网络通信协议

关键词:OSI 模型, 网络通信模型, 网络通信协议

摘要: OSI 模型以及其它任何网络通信模型，都只提供了计算机间通信的概念框架，而模型本身并不提供相关的通信方法。实质的通信是由多种通信协议来定义的。从数据通信来理解，协议是一组正式的规则、协定和数据结构，它们控制计算机以及其它网络设备如何在网络上交换信息。换句话说，协议是一种标准的程序和格式，是两个数据通信设备必需能夠互相理解、接收和交谈的。

OSI 模型以及其它任何网络通信模型，都只提供了计算机间通信的概念框架，而模型本身并不提供相关的通信方法。实质的通信是由多种通信协议来定义的。从数据通信来理解，协议是一组正式的规则、协定和数据结构，它们控制计算机以及其它网络设备如何在网络上交换信息。换句话说，协议是一种标准的程序和格式，是两个数据通信设备必需能夠互相理解、接收和交谈的。

当前，根据 OSI 七层模型或类似的分层模型，协议都是设计为分层模式的。分层是一种设计原则，它将协议设计为许多小部分，每一部分完成各个具体的子任务，并通过一些明确的方式与其它协议互操作。分层法允许设计和测试部分协议，而不用将协议全部更改，这样就保持每个设计相对简单。同时分层法允许常见的协议可以应用在异常情形中。

各层的协议头和协议尾体现了协议结构。协议或协议组的详细规则和过程通常由篇幅较长的文件定义而成。例如，IETF 使用 RFC （请求注解）文件定义和更新协议。

现有的大量通信协议，是由很多遍及世界的不同标准组织以及历经多年技术演变和发展的技术提供商制定而成。其中一种最通用的是 TCP/IP 协议，它是 Internet 网络通信的核心。IP，网际协议，主要负责路由器间的信息交换，确保路由器可以为网络流量选择正确的路径；而 TCP 负责确保数据包在网络上的可靠以及无错误的传输。局域网和广域网协议都是很重要的网络通信协议。LAN 协议适用于有多种 LAN 介质的物理层和数据链路层的通信，如以太网线和无线电波；WAN 协议适用于底三层，并定义了在多种广域媒体上的通信，如光纤和铜缆。

网络通信一直在逐渐的演绎和发展， 当今的新技术是以往多年技术积累的成果，其中有些还一直使用着，有些则已被淘汰。正因为此，网络通信协议之间都是戚戚相关的。许多协议的实现是依赖于其它协议。例如，许多路由选择协议需要结合其它网络协议进行路由器之间的信息交换。

除了传输过程中的独立协议标准，现在还有些关于不同层与各自上下层（通常与操作系统有关）之间对话的接口标准。例如，位于第 4 层与第 5 层间的 Winsock 和 Berkeley 套接字，位于第 2 层与第 3 层间的 NDIS （网络驱动器接口标准）和 ODI （开放式数据链路接口）。

数据通信协议覆盖了在 OSI 模型中说明的所有区域。然而，OSI 模型对此只作了简单说明。一种协议可能完成 OSI 层的一种或多种功能，因此造成了对 OSI 七层模型相关协议理解的复杂性。在现实的协议中，关于如何界定各层仍存在些争议，目前仍没有明确而统一的结论。

为了发展有益于产业的一项完整技术，通常需要在相同层或不同层间定义协议组。不同协议通常描述了一类通信的不同方面，这些协议在一起形成一个协议集。例如，IP 传送话音（VOIP），是由众多厂商和标准组织开发的一组协议，其中含盖了很多用于 OSI 模型上面四层的协议。

协议的实现既可以在硬件上也可以在软件上完成，还可以综合两者完成。一般而言，下层协议在硬件上实现，而上层协议在软件上实现。

协议，根据技术功能或协议导入由来或兼于以上两者可以组成一个集（族或栈）。一种协议可能属于一个或多个协议集，这取决于你如何分类。例如，千兆以太网协议 IEEE802.3z 就是一个局域网协议（LAN），但 同时它也能用于 MAN （城域网）通信 。

目前用于 Internet 网络通信的大多数协议都是由 IETF 制定而成，而应用于 LAN 和 MAN 的都是由 IEEE 制定的。ITU-T 为 WAN 和电信通讯协议的制定做出了较大贡献。ISO 拥有自己的一套 Internet 网络通信协议集，其主要应用在一些欧洲国家。

协议组

TCP/IP Security/VPN VOIP LAN MAN WAN SAN ISO SS7/C7 Mobile/Wireless WLAN
Cisco 思科 IBM Microsoft 微软 Novell Apple 苹果 HP/DEC 惠普 Sun 其他 RFC
网络协议词典

常用协议

IP TCP UDP IPsec HTTP POP3 SNMP MPLS SMTP DNS

TCP/IP 协议 （传输控制协议/网间协议）

TCP/IP 协议集确立了 Internet 的技术基础。TCP/IP 的发展始于美国 DOD （国防部）方案。 IAB （Internet 架构委员会）的下属工作组 IETF （Internet 工程任务组）研发了其中多数协议。 IAB 最初由美国政府发起，如今转变为公开而自治的机构。IAB 协同研究和开发 TCP/IP 协议集的底层结构，并引导着 Internet 的发展。TCP/IP 协议集记录在请求注解（RFC）文件中，RFC 文件均由 IETF 委员会起草、讨论、传阅及核准。所有这些文件都是公开且免费的，且能在 IETF 网站上列出的参考文献中找到。

TCP/IP 协议覆盖了 OSI 网络结构七层模型中的六层，并支持从交换（第二层）诸如多协议标记交换，到应用程序诸如邮件服务方面的功能。TCP/IP 的核心功能是寻址和路由选择（网络层的 IP/IPV6 ）以及传输控制（传输层的 TCP、UDP）。

IP （网际协议）

在网络通信中，网络组件的寻址对信息的路由选择和传输来说是相当关键的。相同网络中的两台机器间的消息传输有各自的技术协定。LAN 是通过提供 6 字节的唯一标识符（“MAC”地址）在机器间发送消息的。SNA 网络中的每台机器都有一个逻辑单元及与其相应的网络地址。DECNET、AppleTalk 和 Novell IPX 均有一个用来分配编号到各个本地网和工作站的配置。

除了本地或特定提供商的网络地址，IP 为世界范围内的各个网络设备都分配了一个唯一编号，即 IP 地址。IPV4 的 IP 地址为 4 字节，按照惯例，将每个字节转化成十进制（0-255）并以点分隔各字节。IPV6 的 IP 地址已经增加到 16 字节。关于 IP 和 IPV6 协议的详细说明，在相关文件中再另作介绍。

TCP （传输控制协议）

通过序列化应答和必要时重发数据包，TCP 为应用程序提供了可靠的传输流和虚拟连接服务。TCP 主要提供数据流转送，可靠传输，有效流控制，全双工操作和多路传输技术。可查阅 TCP 部分获取更多详细资料。

在下面的 TCP/IP 协议表格中，我们根据协议功能和其在 OSI 七层网络通信参考模型的映射关系将其全部列出。然而，TCP/IP 并不完全遵循 OSI 模型，例如：大多数 TCP/IP 应用程序是直接在传输层协议 TCP 和 UDP 上运行，而不涉及其中的表示层和会话层。

主要协议表

IP TCP UDP IPsec HTTP POP3 SNMP MPLS DNS SMTP

应用层（Application Layer）

- BOOTP：引导协议 （BOOTP：Bootstrap Protocol）
- DCAP：数据转接客户访问协议 （DCAP：Data Link Switching Client Access Protocol）
- DHCP：动态主机配置协议 （DHCP：Dynamic Host Configuration Protocol）
- DNS：域名系统（服务）系统 （DNS：Domain Name Systems）
- Finger：用户信息协议 （Finger：User Information Protocol）
- FTP：文件传输协议 （FTP：File Transfer Protocol）
- HTTP：超文本传输协议 （HTTP：Hypertext Transfer Protocol）
- S-HTTP：安全超文本传输协议 （S-HTTP：Secure Hypertext Transfer Protocol）
- IMAP & IMAP4：信息访问协议 & 信息访问协议第 4 版 （IMAP & IMAP4：Internet Message Access Protocol）
- IPDC：IP 设备控制 （IPDC：IP Device Control）
- IRCP/IRC：因特网在线聊天协议 （IRCP/IRC：Internet Relay Chat Protocol）
- LDAP：轻量级目录访问协议 （LDAP：Lightweighted Directory Access Protocol）
- MIME/S-MIME/Secure MIME：多用途网际邮件扩充协议 （MIME/S-MIME/Secure MIME：Multipurpose Internet Mail Extensions）
- NAT：网络地址转换 （NAT：Network Address Translation）
- NNTP：网络新闻传输协议 （NNTP：Network News Transfer Protocol）
- NTP：网络时间协议 （NTP：Network Time Protocol）
- POP&POP3：邮局协议 （POP & POP3：Post Office Protocol）
- RLOGIN：远程登录命令 （RLOGIN：Remote Login in Unix）
- RMON：远程监控 （RMON：Remote Monitoring MIBs in SNMP）
- RWhois：远程目录访问协议 （RWhois Protocol）
- SLP：服务定位协议 （SLP：Service Location Protocol）
- SMTP：简单邮件传输协议 （SMTP：Simple Mail Transfer Protocol）
- SNMP：简单网络管理协议 （SNMP：Simple Network Management Protocol）
- SNTP：简单网络时间协议 （SNTP：Simple Network Time Protocol）
- TELNET：TCP/IP 终端仿真协议 （TELNET：TCP/IP Terminal Emulation Protocol）
- TFTP：简单文件传输协议 （TFTP：Trivial File Transfer Protocol）
- URL：统一资源管理 （URL：Uniform Resource Locator）
- X-Window/X Protocol：X 视窗 或 X 协议（X-Window：X Window or X Protocol or X System）

表示层（Presentation Layer）

- LPP：轻量级表示协议 （LPP：Lightweight Presentation Protocol）

会话层（Session Layer）

- RPC：远程过程调用协议 （RPC：Remote Procedure Call protocol）

传输层（Transport Layer）

- ITOT：基于 TCP/IP 的 ISO 传输协议 （ITOT：ISO Transport Over TCP/IP）
- RDP：可靠数据协议 （RDP：Reliable Data Protocol）
- RUDP：可靠用户数据报协议 （RUDP：Reliable UDP）
- TALI：传输适配层接口 （TALI：Transport Adapter Layer Interface）
- TCP：传输控制协议 （TCP：Transmission Control Protocol）
- UDP：用户数据报协议 （UDP：User Datagram Protocol）
- Van Jacobson：压缩 TCP 协议 （Van Jacobson：Compressed TCP）

网络层（Network Layer）

路由选择（Routing）

- BGP/BGP4：边界网关协议 （BGP/BGP4：Border Gateway Protocol）
- EGP：外部网关协议（EGP：Exterior Gateway Protocol）
- IP：网际协议 （IP：Internet Protocol）
- IPv6：网际协议第 6 版 （IPv6：Internet Protocol version 6）
- ICMP/ICMPv6：Internet 信息控制协议 （ICMP/ICMPv6：Internet Control Message Protocol）
- IRDP：ICMP 路由器发现协议 （IRDP：ICMP Router Discovery Protocol）
- Mobile IP： 移动 IP （Mobile IP：IP Mobility Support Protocol for IPv4 & IPv6）
- NARP：NBMA 地址解析协议 （NARP：NBMA Address Resolution Protocol）
- NHRP：下一跳解析协议 （NHRP：Next Hop Resolution Protocol）
- OSPF：开放最短路径优先 （OSPF：Open Shortest Path First）
- RIP/RIP2：路由选择信息协议 （RIP/RIP2：Routing Information Protocol）
- RIPng：路由选择信息协议下一代 （RIPng：RIP for IPv6）
- RSVP：资源预留协议 （RSVP：Resource ReSerVation Protocol）
- VRRP：虚拟路由器冗余协议 （VRRP：Virtual Router Redundancy Protocol）

组播（Multicast）

- BGMP：边界网关组播协议 （BGMP：Border Gateway Multicast Protocol）
- DVMRP：距离矢量组播路由协议 （DVMRP：Distance Vector Multicast Routing Protocol）
- IGMP：Internet 组管理协议 （IGMP：Internet Group Management Protocol）

- MARS：组播地址解析服务 （MARS：Multicast Address Resolution Server）
- MBGP：组播协议边界网关协议 （MBGP：Multiprotocol BGP）
- MOSPF：组播 OSPF （MOSPF：Multicast OSPF）
- MSDP：组播源发现协议 （MSDP：Multicast Source Discovery Protocol）
- MZAP：组播区域范围公告协议 （MZAP：Multicast Scope Zone Announcement Protocol）
- PGM：实际通用组播协议 （PGM：Pragmatic General Multicast Protocol）
- PIM-DM：密集模式独立组播协议 （PIM-DM：Protocol Independent Multicast - Dense Mode）
- PIM-SM：稀疏模式独立组播协议 （PIM-SM：Protocol Independent Multicast - Sparse Mode）

MPLS 协议（MPLS Protocols）

- CR-LDP：基于路由受限标签分发协议 （CR-LDP: Constraint-Based Label Distribution Protocol）
- GMPLS：通用多协议标志交换协议 （GMPLS：Generalized Multiprotocol Label Switching）
- LDP：标签分发协议 （LDP：Label Distribution Protocol）
- MPLS：多协议标签交换 （MPLS：Multi-Protocol Label Switching）
- RSVP-TE:基于流量工程扩展的资源预留协议（RSVP-TE:Resource ReSerVation Protocol-Traffic Engineering）

数据链路层（Data Link Layer）

- ARP and InARP:地址转换协议和逆向地址转换协议（ARP and InARP:Address Resolution Protocol and Inverse ARP）
- IPCP and IPv6CP：IP 控制协议和 IPV6 控制协议 （IPCP and IPv6CP：IP Control Protocol and IPv6 Control Protocol）
- RARP：反向地址转换协议 （RARP：Reverse Address Resolution Protocol）
- SLIP：串形线路 IP （SLIP：Serial Line IP）

TCP：传输控制协议

（TCP：Transmission Control Protocol）

传输控制协议 TCP 是 TCP/IP 协议栈中的传输层协议，它通过序列确认以及包重发机制，提供可靠的数据流发送和到应用程序的虚拟连接服务。与 IP 协议相结合， TCP 组成了因特网协议的核心。

由于大多数网络应用程序都在同一台机器上运行，计算机上必须能够确保目的地机器上的软件程序能从源地址机器处获得数据包，以及源计算机能收到正确的回复。这是通过使用 TCP 的“端口号”完成的。网络 IP 地址和端口号结合成为唯一的标识 ， 我们称之为“套接字”或“端点”。 TCP 在端点间建立连接或虚拟电路进行可靠通信。

TCP 服务提供了数据流传输、可靠性、有效流控制、全双工操作和多路复用技术等。

关于流数据传输 ,TCP 交付一个由序列号定义的无结构的字节流。 这个服务对应用程序有利，因为在送出到 TCP 之前应用程序不需要将数据划分成块， TCP 可以将字节整合成字段，然后传给 IP 进行发送。

TCP 通过面向连接的、端到端的可靠数据报发送来保证可靠性。 TCP 在字节上加上一个递进的确认序列号来告诉接收者发送者期望收到的下一个字节。如果在规定时间内，没有收到关于这个包的确认响应，重新发送此包。 TCP 的可靠机制允许设备处理丢失、延时、重复及读错的包。超时机制允许设备监测丢失包并请求重发。

TCP 提供了有效流控制。当向发送者返回确认响应时，接收 TCP 进程就会说明它能接收并保证缓存不会发生溢出的最高序列号。

全双工操作： TCP 进程能够同时发送和接收包。

TCP 中的多路技术：大量同时发生的上层会话能在单个连接上时进行多路复用。

协议结构

<table>
<tr><th colspan="8">16</th><th>32 bit</th></tr>
<tr><td colspan="8">Source port</td><td>Destination port</td></tr>
<tr><td colspan="9">Sequence number</td></tr>
<tr><td colspan="9">Acknowledgement number</td></tr>
<tr><td>Offset</td><td>Reserved</td><td>U</td><td>A</td><td>P</td><td>R</td><td>S</td><td>F</td><td>Window</td></tr>
<tr><td colspan="8">Checksum</td><td>Urgent pointer</td></tr>
<tr><td colspan="9">Option + Padding</td></tr>
<tr><td colspan="9">Data</td></tr>
</table>

- Source Port - 识别上层源处理器接收 TCP 服务的点。
- Destination Port - 识别上层目标处理器接收 TCP 服务的点。
- Sequence Number - 通常指定分配到当前信息中的数据首字节的序号。在连接建立阶段，该字段用于设别传输中的初始序列号。
- Acknowledgment Number - 包含数据包发送端期望接收的数据下一字节的序列号。一旦连接成功，该值会一直被发送。
- Data Offset - 4 位。TCP 协议头中的 32 位字序号表示数据开始位置。
- Reserved - 6 位。预留以备用，必须设置为 0。
- Control Bits （Flags） - 6 位。传送各种控制信息。控制位可以是：

U （URG）	Urgent pointer field significant.
A （ACK）	Acknowledgment field significant.
P （PSH）	Push function.

R （RST）	Reset the connection.
S （SYN）	Synchronize sequence numbers.
F （FIN）	No more data from sender.

- Window - 16 位。指定发送端接收窗口的大小，也就是说，数据可用的八位缓存区大小。
- Checksum - 16 位。指出协议头在传输中是否遭到破坏。
- Urgent Pointer - 16 位。指向数据包中的第一个重要数据字节。
- Option + Padding - 指定各种 TCP 选项。可选项有两种可能形式：单个八位可选类型和八位可选类型，八位可选长度和实际可选数据八位位组。
- Data - 包含上层信息。

IP/IPv4：网际协议

（IP/IPv4：Internet Protocol）

网际协议（IP）是一个网络层协议，它包含寻址信息和控制信息 ，可使数据包在网络中路由。IP 协议是 TCP/IP 协议族中的主要网络层协议，与 TCP 协议结合组成整个因特网协议的核心协议。IP 协议同样都适用于 LAN 和 WAN 通信。

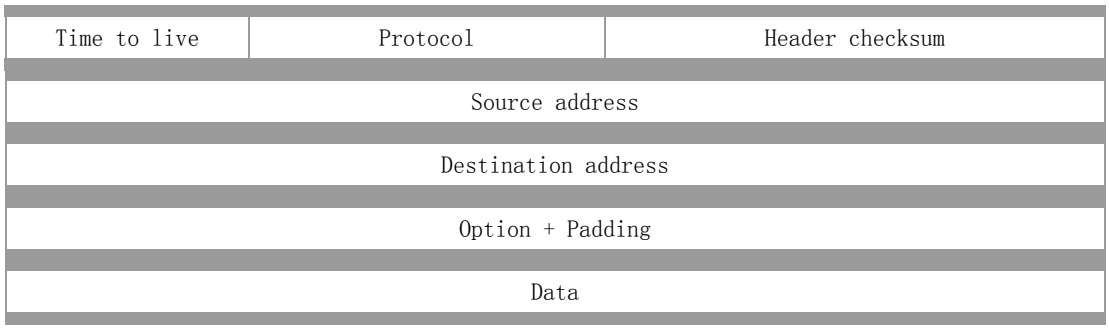
IP 协议有两个基本任务：提供无连接的和最有效的数据包传送；提供数据包的分割及重组以支持不同最大传输单元大小的数据连接。对于互联网络中 IP 数据报的路由选择处理，有一套完善的 IP 寻址方式。每一个 IP 地址都有其特定的组成但同时遵循基本格式。IP 地址可以进行细分并可用于建立子网地址。TCP/IP 网络中的每台计算机都被分配了一个唯一的 32 位逻辑地址，这个地址分为两个主要部分：网络号和主机号。网络号用以确认网络，如果该网络是因特网的一部分，其网络号必须由 InterNIC 统一分配。一个网络服务器供应商（ISP）可以从 InterNIC 那里获得一块网络地址，按照需要自己分配地址空间。主机号确认网络中的主机，它由本地网络管理员分配。

当你发送或接受数据时(例如,一封电子信函或网页),消息分成若干个块,也就是我们所说的“包”。每个包既包含发送者的网络地址又包含接受者的地址。由于消息被划分为大量的包，若需要，每个包都可以通过不同的网络路径发送出去。包到达时的顺序不一定和发送顺序相同， IP 协议只用于发送包，而 TCP 协议负责将其按正确顺序排列。

除了 ARP 和 RARP，其它所有 TCP/IP 族中的协议都是使用 IP 传送主机与主机间的通信。当前 IP 协议有两种版本：IPv4 和 IPv6。本文主要阐述 IPv4 。IPv6 的相关细节将在其它文件中再作介绍。

协议结构

4	8	16	32bit
Version	IHL	Type of service	Total length
Identification		Flags	Fragment offset



- Version — 4 位字段，指出当前使用的 IP 版本。
- IP Header Length （IHL） — 指数据报协议头长度，具有 32 位字长。指向数据起点。正确协议头最小值为 5。
- Type-of-Service — 指出上层协议对处理当前数据报所期望的服务质量，并对数据报按照重要性级别进行分配。这些 8 位字段用于分配优先级、延迟、吞吐量以及可靠性。
- Total Length — 指定整个 IP 数据包的字节长度，包括数据和协议头。其最大值为 65,535 字节。典型的主机可以接收 576 字节的数据报。
- Identification — 包含一个整数，用于识别当前数据报。该字段由发送端分配帮助接收端集中数据报分片。
- Flags — 由 3 位字段构成，其中低两位（最不重要）控制分片。低位指出数据包是否可进行分片。中间位指出在一系列分片数据包中数据包是否是最后的分片。第三位即最高位不使用。
- Fragment Offset — 13 位字段，指出与源数据报的起始端相关的分片数据位置，支持目标 IP 适当重建源数据报。
- Time-to-Live — 是一种计数器，在丢弃数据报的每个点值依次减 1 直至减少为 0。这样确保数据包无止境的环路过程。
- Protocol — 指出在 IP 处理过程完成之后，有哪种上层协议接收导入数据包。
- Header Checksum — 帮助确保 IP 协议头的完整性。由于某些协议头字段的改变，如生存期（Time to Live），这就需要对每个点重新计算和检验。Internet 协议头需要进行处理。
- Source Address — 指定发送代码。
- Destination Address — 指定接收代码。
- Options — 允许 IP 支持各种选项，如安全性。
- Data — 包括上层信息。

IPv6/IPng：网际协议第 6 版

（IPv6/IPng：Internet Protocol Version 6）

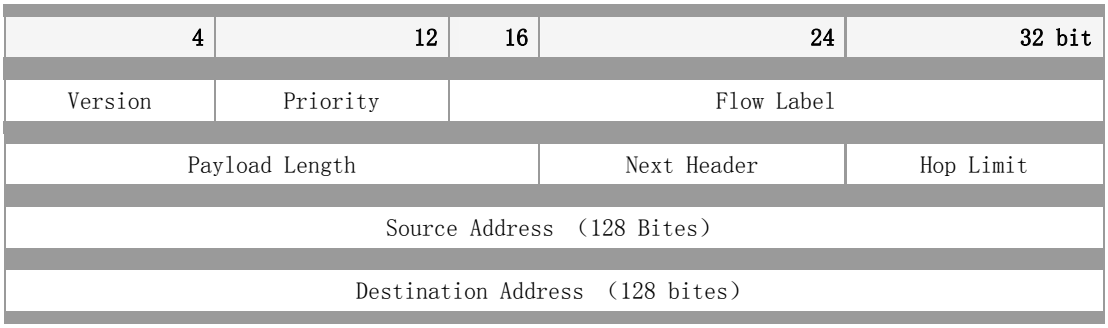
网际协议第 6 版（IPv6）是基于 IPv4 的最新版本， Ipv4 是一个网络层协议，它包含寻址信息和一些控制信息，可使数据包在网络中路由。IP 协议有两种版本：IPv4 和 IPv6，其中 IPv6 也被称之为下一代 IP 或 IPng。IPv4 和 IPv6 都是关于介质层的去复用技术。例如，在 IPv6 中，在以太网上传送数据包采用的是 86DD （十六进制），IPv4 用的是 0800。本文主要介绍 IPv6 细节，有关 IP 和 IPv4 的内容在个别文件中另作介绍。

IPv6 把 IP 地址从 32 位增至 128 位，可以支持更多的寻址层次，更大数量的节点，以及更简单的地址自动配置，引入了组播地址的可缩放性，又定义了一个叫做“任意播”（anycast） 的新地址类

型， 用于给任意节点组发送数据包。相对于 IPv4，IPv6 主要有两个方面的改进：

- 支持扩展和选项的改进 — Ipv6 选项位于 IPv6 头和传输层头之间的单独协议头中。IP 首部选项编码方式的改变使得传输过程更为高效，选项长度限制更少并且添加新选项更为灵活。扩展的头包括下一跳选项、路由选择、片断、目的选项、认证和封装负荷。
- 数据流标签能力 — 标签属于不同流量的数据包，用于发送端提出特殊处理请求，比如：非缺省服务质量或者“实时”服务。

协议结构



- Version — 网际协议版本号（IPv6 是第 6 版）；
- Priority — 流量类字段，识别发送数据包的优先权。优先权值的划分根据信息源提供拥塞控制和非拥塞流量控制的流量进行；
- Flow Label — 流标签用于信息源为需要特殊处理 IPv6 路由器的产品进行标签。该流由源地址和非零流标签共同唯一识别；
- 有效负载长度 — 有效负载长度包括协议头；
- Next Header — 迅速识别 IPv6 协议头后面的协议头类型；
- Hop Limit — 每个节点在转发数据包时的消耗。如果 Hop limit 消耗到 0，则取消数据包；
- Source Address — 数据包发送端 128 比特地址；
- Destination Address — 数据包的设定接收端 128 比特地址（未必是终点接收端）。

IPsec：IP 层协议安全结构

（IPsec：Security Architecture for IP network）

IPsec 在 IP 层提供安全服务，它使系统能按需选择安全协议，决定服务所使用的算法及放置需求服务所需密钥到相应位置。IPsec 用来保护一条或多条主机与主机间、安全网关与安全网关间、安全网关与主机间的路径。

IPsec 能提供的安全服务集包括访问控制、无连接的完整性、数据源认证、拒绝重发包（部分序列完整性形式）、保密性和有限传输流保密性。因为这些服务均在 IP 层提供，所以任何高层协议均能使用它们，例如 TCP、UDP、ICMP、BGP 等等。

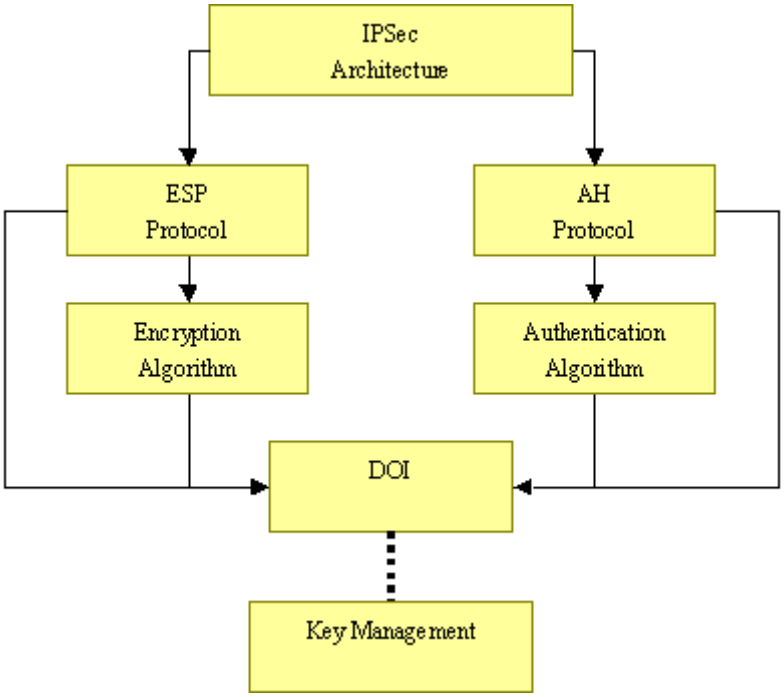
这些目标是通过使用两大传输安全协议，头部认证（AH） 和封装安全负载 （ESP），以及密钥管理程序和协议的使用来完成的。所需的 IPsec 协议集内容及其使用的方式是由用户、应用程序、和/或站点、组织对安全和系统的需求来决定。

当正确的实现、使用这些机制时，它们不应该对不使用这些安全机制保护传输的用户、主机和其他英特网部分产生负面的影响。这些机制也被设计成算法独立的。这种模块性允许选择不同的算法集而不影响其他部分的实现。例如：如果需要，不同的用户通讯可以采用不同的算法集。

定义一个标准的默认算法集可以使得全球因英特网更容易协同工作。这些算法辅以 IPsec 传输保护和密钥管理协议的使用为系统和应用开发者部署高质量的因特网层的加密的安全技术提供了途径。

协议结构 — IPsec：IP 网络安全结构

IPsec 结构包括众多协议和算法。这些协议之间的相互关系如下所示：



IPsec：IP 层协议安全结构

有关每个协议的具体细节，请参考个别文件。

HTTP：超文本传输协议

HTTP：Hypertext Transfer Protocol

超文本传输协议（HTTP）是应用层协议，由于其简捷、快速的方式，适用于分布式和合作式超媒体信息系统。自 1990 年起，HTTP 就已经被应用于 WWW 全球信息服务系统。

HTTP 允许使用自由答复的方法表明请求目的，它建立在统一资源识别器（URI）提供的参考原则下，

作为一个地址（URL）或名字（URN），用以标志采用哪种方法，它用类似于网络邮件和多用途网际邮件扩充协议（MIME）的格式传递消息。

HTTP 也可用作普通协议，实现用户代理与连接其它 Internet 服务（如 SMTP、NNTP、FTP、 GOPHER 及 WAIS）的代理服务器或网关之间的通信，允许基本的超媒体访问各种应用提供的资源，同时简化了用户代理系统的实施。

HTTP 是一种请求/响应式的协议。一个客户机与服务器建立连接后，发送一个请求给服务器，请求的格式是：统一资源标识符（URI）、协议版本号，后面是类似 MIME 的信息，包括请求修饰符、客户机信息和可能的内容。服务器接到请求后，给予相应的响应信息，其格式是：一个状态行包括信息的协议版本号、一个成功或错误的代码，后面也是类似 MIME 的信息，包括服务器信息、实体信息和可能的内容。

HTTP 的第一版本 HTTP/0.9 是一种简单的用于网络间原始数据传输的协议。而由 RFC 1945 定义的 HTTP/1.0 ，在原 HTTP/0.9 的基础上，有了进一步的改进，允许消息以类 MIME 信息格式存在，包括请求/响应范式中的已传输数据和修饰符等方面的信息。但是，HTTP/1.0 没有充分考虑到分层代理服务器、高速缓冲存储器、持久连接需求或虚拟主机等方面的效能。相比之下，HTTP/1.1 要求更加严格以确保服务的可靠性。关于安全增强版的 HTTP （即 S-HTTP），将在相关文件中再作介绍。

协议结构

HTTP 报文由从客户机到服务器的请求和从服务器到客户机的响应构成。 请求报文格式如下：

请求行	通用信息头	请求头	实体头	报文主体

请求行以方法字段开始，后面分别是 URL 字段和 HTTP 协议版本字段，并以 CRLF 结尾。SP 是分隔符。除了在最后的 CRLF 序列中 CF 和 LF 是必需的之外，其他都可以不要。有关通用信息头，请求头和实体头方面的具体内容可以参照相关文件。

应报文格式如下：

状态行	通用信息头	响应头	实体头	报文主体

状态码元由 3 位数字组成，表示请求是否被理解或被满足。原因分析是对原文的状态码作简短的描述，状态码用来支持自动操作，而原因分析用来供用户使用。客户机无需用来检查或显示语法。有关通用信息头，响应头和实体头方面的具体内容可以参照相关文件。