的传输。
  - 数据链路层在不可靠的物理介质上提供可靠的传输。
  - 该层的作用包括：物理地址寻址、数据的成帧、流量控制、数据的检错、重发等。
  - 在这一层，数据的单位称为帧（frame）。
  - 数据链路层协议的代表包括：SDLC、HDLC、PPP、STP、帧中继等。

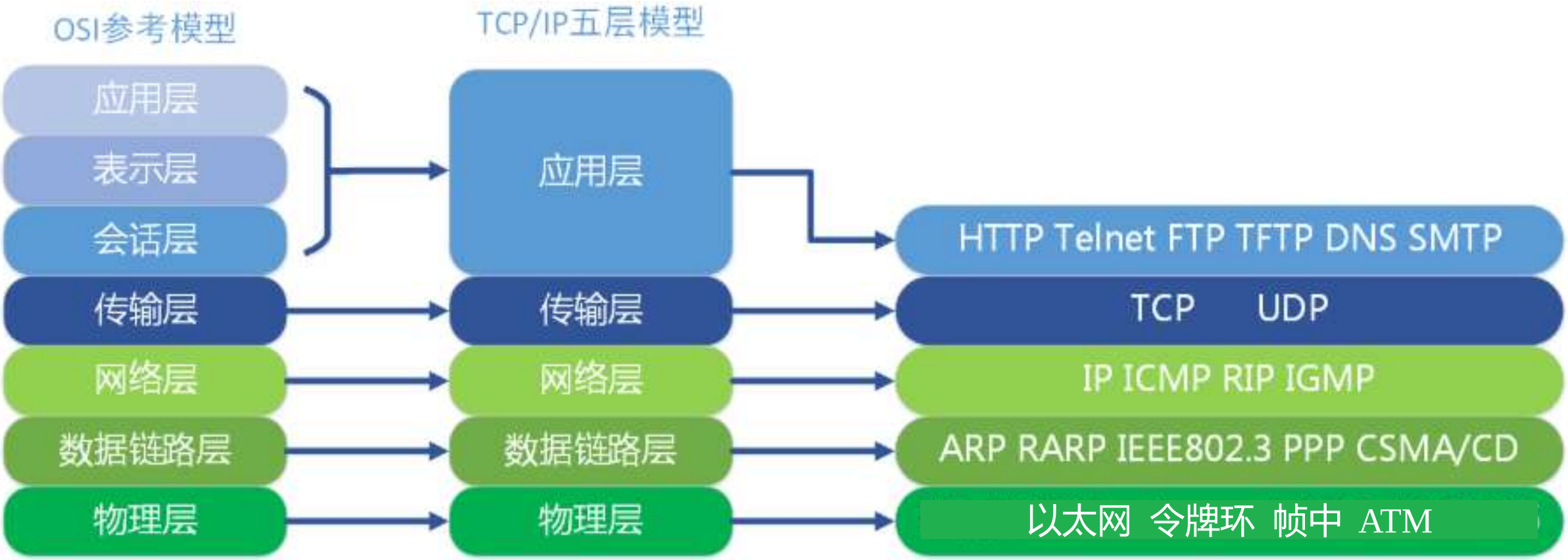
- **网络层(Network layer)**
  - 网络层的任务就是选择合适的网间路由和交换结点， 确保数据及时传送。
  - 网络层将数据链路层提供的帧组成数据包，包中封装有网络层包头，其中含有逻辑地址信息：源站点和目的站点地址的网络地址。
  - 网络层还可以实现拥塞控制、网际互连等功能。在这一层，数据的单位称为数据包（packet）。
  - 网络层协议的代表包括：IP、IPX、RIP、OSPF等。

- **传输层(Transport layer)**
  - 传输层的数据单元也称作数据包（packets）。但是，一般TCP的数据单元称为段 （segments）而UDP协议的数据单元称为“数据报（datagrams）”。
  - 传输层的主要功能是跟踪数据单元碎片、乱序到达的数据包和其它在传输过程中可能发生的危险。
  - 传输层为上层提供端到端（最终用户到最终用户）的透明的、可靠的数据传输服务。所谓透明的传输是指在通信过程中传输层对上层屏蔽了通信传输系统的具体细节。
  - 传输层协议的代表包括：TCP、UDP、SPX等。

TCP/IP协议

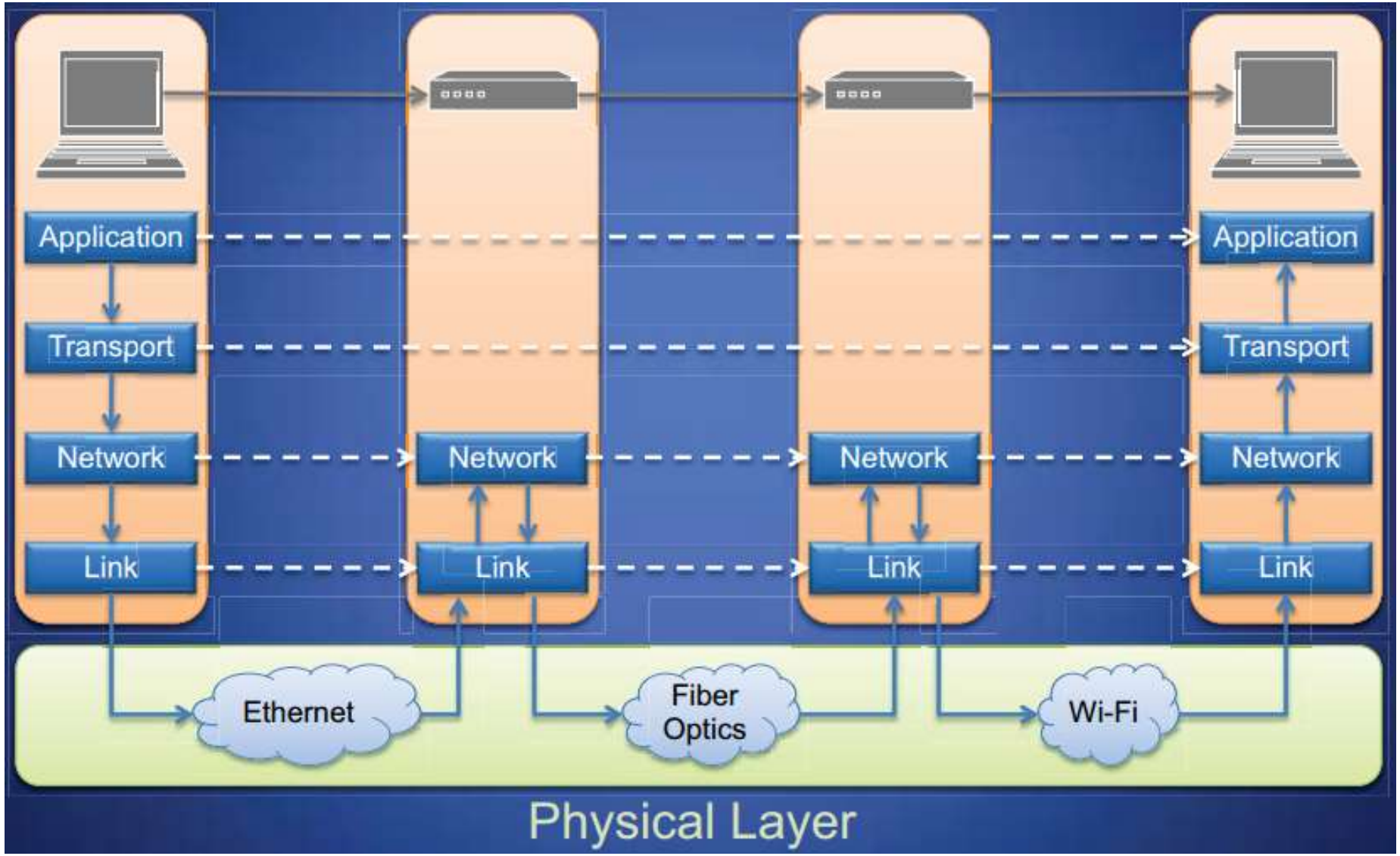
- **应用层(Application layer)**
  - 向用户提供一组常用的应用程序，比如电子邮件、文件传输、远程登录等。常用协议有FTP、TELNET、DNS、SMTP、POP3。
  - 文件传输访问使用FTP协议来提供网络内机器间的文件拷贝功能。 FTP服务数据端口是20H，控制端口是21H。
  - Telnet服务是用户远程登录服务，使用23H端口，使用明码传送，保密性差、简单方便。
  - DNS(Domain Name Service)是域名解析服务，提供域名到IP地址之间的转换。
  - SMTP(Simple Mail Transfer Protocol)是简单邮件传输协议，用来控制信件的发送、中转。

TCP/IP协议



五层网络模型及相关协议

TCP/IP协议



数据在网络中传送过程

网络安全相关问题

- **网络如何影响计算机安全目标CIA**
  - 机密性：网络协议的任何分层中，都没有要求传输数据的机密性。需要修订相关协议来完成机密性。可以在应用层进行加密协议的设计，也可以在网络层。
  - 完整性：封装的数据包中的头和尾部都有简单的校验和，以检查传输数据是否有改变。但这些校验和不是密码学意义下安全的，因此不能提供计算机安全层面的完整性。
  - 可用性：网络协议设计之初主要考虑的是节点发生故障时如何保证可用性，并未考虑攻击者存在时的情形。如拒绝服务攻击会影响系统可用性。

网络安全相关问题

- **网络如何影响计算机安全目标3A**
  - 保证：默认情况下网络中数据包可以在任何两个节点间传输。如果需要引入权限和策略来控制网络中的数据流，必须通过显式得的措施来实现。
  - 真实性：网络协议的数据格式中没有存储数字签名的字段，也没有用户身份的概念。如果需要引入身份证明和数字签名，必须在应用层完成。
  - 匿名：网络协议没有用户身份的概念，因此具有内在的匿名性。对于匿名攻击，可以通过确定用户正在使用网络中的哪台计算机来确定。

提纲

PART 1 网络安全基本概念

PART 2 链路层及其安全

PART 3 网络层及其安全

PART 4 传输层及其安全

PART 5 拒绝服务DoS攻击

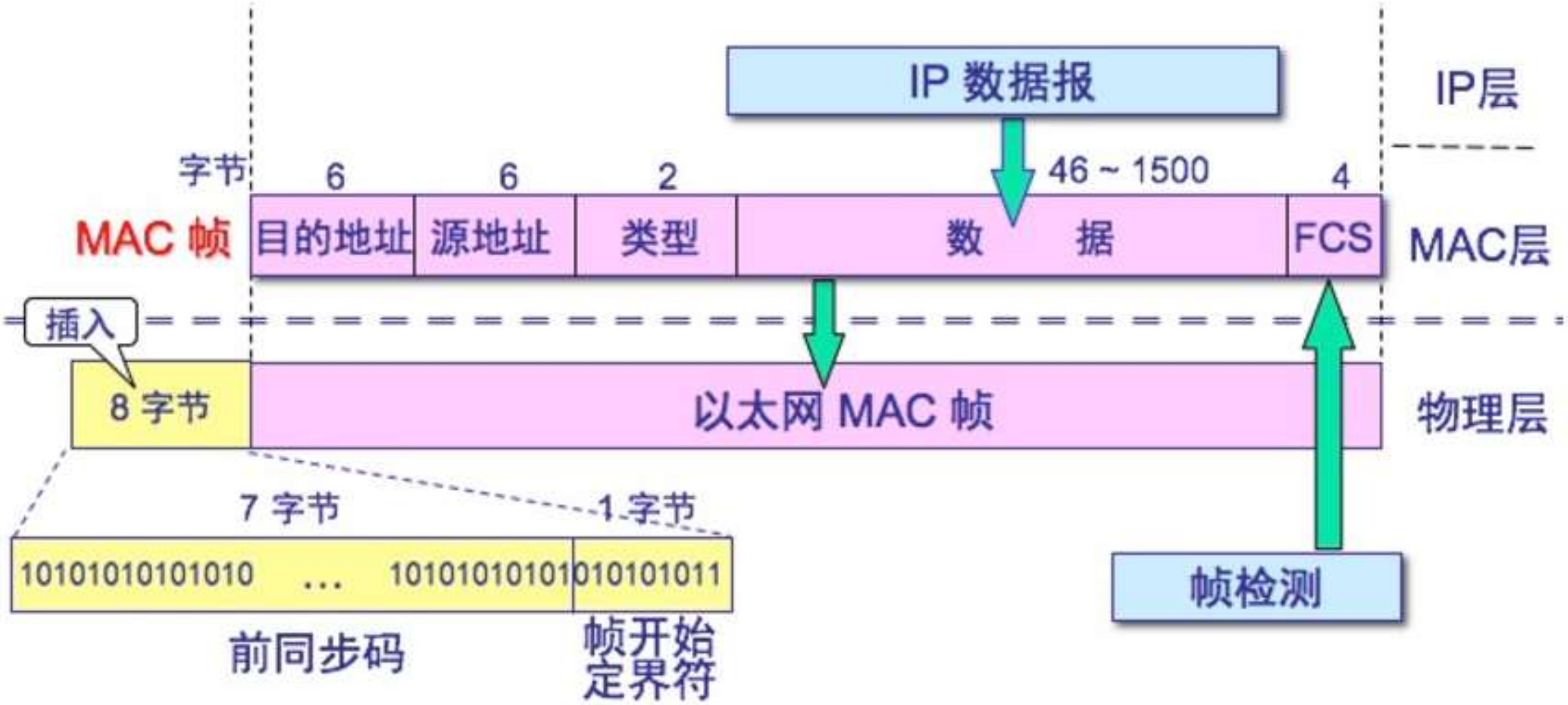
以太网

- 基本概念：以太网包括通信所使用的物理介质以及链路层的协议标准IEEE 802.3，是现有局域网采用的最通用的技术标准。不同帧在以太网电缆上同时传输时会产生冲突，需要丢弃并重传冲突帧。
- 冲突处理：以太网协议使用CSMA/CD（载波监听多路访问及冲突检测）技术来避免冲突。
- 集线器：工作于物理层，将所有帧广播给与之相连的所有设备。缺点是与集线器相连的所有设备共享带宽，传输效率低下。由于是广播，所以数据容易被窃听。
- 交换机：设备首次使用时，与集线器类似。但随着时间的推移，交换机会记录连接到自己各个接口的计算机地址。之后交换机会将接收到的帧发送到特定的接收端，而不是广播出去。

MAC地址

- MAC（Medium/Media Access Control）地址，用来表示互联网上每一个站点的标识符，采用十六进制数表示，共六个字节。其中，前三个字节是由IEEE的注册管理机构RA负责给不同厂家分配的代码(高位24位），后三个字节(低位24位)由各厂家自行指派给生产的适配器接口，称为扩展标识符（唯一性）。一个地址块可以生成2^{24}个不同的地址。因此，在相同网络中两个设备具有相同MAC地址的概率只有百万分之一。
- MAC地址是网卡决定的，一般是固定的。但可以通过网卡的驱动程序软件来修改MAC地址。如Linux下可以通过ifconfig来修改。
- 从安全角度考虑，不能使用MAC地址作为识别网络流源头的依据。

以太网帧结构


IP 数据报
IP层
字节
6
6
2
46 ~ 1500
4
MAC 帧
目的地址
源地址
类型
数
据
FCS
MAC层
插入
8 字节
以太网 MAC 帧
物理层
7 字节
1 字节
10101010101010 ... 10101010101010101011
帧检测
前同步码
帧开始定界符

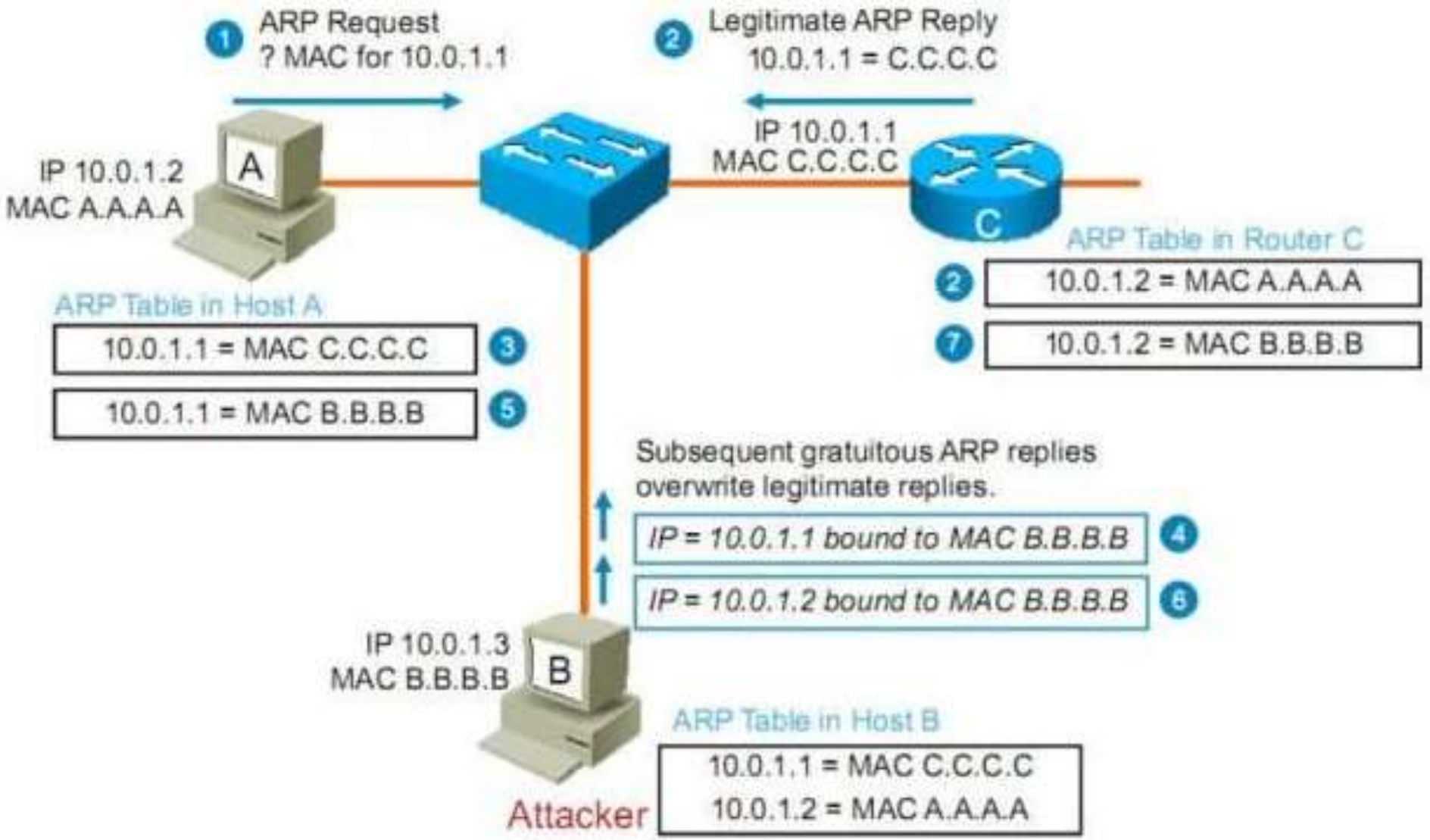
ARP欺骗(ARP spoofing)

- ARP(Address resolution protocol)：地址解析协议。ARP是一种链路层协议，其主要功能是将给定主机的网络层地址解析为主机的硬件地址。
- 主机发送信息时将包含目标IP地址的ARP请求广播到网络上的所有主机，并接收返回消息，以此确定目标的物理地址。
- 收到返回消息后将该IP地址和物理地址存入本机ARP缓存中并保留一定时间，下次请求时直接查询ARP缓存以节约资源。
- ARP建立在网络中各个主机互相信任的基础上。攻击者可以向某一主机发送伪ARP应答报文，使其发送的信息无法到达预期的主机或到达错误的主机，这就构成了一个**ARP欺骗**。

ARP欺骗(ARP spoofing)

- ARP request：`Who has IP address 192.168.1.105`?
- ARP reply：`192.168.1.105 is at 00:16:B7:29:E4:7D.`
- ARP缓存：当计算机接收到ARP响应后，会将IP-MAC地址对存储在本地表中，称为ARP缓存表。
- ARP协议简单高效，但**缺乏身份认证**，容易受中间人攻击。
- 攻击者Eve向 Alice发送一个ARP响应，将Bob的IP地址与Eve的MAC地址关联；同时Eve向Bob发送一个ARP响应，将Alice的IP地址与Eve的MAC地址关联。
- 后果：所有Alice和Bob之间的通信都将经过Eve.

ARP欺骗(ARP spoofing)



ARP欺骗预防措施

- 检查相同MAC地址是否在局域网中多次出现，将其作为是否存在ARP欺骗的标志。
- 静态ARP表：网络管理员手动指定路由器的ARP缓存来将具体的MAC地址和特定的IP地址进行绑定。新设备加入网络时，需要手动添加，不够灵活。
- 更加复杂和灵活的措施：anti-arpsroof、XArp、Arpwatch，这些程序会仔细检查所有的ARP数据包，并将数据包的内容与所存储的ARP表项纪录做比较，以检测并防止ARP欺骗。

提纲

PART 1 网络安全基本概念

PART 2 链路层及其安全

PART 3 网络层及其安全

PART 4 传输层及其安全

PART 5 拒绝服务DoS攻击

网际协议(Internet protocol)

- IP：网络层协议，尽最大努力将一个数据包从源节点路由到目的节点。节点由IP地址标识，IPv4地址为32位，IPv6地址为128位。
- IP包路由：如果数据包的目的地址与发送数据包的主机在同一个局域网内，则使用ARP协议确定目的地址的MAC地址，并发送包；反之，数据包被传送至局域网的网关处，网关根据路由表来确定如何转发数据包。
- 路由器：为数据包寻找一条最佳的传输路径，并将该数据有效地传送到目的站点。选择最佳路径的策略即路由算法。
- 为了便于选择，在路由器中保存着传输路径的相关数据—路由表，供路由选择时使用，表中包含的信息决定了数据转发的策略。

网际协议(Internet protocol)

- TTL(time-to-live)：每个数据包在路由过程中的生存周期，用跳数来决定，一般最大跳数为255。
- 路由器操作：对每个数据包执行丢弃、发送或转发三个操作。
- 路由协议：OSPF(Open shortest path first)协议决定如何在自治系统中路由数据包，其策略是数据包应沿最短路径传输。BGP (Border gateway protocol)决定如何在自治系统之间路由数据包。
- IP地址与子网掩码：例如IP地址为192.168.1.100,子网掩码为255.255.255.0。则该地址的网络部分为192.168.1.0,主机部分为0.0.0.100.
- IPv4地址已经快耗尽，解决方案：(1) IPv6；(2) 网络地址转换(Network address translation, NAT)。

IP数据包格式

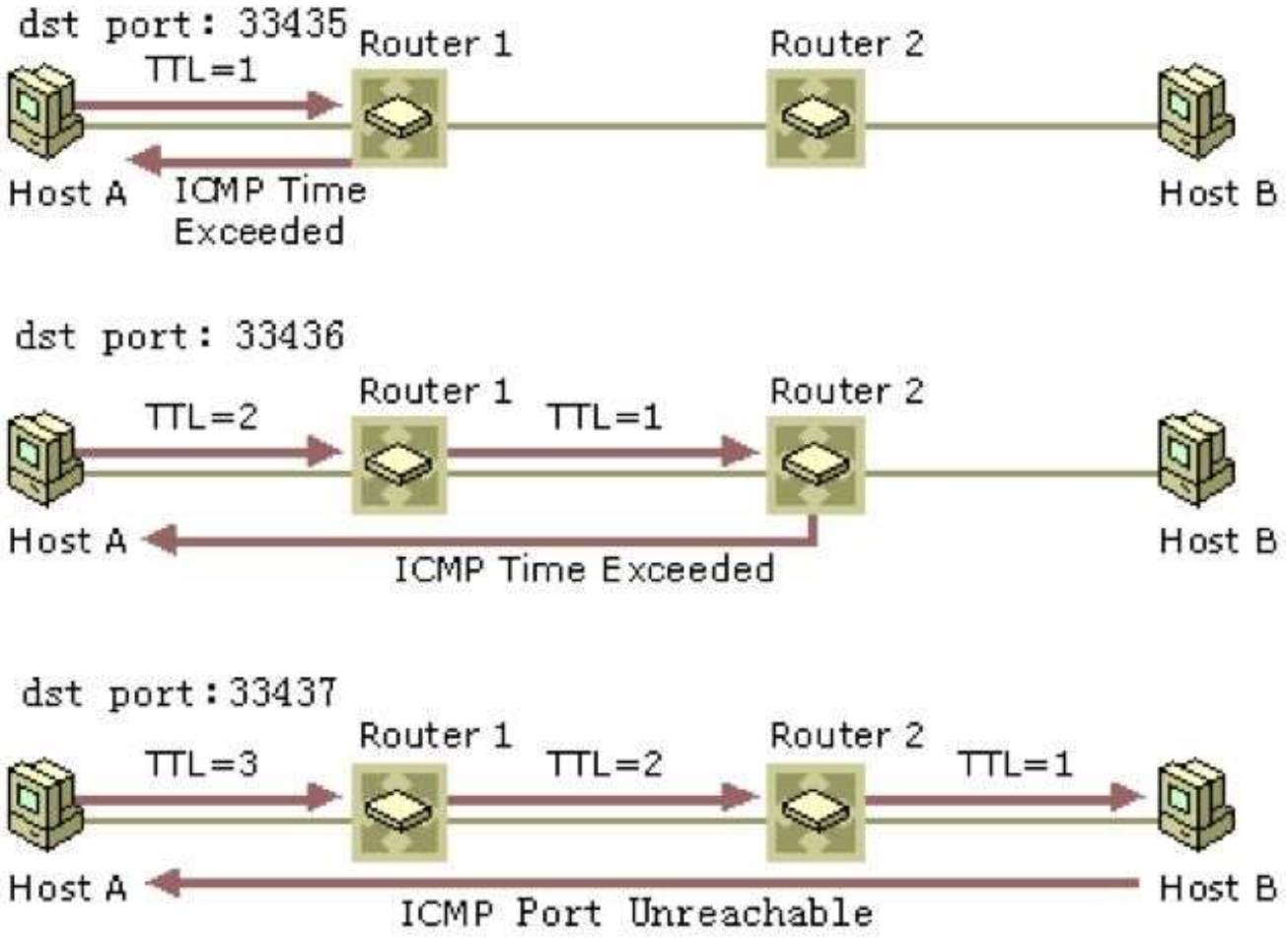
- **IP数据包格式**
  - 黄框：帧数据格式
  - 绿框：IP数据包格式
  - 紫框：TCP报文格式

网际控制消息协议ICMP

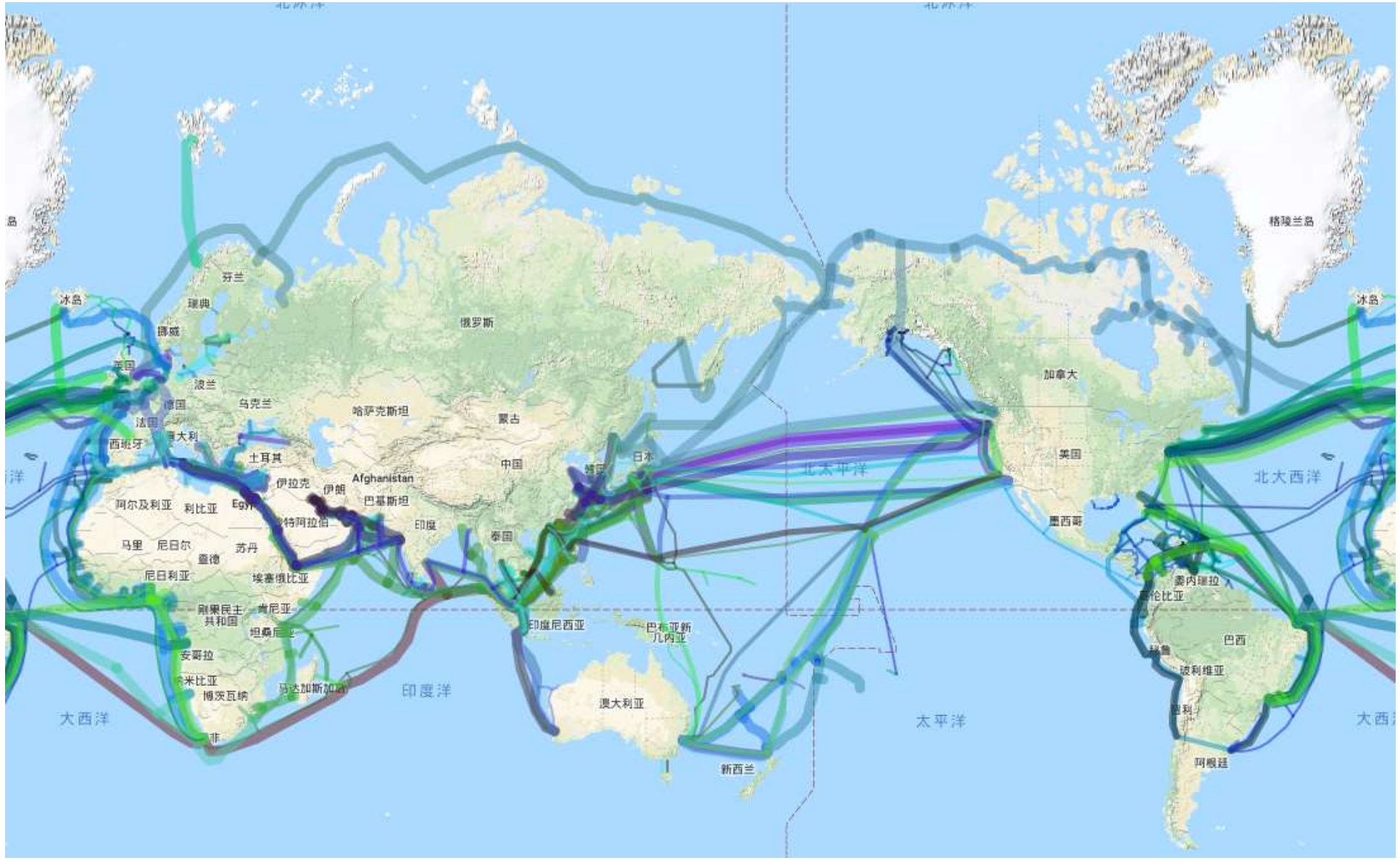
- **网际控制消息协议(Internet control message protocol，ICMP)**
  - ICMP协议：用于在主机、路由器之间传递控制消息。控制消息是指网络通不通、主机是否可达、路由是否可用等网络本身的消息。
  - ICMP消息类型：回显请求(echo request)、回显响应(echo response) 、 超时(time exceeded)、目的地不可达(destination unreachable)。
  - 使用ICMP消息的常用网络管理工具：ping命令和traceroute命令。
  - Ping (Packet Internet Groper)，因特网包探索器，用于测试网络是否通畅或者网络连接速度的程序。Ping发送一个**ICMP回声请求**消息给目的地并报告是否收到**ICMP回声应答**消息。

网际控制消息协议ICMP

- **traceroute命令**
  - 利用ICMP 协议定位给定计算机和目标计算机之间的所有路由器。



网际控制消息协议ICMP



全球海底光缆图

IP地址欺骗(IP spoofing)

- IP地址欺骗：恶意用户产生的IP数据包中的源IP地址是伪造的，以便冒充其他系统或发件人的身份。源IP地址修改后， IP数据包头部校验和也需重新计算。
- 如果攻击者用假冒的源IP地址，那么他不会收到服务器的响应。服务器会把数据包返回给具有假冒IP地址的主机。
- 攻击者采用IP地址欺骗时，表明他不在乎是否能收到响应，或者他有接收到响应的其他方法。如拒绝服务攻击。
- IP地址欺骗可以用在规避防火墙策略(6.2节)或者进行TCP会话劫持(5.4节)中。

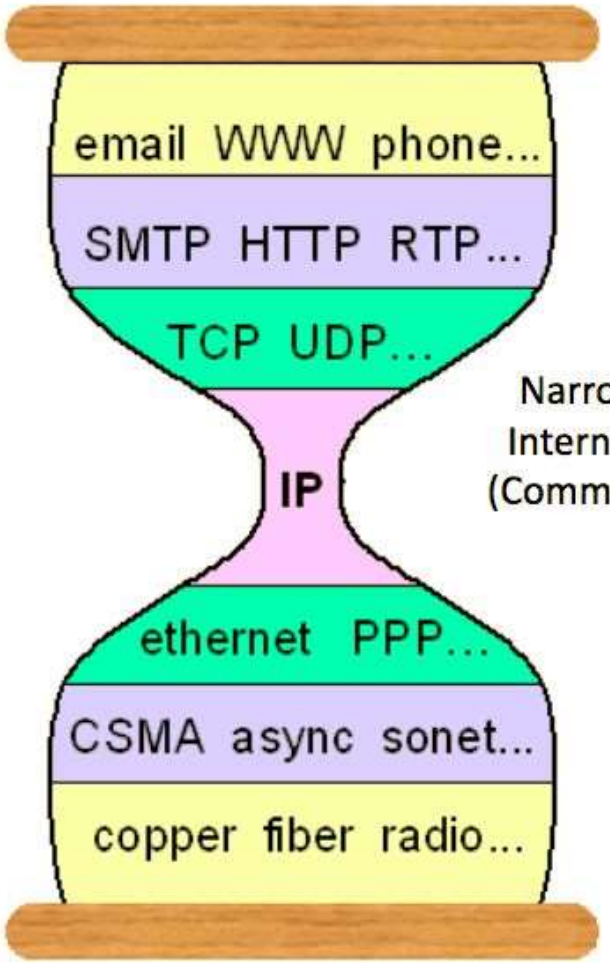
IP地址欺骗应对措施

- 边缘路由器在配置时，可以阻止源地址在域内，但实际地址是域之外的数据包。边缘路由器也可以阻止源地址是域外的，但是从域内往域外发送的数据包。
- IP追踪技术也可以打击IP地址欺骗。这一技术可以追踪数据包返回到实际源地址的路径。
- 根据追踪到的信息，可以向各种自治系统发送请求，要求自治系统阻止来自该路径的数据包，直到确定恶意软件或恶意用户被清除为止。

IP地址回溯 IP Traceback

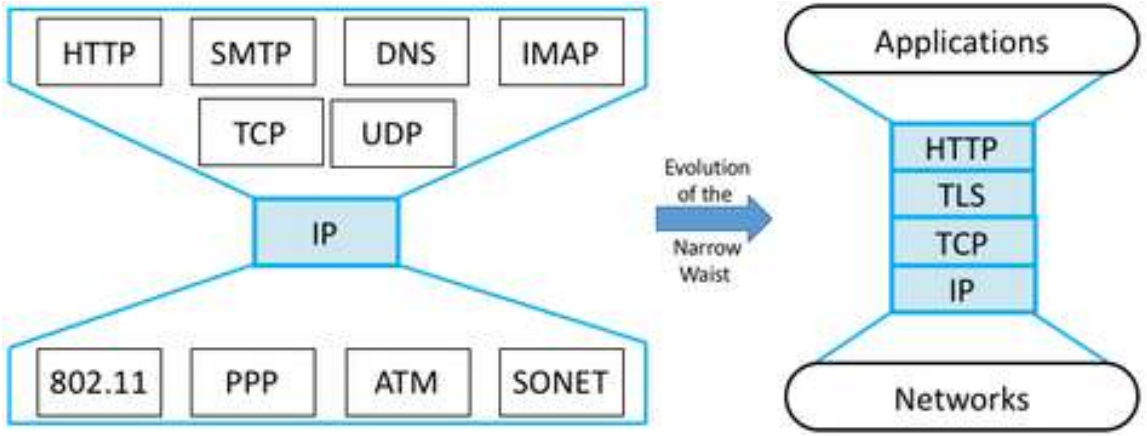
- 由于IP地址欺骗，很难确定攻击者的真正源IP地址。IP地址回溯能够确定数据包的真实来源，而不依赖于数据包头部的IP地址。
- 数据包标记技术：路由器基于数据包的相关路径信息确定地或者概率地标注转发数据包。受害者收集到足够数据包就能够重构攻击者的路径。一个简单的标注方法在经过路由器的数据包中追加其IP地址，但路由器开销会增加。
- 节点采样：不在每个数据包中追加路径信息，而使用IP数据包中的一个字段就可以记录路径信息。每个路由器以概率p用自己的地址覆盖每个数据包的这个字段。如果标记足够多的数据包，受害者就可以使用这个字段来确定攻击者和受害者之间途径的每个路由器。

Everything Over IP Over Everything

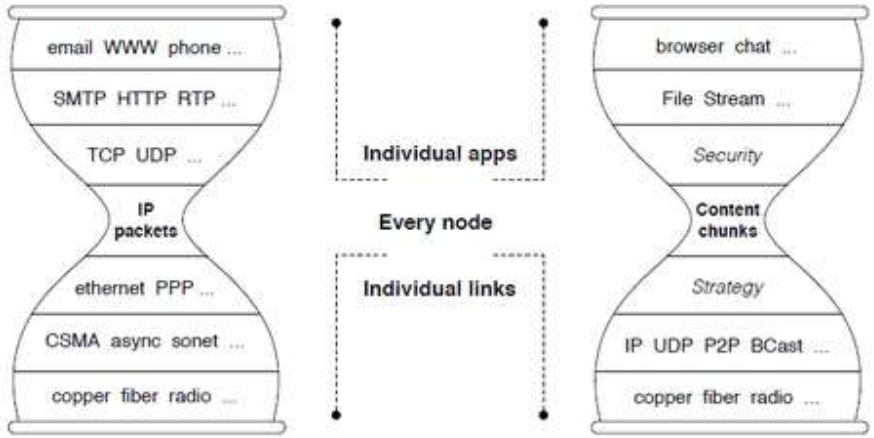


Narrow Waist for
Internet Hourglass
(Common Layer = IP)

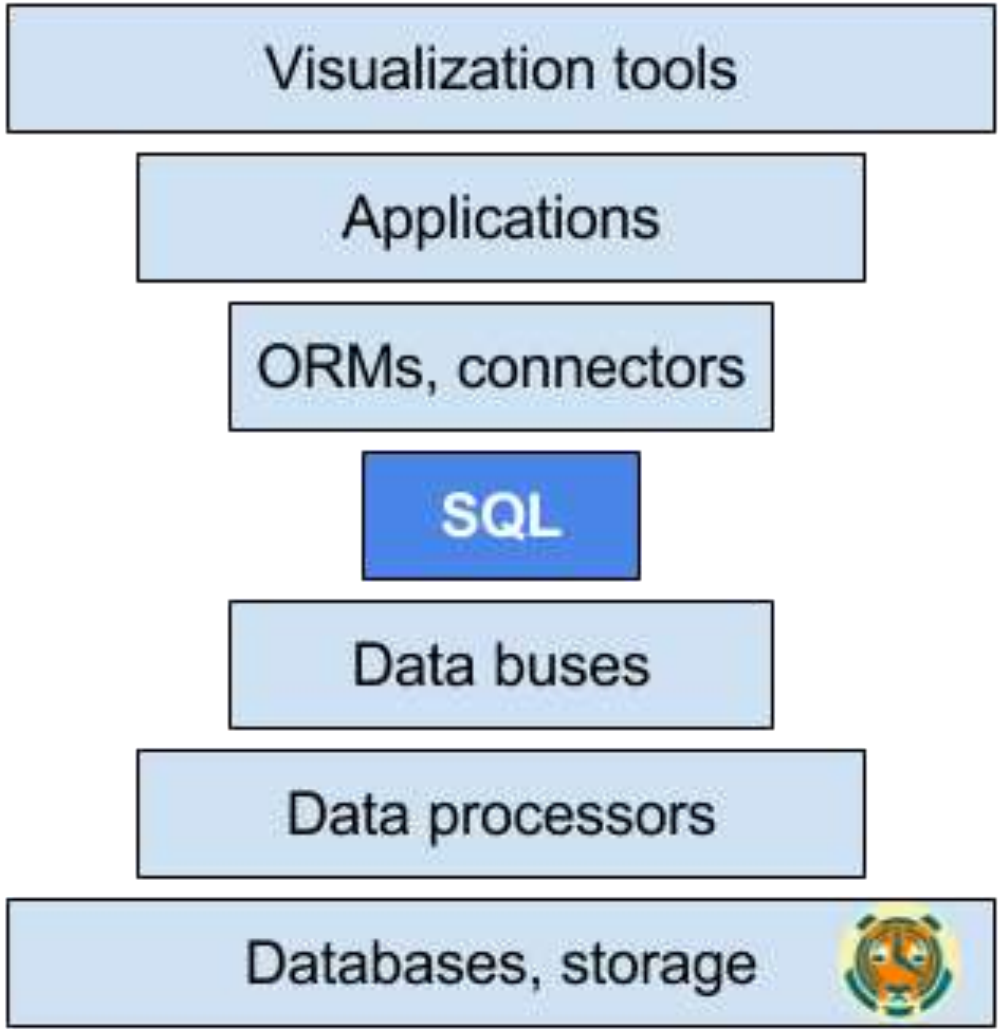
社区推动整个网络协议栈成为细腰



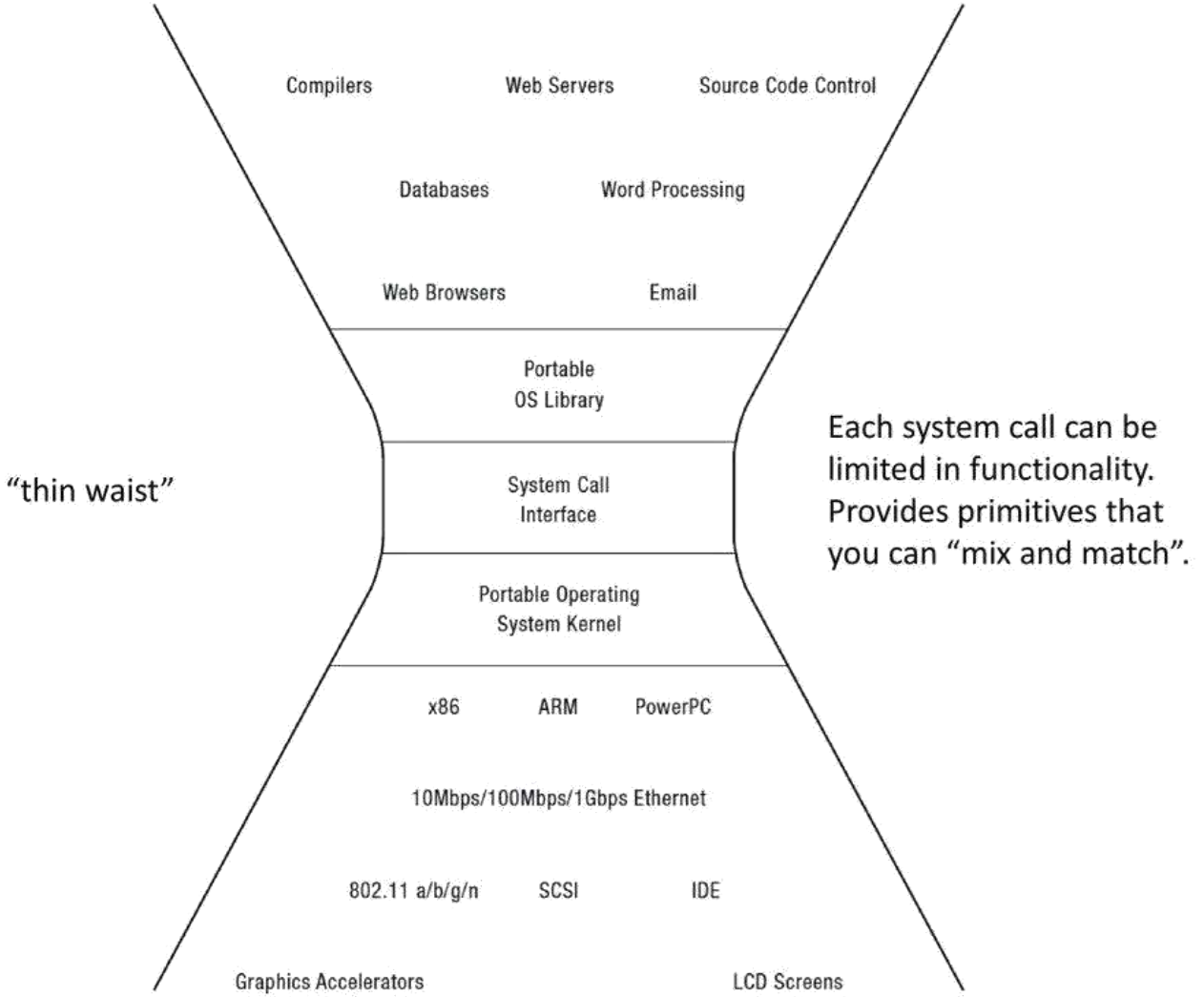
命名数据网络NDN推动IP细腰向内容细腰的转变



扩展：“细腰”战事：技术架构的进化



The Data Universal Interface



扩展阅读：https://www.51cto.com/article/611706.html

网络5.0取得新进展


网络的分代研究
Analog
1.0
TDM
2.0
ATM
3.0
IP
4.0
MPLS
4.5
?
5.0
同步时分复用
统计复用
面向连接
统计复用
不面向连接
多协议标签交换
模拟交换
时隙交换
信元交换
数据路由
?

华为NewIP

专题：数据网络协议架构创新——NewIP

NewIP：开拓未来数据网络的新连接和新能力

郑秀丽，蒋胜，王闯
（华为技术有限公司，北京 100095）

摘　要： 互联网应用深刻地影响着人们的工作与生活，接至首来的新应用对数据网络提出了新的挑战。基于未来应用对数据网络提出的需求，剖析了数据网络需要基于IP进行继承式发展，提出了一种新型的网络协议体系——NewIP，并介绍了5种关键使能技术，包括确定性IP、内生安全、面向万网互联的新寻址与控制机制、用户可定义、新传输层等。

关键词： NewIP；数据网络；确定性；异构；万网互联；内生安全；高吞吐
中图分类号： TP3
文献标识码： A
doi: 10.11959/j.issn.1000-0801.2019208

NewIP: new connectivity and capabilities of upgrading future data network

ZHENG Xiuli, JIANG Sheng , WANG Chuang
Huawei Technologies Co., Ltd., Beijing 100095, China

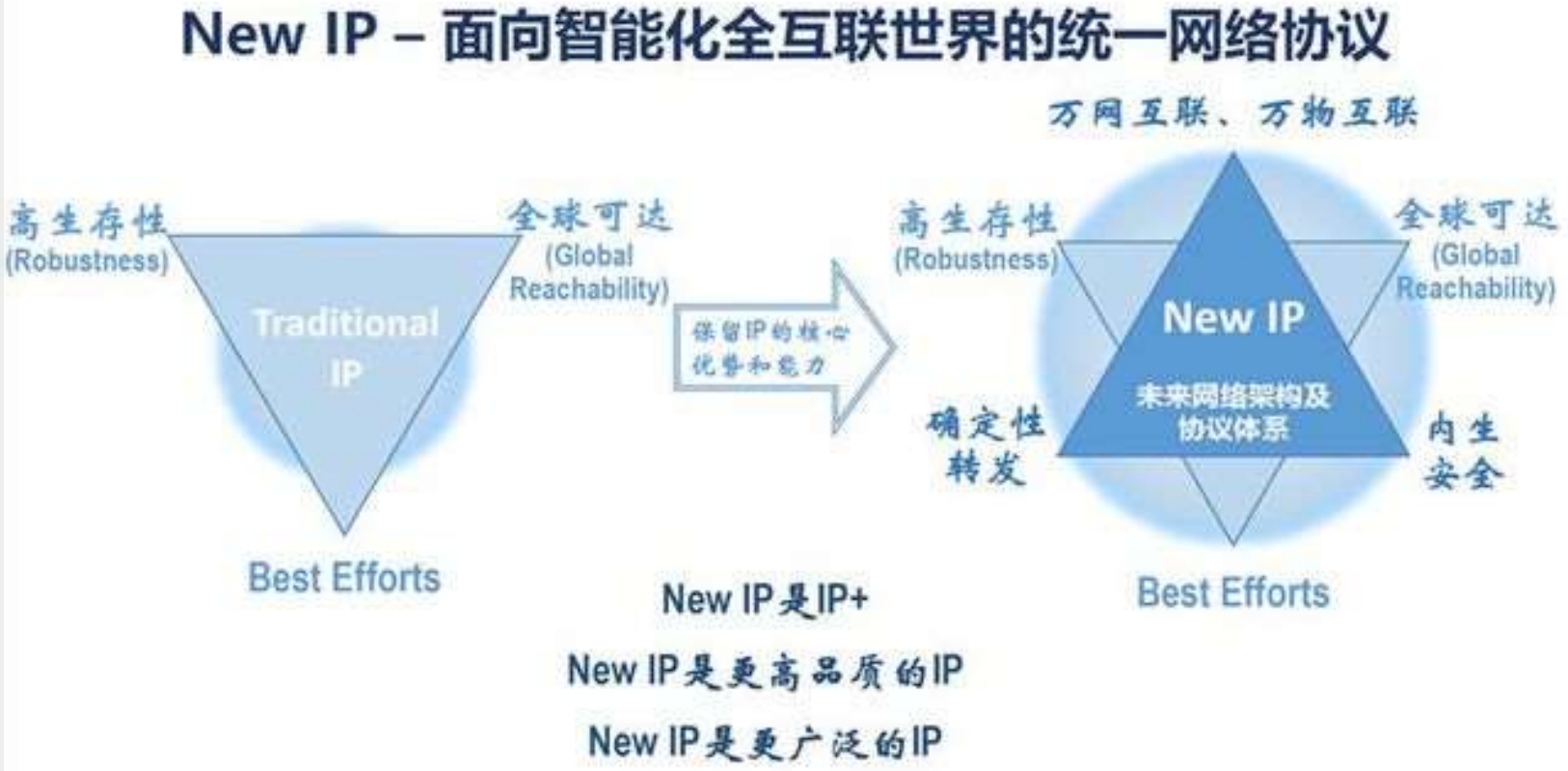
Abstract: Internet applications deeply affect people's work and life. As the booming of internet applications, the data network faces more and more challenges. Based on the requirements of future applications, the trend for inheritance development based on traditional IP of data networks was analyzed and a new network protocol suite——NewIP was proposed. The core technologies including deterministic IP, intrinsic security, new control and addressing mechanisms for ManyNets, user definable and new transport were also introduced.

Key words: NewIP, data network, deterministic, heterogeneous, ManyNets, intrinsic security, ultra-high throughput

1　引言

互联网发展40多年来，随着IP技术的不断演进，其承载的应用越来越丰富，邮件、云计算、社交网络、在线购物、电子银行、视频直播等正在深刻影响着人们的学习、工作与生活，取得了巨大的成功。AR/VR、远程医疗、工业互联网、车联网等已悄然而至，全息通信、意识通信、空天地一体化通信等在不久的将来也将揭开神秘的面纱，人们正在快速进入一个万物感知、万物互联的智能世界。纷繁的新应用对IP网络提出了新的需求与挑战，网络技术创新是新应用创新的基

收稿日期：2019-08-10；修回日期：2019-09-10
基金项目：国家重点研发计划基金资助项目（No.2018YFB1800100）
Foundation Item: The National Key Research and Development Program of China (No.2018YFB1800100)

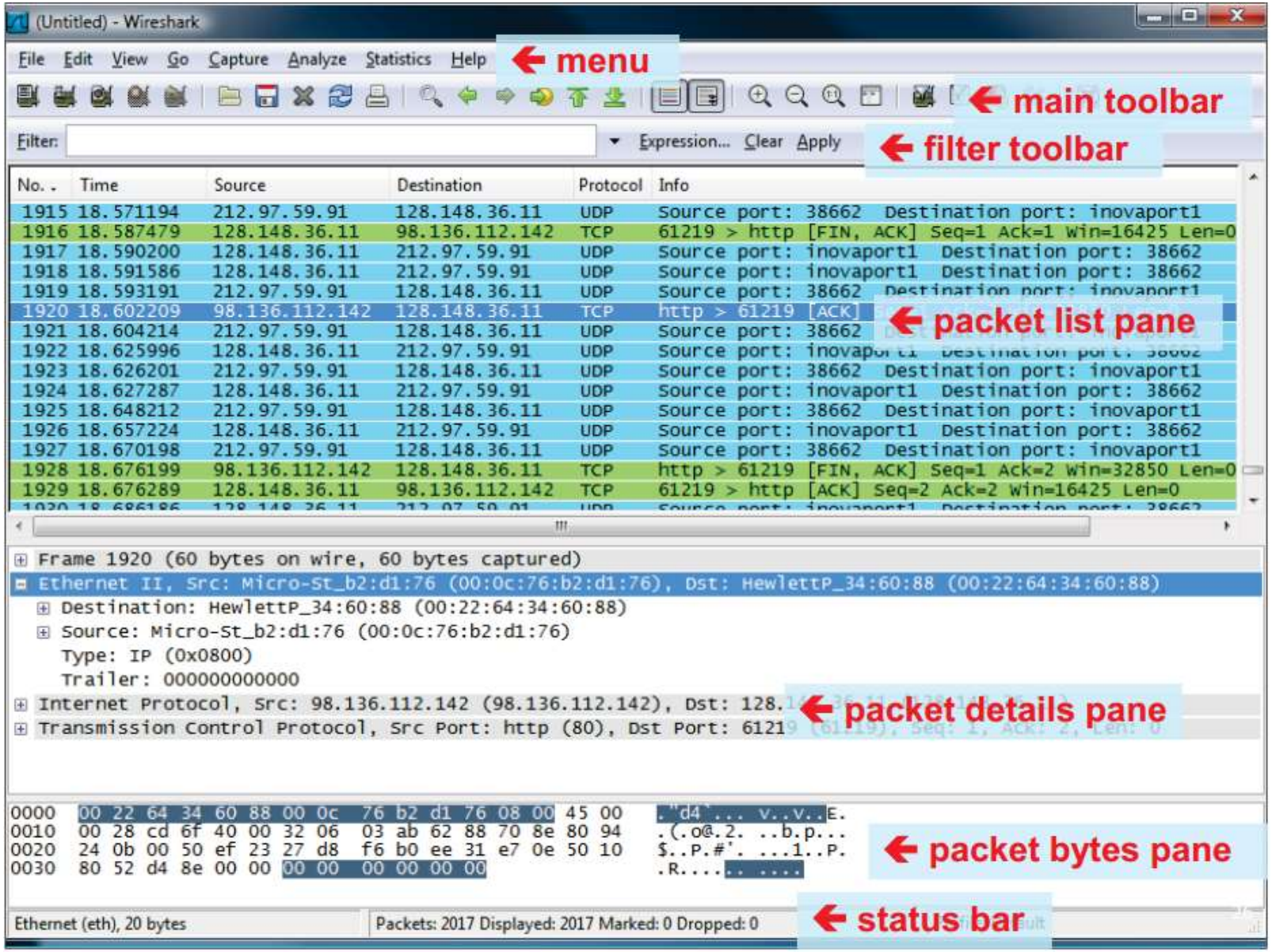


扩展阅读：[为什么华为的「New IP」，遇到了 New 问题？]

数据包嗅探

- Wireshark（前称Ethereal）是一个网络数据包分析软件。其功能是撷取网络封包，并尽可能显示出最为详细的网络数据包资料。
- Wireshark使用WinPCAP作为接口，直接与网卡进行数据报文交换。使用时网卡被设置为混杂(promiscuous)模式。
- 网络管理员使用Wireshark来检测网络问题，网络安全工程师使用Wireshark来检查资讯安全相关问题，
- 开发者使用Wireshark来为新的通讯协定除错，普通使用者使用Wireshark来学习网络协定的相关知识。
- 当然，有的人也会“居心叵测”的用它来寻找一些敏感信息

数据包嗅探


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
menu
main toolbar
Filter:
Expression... Clear Apply
filter toolbar
No. . Time Source Destination Protocol Info
1915 18.571194 212.97.59.91 128.148.36.11 UDP Source port: 38662 Destination port: inovaport1
1916 18.587479 128.148.36.11 98.136.112.142 TCP 61219 > http [FIN, ACK] Seq=1 Ack=1 Win=16425 Len=0
1917 18.590200 128.148.36.11 212.97.59.91 UDP Source port: inovaport1 Destination port: 38662
1918 18.591586 128.148.36.11 212.97.59.91 UDP Source port: inovaport1 Destination port: 38662
1919 18.593191 212.97.59.91 128.148.36.11 UDP Source port: 38662
1920 18.602209 98.136.112.142 128.148.36.11 TCP http > 61219 [ACK]
1921 18.604214 212.97.59.91 128.148.36.11 UDP Source port: 38662
1922 18.625996 128.148.36.11 212.97.59.91 UDP
1923 18.626201 212.97.59.91 128.148.36.11 UDP Source port: 38662 Destination port: inovaport1
1924 18.627287 128.148.36.11 212.97.59.91 UDP Source port: inovaport1 Destination port: 38662
1925 18.648212 212.97.59.91 128.148.36.11 UDP Source port: 38662 Destination port: inovaport1
1926 18.657224 128.148.36.11 212.97.59.91 UDP Source port: inovaport1 Destination port: 38662
1927 18.670198 212.97.59.91 128.148.36.11 UDP Source port: 38662 Destination port: inovaport1
1928 18.676199 98.136.112.142 128.148.36.11 TCP http > 61219 [FIN, ACK] Seq=1 Ack=2 Win=32850 Len=0
1929 18.676289 128.148.36.11 98.136.112.142 TCP 61219 > http [ACK] Seq=2 Ack=2 Win=16425 Len=0
packet list pane
Frame 1920 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: Micro-St_b2:d1:76 (00:0c:76:b2:d1:76), Dst: HewlettP_34:60:88 (00:22:64:34:60:88)
Destination: HewlettP_34:60:88 (00:22:64:34:60:88)
Source: Micro-St_b2:d1:76 (00:0c:76:b2:d1:76)
Type: IP (0x0800)
Trailer: 000000000000
Internet Protocol, Src: 98.136.112.142 (98.136.112.142), Dst: 128.
Transmission Control Protocol, Src Port: http (80), Dst Port: 6121
packet details pane
0000 00 22 64 34 60 88 00 0c 76 b2 d1 76 08 00 45 00 ."d4`... v..v..E.
0010 00 28 cd 6f 40 00 32 06 03 ab 62 88 70 8e 80 94 .(.o@.2. ..b.p...
0020 24 0b 00 50 ef 23 27 d8 f6 b0 ee 31 e7 0e 50 10 $..P.#'. ...1..P.
0030 80 52 d4 8e 00 00 00 00 00 00 00 00 .R...... ....
packet bytes pane
Ethernet (eth), 20 bytes
Packets: 2017 Displayed: 2017 Marked: 0 Dropped: 0
status bar

防止数据包嗅探

- 使用以太网交换机而不是集线器，降低数据包被嗅探的可能性。但对于无线网络，该方法无能为力。
- 检测网卡是否被设置为混杂模式。可能的检测方式：(1) 当处于混杂模式时，计算机系统处理所有数据包会比较慢。(2) 对无效数据包的响应有可能表明网卡处于混杂模式。
- 例如向一台被怀疑的主机发送数据包，其IP地址与MAC地址不匹配，网卡会丢弃数据包。但如果网卡运行在混杂模式，有可能会发送一个响应。
- 高层协议使用加密防止敏感信息泄露，如HTTPS协议。

提纲

PART 1 网络安全基本概念

PART 2 链路层及其安全

PART 3 网络层及其安全

PART 4 传输层及其安全

PART 5 拒绝服务DoS攻击

传输层(Transport layer)

- 端口：16比特的端口号，用来标识应用层不同服务。例如，FTP使用21端口号，Telnet使用23端口号，SMTP使用25端口号， HTTP使用80端口号， HTTPS使用443端口号。
- TCP(Transmission control protocol)：面向连接的、可靠的。面向连接意味着实现会比较复杂，可靠的是指信息会完整、有序地到达。如果数据包丢失，TCP会保证重传。 TCP是传输文件、网页和电子邮件的首选协议。
- UDP(User datagram protocol)：无连接的、不可靠但速度快。基于IP的语音会话(VoIP)适合于使用UDP协议。

TCP协议

- 基于IP协议，使用三次握手协议初始化，每个数据包都有编号。
- 累积确认：发送方向接收方发送指定的数据包后，接收方向发送方发送确认收到这些数据包。
- 流量控制：负责管理发送方发送的数据量，避免发送数据过多接收方无法及时处理。流量控制主要使用滑动窗口协议。
- 校验和：使用循环冗余校验(CRC)来确保传送数据的正确性，检测由网络错误引发的数据不一致性，但不能检测恶意篡改。
- 拥塞控制：拥塞会导致传输速率急剧下降和数据包的丢弃。拥塞控制是防止流量淹没网络的一种技术，通过收集确认数据包等信息来调整数据的传输速率，防止拥塞。

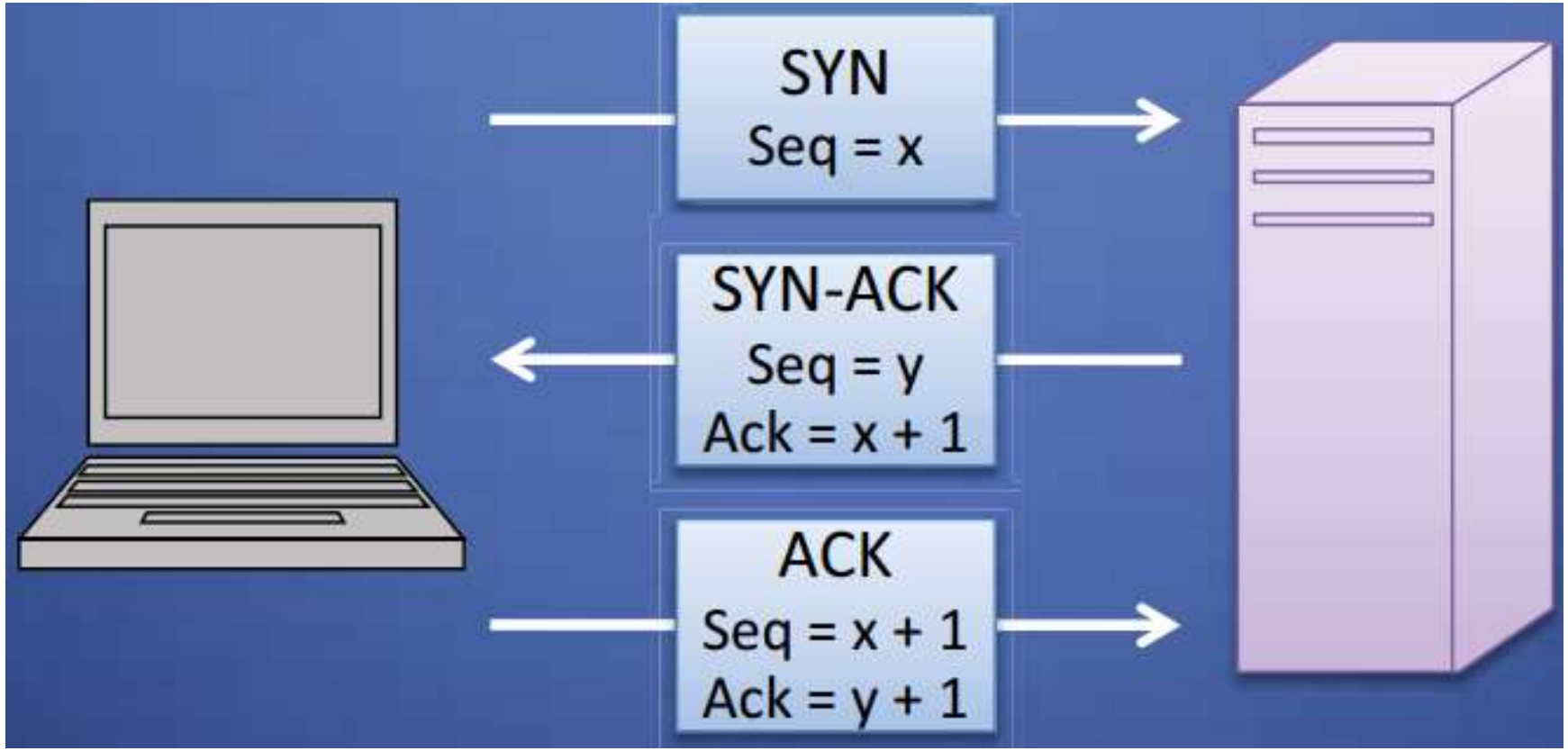
TCP协议

TCP 分组格式示意图

TCP连接：三次握手

初始序列号是随机选择的，以防止针对预测初始序列号的攻击。

客户端　　服务器端



TCP会话劫持

• TCP序列号预测

- TCP序列预测攻击企图猜测TCP会话时的初始序列号，以建立伪造的TCP会话。
- 一个可能的攻击方案如下：

(1) 攻击者针对受害客户端发动拒绝服务攻击，防止客户端干扰自己的攻击；

(2) 攻击者向服务器发送一个SYN包，将源IP地址伪造成受害客户端的IP地址；

(3) 在等待服务器向客户端发送响应之后，攻击者通过发送一个ACK数据包来结束TCP握手，该数据包的序列号是预测的下一个序列号；

(4) 攻击者以受害客户端名义向服务器发送请求。

TCP会话劫持

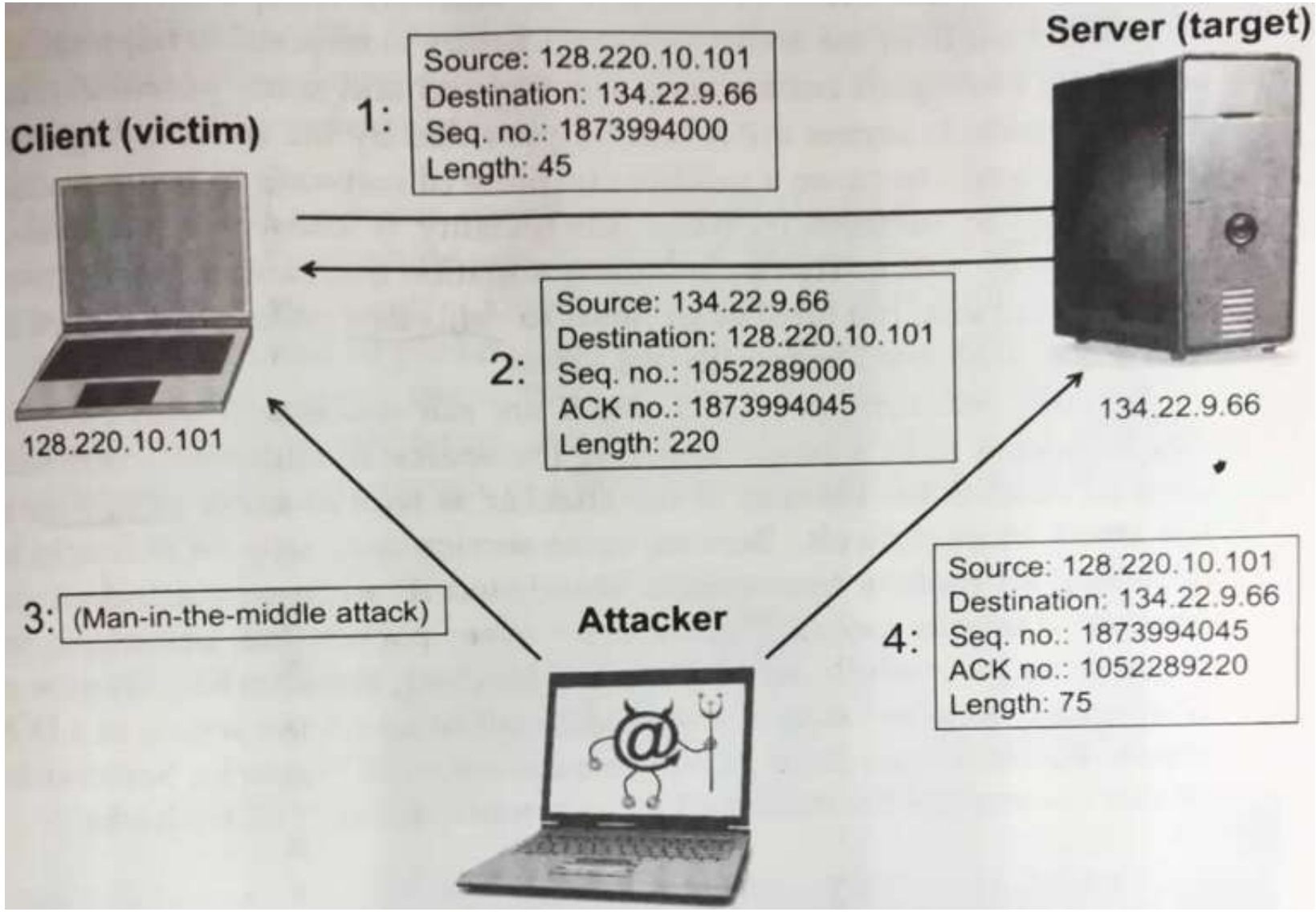
- **盲注入(Blind injection)**
  - TCP序列号预测攻击中使用了IP欺骗，攻击者将无法从服务器收到任何响应。盲注入允许攻击者使用请求者的源IP地址来执行某些命令，从而破坏系统。
  - 盲注入一般会注入包含命令的数据包，从而建立将响应返回给攻击者的连接。
- **ACK风暴(Blind injection)**
  - 盲注入后客户端不会向服务器发送同步消息，导致不同步现象。
  - 此时，客户端和服务器会向对方发送ACK消息，每一方都想告诉对方需要开始使用正确的序列号。
  - 这种反复的通信被称为ACK风暴。

TCP会话劫持

- **完全会话劫持 (complete session hijacking)**
  - **当攻击者与目标服务器或客户端在同一网段时**，攻击者可以完全劫持**已有的**TCP会话。使用数据包嗅探攻击，攻击者可以知道建立会话时数据包的序列号。
  - 完全会话劫持与ARP欺骗结合的中间人攻击：攻击者首先使用ARP欺骗，将会话双方的通讯流暗中改变，这种改变对会话双方来说是透明。其次，攻击者利用完全会话劫持来截获会话双方所有消息。
- **针对会话劫持的安全措施**
  - 在IP层或者应用层使用认证和加密，如IPSec或者应用层安全协议。
  - 网站应避免创建以安全身份验证措施开始，但后来切换到未加密交换的会话，这样会产生TCP会话劫持攻击的风险。

TCP会话劫持

- **完全会话劫持 (complete session hijacking)**



UDP协议

- 无需三次握手建立连接，允许直接发送数据报(datagram)。
- UDP是不可靠连接，不保证数据包的有序到达。它假定检查数据报序列中丢失数据报的工作由应用程序完成。
- 使用16位的校验和来验证每个数据包的完整性。
- UDP的数据传输速度要远远快于TCP。它常用于对时间敏感的应用程序，其更加注重传输速度而不是完整性，如DNS和VoIP。

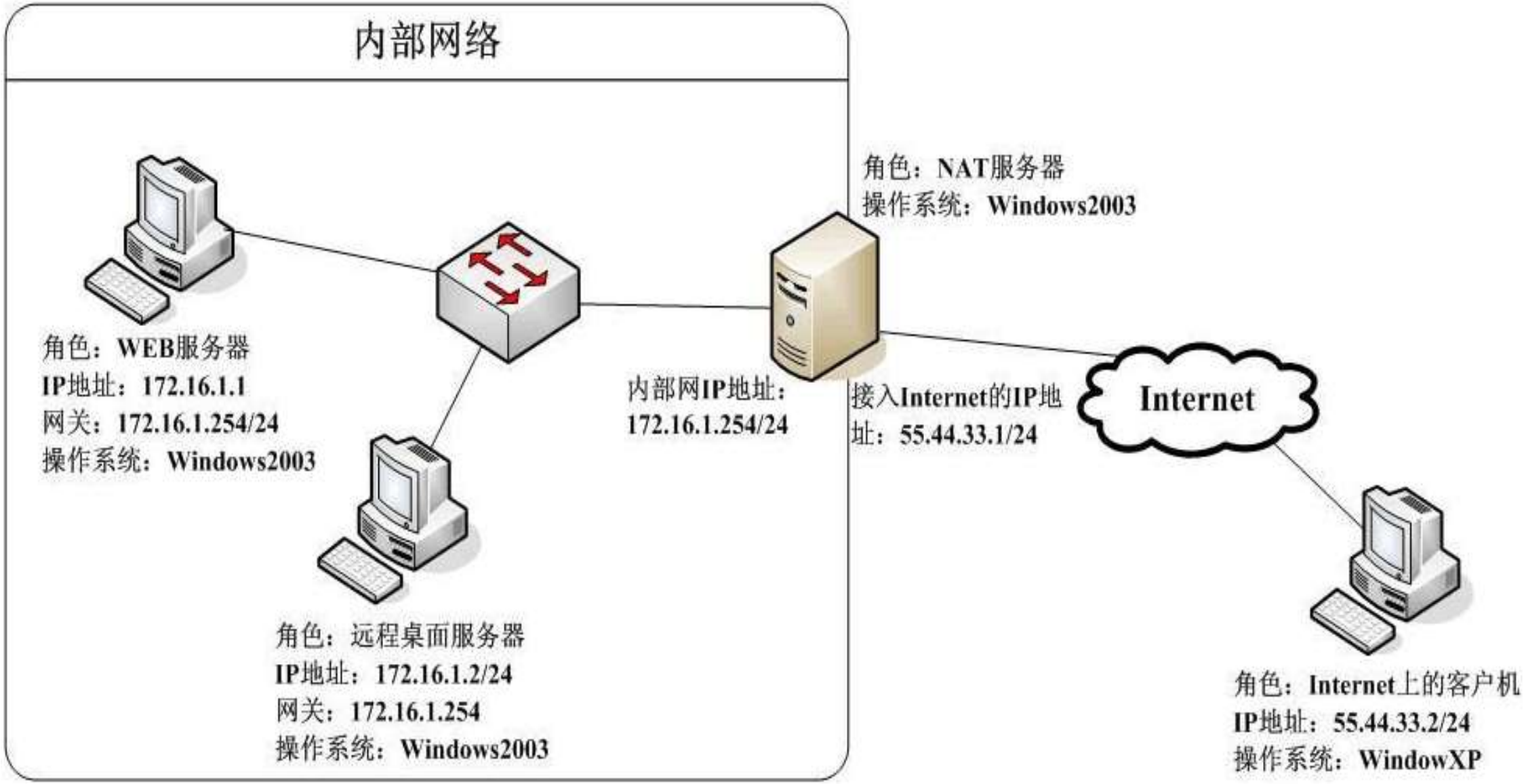
16 位源端口号	16 位目的端口号
16 位 UDP 长度	16 位 UDP 检验和
数据（如果有）	

网络地址转换

- **Network address translation (NAT)**
  - NAT允许局域网的机器共享一个公共的IP地址，以接入因特网。
  - NAT不仅完美地解决了lP地址不足的问题，而且还能够有效地避免来自网络外部的攻击，隐藏并保护网络内部的计算机。
  - NAT路由器：私有网络和公共internet间的网关，负责管理流入和流出的互联网流量。
  - NAT路由器通过维护一个查找表来实现私有和公有IP地址转换：

    (私有源IP地址，私有源端口，目的IP地址,公有源端口)
  - 流入和流出NAT路由器的数据包的头部会根据具体情况进行修改。
  - 使用NAT设备时，互联网的流入流量不能到达内部网络，能够阻止来自外部网络的威胁。

网络地址转换


内部网络
角色：NAT服务器
操作系统：Windows2003
角色：WEB服务器
IP地址：172.16.1.1
网关：172.16.1.254/24
操作系统：Windows2003
内部网IP地址：
172.16.1.254/24
接入Internet的IP地址：55.44.33.1/24
Internet
角色：远程桌面服务器
IP地址：172.16.1.2/24
网关：172.16.1.254
操作系统：Windows2003
角色：Internet上的客户机
IP地址：55.44.33.2/24
操作系统：WindowXP

提纲

PART 1 网络安全基本概念

PART 2 链路层及其安全

PART 3 网络层及其安全

PART 4 传输层及其安全

PART 5 拒绝服务DoS攻击

拒绝服务攻击

- **Denial-of-service attacks**
  - **拒绝服务攻击**亦称**洪水攻击**，其目的在于使目标电脑的网络或系统资源耗尽，使服务暂时中断或停止，导致其正常用户无法访问。
  - 当攻击者使用网络上两个或以上被攻陷的电脑作为“僵尸”向特定的目标发动“拒绝服务”式攻击时，其称为**分布式拒绝服务攻击**。
  - 攻击发起者一般针对重要服务进行攻击，如银行，信用卡支付网关，甚至根域名服务器。
  - 攻击症状：网络异常缓慢(打开文件或访问网站)、特定网站无法访问、无法访问任何网站、垃圾邮件的数量急剧增加、无线或有线网络连接异常断开、长时间尝试访问网站或任何互联网服务时被拒绝、服务器容易断线、卡顿等。

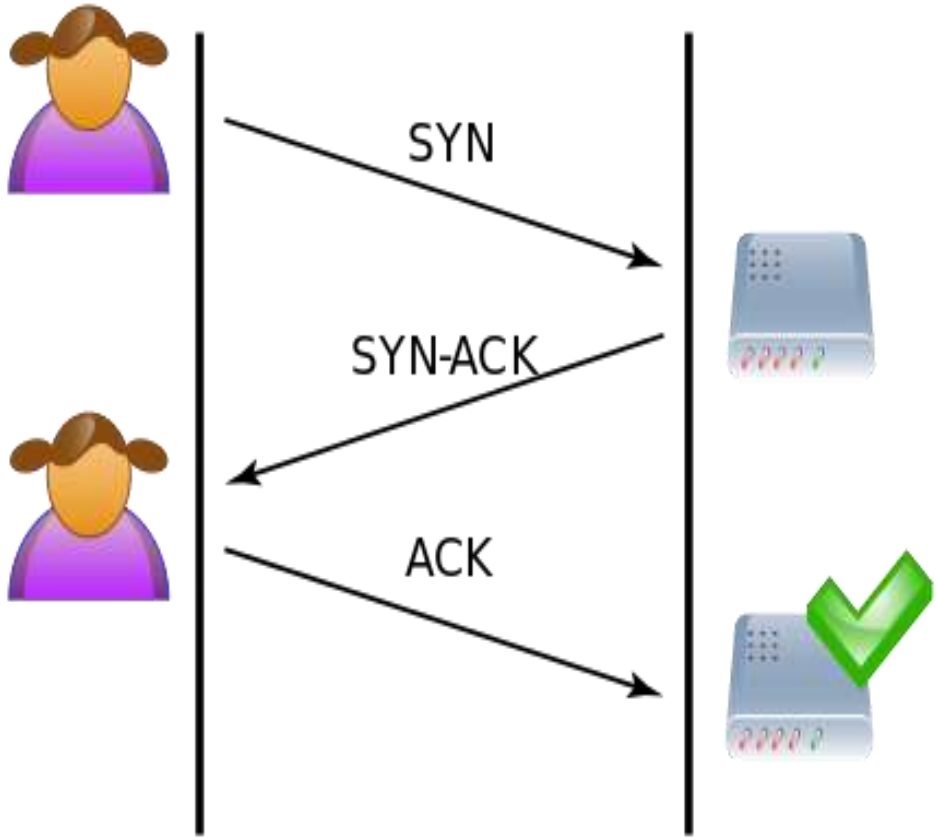
拒绝服务攻击分类

- **带宽消耗型攻击**：可分为洪泛攻击和放大攻击。
  - ✓ **ICMP洪水攻击：**通过向未良好设置的路由器发送广播信息以占用系统资源
  - ✓**UPD洪水攻击：**大量UDP数据包发送给受害系统，可能会导致带宽占用
  - ✓**死亡之ping：**产生超过IP协议能容忍的数据包数，可能会导致死机
  - ✓**泪滴攻击：**数据在发送前都会经过切割，每个小切割都会记录位移的信息，以便重组。此攻击模式就是捏造位移信息，导致重组时发生问题，造成错误
- **资源消耗型攻击**
  - ✓ **SYN洪水攻击：**大量TCP SYN请求反复发送，导致系统资源耗尽
  - ✓ **LAND攻击：**与SYN floods类似，会导致被攻击的机器死循环
  - ✓**分布式HTTP洪水攻击：**使用代理服务器向受害服务器发送大量貌似合法的请求，通常使用HTTP GET。
  - ✓**僵尸网络攻击：**大量被命令与控制服务器所控制的互联网主机群协同攻击

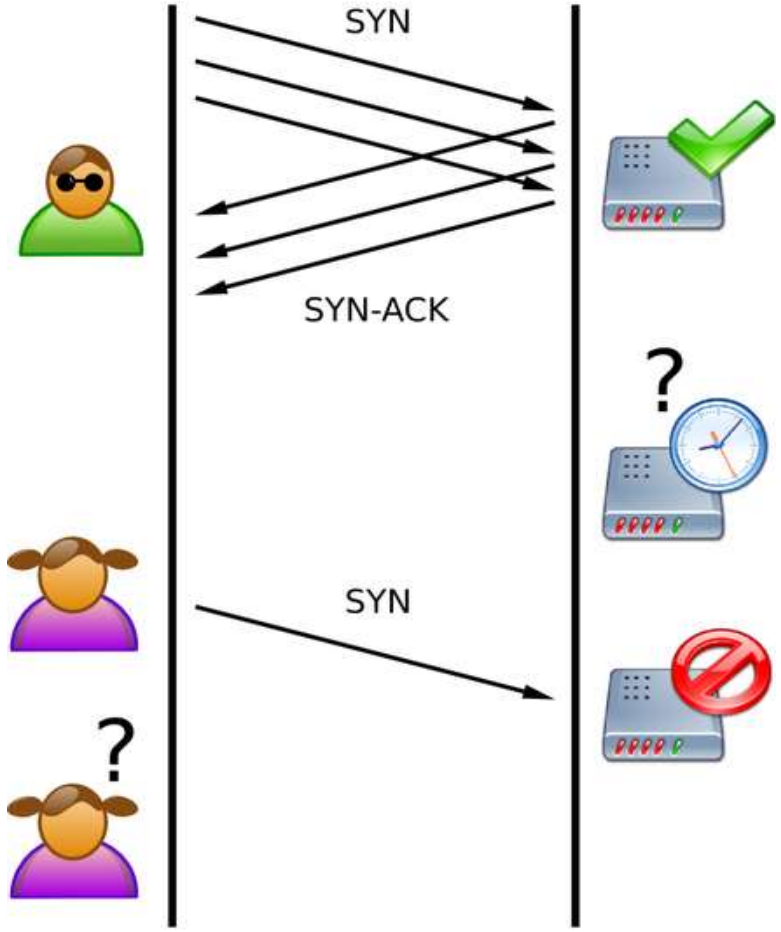
ICMP攻击

- **ping洪水攻击**：通过功能强大的计算机向单个受害服务器发送大量回显请求(echo request)命令。这样受害服务器会被这些网络流量淹没，无法响应合法的请求。
- **Smurf攻击：**攻击者向网络广播地址发送ICMP包，并将回复地址设置成受害网络的广播地址，通过使用ICMP应答请求数据包来淹没受害主机的方式进行。
- **如何阻止Smurf攻击：**(1)管理员应该将网络中的主机和路由器配置为忽略广播请求；(2) 避免直接向广播地址转发数据包；(3) 忽略ping请求。

SYN洪水攻击



正常情况下TCP三次握手过程



SYN洪水攻击时的握手过程

SYN洪水攻击

- 攻击者故意延迟或不发送握手确认消息。
- 假设连接发起方是A，接受方是B。A发送SYN消息给B，B反馈SYN-ACK消息给A，使连接进入半开状态。此时B会给每个半开连接都设一个Timer，如果超过时间还没有收到A的ACK消息，则重新发送一次SYN-ACK消息给A，直到重试超过一定次数时才会放弃。
- B维护半开连接需要分配内核资源，如果A发送大量的SYN消息给B而不回复ACK时，SYN Flood攻击就形成了。
- 攻击方A可以控制肉鸡向B发送大量SYN消息但不响应ACK消息，或者干脆伪造SYN消息中的Source IP，使B反馈的SYN-ACK消息石沉大海，导致B被大量注定不能完成的半开连接占据，直到资源耗尽，停止响应正常的连接请求。

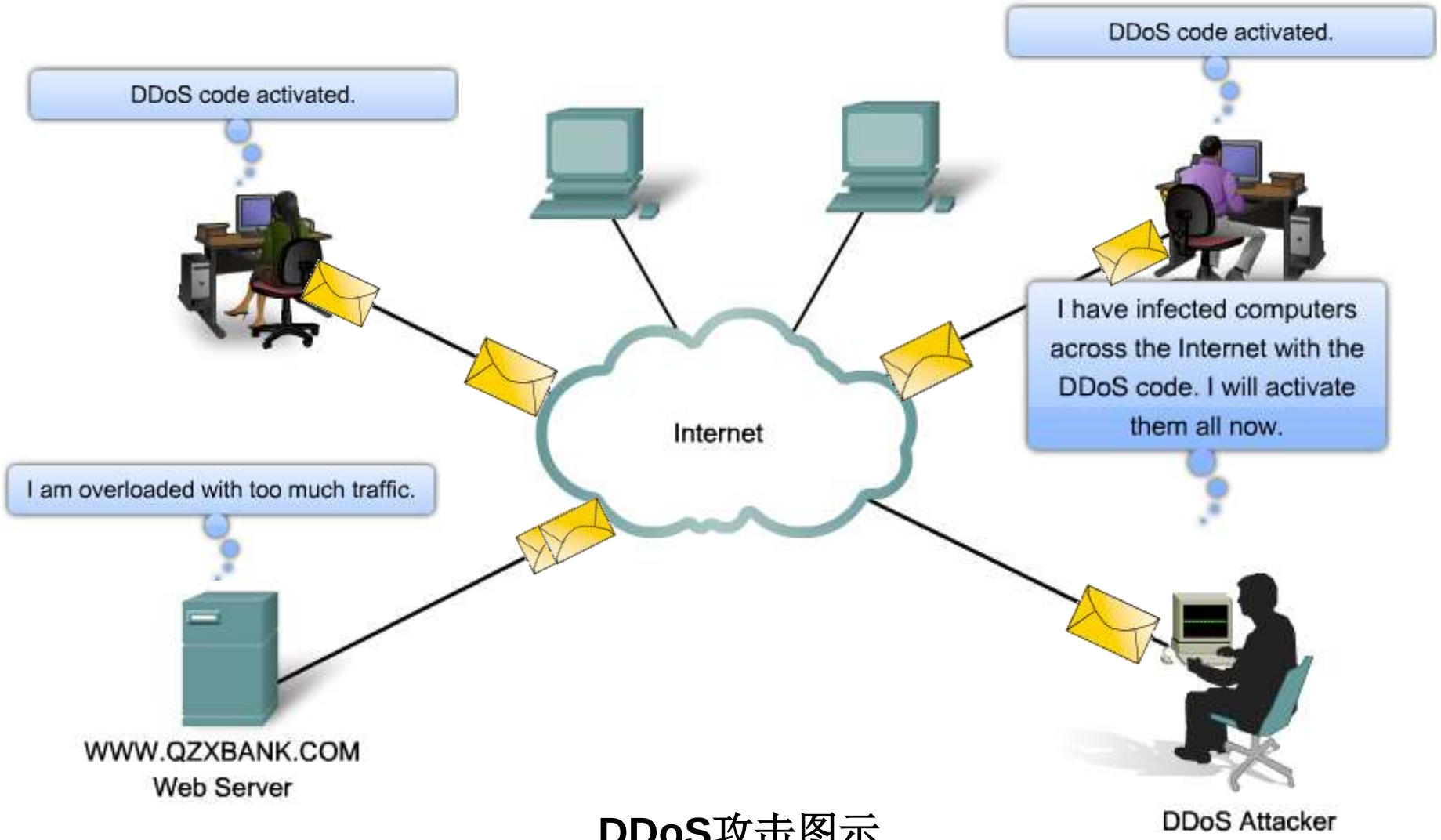
防范SYN洪水攻击

- SYN Cookie机制：在TCP服务器接收到TCP SYN包并返回TCP SYN+ACK包时，不分配专门的数据区，而是根据SYN包计算一个cookie值。 这个cookie作为将要返回的SYN ACK包的初始序列号。
- SYN + ACK包的32比特结构如下：(1) 前5比特是时间戳，由每分钟按模32递增的计数器实现。(2) 中间3比特是编码值，表示传输段的最大值。(3) 最后24比特是基于密钥k，由服务器和客户端IP地址，端口号和前面使用的时间戳计算出来的MAC值。
- 当客户端返回一个ACK包时，服务器首先根据其前5比特判断是否过期；其次服务器根据包头信息重新计算24比特的MAC值，与返回的确认序列号(初始序列号 + 1)进行对比；最后，服务器对中间3比特进行解码，完成对SYN队列项的重构。如果验证通过，则服务器发起TCP会话。

Optimistic TCP ACK攻击

- 该攻击利用TCP协议的拥塞控制机制。在TCP的滑动窗口协议中，随着接收ACK的增多，窗口的大小会增大。
- 恶意客户端试图使服务器增加自身的发送速率，直至服务器的带宽耗尽。如果同时针对多台服务器进行TCP ACK攻击，它会通过淹没网络带宽资源，导致互联网范围内的拥塞。
- 恶意客户端在没有收到SYN-ACK时，就提前发送ACK，使得服务器增加其传输速度。
- 防御TCP ACK攻击：通过在服务器端实现对每个客户端最大流量的限制可以缓解这种攻击，也能及时阻止来自客户端的拒绝服务攻击流量。

分布式拒绝服务攻击DDoS



DDoS攻击图示

小结

- 网络基本概念
  - 网络拓扑、因特网协议、相关安全问题
- 链路层
  - 以太网、MAC地址、ARP欺骗
- 网络层
  - IP、ICMP、IP欺骗、网络包嗅探
- 传输层
  - TCP、UDP、NAT、TCP会话劫持
- 拒绝服务攻击

- 习题

  R-5.10 R-5.15 R-5.16

  C-5.7

本章结束

~End~

但行好事，莫問前程。
Those that can, do.
Those that cannot,
complain.